Response from the UK Computing Research Committee (UKCRC) to the review of the legislative and regulatory framework for testing driverless cars: discussion document and call for evidence

http://www.ukcrc.org.uk/

The UK Computing Research Committee (UKCRC), an Expert Panel of the British Computer Society, the Institution of Engineering and Technology and the Council of Professors and Heads of Computing, was formed in November 2000 as a policy committee for computing research in the UK. Its members are leading computing researchers who each have an established international reputation in computing. Our response thus covers UK research in computing, which is internationally strong and vigorous, and a major national asset. This response has been prepared after a widespread consultation amongst the membership of UKCRC.

UKCRC would be pleased to clarify or expand this response if required.

Introduction

UKCRC recognises the opportunity for increased vehicle automation to greatly reduce the deaths and injuries caused by road accidents. We believe that progress towards full automation is desirable and inevitable and that this represents a significant opportunity for the UK to contribute to international safety standards and to win a substantial share of the automated vehicle market.

Driverless vehicles should be seen as part of a complex, safety-critical system that includes the driverless vehicles, other vehicles with drivers, passengers, pedestrians, other road users, and all the electronic, physical and human systems on which safe automated behaviour depends.

The UK has particular expertise in assuring the dependability of complex socio-technical systems such as this. UKCRC would like to emphasise the importance of taking a whole-system view of the issues and of being rigorous in identifying the requirements and the assurance criteria.

The consultation

The consultation addresses a range of issues related to the *testing* of driverless vehicles.

UKCRC believes that testing will be essential at several points in the development and certification of fully autonomous vehicles but that it would be unprofessional to undertake a test programme without first identifying, clearly, unambiguously and in detail, what questions the testing is required to answer. Without this clarity, it will be unclear:

- whether testing is able to provide the required answers at all, or with the required confidence;
- whether testing is the most cost-effective way to provide the required answers; and
- how much testing, of what sort, and under what conditions, could provide the required answers.

Testing cannot feasibly demonstrate the *absence* of unsafe behaviour. Testing is already hitting limits of effectiveness because cars already contain so many different software systems, from many firms in the supply chain, that interact concurrently. Electronic Control Units from tier 1 and lower are effectively integrated into the car as black boxes.

The current consultation addresses issues related to testing that involves high automation vehicles, but it is important to set such testing in context, because it would be inappropriate (and could be unlawful) to put such vehicles on UK roads if (a) doing so increases the risk to other road users and (b) the questions addressed by the testing could be answered in other, reasonably practicable ways. Much of the work that the UK will need to do to prepare for driverless vehicles on UK roads need not involve actual driverless vehicles; for example,

- deciding certification requirements
- deciding liability issues
- deciding the level of autonomy and the circumstances under which the vehicle must remain or become under human control (i.e. what decisions when "driving" is the vehicle responsible for and what decisions must the human driver still take?)
- setting standards for data capture, data recording, data formats and related issues to facilitate market competition and to permit independent analysis following an incident.
- Exploration of the variety of road topologies, weather conditions and other environmental conditions in which the sensors and control algorithms will have to operate successfully.
- Establishing the resilience of the vehicle behaviour to deliberate or accidental interference with the sensor inputs, to GNSS (eg GPS) signals and mapping data, and to cybersecurity attacks through other channels.
- … and many other issues that can be determined through analysis, simulation, evaluation in a vehicle with a human driver, expert review etc.

Driverless cars are an example of a robot and EPSRC has published a set of guidelines for robot design, including this principle: "Humans, not robots, are responsible agents. Robots should be designed; operated as far as is practicable to comply with existing laws & fundamental rights & freedoms, including privacy." See
http://www.epsrc.ac.uk/research/ourportfolio/themes/engineering/activities /principlesofrobotics/

The consultation questions.

UKCRC has only responded to questions where our expertise in sociotechnical systems and computing research is relevant.

Q1. Should any special training/testing or a minimum number of years of driving experience be specified for drivers involved in testing driverless cars with high automation?

Such testing has more in common with supervising a learner driver than with normal driving, so the rules for supervising a learner driver would appear to be the minimum requirement.

Q2. Should a second person be required to be present, as an observer?

It is important that there is adequate evidence to enable a proper investigation of the causes of any accident or incident in which the vehicle is involved, including establishing civil (and if necessary criminal) liability. The requirements for an observer should be determined in the context of all the other data capture requirements that will be in force.

Q3. Do you believe that the normal set of requirements for driver behaviour should still apply or are any exemptions from these required, if so please specify?

If the testing is intended to provide statistically valid information about the probability that the car will behave in a particular way in the future, then all the circumstances of the test must match, as closely as possible, the future environment in which the car will be operating. Some testing is therefore likely to require significant changes to "the normal set of requirements for driver behaviour*".* The requirements set by the law will constrain what testing can be carried out.

In this context, it has been reported that the cars Google has been testing on US roads have been designed to exceed the speed limit slightly as the Google engineers have determined that this improves safety. If this is true, it provides a useful example of the issues that arise.

The "normal set of requirements for driver behaviour" (perhaps amended, following this consultation) will form part of the requirements for driverless cars, but there will be many other requirements (for example, reliability, data recording and cybersecurity) that will have to be met before driverless cars could be licensed for widespread use on UK roads. The totality of these requirements will provide the context for testing high automation vehicles so, in the opinion of UKCRC, this is where work should be focussed. It is premature to set criteria for testing until the Department for Transport has specified clearly what the vehicles are required and permitted to do.

Q4. Are any new requirements or constraints necessary?

It will be important to ensure that incident data is available, comprehensive and that it can be used for independent analysis, because vehicle manufacturers (who otherwise would hold the key to interpreting data recordings) will have commercial interests that may inhibit them from disclosing all the data necessary for a rigorous safety analysis. Attention should be paid to the experiences from the pharmaceutical industry where there have been concerns that only the data from successful clinical trials are published.

Q5 Do you have any suggestions for an indication to other road users that the vehicle is operating autonomously, or capable of autonomous operation? For example, a ***warning signal*** *showing autonomous operation or a* ***distinguishing sign*** *(different number plate, sticker on windscreen, etc.) indicating the potential capability of autonomous operation?*

If other road users are made aware of the degree of automation in a vehicle, it may affect the way they interact with it. For example, other drivers may be more willing to assert priority at crossings if they know that the oncoming vehicle will make an automatic emergency stop to avoid a collision.

It may be necessary to test such changes in behaviour and the consequences. It may also be necessary to avoid such changes in the behaviour of other road users whilst testing other aspects, and therefore to conceal the automation during such tests.

Q6. Should educational materials be developed to advise other road users about the testing of highly autonomous cars?

This may be required for some tests, as part of a properly constructed test plan.

Q7. Do you have any observations on the possible reactions of other road users, or the risks of interaction with driverless cars, and possible mitigation measures?

It seems likely that other road users will take advantage of any aspects of the automation that they perceive as helpful. Pedestrians, cyclists and other drivers may assert priority. Children may find that "playing chicken" has additional attractions. Vandals may attempt to induce emergency braking for a range of reasons. Criminals may use the automatic emergency braking to stop cars for criminal purposes. It will be important to identify as many potential issues as possible and to design out all significant vulnerabilities.

There is a convergence between increased automation of driving and other developments in Vehicle to Vehicle communication that may lead to gaming the system for advantage e.g. clearing traffic in the way of a journey.

Q8. Do you see any difficulties with the existing product liability regime, when operating driverless cars with high automation?

Liability can only be established and civil or criminal sanctions pursued once the causes of an accident have been established to the relevant level of proof. That may require access to data that the vehicle manufacturer does not choose to collect or that is regarded as proprietary. It may be necessary to legislate for data collection, retention and controlled release. The complex supply chain will make it difficult to apportion liability beyond the vehicle integrator.

Q9. Do you have any suggestions for standards to regulate the testing of prototype cars with high automation?

The Health and Safety at Work Act requires that risks from work activities should be tolerable and reduced *as low as reasonably practicable* (the ALARP principle). It would reduce risks if the systems engineering and the software were developed using mathematically formal methods (*formal methods)* and shown by rigorous analysis to have the properties required for safety. The burden of proof should be on the vehicle manufacturer to show that risks have been reduced ALARP. Third party Independent Safety Assessment has been required in other industries (e.g. rail).

In general, whilst automotive OEMs have strong commercial reasons to develop safe systems, there is insufficient use of formal methods and, following accidents in the USA, there have been expert reports that have identified very poor quality software in critical subsystems.

If high automation cars incorporate commercial off-the-shelf software (COTS) (for

example, for GPS navigation or sensing) there will be a need to ensure that such subsystems are safe enough and secure enough for their role in the vehicle. It can be difficult, or even impossible, to assure this with high confidence for COTS, as it is unusual that the software has been developed to the standards or with the evidence chain that is needed to support a rigorous safety assessment.

Manufacturers should be required to deliver a *safety case* for independent review, explaining what the safety criteria were for the design and providing auditable, scientifically valid evidence that these criteria have been met. The regulatory framework being developed (for example by the CAA) for unmanned air systems might well be of relevance here. This goal-based approach to safety standards for software is exemplified by SW01, the UK CAA standard for software in ground-based air traffic management systems.

The automotive standard ISO 26262 does allow use of better V&V standards from other industries, therefore Aerospace's DO-178C, DO-333 could also be used. If allied with automated V&V methods then aerospace practices could be used for automotive systems. (This is being investigated by the PICASSOS project under the Advanced Manufacturing Supply Chain Initiative).

Q10. Are there current type approval or construction rules that prototype cars with high automation might not comply with?

Braking and steering regulations e.g. UNECE 13H and R79.

Q11. Are you able to suggest any specific areas (e.g. braking, steering) or any specific systems/technologies (e.g. ABS, ESC) where regulation needs to be amended or developed, as a priority ?

Particular attention should be given to cybersecurity within individual control units, the vehicle networks and with external communications.

There must be strong requirements for the data that must be collected and preserved in the event of an accident or a subsystem failure. The semantics of this data must be defined and published and the data itself must be made available to independent experts so that the causes of accidents can be determined and so that the public can have confidence that commercial interests are not influencing the allocation of liability.

Q12. Are any changes to the current roadworthiness regime required to permit the testing of driverless cars, or ensure their safety?

The type approval requirements following a software or data change will need careful consideration, because such changes may invalidate the safety analyses and test results that underpin the original type approval. There are cyber security implications for businesses that provide automotive maintenance as well, because a hostile compromise of a maintenance facility could lead to malicious software being introduced into many cars.

There should be expert review of standards including UNECE R13H and in particular annex 8 *Special requirements to be applied to the safety aspects of complex electronic vehicle control*

systems and UNECE R79 Annex 6 (ditto). By implication, these requirements should be applied to the controlling systems and their sensors should be evaluated to conform to a standard such as ISO 26262 as a minimum.

Q13. Have you any initial thoughts about any longer term risks and issues as driverless cars age, and possible requirements to address this?

There will be significant issues relating to ensuring that solutions to faults or security vulnerabilities, once found, are applied to all affected vehicles. Vehicles remain in use for much longer than is usual for personal computers and other consumer equipment, and third-party maintenance will be difficult or impossible. Where COTS components are incorporated into vehicles, the vehicle integrator may need to take responsibility for long-term maintenance of those bought-in components, which could require a large investment in the case of complex software.

Q14. Do you have any comments on this approach?

No comment

Q15. Do you anticipate a need for special infrastructure to permit the testing of cars with high automation?

It depends on the requirements of the testing. Testing that uses special infrastructure would provide limited information about the behaviour of the vehicle in the absence of that infrastructure.

Q16. What issues would need to be addressed, to enable insurers to offer suitable insurance products?

Actuarial data is the usual basis for an insurance market. Until enough data has been accumulated for actuarial analysis, it seems likely that premiums will be very high and manufacturers will have to provide substantial financial bonds, as is the case for new aircraft models.

Q17. Are there other insurance-related issues which may affect the introduction and testing of driverless cars?

Attention must be paid to ensuring that accident victims have fair access to the data that would help establish liability.

Q18. Do you have any suggestions or concerns over data collection and privacy, when considering the testing of cars with high automation?

No special problems should arise so long as all the data is collected with the fully informed consent of the data subject.

Q19 Do you (a) support amending diverse current regulations to cater for driverless cars alongside conventional ones, or (b) support creating a special regime via specific regulations to permit the testing of driverless cars under certain circumstances or

constraints? (Or does it not matter as long as the regulations are appropriate and clear?)

It is essential that the requirements for the behaviour of driverless cars are clearly defined and agreed *before* considering what will be needed to provide adequate assurance that particular vehicles conform to these requirements. Testing will be one source of evidence for this assurance, but not the only nor the strongest source of such evidence.

Q20 Do you have any other comments on the need for a special regime to cover the testing of driverless cars with high automation? Do you consider any other regulations or aspects of driving practice would pose a barrier, or do you consider that extra conditions would need to be imposed? Please give full details.

The current notion of "driverless cars" appears to require that a human driver be attentive and responsible. As vehicles move towards greater autonomy, then improved verification and validation methods will be required. As we have said above, a critical first step is to establish clear requirements for the permitted and required behaviour of high automation and fully autonomous vehicles.