Secure connected and autonomous vehicles: the long road ahead

Authors
Juliet Flavell, MSc (Royal Holloway, 2019)
Paul Dorey, ISG, Royal Holloway

Abstract

Recent advances in technology have led to new safety and comfort features being added to vehicles, with ambitious plans for driverless cars and other connected and autonomous vehicle (CAV) systems being developed which are expected to reduce accidents, pollution and congestion. The Department for Transport 2019 publication, *UK Connected and Automated Mobility Roadmap to 2030*, is a comprehensive foundation to build on and the next decade promises to be an exciting time. At the same time as technology is progressing, society is changing, and urban populations are becoming more dense. Vehicles are set to become highly sophisticated mobile computers which monitor their surroundings and make instant decisions based on what they detect, independently and unsupervised. They will simultaneously exchange information across networks, using the information received from wide area services and also the digital devices around them as input for decision-making. CAVs will operate as nodes in the intelligent transport networks they rely on, consisting of dynamic and fixed elements. This article will look at some of the requirements, constraints and challenges, including two areas of uncertainty: data and software updates. This technology is in its infancy. What if CAVs malfunction or their processors hang? It is difficult to see how there can be any error margin – yet lives will rely on them functioning safely. In this new paradigm, mobile computers will be out and about, under no one's direct control, and they will be too numerous to individually monitor. Will all go according to plan or should we strap in for a bumpy ride? [a]

[a] This article is published online by Computer Weekly as part of the 2020 Royal Holloway information security thesis series `https://www.computerweekly.com/ehandbook/Royal-Holloway-Secure-connected-and-autonomous-vehicles-the-long-road-ahead`. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at `https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/`.

The last decade: technological advances and societal shifts

In its 2017 *Industrial Strategy* the UK Government announced long-term post-Brexit plans, including an ambition to become a world leader in shaping the future of mobility. This is being facilitated via a *Future of Mobility Grand Challenge* with the goal of putting fully autonomous vehicles on UK roads by 2030. But well before this, new societal trends had already been emerging, in response to increases in urban populations, the development of the service economy and advances in technology. At the same time technology companies aligned with those shifts, introducing pioneering services. New shared ownership and on-demand mobility as a service (MaaS) transport models emerged like ride hailing, lift sharing and bike hire schemes.

As to the automotive industry, for some years now, traditional automotive manufacturers (OEMs - original equipment manufacturers) have been upping their technological game, equipping new models of vehicle with mobile phone connectivity, wifi hotspots and autonomous driver assist features like remote control parking, adaptive cruise control and blind spot detection. Congestion and pollution have been issues in urban areas for

Mobility as a service (MaaS)

- ride hailing
- lift sharing
- bike hire

decades. Road accident numbers have reduced but largely levelled off in the last few years. Now high tech MaaS will blend public and on-demand transport options. The result? Safer, cleaner and smarter road transport.

Technology disruptors like Google, Tesla and Uber were key players early on in the CAV sphere. A decade ago in 2010 Google hired Sebastian Thrun – who had led the winning team in the Defense Advanced Research Projects Agency (DARPA) Grand Challenge for driverless cars in 2005 - and embarked on its own project, Google X. Rather than gradually enhancing existing vehicles with new smarter technologies, Google's vision was to aim for high levels of autonomy from the start. The OEMs have the advantage, however, of their vast experience of designing, manufacturing and distributing vehicles safe enough to comply with rigorous laws. As a natural consequence, new strategic alliances have emerged through the winning entries in the *Future of Mobility Grand Challenge*, encompassing sectors including automotive, technology, communications, insurance, legal, academia and local authorities. This pooling of expertise will go a long way towards ensuring sufficient levels of vehicle safety and security to make the projected start date of 2030 achievable.

Connected vehicles: have a wifi hotspot or data connection allowing two-way communication with other vehicles, road infrastructure and wider connectivity services.

Autonomous vehicles: take information from built-in sensors and other systems to understand their geographical position and local environment, enabling operation with little or no human input for some or all of the journey.

Trials have been underway since 2015, always with a mandatory human safety driver either present in the vehicle or remotely monitoring it. The DfT's *Pathway to Driverless Cars Review*, which assessed the feasibility and legality of trials on UK roads, advocated a deliberately light-touch and non-regulatory approach in order to encourage testing and innovation, which has succeeded. The flip side of this coin, however, is that businesses do like certainty, so uncertainty about the future impact of changes to regulations may actually have the unintended consequence of discouraging manufacturers from developing CAVs in the UK, in case they have to later modify them to make them legal. Other countries less subject to regulatory change may therefore be more appealing. In China, for example, infrastructure is being built for the first time, and with less regulatory burden, so can be implemented more quickly.

Change	Predicted benefit
Less individual ownership	Urban areas could be redesigned
Intelligent traffic management	Less congestion and fuel use
Less time spent behind the wheel	Greater productivity
New mobility industry	Job creation
Increased safety levels and less driver error	Fewer accidents
Cleaner technology	Reductions in pollution

Introduction to CAV technologies and dependencies

CAVs employ a variety of technologies for autonomy, including internal and external sensors, GPS, inertial measurement units and vehicle control modules. Each component has its own engine control unit (ECU) which enables it to communicate with other components on the internal network using a broadcast protocol across the controller area network (CAN) bus, providing no verification of the origin of a message and no encryption. The ECUs use communications protocols both internally on the CAN bus and externally using the wifi or data connection, with the goal of maintaining the constant, reliable, two-way exchange of information needed with other nodes in the intelligent transport systems (ITS) to understand its surroundings and make decisions. The outcome is that the CAV can safely perform driving tasks in a way which does not harm passengers, other road users or pedestrians.

As well as other vehicles, more and more other nodes will be added to the dynamic ITS network as more distributed and centralised infrastructure like signs, roadside sensors and traffic monitoring services are added. The *UK Connected and Automated Mobility Roadmap to 2030* refers to connections

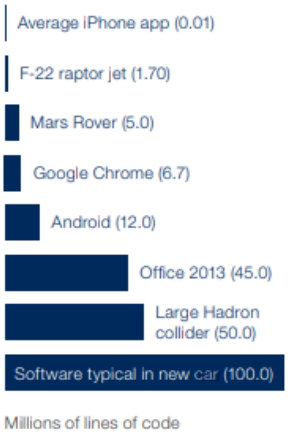

Figure 1: Size of codebase for popular software (World Economic Forum and Boston Consulting Group)

over this type of network as V2X (vehicle to everything). So, the ITS will be a set of large-scale concurrent and distributed systems with components which are complex systems themselves – known as systems of systems. One system may be secure, but the model depends on *all* being secure. Unlike conventional computer systems, they have another dimension too: a collaborative nature and collective shared purpose. It is clear that defence in depth through layered security architectures is essential but, as it stands, although they are interconnected and interdependent, systems of systems are too distributed to make securing or auditing them feasible. When travelling at speed or navigating busy urban areas, CAVs will rely on real-time information from this source having confidentiality, integrity and availability.

Analysis at the end of 2019 by KPMG in its *Autonomous Vehicles Readiness Index*, which assesses countries' preparedness for autonomous vehicles, ranks the UK seventh out of twenty - a drop of two places from the previous ranking - concluding our strong points are legislation, having a coordinated national strategy and running public trials. But it is our lack of the necessary infrastructure that keeps our readiness score down and puts our desire to be at the global forefront at risk. BSI's work programme with industry to develop standards for V2X began in July 2019, four years after trials began on public roads in the UK, and it is very early days for the 5G networks which will offer the right level of speed and bandwidth.

Glossary

CAV: Connected and autonomous vehicle.

ITS: Intelligent transport systems.

V2X: Vehicle to everything.

The new ITS networks will be part of the UK's Critical Information Infrastructure (CII) which is used by Critical National Infrastructure (CNI). The May 2019 Progress Report on the *National Cyber Security Strategy 2016-2021* notes that "while Government can create the incentives and frameworks to drive good behaviours and support CNI organisations, ultimately the boards of these organisations are responsible for investing to properly manage the risks to critical systems". The reality is that no single entity owns CII or CNI. It is therefore also not clear who governs its use and monitors its overall security.

It's also worth mentioning the amount of programming in CAVs as this is a factor in securing them due to the need to verify their code. Figure 1 compares a typical car's lines of code with that of other computer systems. The wealth of infotainment and passenger comfort features on offer contribute significantly to this high figure.

We have so far seen that CAVs are mobile, safety-critical, cyber physical systems which will need to be secure to be safe. However, there are even more unique challenges arising from their complex features and interdependencies.

For example, CAV safety will rely on the data received via the ITS network described above but if modern 5G networks are only just being introduced, and issues like lack of coverage, dropped and slow connections are still commonplace, how will this happen? The millions of lines of code in all the

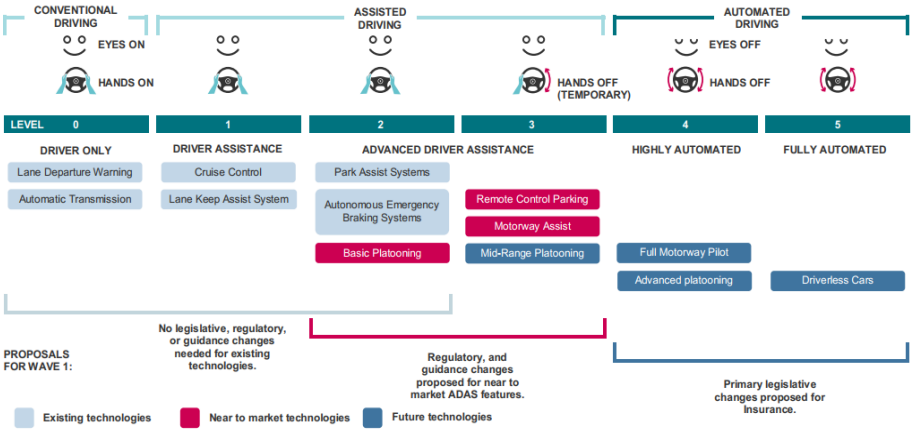

Figure 2: Centre for Connected and Autonomous Vehicles (CCAV)'s adaptation of the US-developed J3016 taxonomy introducing the concept of "eyes on/hands on" (Level 0) through to "eyes off/hands off" (Level 5).

interconnected components - provided by a multitude of specialist tier suppliers - must be validated and seamlessly interconnect without malfunctioning, as must their patches. Two issues spring immediately to mind here. Firstly, supply chains are frequently used as an attack vector. Will OEMs be responsible for the security of their entire supply chain? Secondly, system errors are likely to occur where a vehicle may enter an unknown state. If a conventional car experiences a failure its driver can put its hazard lights on and pull over to the side of the road. If a CAV enters an unknown state, what will the outcome be and will it pose a threat to other road users and pedestrians? Could this be exploited for criminal or terrorist purposes? Who will declare CAVs safe, or will it need to just be "safe enough"? What will resilience look like, and what sort of incident response arrangements will be needed?

CAVs will operate in an almost infinite variety of unique conditions; sometimes at speed and sometimes in busy urban environments. Let's not forget the dynamic and fast-changing location and surroundings information to be processed by these mobile computers. Finally, some vehicles will be stored in public places where direct physical access will be possible. This level of complexity could rightly be termed a new paradigm.

The connectivity features increase the exposure of vehicles to attack. Researchers have already identified many theoretical attacks on CAVs. A denial of service attack was demonstrated through remotely hijacking the steering and brakes of a Jeep already in public use in 2015. Key features of safety testing are predictability and repeatability and a safe system must have fault tolerance. Vehicle safety is traditionally achieved through engineers repeatedly testing components and systems to meet long-standing and widely accepted safety standards, contrasting with penetration testing techniques used in security which aim to break systems by adapting and altering attacks until they succeed. It remains to be seen how the two approaches will be merged. As mentioned above, will some CAVs be allowed to be safer than others, as is currently the case with cars? Or will an overall reduction in fatalities be acceptable even if there are some large-scale accidents caused by CAVs? Requiring manufacturers to guarantee that there will be no accidents is controversial but at the same time, not asking them is counter-intuitive, particularly when it is not yet known what fault tolerance will look like. The Government has an unenviable task to strike an acceptable balance between ensuring public safety while encouraging the enterprise innovation envisaged in the Industrial Strategy. Scrutiny of AI systems has already started and there is increasing interest in the ethical dimensions of new technologies becoming entwined throughout modern society.

Two areas key to the safe functioning of CAVs are examined below.

1. **Software updates:** Vulnerabilities in CAV and ITS components and their interactions are likely to be discovered almost continuously because of the sheer scale of these interconnected systems of systems. The unavoidable implication of this is that the CAV's secure baseline will be almost continuously out of date and therefore need continuous updating; something which is unprecedented and frankly incomprehensible. Testing of patches will not even be viable because of the need to distribute them immediately in order to comply with safety laws before they become redundant.
   But how can patching possibly be continuous, especially of mobile, safety-critical systems, with potentially poor connectivity? How updates will be distributed remains to be seen, but the *UK Connected and Automated Mobility Roadmap to 2030* anticipates a new, continuous assessment model of MOT. How will insurance be affected if an accident happens where a car doesn't have the latest patches? Under the Automated and Electric Vehicles Act 2018, if an individual policyholder has made unauthorised modifications to the vehicle's software or failed to install safety-critical software updates, resulting in an accident, the insurer will not be liable to the policyholder, only to a third party.

2. **Data:** IBM have described connected cars as datacenters on wheels. CAVs will need to be capable of collecting and processing terabytes of data and this is likely to be how OEMs will create value under new transport models. Yet the value and ownership of data and who has the right to use it are key issues to be resolved.

   Diagnostic data will be relied on for safe operation and real-time decision making. Encrypted communication with authentication of its origin will be needed for confidentiality and integrity, but in a time-critical scenario, like travelling at speed on a motorway, establishing these encrypted communications will cause a slight but contextually significant delay. Anything less however introduces risk of successful man in the middle attacks. Consider also that OEMs have obligations, for example, under the Data Retention and Investigatory Powers Act 2014 to collect and retain large amounts of communications data.

   Personal data will be generated about the passengers and must be encrypted under GDPR. Sensor data for example could be used to identify data subjects from the starting point of their journey. At the same time OEMs may be subject to contractual requirements with suppliers to share encrypted safety data with them. Personal data may allow passengers to be identified, therefore it should be encrypted, but if safety data is encrypted, it can't be monitored or acted on as real-time data to support safety. These types of ambiguities may lead to conflicting requirements for storing or transferring data - again, creating uncertainty.

The next decade: all systems go or should we expect delays?

This article has looked at some of the key unresolved issues pertinent to the development of CAVs - reflecting the early stage of development of MaaS and the long road ahead. The *UK Connected and Automated Mobility Roadmap to 2030* is a positive and comprehensive foundation which will address these issues.

As seen, there will certainly be many benefits to safely functioning CAVs, including fewer accidents, less congestion and cleaner air. But there will also be challenges from new risks to confidentiality and availability like remote hijacking or unpredictable behaviour as a result of system errors causing unknown states. A key requirement is for mobile, safety-critical systems to rely on interconnected systems where no single entity can have control over or visibility of what the whole system is doing. Systems will need constant updating. Our increasingly data-driven society will need to carefully refine its laws and requirements for use of data. New, modern infrastructure is needed, soon.

It is difficult to predict whether CAV development will follow a linear or predictable path. Based on the last 20 years of technological disruption, it's unlikely. But exciting times lie ahead, and the *Industrial Strategy* is clear that its intention is not to let a fear of failure make it unimaginative or risk averse, declaring that a strategy that avoids risks is no strategy at all. In this it seems to have succeeded so far. But before we become world leaders in shaping the future of mobility, we must resolve some of the tricky and so far unanswered questions, and only then can we be sure of reaching our destination.

Biographies

Juliet Flavell is an Information Security Risk and Compliance Manager at Marie Curie, having recently specialised in information security after working for over 15 years as an IT manager in the legal profession. She completed the MSc with Distinction at Royal Holloway in 2019 and is particularly interested in the ethical dimensions and cyber security implications of smart cities.

Paul Dorey is a Visiting Professor in Information Security at Royal Holloway College, University of London. He also consults for companies and governments in cyber security and information security strategy, including information security corporate governance and metrics for executives and Boards of Directors. He acts as an expert witness for contract and regulatory issues. Paul has gained his knowledge with over 30 years management experience in risk management and information security in financial services, energy, technology, pharmaceuticals and transportation. He has won several awards recognising his practical leadership in information security and has been Chair of both the Chartered Institute of Information Security and the IoT Security Foundation.

Series editor: S.- L. Ng