Transport Certification Australia Limited
ABN 83 113 379 936

Level 12, 535 Bourke Street
Melbourne VIC 3000

T: +61 3 8601 4600
F: +61 3 8601 4611

8 August 2017

Automated Vehicle Team
National Transport Commission
Level 15/628 Bourke Street
Melbourne VIC 3000

REGULATORY OPTIONS TO ASSURE AUTOMATED VEHICLE SAFETY IN AUSTRALIA

TCA welcomes the opportunity to contribute to the consultation process on regulatory options to assure automated vehicle safety in Australia.

In addition to providing brief commentary on the four options developed by the NTC, TCA seeks clarity on whether a Safety Assurance System – regardless of the regulatory option/s pursued – would be fit for purpose without the inclusion of connected vehicle technologies and compliance assurance and governance frameworks.

TCA largely subscribes to the European Commission's view (acknowledged by the NTC) that there are key aspects of connected and automated vehicles that 'should be approached horizontally'[1] – namely, those related to security and connectivity.

In principle, TCA believes that adopting a holistic approach would be both beneficial, and greatly align with developments overseas.

However, with regard to the discussion paper, TCA suggests that:

- If the Safety Assurance System and the proposed regulatory options intend to encompass both connected and automated vehicles, technologies and regulatory frameworks, the document would benefit from making this explicit
- If the intent is to put forward a system and options for automated vehicles alone, to the exclusion of connected vehicles, this is also a point worthy of clarification.

Furthermore, if the latter prevails, the NTC may wish to clarify their assumptions and expectations as to how these 'horizontal' issues would be managed by what would then be parallel policy, regulatory and compliance frameworks for connected vehicles.

It may be beneficial for the NTC to take the opportunity to bring some much needed attention to what will be coexisting and potentially overlapping concerns from regulatory, governance and compliance assurance perspectives; either by clearly articulating the boundaries of what

[1] European Commission. 2017. Vehicle certification (mass market products, not testing). Available at https://webcache.googleusercontent.com/search?q=cache:Uu-0YTD0V0kJ:https://wiki.unece.org/download/attachments/50856157/%2528ITS_AD-12-09%2529%2520GEAR%25202030%2520WG2%2520one%2520pager%2520on%2520vehicle%2520certification%2520v2%2520ITS-AD%2520%2528EC%2529.pdf%3Fapi%3Dv2+&cd=1&hl=en&ct=clnk&gl=au

they envision as two separate regulatory frameworks, or by scoping (or by noting, with a view to the future) a more holistic framework.

Progressing connected and automated vehicles in unison

TCA suggests that the discussion paper in particular, and the NTC approach more generally, could benefit from a more nuanced approach with regards to the convergence of connected and automated vehicles.

The 'technology neutral' and 'non-application specific' philosophy guiding the discussion paper and informing the regulatory options is to be supported in principle, but not at the expense of certainty as to the scope of the proposed Safety Assurance System.

The prevailing assumption seems to be that connected vehicle safety and compliance assurance is focussed on interoperability, and thus perceived to be a debate focussed on – and to be chiefly resolved by – standards.

Safety assurance and compliance assessment activities for connected vehicles are being progressed internationally, and with high levels of cooperation and harmonisation. With technical and standards work now well progressed, attention is shifting more concretely towards the same issues currently being addressed by the NTC – that is, towards regulatory and compliance assurance frameworks, and determining their governance.

TCA are pleased to note the inclusion of cybersecurity within the NTC's proposed assessment criteria for the design of the Safety Assurance System. TCA does suggest that the matter is less a 'non-safety' or 'other policy' objective, as is currently put forward by the NTC.

The NTC note that 'In many ways, the regulatory options reflect the risk appetite of the community and how the optimum role of government is perceived and understood by the community.'

However, gauging the community's 'risk appetite' – and translating it into regulatory options – may in this case be difficult. Industry and governments are familiar with identifying the boundaries of regulations, roles and responsibilities, and skilled at making careful distinctions between technologies, even when the same 'device' relies on multiple technologies.

The community does not often share these skills. Users of these systems will not view connected and automated vehicles as distinct technologies – they will expect a truly connected and cooperative experience incorporating both across the transportation network.

Additionally, daily events demonstrate that community awareness of cybersecurity vulnerabilities and risks is low.

In short, there is every reason for the 'risk appetites' of communities and governments to differ in this case, albeit their understandings and hence thresholds may be different.

Connected and automated vehicles will have different security requirements: there will be different risks, threats and vulnerabilities that will need to be considered and managed. However, some of these threat and vulnerabilities will overlap, along with security requirements and techniques.

For users, a secure system that protects their *safety* and *security* will be both an assumption and an expectation. Like any other digital environment, security is an assumption and an expectation for users. For connected and automated vehicles the stakes are higher, such that now physical safety and digital security are one and the same.

Moreover, a commercially sustainable global market will not be possible without security, and neither will safety nor true connectivity.

TCA also notes that another two of the proposed criteria – 'International and domestic consistency' and 'Regulatory efficiency' – have the potential to overlap substantially with work that is progressing internationally on connected vehicles.

Cooperative and connected and automated vehicles are progressing at different speeds, but will come to be interdependent. As one writer puts it, 'Autonomous vehicles that aren't connected to each other is a bit like gathering together the smartest people in the world but not letting them talk to each other.'[2]

Connectivity in vehicles, infrastructure and mobile devices will create a truly connected environment, inclusive of automated vehicles. At a minimum, it will supply information that automated vehicles themselves cannot sense or see within their immediate field of vision.

Beyond in-vehicle convergence, the work that has been undertaken and is being progressed for connected infrastructure from security, standards and interoperability perspectives will be indispensible for automated vehicles and a connected Smart City.

Additionally, both connected and automated vehicles will challenge received understandings surrounding what qualifies as an 'in service' product, what is the impact of software updates on type-approval, certification and compliance assurance, and where responsibilities fall.

International best practice

It is accepted that Australia's deployment of connected and of automated vehicles relies strongly on international developments: where appropriate, it is in Australia's interest to adopt, adapt and overall align with what will be the fundamentals of a global market.

For a variety of technical, policy, operational and commercial reasons, Australian stakeholders have closely monitored, cooperated – and, in some cases, taken up co-leadership positions – with the European Commission and the United States as they progress connected and automated vehicle technologies, policies and regulatory approaches.

The publication of two landmark documents regarding connected and automated vehicles from both regions should therefore not go unmarked by Australia.

Notably, Australia's involvement in pre-deployment activities – including the collaborative development of security solutions with international harmonisation task groups – is acknowledged in these documents.

United States

In December 2016, the United States National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT) formally published a Notice of Proposed

[2] Huei, P. 2016. Saving lives by letting cars talk to each other. The Conversation. Available at https://theconversation.com/saving-lives-by-letting-cars-talk-to-each-other-59221

Rulemaking (NPRM), which proposed to establish a new Federal Motor Vehicle Safety Standard (FMVSS) to mandate vehicle-to-vehicle (V2V) communications for new light vehicles, and to standardise the message and format of V2V transmissions.[3]

The NPRM made formal what has thus far been indicated through Advanced Notices (and subject to substantial investment by both government and industry) – namely, the goal to increase the safety, reliability and productivity of the transportation network through cooperative and connected vehicles.

Critically, the NPRM makes clear the interconnections between connected vehicles and automated vehicles.

It is the view of the DOT that connected vehicles – and the particular focus of the proposed rulemaking, vehicle-to-vehicle (V2V) communications – are complementary technologies:

> This fusion of V2V...will advance the further development of vehicle automation systems, including the potential for truly self-driving vehicles... Communication-based technology that connects vehicles with each other could not only improve the performance of automated onboard crash warning systems, but also be a developmental stage toward achieving widespread deployment of safe and reliable automated vehicles. Equipping vehicles with V2V could also lead to deployment of connectivity hardware that could potentially be used for other applications, such as connectivity with roadway infrastructure (V2I) and with pedestrians (V2P). These technologies (collectively referred to as "V2X") could increase the vehicle's awareness of its surroundings and enable additional applications.

The position of the NHTSA was supported by QUALCOMM Incorporated, Honda Motor Col, Ltd., Meritor WABCO, the Automotive Safety Council, Systems Research Associates, Inc., and IEEE USA, all of whom noted the interdependency of connected and cooperative and automated vehicles.

Other stakeholders, such as Robert Bosch LLC and Motor & Equipment Manufacturers Association noted the undesirable adoption and implementation outcomes of connected and automated vehicles having their own separate infrastructure and communications mediums.

That other stakeholders such as Competitive Enterprise Institute expressed concerns about the possible cybersecurity threats posed by combining the two technologies only makes the case for approaching them together more important – and potentially beneficial.

Europe

In November 2016, the European Commission published its connected vehicles strategy, and articulated the activities that would enable deployment of cooperative, connected and automated mobility.[4]

The strategy acknowledges, and seeks to foster, the ability of cooperative and automated vehicles to improve road safety and traffic management, reduce energy consumption and emissions, and boost European industry competitiveness and job creation.

---

[3] Department of Transportation. 2016. Federal Motor Vehicle Safety Standards; V2V Communications. Available at https://www.transportation.gov/briefing-room/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands

[4] European Commission. 2016. A European Strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility. Available at http://ec.europa.eu/transport/sites/transport/files/com20160766_en.pdf

The strategy acknowledges the importance of a legal framework, and notes that regulatory frameworks need to converge across Europe in order ensure continuity of services, interoperability, and compliance assessment.

Of equal importance and urgency in the European strategy is the need for assurance surrounding security of communications, and privacy and data protection safeguards – indeed, these two areas have their own associated activities, in addition to being included as part of a legal framework.

Like the United States, the European Commission have recognised that C-ITS and automated vehicles will together deliver a safer and smarter transportation network.

The European strategy makes very clear the interdependency of these two advancements:

> Communication between vehicles, infrastructure and with other road users is crucial also to increase the safety of automated vehicles and their full integration into the overall transport system. *Cooperation, connectivity, and automation are not only complementary technologies, they reinforce each other and will over time merge completely...* Connectivity, cooperation and automation must all come together to make it work. But even more so will cooperation be needed when future automated vehicles have to negotiate much more complex traffic situations safely and efficiently. (Emphasis added)

The Commission has acknowledged that it is being urged by European transport ministers to develop a strategy that considers cooperative, connected and automated vehicles holistically.

In addition to the strategy document, the Declaration of Amsterdam sets out the joint goals of European member States, the European Commission and industry.[5]

The parties note that automated driving functions will be expanded with the help of connectivity, in both the medium and long term.

It is for good reason that the Declaration highlights (among others) security, data, interoperability and privacy concerns, and emphasises the need to draw these together under a coherent framework. In particular, it notes that:

> In the light of the increase in cyber-threats and serious vulnerabilities, it is essential to ensure security and reliability of connected and automated vehicle communications and systems. Common trust models and certification policies should be developed to prevent risks and support cybersecurity, whist ensuring safe and interoperable deployment.

Commentary on options

TCA is aware that the implementation of a Safety Assurance System is largely intended to bridge the gap between where Australia and the international community are now (from technology, policy and regulatory perspectives) and where they will be in, say, ten to fifteen year's time.

TCA appreciates that the four options put forward by the NTC are intentionally 'pure': they capture high level approaches, and sketch out some of the potential advantages,

---

[5] https://www.government.nl/topics/mobility-public-transport-and-road-safety/question-and-answer/what-is-the-declaration-of-amsterdam-on-selfdriving-and-connected-vehicles

disadvantages, and implementation challenges. In this sense they successfully capture four distinct options on a spectrum.

TCA also understands that, looking ahead, the result is likely to be a hybrid of two or more of these options by necessity.

The NTC has taken care to include in-service updates and changes in their presentation of options – a concern similarly registered by the European Commission.

For Options 2 (Self-certification) and 3 (Pre-market approval), the NTC have sketched out approaches whereby updated statements of compliance could be provided by the Manufacturer and the Automated Driving System Entity; in option 4 (Accreditation), changes would require approval of an accreditation body.

In-service compliance will be one of the most challenging aspects of the regulatory program. Indeed, it will challenge long-held assumptions about what in-service and ongoing compliance mean for the vehicle industry, and for all parties in the regulatory environment.

Certification processes and re-certification processes for automated vehicles requiring updates and changes will need careful consideration.

It is clear that a 'one size fits all' approach will not work. A key consideration should be the benefits of adopting a risk-management approach that both manages safety and compliance concerns, while at the same time remaining flexible (as not all changes are similar), and such that it *encourages* innovation.

TCA appreciates that detailed consideration of these processes is not yet in scope for the NTC.

TCA looks forward to further engagement on the detailed the principles and criteria of the Safety Assurance System as the NTC progress with their proposed options.

Option 1, *Continue current approach*, is the least attractive of the four options, given that it would give significant power to suppliers through narrow focus on commercial risk, and any damage/loss, injury or death arising would need to be legally proven as arising from 'unsafe' behaviour of the automated vehicle, and thus culpability of the supplier.

A regulatory framework that is based purely on one of the remaining options, however, may not be fit for purpose.

A regulatory framework will need to be flexible enough to balance the traditional objectives of an approval process, but also be responsive to what will be one of the biggest changes – providing assurances for in-service operation and corresponding re-approval processes.

TCA's experience in managing Australia-wide V2X and V2I applications, and in administering an operational environment comprising end-users, government agencies, service providers, devices and back-office systems provides an indication of what can be expected of such a process: twenty applications for certification and type-approval, and over 300 individual update and change requests for systems over a relatively short period of operation.

The framework used to manage these change requests is premised on risk-based decision making, in order to streamline processing for re-certification, type-approval and auditing. Based on a risk assessment, multiple levels are used to identify the required response.

These range from fast-tracked approval (i.e. Option 2) to TCA based oversight (i.e. Option 4).

An approval process that was neither robust nor agile could simply neither facilitate innovation nor meet the need for risk management; nor could it cater to the volume of requests, or efficiently identify when and where an in-depth assessment is called for or unwarranted given the risk profile.

The assurances afforded by Option 3, *Pre-market approval* – that is, engaging the expertise of a third party – will be necessary in some cases. Changes to core functionality, or changes that may have unintended impacts on integrity or other functionality may trigger a more in-depth re-approval process.

There will certainly be cases where Option 2, *Self-certification*, in the interests of efficiency and managing low-risk profiles, is called for. In these cases, the following principles can provide levels of confidence that accompany self-certification:

- Documenting the purpose and scope of proposed changes and updates
- Appreciating the extent to which changes and updates may unintentionally impact other performance aspects
- Factoring in the historical performance and compliance of the organisation proposing to make the update.

However, in the United States, 'self-certification' entails something very different to what would be expected in Australia and Europe. Establishing what 'self-certification' would mean in a different compliance culture would need careful consideration. It would almost certainly require an assessment of what may potentially be broader impacts to an overall legal framework.

Finally, Option 4, *Accreditation*, may be desirable in cases where a high level of assurance is required over the standards, policies and processes used (and provided that accreditation applies not to the driver, and to the supplier rather than its products). Combined with self-certification of products brought to market using those accredited standards, policies and processes, it could set an effective 'high bar' for the industry, without restrictive third-party technical assessments.

TCA would be pleased to further discuss with the NTC the certification and re-certification framework used for TCA certified Service Providers, which is inclusive of Options 2, 3 and 4.

TCA thanks the NTC for the opportunity to contribute to the consultation process on regulatory options to assure automated vehicle safety in Australia.

Should you have any queries, please feel free to contact Philip Lloyd, General Manager Implementation, on (03) 8601 4674 or PhilipL@tca.gov.au

Yours sincerely

Chris Koniditsiotis
Chief Executive Officer
Transport Certification Australia