A NATIONAL IN-SERVICE SAFETY LAW FOR AUTOMATED VEHICLES

Submission in response to National Transport Commission's 2020 discussion paper

Mr. Kevin Anderson, Dr. Vamsi Madasu, Mr. Michael Gregorevic

SYSTRA Scott Lister

Date
11/12/2020

SYSTRA

CONFIDENCE MOVES THE WORLD

ABOUT SYSTRA

SYSTRA is one of the world's leading engineering and consulting groups specialised in public transport and mobility solutions. For more than 60 years, the Group has worked alongside cities and regions to contribute to their development by creating, improving and modernising their transport infrastructures. We are now present in over 80 countries and have over 7300 employees, including 1500 in the Asia Pacific region. Today, SYSTRA is involved in more than 3500 transport projects, working across both the public and private sectors, across all modes of transport, and supporting our clients wherever and whatever the need.

Our vision is to plan and create sustainable mobility for the world, which means being a positive influence on society through:

- Delivering transport solutions that promote inclusion and freedom of movement
- Preserving the environment through use of sustainable technologies and practices
- Making safety a top priority, and operating with exemplary ethics

Connected Autonomous Vehicles are therefore a very important building block for creating this vision of tomorrow, which is why we at SYSTRA are involved multiple CAV initiatives such as technology trials, applied research together at CETRAN, AV strategy committees, and policy guidance.

ABOUT THE AUTHORS

Kevin Anderson

Kevin Anderson is a long-term associate of SYSTRA Scott Lister, providing expert advice on complex systems safety related projects. He was the Chief Planner at GHD on 16 February 1983 when the Ash Wednesday bushfires claimed 75 lives and extensive property damage amongst Kevin's many country municipal Clients. Within four years Kevin had mutated into a thirty-year career of fire life safety and property loss prevention. Safety risk assurance in airspace and railways followed and by 1997 Kevin was Functional Safety Assessor to NSW Country Train Management and Control System (TMACS): an early adopter of GPS. Kevin is a 20-year veteran of aSCSa and still acts as the FSA for TMACS.

Dr Vamsi Madasu

Dr. Vamsi Madasu is a Technical Director in SYSTRA Scott Lister, primarily working within the Defence and Transportation sectors. Prior to consulting, he was the Deputy Director for UAS within DGTA-ADF (now Defence Aviation Safety Authority) where he played a key role in progressing the regulations surrounding Defence UAS. And in his previous Avatar, Vamsi was a researcher at QUT, UQ and NICTA Queensland Research Lab. Vamsi holds a PhD in Electrical Engineering from the University of Queensland and is a Fellow of Engineers Australia and a Senior Member of IEEE. He has published extensively on various complex systems with more than 75 publications and an impact factor of 21.

Michael Gregorevic

Michael Gregorevic is a Principal Consultant for Innovation & New Mobility Services in SYSTRA Scott Lister, where he leads the Australia and New Zealand team's focus on areas such as Connected Autonomous Vehicles, Electric Vehicles, and On-Demand/Shared Mobility. Prior to consulting he was the Head of Powertrain Integration & Program Management at the Ford Motor Company Australia and has 17 years' experience in engineering vehicles for global markets, with expertise across vehicle systems engineering and certification, various automotive technologies and trends, and the wider automotive industry businesses for locally and internationally.

RESPONSE TO:
A NATIONAL IN-SERVICE SAFETY LAW FOR AUTOMATED VEHICLES

SUMMARY

All vehicles eventually break down and Automated Vehicles (AVs) are no exception. However, AVs pose two unique problems: First, the removal of the driver means that there is no person providing feedback on how the vehicle performs over time. More specifically, there is no one to say that, "*something feels wrong, this needs to be checked out*". Secondly, an AV could easily arrive at its destination with a non-safety critical defect, without recognizing there is a problem. This could lead to a potentially dangerous situation in the future. For instance, an AV operating with a faulty sensor is a road hazard. Imagine the wheel-speed sensor that reports the vehicle has stopped when it is actually travelling at highway speeds. A human would know to disregard that faulty input because it "feels" wrong. An AV, on the other hand, could respond by continuously accelerating. Therefore, it is critical for AVs to not only drive autonomously, but also self-diagnose future and upcoming issues.

Safety of in-service AVs should be ensured through regular and comprehensive maintenance and the inspection of automated driving systems (ADS). Additionally, ADS entities (ADSEs) should record and analyse all available documentation to facilitate the maintenance and repair of ADSs, after a crash. Such documentation would likely identify the equipment and the processes necessary to ensure safe operation of an AV, after repair.

SYSTRA strongly believes that all future Automated Vehicle (AV) safety standards in Australia, including in-service safety standards, need to be flexible and open, technology-agnostic, and performance-oriented to account for the rapid pace of technological innovation. AV laws and regulations should consist of simple and generic inspection, repair, maintenance and record-keeping requirements designed to validate that an ADS can safely operate in the real-world road environment for its life of type. ISO 3888 — Diagnostic, maintenance and test equipment, could be utilised for developing requirements for routine maintenance of ADSs for optimal performance and operations.

Performance-based safety standards for ADSEs should ensure that the AV is maintained in an operationally safe condition for their entire operational lives, and:

- ADS equipment fitted is correctly installed and serviceable or clearly identified as unserviceable;
- The initially operational certificate for the AV remains valid at all times;
- The maintenance of the ADS is performed in accordance with the approved maintenance programme by qualified personnel.

All things considered, with regard to in-service safety, SYSTRA recommends that ADSEs in Australia should:

- Develop a maintenance programme for the vehicles including any applicable reliability programme;
- Develop a process for the approval of safety-related modifications and repairs;
- Ensure that all maintenance is carried out by qualified personnel, in accordance with the approved maintenance programme;
- Ensure system updates occur as needed in a safe and secured way and provide for after-market repairs and modifications as needed;
- Demonstrate how they incorporated vehicle cybersecurity considerations into ADSs, including all actions, changes, design choices, analyses and associated testing, and ensure that data is traceable within a robust document version control environment;

- Ensure the recording of safety-critical events for operation on public roads, including collection, analysis and dissemination of all data related to the occurrence of malfunctions, degradations or failures related to crashes;
- Ensure that all defects discovered during scheduled maintenance or reported are corrected by an appropriately approved maintenance organisation;
- Ensure that AVs are taken to an appropriately approved maintenance organisation, whenever necessary;
- some minimal level of cybersecurity to prevent ADSs from being hacked and weaponized.
- Coordinate scheduled maintenance, the application of upgrades, the replacement of parts, and component inspection to ensure the work is carried out properly; and
- Manage and archive all in-service records and/or driver logs.

Additionally,

- ADSs should have a self-diagnostic capability.
- ADS operators should be aware of maintenance requirements of ADSs to enable safe and optimum operation. This includes understanding self-diagnostic capabilities of the ADS and the status or error messages the system may display.
- NTC should distinguish between a safety-critical failure versus a minor failure to determine whether an ADS can continue to be operated without the automated system
- The Vehicle Inspection requirements will need to be changed to include new technologies, with substantially more detailed inspections for fully automated vehicles.
- There should be a standard language and a data dictionary for reporting records and data from ADSs.

The following pages address a selection of the specific questions raised by the discussion paper.

ADSE duties and enforcement framework

Question 1*: What prescriptive duties under the general safety duty should be included in the AVSL to manage in-service safety risks?*

A fundamental component of the AVSL is the principle of self-certification by the ADSEs "against certain safety criteria". Although this principle is common throughout the automotive industry both in ANZ and more broadly across the world, and for a variety of requirements, we believe the application of it to ADSEs has a unique risk and significant profile attached to it, that therefore requires more "checks and balances" to protect the community. Specifically, the issue arises from a lack of defined verification methodology and pass criteria. So, while an ADSE may decide they are capable to self-certify to the "certain safety criteria", we do not see in the AVSL detail how their claims can be checked and verified allowing undue risk to be introduced to the process.

The Volkswagen Diesel emissions scandal of recent years has demonstrated that it is entirely possible for some of the largest and most respected companies to behave unethically on a large scale. With billions of dollars at stake in the global race to mass deployment of Autonomous Vehicles, the possibility of similarly unethical or (or negligent) decision-making with ADS self-certification cannot be overlooked.

Finally, while we recognise and appreciate that no test regime can cover every eventuality, particularly for an ADS, we see strong merit in an additional requirement for ADSEs analogous to crash testing. In crash testing, select conditions are required to be physically tested despite being a small subset of what may actually happen in real-world conditions. This provides authorities, the public, and the OEMs with meaningful and transparent data on how one OEM's system compares to another in controlled conditions. Likewise, there is merit in requiring ADSE's to conduct a similar suite of testing in addition to their self-certification process. This would create a body of evidence for back-to-back system performance, whether it be from ADSE to another, or from one ADS version to another from the same ADSE. This testing is proposed to supplement overall self-certification process, not replace it.

Further commentary on elements of the discussion paper:

- p.8 Self-certification by ADSE: results hinge on availability of safety data /Safety Case to independent parties p.9 Suggest to classify INPUT reliability – vision, Radar, Lidar, GPS, then PROCESS – knowledge, hardware /software integrity, artificial intelligence, then OUTPUT – brake, steering, accelerator
- p.23 Examples and scenarios of general safety duty seem to be drawn from Workplace Health and Safety whereas the technical functional safety should be drawn from the safety-critical systems domain and standards
- p.28 SFARP is but one criterion albeit the leading principle, but ,'not less safe', 'compliance with standards', 'good practice' and 'continuous improvement' are others
- p.125 As to principles outlined above, 'not less safe' will not be sufficient, compliance with standards' is but a starting point' and 'good practice' as envisaged by prescriptive duties is but support not the full story
- p.36 Correlate due diligence to risk-based SFARP
- p.30 As above, software safety is part of the domain of safety-critical systems not WHS
- p.31 Some relevant standards such as AS/IEC 61508 provide hundreds of techniques and measures to support the risk-based approach, tying SFARP in with 'due diligence' and evidence. A lifecycle approach is embedded in safety-critical standards such as 61508
- p.33 We support the Safety Case and the identified 11 topics and three obligations

ADSE duties and enforcement framework

Question 3: *Are existing and proposed regulatory frameworks (state and territory laws, first-supply requirements and general safety duty obligations) sufficient to address third-party interference with an ADS? If not, should interference with the safe operation of an ADS be a specific offence, and how should this offence be enforced?*

The introduction of ADS technology creates a myriad of new use case and possible scenarios of vehicle to vehicle and vehicle to object (human, animal, inanimate) interaction. While ADS are being designed with intent of detecting these and preventing accidents, it is nevertheless an unfortunate reality that there will always be an element of society involved in criminal activities or other misdemeanours. Due to general operational behaviour of ADSs that means they will default to stationary movement in the event that continuous movement is deemed unsafe, which then creates a whole new set of opportunities for such people to easily interfere with ADS, such as theft, assault, car-jacking, kid-napping. Similarly, just as some people in society continue to throw rocks off overpasses at moving cars, in a similar way such people may for example seek to trick ADS systems by 'hacking' road and sign markings, or disabling vehicles by covering external cameras or damaging expensive sensors. It is therefore recommended that detailed thought is put into both the enforcement aspect of these scenarios as well as a minimum set of ADS behaviour responses to these scenarios that the ADSE must self-certify – and these are included in their design.

Further commentary on elements of the discussion paper:

- p.7 ADS without human input only at Level 5. Level 3 is a no-man's land as human must remain 'competent'
- p.13 Quite a challenge – risks must be eliminated or mitigated SFARP. We suggest Target Levels of Safety (TLOS) could be one tenth of the current road toll
- p.18 Disagree that prescriptive rules will ensure predictability. Just as brake and indicator lights communicate to other vehicles, appropriate parallels for ADS must be considered – some form of communication/internet for ADS should be considered
- p.20 We concur with the dynamic driving task and suggest to expand on 'and so on'. Some functions relate more to navigation, lane following etc. Others are safety-related – i.e. threat detection and response
- ODD restrictive approvals, such as maximum speed, not in rain etc have the potential for malicious modifications
- Suggest to monitor continuous improvement – todays' cars are very different to 10 years ago, new functions such as bicycle[AC1] /door interlock

In-service modifications and after-market installations

***Question 9**: Are there any gaps in the regulation and proposed regulation of in service modifications that the NTC has not identified? Are there other options that should be considered?*

The discussion paper states 3 conditions of in-service modifications to be considered. Notably, these conditions exclude modifications to the vehicle (hardware or software) that do not directly intend to add or modify the vehicle's ADS capability; we view this as a gap in the regulation that needs to be addressed. Today, there is a large industry for after-market vehicle modifications, including 2nd Stage Manufacturing as defined by the ADRs, and ranging in scale from one-off bespoke modifications to low-volume manufacturing lines. Not only do they employ thousands of people across Australia and contribute significantly to the economy, but they also provide a very real service of providing both private and commercial customers access to vehicle modifications that enhance the vehicle's capability far beyond the superficial. Such examples include:

- Increased load carrying capacity
- Increased towing capacity
- Custom storage to suit unique business/organisation demands
- Increased off-road capability unique to Australian conditions

We mention these examples, because today the ADRs define a clear process for such modifications to be engineered and certified that takes into account the impact on the overall vehicle safety and attribute performance. In the proposed AVSL however, it appears the impact of such modifications on ADS performance has not been considered, and any modification that changes the vehicles mass, Centre of Gravity, or acceleration/braking capacity for example, will clearly have an impact on the ADS performance and therefore the ability to continue meeting the "certain safety criteria". Requiring every modifier of such actions as those listed above to be an ADSE is not practicable. A further and quite likely scenario is the new after-market offerings which will emerge specifically to upgrade capabilities of individual ADS componentry, for example LiDAR upgrades with increased range or resolution. Unlike the prior examples, this modification does directly relate to ADS performance but equally is not a scenario currently addressed sufficiently by the proposed AVSL. We therefore recommend the need for further study in consultation with planned first-supply ADSEs and the after-market engineering industry.

Further commentary on elements of the discussion paper:

- Recommend clarify relationship between 'due diligence' and risk-based SFARP obligation
- p8. A risk-based regulatory approach supported, but yet to be defined in detail

In-service modifications and after-market installations

Question 10*: Do you agree that the additional functions the NTC has identified may need to be undertaken by the regulator to ensure in-service safety? - Reporting - Crash investigations (for enforcement, with a specialist agency like the ATSB to undertake no-blame investigations) - Accreditation - Regulatory approvals*

Recording of data and reporting for crash investigations makes good sense, but we see a clear opportunity and need to go a step further. As is common in workplace health and safety practice, in particular the manufacturing or construction industry, reporting of near-misses is equally important as from it comes data and learnings to prevent the probability of future events occurring, potentially with more severe consequences. In the case of an ADS, it should be straightforward to log and report a near-miss event, even if the occupant was unaware that a near-miss had just occurred. Such reporting should not be considered for a punitive response (unless it was deemed road laws were broken) but rather should serve as an opportunity for learning and continuous improvement shared cross Australia and the participating ADSEs.

Further commentary on elements of the discussion paper:

- p.11 Which entity is in control? Recommend the equivalent of 'black box'
- p.27 The scenarios are illuminated but not necessarily complete, consistent and correct
- p.29 Minimum prescriptive requirements presages a risk-based model – Minima may not achieve TLOS unless multiple system redundancy is invoked
- p.29 ATSB has a systemic role
- p.30 Compliance with relevant road traffic laws is a major task of matching a journey to the environment – may require new technologies to communicate conditions, not just cameras to replicate red light response

Access and exchange of information by the in-service regulator

Question 28*: Do you agree that a specific power authorising collection, use and disclosure of personal information is required in the national law and in state and territory legislation?*

While Autonomous Vehicles are expected to bring many benefits to road users, and society as a whole, we must not be naïve to think that their use will not be exploited for criminal purposes. Indeed, by taking the human element out of the loop, and out of the vehicle altogether, this create new opportunities for the illegal trafficking of goods. Careful consideration will therefore be required on countermeasures for both prevention and enforcement, and central this will be access and powers authorising the collection, use and disclosure of personal information for ADS-equipped vehicles and operators.