iTech Labs
Submission to National Transport Commission

for

Safety Assurance for Automated Driving Systems

Consultation Regulation Impact Statement

on Automated Vehicles

09 July 2018

iTech Labs Australia ACN 108 249 761 www.itechlabs.com **e-mail:** info@itechlabs.com
Suite 24, 40 Montclair Ave, Glen Waverley, VIC 3150, Australia. Tel. +61 3 9561 9955 Fax. +61 3 9545 1596
iTech Labs is an ISO/IEC 17025 NATA accredited testing laboratory

Table of Contents

1. Executive Summary

iTech Labs ("iTech") has been testing complex software systems since May 2004. With many years of testing and certification experience already behind iTech Labs' founding staff members, the company was set up specifically to test software systems to ensure that they meet regulatory requirements and provide a high level of software quality assurance. Our staff experience also includes development, operation and maintenance of control & monitoring systems for public transport.

iTech Labs is an ISO/IEC 17025 certified testing laboratory for software systems with a wide range of global clients. Integrity, accountability and a commitment to protecting public interests are the foundational priorities of our business.

Further details about iTech Labs can be found at our website www.itechlabs.com .

iTech labs is responding to the "NTC Safety Assurance for Automated Driving Systems: Consultation Regulation Impact Statement" ("the Consultation RIS") as we believe that it is in the public's best interest that we contribute to the debate over how to regulate automated vehicles, involving complex software. Our collective experience in the testing and regulation of real-time software systems in the gaming industry, informs our identification in this submission, of risks that may not have been considered in the preparation of the Consultation RIS. We welcome the opportunity to contribute to this consultation and we offer the following submission on the Consultation RIS.

In summary, we are strong advocates for independent testing of vehicle types and a pre-approval regime, as a means of ensuring that automated vehicles operate with a high level of safety, and with minimal risk of collisions. We believe that the general public will rightly expect a level of independent testing of automated vehicles.

We understand that a number of European countries and US states are moving towards such a regime, and we encourage you to investigate further, before settling on Option 4 of the Consultation RIS.

Our submission is comprised of the following: section 2, which summarises our responses to those of your questions for which we are qualified to answer; Section 3 outlines our understanding of the NTC SAS RIS and its recommendations; Section 4 provides a detailed outline of risks that we think have been overlooked, together with iTech's concerns over the recommendations made in the Consultation RIS.

We thank NTC for the opportunity to make this submission, and we will make ourselves available for future discussions on the regulation of Automated Driving Systems.

2. Response to 21 Questions

This section of our submission outlines how iTech's submission addresses the 21 consultation questions listed in the Consultation RIS.

Our submission advocates independent testing of vehicle types and a pre-approval regime.
We have therefore not attempted to provide responses to questions 8-19.
Our responses to the other questions are embedded in our submission document.

> **(8.2) Consultation questions**
> The following questions are intended to assist stakeholders in their assessment of the options:
>
> 1. To what extent has the consultation RIS fully and accurately described the problem to be addressed? Please provide detailed reasoning for your answer.
> The Consultation RIS describes the problem well, but we feel that it underestimates safety risks, and over-estimates the benefits of self-regulation.
>
> 2. What other factors should be considered in the problem statement?
> In our submission, we have tried to outline as many other factors as we can currently identify.
>
> 3. Has the consultation RIS provided sufficient evidence to support the case for government intervention? What else should be considered and why?
> Yes, the Consultation makes a good case for government intervention, but we feel that the proposed intervention does not go far enough. We advocate independent testing of vehicle types and a pre-approval regime.
>
> 4. To what extent have the community and industry expectations of a regulatory response been accurately covered?
> We believe that community expectations would and should include independent testing.
>
> 5. Are the four options clearly described? If not, please elaborate.
> The differences between the four options could be better described.
>
> 6. Are the proposed safety criteria and obligations on ADSEs (detailed in chapter 4 and Appendix C) sufficient, appropriate and proportionate to manage the safety risk?
> No. We identify in section 4.3 of this submission, many areas of risk that we feel will not be sufficiently managed by the proposed safety criteria and obligations on ADSEs.
>
> 7. Are there any additional criteria or other obligations that should be included?
> Yes, we believe that we have outlined in section 4 of our submission, many such criteria and obligations.
>
> 8. Do you agree with the impact categories and assessment criteria? If not, what additional impact categories or assessment criteria should be included?
> No comment.
>
> 9. Has the consultation RIS captured the relevant individuals or groups who may be significantly affected by each of the options? Who else would you include and why?
> No comment.
>
> 10. Does our analysis accurately assess the road safety benefits for each reform option?

Please provide any further information or data that may help to clearly describe or quantify the road safety benefits.
No comment.

11. What additional safety risks do you consider the primary safety duty in option 4 would address compared with option 3?
No comment.

12. Does our analysis accurately assess the uptake benefits for each reform option? Please provide any further information or data that may help to clearly describe or quantify the uptake benefits.
No comment.

13. Does our analysis accurately assess the regulatory costs to industry for each reform option? Please provide any further information or data that may help to clearly describe or quantify the regulatory costs.
No comment.

14. Are there any specific regulatory costs to industry that we have not considered?
No comment.

15. Does our analysis accurately assess the costs to government for each reform option? Please provide any further information or data that may help to clearly describe or quantify the costs to government.
No comment.

16. Does our analysis accurately assess the flexibility and responsiveness for each reform option? Please provide any further information or data that may help to clearly describe or quantify the flexibility and responsiveness of the options.
No comment.

17. Do you consider the relevant factors and conditions for government in choosing an option to be valid? Are there any factors and conditions you do not agree with?
No comment.

18. Do you agree with our view on the relevant factors and conditions for government in choosing an option?
No comment.

19. Has the consultation RIS used an appropriate analytical method for assessing the benefits and costs of the options? What else should be considered?
No comment.

20. On balance, do you agree that the preferred option best addresses the identified problem? If not, which option do you support?
We advocate independent testing of vehicle types and a pre-approval regime.

21. How does your choice of option better address the problem than the preferred option?
Independent testing of vehicle types and a pre-approval regime will improve public safety.

3. Background

3.1 What the NTC SAS RIS is recommending:

The NTC recommends Option 4: Legislative safety assurance system + primary safety duty that –

- establishes a safety assurance system with a dedicated national agency for automated vehicle safety.
- requires an automated driving system entity (**ADSE**) to self-certify against principles-based safety criteria.
- creates offences and compliance and enforcement tools that are specific to safety assurance and a general duty on ADSEs to ensure safety ('primary safety duty').

The NTC claims that Option 4 will:

- ensure that automated vehicles entering the Australian vehicle fleet are reasonably safe to avoid the potentially high social cost of poor road safety outcomes
- provide users with reassurance that automated vehicles are reasonably safe so that a lack of confidence does not become a barrier to the uptake of automated vehicles
- create a suitable regulatory environment that is flexible and responsive and does not impose unreasonable costs, so that ADSEs can enter the Australian market.

3.2 The NTC proposed safety assessment criteria

The NTC is proposing 11 safety criteria that the applicant must self-certify against, to demonstrate its processes for managing safety risks:

1. Safe system design and validation processes
2. Operational Design Domain
3. Human Machine Interface
4. Compliance with relevant road traffic laws
5. Interaction with enforcement and other emergency services
6. Minimal risk condition
7. On-road behavioural competency
8. Installation of system upgrades
9. Testing for the Australian road environment
10. Cybersecurity
11. Education and training

4. Summary of iTech Labs' concerns

iTech believes that:

- The assumptions made in the NTC SAS RIS largely avoids the risks associated with real-time complex software, and have failed to identify the extent and magnitude of the risks
- The NTC SAS RIS has failed to identify the extent and magnitude of the risks of the introduction of AVs and the complexity of the interactions with other road users, road infrastructure and the contributing environmental conditions.
- The options considered are too narrow and there needs to be some form of independent testing to confirm the performance of the safety assessment criteria. Reasonably safe AV's are not good enough when public lives are involved. A high level of safety and reliability are required.
- Option 4 will not be able to achieve the stated benefits.

4.1 Assumptions about AVs

iTech believes that the assumptions in the NTC SAS RIS about safety of automated vehicles (**AVs**) are not proven. There may be greater risks. Claims of a more than 90% reduction in road traffic deaths resulting from automation, eliminating crashes linked to human error, are untested. The key NTC assumptions in the NTC SAS RIS are not sound:

- It is not proven that AVs will take human failure/error out of driving, making AVs safer (algorithms, environmental factors, data entry, back up drivers, misuse, hacking, car-jacking, stolen vehicle issues, will still be there) there may be greater risks.
- Assumes that AVs can be separated from electric, connected, heavy vehicles, etc.
- Assumes that approval of AVs doesn't need local government involvement in planning the appropriate introduction, infrastructure needs, and in providing the capacity to update inappropriate roads and road conditions.

> The International Transport Forum (ITF Report 2018): Safer roads with automated vehicles? (page 5) [1] recently stated that:
>
> *"Claims of a more than 90% reduction in road traffic deaths resulting from automation eliminating crashes linked to human error are untested. It seems likely that the number of road casualties will decrease with automation, but crashes will not disappear. In certain circumstances, more crashes may occur among "average" drivers that are not prone to risky behaviour. This is particularly likely in circumstances where drivers must take over from automated driving in emergency situations."*

iTech Labs is aware that there is much debate about AVs. This debate indicates that unplanned deployment of AVs on roads will cause:

- A significant increase in vehicles on roads and increase congestion
- A mode shift from public transport to private vehicles
- Lack of consumer control, making cities less liveable
- Increase in injury risks, especially during the development of automated vehicles and mixed use of the road with other road users

[1] International Transport Forum (2018): "Safer roads with automated vehicles?" International Transport Forum at the OECD, Paris. page 22 downloaded on 22 June 2018. see https://www.itf-oecd.org/safer-roads-automated-vehicles-0

- More dependence on technology and greater impact of disruptions to the transport network.

While a safety assurance system may be one part of gaining permission to use the automated driving technology on the road, so too is the primary safety duty on the ADSE.

The complex and changing environment of the broader applications of ADSs and AVs, such as vehicle-to-vehicle, vehicle-to-infrastructure and vehicle-to-x, will also need to be considered as part of the regulation process. Dr Shladover, a world leader in transport solutions and vehicle infrastructure integration, argues that "Automation without connectivity will be bad for traffic flow, efficiency and probably safety"[2].

The narrowness of the NTC approach becomes more apparent considering the real transport objective in Australia, which is for improved road safety and mobility. ADSs/ADSEs will need to communicate, connect and interact.

The table below published in the ITF Report 2018, demonstrates that connected AVs are more likely to bring about road safety, as well as other benefits. [3]

Table 4: **Assessment of sensor performance across driving tasks**

Performance aspect	Human	Automated Vehicle			Connected vehicle	Connected, automated vehicle
	Eyes	Radar	Lidar	Camera	DSRC	Radar, Lidar, Camera and DSCRC
Object detection	Good	Good	Good	Fair	n/a	Good
Object classification	Good	Poor	Fair	Good	n/a	Good
Distance estimation	Fair	Good	Good	Fair	Good	Good
Edge detection	Good	Poor	Good	Good	n/a	Good
Lane tracking	Good	Poor	Poor	Good	n/a	Good
Visibility range	Good	Good	Fair	Fair	Good	Good
Poor weather performance	Fair	Good	Fair	Poor	Good	Good
Dark or low illumination performance	Poor	Good	Good	Fair	n/a	Good
Ability to communicate with other traffic or infrastructure	Poor	n/a	n/a	n/a	Good	Good

Source: (Sheettle, 2017)

4.2 Risks Identified in the NTC Consultation RIS

The NTC SAS RIS identified three types of risks associated with AVs:

- A1 - Design risks
- A2 - Organisational risks
- A3 - Operation/use risks

The NTC SAS RIS explains that A.1 Design risks are those that are inadequately designed, and that tested automated driving systems (ADSs) or associated modifications, have the potential to lead to crashes. New risks or hazards could include:

- Technological failure (malfunction due to poor design)

[2] Shladover, S. E, Sc.D (2018), Practical Challenges to Deploying Highly Automated Vehicles; California PATH Program (Retired) Institute of Transportation Studies University of California, Berkeley Drive Sweden Göteborg, May 14, 2018 downloaded on 22 June 2018 from https://www.drivesweden.net/sites/default/files/content/bilder/practicalchallenges4drivesweden.pdf

[3] International Transport Forum (2018): "Safer roads with automated vehicles?" International Transport Forum at the OECD, Paris. page 22 downloaded on 22 June 2018. see https://www.itf-oecd.org/safer-roads-automated-vehicles-0

- Cyber security failure (for example, hacking or attacks due to poor design)
- Software updates that introduce new safety issues (such as poor quality control, or an update that is not supported by the vehicle's operating system)
- Failure to function as expected, in approved operating environments/conditions (system not up to the task)
- The ADS not being suited to Australian environmental or driving conditions
- The after-market system not integrating safely with the existing vehicle
- The vehicle meeting design criteria, but still causing a safety risk in operation. These types of risks would be best managed by the vehicle manufacturer or the automated driving system entity (ADSE).

The NTC SAS RIS then explains that A.2 Organisational risks include:

- Failure by the ADSE to address safety issues that emerge over time (software or hardware) – for example, through a lack of appropriate support
- Failure to monitor the performance of the system
- Failure to adapt the system to changes in regulation over time
- Failure to adapt the system to changes in the road environment over time
- Insolvency of the ADSE
- The ADSE no longer supporting legacy versions of the ADS
- The company deploying an ADS (native, after-market or through software upgrade) that has not been through the self-certification process
- Failure to monitor and issue security updates as required. These types of risks would be best managed by the vehicle manufacturer or the ADSE.

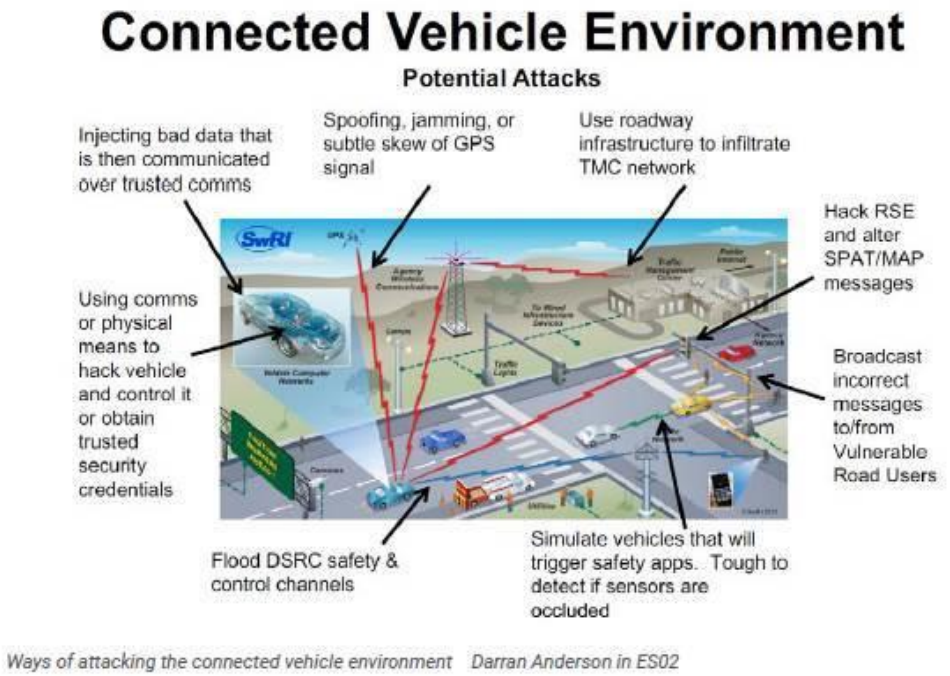
The NTC SAS RIS then further explains that A.3 Operational/use risks include:

- Use in inappropriate environments/conditions
- Technological failures (degradation of hardware due to poor maintenance or repair)
- Cybersecurity failure (for example, hacking or attacks due to failure to follow security protocols)
- Software updates (failure to apply)
- Divided/competing or contradictory responsibilities (between the driver and the ADS) ♣ unclear responsibilities of human drivers in different vehicles
- After-market fitment and vehicle modifications adversely impacting the ADS's performance
- Vehicle repairs adversely impacting the performance of the ADS, due to error or lack of understanding of the ADS's operation
- Repairers unable to assess the impact of repairs to an ADS.

4.3 Risks not addressed

iTech is of the view that the NTC's Consultation RIS has not properly considered the complexity, magnitude, and the seriousness of the impact of the risks of using immature and untested AVs with other road users, and the road environment.

There are the known and the unknown risks with AVs.



Source: ITS World Congress (2017) Post Congress Report [4]

The risks addressed in the RIS are important, however, iTech believes that there are many more risks that are not covered. These must be considered and evaluated.

We are assuming that the implementation of automated vehicles will include a central computer system or control centre. We assume this would issue the commands, back-up the data, remotely update vehicle software, have the "road map" data, answer traditional help request phone calls for help that a hotline does, and more.

The following are several additional risks that need to be evaluated and ameliorated before open use of AVs is permitted:

4.3.1 Business Continuity

All major computer systems must be able to retain business continuity issues caused by a variety of potential problems / faults. Some examples:

- Disaster recovery measures, e.g. if the main control / computer site is destroyed by a bomb or flood.
- Data recovery – in the event of a main database wipe-out, there needs to be means to recover it by playing back the transaction logs. Of course there needs to be these logs in the first place.
- Redundancy – there should be no single point of failure within the system(s).
- Appropriate environment for computer systems, communication equipment and staff, e.g. air conditioning and other climate control.

[4] ITS World Congress (2017) Post Congress Report.(page 36) See link: http://itsworldcongress2017.org/wp-content/uploads/2018/04/ITSA-Montreal-Post-Congress-Report_REV.pdf

Also see: Marks, Jason (2018) "How to ensure the safety of Self-Driving Cars " published by Medium. See Link: https://medium.com/@olley_io/how-to-ensure-the-safety-of-self-driving-cars-part-1-5-2fcc891ea90b

- Security of the main control / computer site including:
  - Physical access e.g. card or body tracking system with full logging
  - Logical security – e.g. a very sound, graduated password control system
- Robust communication systems (e.g. Telstra had total failures at least twice in the last month or so).
- Multiple personal communication channels (e.g. voice / Internet / SMS) to report problems from users of the AV systems to a "Hotline".
- Availability of key staff – should there be a serious problem, there needs to be sufficiently skilled staff member to lead the recovery procedures. Note that if there were a bomb attack, many key staff could be permanently unavailable.

4.3.2 Database Backup and Recovery

All computer databases must be backed up so they can be recovered and used for emergency or research purposes. Specific issues:

- Backups should be frequent
- Backups should be scheduled to occur without human intervention
- Backups should be stored remotely, as well as locally
- Security and access to database backups is vital – see next section
- Release of backup data to third parties should be under the strictest guidelines and permissions

4.3.3 Security

There are many aspects of security that need to be addressed and cannot be ignored. For example, hackers have managed to break into some of the "highest security" locations in the world, like the USA Nation Security Agency and the USA 2016 Federal election. Some aspects to be considered are:

- Physical access to operations / development centres
- Anti-malware protection in all levels of equipment and communications
- Robust and timely password / security access options and procedures
- Licensing and background checks on programmers and developers
- Is the download process of new software / firmware secure against all forms of attack?
- Are the communications between all parts of the systems secured via high level encryption? Or are there other such protection systems against spying or attacks?

4.3.4 Software bugs

YES, there will be many. Some of the areas where software has failed in the past are Leap Day, February 29 and the turn of century (Y2K). The only way to lower the number and effects of software bugs, is through a well-documented, strong and independent testing regime, which must cover a wide range of functionality and failure modes. [5]

[5] Shladover, S. E,, Sc.D (2018), Practical Challenges to Deploying Highly Automated Vehicles; California PATH Program (Retired) Institute of Transportation Studies University of California, Berkeley Drive Sweden Göteborg, May 14, 2018 downloaded on 22 June 2018 from https://www.drivesweden.net/sites/default/files/content/bilder/practicalchallenges4drivesweden.pdf and included with this iTech submission

4.3.5 Urgent safety and emergency situations

iTech is concerned that urgent safety and emergency situations that the proposed safety assurance system has not dealt with, are the most important and prevalent concern of the community. Can the proposed model respond to these issues?

- Hacking and cybersecurity attacks
- Use of AVs for crime and terrorism, and the ability of the police to act or respond in a safe and timely manner
- Inability for police and authorised officers to identify who or what was driving, for law enforcement and accident investigation
- Technological failures due to extreme environmental conditions (eg. electric storms, fog, floods and heat)
- Stolen automated vehicles and the ability of the police to respond/trace/deactivate stolen AVs
- Car- jacking and hold ups of passengers, and the ability of police to communicate with the ADSE to respond appropriately to such an emergency
- Ability of police and authorities to enforce road rules or investigate accidents, in order to confirm who or what was driving

4.3.6 Sabotage

iTech believes that sabotage should be a major risk concern:

- Can be deliberate or accidental
- Can be internal or external
- Can be to systems / hardware / software / operations / communications / AVs themselves

iTech noted as we were preparing this submission, that Elon Musk has indicated that there has been serious internal sabotage of Tesla's AV software.

4.3.7 Environmental

There are many different environmental aspects that can hinder correct operation and security. Some examples are:

- Some data communication methods can fail in adverse weather conditions (e.g. a microwave can fail during heavy rain storms)
- A car wash damaging ADS hardware
- If "computer centres" or charging stations are near a large refrigerator, every time it turns on or off there is the risk of severe damage, caused by fast transients induced into power or communication lines
- Other kinds of power surges have been known to blow up key equipment
- Electrostatic charge can be built up by humans (e.g. by sliding across seats). Discharge (sparks) can lead to extensive damage to control screens, sensors, etc.
- Extremes in temperature and/or humidity can be disastrous. Or something like a heavy rain storm could disable and destroy key sensors
- Bridges and tunnels can stop communications (e.g. the "cage bridge" at the start of the Tullamarine Freeway, or the long tunnels under the Yarra river)
- Bumpy roads can lead to sensors being dislodged or damaged

- Low bridges may knock off key equipment (e.g. like the South Melbourne railway bridge, which gets one or two trucks stuck every year)
- Flooded roads
- Failure of the system due to dust or a leaf on an AV
- Electromagnetic pulse disturbance (lightning)
- Precipitation (rain, snow, mist, sleet, hail, fog)
- Other atmospheric obscurants (dust, smoke)
- Night conditions without illumination
- Low sun angle glare
- Glare from snowy and icy surfaces
- Reduced road surface friction (rain, snow, ice, oil)
- High and gusty winds
- Road surface markings and signs obscured by snow/ice
- Road surface markings obscured by reflections off wet surfaces
- Signs obscured by foliage, or displaced by vehicle crashes

4.3.8 Dynamic External hazards

- Behaviours of other vehicles:
  - Entering from blind driveways
  - Violating traffic laws
  - Moving erratically following crashes with other vehicles
- Law enforcement (sirens and flashing lights)
- Law enforcement - officers directing traffic
- Pedestrians (especially small children)
- Bicyclists
- Animals (from domestic pets to large wildlife)
- Opening doors of parked cars
- Unsecured loads falling off trucks
- Debris from previous crashes
- Landslide debris (sand, gravel, rocks)
- Any object that can disrupt vehicle motion.

4.3.9 Internal Faults

- Mechanical and electrical component failures
- Computer hardware and operating system glitches
- Sensor condition or calibration faults requiring more fundamental breakthroughs
- System design errors
- Undiagnosed faults in the vehicle
- System specification errors

- Software coding bugs
- Software bugs not exercised in testing

4.3.10 Future road planning and management

- Lack of ability and resources for transport authorities and road authorities to plan and invest in the road infrastructure required to support AVs
- Ability for local government, police and authorities to manage and monitor appropriate and safe use of the road network, in order to reap the benefits of the AV technology – reduce congestion and safety
- A basic set of threshold or minimum requirements for stopping, parking, and road infrastructure requirements

4.4 Opportunities to plan better safety and transport outcomes

If States and Local Governments have the responsibility to plan, manage and maintain the road and transport network, then States and Local Governments need to be directly involved in the deployment and use of AVs.

States, Local Government police and the community, therefore, need to have direct input into the approval and opportunities that AVs provide to the community. There could be partnership opportunities developed to upgrade road infrastructure, and provide more innovative transport solutions.

The City of Melbourne[6] recently reported:

- Automation has many implications for Melbourne. Some of these implications, be they opportunities or challenges, will depend on how the technology is deployed. For example, forecasts indicate that private automation is likely to increase the number of trips on the road, leading to rising congestion and urban sprawl.
- Some of these issues, however, might play out in unknown ways. Access and equity issues are a particular area of uncertainty, and researchers have made widely differing predictions about whether automation will reduce or increase the cost of transport for those vulnerable to economic and other changes.

Other recent reports also suggest that AVs will need to be deployed as part of a coordinated and integrated transport plan, developed on both a State and local level.

4.5 National Government Regulator

A new 'national' government agency with the responsibility for administering a safety assurance system may not bring any benefits.

For example, the new government agency may potentially:

- overlap with registration and licensing, which is a State responsibility

[6] City of Melbourne (2018) Background paper: impacts of emerging transport technology on the City of Melbourne. (p.20) **See link:** https://participate.melbourne.vic.gov.au/application/files/7915/2635/8581/Transport_Strategy_Refresh_-_Background_paper_-_Emerging_transport_technology.pdf

- duplicate existing product liability/OHS/ Consumer protection
- limit the States' and local Government's capabilities to monitor and manage the use of automated vehicles, to reap the benefits of the technology for the community. The preferred option fails to recognise that the State and Local Government plan manages and maintains road infrastructure, and the transport system.
- add complexity and not recognise that the States, police and Local Governments will have key roles in making sure that these vehicles are only used within its ODD, but also on appropriate roads and conditions
- be too slow to respond to immediate safety issues. For example, not able to read traffic signs and respond to being hacked
- duplicate the roles and responsibilities of police and local governments in law enforcement. How would police enforce current road rules when the vehicle is in automated mode? Would the model undermine the enforcement of current road rules and traffic law?
- be effective in ensuring there is a safety assurance framework for new vehicles being deployed, however, the RIS fails to explain how the proposed option will effectively manage modified vehicles, and the inappropriate use of automated vehicles
- A single national regulator is not able to best manage driving risks, faults and failures through investigations and penalties based on primary safety duty. It would be too slow to respond to key safety and security risks... and possibly ineffective.

The US Government Accountability Office [7] recently reported:

"Policymakers have regulatory and enforcement tools to assure that vehicles on the road are safe, but these tools may need to be modified or enhanced to address automated vehicles, according to stakeholders we interviewed and our literature review. For example, we have previously found that NHTSA faces challenges in conducting defect investigations because of the difficulty in keeping up with changing technologies, among other things. Such challenges might result in difficulty determining when recalls are warranted".

4.6 The full range of regulatory tools available

The NTC should consider the full range of regulatory tools available to it, to manage these risks. Although AV and ADS technology will continue to evolve, it can be predicted that AVs will evolve with connected vehicles, alternative powered vehicles and possibly flying vehicles (e.g. drones). Therefore, the regulatory model needs to have the ability to adapt or respond to risks in a timely and effective manner.

The regulatory model for AVs should be able to take a proactive approach to regulating AVs. This should involve considering all the regulatory tools available that are considered to align, and to not undermine the proven Safe System approach in dealing with the complexity of events that cause road traffic accidents.

iTech believes that the NTC should:

- Further consider its assumptions about the safety of the use of AVs, the complexity of interactions with other road users, road infrastructure and the road environment
- Consider and include the broader use of connected and automated driving technology

[7] U.S. Government Accountability Office (2017) Automated Vehicles: Comprehensive Plan for Department of Transportation (page 12) **(See link: http://www.trb.org/main/blurbs/176953.aspx)**

- Reconsider the options and regulatory tools available to it in order to address the identified problems:
  - ensuring that automated vehicles entering the Australian vehicle fleet are highly** safe. This is in order to avoid the potentially high social cost of poor road safety outcomes
  - providing users with reassurance that automated vehicles are highly** safe, so that a lack of confidence does not become a barrier in the uptake of automated vehicles
  - creating a suitable regulatory environment that is flexible, responsive and does not impose unreasonable costs, so that ADSEs can enter the Australian market.

** we have used the term "highly" safe to mean that an absolute minimum of collisions should be expected.

5 Conclusion

Section 4 above, clearly outlines the areas in which iTech believes that the NTC SAS RIS has not fully identified the extent and magnitude of the risks involved with the introduction of AVs, as well as the complexity of the interactions with other road users, road infrastructure and the road environment.

iTech strongly believes that a suitable NTC regulatory environment will provide assurance that ADSEs can safely enter the Australian market, providing the benefits that the industry and the general public expect. This regulatory environment should encourage independent testing of vehicles under a range of realistic scenarios. We also believe that self-regulation may compromise safety.

We can offer consulting and/or testing services, which will contribute significantly to improving the regulatory environment being proposed. iTech Labs can do this by bringing to the table our 100+ years' collective experience in regulatory environments in the international Online Gaming Systems testing and certification industry, as well as in the public transport industry.

As mentioned earlier, we will be pleased to make ourselves available for any future discussions on the regulation of Automated Driving Systems.