



SNC • LAVALIN

Review of Regulatory Options for Autonomous Vehicles in Australia

Issue No. 1

   snclavalin.com



NOTICE


This document contains the expression of the professional opinion of SNC-Lavalin Rail & Transit Pty Limited (SNC-Lavalin) as to the matters set out herein, using its professional judgment and reasonable care. This document is meant to be read as a whole, and sections or parts thereof should thus not be read or relied upon out of context.

SNC-Lavalin disclaims any liability to the Client and to third parties in respect of the publication, reference, quoting, or distribution of this report or any of its contents to and reliance thereon by any third party.

© SNC-Lavalin Rail & Transit Pty Ltd, 2017. All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, or stored in any retrieval system of any nature, without the written permission of Client, application for which shall be made to Mark Carling, Level 14, 55 Clarence Street, Sydney, 2000.

Title : Review Regulatory Options for Autonomous Vehicles in Australia
Report No. : RTAU/TA4291/No
Issue : 1
Date : 28th July 2017


Originator


..... **Date:** 28th July 2017
Greg Newman *BEng, MBA, MIE(Aust), MIRSE, CPEng, RPEQ, TuV FSE, CAMA, Cert IV Training and Assessment*

Principal Consultant

+61 (0) 400 133 234
greg.newman@snclavalin.com


Checked By


..... **Date:** 28th July 2017
Candice Augur , *MMaintReliabEng , TuV FSEng, BEng(Hons), MIEAust, CISCAM*

Section Lead, Safety and Assurance

+61 (0) 419 403 117
candice.augur@snclavalin.com

Approved By


..... **Date:** 28th July 2017
Mark Carling , *BEng (Hons) CEng MIMechE*

Director, Rollingstock

+61 (0) 410 584 482
mark.carling@snclavalin.com

Distribution

James Williams
Manager Policy – Compliance & Technology | National Transport Commission

1 Executive Summary

Autonomous Vehicles (AV) that do not require human driver input into the driving task for at least part of the journey are expected to arrive on Australian roads from around 2020. Currently there is no explicit regulation covering these automated driving functions. Manufacturers are aiming to ensure automated driving functionality improves road safety, but this technology may also create safety risks for road users.

The National Transportation Commission (NTC) has prepared the "*Regulatory options to assure automated vehicle safety in Australia Discussion Paper*" [Ref 1] seeking feedback on the following issues:

- whether there is a need for explicit regulation of automated driving functions, above existing transport and consumer law;
- if there is a need for regulation, what form this should take;
- how safety of automated vehicle functions should be assessed ;
- the options for a safety assurance system;
- the criteria that should be used to decide among those options; and
- institutional arrangements, road access and compliance.

NTC is seeking feedback on these regulatory options, recognising that the regulatory solution may draw upon elements across these options. Stakeholders are also welcome to propose new regulatory options.

As a party interested in the debate and with experience in the assessment and regulation of safety-critical automated vehicles and with the personal experience of its current staff, SNC-Lavalin Rail & Transit Pty Ltd (SNC-Lavalin) has prepared this document for submission as requested on the NTC website. The objective of this document is to submit SNC-Lavalin's input into the formulation of a legislative framework for the safety assurance system of AV within Australia as per the NTC discussion paper [Ref 1].

SNC-Lavalin have also proposed an alternative regime in Appendix B which combines elements of the self-certification, pre-market and accreditation models which are currently expressed in the "*Regulatory options to assure automated vehicle safety in Australia Discussion Paper*" [Ref 1].

SNC-Lavalin welcomes the opportunity to further discuss the findings in this document with NTC or any other interested stakeholders. Our point of contact for this submission is Greg Newman and Candice Augur.



Intentionally
blank page

Contents	Page
1 Executive Summary	4
2 Introduction	8
2.1 Background	8
2.2 Objective of this Document	8
2.3 Structure of This Document	9
2.4 Glossary of Abbreviations and Acronyms	9
3 SNC-Lavalin Involvement in Automation of Vehicles	10
3.1 Initial Approach to NTC	10
3.2 SNCL's involvement in the Safety Assessment of Automated Systems	10
3.3 SNCL's experience in assessing safety within an Australian Regulatory Framework	10
3.4 Prior Reading	10
4 Commentary on the Discussion Paper	12
4.1 Review of the Discussion Paper	12
4.2 General Experience	12
5 Consultation Questions	15
5.1 Question 1	15
5.2 Question 2	16
5.3 Question 3	19

5.4	Question 4	20
5.5	Question 5	24
5.6	Question 6	26
5.7	Question 7	27
5.8	Question 8	28
5.9	Question 9	29
5.10	Question 10	30
5.11	Question 11	31
5.12	Question 12	32
6	Conclusions	35
7	Recommendations	36
8	References	37
	Appendices	38
	Appendix A General and Specific Commentary	39
	Appendix B Hybrid Accreditation Model (Self Certification / Pre-Market Approval / Accreditation)	44
	Amendment Record	48

2 Introduction

2.1 Background

Autonomous Vehicles (AV) that do not require human driver input into the driving task for at least part of the journey are expected to arrive on Australian roads from around 2020. Currently there is no explicit regulation covering these automated driving functions. Manufacturers are aiming to ensure automated driving functionality improves road safety, but this technology may also create safety risks for road users.

The National Transportation Commission (NTC) has prepared a the *Regulatory options to assure automated vehicle safety in Australia Discussion Paper* [Ref 1] seeking feedback on the following issues:

- whether there is a need for explicit regulation of automated driving functions, above existing transport and consumer law;
- if there is a need for regulation, what form this should take;
- how safety of automated vehicle functions should be assessed ;
- the options for a safety assurance system;
- the criteria that should be used to decide among those options; and
- institutional arrangements, road access and compliance.

NTC is seeking feedback on these regulatory options, recognising that the regulatory solution may draw upon elements across these options. Stakeholders are also welcome to propose new regulatory options.

As a party interested in the debate and with experience in the assessment and regulation of safety-critical automated vehicles and with the personal experience of it current staff, SNC-Lavalin Rail & Transit Pty Ltd (SNC-Lavalin) has prepared this document for submission as requested on the NTC website.

2.2 Objective of this Document

The objective of this document is to submit SNC-Lavalin's input into the formulation of a legislative framework for the safety assurance system of AV within Australia as per the National NTC discussion paper [Ref 1].

SNC-Lavalin have also proposed an alternative regime in Appendix B which combines elements of the self-certification, pre-market and accreditation models which are currently expressed in the *Regulatory options to assure automated vehicle safety in Australia Discussion Paper* [Ref 1].

2.3 Structure of This Document

Provided below is an overview of this document:

- Section 1, Executive Summary provides a high level summary of this document and the findings presented.
- Section 2, Introduction provides a background to the review and overview of the objective and subsequent structure of this review;
- Section 3, SNC-Lavalin Involvement in Automation of Vehicles provides a background of SNC-Lavalin previous involvement with Autonomous Vehicles
- Section 4, Commentary on the Discussion Paper. This section provides both SNC-Lavalin commentary on the “*Regulatory options to assure automated vehicle safety in Australia Discussion Paper*” [Ref 1] and also SNC-Lavalin’s general reflections regarding safety assurance, assessment, certification and regulation based upon the experience of the SNC-Lavalin Safety & Assurance Section.
- Section 5, Consultation Questions presents SNC-Lavalin’s specific answers to the twelve (12) Consultation questions presented within “*Regulatory options to assure automated vehicle safety in Australia Discussion Paper*” [Ref 1] .
- Section 6, Recommendations provides a summary of SNC-Lavalin’s recommendations made in the context of the review of “*Regulatory options to assure automated vehicle safety in Australia Discussion Paper*” [Ref 1] .
- Section 7, Conclusion provides the high level summary of this document and the findings presented.

2.4 Glossary of Abbreviations and Acronyms

The following abbreviations and acronyms are used within this document.

Abbreviation	Description
ADR	Australian Design Rules
AV	Autonomous Vehicle
RSNL	Rail Safety National Law
NTC	National Transport Commission
ONRSR	Office of the National Rail Safety Regulator
SFAIRP	So Far As Is Reasonably Practicable
SRAC	Safety Related Applicable Condition

3 SNC-Lavalin Involvement in Automation of Vehicles

3.1 Initial Approach to NTC

For some years staff within our Safety & Assurance Section at SNC-Lavalin, have been monitoring the development of AV and have been interested in the development of the safety justification and potential regulation of AV's as they move from developmental prototypes to mass produced forms of transport and their deployment into the Australian transportation scene.

SNC-Lavalin approached Mr James Williams, Manager Policy – Compliance & Technology; National Transport Commission via email on 29th June 2017 [Ref 13] and in a following teleconference held on the 10th July at which SNC-Lavalin was invited to participate more fully in the activities of the NTC.

3.2 SNCL's involvement in the Safety Assessment of Automated Systems

For nearly a decade, our team of safety and assurance specialists at SNC-Lavalin have been involved with the development of automated and driverless technology for rail systems. SNC-Lavalin's engagement as Independent Safety Assessors (at the system/railway level) has seen the Safety & Assurance Section providing oversight to the development on the requirements capture and analysis phase, through system integration and, currently, the preparations for transfer to in-service operation and the seeking of the Variation to Accreditation through National Rail Safety Regulator (ONRSR).

3.3 SNCL's experience in assessing safety within an Australian Regulatory Framework

Being from the rail industry, SNC-Lavalin's experience is predicated on the Rail Safety National Law (RSNL) [Ref 2] (as implemented on a state-by-state-basis), or the prior State-based Rail Regulatory regimes. SNC-Lavalin acknowledges that the RSNL [Ref 2] is based around a co-regulatory model which differs somewhat from the regulatory model proposed in the Nova Systems report "*Safety Assurance Systems for Automated vehicles in Australia*" [Ref 3].

3.4 Prior Reading

As part of the development of this document, SNC-Lavalin has performed an independent review of the "*Safety Assurance Systems for Automated vehicles in Australia*" [Ref 3] as preparation for this submission and confirm SNC-Lavalin broad based support for the content and recommendations given therein specifically noting the following:-

- The assertion that there are three core elements to safe operation of an AV:- Vehicle Technical Integrity, the Operating Environment, and Human Performance;
- The benefits of a case-by-case risk-based approach to regulation in terms of its efficacy and accommodation of technological innovation on the part of the AV designers;
- The assertion that simple testing and inspection, on their own, are inadequate for the certification of highly complex, software-intensive, safety-critical products such as AV's;
- The need for configuration management of the AV;
- The need for continuing safety assurance of the AV; and
- The assertion that a very specific and uncommon set of engineering skills is necessary for the evaluation of AV's.

SNC-Lavalin would, however, contend that the demonstration that safety risks have been either eliminated or reduced so far as is reasonably practicable, will play a larger part in the overall assessment process that inferred in the *"Safety Assurance Systems for Automated vehicles in Australia"* [Ref 3]. SNC-Lavalin recommends that stakeholders involved with the development of the Regulatory Options for Autonomous Vehicles in Australia review the ONRSR *"Meaning of Duty to Ensure Safety So Far As Is Reasonably Practicable Guideline"* [Ref 4].

4 Commentary on the Discussion Paper

This section provides both SNC-Lavalin commentary on the *“Regulatory options to assure automated vehicle safety in Australia Discussion Paper”* [Ref 1] and also SNC-Lavalin’s general reflections regarding safety assurance, assessment, certification and regulation based upon the experience of the SNC-Lavalin Safety & Assurance Section.

4.1 Review of the Discussion Paper

There are two (2) aspects of the review of the *“Regulatory options to assure automated vehicle safety in Australia Discussion Paper”* [Ref1].

- Specific commentary on cited paragraphs or sections of the *“Regulatory options to assure automated vehicle safety in Australia Discussion Paper”* [Ref 1]; and
- General commentary on the subject matter of the *“Regulatory options to assure automated vehicle safety in Australia Discussion Paper”* [Ref 1].

For contextual readability, these two forms are interleaved within a tabular structure which follows the structure of the *“Regulatory options to assure automated vehicle safety in Australia Discussion Paper”* [Ref 1].

These are provided in Appendix A.

4.2 General Experience

Following the review of the *“Regulatory options to assure automated vehicle safety in Australia Discussion Paper”* [Ref 1], SNC-Lavalin compiled a list of observations which are aimed at providing guidance on the formulation of policy. These are provided on the basis of:-

- a) SNC-Lavalin experience in the safety assessment and certification of highly complex, software-intensive, safety-critical products; and
- b) SNC-Lavalin experience with the regulatory framework (strengths and weaknesses) as it applies in the rail industry under the Rail Safety National Law [Ref 2].

These observations which are aimed at providing guidance on the formulation of policy are provided in the table below.

Table 1: General Experience Commentary

Issue	Commentary
1	Co-Regulation
1.1	The state-by-state co-regulatory model, as applied in the rail industry, appears to have evolved into a model whereby, on a state-by-state basis “You tell us how (un)safe you want to be and how you are going to achieve it, and we will hold you to it”.
1.2	It appears to produce differing safety results across differing railways, the extension of which, if applied to AV’s, SNC-Lavalin is of the opinion that it would not be acceptable to the general public. It may result in an AV journey from Brisbane to Melbourne being conducted in three different driving modes which have to change at the various state borders.
1.3	Even a national (as opposed to a state-by-state) co-regulatory model may result in a “lowest common denominator” approach to safety.
2	Testing Versus Assurance
2.1	Ultimately for AV’s there will be safety requirements that are complex but still must be validated. Testing is only one of several ways of confirming that a requirement has been met (validation). The others are demonstration, inspection and analysis. The level of complexity of the AV functions will, in SNC-Lavalin’s experience, require both testing and analysis in order to fully validate these safety requirements.
2.2	Analytical process standards (compliance to which is assured by appropriate surveillance/regulation) are far more effective in a complex, rapidly changing application domain, than (only) testing against prescriptive design standards
2.3	Testing is best suited to non-functional requirements and is not suited to complex functional requirements implemented by software and/or electronic hardware.
3	Competency and skill sets

Issue	Commentary
3.1	<p>The skills necessary to firstly achieve safety of electronic systems (the manufactures) and then robustly to assess their safety (Regulation) are:</p> <ul style="list-style-type: none"> a) extensive; b) diverse; and c) technically complex. <p>They are therefore rare.</p> <p>These issues will impact both the development and regulation of the AV space. AVs are coming; in fact some would argue that with the current sale of vehicles that have "intelligent cruise control", they are already here.</p> <p>There is no effective regulatory model that does not intrinsically rely on this extensive and diverse skill set. Indeed assessing the competency and skill set of those developing and regulating such systems will be a necessary. EN50128 [Ref 6] has much to say about the necessary competence of such people.</p>

5 Consultation Questions

The “Regulatory options to assure automated vehicle safety in Australia Discussion Paper” [Ref 1] specifically requests responses to twelve (12) Consultation questions. The sub-sections below record SNC-Lavalin’s considered responses to these questions.

5.1 Question 1

Should government have a role in assessing the safety of automated vehicles or can industry and the existing regulatory framework manage this?

What do you think the role of government should be in the safety assurance of automated vehicles?

Yes, the government should have a role in assessing the safety of automated vehicles. The exiting regulatory framework is not adequate to cover the safety of complex, high integrity electronic hardware and software, relying as it does on testing.

SNC-Lavalin’s experience on the development and application of high integrity, complex electronic hardware and software (within the rail industry) makes it clear that testing alone is insufficient for the assessment and certification of safety critical systems. The complex functionality of such systems can only be assured by rigorous implementation of safety assurance processes and of software development measure and techniques, the details of which cannot be fully confirmed by testing only, but rather must be assured throughout the development life (and operational) life-cycle.

The rail industry relies on implementation of three key standards:

- EN50126 [Ref 5];
- EN50128 [Ref 6]; and
- EN50129 [Ref 7].

These are the railway-specific implementation of the overall IEC61508 referred to in “*Safety Assurance Systems for Automated vehicles in Australia*” [Ref 3]

SNC-Lavalin opinion is that the governments’ role in the safety assurance of automated vehicles should be to:-

- Develop automated vehicle safety criteria;
- Assess initial functions against criteria/standards;
- Assess changes to initial functions against criteria/standards;

- Monitor ongoing safety performance of vehicles (modelled on the Mandatory Reporting activities as per the RSNL [Ref 2]);
- Monitor ongoing compliance; and
- Report defects/ product recalls.

SNC-Lavalin has proposed an alternative regime in Appendix B which combines elements of these roles as currently expressed in the “*Regulatory options to assure automated vehicle safety in Australia Discussion Paper*” [Ref 1] .

5.2 Question 2

Should governments be aiming for a safety outcome that is as safe as, or significantly safer than, conventional vehicles and drivers?

If so, what metrics or approach should be used?

As stated in the *Regulatory options to assure automated vehicle safety in Australia Discussion Paper*” [Ref 1] at § 3 page 23, the current level of road safety is based on four pillars:

- Safe vehicles;
- Safe people;
- Safe roads; and
- Safe speeds.

In reality, the Safe Speeds pillar is just a part of the Safe People pillar in that it is the driver of the car that continually makes the decision as to what represents a Safe Speed, noting that the roads themselves are also “labelled” with a maximum legal speed limit which imposes an upper bound on what might reasonably constitute a Safe Speed.

It should also be noted that when an otherwise “safe road” is damaged, then it falls to the “safe driver” to notice this and to amend their judgement of (among other things) what constitutes a safe speed (noting that applying steering input to avoid the damaged section of road is most often also required).

By and large the driver does an excellent job of performing these safety functions and it is only when the driver is in some way performing “below specification” that safety becomes compromised. This may be due to the effects of tiredness, drugs or alcohol, distraction, inattention to task.etc.

With automated vehicles, the claim is made that such things will not be an issue and that therefore an automated vehicle (all other things being equal) will be safer than a driver.

What this line of argument omits is that the vehicle automation systems must take over the decision making functions and perform these just as accurately and just as reliably as or better than a driver (in terms of error or failure rate). Hence the contribution to safety currently provided by a driver must now be shared across the other two independent pillars, that is shared between safe vehicles and safe roads.

Further, if roads are to remain largely as they are, then the vast majority of this burden for safety falls upon the automated vehicle and hence the automated vehicle must have a much higher level of safety.

With automated vehicles, we are now in the realm of functions (steering, braking accelerating, detecting etc.), the failure of which can lead directly to human harm. This is Functional Safety as defined in Clause 3.1.12 of *IEC61508: 2010 Functional safety of electrical/electronic/programmable electronic safety related systems* [Ref 8] (and railway derivative standards EN50126 [Ref 5], EN50128 [Ref 6], and EN50129 [Ref 7]) with each defining a safety function having an associated probability of failure (under a defined operating environment). Depending on the industry, this can be expressed as a Wrong Side Failure Rate, a Tolerable Hazard Rate, or, at the design/development stage, as a Safety integrity level.

However it may be expressed, the correct way of conceiving the question of how to measure safety of a function is by *"the rate of occurrence of incidents that result in harm to people"* (on the understanding that in this definition, the term "people" relates to all people, not just the driver or occupants of the vehicle in question, but also any person within the vicinity of the autonomous vehicle. Any other measure is inadequate for addressing this issue.

A *"crash rate"* or *"fatality rate"* is a reactive, post-factum measure and will simply measure how safe the system wasn't. In order for this measure to even reveal that, it is necessary to deploy a large number of autonomous vehicles into the general public, and potentially to harm many of them.

5.2.1 Additional Commentary Regarding Risk Managed SFAIRP

Reducing risks So Far As Is Reasonably Practicable (SFAIRP) is a key concept in safety. In contrast to the concept of a numerical *"rate of occurrence of incidents that result in harm to people"*, it introduces the notion that there is a balance to be made between the degree of further reduction in harm which can be achieved, and the effort (measured in terms of time, trouble, cost etc) in achieving that further reduction. SFAIRP is a process of demonstration applied to each hazard, not a single number applicable to the overall system.

The rail industry has been developing its understanding of this for some time now and the ONRSR has released its publication *"The Meaning of Duty to Ensure Safety So Far As Is*

Reasonably Practicable" [Ref 4]) This guideline presents a discussion on, and description of, this process and SNC-Lavalin recommends this as a worthy reference source.

The rail industry has recently begun to specify both:

- the achievement of a demonstratable maximum rate of occurrence of incidents that result in harm to people (which is driven by corporate appetite for risk); and
- the application of the SFAIRP process (which is embodied in the Rail Safety National Law [Ref 2]). The former must be achieved and the latter adequately demonstrated.

Please note, however, that the demonstration of SFAIRP usually involves the concept of a Value of Statistical Life (VoSL) (see page 11 of the ONRSR guideline [Ref 4]) or some equivalent. To quote from the guideline:-

"Currently there is no standard VoSL in the Australian rail industry although various values have historically been published by government departments. In 2010 RISSB published its Railway Level Crossing Incident Costing Model⁴ which utilises a VoSL of \$6,287,873 (2010 figures).

SNC-Lavalin is of the opinion that the demonstration of SFAIRP in conjunction with the achievement of a target *"rate of occurrence of incidents that result in harm to people"* is preferable to one or the other.

Even if a target *"rate of occurrence of incidents that result in harm to people"* cannot be agreed upon, the doctrine of SFAIRP contains the following:- **5.2 What the Person Concerned Knows, or Ought Reasonably to Know, About the Hazard or Risk and any Ways of Eliminating or Minimising the Risk** *The knowledge about a hazard or risk, and any ways of eliminating or minimising the hazard or risk, will be what the duty holder actually knows, and what a reasonable person in the duty holder's position (e.g. a person in the same industry) would reasonably be expected to know. This is commonly referred to as the 'state of knowledge'.*

This may read as implying that the target safety level for general functional safety, failures of which can result in injury or death should be the same as for other transport industries (where functional safety is applied) to which the general travelling public are exposed. Generally the default specification for this in the rail industry is Safety Integrity Level (SIL) 4 (risk reduction of 1 exp ^{-9} per hour).

SIL 4 can also be arrived at from the view that there are ways of achieving a SIL 4 result that are commonly practiced around the world (in the rail industry), and that these methods are public knowledge, hence the designers of autonomous vehicles should be expected to know of them as well. These methods are obviously *"practicable"* because they are in widespread use internationally in a parallel industry.

5.3 Question 3

Should the onus be placed on the automated driving system entity to demonstrate the methods they have adopted to identify and mitigate safety risks?

It is SNC-Lavalin opinion that the only option for upon whom the onus of proof of safety should be placed, is the automated driving system entity- Option 3.

Option 3 also flows from the SFAIRP concept discussed above. The only entity in a position to make a SFAIRP argument is the Automated driving system entity, as they best know the costs associated with each risk reduction measure, and how their current (and future) systems do (and will) mitigate these risks.

SNC-Lavalin further proposes that the general process for of this safety validation should be linked to the international functional safety standard *IEC61508: 2010 Functional safety of electrical/electronic/programmable electronic safety related systems* [Ref 8]. It should be clearly understood that IEC61508 [Re8] speaks of how to demonstrate safety, not how to achieve safety. This approach leaves the manufactures free to develop their own safe designs in their own way allowing freedom in the development and implementation of future autonomous systems.

This proof should not be viewed as a self-certification in that the Regulatory body would then assess this body of proof (or have it assessed by a suitably competent and independent body).

Such a doubly augmented approach to Option 3 provides both the freedom for innovative development, and increases the "certainty for government and the community that specific vehicles or technologies will be safe" [Ref 1].

Any safety assurance and assessment system must be in place from the first introduction of commercial autonomous vehicles. The concept of delaying or deferring any safety assurance and assessment regime would allow unproven autonomous vehicles to be "set loose" in the public domain.

As George Stephenson put it, regulation is there *"To prevent wild and visionary schemes being tried out on the public at great risk to life and limb."*

5.4 Question 4

*Are the proposed assessment criteria sufficient to decide on the best safety assurance option?
If not, what other assessment criteria should be used for the design of the safety assurance system?*

The following table records refinements to some of the criteria proposed with a view to transferring observations and lessons learned from the rail industry.

Table 2: Proposed Modifications to Assessment Criteria

Description	Proposed revision	Rationale
Criteria 1: Safety		
The model should support automated vehicle safety, including the ongoing safety over the full lifespan of the vehicle	Nil	Given that an AV may be operated by someone who is no longer paying attention to the vehicle (vehicle noises, behaviour under braking or cornering etc), there might be a need for periodic safety inspections to replace this “real time condition monitoring” that is subconsciously performed by the driver.
The model should provide certainty about who is responsible for testing, validating and managing safety risks.	Nil	
Criteria 2 Innovation, flexibility and responsiveness		
The model should be technology-neutral and allow innovative solutions	Nil	
The model should allow government to respond and adapt to the changing market and evolving technology.	Nil	

Description	Proposed revision	Rationale
Criteria 3: Accountability and Probity		
The model should ensure the decision-making process is transparent, accountable and, where appropriate, appealable	Nil	
There should always be an entity (whether an individual or a corporation) that is legally accountable for the automated driving system.	There should always be an entity (whether an individual or a corporation) that is legally accountable for the safety of the autonomous vehicle automated driving system	This expansion acknowledges that the operational safety will depend variously on the autonomous sub-systems as generic products; the vehicle into which these generic products are incorporated (a generic application), and that there may be some specific action (by way of a Safety Related Application condition) for which the driver is responsible
Criteria 4: Regulatory efficiency		
The assurance process should be as efficient as possible and result in the least cost for industry and government, proportionate to the risk.	The assurance process should be as efficient as possible practicable and result in the least optimal cost for industry and government, proportionate to the risk.	The revised wording acknowledges that there are no absolutes (e.g. "possible", "least") in the trade-off between robustness of regulation and costs.
The process of assurance should minimise structural, organisational and regulatory change necessary to implement the model	Nil	
Criteria 5: International and domestic consistency		

Description	Proposed revision	Rationale
The model should support a single national approach, or state-based approaches that are nationally consistent	The model should support a single national approach, or state-based approaches, or a combination of national and generic state-based approaches that are nationally consistent	This acknowledges that regulation of the vehicles themselves will likely remain at a national level whereas the Safety Related Application Conditions allocated to the road environment and the driver/operator will likely fall to the State level.
The model should support international consistency. International approval processes and standards should be recognisable	The model should support international consistency. There should be a mechanism for the conditional cross-acceptance of products / systems/vehicles approved in other countries. International approval processes and standards should be recognisable	This conditions for cross acceptance should be based in iESM and CENELEC TR-50506-1 Railway applications - Communication, signalling and processing systems - Application Guide for EN 50129 -Part 1: Cross-acceptance [Ref 9]
Criteria 6: Safe operational design domain		
The model should be able to take into consideration the operational design domain of an automated driving system	Nil	
Criteria 7: Other Policy Objectives		

Description	Proposed revision	Rationale
<p>The model should be able to support non-safety policy objectives, including cyber security, traffic management, environmental protection and the provision of data for enforcement or insurance purposes</p>	<p>The model should be able to support non-safety policy objectives, including cybersecurity, traffic management, environmental protection and the provision of data for safety monitoring/regulation/reporting and improvement purposes, as well as for enforcement or insurance purposes</p>	<p>Cyber security will be a defence to the risk of cyber hacking and hence should be identified as a cause of a safety hazard (and dealt with accordingly).</p> <p>Data should be recorded also for the purposes of reporting to NTC (or the regulator) about the safety performance of the autonomous vehicle – similar to the Mandatory reporting requirements of ONRSR (See https://www.onrsr.com.au/operations/reporting).</p> <p>Manufacturers should also record data as an input to their DRACAS systems for the continual improvement of their products.</p>
<p>The model should be able to be implemented and operational when the technology is ready</p>	<p>Nil</p>	<p>The assurance model based on a slightly modified rail safety model, can be ready to go in a short period of time (by approving vehicles for only the very limited road space that meets the SCRACs)</p> <p>To step on the path of self certification is to place one foot over the precipice.</p>

5.5 Question 5

Should governments adopt a transitional approach to the development of a safety assurance system?

If so, how would this work?

In general, the only reason for adopting a transitional approach would be that the preferred final approach cannot be implemented within the necessary timescales.

The case has not been made that the preferred approach cannot be implemented, (albeit with limited capacity).

While the first vehicles with high automation are projected to be available on the market by 2020, the paper does not indicate how many different types of such vehicles will require safety assurance.

Incorporation of a staged or interim certification as used within the rail industry and as indicated by the iESM, could see the first AV model satisfactorily assessed but with a Safety Related Application Condition (SRAC) (i.e. a caveat) that limits its operational domain. Following further assessment, this SRAC on the limitation of operational domain could be progressively lifted as further assessment resources are established.

SNC-Lavalin, with the agreement of the surrieved project, have utilised this approach successfully on a recent project in the rail industry in Western Australia, to the satisfaction of the Western Australia ONRSR.

Also, depending on exactly what architecture these systems utilise, it may also be possible to utilise the concept of a Generic Product Safety case (covering the core automation sub-systems and its sensors, which is assess as satisfactory albeit perhaps with some Safety Related Application Conditions to be “passed up” to the Generic Application Safety Case, which is turn assess as satisfactory, again albeit perhaps with some SRACs to be fulfilled generally in terms of requirements on the owner/driver, maintenance regime and/or limitations on the operational domain and parameters).

The process is described in EN50129 [Ref 7] at Clause 5.5.2 from which the following diagram is taken.

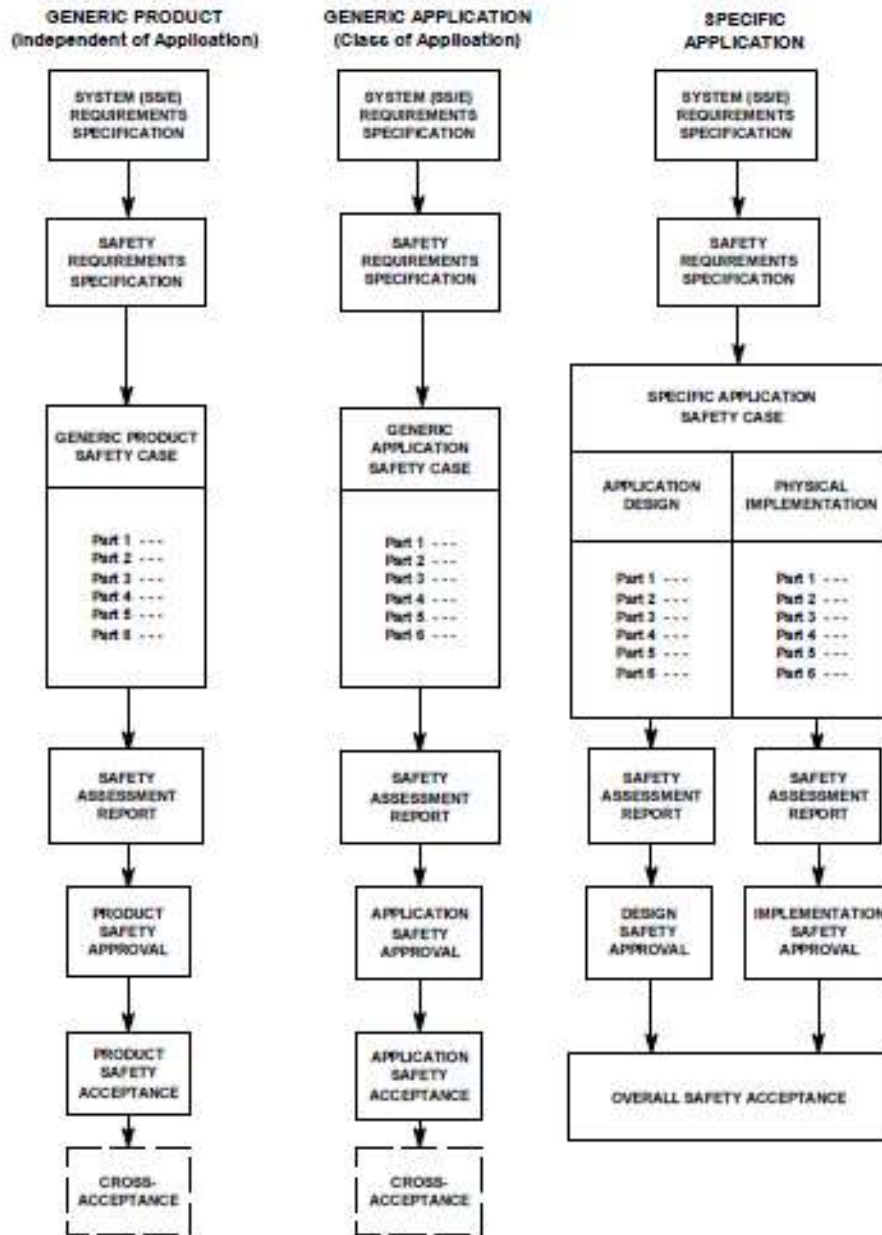


Figure 1: Safety Case Model

This model is used extensively in the rail industry and allows for considerable re-use and cross-acceptance of safety certifications. Additionally, the *international Engineering Safety Management* publication [Ref 12] at Chapter 12, provides guidance on cross acceptance of existing safety approvals.

By way of an exemplar scenario, consider the following:

The core AV sub-systems comprised sensors, a computational device comprising electronic hardware and software (which has the capability to “read” application data like GPS maps, and sets of road rules etc.), and output drivers (but not the actuator mechanisms). This could be assessed as satisfactory but with SRACs’ placed possibly in the characteristics of the vehicle into which it is incorporated and limitations upon its use.

Such an assessment might read thus: “This core AV sub-system is safe to use but only in vehicles with electric steering boxes (of type A or B), only on paved roads, only in conditions of no fog, and only below 100 kph”. The manufacturers of the subsystem install a speed limiting function (again subject to assessment) that fulfils the speed limitation SRAC.

This subsystem may then be incorporated into not one but several different models (or even makes) of car all of which have electric steering boxes of either type A or B (the fulfilment of the first SRAC) and the remaining SRACs (paved roads, no fog) are passed on to the driver or others. The safety assessment then only needs to address the fulfilment of the SRAC’s and any hazards relating to the way in which this AV subsystem is installed into the various vehicle types. This assessment would produce a Generic Application Safety report. This report would be analogous to the concept of “Type Approval”.

Each manufactured vehicle would then be subject to the usual production quality assurance processes as they are today, with additions specifically for the installation of the AV subsystems and for the target operational domain (i.e. Australia as opposed to say Britain).

SNC-Lavalin experience shows that the majority of safety assurance and assessment effort is at the Generic Product level.

Thus AV subsystem X could be assessed once, then incorporated in make/model A, make/model B, and make/model C etc, each of which would then only require assessment of a Generic Application safety assurance program which is less effort-intensive than assessing, from scratch, each of make/model A, B, and C.

5.6 Question 6

Is continuing the current approach to regulating vehicle safety the best option for the safety assurance of automated vehicle functions?

If so, why?

The continuance of the current approach is not a tenable situation as there are currently no Australian Design Rule (ADR)’s that cover AVs. In effect, this would mean that AV’s were “unregulated” until such time as ADRs specific and relevant to AV’s are developed.

ADRs are generally aimed at a particular control measure in respect of a particular hazard cause; by either reducing the likelihood of an accident (e.g. brake pads) or reducing the resultant consequences (e.g. airbags and seatbelts). By their very nature they cannot be targeted against the new hazards (or hazard causes) implicit in AV's until such time as the technology is fully developed. Given that the greatest scope for causing a hazard resides with the possibility of defective software, it is also not clear how an ADR can be specified, after the software is developed, in relation to any hazard cause.

The explicit reliance on Consumer Law, only becomes effective after an accident has happened whereas the assurance approach is aimed at reducing the likelihood of a defect being present in the first place. There is also the issue of whether Consumer Law would operate in relation to a bystander (someone who did not have a legal relationship with the product manufacturer through the purchase of the AV).

5.7 Question 7

Is self-certification the best approach to regulating automated vehicle safety?

If so, should this approach be voluntary or mandatory?

Should self-certification be supported by a primary safety duty to ensure automated vehicle safety?

It is SNC-Lavalin experience that self-certification is not a successful concept in the long run, and certainly not for new and innovative technology.

With the concept of self regulation, there appears to be little to protect road users (and indeed pedestrians) from the type of corporate behaviour evident recently at VW [Ref 14] where they knowingly introduced a new functionality into the engine management system of some of their diesel powered cars, in order to achieve falsely claimed fuel economy while also meeting vehicle emission standards and power performance figures. It took several years for this to be uncovered via a "Consumer Law" or "product liability" approach.

The Self-certification approach, if modified, could involve mandatory compliance with AV safety principles and criteria. In the rail industry, this is called a Safety Case. It is a compelling justification, logically constructed and based on verifiable evidence, that a product meets a set of adequate and rigorously derived safety requirements, and is fit for an intended purpose. The rail industry has a standard (EN50129 [Ref 7] that governs the mandatory content of such a document, and it relies on the application of processes defined in EN50126 [Ref 5] and EN50128 [Ref 6]. Making a false or misleading claim should be an offence.

If an interim state for regulation cannot be avoided, then such a prescriptive process for the justification of safety could be applied with each AV manufacturer compiling and publishing the safety case for each vehicle type. This could result in an interim certification from a legislative

point of view. Once sufficient resources have been assembled, the independent assessment agent would then assess the safety case, and if it is favourably assessed, then the interim status could be lifted to permanent.

SNC-Lavalin have proposed an alternative regime in Appendix B which combines elements of the self-certification, Pre-market and Accreditation models as currently expressed in the discussion paper [Ref 1]. This alternative model takes the following from the self-certification model:-

- Manufactures make a mandatory claim for the safety of their AV's in relation to safety criteria (which are not prescriptive of a solution). The safety criteria are an overarching responsibility for safety and demonstration that risks associated with the automatic driving system have been reduced So Far As Is Reasonably Practicable (SFAIRP);
- ADR's and existing safeguards continue to apply; and
- Overseas approval are considered in a manner as described in CENELEC TR-50506-1 Railway applications - Communication, signalling and processing systems - Application Guide for EN 50129 -Part 1: Cross-acceptance [Ref 9].

5.8 Question 8

Is pre-market approval the best approach to regulating automated vehicle safety?

If so, what regulatory option would be the most effective to support pre-market approval?

As a concept, SNC-Lavalin recommends a Pre-market approval approach to regulation, but not entirely as described in the discussion paper [Ref 1].

SNC-L have proposed an alternative regime in Appendix B which combines elements of the self-certification, Pre-market and Accreditation models as currently expressed in the "*Regulatory options to assure automated vehicle safety in Australia Discussion Paper*" [Ref 1] . This alternative model takes the following from the Pre-market approval model:-

- Automatic driving systems are certified by a government agency (or an approved third part on its behalf) as meeting not minimum required technical standards, but as having produced a compelling safety case that their system meets the revised safety criteria of an overarching responsibility for safety and demonstration that risks associated with the automatic driving system have been reduced So Far As Is Reasonably Practicable (SFAIRP);
- The government developed (or secures access to) expertise to assess these safety cases. It does not, however, rely solely on testing;

- The manufacture still reports safety-critical events (and other statistics/occurrences) to government and still seeks reapproval of any changes to the approved system baseline (via an update to its safety case);
- There is an onus on the government to adequately have the safety case assessed, but the onus for safety still rests with the AV systems manufacturer;
- ADRs continue to apply; and
- Able to recognise equivalent processes in the manufactures home country but in a manner as described in CENELEC TR-50506-1 [Ref 9].

5.9 Question 9

Is accreditation the best approach to regulating automated vehicle safety?

If so, why?

There appears to be an important distinction here in relation to accreditation which has gone unnoticed. In the rail industry, operators and maintainers are accredited for their day to day operations. They are not accredited for the development of new products or physical/electronic systems. The difference here is exemplified by the difference between the operation of a road traffic management centre (which manages the safe operation of the traffic which comprises a multiplicity of cars), and the safety of the car itself.

Accreditation, as proposed in the *"Regulatory options to assure automated vehicle safety in Australia Discussion Paper"* [Ref 1] assumes that the accredited automated driving system entity is accredited once with no regular surveillance to ensure that those procedures, processes, measures and techniques as supported by underlying corporate activities such as quality assurance, configuration management, and competency management etc.

SNC-Lavalin have proposed an alternative regime in Appendix B which combines elements of the self-certification, pre-market and accreditation models as currently expressed in the *"Regulatory options to assure automated vehicle safety in Australia Discussion Paper"* [Ref 1].

This alternative model takes the following from the Accreditation model:-

- It is the Automatic driving system that is certified (not the automated driving system entity (AV system designer) by a government agency (or an approved third part on its behalf) as meeting as having produced a compelling safety case that their system meets the revised safety criteria of an overarching legal standard of care and

demonstration that risks associated with the automatic driving system have been reduced So Far As Is Reasonably Practicable (SFAIRP);

- There are basic elements of safe design: vehicle integrity, environment (including operational design domain) and driver (including human machine interface);
- There are no proscribed technical (physical) standards, rather a responsibility to have implemented a holistic process standard – IEC61508 [Ref 8];
- Safety-critical changes to functionality and errors are reported to government in a manner modelled on the Mandatory Reporting activities as per the RSNL;
- ADRs continue to apply; and
- Able to recognise equivalent processes in the manufactures home country but in a manner as described in CENELEC TR-50506-1 [Ref 9].

5.10 Question 10

Based on the option for safety assurance of automated vehicle functions, what institutional arrangements should support this option?

Why?

SNC-Lavalin recommends Option 1 ahead of Option 2. Options 4 and 5 are not recommended. No view is expressed on Option 3.

This recommendation is based on the assumption that AV's (indeed any single AV) may need to travel anywhere within Australia. The listed dis-benefits of each model are discussed briefly below.

- **Option 1 – Commonwealth**

It is not clear who will accredit the accredited certifiers or how. It is not clear why or how it would necessarily duplicate some state and territory functions for non-automated vehicles. The proposed Commonwealth Entity could be placed under the auspices of the Vehicle Standards Branch, thereby avoiding such overlap. Agreed that it will take time to establish and processes and ensure technical expertise is available, but useful processes already exist within the rail industry and the necessary technical expertise can be found in rail, defence and aviation. Any option is going to require staff, resourcing and capability (with the associated costs), so it is not clear why this is a problem uniquely for this option.

- **Option 2 – National Entity**

Any option is going to require staff, resourcing and capability (with the associated costs), so it is not clear why this is a problem uniquely for this option. If the national entity was

ONLY responsible for the automation systems and not for the automated vehicles in its entirety, then there would be no duplication across state or territories if the current state/territory schism simply additionally required a certification of the automation systems from this national entity. While it is acknowledged that legislation would be required, the legislation could be closely modelled on the Rail Safety National Law [Ref 2], applied to the automation system, not the operator. This would speed the development and ease the acceptance of the necessary legislation.

- **Option 3 – One State or Territory**

Any option is going to require staff, resourcing and capability (with the associated costs), so it is not clear why this is a problem uniquely for this option. It has not been clearly explained how or why differences in legislation between the states and territories would reduce the effectiveness of the designated state or territory's decisions.

- **Option 4 – Each state or Territory**

This is clearly not a preferred option for the reasons given in the NTC paper [Ref 1].

- **Option 5 – Quasi-government entity**

It is not clear that safety and performance criteria beyond those already listed in the "Regulatory options to assure automated vehicle safety in Australia Discussion Paper" [Ref 1] are actually required.

If this option's scope is confined to the automation systems only and not the entire AV, then the additional administrative step between the ADR approval and the road transport agencies responsible for safety regulation would only be a small one.

While it is acknowledged that states or territories may not accept the entity's recommendations or may feel obliged to do additional work to check them before issuing approvals, this hinges on the credibility of the quasi-government entity and the competency/capability/capacity it has. The issue of competency/capability/capacity is one for any of the proposed options.

If the states and territories are not obligated to accept the entities recommendations, then AV's that are considered safe in one state or territory may not be considered safe in another. This would be a considerable barrier to the adoption of innovation.

5.11 Question 11

How should governments manage access to the road network by automated vehicles?

Do you agree with a national approach that does not require additional approval by a registration authority or road manager?

It is conceivable that particularly advanced Automation systems will be able to dependably determine, in real time, what roads they can and can't safely operate on. If this is the case, and it can be independently assured, then this issue becomes irrelevant for those vehicles because road access will, in effect, be covered by the initial assurance activities. For other AV's, the issue must be addressed by consideration of the safety linkage "safe vehicles<-> safe roads".

Given that the designers of the automation systems will have made their own assumptions or observations about the roads for which they have designed their systems, the burden rests entirely on them to define what constitutes a "safe road" for their particular system. In the SNC-Lavalin proposed model (see Appendix B), this is one of the key Safety Related Application Conditions (SRAC) and must be clearly and unambiguously specified by the Designers. Note that this definition of a "safe road" may be different from one automation system to another.

The question then becomes who is responsible for "surveying" Australia's roads and confirming which roads comply with the SRAC (and hence are "safe" for a particular automation system), and who is responsible for preventing an AV entering an "unsafe" road.

The latter question is easy – the AV itself must only attempt to operate on a road confirmed to be safe for its operation. In any other event, the vehicle must not enter an automated mode of operation, or, if it is moving, it must immediately come to a controlled safe stop.

The former question has some options. Either the AV manufacture undertakes the survey themselves, or the current road manager must undertake the survey and report the results to the AV manufacturer. In either case the Regulating authority and road manager should be advised of the results. The road manager would then take this into consideration when registering a vehicle.

The proposal above is a slight modification to the Option 3: "Road Manager is notified of an access decision", but ensures that compatibility with the road network is adequately addressed which a disadvantage of the Option 3 as was presented.

5.12 Question 12

How should governments ensure compliance with the safety assurance system?

SNC-Lavalin is of the view that a primary safety duty to provide safe automated vehicles is mandatory. Acknowledging, however, that there is no such thing as absolute safety, we would encourage this primary safety duty to be expressed in terms similar to the Rail Safety National Law [Ref 2] in relation to the duty of those who design, manufacture and supply AV's to ensure that risks to safety are either eliminated or reduced so far as is reasonably practicable.

SNC-Lavalin is also of the view that while the AV systems are in control of the vehicle, the human ‘driver’ should retain some level of observation of the vehicles behaviour and should disengage the AV systems if the driver is in any doubt about the safety of the manner in which the vehicle is behaving under the control of the AV systems. Under the option presented in Appendix B, this duty is likely to be a SRAC imposed upon the “driver”.

On the general question of “compliance”, SNC-Lavalin is of the opinion that the AV systems should be required to continually monitor its own condition and operational performance actions (much in the manner of an airplane’s block box flight recorder). These records should be regularly down loaded (for example at the time of periodic service and scheduled maintenance). These records should form the basis of the mandatory periodic reporting to the Regulator. SNC-Lavalin also notes that the collection of such data is also in the AV systems designer’s best interests for product improvement purposes.

SNC-Lavalin is of the opinion that there should also be a mechanism that provides assurance that the approved version of the product is still being manufactured to the approved configuration baseline. To this end SNC-Lavalin would recommend a process, as part of the regulation, modelled upon the requirements of *BS/EN/ISO/IEC 17067:2013 “Conformity assessment – Fundamentals of product certification and guidelines for product certification schemes”* [Ref 10]. These would be implemented by periodic audits of the AV systems manufacturing processes by any organisation with certification to domain knowledge and complying with *BS/EN/ISO/IEC 17065:2012 “Conformity Assessment – Requirements for bodies certifying products, processes and services”* [Ref 11]. The need for such surveillance comes about from the many instances in the rail industry where what were seen as “minor” modifications to approved products (in terms of component substitution, differing construction layouts etc.) have caused failures of safety-critical functions. Given the likely ultimate exposure to society of these potential introduced “defects” (by dint of the sheer number of autonomous vehicles likely to be on the road), any regulatory regime should in appropriate such surveillance. We also note that other regulatory regimes in other countries are likely to require some similar type of regular monitoring and that such monitoring, if performed as described above, should be transferable across international regimes.

SNC-Lavalin recommends a multi-pronged approach to ensuring compliance as follows:-









- Mandatory reporting;
- Financial penalties (with the proposed corporate multiplier of 10) for breaches which relate to “non-safety” functions;
- Issuance variously of notices or orders (paralleling those in the RSNL – for consistency) for breaches which relate to “safety” functions in addition to the above financial penalties;

- A power to require an automated driving system entity to deactivate the automated functions of its vehicles if its accreditation is cancelled; and
- Periodic surveillance in accordance with the principles defined *BS/EN/ISO/IEC 17065:2012 "Conformity Assessment – Requirements for bodies certifying products, processes and services"* [Ref 11].

6 Conclusions

In board terms, SNC-Lavalin agrees with the recommendations made variously throughout the body of the report for the pre-market approval model. The dis-benefits of the pre-market approval model as listed in the “*Regulatory options to assure automated vehicle safety in Australia Discussion Paper*” [Ref 1] can be eliminated or significantly mitigated by making the recommended adjustments to the model. Table 3 below provides an indicative reassessment of the modified Pre-market approval model with justifying commentary.

Table 3: Assessment of Regulatory Options against Proposed Assessment Criteria – Pre-Market Approval (Current v’s modified)

Criteria	Pre-market approval (current)	Pre-market approval (modified)	Commentary
Are safety risks managed?			
Is the model flexible and does it support innovation?			By removing compliance with physical technical standards and replacing this with compliance to a safety demonstration process standard (like IEC61508 [Ref 8]), the regulation model becomes very flexible allowing AV entities to pursue any innovation that they can justify (in the prescribed manner of a safety case) as adequately safe.
Does it support legal accountability and probity?			
Is the regulatory approach efficient?			Using the safety case approach, with cross-acceptance, the regulatory model becomes more efficient as the technology becomes more mature, with a significant step improvement in efficiency at the second generation of each safety case.

Criteria	Pre-market approval (current)	Pre-market approval (modified)	Commentary
Does it support consistency?	F	F	
Can it evaluate a safe operational design domain?	F	F	
Can the model support other policy objectives	F	F	
Can it be implemented within two years?	N	F	By linking pre-market approval to a regulatory model (but at a federal level, and not co-regulatory) derived from the Rail Safety National Law, there is a known-good legislative model that can be adapted (albeit with minor modifications).

7 Recommendations

SNC recommends the consideration of the alternative regulatory model presented in Appendix B. This alternative regime in Appendix B which combines elements of the self-certification, pre-market and accreditation models which are currently expressed in the *“Regulatory options to assure automated vehicle safety in Australia Discussion Paper”* [Ref 1]. Failing this, SNC-Lavalin recommends adoption of the Pre-market approval model but with the modifications suggested in Section 6.8 above.

SNC-Lavalin further recommends that stakeholders involved with the development of the Regulatory Options for Autonomous Vehicles in Australia review the ONRSR *“Meaning of Duty to Ensure Safety So Far As Is Reasonably Practicable Guideline”* [Ref 4].

8 References

Provided below are the details of all documents and citations referred to in this document.

- [1] "Regulatory options to assure automated vehicle safety in Australia Discussion paper"
NTC June 2017
- [2] Rail Safety National Law (South Australia) Act 2012
- [3] "Safety Assurance Systems for Automated vehicles in Australia" 7103-ENG-RPT-001 Issue
1.0, NOVA Systems, dated 16 February 2017
- [4] "Meaning of Duty to Ensure Safety So Far As Is Reasonably Practicable Guideline" (rev
2.0, ONRSR, dated 24 Dec 2014)
- [5] EN50126-1:1999 "Railway applications – The specification and demonstration of
Reliability, Availability, Maintainability and Safety (RAMS)"
- [6] EN50128:2011 "Railway Applications – Communication, signalling and processing
systems – Software for railway control and protection systems"
- [7] EN50129:2003 "Railway applications – Communication, signalling and processing
systems – Safety related electronic systems for signalling".
- [8] IEC61508: 2010 Functional safety of electrical/electronic/programmable electronic safety
related systems
- [9] CENELEC TR-50506-1 Railway applications - Communication, signalling and processing
systems - Application Guide for EN 50129 -Part 1: Cross-acceptance.
- [10] BS/EN/ISO/IEC 17067:2013 "Conformity assessment – Fundamentals of product
certification and guidelines for product certification schemes"
- [11] BS/EN/ISO/IEC 17065:2012 "Conformity Assessment – Requirements for bodies certifying
products, processes and services"
- [12] "international Engineering Safety Management" TPD, Good practiced handbook, Volume
2, Methods tools and techniques for projects; issue 1 April 2013.
- [13] Email from G.Newman to J.Williams, Subject "Autonomous Vehicles", Date 29 June 2017
- [14] Volkswagen Australia, 2017, viewed 27 June 2017 <
https://au.volkswagen.com.au/emission/?&gclid=EAIaIQobChMIrru8me2o1QIV1QcqCh2ddQgNEAAYASAAEgLYbfD_BwE&mkwid=sR563kr9Z_189630776099_vw%20diesel%20scandal_e_c&mtid=27891kna54764&slid=&product_id=&AspxAutoDetectCookieSupport=1
>

Appendices

Appendix A General and Specific Commentary

Provided below are the submission comments of the *"Regulatory options to assure automated vehicle safety in Australia Discussion Paper"* [Ref1]. There are two (2) aspects to this review:

- Specific commentary on cited paragraphs or sections of the *"Regulatory options to assure automated vehicle safety in Australia Discussion Paper"* [Ref 1]; and
- General commentary on the subject matter of the *"Regulatory options to assure automated vehicle safety in Australia Discussion Paper"* [Ref 1].

For contextual readability, these two forms are interleaved within a tabular structure which follows the structure of the *"Regulatory options to assure automated vehicle safety in Australia Discussion Paper"* [Ref 1].

Table 4 General and Specific Commentary against "Regulatory options to assure automated vehicle safety in Australia Discussion Paper" [Ref 1]

Section Reference	Specific Commentary	Generic Commentary
<p>Executive Summary</p> <p>"Automated driving technologies are progressively undertaking more of the driving task, and it is likely this technology will improve road safety, mobility, productivity and environmental outcomes."</p>		<p>As automated functions progressively take over more of the driving functions, drivers will become deskilled and therefore be less capable of taking over the driving task (especially at short notice in the event of system failure).</p> <p>This de-skilling should be taken into account during the design of the systems addressed in their safety justification and included within its independent assessment along with a need for high functional availability and no Single Points of Failure</p>
<p>Page 7, How to evaluate safety</p> <p>"We are seeking feedback on whether safety should be defined and measured according to the rate of technical failure and incidents that result in harm to people, or be based on an agreed metric of safety such as crash rates."</p>	<p>Crash rates will only tell us how safe it wasn't or how lucky we have been so far. It is a post-factum measure and is not appropriate for the prospective measurement of safety</p>	

Section Reference	Specific Commentary	Generic Commentary
<p>Page 7, How to evaluate safety</p> <p>“The NTC is proposing that the onus be placed on the automated driving system entity to demonstrate the methods they have adopted to identify and manage safety risks.”</p>	<p>The driving system entity will have to</p> <ul style="list-style-type: none"> a) Justify the validity of the methods they have adopted to identify and manage safety risks, and b) Demonstrate they these methods have been systematically and rigorously implemented 	
<p>Page 7, Institutional arrangements to support the approach</p> <p>“We are seeking feedback on institutional arrangements, including the types of government entities that could support a safety assurance system.</p>	<p>Given that the safety of an AV revolves around the vehicles itself (which can travel anywhere in the country), the road on which it travels (which are located in the States and vary slightly from State to State) and the human it carries (who is licensed by the State), it seems unavoidable (and entirely logical) that both Federal and State are required for the safety assurance systems</p>	

Section Reference	Specific Commentary	Generic Commentary
<p>Page 7, How to ensure compliance.</p> <p>"We suggest that compliance could be ensured through a primary safety duty for parties to provide safe automated vehicles with associated penalties and/or specific sanctions and penalties for the automated driving system entity"</p>	<p>Agreed but this will involve a SRAC on the roads</p>	
<p>Section 14, Key Terms</p> <p>Safety assurance system means a regulatory mechanism to provide affirmation of the safety performance of an automated vehicle to assure it can operate safely on the network</p>	<p>The definition is not fully correct.</p> <p>It is up to the AVE to make the affirmation (that their system is safe), it is up to the safety assurance system to provide confirmation that the affirmation is credible</p>	

Section Reference	Specific Commentary	Generic Commentary
<p>Page 36.</p> <p>“This approach (option 3) is also aligned with the direction being taken in the US and with rail and WHS regulation in Australia.”</p>	<p>This statement is not entirely correct. While the Rail Safety National Law speaks of reducing risks SFAIRP and the onus of proof being on the protagonist, current practice indicates that the industry players (railway operators) have also defined a set of process specification to the specification and demonstration of high levels of safety integrity (EN50126/8/9) and the suppliers may develop their safety proof (a Safety Case) in accordance with these standardised processes.</p> <p>This is one small but significant step forward from the statement in Option 3.</p>	

Appendix B Hybrid Accreditation Model (Self Certification / Pre-Market Approval / Accreditation)

Provided below alternative regime in combines elements of the self-certification, pre-market and accreditation models which are currently expressed in the “*Regulatory options to assure automated vehicle safety in Australia Discussion Paper*” [Ref 1].

Step 1: AV Entity Initial Application for Approval of Vehicle

The applicant (AV entity) makes an initial request for approval of a vehicle and provides the accreditation agency with a safety case presenting claims that the vehicle is safe for operation on the type of roads specified therein. The safety case (Generic Product or Application) is presented in the format and content defined in EN50126 [Ref 5] and also addresses the issues indicated in the discussion paper [Ref 1] as listed below:-

- Mandatory safe obligations:-
 - Reducing risk SFAIRP
 - Overarching duty of care to provide a safe product.
- Data recording and sharing
- Privacy
- System safety
- Vehicle cyber security
- Human-machine interface
- Crashworthiness
- Consumer education and training
- Registration and certification
- Post-crash behaviour
- Federal, state and local laws
- Ethical considerations
- Operational design domain
- Object and event detection and response
- Fall back (minimal risk condition)
- Validation methods
- Temporary speed zones (such as roadworks)
- Traffic controls (such as stop signs, variable speed signs and traffic lights)
- All likely road conditions (such as unsealed roads)
- All likely environmental conditions (such as dust storms or flooding)
- Interaction with trains and light rail (such as railway level crossings)
- Interaction with vulnerable road users (such as compliance with the one metre rule for cyclists).

It may draw upon other certifications granted for the Generic product, if it is a Generic Application safety case, in accordance with CENELEC TR-50506-1 [Ref 9] or iESM [Ref 12].

The safety case specifies (as Safety Related Application Conditions) the type of roads (or characteristics thereof) for which the applicant assures safe autonomous operation and (again as SRACs) any requirements for operation or maintenance of the vehicle's autonomous systems to assure that the vehicle remains in a state which fulfils the mandatory safety obligations.

Step 2: Accredited Party Independent Assessment

An Accredited party outsourced provider (as a technical expert approved by government) independently assess the Safety Case on behalf of the government against the demonstration of SFAIRP and the overarching duty of care. If the outcome of this assessment is positive, then a recommendation is made to government to certify the vehicle type for operation on the class of roads defined in the relevant SRAC. The accredited party will also make a recommendation as to whether SRAC's imposed upon the driver of the vehicle are significant enough to require a special class of drivers license or simply instructions in the vehicles owner's manual.

Step 3: State and Territory Government Registration of Vehicle Type

State and territory governments allow registration of this vehicle type, and, if necessary create a new class of driver's license.

Step 4: AV Entity On-Going Reporting

The AV entity provides on-going reporting of safety critical events to the government agency (outsourced provider) or approved Accredited party.

Step 5: Government Review of AV Entity On-Going Reporting

Government analyses event information and responds proportionally.

Step 6: AV Proposes Changes to Approved AV









Step 6: The AV entity advises government of a proposed change to the approved AV vehicle baseline (in relation to the autonomous functions) and, in conjunction with the Accredited party outsourced provider (as a technical expert approved by government), reach a decision on whether an update to the safety case is required. If so, then the process recommences from Step 1, but only in relation to the changes (the 'delta') from the currently approved baseline to the new.

Provided below is an indicative responsibility model of the hybrid accreditation model.

Table 5: Indicative responsibility Matrix of Hybrid Accreditation Model

Option/Step	Responsibility				
	Government		Industry/other		
Hybrid Accreditation Model	Government directly	Outsourced provider	Manufacturer	Registered owner	Accredited party
Develop automated vehicle safety criteria	Yes				
Develop detailed safety standards			Yes		
Develop testing protocols			Yes		
Assess initial functions against criteria/standards		<i>Either</i>			<i>Or</i>
Assess changes to functions against criteria/standards		<i>Either</i>			<i>Or</i>
Install upgrades/modifications			<i>Either</i>		<i>Or</i>
Monitor ongoing safety performance of vehicles	<i>Is Report To</i>		<i>Reports</i>		
Address safety defects			<i>Fixes defects</i>	<i>Monitors</i>	
Arrange repairs				Yes	
Monitor ongoing compliance	<i>Any</i>			<i>Any</i>	
Provide data about safety events and incidents			<i>Any</i>	<i>Any</i>	
Recall defects/product recalls	<i>Any</i>	<i>Any</i>	<i>Any</i>	<i>Any</i>	<i>Any</i>

Table 6: Assessment of Hybrid Accreditation Model Regulatory Options against Proposed Assessment Criteria

Criteria	Hybrid	Commentary
Are safety risks managed?		Safety risks will be identified by the AVe (Applicant) and assessed by the Accredited party or outsources technical expert.
Is the model flexible and does it support innovation?		The AVe may innovate as they wish, but the manner in which they present the claim for safety is specified.
Does it support legal accountability and probity?		The AVe remains accountable for the safety of the AV at all times (on the understanding that the SRAC's they nominate are the responsibility of the maintainer or "driver")
Is the regulatory approach efficient?		The initial development and independent assessment of it is initially effort-intensive, but efficiencies in cross-acceptance and updating for further innovation will accrue in this process as time passes and more models/version s are released onto the market
Does it support consistency?		Yes, there is single consistent approach to how safety is claimed and demonstrated.
Can it evaluate a safe operational design domain?		The operational domain is represented in SRAC's which are derived by the AV entity and independently assessed by the Accredited party or outsources technical expert.
Can the model support other policy objectives		Other policy objectives can be added to the list provided in Step 1 of the Hybrid model.
Can it be implemented within two years?		SNC-Lavalin is of the opinion that this accreditation model can be implemented in two years. It is based upon a slight modification to the Rail Safety National Law [Ref 2] – a known good model – and simple administrative extensions to the state and territories drivers licensing processes.

Amendment Record

Issue	Description	Distribution	Date
1	First Issue Released to NTC	James Williams, NTC	28 July 2017