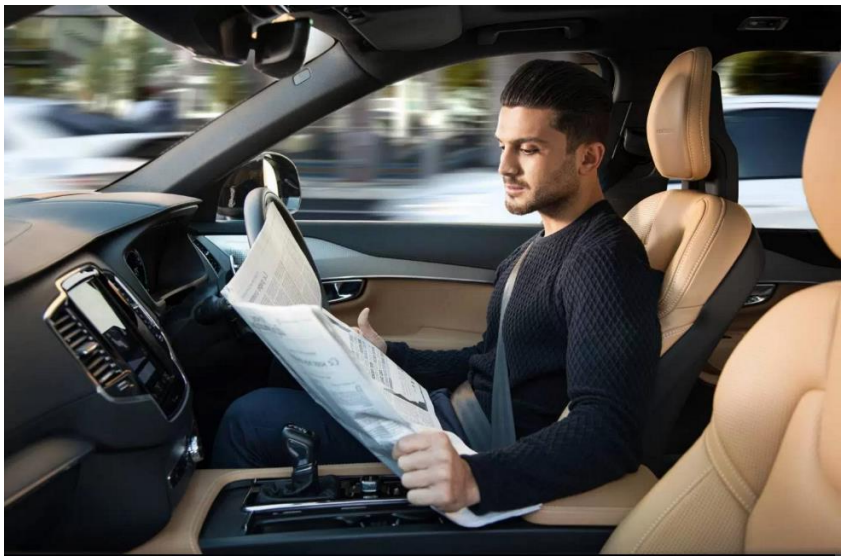
Safety Assurance System for Automated Vehicles in Australia

Nova Systems

Experience Knowledge Independence

February 2017



SAFETY ASSURANCE SYSTEM FOR AUTOMATED VEHICLES IN AUSTRALIA

Prepared for:

THE NATIONAL TRANSPORT COMMISSION

Document Number: 7103-ENG-RPT-001-Issue 1.0

Date: 16 February 2016

Nova Systems
Experience, Knowledge, Independence

APPROVAL RECORD

Prepared by	Signature	Date
Dr Lennard Mitchell PhD, BEng(Elec) Systems Safety and Certification Engineer Nova Systems		16 February 2016
Supported by	**Signature**	**Date**
Mr Dean Boyd-Clark MSc, BEng(Mech) Senior Systems Engineer Nova Systems		16 February 2016
Reviewed by	**Signature**	**Date**
Mr Brett Martin BEng(Aero) Safety and Certification Capability Lead Nova Systems		16 February 2016
Approved & Released by	**Signature**	**Date**
Mr Jim Kira MBA, BTech, BEng(Aero) Program Manager - Transport Nova Systems		16 February 2016

CLIENT ACCEPTANCE

Accepted by	Signature	Date
Mr James Williams National Transport Commission Level 15 / 628 Bourke Street Melbourne VIC 3000		09 March 2017

CHANGE RECORD

It is certified that the changes promulgated in the undermentioned change record have been incorporated in this copy of the Safety Assurance System for Automated Vehicles in Australia.

Issue	Change Type	Approval Date	Version / Change Description
1.0	Initial Issue	16 February 2017	Initial Issue

Point of Contact:

Mr Jim Kira
Program Manager – Transport
Nova Systems
Level 3, 100 William Street
Woolloomooloo NSW 2011
T: +61 (0)2 9043 2512
M: +61 (0)409 690 329
E: jim.kira@novasystems.com

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. Executive Summary

1.1.1. In November 2016 the Australian Transport Council approved recommendations outlined in the National Transport Commission (NTC) policy paper, "*Regulatory reforms for automated road vehicles*" [3]. One approved recommendation was for the design and development of a Safety Assurance System (SAS) for Automated Vehicles (AVs) in Australia.

1.1.2. Nova Systems is an Australian Professional Service Provider (PSP) of engineering services with a focus on complex engineering systems and integration of emerging technologies into established systems. Nova Systems has significant experience with safety assurance systems and consults to major government organisations within this field of regulation and certification.

1.1.3. In early December 2016 Nova Systems was contracted by the NTC to provide the following:

a. A report setting out the options for the development of a national safety assurance system, including potential governance and process models, technical performance requirements and safety validation.

b. A high-level project plan for achieving a national safety assurance system in Australia, considering the time and methods by which such a system might be implemented.

1.1.4. During December 2016 and January 2017 the concepts contained in this report were reviewed with several stakeholders in the Australian AV sector and comments and issues provided by stakeholders have informed the discussion in this policy paper.

1.1.5. This paper documents discussions with stakeholders regarding the nature of a SAS. Stakeholders suggested that the SAS for AVs should:

a. be nationally consistent;

b. adopt a safety case approach based on the risk profile of the application, with responsibility of the applicant to demonstrate the safety performance of the automated vehicle;

c. manage where and how the vehicle can operate;

d. ensure the ability for agencies, police and the National Heavy Vehicle Regulator (NHVR) to read and interpret reliable data, including crash data and who was in control of the vehicle at a point in time;

e. include Human Machine Interface (HMI) requirements;

f. address vehicle modification and maintenance, including over-the-air software updates;

g. ensure safety redundancy;

h. include a mechanism to ensure offshore entities can be held legally responsible for their vehicles and systems;

i. be technology neutral and consistent wherever possible with international developments, taking into consideration international testing results;

j. manage minor road rules breaches; and

k. be aligned with the *"National Road Safety Strategy 2011–2020".*

1.1.6. This report develops a *concept* of a Safety Assurance System that would be able to address these requirements.

1.1.7. The SAS suggested is based around the concept, as demonstrated at Figure 1, that safety can be assured so long as three core elements are addressed in a holistic and systematic manner. These three core elements are:

a. Vehicle Technical Integrity;

b. Operating Environment; and

c. Human Performance.

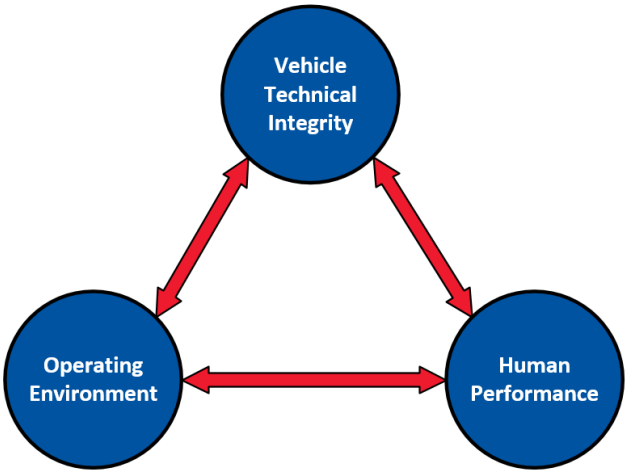


Figure 1: Context of AV Safety Assessment

1.1.8. The SAS structure is based around a two-stage process of:

a. **Initial safety assurance** – which involves establishing and finding compliance against a set of requirements established for a vehicle on a case-by-case basis; and

b. **Continuing Safety Assurance** – which involves controlling the configuration of the vehicle such that the safety findings that were made during the initial investigation remain valid.

1.1.9. The report suggests that the SAS concept developed can be implemented using three organisational entities:

a. Initial Safety Assurance entity (ISAe);

b. Automated Vehicle Entity (AVe); and

c. State Roadworthiness Authority.

1.1.10. Based on the above the final arrangement of the SAS can be summarised in the following diagram:

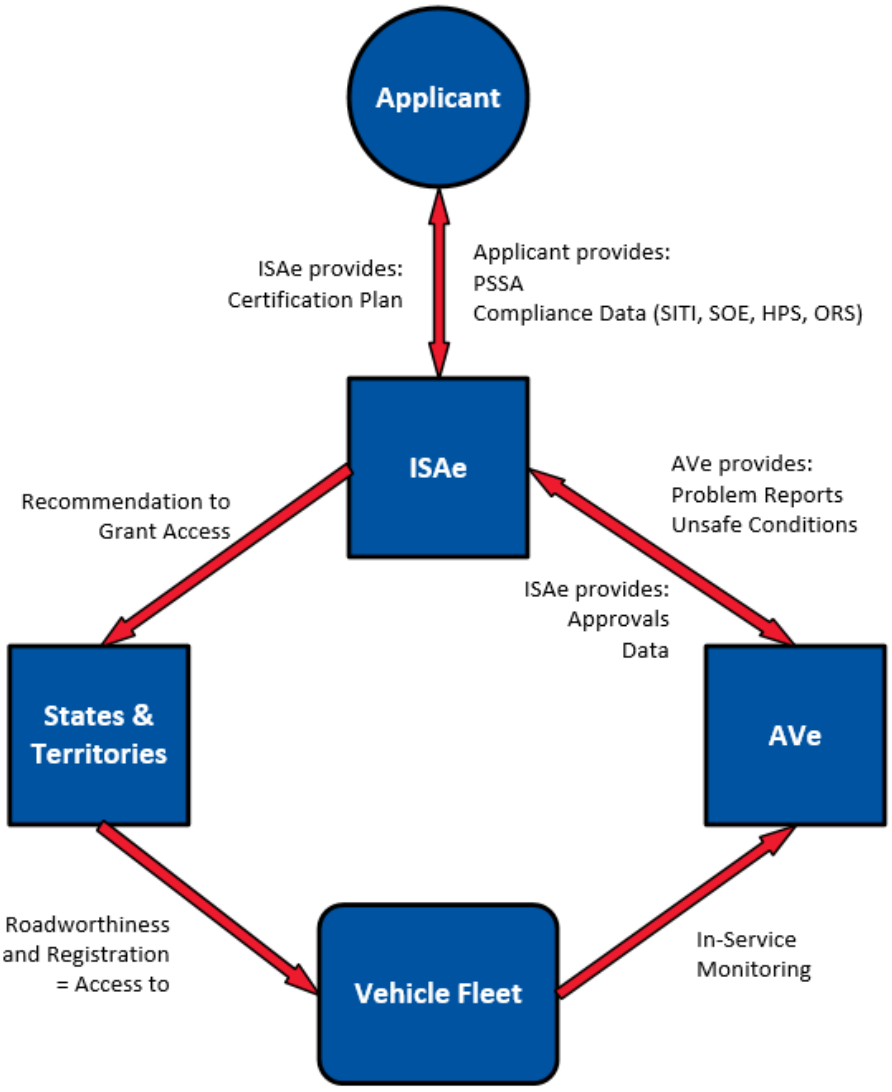


Figure 2: Safety Assurance System Core Elements

Initial Safety Assurance Entity (ISAe)

1.1.11. The ISAe is recommended to be a national body that manages the initial certification process for AVs. The certification process suggested is one designed around treating each AV or AV technology being proposed by an applicant on a case-by-case basis. The concept outlined is that a certification plan is developed for each application based around a Preliminary System Safety Assessment (PSSA). This ensures that certification is safety case centric.

1.1.12. It is proposed that the ISAe would complete all compliance findings including compliance against the existing Australian Design Rules (ADRs). It is proposed that the ISAe will recommend to States that a given AV is suitable to be registered and hence granted access to the road network.

1.1.13. The report outlines four governance arrangements for the single, national ISAe and notes that because the ISAe is providing technical assessment services and advice to State registration authorities it does not need to be supported by any specific regulation or legislation.

Automated Vehicle Entity (AVe)

1.1.14. The AVe is the organisation that conducts the continuous in-service technical integrity tasks. Importantly the AVe becomes the legally responsible entity for the ongoing safety, performance and compliance of the AV.

1.1.15. It is recommended that the SAS supports a model where processes are established so any organisation can be approved by the ISAe to operate as the AVe for a given model or fleet of vehicles.

State Roadworthiness Authority

1.1.16. The third entity within the SAS is the State roadworthiness authorities who, based on recommendations from the ISAe will grant to, or remove from, the AV the right to access the road network using the existing road-worthiness and registration processes.

Conclusion & Recommendation

1.1.17. This report concludes that if a SAS of the form described was established then it would be able to meet the requirements identified by the stakeholders recommendations outlined in the NTC policy paper, "*Regulatory reforms for automated road vehicles*" [3] as well as a further group of requirements developed as an element of this task.

1.1.18. The recommendations within this report are aligned with the NTC's intended approaches. Developing an implementation framework with greater detail and stakeholder engagement, which accounts for global synergies, will maintain the momentum of this initiative and ensure Australia's readiness to safely embrace the new AV technology.

2. Context

Key points:

The objectives of this report are to:

- identify options for the governance models that support a nationally consistent process to approve AVs;
- identify possible structures for an approval process for AVs;
- discuss technical performance requirements that could be applicable to AVs; and
- identify possible safety validation methodologies for AVs.

Additionally, the report is required to provide an outline schedule to implement a SAS.

2.1. Background

2.1.1. Throughout 2015 and 2016 the National Transport Commission (NTC) reviewed issues surrounding the introduction of Automated Vehicle (AV) functions into the Australian market.

2.1.2. In February 2016 the NTC published "*Regulatory barriers to more automated road and rail vehicles*" [1]. The issues paper was an initial review of regulations in Australia, provided an overview of current rules and identified key issues and potential solutions.

2.1.3. In May 2016 the NTC published "*Regulatory options for automated vehicles*" [2]. This discussion paper confirmed the key issues, summarised stakeholder feedback to the issues paper [1] and discussed potential options to address the identified issues.

2.1.4. In November 2016 the Australian Transport Council approved recommendations outlined in the NTC policy paper, "*Regulatory reforms for automated road vehicles*" [3]. Included in these recommendations was the need for a Safety Assurance System (SAS) for AVs. The relevant policy finding was:

> ***Policy finding:*** *In conjunction with the removal of regulatory barriers, Australian governments should develop a national SAS in close consultation with industry partners and in alignment with international practices. The SAS should establish an approvals process to assess the safety performance and data handling of applications to operate AVs that do not require a human driver some of the time or all of the time.*
>
> *Preparatory work to develop the national SAS should have regard to scoping:*
>
> *a. Nationally agreed safety principles and criteria;*
>
> *b. Operational models and processes to ensure that the SAS is nationally consistent, efficient, affordable and creates minimal administrative burden for applicants;*
>
> *c. Enforcement;*
>
> *d. Road access; and*
>
> *e. Governance and funding options.*

2.1.5. Policy finding recommendation 5 was the specific impetus for NTC to requisition this report on the SAS for AVs in Australia.

> ***Recommendation 5 (of the policy finding):*** *That the NTC develop a national performance-based assurance regime designed to ensure the safe operation of AVs, with an initial focus on vehicles with conditional automation (level 3).*

2.2. Informal Stakeholder Consultation

2.2.1. During December 2016 and January 2017 the concepts contained in this report were reviewed with several stakeholders in the Australian AV sector. This included the Commonwealth government, State and Territory (State) road authorities, vehicle and vehicle system manufactures, vehicle industry groups, automobile owner groups and existing vehicle regulatory authorities.

2.2.2. Comments and issues provided by stakeholders have informed the discussion in this policy paper. A complete list of all stakeholders consulted is provided at Appendix C.

2.3. AV Functional Taxonomy

2.3.1. Throughout the initial work on AVs the NTC adopted the SAE International Standard J3016 *"Levels of Driving Automation"* [4] classifications to describe the 'degree of automation' of AVs. In the November 2016 NTC policy paper [3] the range of existing taxonomies in use was reviewed. The J3016 taxonomy was nominated for further use by the NTC mainly because it was presently the most commonly used and understood taxonomy [2].

2.3.2. This report will not be referring to any other taxonomies used within the AV industry to describe the scope of automation.

2.3.3. As a result of the stakeholder feedback in the November 2016 NTC policy paper [3] the SAS that Nova Systems envisages is based on risk-based analysis and follows a safety case approach, with applicants demonstrating the safe performance of the AV. This is also in line with the United States (US) Department of Transportation (DoT) National Highway Traffic Safety Administration (NHTSA) philosophy [8].

2.3.4. Inherent in the notion of an SAS based on individual safety cases is that the system will address each AV function offered for review on its merits. Any attempt to determine SAS response based on pre-classification of functions against the SAE J3016 taxonomy will remove the flexibility necessary to address each system on a case-by-case basis.

2.3.5. Consequently, this report is not a deviation from either the existing NTC (or SAE J3016) work but rather a prioritisation based on the functional safety of individual behavioural competencies

2.3.6. It is noted that there have been previous attempts in similar SASs, most notably in the initial years of Unmanned Airborne Systems (UAS), to use a taxonomy as a foundation for regulatory structure and such assurance systems have been found to lack the flexibility necessary to deal with unforeseen technological innovation.

2.4. A Discussion on Safety

2.4.1. It has been noted during stakeholder engagement that there is a requirement to better qualify the term "safety" as it applies within the context of this evolving regulatory area. The broadening of the definition of safety that comes with the introduction of AV technologies becomes important as the details of the SAS are explored in later chapters.

2.4.2. Traditionally, the notion of vehicle safety in Australia is linked to the concept of 'the road toll'. Reduction of fatalities has been a major focus and a measure-of-success for road safety programs. Fatality reduction efforts have led to a series of road safety measures (i.e. seatbelts, vehicle crashworthiness requirements, speed controls, roadside infrastructure) to protect vehicle occupants and pedestrians.

2.4.3. Implicit within the existing road safety approaches is the notion that 'accidents' (primarily driver errors) will occur. Road safety measures seek to minimise both the probability and consequence of accidents. The clear majority of vehicle related accidents (94%) are the result of driver error vice vehicle technical failure [5].

2.4.4. AV technologies introduce a new paradigm. The way in which AV technologies impact upon the probability of harm opens the potential for a definition of AV vehicle safety that is wider than that presently assumed for Australian road vehicles. Significant safety improvement will come about by reducing or removing the occurrence (probability) of incidents that put people at risk. Where incidents do occur, they will be a result of technical failure. Human failure leading to incidents is likely to have a basis in the form of "design error".

2.4.5. This report does not rely upon an agreed definition of 'safety'; however, it is worthwhile considering what the introduction of AV technologies will mean for the notion of safety of Australian road users and the secondary impact of incidents on network disruptions.

2.4.6. An AV technologies-based safety goal could be expressed as "the rate of occurrence of incidents that result in harm to people". This would be a far more encompassing goal than reducing fatalities and it reflects the opportunity that AV technologies offer for safety improvement.

2.5. A Discussion on Ethics

2.5.1. Work on AV safety assurance and regulation often includes a discussion regarding ethics as it applies to automated decision-making algorithms [8]. Ethical questions are often summarised by a discussion on the ability of an algorithm to resolve decision conflicts. There is a wide range of academic work that attempts to explore these issues, including discussion regarding whether such questions exist in reality [23].

2.5.2. It is beyond the scope of this report to commence a discussion on ethical issues and such a discussion is not necessary to achieve the aims of the report. This report proposes a SAS process that supports the review and certification of each AV functionality presented on a case-by-case basis. This approach could, however, support an analysis of the design of any decision-making algorithm and assessment of the safety case associated with that algorithm. If ethical issues do exist with the design of any decision algorithm then those issues will be explored on a case-by-case basis.

2.6. International Context

2.6.1. In 2016, the US DoT NHTSA released a *"Federal Automated Vehicles Policy"* [8] containing "Vehicle Performance Guidance for Automated Vehicles" (including a 15-point safety assessment to be used in design and manufacture of highly automated vehicles) and a "Model State Policy" addressing proposed divisions of responsibilities between Federal and State governments in the US. The goals of this publication have a bias towards a significant design and manufacturing base as well as a regulatory group similar to that held by the NTC.

2.6.2. The proposals in the NHTSA policy document form a reasonable basis of expectations for documentation and evidence likely available from manufacturing and market states responsible for significant vehicle importation and type approval. The SAS advocated and described herein will support and harmonise with the approaches advanced by the NHTSA.

3. Assessment Criteria

Key points:

This chapter sets out 10 high-level assessment criteria that can be used throughout the development of the SAS to both guide development and test the processes created to ensure they are relevant and address the key issues required of the SAS.

3.1. Prerequisites to Restructure – Assessment Criteria

3.1.1. The assessment criteria will be used throughout this report to not only test safety assurance concepts but, over time, to test discrete system elements. It is important to keep asking throughout the SAS development process two questions:

a. How does this aspect of the system enhance safety? (i.e. if it does not enhance safety is it necessary?); and

b. Does this aspect of the system meet the goals set out in the assessment criteria?

3.1.2. Viewed in this way the assessment criteria become a series of tests that are applied to ensure that the development of the SAS remains focused. The assessment criteria are a mechanism to prevent the development of 'regulation for regulations sake'.

3.1.3. It is suggested that, based on a review of previous work and the stakeholder feedback, the following assessment criteria be utilised:

1. Is safety achieved?
2. Does the SAS support national road safety strategy?
3. Does the SAS support technological innovation and evolution?
4. Does the SAS support international product assessment?
5. Does the SAS support low-cost approval of new technologies?
6. Does the SAS support environmental variation and evolution?
7. Does the SAS support legal accountability?
8. Does the SAS support road system operational management rules?
9. Does the SAS account for a wide range of driver competencies?
10. Does the SAS support existing consumer protections?

3.1.4. Each of these points are addressed in the following sections.

3.2. Safety is achieved

3.2.1. While it is self-evident that a SAS should aim to achieve some form of a safe outcome it is necessary to assert this criterion clearly. A safe outcome should not be assumed to occur because of the

existence of an SAS. The development process should seek to explain at every step how the safe outcome is being achieved.

3.2.2. During detailed development of the SAS there will be a need to establish what constitutes a safe outcome. For suppliers of products the legal test applied in Australia (to comply with trade practice and workplace health and safety requirements) would be to ensure that the vehicle is safe 'So Far As Is Reasonably Practical' (SFAIRP). While such an approach provides a framework to support striking a balance between cost and safety it may not be the whole answer for AVs.

3.2.3. Any deployment of AVs on existing open access roads will require the development and maintenance of a sound social licence as much as the legal licence that is the focus of this regulatory development process. Regulation can be seen as the mechanism that supports the social licence. It is likely that safety goals will be established around the notion of the public's perception of safety as much as the more technical assessments that underpin a SFAIRP style assessment.

3.2.4. It should be remembered that much of the safety outcome associated with AVs will not flow from any new regulation but from the maintenance of existing regulation and design standards. Regardless of how rigorous the regulation, on occasion an AV driving system will fail and drive into elements of the environment and other vehicles will crash into the AV. Consequently, a significant contribution to safe outcomes will be all the existing, evolutionary, safety regulations and technology ranging from structural crashworthiness to seat belts and airbags.

3.2.5. Accepting that the final definition of a 'safe outcome' will need to be refined across the detailed development phase of the regulations, the following high-level aims will be used as a starting point:

a. The safety outcomes for AV passengers should be *at least* equivalent to commensurate outcomes achieved in non-AVs using existing vehicle standards and driving environments.

b. The safety outcomes for people who share the environment with AVs should *exceed* the commensurate outcomes achieved in non-AVs using existing vehicle standards and driving environments.

c. Regulations should support and promote an ongoing, evolutionary, improvement in the safety outcomes for AV as lessons are learnt and incorporated.

3.2.6. These high-level aims do contain significant value judgments that should be transparent.

3.2.7. The first concept embodied is that there is a difference between the active acceptance of risk by a driver or occupant of an AV and the *imposed risk* experienced by members of the public sharing the environment with an AV.

3.2.8. The driver, or occupant of a highly AV (SAE J3016 Level 3 or higher), by choosing to enter the vehicle is accepting the risks associated with traveling in the vehicle. This is not necessarily a fully informed quantitative judgment but a relative notion of the risks associated with road travel, the normal risk mitigations that should be used (i.e. wearing a seat belt) and some understanding that the vehicle meets some minimum design standard. This passive risk assessment occurs today with drivers accepting that road travel is more dangerous than rail travel and accepting that risk in exchange for the convenience of road travel.

3.2.9. Today's drivers mitigate risk by wearing seat belts and could further mitigate risks by wearing helmets, but choose not to. These are decisions that reflect the ability of users to assess and address risk.

3.2.10. The members of the public sharing the environment with the AV do not actively accept risk. The risk is imposed on the public by virtue of the decision of the AV operator to access the common road environment. The public treats the imposed risk by a common application of rules and laws and by

case-by-case judgments. A cyclist can in part rely upon road rules and laws to build confidence that the driver of a car will avoid colliding with them but also may use contextual risk reduction such as looking directly at the face of the driver to assess if the driver has seen the cyclist.

3.2.11. AVs may not provide the same case-by-case risk reduction opportunities for people within the operating environment and hence there will be a much greater role for the regulatory process in addressing and accepting the imposed risk presented by these vehicles. This notion of imposed risk that is addressed by some common, community process implies that these risks may need to be less than the risk accepted by the party choosing to be exposed to the risk, and having the direct benefit associated with the risk producing activity.

3.2.12. The second implied judgment is that continuing safety improvement is desirable. This report does not make a case for or against this notion but rather accepts that this seems to be the approach presently adopted by Governments (Australian Transport Council 2011) [6].

3.2.13. Diverse opinion was noted during informal stakeholder feedback. One response suggested that the aim of facilitating ongoing safety improvements was not the role of a Safety Management System (SMS). One response suggested that by starting with the existing system safety performance the SAS was not supporting the obvious safety improvement inherent with the AV technologies. The practical outcome of the requirements noted is that they provide a mechanism to develop technical requirements for probability of failure of AV system components. Stakeholders will have the opportunity during the development of the SAS to see the impact of these requirements and further discuss the exact target performance of the SAS.

3.3. Supports national road safety strategy

3.3.1. The *"National Road Safety Strategy"* (Australian Transport Council 2011) [6] aims to 'set out a path for national action on reducing fatal and serious injury crashes on Australian roads'. The strategy, endorsed by all Australian States and Territory governments and the Commonwealth sets out a series of targeted interventions that are designed based on gathered evidence regarding the nature and causes of fatal and serious injury crashes.

3.3.2. In safety terms the strategy is a SMS in that it analyses data, develops (suggests) interventions, monitors outcomes and then corrects the interventions based on the learned lessons.

3.3.3. The AV SAS sits within the environment created by the National Road Safety Strategy and shares the same global aims. Consequently, it is important the AV SAS should:

a. be consistent with the strategy,

b. support the aims of the strategy, and

c. not hinder the application of the higher-level implementation of the strategy.

3.3.4. Specifically, the SAS should not place limits on data that is necessary for the correct execution of the strategy projects.

3.4. Supports technological innovation

3.4.1. The SAS should support continuous technical innovation on the basis that:

a. technical innovation is often about improving safety outcomes,

b. technical innovation is often about reducing costs and improving productivity, and

c. AV technologies and functions are likely to be introduced to consumers in incremental functional steps.

3.4.2. This assessment criterion is based on the notion that it is not possible to predict either the functionality or enabling technologies that may be applied to AVs. This suggests that the SAS should be designed assuming ongoing and unforeseen technical innovation and should be able to support this development environment.

3.4.3. The implication of this assessment criterion is that it requires a SAS that is not based upon a series of technically explicit design standards such as the existing Australian Design Rules (ADRs) [Department of Infrastructure and Regional Development (DIRD) 1989] [7] but rather encompasses a safety assessment process that can deal with technical innovations on a case-by-case basis.

3.5. Supports international product assessment

3.5.1. The rate of technological development in AVs together with the global nature of the markets means that much technology development will occur outside Australia and will reference non-Australian environments. AVs will likely be assessed by other national entities using a range of similar, technical assessment processes before they are offered to the Australian market.

3.5.2. While international agreement on standards and assessment processes is desirable it is unlikely that such agreements can or will occur in a timeframe that matches the rate of technology development. Consequently, the Australian SAS should be designed to accommodate variation in standards and processes applied in the international community.

3.5.3. Furthermore, the SAS should have the ability to accept previous approvals by other national authorities. The implication of this assessment criterion is that:

a. the SAS will need a process to allow use of a wide range of standards, and

b. the SAS will need a process to assess and accept processes used by national authorities and entities.

3.5.4. This assessment criterion also reflects Australian Government policy to adopt international standards as a way of ‘reducing red tape’ [23].

3.6. Supports low cost approval of new technologies

3.6.1. Accepting that the AV technologies being addressed have safety and productivity improvements, and recognising that Australia may be a small proportion of total global market for a given vehicle or technology, then it is reasonable to aim for a SAS that does not add costs such that vendors are discouraged from bringing innovative AV technologies into the Australian market.

3.6.2. One implication of this assessment criterion is that it encourages the development of a SAS that focuses on issues (and adds cost) proportional to the risks associated with a particular AV functionality. The safety assurances processes will need to be scalable and adaptable relative to the consequence of the risks associated with the particular functionality being proposed for the AV.

3.6.3. Another implication of this criterion is that it requires a SAS that allows suitable authorised third parties to undertake specific functions within the system. This allows competition between organisations implementing the functions of the process.

3.7. Supports Australian industry

3.7.1. Within the constraints of existing multilateral and bilateral trade agreements and treaties the SAS should create an environment that supports the development of Australian industry in the international AV marketplace, including the market for aftermarket systems.

3.7.2. This should not be taken to mean that the SAS should inhibit international vendors or competition but rather the SAS should create an environment whereby products and technologies approved firstly in Australia are of a highest standard that can be readily accepted as safe in other countries.

3.7.3. The implication of this assessment criterion is that the assessment processes used in Australia should be as transparent and as understandable as possible. The artefacts created by the safety assurance process should likewise be clear and unambiguous.

3.7.4. This is in accordance with broad Australian Government innovation policy aims as described by the Department of Industry, Innovation and Science *"Industry Growth Centres – Initiative Summary*" [25].

3.8. Supports environmental variation and evolution

3.8.1. In the context of this report the operational environment of the AV includes the widest range of attributes including:

a. weather related variation (rain, light, dust);

b. road physical conditions (surface, road side conditions, markings);

c. road related infrastructure (traffic signals, signs); and

d. AV related infrastructure (digital infrastructure, specific line marking).

3.8.2. The Australian operational environment for AV is complex and highly variable. Additionally, infrastructure changes are likely to be incorporated into the road network infrastructure to assist or interact with AVs.

3.8.3. Note that the concept of environment as used in this report is similar to, but possibly wider than, the concept of Operational Design Domain (ODD) as used by the US DoT NHTSA [8].

3.8.4. The SAS should not be constrained by the variation in operating environments. Furthermore, the SAS should assume that the environment could create operational constraints and conditional approvals. The system should assume and support ongoing development of the road network infrastructure.

3.8.5. The implication of this assessment criterion is that it is likely that a significant attribute of the SAS will be an ability to assess and communicate the boundaries of operational environment within which the given AV function has been found to be safe.

3.9. Supports legal accountability

3.9.1. In both the stakeholder discussion regarding safety assurance and in the wider discussions being undertaken by the NTC about AVs there is a substantial emphasis on the allocation of legal accountability for the safety and behaviour of the AV.

3.9.2. Consequently, it is a requirement of the SAS that the entity legally accountable for initial and ongoing compliance with every aspect of the safety assurance process is clearly defined.

3.10. Supports road system operational rules

3.10.1. The Australian road system operational rules (road rules and traffic laws) are State based and while harmonisation will continue between State operational rules it can reasonably be expected that the State based nature of the operational rules will remain well into the period when the AV SAS is in place.

3.10.2. Furthermore, it is assumed that regardless of any harmonisation the operational road rules will need to continually evolve in support of the ongoing aim to improve road safety.

3.10.3. It is noted that this issue is not unique to Australia. It is reasonable to assume that AV functions under development and approved in other operational environments will need to address variation in road operational rules. Thus, a main consequence of this assessment criterion is that the SAS should support a wide range of methods to accommodate variation in operational rules and must not suggest an Australian unique solution.

3.10.4. Another impact of this assessment criterion is that it will result in detailed technical requirements to ensure that State based operational regulations can be accommodated in designs.

3.11. Supports variation in driver competency

3.11.1. Driver competency varies within States (age, operational hours, environmental exposure, vehicle weight) and from State to State (curriculum, environmental exposure). Additionally, the development of AV functionality overseas will assume driver competencies that may not match those of Australian drivers.

3.11.2. The consequence is that the SAS will need to accommodate both assumptions about driver competency and driver competency variation within Australia.

3.11.3. The main consequence of this assessment criterion is that the SAS will need to assess and communicate issues associated with driver competency in a standardised and transparent manner.

3.12. Supports existing consumer protections and other related legislation

3.12.1. A significant body of regulation already exists in Australia regarding the protection of consumer rights and citizen protections. This regulation ranges from product liability [9] to data protections and privacy [10].

3.12.2. Additionally, there are the overarching protections afforded by the Workplace Health and Safety (WHS) Act [11]. Issues raised by the introduction of AV functionality cross across all these existing regulatory jurisdictions.

3.12.3. Consequently, it is thought that the SAS should not conflict with or nullify the protections and operation of any existing regulation. The SAS should address only safety issues and should not cover other issues that have been raised in relation to AVs (e.g. data protection) other than where those issues have a direct impact on safety outcomes.

4. The overarching vehicle safety system and how AVs integrate.

Key points:

The AV SAS can be viewed within a wider road safety context. This report proposes that the three core elements Vehicle Technical Integrity, Operating Environment and Human Performance represent the context that can be used to structure the development of a SAS.

Vehicle Technical Integrity is defined and broken into two elements, Initial Technical Integrity and Continuing Technical Integrity.

4.1. Introduction – Existing Constructs

4.1.1. In the existing national road safety strategy (Australian Transport Council 2011) the road safety actions or interventions discussed are grouped within the four 'cornerstone' areas of the strategy. These cornerstone areas are:

a. Safe Roads,

b. Safe Vehicles,

c. Safe Speeds, and

d. Safe People.

4.1.2. This taxonomy for safety assurance interventions reflects both the key issues that have previously been addressed and the demarcation between regulations and regulatory authorities. This framework provides a good starting point to explore how vehicle technology changes have previously been addressed and what the limits of technology changes are that may be accommodated by the existing systems.

4.1.3. Rather than an esoteric discussion, issues are explored by considering a specific technology example; in this case, automated speed control (cruise control):

a. Cruise control is an AV technology that was successfully introduced within the existing safety framework.

b. Safe operation of cruise control is dependent upon road conditions but there has been no attempt to regulate or control the road conditions where the technology can be employed.

c. Use is dependent upon driver judgment (Safe People). This is possible because the assessment of safe driving conditions is a core, pre–existing driver skill, which is augmented by a regulatory framework (Safe Speeds).

d. Cruise control could be included into the ADRs [7] (Safe Vehicles) as a simple specification without undue consideration of driver skill, which is assumed suitable based on existing practices and training.

e. The existing HMI [the speedometer] is re-useable with minor amendment and low risk.

f. In this case, the attribute Safe Roads is incorporated in an indirect way by incorporating a lower speed engagement limit. Lower speed engagement limits are a proxy for road conditions.

4.1.4. We see with cruise control that all the key safety attributes are in play, but the 'swap in, swap out' nature of the function (driver reads speedo data vs. machine reads speedo data, machine operates accelerator vs driver operates accelerator) together with the existing training and regulatory focus on speed control means the technology 'slots into' the existing framework successfully. It is noted that as cruise control functions becomes more complex the above discussion may become incorrect. This has led to the creation of a SAE standard for adaptive cruise control [12]. (It is noted that this SAE standard has yet to be adopted by the ADRs).

4.1.5. What the cruise control example demonstrates is that the existing safety framework contains the basic attributes necessary to support AV technologies. The existing framework supports the safe introduction of certain automation technologies and hence, the development of a new SAS for AVs, could interpreted an iteration of the existing concepts rather than a complete 'clean sheet' development.

4.1.6. Recognising that the SAS is best viewed as an evolutionary iteration rather than a new start is also important since the existing regulations are nothing more than an aggregation of lessons learned over many years.

4.1.7. It is crucial to remember that the existing regulations are built upon many years of learning. The existing regulations address safety issues that will remain relevant and possibly take on additional significance as new technologies are introduced.

4.1.8. One way to look at the issue raised by the introduction of more complex automation in vehicles is to look at how complex automation impacts the complexity of interactions between the four existing safety cornerstones.

Safe Roads – Safe Vehicles

4.1.9. The US DoT NHTSA report "*Federal AVs Policy*" [8] outlines a set of "behavioural competencies" that are used to assess the capability for AV guidance systems. The competencies include such things as:

a. Detect and respond to speed limit changes and speed advisories;

b. Perform high-speed merge (e.g. freeway);

c. Perform low-speed merge;

d. Move out of the travel lane and park (e.g. to the shoulder for minimal risk);

e. Detect and respond to encroaching oncoming vehicles, etc.

4.1.10. It would not be possible to design, assess or approve these types of AV functions without having a defined road environment. It is not possible to either design or assess any of these functions without knowing the road configurations that the system must be able to accommodate. 'Perform high speed' merge is a much harder task on an 'Italian style' motorway interchange than on the long merge ramps in many Australian high speed merge lanes.

4.1.11. This illustrates how the complexity of the automation being discussed introduces interaction between what previously were quite separate aspects of the overall safety system.

Safe Vehicles – Safe People

4.1.12. As levels of automation increase there is a significant change in the role of the vehicle occupants and the relationship of this role to the safety of the vehicle. In all but the high-end automation cases,

such as defined by SAE J3016 Level 5 [4], the vehicle 'operator' will be allocated monitoring and intervention tasks as an element of the design.

4.1.13. The ability of the operator to 'monitor and intervene' and the ability to train for specific tasks becomes a crucial aspect of the vehicle safety. It is not possible to complete the design or the safety assessment of an automated functionality that relies upon a human performance that cannot be defined or assumed to be executed correctly when required. The safety of such a system cannot be asserted without an understanding of the competencies of the operator and a proposed / agreed method of ensuring that the operator has been trained and tested in those competencies.

4.1.14. What was a simple assumption in the cruise control case (drivers monitor speed in existing driving task hence drivers can monitor automatic speed control), will not necessarily occur with more complex automation and system behaviours.

4.1.15. It is possible to explore interactions between each of the existing safety cornerstones and show, as in the two examples noted, that AV system functionality and complexity adds to the interrelationship between these basic elements, which is not evident in existing vehicles.

4.1.16. This discussion suggests that the safety of AV functions is dependent upon, and influenced by, the interactions between:

a. the technical integrity of the automated function;

b. the environment within which the automated function must operate; and

c. the human operator actions and behaviours that support that automated function.

4.1.17. This is expressed in the following simple context diagram.

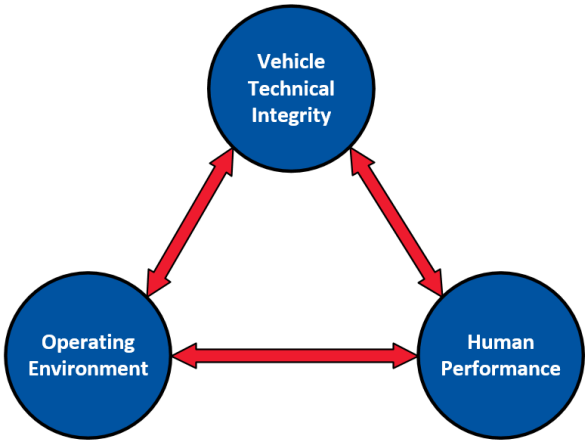


Figure 3: Context of AV Safety Assessment

4.1.18. If 'Safe Speeds' are assumed as an element of both vehicle integrity and the environment (which is the case as existing speed limits are a function of road physical environment, congestion, foot traffic density, building density etc.) then these three high-level contextual boundaries for safety regulation map directly to the existing national road safety strategy 'cornerstones'.

4.1.19. What this context relationship suggests is that a SAS cannot assert a safe outcome unless all three elements are addressed and that no one element can be addressed in isolation from the other two. All elements need to be addressed in a coordinated and holistic fashion for safety to be assured.

4.1.20. The three core elements shown in Figure 3 should not be confused with levels of regulation or jurisdictions. Levels of safety assurance, implementation mechanisms and regulatory authorities will contribute to each of the core elements.

4.1.21. Following is a preliminary discussion of the three core elements:

a. vehicle technical integrity,

b. human performance, and

c. environment and operator competency.

4.2. Vehicle Technical Integrity

4.2.1. Vehicle technical integrity is a 'through life' issue and it is highly likely that the SAS, detailed regulation and jurisdictional breakdown will also be organised along vehicle life-cycle lines.

4.2.2. As AVs become more complex an agreed definition of technical integrity allows elements of that definition to inform the development of the safety assurance system. An agreed definition of technical integrity also provides a framework to assess the validity of any discreet aspects of any proposed SAS.

4.2.3. The simple question 'which aspects of technical integrity are impacted by the system attribute under discussion?' becomes a powerful tool to guide any discussion, not only during the initial development of the SAS but throughout training, deployment and oversight of any new system. For the purposes of this discussion an AV can be said to have technical integrity if all the following conditions are met.

a. It has been designed by suitably qualified people, in accordance with agreed design requirements and processes, with a knowledge of the agreed intended operating environment;

b. It has been accepted as complying with the design requirements by a competent, authorised organisation;

c. It has been produced by an approved organisation using agreed standards and processes;

d. Its configuration is controlled and fully defined at any time;

e. It is monitored for ongoing serviceability such that critical deviations from the approved configuration and functionality are immediately obvious to the operator;

f. It is maintained by a competent organisation using defined procedures and suitably qualified maintainers; and

g. Its design and configuration changes are approved and implemented by suitably qualified and authorised people working within approved organisations.

4.2.4. It is noted that this concept of technical integrity is common to the aerospace and rail industries. Additionally, all these elements, to a certain extent, already exist in the Australian motor vehicle industry.

4.2.5. The following section expands some of the concepts outlined in the definition of technical integrity in order that issues that may impact upon the design of the SAS can be explored.

Initial Technical Integrity

4.2.6. Initial technical integrity is a terminology that can be applied to the design of the vehicle. Within the existing regulatory structure initial technical integrity is the process of showing compliance with the ADRs. This process is outlined in the *"Administrator of Vehicle Standards Circular 0-1-2"* (Administrator of Vehicle Standards 2015) [13].

4.2.7. Experience from other technology application areas suggests that for complex AVs the initial technical integrity process must evolve from a process of simple compliance finding against defined standards, as outlined in Circular 0-1-2, to a process that supports:

a. initial review of the proposed functionality;

b. agreement of the design requirements applicable to the functionality;

c. agreement of the design processes and compliance finding process to be used; and

d. acceptance of the compliance findings by a process of analysis, inspection and test.

4.2.8. Such a high-level process is required to support innovation. Strict adherence to pre-defined design rules can only ever apply to known technologies. Technologies that emerge through innovation, especially rapidly evolving technologies, require a regulatory framework that controls overall process and development methodology as much as final product compliance to a pre–existing rule. In addition, many modern implementation technologies, notably the use of software and complex hardware, mean that compliance by test or prototype inspection is not a suitable method to assure safety.

4.2.9. This does not mean that the sort of technical standards that are presently included within the ADRs or emergent industry rules for automated functions, such as those in development for 'automated commanded steering function' (82nd GRRF 2016) [14], are not valid or applicable to the process of initial technical integrity. Rather, to support rapid technical innovation, the SAS needs to allow vehicle and system vendors to suggest standards and design and performance goals beyond those that may already be promulgated by regulators.

4.2.10. What the above discussion suggests is that, for vehicles with some automated functions, the initial technical integrity will include consideration of:

a. existing ADR rules;

b. potential new ADRs that flow from future United Nations Economic Commission for Europe (UNECE) [14] style processes; and

c. AV specific requirements established for a given vehicle on a case-by-case basis.

4.2.11. Inherent in the notion of initial technical integrity is the need for designs to be assessed relative to a defined operational environment and an agreed understanding of operator competency. The contribution of the initial technical integrity process to overall AV safety can only ever be asserted if people suitably competent to operate the vehicle do so within the vehicle's defined design environment.

4.2.12. Such an approach to initial technical integrity will inevitably result in the need to develop a very high technical skill level in the organisations responsible for compliance finding. Especially where design is being conducted for an international market and where Australian compliance engineers will need to be responsive to innovation being accepted by other countries' regulators. For these reasons, it is

likely that initial technical integrity will be a national level endeavour; a national process executed by a national body (or entities approved by a national body).

Production Integrity

4.2.13. The compliance finding process utilised during initial technical integrity can only assert a contribution to the overall safety outcome if every vehicle produced complies with the 'approved' design. This process is already an element of the Australian Motor Vehicle Standards (AMVS) process. This process is outlined in the *"Administrator of Vehicle Standards Circular 0-13-1"* [15].

4.2.14. Where AV safety critical functions are implemented using software or complex hardware the commercial electronics industry notion that the impact of manufacturing errors or input material deviations will be identified and corrected during initial customer use will not be suitable. It is likely that existing 'consumer / product quality' laws will not be suitable as they, by nature, are post error legal processes which only ensure compliance through threat of commercial harm.

4.2.15. It is likely that, to ensure safety of consumers and non-participating but at risk public, production integrity will need to become more controlled than it is today. It is likely that the style of production conformity process that is applied at the vehicle level using *"Vehicle Standards Circular 0-13-1"* [15] will need to be applied in a more detailed manner to equipment and systems vendors.

Continuous Technical Integrity – Configuration Management

4.2.16. With complex systems such as AVs the ongoing ability of the vehicle to assert the safety performance that was agreed at the initial technical integrity stage can only be achieved if the vehicle remains in its original or a known configuration.

4.2.17. The existing regulatory process achieves the concept of Configuration Management (CM) via the process of 'roadworthiness'. Roadworthiness is presently a State-by-State responsibility. Roadworthiness tends to be a process of vehicle inspections and test, conducted by authorised testers, as exemplified by the VicRoads process [16].

4.2.18. For complex functions hosted in software and complex hardware, especially where those functions are subject to ongoing design updates throughout the life of the vehicle, a process of routine or non-routine inspection and test (such is the case with existing roadworthiness approvals) will not be suitable to allow an assertion of ongoing system safety.

4.2.19. For the complex systems used in AVs, CM needs to encompass:

a. active management and ongoing recording of vehicle configuration;

b. approval of design changes (using a process like that used during initial technical integrity certification); and

c. approval to incorporate design changes on previously approved designs.

4.2.20. Whether it is appropriate, reasonable or possible for the 'registration holder' to remain responsible for CM (and serviceability) is a complex question for AVs given the technical complexity associated with the vehicle functions.

4.2.21. It is likely that the task of CM will need to be implemented by technically competent individuals or entities that can be approved to perform the role and be held legally accountable. Importantly the ongoing CM is unlikely to need to be conducted by the entity that conducts the initial technical integrity assessment. CM is most likely to be performed by organisations approved by the Initial Safety Assurance entity (ISAe).

Continuous Technical Integrity – Serviceability

4.2.22. As complexity increases, especially as AV functions rely upon sensor fusion, determining the serviceability of systems will become more complex. The most significant challenge may be in the identification of failed, or partially degraded systems. The suitability of vehicle self-diagnostics may lay within the ambit of initial technical integrity.

4.2.23. It may be that just as now the responsibility to address an Automatic Braking System (ABS) failure 'ABS Failed" message is clearly the responsibility of the operator, with all but fully automated (SAE J3016 Level 5) vehicles, the responsibility to act on an enunciated AV un-serviceability remains with the operator. It seems likely that the vehicle itself will need to identify failures and 'lock out' specific functions.

4.2.24. It is possible to foresee a situation where the vehicle advises the configuration manger, via data link, of the serviceability issue.

4.2.25. Serviceability is an area where the SAS must be adaptable to accommodate a range of vendor approaches.

4.3. Human performance

4.3.1. Existing work by the NTC [2], the US DoT NHTSA [8] and others mentions in different ways the need to address HMI. The impact of human performance on the safety outcomes for AVs is fundamental and addresses a much wider scope than the narrow notion of HMI. The impact of human performance on the safety objectives of AVs can be viewed in two broad categories:

a. driver / operator competency; and

b. operator / vehicle interaction and performance.

Driver / Operator Competency

4.3.2. As the AV technologies are introduced the role of the driver translates to that of an operator and that operator translates from decision maker and primary inceptor to a role of monitoring and irregular intervention. It is likely that the skills and competencies required of the operator will become less generic and more specific to vehicle type and vehicle operations.

4.3.3. If the safety improvement gains that flow from AV innovation are to be fully realised it is possible that operator competency must become a two-part process. Operators may be required to have base competency (related to today's driver licenses) that is then augmented by specific 'type ratings'.

4.3.4. The alternative is that AV and system designers will create systems assuming a minimum human performance that aligns with the existing driver competencies. An example of this approach can be seen in Volvo's highway driving system [17].

4.3.5. For full automated (SAE J3016 Level 5) AVs, while it is easy to imagine that a passenger could have no role in the safety outcome, the reality is likely to be more complex. At a minimum, there may need to be emergency procedures training and competency for SAE J3016 Level 5 vehicle occupants. These competencies may never involve motion or guidance but, even if they are limited to safe egress in an emergency, they may require some training and demonstration of understanding.

4.3.6. The safety assurance process that governs competency is going to have to be generic / process centric in nature rather than based on specific narrow competencies inherent in today's training regulation. The process will need to support a range of approaches that vehicle and system vendors choose to adopt.

4.3.7. The safety assurance process will need to:

a. identify for a given vehicle the competencies required by an operator (assumed to be in the vehicle), or accept a vendor's assessment;

b. review and approve training for those competencies; and

c. allow assessment and approval of trainers.

4.3.8. If a type rating approach is adopted, then assessment and approval of the training system design becomes in part an aspect of the initial technical integrity certification.

Operator / Vehicle Interaction and Performance

4.3.9. Formal human engineering processes such as task assessment and workload assessment are likely to be required to ensure the safety of AV functions. This is especially true where AV functions are designed such that the operator must perform monitor and intervene functions.

4.3.10. Monitor and intervene is a complex role that requires attentiveness during long periods of inaction followed by rapid decision making followed by rarely repeated or practiced actions.

4.3.11. To assign safety related functionality to a human operator the designer and certification engineer will need a sophisticated human engineering analysis based on a common understanding of what is reasonable to expect from self-selecting semi expert operators.

4.3.12. Consequently, the SAS will need to support the requirement for detailed, evidence based human engineering to be incorporated in all system designs, including;

a. agreed understandings of the likely performance of operators;

b. agreed analysis and assessment methodologies;

c. agreed understanding of the limitations and affectivity of training; and

d. a robust incident and accident feedback mechanism that is likely to include semi real time performance monitoring.

4.3.13. Human engineering issues are at the core of questions already being raised in the NTC work regarding the difference between a driver and an operator and issues of liability.

4.4. Environment

4.4.1. Environment is a broad grouping of issues that directly relate to the safety and roadworthiness of an AV but may be outside the control of the vehicle designer and possibly the vehicle regulator. Some examples of issues that fall under the environment heading are:

a. road and related infrastructure design;

b. road operational rules;

c. weather;

d. geo-data (provision and integrity); and

e. AV support infrastructure (e.g. data linked speed advice).

4.4.2. The safety assurance common thread in all these attributes is that, while they cannot be controlled as an element of the vehicle safety assurance process, they do impact on vehicle safety. Currently it is thought that the AV safety assurance process will require that each vehicle approval must fully define the 'approved environment'.

4.4.3. This will allow the 'operational' regulators to limit the operation of a vehicle to a specific environment. The reciprocal will be that operational regulators will increasingly need to define 'target environments'. It is in the commercial best interest of the vehicle manufactures to offer vehicles that are compatible with a wide range of environments and it will become a community expectation that environments are tailored and raised to a standard that supports the widest possible range of AV functionality.

4.4.4. Certain aspects of the environment may become subject to international standard development. It is possible to imagine, for example, a Vehicle to Infrastructure (V2I) data link standard that defines the format for the transfer of vehicle speed and road condition data.

4.4.5. Environments are complex and under constant change and, as such, the AV safety assurance process must be 'open' with respect to definition of environment. This means that the process should not attempt to define environment (e.g. developing standard definitions of environment) in any way but rather ensure that the initial technical integrity process requires that the vehicle Original Equipment Manufacturer (OEM) fully defines the environment for which a specific vehicle automated function is designed and approved.

4.4.6. Safety assurance may be required to translate the design environment into a common form that is accepted by Australian operational approval entities.

4.4.7. The proposed approach leaves road mangers free to develop the network as they require. They can choose to update roads over time to improve AV compatibility. In the approach being suggested the vehicle OEM is required to assess the network and determine those roads upon which their vehicle can operate.

Environment and Operator Competency

4.4.8. For all AVs, there may be a judgment required by the operator as to whether the environment that they have placed the vehicle in is compatible with the design approval of the vehicle.

4.4.9. It is foreseeable that vehicles will over time be developed with functionality to 'self-assess' their environmental compatibility and such functionality will be just an additional attribute of the vehicle approved by the initial technical integrity process.

4.4.10. The requirement for the operator to assess the compatibility of the vehicle to the environment and make a judgment may require specialised training and assessment of competency. This is another concept that sits behind the aforementioned suggestion (4.3.3) that specific vehicles may require a specific 'type rating'.

4.4.11. This notion of drivers / operators making environmental assessments in support of the operation of automated functions is not necessarily a new competency. Drivers must make a judgment, based on an assessment of the environment, as to whether it is safe to use cruise control. This competency is not presently specifically trained and drivers are not required to hold a specific type rating to allow them to use cruise control (for the reasons noted earlier). However, that aside, the concept that new technologies require competency adaptation is not unknown.

4.4.12. The cruise control example may point to a potential approach that could be adopted by vehicle designers when examining the 'environmental compatibility judgement' question. For the early-to-

market, simpler technologies it may be possible for a vehicle OEM to make a case that the existing driver competencies are sufficient to allow drivers to make this judgment without further training (probably based on the data provided to the driver/operator by the vehicle). Again, the regulations need to be 'open' on this issue.

4.4.13. The regulation should not set a hard rule that certain new vehicle attributes need training and certain attributes do not. Rather the regulation should contain, within the initial roadworthiness determination, the need to assess (using human engineering techniques) the need for (and detail of any) training required.

5. Safety Assurance Process Concept

Key points:

Expanding on the three core elements previously described the processes that make up a SAS are outlined in terms of an Initial Safety Assurance process and In-Service Safety Assurance processes.

Chapter 4 suggests that to ensure safety of AVs a system should be developed that addresses:

- initial technical integrity;
- continuing technical integrity; and
- system performance monitoring (both technical and human).

This report will refer to the overall system that implements each of these processes (and in doing so 'regulates' AVs to ensure safety) as the SAS. This chapter explores the nature of the SAS.

5.1. Fundamental choices regarding a safety assurance system

5.1.1. There are two options for the basic approach to a SAS:

a. **Option 1:** A definitive regulation and technical standard based approach; like the existing DIRD, Road Vehicle Certification System (RVCS) style approach [7][13].

b. **Option 2:** A safety analysis case-by-case basis assessment approach; similar to the various aircraft certification models.

Option 1 – Definitive Regulation and Standards

5.1.2. In this option the SAS is an extension of the existing ADR style of regulation. The requirements for the AV functions are fully defined by design rules and associated performance standards. The AV vendor must demonstrate compliance against these standards and this compliance then asserts that the vehicle is safe.

5.1.3. Advantages of Option 1 are that the:

a. standards are known by all those involved in the industry, and

b. existing regulatory mechanism that are used to support the ADR compliance process all apply to this approach.

5.1.4. Disadvantages of Option 1 are that it:

a. requires that those developing the standards can foresee the technologies that will be offered to the market and a new technology can only be certified after a standard is developed; and

b. exposes road users to risk from technologies that are in vehicles but not covered in the standards and, hence, are not ever reviewed by regulators.

Option 2 – A vehicle unique safety assessment based approach

5.1.5. In this approach, each AV or AV functionality is addressed on a case-by-case basis. The certification requirements applied could be unique to each vehicle and would be based on the proposed functionality and the safety risks associated with that functionality. The approach looks to acceptance of previous compliance findings with an examination of changes that may flow from the Australian operating environments.

5.1.6. Advantages of this Option are that it:

a. allows new technologies to be approved on merit;

b. doesn't require the regulator to develop standards for technologies in advance of those technologies being offered to the market;

c. supports efficient approval of technical innovation;

d. can re-use many pre-existing process and lessons from rail, aerospace and like industries; and

e. supports assessment of vehicles approved overseas to a wider range of standards.

5.1.7. Disadvantages of this Option are that it:

a. requires a SAS to be developed and staffed with technical experts.

Recommendation

5.1.8. This report recommends that **Option 2** is adopted, primarily because it is the only option that can provide the ability to address AV technologies as they enter the market without having to predict in advance what technologies will be employed.

5.1.9. Several stakeholder comments addressed the advantages of keeping an ADR style approach. These comments assumed that the international community could and would develop standards (including performance based standards) for AV functionality and sub-systems and that the existing Australian vehicle certification process would be fit-for-purpose in finding compliance with these emergent standards.

5.1.10. This report considers such an approach would not meet assessment criteria 3 and 5, which recommends the Australian approach to the safety assurance of AVs should support technological innovation and keep cost down, respectively.

5.1.11. The development of international standards, including performance-based standards, is a slow committee based process that is unlikely to keep pace with the rate of innovation presently occurring AV technology area. Development of such standards can only ever make assumptions about what technologies may be deployed and, therefore, may lag technology development.

5.1.12. Use of standards, as the basis of the SAS, would result in a system that could not easily address innovative technologies that are not covered by existing standards. Furthermore, such a system would have difficulty dealing with pre-existing international approvals that do not use the recognised standards. Hence such as system would not meet the assessment criteria.

5.1.13. A standards based approach exposes road users to risk from technologies that are in vehicles but not covered in the standards. This approach produces a risk window where new technologies would be in the market not having been assessed. This is a significant deficiency of the standards based approach.

5.1.14. The remainder of this chapter describes what an Option 2 style SAS could look like.

5.2. Initial Safety Assurance

5.2.1. The initial safety assurance process establishes initial technical integrity. The basic process is shown as Figure 4 and the following is a discussion of each step of the process.

5.2.2. It is noted that many of the steps outlined in Figure 4 may be conducted in the vehicle's country of origin. Where this occurs, the Figure 4 process becomes one of reviewing work already conducted to confirm that it is applicable to Australian operations.

5.2.3. Throughout this discussion, the terminology 'approval authority' is used describe the organisation that performs the review and acceptance aspects of the process. This terminology should not be assumed to mean any particular entity. This role could be performed by more than one entity across the developmental life of an AV system.

5.2.4. The process of initial safety assurance is a certification process. Certification is a terminology (and process) already used in Australian motor vehicle initial technical approval as outlined in *"Vehicle Standards Circular 0-1-2"* [13]. To differentiate between the existing process and the AV process the term certification is not used in this discussion.

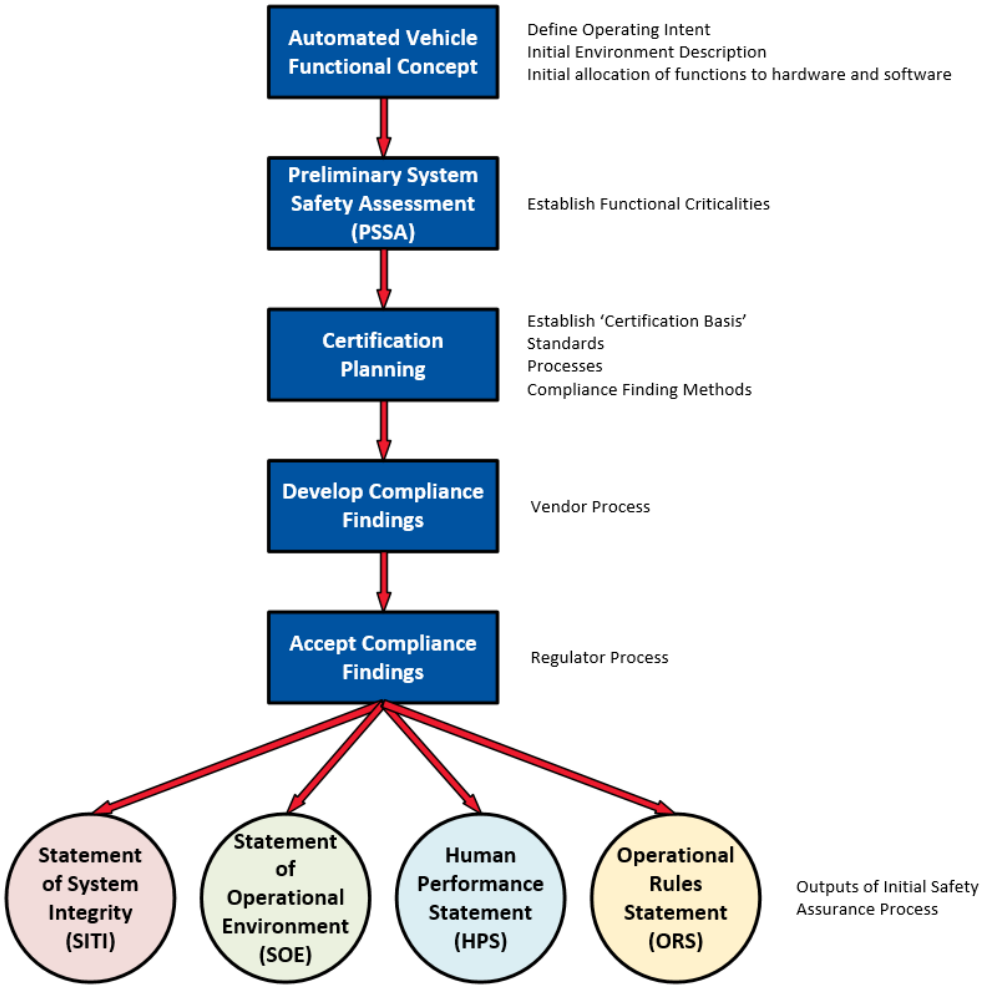


Figure 4: Initial Technical Integrity Summary Safety Assurance Process

AV Functional Concept

5.2.5. The start of the initial safety assurance process is for the vendor of the vehicle (or automated system) to provide the approval authority with a functional system description suitable to support a Preliminary System Safety Assessment (PSSA).

5.2.6. The automotive engineering sector produces a vast array of documentation for any particular project and there are often 'specification level' descriptions of systems contained in a suite of documents. Often these system descriptions, while suitable for their original purpose are far less suitable for a system safety analysis. The system description for a system safety analysis must be tailored to the analysis to ensure that there is a reasonable chance that all the key hazards (and associated risks) will be identified and that a reviewer has suitable information to understand the hazards, the risks and the bounds of the analysis.

5.2.7. In general, a system description for a system safety analysis should contain the following key attributes:

a. A description of key system components and architecture;

b. A summary of overall functions and the functional allocation;

c. A description of internal and external interfaces;

d. A summary of operators' roles and the HMI;

e. Details of the physical installation; and

f. Details of the assumed operating environment.

5.2.8. It is unlikely that a form of standard description template can be created and each system description will need to be structured to support the initial discussion with the approval authority and the PSSA.

Preliminary System Safety Assessment

5.2.9. The PSSA is the key aspect of the process as it is used to establish the risk associated with the functions being discussed. Once the risks are identified and agreed the scope, complexity and hence cost of the remainder of the safety assurance process can be established.

5.2.10. The PSSA is the artefact that most directly addresses the system assessment requirement for a process that supports the low cost of approval of new automated technologies.

5.2.11. The safety assurance process should be open to a range of PSSA techniques. SAE Standard J2980 [18] provides guidance on how to conduct a PSSA style analysis using the ISO 26262:2011 [28] framework. This is a comprehensive technique but may not be necessary in all cases for all proposed AV functionalities.

5.2.12. In developing the Australian safety assurance process there should be an assumption that safety assurance artefacts such as PSSA style analysis are likely to have been created for approval in other countries and the safety assurance process should be flexible enough to accommodate a range of analysis techniques provided that the minimum requirements are achieved.

Safety Design Requirements

5.2.13. The PSSA analysis will assign safety criticalities to AV functions and the systems that implement those functions. SAE J2980 [18] addresses these safety criticalities by allocating an Automotive Safety Integrity Level (ASIL) for each identified hazard.

5.2.14. If a vendor were to conduct an analysis using SAE J2980 [18] then the ASIL would be used as the guide to the form of standards that would need to be used for the function development and the compliance finding methodology.

5.2.15. Importantly, the ASIL can be used to establish:

a. failure probability objectives for hardware, and

b. development assurance levels for software and complex electronic hardware.

5.2.16. What this means is that the AV safety assurance process will, by its nature, translate the high-level aspirational safety goals inherent in the process assessment criteria into quantitative technical integrity targets.

5.2.17. The implication of this is that, as a part of the SAS detail design, there will need to be an analysis that translates criticality assessments (such as the SAE J2980 ASIL) into quantitative developmental targets. This notion of using quantitative technical integrity targets, is common place in other safety critical technical development domains.

Certification Planning

5.2.18. Using the system description and PSSA as inputs the primary aim of the planning stage is for the applicant and approval authority (ISAe) to reach agreement on the detail of the initial safety assurance process.

5.2.19. The sort of issues that could be agreed and captured within a Certification Plan (CP) include:

a. What standards will be used as the basis of compliance?

b. What design assurance process will be utilised?

c. What is the breakdown of compliance demonstration between analysis, test and inspection?

d. What compliance finding will be conducted by accepting previous approvals?

e. Which entity will perform the compliance finding?

5.2.20. The planning step and its link to the risk associated with the proposed functionality is fundamental to ensure that the overall safety assurance processes:

a. remains focused on addressing the key hazards and risks only;

b. is flexible and able to accommodate a range of functionalities without having to predict those technologies or functionalities that may be offered to the market;

c. can accept pre-existing compliance finding activities conducted outside Australia; and

d. is as low cost as possible.

5.2.21. These first three steps are the primary difference from the existing Australian motor vehicle certification processes, as outlined in *"Vehicle Standards Circular 0-1-2"* [13].

5.2.22. What is being proposed for AV initial safety assurance is a flexible, case-by-case, hazard centric process rather than a system of compliance finding against pre-established, generic technical standards.

5.3. Outputs for the Initial Safety Assurance Process

Statement of Initial Technical Integrity:

5.3.1. The Statement of Initial Technical Integrity (SITI) is the technical statement that asserts for the defined system that:

a. a safety analysis has been conducted,

b. functional hazards have been identified,

c. the design has been completed using design assurance processes commensurate with the functional hazards identified,

d. the technical estimate of the probability of the loss of functions is commensurate with the hazards identified, and

e. the compliance finding, as outlined in the CP, has be satisfactorily concluded.

Statement of Operational Environment

5.3.2. The Statement of Operational Environment (SOE) is a detailed statement of the operating environment that the initial technical safety assurance process has considered. The SITI is deemed only to be valid if the vehicle is operated within the bounds of the SOE.

5.3.3. It is likely that the format of this statement may become unique to Australia and use a standardised terminology acceptable to all Australian operation regulators (the States).

Human Performance Statement

5.3.4. The Human Performance Statement (HPS) is a detailed statement of the human performance that the initial technical safety assurance process has considered. The SITI is deemed only to be valid if persons suitably qualified, as described by this statement operate and maintain the vehicle.

5.3.5. This HPS will define any specialised training required (if any). In addition, this statement will nominate the training material and assessment criteria required to meet the assumptions contained within the initial safety assurance process.

5.3.6. It is likely that the format of this statement may become unique to Australia and use a standardized terminology acceptable to all Australian operation regulators (the States).

Operational Rules Statement

5.3.7. The Operational Rules Statement (ORS) is a summary statement that explains to operational regulators:

a. how local operational (road and traffic) rules are incorporated into the automated functionality, and

b. how correct incorporation of local operational rules can be confirmed.

5.3.8. The SOE, the HPS and the ORS address the requirements for environmental, driver and maintainer competency and operational rules variation outlined in the assessment criteria.

5.3.9. These four outputs represent the formal interface between the initial safety assurance processes and the in-service safety assurance processes. It is foreseeable that, for designs that have been approved already once by a recognised authority, the only Australian specific initial safety assurance task will be to review the existing design data to produce the four output reports.

5.4. Identification of the organisation conducting the initial safety assurance process

5.4.1. The organisation that conducts the initial safety assurance process does not necessarily need to be a government or government based enterprise. The process outlined is a technical review that produces reports and recommendations and which can be executed by organisations established in number of different ways. These options are described in Chapter 7.

5.4.2. For this report the organisation conducting the initial safety assurance process will now be referred to as the Initial Safety Assurance entity (ISAe).

5.5. In-Service Safety Assurance

5.5.1. The in-service safety assurance process is managed by the CM organisation. The elements of the process are shown in generic terms in Figure 5.

5.5.2. To ensure alignment of this report with other work being conducted by the NTC the organisation that is responsible for CM throughout the life of the AV will be known as the AV entity (AVe).

5.5.3. It is important to note that the AVe does not need to be the ISAe or a government authority of any kind. AVe functions could be performed by a wide range of organisations that would be authorised by the ISAe to be an AVe for a particular AV model or range of models.

5.5.4. The key aspect is that the AVe becomes the legal entity responsible for on-going, through-life technical integrity. It is likely that initially AV vendors could take up the AVe roles.

5.5.5. In-service safety assurance can be seen to be broken into two discrete phases:

a. Entry into service, and

b. Operation.

5.5.6. It is likely that the entry into service phase will involve the existing operational authorities, or entities authorised by those authorities to utilise the data produced by the initial safety assurance process to:

a. define the roads on which the vehicle is authorised to operate,

b. define the environmental limitations,

c. define the operational rules that will apply, and

d. authorise the operators and configuration managers, if any authorisation is required.

5.5.7. Further discussion on this process is contained in Chapter 8.

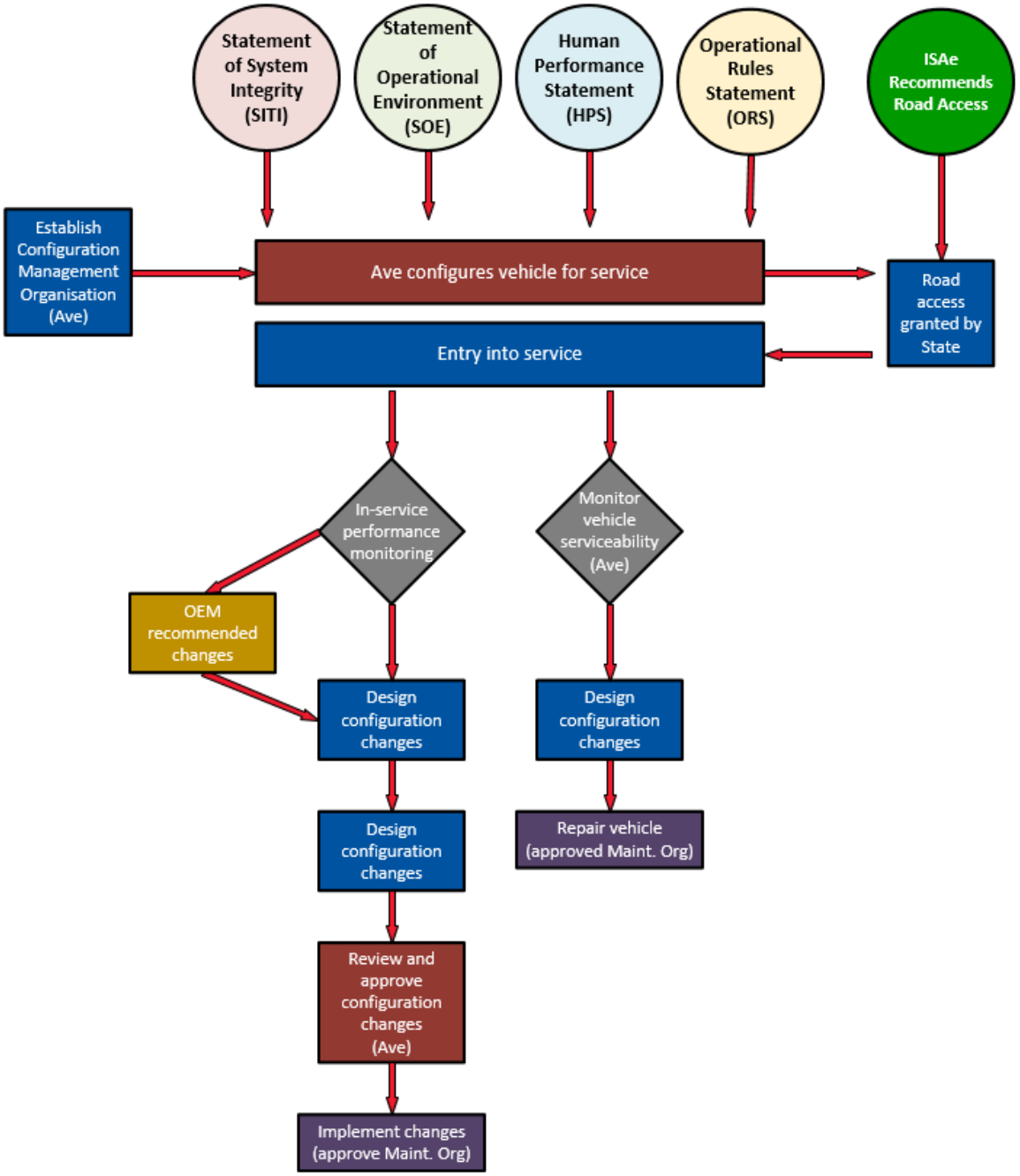


Figure 5: Summary of In-Service Safety Assurance Process

5.5.8. The entity responsible for CM (AVe) oversees the operational phase. The primary task for the AVe is to ensure that the levels of safety established during the initial safety assurance phase are maintained throughout the vehicle life. It is likely that the AVe may be called upon to perform a range of tasks that include but are not limited to:

a. monitoring ongoing serviceability and authorising maintenance,

b. reviewing and authorising incorporation of OEM modifications,

c. review and authorising incorporation of third party modifications, and

d. system performance monitoring.

5.5.9. As the AVe function is critical to the continued safety of the AV functions, the AVe holds a significant degree of legal liability. For this reason, the AVe will need to be operated:

a. by people determined to be competent,

b. operating within a defined process, and

c. having access to all the data necessary to perform the defined role.

5.5.10. The nature of the AVe role suggests that the AVe and the key personnel within the AVe will need to be licensed or approved in some manner.

In-Service Performance Monitoring

5.5.11. Given the nature of the technologies being utilised approvals to operate will be based on a safety analysis that includes many assumptions. Consequently, is highly likely that in-service performance monitoring will be required to confirm that automated vehicle functions are achieving required performance outcomes and that the assumptions are correct.

5.5.12. Likewise, with assumptions regarding operator performance, it is highly likely that in-service performance monitoring of operator performance will be required to confirm that AV functions are achieving required performance outcomes.

5.5.13. In keeping with other aspects of the SAS it is proposed that the data requirements for any given system are assessed and defined on a case-by-case basis. The SAS should not mandate particular data or particular data gathering methodologies. Rather, the system should suggest a process. It is conceivable that the process would require an in-service Data Monitoring Plan (DMP) to be approved as an aspect of initial safety assurance process then past to the AVe to execute.

5.6. Unsafe Conditions and the link to Penalties and Fines

5.6.1. The proposed SAS includes the concept of continuing or ‘in-service’ safety assurance. The continuing aspect of the SAS is in place to ensure that anything that could reduce the approved safety performance of the vehicle does not occur. This is achieved by:

a. managing changes in vehicle configuration,

b. managing maintenance, and

c. monitoring in-service technical and human performance.

5.6.2. Anything that impacts or could impact on safety performance of the AV is considered an ‘unsafe’ condition.

5.6.3. It is the primary responsibility of the AVe to identify the existence of unsafe conditions. When an AVe identifies an unsafe condition the ISAe will be advised by the AVe and the ISAe that will conduct an initial assessment of the unsafe condition. That initial assessment will involve an assessment of the fleet wide risk associated with the problem.

5.6.4. AV function’s non-compliance with road rules represent a design failure and an unsafe condition. If monitoring shows that an AV fleet is, under certain operating conditions, violating road rules then this could be a design error and a fleet wide problem that would be addressed via a design change.

Conversely, if monitoring shows that a single vehicle is violating road rules then this is likely to be an unserviceability that can be correct by maintenance.

5.6.5. In either case, the concept of a punitive penalty being applied to an individual (either AVe, operator or owner) because of a technical failure (design or serviceability) that results in a deviation from a road rule is inappropriate and counter-productive to the aims of the SAS. The SAS should encourage constant monitoring, identification and correction of unsafe conditions. Furthermore, the SAS should provide a mechanism for continuing improvement of the AV safety outcomes. Lesson learnt on one AV should inform the design and analysis on other AV systems. Such aims require that the AV SAS is not a penalty based system but one where unsafe conditions are dealt with in an open manner, not encumbered by the thought of potential simplistic punitive legal sanctions, such as speeding fines.

5.6.6. That is not to say that within the AV SAS there are no actions that will result in a penalty. Penalties would need to be in place for AVe entities that fail to fulfil their obligations. For instance, failure to manage configuration or advise the ISAe of an unsafe condition could result in a penalty. If a person was to change the configuration of an AV without approval being granted by the AVe then a penalty could be applied.

5.7. Technical Performance Requirements

5.7.1. Technical performance requirements are used in other automated systems that have a safety related aspect. An example of such requirements can be found in the Federal Aviation Regulation (FAR) part 25.1329 [19] that deals with autopilots.

5.7.2. Further advice in support of this requirement is provided in FAA Federal Aviation Authority (FAA) Advisory Circular 25.1329 "*Approval of Flight Guidance Systems*" [20]. The Advisory Circular is considered to be 'acceptable means of compliance' advice. What is illustrated by both the base requirement and within the detail of the advisory circular is that:

a. the technical requirements are expressed as high level performance outcomes, and

b. the requirements are written with a pre-existing knowledge of how autopilots and flight directors work.

5.7.3. Importantly these requirements have evolved over time and incorporate understandings that come from having such systems in service for many years.

5.7.4. The approach being suggest for AV technical specifications is based on the aerospace model and can be described as follows:

a. The AV SAS does not guess likely technologies and create technical specifications for systems not yet designed or envisaged.

b. Vendors develop concepts for automated functions and create suggested performance standards, preliminary safety analysis and prototypes.

c. The entity conducting the safety assurance compliance findings then negotiates with the vendor and agrees a performance standard and compliance finding methodology.

d. Compliance is found against this agreed certification plan.

e. If over time a particular style of automated functionality becomes more commonly fielded then it may become possible to create generic higher-level technical standards based on lessons learned.

5.7.5. The advantages of this approach are that:

a. innovation is not constrained by ill-formed technical standards;

b. the time taken to develop 'industry agreed standards' does not delay the introduction of new technologies; and

c. the final standards developed are based on real world lessons rather than assumptions.

5.7.6. It is noted that even when this approach to functional technical specification is adopted there is still a need to agree to standards for equipment environmental and durability compliance and other issues related to the ability of items of equipment to perform the functions allocated to them under all the prescribed operational conditions.

5.7.7. Individual items of equipment may be required to meet specific performance specifications [i.e. a Global Navigation Satellite System (GNSS) receiver may be required to meet a specific technical specification], however, in general, the requirements placed on individual system components will flow down from the higher-level safety assessment and hence will be only valid on a case-by-case basis. For instance, the performance specification for a GNSS receiver will depend on the function it performs and how it contributes to the safety outcome for the automated function.

5.8. Additional Requirements beyond Safety Assurance

5.8.1. During stakeholder meetings for the development of this report, the question of how additional requirements for advanced vehicles, such as environmental and cyber security requirements should be addressed.

5.8.2. While the process being discussed is centred on safety it is a process that finds compliance against agreed requirements. Consequently, the process could be expanded to address other requirements that a Government may wish to apply. The proposed SAS is flexible enough to accommodate non-safety related requirements.

5.8.3. There are precedents for this approach in other like SASs. In the aerospace sector, noise requirements, while not related to safety and not contained within the safety legislation or design rules, are addressed and compliance is found during the initial type certification process.

5.8.4. It is not within the scope of this report to explore other non-safety requirements within the processes outlined.

5.9. Safety Validation Methodology

5.9.1. The safety validation methodology being proposed is inherent in the initial safety assurance process shown as Figure 4.

5.9.2. The core elements of the safety validation are:

a. Vehicle or system vendor proposes a functionality and preliminary architecture.

b. Functionality is assessed using the PSSA process, which may use SAE J2980 [18] or equivalent.

c. Output from the PSSA allows the certification planning process to set safety goals for hardware failure modes and probability of failure.

d. Output from the PSSA allows the certification planning process to set safety design assurance levels for software and complex hardware.

e. Compliance finding is based on analysis of designs and on the artefacts produced by the software and complex hardware development process.

f. Compliance may also be based on system functional level testing (i.e. sensors work correctly with processors).

5.9.3. Once the vehicle enters service there is a further input to safety validation for in-service monitoring. In-service monitoring contributes to safety validation and highlights if intended safety outcomes are not being achieved and corrective action is required.

Safety Validation Methodology – Vehicle Level Testing

5.9.4. There has been a recent focus of AV testing using roads in the public domain. It is important in this discussion to understand the role of vehicle level testing in the overall AV safety validation.

5.9.5. The primary role of vehicle level testing is to:

a. provide data during the development process,

b. provide final confirmation of correct integration of all system components, and

c. assess assumptions regarding human performance and the HMI.

5.9.6. Importantly, it is noted that where AV functions are implemented in software and complex hardware then it is not possible, from a technical perspective, to assert a safety outcome by only using evidence gathered during vehicle level testing.

5.9.7. For software and complex hardware, safety can only be asserted if the design and test of those components is conducted using a design assurance process [21].

5.9.8. This is a key difference between the existing Motor Vehicle Standards Act (MVSA) vehicle certification process [13] and the safety assurance process proposed by this report. The existing motor vehicle certification process is a post-design, test-based methodology. While the system recognises that some complex aspects of compliance finding can be conducted via analysis and

modelling (see Circular 38-1-8 "*Approval for Computer Simulation of ADR 38 Service Brake effectiveness*" [22], in general terms the MVSA certification process relies on a process of inspection and test.

5.9.9. For AV function, vehicle level inspection and test will not be a suitable method to ensure the safety integrity of products and requires a move to a design assurance style process as proposed by this report.

5.10. Generic Case Study

5.10.1. This example is provided to illustrate how this system may be applied in a simplified, real world example.

5.10.2. A European car manufacturer applies to import to Australia a vehicle with automated functionality. The vehicle is an existing product that is being augmented with automated guidance designed to work in a limited environment. The vehicle has been approved for use in Europe with the initial technical integrity assessment and approval completed in Germany.

5.10.3. The basic automated functionality is described as follows:

a. Automated guidance and speed control is available on specific dual lane motorways.

b. Available roads are pre-determined and programmed into the GNSS guidance system.

c. Drivers enter a route plan.

d. Drivers enters an established lane keeping and speed keeping lane on the motorway.

e. The vehicle HMI advises the driver that the system can take control.

f. The driver enables the system then must keep their hands on the wheel for a further 30 seconds during which time the vehicles advises the driver that it has control of the vehicle.

g. The driver is required to 'monitor' correct performance of the system while it is in automated mode.

h. 90 seconds before the planned turn-off from the motorway the vehicle advises the driver to take back control.

i. If the driver has not actively confirmed control within 20 seconds of the turn-off the vehicle reverts to a fall-back, minimum risk condition by moving to the emergency stopping lane and stops.

Initial review

5.10.4. The vehicle OEM makes an initial request for approval and provides to the ISAe a system safety analysis for the vehicle and a certification report from the German authority. The system safety analysis is in accordance with SAE J2980 and the ISAe review confirms that the safety analysis does not contain any assumptions that would be invalid for Australian operations. As a result of this initial review the ISAe holds a formal certification planning meeting with OEM and it is agreed that the OEM will provide to the ISAe:

a. the standard ADR compliance test results and reports,

b. a series of artefacts form the software design assurance process,

c. environmental qualification data for the automated system components,

d. information regarding the data integrity and update control for the GNSS database, and

e. the human engineering test reports.

5.10.5. In addition, the OEM advises its intention to establish a single AVe for all these vehicles in Australia and the ISAe provides a briefing on all the requirements for the establishment of the AVe. Finally, there is agreement between the OEM and ISAe on the schedule for the assessment.

5.10.6. The ISAe review raises a question regarding the environmental qualification of an ultra-sonic senor on the vehicle and suggest that the senor performance has not be qualified for the operational dust environment likely to be encountered in Australia. The OEM agrees that there is an issue and undertakes further environmental testing of the sensor.

5.10.7. Once this testing is completed and all the other requested data has been reviewed the ISAe requests that the OEM provide a detailed list of the roads deemed suitable for the automated functions of their vehicle (the list that will be programmed into the Australian version of the vehicles).

5.10.8. Following the establishment and approval of the AVe the OEM advises that, since the AVe is based in Melbourne, it is their intention that all vehicles will be registered and granted roadworthiness certificates in Victoria. Where the AV functionality is only relevant for specific roads the AVe will discuss and agree with each State authority the roads on which the AV functions will be allowed to operate. The AVe will need to advise this to VicRoads and the ISAe so there can be confirmation that the agreed road access is correctly managed by the vehicle system.

5.10.9. The ISAe provides to VicRoads recommendations regarding the allocation of roadworthiness approvals for the vehicle.

In-Service Management

5.10.10. Vehicles go on sale and are delivered to customers with a contractual understanding that:

a. all vehicles must remain under the control of the AVe,

b. no modifications are allowed without approval of the AVe, and

c. maintenance can only be conducted by AVe authorised workshops.

5.10.11. Owners' contracts advise that if these conditions are invalidated the AVe will advise VicRoads to suspend registration and vehicle insurance will be invalid.

5.10.12. As part of the pre-delivery process the AVe ensures that the latest GNSS database is loaded and that the road traffic laws for each of the approved roads is correct.

5.10.13. 18 months after initial entry into service the M66 motorway in Tasmania is opened. The AVe conducts a preliminary assessment and confirms that M66 design matches the capability of the vehicle system. The AVe asks the OEM for approval to use this road. The OEM has been granted a 'design approval authority' by the ISAe and changes to road applicability are within the scope of approval for the OEM design entity.

5.10.14. The OEM reviews and approves the vehicle for the M66 road and releases a software update for the AVe. The AVe completes its review of configuration compatibility and finds that all vehicles delivered after May 2019 can have the new software uploaded but vehicles delivered before May 2019 require a minor hardware update to be compatible. The AVe advises owners and operators and commences the update program.

5.10.15. Monitoring of vehicle performance by the AVe identifies an issue whereby the fleet experiences seemingly random excursions beyond closing distance and closing rate limits for traffic ahead of the vehicle. These failures do not result in incidents and are within the safe allowable limits but outside the design limits.

5.10.16. The AVe notifies the OEM, ISAe and VicRoads of an 'Unsafe Condition'. The ISAe and the OEM review the issue and agree that a resolution is required within 3 months or 300,000 fleet operating hours, whichever comes first. The AVe is requested to provide daily reports on aggregate hours to the ISAe and to increase the reporting rate on the data related to this failure.

5.10.17. The OEM identifies that the failure can be correlated with days of higher humidity and subsequent analysis shows that the radar sensor performance does not remain within specification above a certain humidity level. The fault is found to be related to incorrect testing by the test house used by the radar sensor vendor. The ISAe contacts the German regulator to advise the problem and the solution being proposed.

5.10.18. The OEM advises the ISAe of the rectification plan. The OEM releases a design change, which is approved by the ISAe, (because it is outside the OEM scope of approval) and the change data and parts are provided to the AVe. The AVe, the ISAe and VicRoads meet to discuss the recall program. The AVe has advised that it will take 4 months and 400,000 fleet hours to fully complete the recall and has provided a schedule. The ISAe conduct a risk analysis and advise the AVe and VicRoads that the plan is acceptable.

5.10.19. The AVe executes the corrective action using its network of approved maintenance organisations.

6. How does the Safety Assurance System integrate into the regulatory framework?

Key points:

The objectives of this report where set by the NTC and are defined as follows:

- Identify options for the governance models that support a nationally consistent process to approve AVs.
- Identify possible structures for an approval process for AVs.
- Discuss technical performance requirements that could be applicable to AVs.
- Identify possible safety validation methodologies for AVs.

To answer these questions the review conducted has:

- established the context within which an approval process exists, this is shown in Chapter 4; and
- nominated a candidate, reference SAS that is shown in Chapter 5.

Once the Chapter 5 SAS approach is adopted the questions that need to be addressed by this report, to answer the higher-level aims, are as follows:

- What is the most appropriate governance structure for the ISAe?
- Who should authorise and oversee the operation of the AVe entities?
- Who should authorise AV access to the road network?
- What is the relationship between the ISAe and the entities that authorise access to the road network?

Does the ISAe:

- provide ‘reports’ to the road network manager?
- provide a recommendation to the road network manager to grant access?
- provides an approval to access the road network?

6.1. Criteria for assessing Governance Options

6.1.1. The following criteria have been used to develop the list of potential governance options. These same criteria provide a means to choose between options.

6.1.2. **National Entity Preferred** – Most stakeholder feedback has noted a preference for a national entity to perform as many SAS functions as possible. This is to manage cost and resources and to ensure that vendors go through a single process for vehicle or system approval for the whole country. This was a specific concern of smaller states who were concerned about resources (both cost and expertise) required to implement the proposed SAS.

6.1.3. **Timeliness** – Stakeholder feedback unanimously expressed concern regarding the impending introduction of AV functionality into the Australian market in the absence of any consistent regulatory framework or SAS.

6.1.4. **Degree of legislative change required** – Some stakeholders expressed concern that complex legislative changes can be slow to implement and prefer options that minimise the requirement for legislative change.

6.1.5. **Removal of authority to access road networks** – Many stakeholders where seeking a governance structure that was clear on how access to the road network (approval to operate) could be removed if a vehicle was determined to be unsafe.

6.2. Assumed Safety Assurance Process

6.2.1. This report discusses governance structure options that would be used to implement the SAS. No options are offered regarding the form of the SAS. This discussion assumes that the SAS being implemented is that outlined in Chapter 5 and summarised in Figure 4 and Figure 5. This approach has been adopted because the SAS of similar industries (rail, aerospace, oil and gas, nuclear power, shipping) contain the same key attributes, including:

a. an interrelationship between technical, environment and human performance factors;

b. an initial examination of technical integrity that is based around a formal safety analysis;

c. an understanding the safety analysis is bounded by an expectation of environment and human performance;

d. an in-service CM process; and

e. a facility for in-service monitoring and correcting action.

6.2.2. The Australian AV SAS proposed in Chapter 5 has all these elements. It is asserted that while the details of the eventual SAS will vary from what is shown in Chapter 5 the general form will be the same and all the same basic functions will need to be implemented in some manner. Consequently, given the likely 'standard form' of the SAS it is unlikely that any change in the SAS detail would invalidate the choice of Governance structure.

6.3. Assumed Allocations

6.3.1. A proposed process structure for the SAS is shown in Appendix A. Using the ideas shown in Appendix A and the detail in Chapter 5 the basic functions required for implementing the SAS were identified and are outlined in Table 1 below. This table represents an allocation of the processes between those where optional solutions are possible and those where there is only one obvious solution.

Safety Assurance System Process	Possible allocation	Rationale
Approval of Design Organisations	Options available	Once a process is defined this looks like an audit Q/A process.
Recognition of National Authorities	Options available	Once a process is defined this looks like an audit Q/A process. May require Commonwealth introduction.
AV Initial Safety Assurance Process	Options available	Once process is defined, including appeals mechanism, this is a technical task that could be conducted by a suitably qualified entity.
Ongoing support and maintenance of Australian Design Rules	Leave with DIRD	Could in the long term be undertaken by third party but change not justified by present AV introduction.

Safety Assurance System Process	Possible allocation	Rationale
Compliance finding against non-AV ADRs	Options available	Could be conducted by same group conducting AV Initial Safety Assurance Process if this was most efficient manner for States and vehicle Vendors.
Production Integrity	Options available	Once a process is defined this looks like an audit Q/A process.
Configuration Management	Options available	New process, existing models on how to set up approved organisations.
Tech data performance monitoring and reporting	Options available	Due requirement for technical understanding and background probably best done as a joint AVe and Initial safety assurance organisation joint task.
Approval of Organisations conducting Maintenance of AV systems	Options available	Once a process is defined this looks like an audit Q/A process.
AV – specific operator approval	States	Training / Assessment could be conducted by third parties but final approval should be in line with State licensing due ability to remove authority.
Human Performance monitoring and reporting	Options available	Due requirement for technical understanding and background probably best done as a joint AVe and Initial safety assurance organisation joint task.
AVs Navigation databases	Options available	Once process is defined this is a technical task that could be conducted by a suitably qualified entity.
AVs Infrastructure	Options available	Once process is defined this is a technical task that could be conducted by a suitably qualified entity.
AV Environment approvals	States	Only states have the data on the road networks they are responsible for and have the present registration (approval to operate on State roads) authority. Need ability to remove authority

Table 1: Safety Assurance System Elements and Allocation of Responsibility

6.3.2. Chapter 7 addresses the questions regarding the form of the ISAe and the supervision of the AVe and Chapter 8 addresses questions around the outputs from the ISAe and who approves access to the road network.

7. Initial Safety Functions Governance Structure Options

Key Points:

- Four options for governance arrangements for the Initial Safety Assurance entity (ISAe) are discussed.
- Each of the options are feasible and do not require any additional legislation to establish.
- Beyond the ISAe governance the most appropriate ways to organise the following is discussed:
  - Approval of Design organisations;
  - Recognition of National Authorities;
  - Conduct of Product integrity review;
  - Approval of AVe;
  - Approval of maintenance organisations;
  - Conduct of in-service monitoring; and
  - Approval of AV navigation databases.

7.1. Options for the ISAe Organisation

7.1.1. Four options for the governance arrangements for the ISAe are:

a. **Option 1**: no additional SAS function for AV beyond existing ADR process.

b. **Option 2**: extension to existing road vehicle certification system.

c. **Option 3**: new or existing Government corporate entity.

d. **Option 4**: full industrial entity.

Initial Safety Assurance Option 1 – No Additional Regulation

7.1.2. It would be possible to make no immediate changes to the existing regulatory systems. If this occurred, then it is assumed that in the medium term DIRD will continue to add to the ADR structure as international working groups.

7.1.3. This approach is not in line with the accepted recommendations in the NTC policy paper "*Regulatory reforms for automated road vehicles*" [3].

7.1.4. This approach would, given the changes occurring within the industry relative to the rate of international standard development, mean many new technologies being un-regulated. This is already occurring with new automated technologies such as adaptive cruise control and automated parking systems.

7.1.5. Notwithstanding the potential application of Compulsory Third Party (CTP) insurance, this no-regulation approach leaves safety assurance to be addressed by consumer protection laws and the threat of civil action against vendors by those injured by the products. This approach of treating safety assurance as a contractual issue between customer and supplier may be satisfactory were it not for the concept that many people beyond the customer are exposed to the risk from the AV.

7.1.6. The fundamental issue with this approach is that using legal sanction as a safety assurance mechanism is a reactive approach. Harm must be done before the sanction can be applied. In this case, the protection of people from harm is left to a commercial decision by the equipment vendor.

7.1.7. A secondary issue is that a spate of accidents from one vehicle vendor would have a substantial impact on the community acceptance of AV technologies in general. If it is accepted that these automated technologies should support an increase in road safety and productivity, then any loss of social license for AVs will have an overall detrimental impact on the community well beyond the direct harm caused by the accident(s). Furthermore, there is the potential for damage to a range of businesses working with AVs because of poor performance by one individual company.

7.1.8. The logical extension of this 'no regulation' approach is that there would no longer be a need for the existing ADRs and vehicle certification process; which is not being suggested by any of the stakeholders.

7.1.9. It is noted that this option was not raised by the majority of stakeholders, all of whom expressed that there was a need for some form of SAS. The option is included in this report for completeness.

7.1.10. Advantages of Option 1 include:

a. No regulatory change required.

7.1.11. Disadvantages of Option 1 include:

a. Harm needs to occur before risk that public is exposed to is understood.

b. Possible loss of social licence for AV technologies, which slows gains in safety and productivity.

c. Significant periods of time where new technologies are not covered by any standards leave public at risk.

Initial Safety Assurance Option 2 – Extension of Existing New Vehicle 'Certification' Process

7.1.12. The existing Commonwealth DIRD RVCS, as administered by the Vehicle Standards Safety Branch (VSSB), presently administers a process of new vehicle certification and could expand that process to include the Initial Safety Assurance Process as shown in Figure 4.

7.1.13. It is noted that the existing RVCS system is a substantially different process than that being proposed Figure 4. The primary differences are that the existing RVCS system is based on a system of testing to show compliance against reasonably simple technical specifications. The proposed process involves establishing the certification requirements for an AV function on a case-by-case basis using the safety analysis as a guide.

7.1.14. The existing VSSB team is unlikely to have the necessary skills to execute the initial safety assurance process being proposed for the AV initial technical assurance process. The skill requirements include:

a. a design-level knowledge of sensor-based technologies and sensor data fusion,

b. a design-level knowledge of automated guidance methodologies,

c. an understanding of design assurance for software and complex hardware,

d. a detailed knowledge of system safety engineering process, and

e. an understanding of human engineering issues and methodologies.

7.1.15. However, within DIRD the necessary skills may already exist within the Civil Aviation Safety Authority (CASA) Initial Airworthiness Group.

7.1.16. Noting that the initial safety assurance process proposed for AVs is not dissimilar to existing CASA processes of initial airworthiness; an opportunity may exist to create a single specialist technical safety assessment group within DIRD. This safety assessment group would be a technical specialist group whose resources and expertise could be shared by CASA and the VSSB [and possibly other related government entities such as the Office of the National Rail Safety Regulator (ONRSR)] who would maintain administrative responsibility for aviation and AVs respectively. The aim is to build an expertise base that can be shared across government functions with the aim of being able to support a centre of expertise in a cost-efficient manner.

7.1.17. Alternatively, it would be possible for any Government entity, including the existing DIRD team to subcontract the necessary expertise.

7.1.18. Having the initial safety assurance process managed and executed by the VSSB would mean that both aspects of new vehicle certification (automated functionality safety assurance and compliance against Australian Design Rules) would be managed by the same organisation, providing a single point for all certification activities for vehicles.

7.1.19. One issue to be considered is whether the existing legislative instrument, the MVSA 1989 [7], would need to be amended to support the initial safety assurance process. This question is only seen as important because it is known that changes to the basic legislation are slow, possibly taking many years.

7.1.20. Advantages of Option 2 are that it:

a. builds on existing processes, and

b. is simple to address ADR compliance and SAS compliance in one entity.

7.1.21. Disadvantages of Option 2 are that it:

a. may need change to MVSA legislation, which can be slow; and

b. requires a significant increase in DIRD technical capability.

Initial Safety Assurance Option 3 – New or Existing Government Corporate Entity

7.1.22. If the ISAe is primarily conducting assessments for and providing recommendations to States then a possible model is to create a corporate entity that is funded by a combination of State Governments, Commonwealth Government and user charges.

7.1.23. There are examples of such bodies in the transport and energy sectors. A range of State and National legislative structures are used. An AV initial safety assessment entity may not require legislative support if it is only providing technical advice to States.

7.1.24. It would be possible to either create a new Government entity or use an existing entity.

7.1.25. An existing entity could be used to host the initial safety assurance process for a limited period (e.g. 5 years). Such an approach would leverage off the idea that:

a. administrative functions are already in place,

b. a base funding mechanism that is a State / Commonwealth mix may already be in place.

7.1.26. In this approach, it is envisaged that following development of the process documentation and systems the ISAe would maintain a small administrative team. Most the technical assessment work could be contracted out to industry partner(s) who would work under a Government organisation banner

7.1.27. The advantage of this approach is that it is quick to establish and would allow very tight cost control, as technical support services would only be procured as required by the market.

7.1.28. Advantages of Option 3 are that it:

a. requires minimal Legislative change (States only, if at all);

b. shares cost sharing with users;

c. is quickest option as administrative constructs and relationships may already be in place; and

d. can scale costs to market requirements by use of consultants.

7.1.29. Disadvantages of Option 3 are that it:

a. may need some changes to enabling legislation;

b. has potential to require applicants to deal with this entity and the existing DIRD process.

Initial Safety Assurance Option 4 – Full Industrial Entity

7.1.30. This final option involves an industry group establishing the ISAe to execute the Initial SAS functions. This is a similar approach to that used in shipping where private companies such as Lloyds Register provide a similar service.

7.1.31. In this model the vehicle or system vendors work directly with the industry based ISAe to create the SAS artefacts that would then be used by States to grant road access.

7.1.32. The main issue with this approach is that the States would need some way to assess and approve the industrial entities that may be interested in performing this role. To create this approval process, a series of procedures, assessment criteria and guidance material would need to be created by an applicable Government entity to ensure a level playing field existed between all companies wishing to provide SAS services.

7.1.33. Advantages of Option 4 are that:

a. it is reasonably quick to establish, and

b. all costs are born by industry and users.

7.1.34. Disadvantages of Option 4 are that:

a. it requires some government group to develop assessment and approval processes to ensure commercial level playing field.

Certification the Responsibility of a Single Entity

7.1.35. One issue with creating an entity that is not the existing DIRD VSSB is that companies wishing to import vehicles into Australia with automated functionality may need to deal with two 'regulatory bodies', the VSSB for ADR compliance issues and the new entity for the overall approval of the vehicle. This is considered a sub-optimal outcome.

7.1.36. Where a vehicle contains automated functionality, a possible solution is that the National Minister delegates authority for ADR compliance finding to the new entity (in the same manner that the existing VSSB administrator is delegated authority for ADR compliance finding). Such a delegation should be possible as the new entity will have in place compliance finding processes that are already more detailed than those presently utilised by the RVCS. Delegation by the Minister is supported by the existing MVSA [7].

7.2. Approval of Design Organisations and Recognition of National Authorities

7.2.1. Once the necessary processes are developed then the approval of design organisations becomes a simple audit process that could be executed by the same entity that is responsible for the initial SAS.

7.2.2. Recognition of National Authorities is a more complex issue, as it is ultimately a Government-to-Government negotiation. It is thought to be most appropriate if this activity is hosted by DIRD with technical support provided by the ISAe.

7.3. Production Integrity

7.3.1. For the technologies being discussed production integrity issues are far more complex than can be addressed by the processes presently in place as an element of the RVCS system [13].

7.3.2. Initially it was thought that the technical competencies required complement those required for the initial safety assurance. Consequently it is thought that the ISAe should be responsible for the production integrity processes. If the ISAe ends up being the VSSB then production integrity will be conducted by a single entity.

7.3.3. If a non-DIRD approach is adopted for the ISAe then it may be appropriate for the production integrity process, as well as the ADR compliance, to be delegated to the ISAe. This prevents the applicant having to deal with two entities.

7.4. Approval and monitoring the operation of the AVe entities

7.4.1. CM is a new concept for the industry that will require significant effort to establish. It is thought that the SAS should support the ability for vehicle OEMs, system OEMs or third-party companies to perform the CM role for a given AV fleet or system.

7.4.2. To achieve this the following is required:

a. Establish the CM regulatory processes and requirements that support the appointment of configuration managers (AVe).

b. Provide support for entities wishing to apply to be an AVe.

c. Initial approval of each AVe.

d. Ongoing supervision of each AVe.

7.4.3. The two options for managing the AVe is to use either a National body or State based bodies aligned with the existing roadworthiness process.

7.4.4. It is recommended that the management of each AVe should be a national process since the expertise requirements will take time to establish and would be cumbersome for each individual State. A national approach also more easily supports the concept that a vehicle OEM may wish to establish one AVe to cover all its Australian customers in order to control costs.

7.4.5. To get the CM processes established as quickly as possible, it is recommended that the existing CASA Part 42 "*Continuing airworthiness requirements for aircraft and aeronautical products*" be scaled back to the level necessary to support AVs and used as an interim starting process. This will assist industry develop their level of understanding and what is required of them.

7.4.6. This approach is suggested because it can be implemented quickly, the existing CASA support material (including training) has been designed and tested to fulfil and very similar requirement, and the material is already all owned by the Commonwealth.

7.4.7. Once the processes are in place it is thought most appropriate if, in the initial 5 years, the approval and monitoring of AVe entities is executed by the ISAe. This will provide industry, in the nascent period of the SAS, with one group to deal with while the SAS is established and understood. After the initial 5 years it would be possible to split AVe management from the ISAe, if required.

7.5. Approval of Organisations Conducting Maintenance of AV Systems

7.5.1. The three options for the approval of maintenance organisations are:

a. Approval by the ISAe,

b. Approval by the AVe, or

c. Approval by existing State authorities.

7.5.2. Given the potential for highly distributed maintenance support organisations, a national entity is not seen as viable, at least in the initial stages of the introduction of the AVs.

7.5.3. From a legal accountability perspective, the AVe will be required to assert that the vehicle maintains ongoing safety. To do this the AVe will need to:

a. manage what maintenance is necessary to ensure ongoing safety,

b. ensure any modifications do not compromise safety, and

c. authorise modifications that will be conducted by maintenance organisations.

7.5.4. Given these responsibilities, it is thought that approval of maintenance organisations should be conducted by each AVe. Part of the approval of each AVe will involve confirming that those entities have in place the processes to ensure that maintenance organisations have the data, the tools and the people necessary to ensure that the maintenance or changes to configurations that they have authorised are correctly executed.

7.6. Tech Data and Human Performance Monitoring and Reporting

7.6.1. The nature of the data that will need to be collected and analysed across the life of the vehicle, to ensure ongoing safety, will be defined at the initial safety assurance certification planning stage.

7.6.2. The gathering of data is essential to ensuring the ongoing safety of the AV and the identification of the emergence of unsafe conditions. Given that it is the AVe that has overall responsibility for ongoing safety it is most appropriate that the AVe manages and analyses the in-service data.

7.6.3. The AVe could be assigned the responsibility to report to the ISAe (and the road agencies) if the data shows that safety assumptions and safety goals are not being achieved.

7.7. AVs Navigation Databases

7.7.1. The degree to which navigation databases must be managed will depend on how the data integrity impacts the safety outcome for the vehicle. Consequently, the data base management requirements will be defined at the initial safety assurance certification planning stage.

7.7.2. Depending on the nature of the data and its use the entity providing the data may need to be approved as a design organisation. Once this is done the AVe will know that databases are being provided by an approved entity and hence will be able to authorise updates to vehicle databases.

8. Access to the road network

Key Points:

For the SAS approach nominated in Chapter 5 the final act is to authorise the AV to access the road network. This authorisation will be based on:

- the details contained in the reports resulting from the initial safety assessment;
- the existence of an AVe that can ensure ongoing technical integrity; and
- the existence of an in-service monitoring function.

Several questions surrounding the granting of access where identified in Chapter 6. These are:

- Who should authorise AV access to the road network?
- What is the relationship between the ISAe and the entities that authorise access to the road network?

Does the ISAe:

- provide 'reports' to the road network manager?
- provide a recommendation to the road network manager to grant access?
- provide an approval to access the road network?

There are two issues that need to be considered in addressing the above questions.

1. Which is the most appropriate regulatory level for road access to be assessed and granted. Should this be done at the state level or at a national level?
2. What is the best method to support an assessment of the ability of the vehicle to address environmental variation? The answer to the second question informs the first question. Further, the answer to the second question is heavily dependent on the technology being discussed.

8.1. Variations with AV technical architecture

8.1.1. As options regarding who should authorise access to road networks were being discussed with stakeholders, an issue surrounding the nature of vehicle technical architectures that informs this discussion, was identified.

8.1.2. How AV technologies address variation in operational environments can be divided into three categories:

a. **Type 1** – Vehicle systems that assess the environment and decided continuously if the environment being encountered is suitable to operate in.

b. **Type 2** – Vehicle systems where the suitable operating environment is pre-determined by analysis of the road network and then compatible or supported roads are added into the guidance system database. Using its GNSS location the vehicle then determines if it can safely engage an automated function.

c. **Type 3** – Vehicles systems operating on a closed network or fixed pre-determined network where compatibility can be simple pre-surveyed.

8.1.3. It would be possible with a Type 1 or Type 3 vehicle for a single national entity to conduct a safety assessment of the vehicle function. For Type 1 vehicles the ability of the vehicle to correctly assess its environment is a design attribute that gets assessed during the initial safety assurance process.

8.1.4. Type 2 vehicles require a much more complex process. Type 2 vehicles require that:

a. the environment within which the vehicle has been designed to operate is fully disclosed;

b. someone, possibly the vehicle OEM or applicant, has surveyed Australian roads to identify those roads that match the vehicle capability are identified;

c. the safety assurance process must confirm that the survey process has been correctly completed and that assumptions about road environments are correct.

8.1.5. This confirmation that roads have been correctly identified and surveyed could become a complex task that requires a sound working knowledge of the nature of the road design, infrastructure details, and climate and weather variation for the roads that are being suggested.

8.1.6. This will mean that the ISAe will need to work in close co-operation with State road authorities to ensure that OEM assessment and recommendations on roads are correct.

8.2. Who should authorise AV access to the road network?

The existing process that grants roads access approval – light vehicles

8.2.1. The existing Commonwealth MVSA establishes:

a. the authority of the Commonwealth to control the import of motor vehicles in to Australia;

b. the process of certification against defined standards (the ADRs); and

c. the process and authority to fix and remove ‘compliance plates’.

8.2.2. The MVSA does not provide an authority to access public roads. That authority is, except for heavy vehicles registered nationally using the “*Federal Interstate Registration Scheme”* [29], provided by States issuing Certificates of Roadworthiness and Registration.

8.2.3. Once a vehicle has been imported (or manufactured in Australia) the individual State authorities often rely on the ‘notion’ that the vehicle has compliance against the ADRs. However, the State authorities don’t necessarily require that each vehicle being granted a road worthy certificate has a physical compliance plate. The following extracts from VicRoads Vehicle Standards Information leaflet 26 “*Roadworthiness Requirements*” [16] notes the following:

> *Identification plates were required on vehicles manufactured after June 1988 as evidence that, at the time of first registration, the vehicle complied with the applicable ADRs. However, Identification plates are often damaged, lost or stolen during the life of the vehicle. Therefore, the presence of an Identification (compliance) plate is not a mandatory requirement for the issue of a Certificate of Roadworthiness, and a Vehicle Assessment Signatory Scheme (VASS) approval certificate should only be requested by a Licensed Vehicle Tester, when a vehicle modification, which effects handling, structural integrity, or compliance with the standards for registration, does not appear to comply with good industry practices.*

8.2.4. It is noted that the requirement for heavy vehicles is different to this.

Discussion of options

8.2.5. The initial safety assurance process outlined in Figure 4 suggest that the ISAe process will output:

a. a compliance plate asserting compliance with ADR(s);

b. a statement of AV safety assurance compliance;

c. a statement of AV environmental design assumptions and limitations; and

d. a statement of AV human performance design assumptions and limitations.

8.2.6. Given that the ISAe has already been identified as being a single national entity, if this entity was to grant an approval for road access this would be a national approval to operate on State, Territory (and local government) roads.

8.2.7. The alternative option is that the States keep the final access authority that they have today.

Option 1: National Authorisation

8.2.8. The advantage of national authorisation is that:

a. the national entity will have established the best understanding of the vehicle capability and would be able to provide a single service for all States.

8.2.9. The main disadvantages of national authorisation are that:

a. the issues of Type 2 vehicle compatibility as noted in sections 8.1.4 to 8.1.6, and

b. this approach may require both State and National legislative changes.

8.2.10. While the need for legislation is not in and of itself a problem, it does take time, and timeliness was identified in Chapter 6 as an important criterion when assessing options.

Option 2: State Authorisations

8.2.11. The advantages of State access approvals are that:

a. existing legislative structures can be used – see section 8.5 for a possible mechanism.

b. this approach accommodates Type 2 vehicles

8.2.12. The disadvantage of State access approvals is that:

a. applicants must deal with multiple states. Note: this disadvantage is only applicable to Type 2 vehicles.

Recommendation

8.2.13. Given that the State based system of access approval can be implemented in a timely manner (possibly without any legislative change), this aligns with existing regulatory processes (i.e. represent the minimum change) and more easily accommodates Type 2 vehicles than a National based system, a system of State based access approval is recommended.

8.2.14. As identified at Figure 6, the ISAe provides to each State a recommendation to grant access of Type 1, Type 2 and Type 3 vehicles. The States in turn grant access to road network based on the recommendation from the ISAe.

8.3. What is the relationship between the ISAe and the entities that authorise access to the road network?

8.3.1. Earlier three options where outlined. It was suggested that either the ISAe:

a. provides **reports** to the road network manager;

b. provides a **recommendation** to the road network manager to grant access; or

c. provides an **approval** to access the road network.

8.3.2. The third option has already been excluded for the reasons outlined in section 8.2.

8.3.3. Providing reports only would mean that the States might need to establish an expertise base that would mimic the expertise in the ISAe and that is not considered as either ideal or possible.

8.3.4. It is thought, because the ISAe holds all the expertise, that the ISAe should recommend to States that access to the road network be granted. This recommendation assumes that the ISAe would advise the States of any special considerations or limitations that should be applied.

8.3.5. For Type 2 Vehicles the ISAe will need to work with the States (and the AVe) to assess the technical aspects of road compatibility and approve access.

8.4. Removal of Authority to Operate – The Unsafe Condition

8.4.1. The SAS described in Chapter 5 includes the concept of continuing or 'in-service' safety assurance. The continuing aspect of the SAS is in place to ensure that anything that could reduce the approved safety performance of the vehicle does not occur. This is achieved by:

a. managing changes in vehicle configuration,

b. managing maintenance, and

c. monitoring in-service technical and human performance.

8.4.2. Anything that impacts or could impact on safety performance of the AV is considered an **'Unsafe'** condition.

8.4.3. It will be the primary responsibility of the AVe to identify the existence of unsafe conditions. When a AVe identifies an unsafe condition this will be advised to the ISAe which will then conduct an initial assessment. That initial assessment of the unsafe condition will involve an assessment of the fleet wide risk associated with the problem.

8.4.4. This is essential to meet the high-level requirement for legal accountability to be clear throughout the life of the vehicle.

8.4.5. Once the initial assessment is conducted the ISAe entity will advise all States that have approved access:

a. the nature of the unsafe condition;

b. an estimate of the fleet wide risk;

c. a recommendation to immediately remove access authority for the AV or AV function; and/or

d. a recommendation on how many fleet operating hours are acceptable (from a risk perspective) until the unsafe condition is rectified.

8.4.6. Where individual vehicles are found to be unsafe (e.g. an unauthorised modification to a single AV) then the AVe would notify the State authorities directly.

8.5. The possibility that no legislative change is required.

8.5.1. If the recommendation that the States hold the final authority to allow road access then the potential exists, due to the nature of the existing roadworthiness and registration processes, that there may not need to be any legislative changes to implement the AV SAS process. The situation in Victoria is used as an example.

8.5.2. In Victoria, a requirement for a vehicle to be registered (and hence legally allowed to access the network) is a certificate of roadworthiness. The *"Victorian Road Safety Vehicle Regulation 2009"* controls the relationship between the roadworthy certificate and registration.

8.5.3. The regulation does not define what constitutes a roadworthy vehicle. Rather, it gives the Corporation the right to define what roadworthiness means as an administrative act. (Refer to "*Road Safety Vehicle Regulation 2009 – Reg 220"*). VicRoads uses its power granted under Reg 220 to issue an administrative instruction VSI26 Dec 2012. It is this instruction that defines what is required for a vehicle to be deemed roadworthy and hence able to be registered.

8.5.4. To cover AVs VicRoads could up-issue VSI26 to note the following:

a. Provide a definition of those automated functions that need special consideration (e.g. anything that provides auto, hands-off-wheel, steering guidance, auto braking, auto throttle control, auto separation).

b. Require such a vehicle to have an approval from the ISAe.

c. Require such a vehicle to have evidence that it is under the control of an approved AVe.

d. Require that the registration applicant is an approved AVe.

8.5.5. Such requirements are similar to the requirements that cover modifications and the VASS process, all of which are administrative not legislative.

8.5.6. If VicRoads establish an ISAe, authorise the ISAe to approve an AVe and make the changes noted above then they have AVs under total control and have locked in the SAS methodology. This is possible without any changes to the Road Safety Vehicle Regulation 2009 because REG 220 already provides a power to define technical integrity. Similar legislative approaches exist in NSW. Other State legislation has not been investigated.

8.5.7. Given that the ISAe is providing a service to States, and can be mechanised by a private company, there is no reason for its establishment to be supported by legislative changes.

8.5.8. This would mean that ISAe establishment, AVe establishment and management, and road network access could all be implemented without the need for legislative change.

9. Summary of recommended allocations

9.1.1. In Table 1 outlined the functions that needed to be allocated to specific entities. The ensuing discussion has resulted in the following suggested approach to functional allocations:

Safety Assurance System Process	Recommended Allocation
Approval of Design Organisations	ISAe
Recognition of National Authorities	ISAe
AV Initial Safety Assurance Process	ISAe
Ongoing support and maintenance of Australian Design Rules	ISAe with DIRD
Compliance finding against non-AV ADRs	ISAe
Production Integrity	ISAe
Configuration Management	Ave (industry / OEM based)
Approval of AVe Entities	ISAe
Tech data performance monitoring and reporting	AVe Entities
Approval of Organisations conducting Maintenance of AV systems	AVe Entities
AV – specific operator approval	States – as part of granting access
Human Performance monitoring and reporting	AVe Entities
AVs Navigation databases	Approval of Data Base suppliers - ISAe
AV Environment approvals	States – as part of granting access

Table 2: Recommended Safety Assurance System Allocations

9.1.2. Based on the above the final arrangement of the SAS can be summarised in the following diagram:

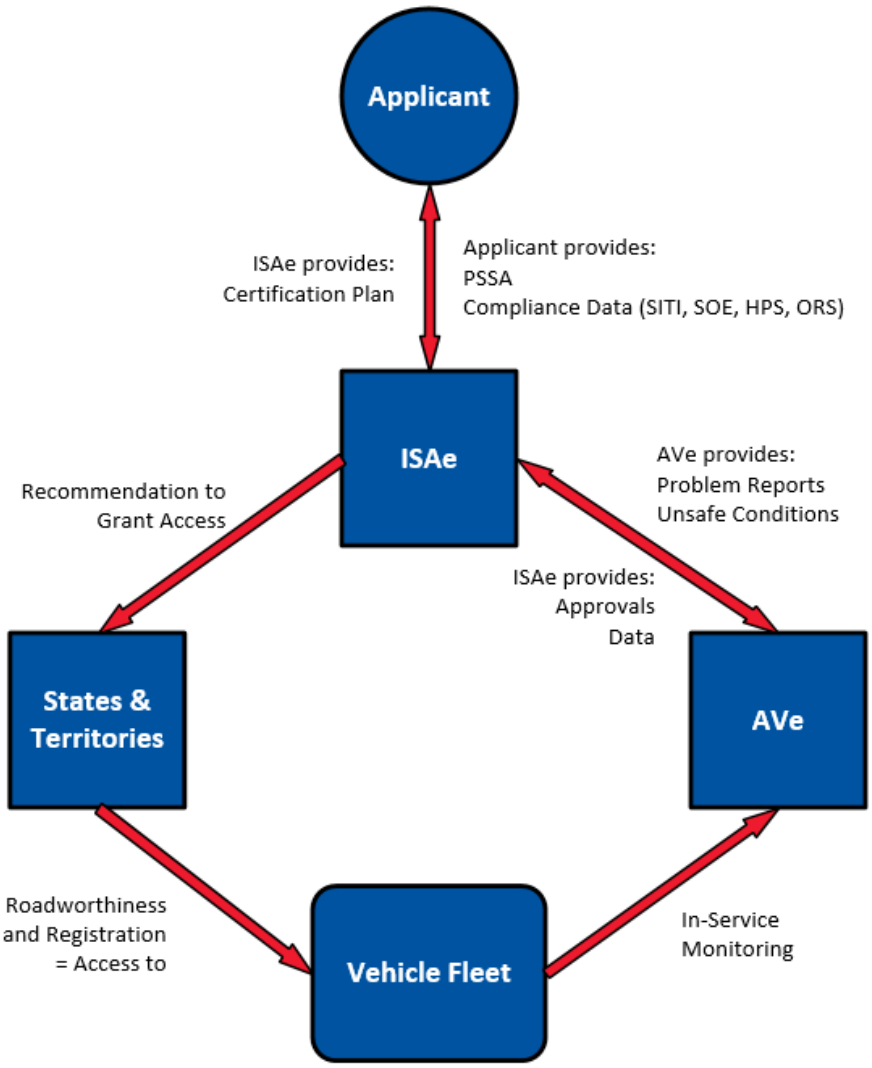


Figure 6: Safety Assurance System Core Elements

10. Conclusion

10.1. Summary

10.1.1. In November 2016, the Australian Transport Council approved recommendations outlined in the NTC policy paper, "*Regulatory reforms for automated road vehicles*" [3] The paper identifies the need for a safety assurance system for automated vehicles. This paper documents discussions with stakeholders regarding the nature of a safety assurance system. Stakeholders suggested that the SAS for AVs should:

a. be nationally consistent;

b. adopt a safety case approach based on the risk pro le of the application, with responsibility of the applicant to demonstrate the safety performance of the automated vehicle;

c. manage where and how the vehicle can operate;

d. ensure the ability for agencies and the NHVR to read and interpret reliable data, including crash data and who was in control of the vehicle at a point in time;

e. include human–machine interface requirements;

f. address vehicle modification and maintenance, including over-the-air software updates;

g. ensure safety redundancy;

h. include a mechanism to ensure offshore entities can be held legally responsible for their vehicles and systems;

i. be technology-neutral and consistent wherever possible with international developments, taking into consideration international testing results;

j. manage minor road rules breaches; and

k. be aligned with the "*National Road Safety Strategy 2011–2020"*.

10.1.2. The NTC task that commissioned this report was established to address these identified needs.

10.1.3. This report develops a *concept* of a Safety Assurance System that would be able to address all these requirements.

10.1.4. The SAS suggested is based around the concept that safety can be assured so long as three core elements of:

a. Vehicle Technical Integrity,

b. Operating Environment, and

c. Human Performance.

The SAS structure is based around a wo-stage process of:

d. **Initial safety assurance** – which involves establishing and finding compliance against a set of requirements established for a vehicle on a case-by-case basis; and

e. **Continuing Safety Assurance** – which involves controlling the configuration of the vehicle such that the safety findings that were made during the initial investigation remain valid.

10.1.5. The report suggests that the SAS concept developed can be implemented using three organisational entities:

a. Initial Safety Assurance entity (ISAe);

b. Automated Vehicle Entity (AVe); and

c. State Roadworthiness Authority.

10.1.6. **Initial Safety Assurance Entity (ISAe):** The ISAe is recommended to be a national body that manages the initial certification process for AVs. The certification process suggested is one designed around treating each AV or AV technology being proposed by an applicant on a case-by-case basis. The concept outlined is that a certification plan is developed for each application based around a Preliminary System Safety Assessment (PSSA). This ensures that certification is safety case centric. It is proposed that the ISAe would complete all compliance findings, including compliance against the existing ADRs. It is proposed that the ISAe will recommend to States that a given AV is suitable to be registered and hence granted access to the road network.

10.1.7. The report outlines four governance arrangements for the single, national ISAe entity and notes that because the ISAe is providing technical assessment services and advice to State registration authorities it does not need to be supported by any particular regulation or legislation.

10.1.8. **Automated Vehicle Entity (AVe):** The AVe is the organisation that conducts the continuous technical integrity tasks. Importantly the AVe becomes the legally responsible entity for then ongoing safety, performance and compliance of the AV.

10.1.9. It is recommended that the SAS supports a model where processes are established so any organisation can be approved to operate as the AVe for a given model or fleet of vehicles.

10.1.10. **State Roadworthiness Authority:** The third entity within the SAS is the State roadworthiness authorities who, based on recommendations from the ISAe will grant to, or remove, the AV the right to access the road network using the existing road-worthiness and registration processes.

10.1.11. This report concludes that if a Safety Assurance System or the form described was established that it would be able to meet the requirements identified by the stakeholders in the earlier consultation as well as a further group of requirements developed as an element of this task.

Appendix A: The Elements of a Regulatory Structure

It is not the role of this report to nominate a complete regulatory structure. The follow-on task, if it is to proceed, will develop the regulation set once guidance is provided on what direction is required.

This report includes a summary regulatory structure. This is done to:

- allow issues associated with the SAS approach, and the implications that has on the structure of the regulatory approach to be explored; and
- support the development of an estimate of the developmental task.

A generic regulatory structure has been created using the three pillars of the SAS proposed earlier in this report as a starting point. The structure is shown as Figure 7.

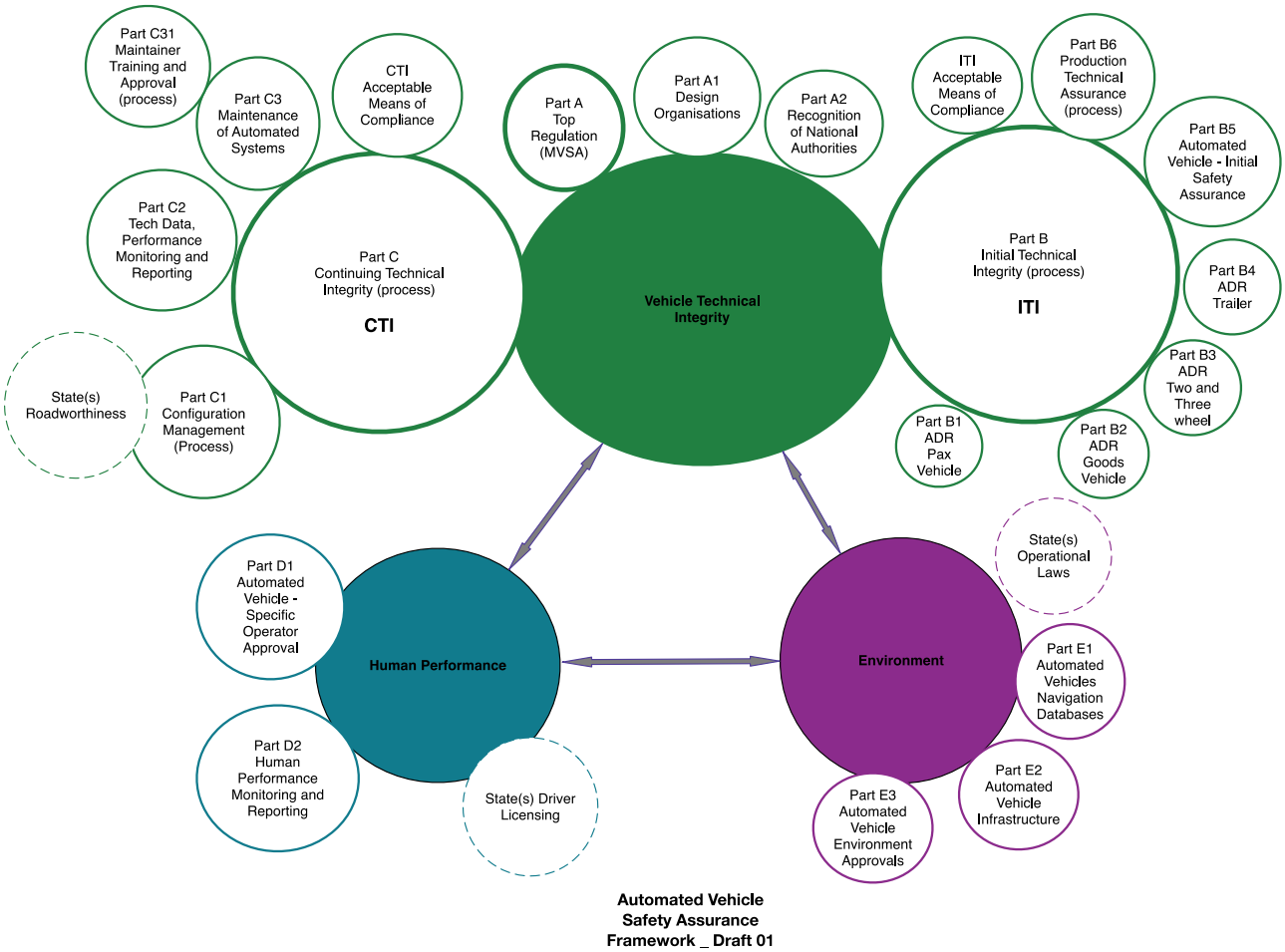


Figure 7: Generic Regulatory Structure

Part A – Top Regulation

This generic structure includes a top-level legislative instrument that would coordinate the whole SAS. This approach is in keeping with similar approaches adopted in Australia, such as the MVSA [7] and the Civil Aviation Standards Regulation (CASR) [26].

While this approach is possible it is not the only possible arrangement. The current holistic approach to motor vehicle safety assurance in Australia sees the Commonwealth Government provide a mechanism to create an assertion of initial technical integrity (the MVSA / ADR process). The States utilise this certification as the basis of granting, on a State-by-State basis, vehicle registration that includes both an assertion of 'roadworthiness' and an approval to use the road network.

It would be possible that without any change to the existing Commonwealth MVSA process or legislation that States could amend their registration legislation to require the input of both the existing ADR conformity and the output from a defined AV functionality SAS.

If an approach of this type was adopted what is annotated as the 'Part A top regulation' would not need to be a legislative instrument but rather a published process accepted by the States' Part A1 Design Organisations.

A process to authorise design organisations to make compliance findings is a common element of many SAS for complex technologies. The ability to authorise third parties or OEMs to certify certain products within a certain scope is an important way to reduce the time and cost associated with compliance finding.

The MVSA process already includes a process to 'approve design organisations'. (refer to Circular 0-13-1 Conformity of Production [15]). This is done within the wider coverage of the production conformity processes.

It is likely that if the ability to find compliance for the complex systems associated with AVs is going to be granted to third party or OEM design organisations then more complex processes than those in Circular 0-13-1 [15] will be required. It is thought that the design organisation approval process from the aerospace industry such as CASR 21J or EASA 21J would make reasonable tested models to start with.

As is the case with the 'top regulation' there is no need that this design organisation approval process must be commonwealth legislation.

Part A2 – Recognition of National Authorities

To meet the intent of the assessment criteria for the SAS to support international product assessment there must be a regulatory process that defines what attributes of a national regulatory process are important to ensure equivalence with the Australian SAS.

Part B1 through B4 – Use of Existing ADR

The SAS for AVs could include all the existing Australian Design Rules (ADRs). It is probable that new vehicles will need to show compliance against all existing ADRs, future non-automated ADRs and automated function requirements.

Given that 'self-certifying' (governance sampling) nature of the existing system, as outlined in Circular 0-1-2 [13], it is possible that the entity certifying the automated functions could also certify against the existing applicable ADRs.

While the use of the ADRs seems a reasonable way to ensure safety surrounding non-automated attributes in AVs, the way this is accomplished is not crucial so long as the:

- ADR system continues to be maintained by the Commonwealth;
- AV safety assurance process recognises the need for the ADRs; and

- State authorities receiving the SITI (an output from the initial safety assurance process) confirms against which ADRs compliance has been asserted.

It is also possible that an element of the initial safety assurance process for AVs may be the assessment of requests for exceptions from the ADRs.

Hence the ADRs are shown as an element of this draft structure as a reminder that the ADRs will remain a key set of requirements for AVs. Inclusion of consideration of the ADRs should not be considered as a suggestion of the manner in the way they should be included.

Part B5 – AV – Initial Safety Assurance

This will be the requirement to complete the process shown as the initial safety assurance in Figure 4. In terms of the regulatory structure this is a requirement to execute a process, and rules on who can execute the process.

Part B6 – Production Technical Assurance

This is included in the generic regulatory structure as a reminder that while the existing Vehicle Standard Circular 0-13-1 [15] addresses production conformity at the vehicle-level it is likely that for safety related AV functions the production conformity requirements:

- will need to be applied at the system vendor level;
- will need to be more detailed than a simple reference to generic requirements such as AS/NZS ISO 9001:2016 [27]; and
- may need to involve requirements for software and complex hardware CM.

ITI Acceptable Means of Compliance

The existing motor vehicle standards process includes several Administrators Circulars that contain a range of information about standards for the existing certification process. Some of these circulars would meet the intent of providing guidance on the Acceptable Means of Compliance (AMC).

The AV SAS is likely to rely heaving on advisory documents that outline AMC. If the AMC are advisory only in nature, that is, a suggested means of compliance rather than the only means of compliance then it is possible for them to be created quickly as an administrative process rather than a more complex regulatory or legislative process.

The use of AMC in the AV SAS is a key element of the ability of the system to meet the assessment criteria for technical innovation (Criteria 3), acceptance of international product assessment (Criteria 4) and low cost (Criteria 5).

The AMC also provide a convenient mechanism to share lessons learned on one project with the wider industry.

The SAS being described is an open process centric system that is designed to allow vehicle and system vendors to propose the system standards, design assurance standards and compliance finding methodology that they believe best suites their product. The AMC represents an important support to this process as they allow guidance to be provided to vendors regarding what approaches may or may not be acceptable.

Part C1 – Configuration Management

CM is seen a key element of the in-service safety assurance process. In previous sections the key tasks associated with CM have been noted as:

- monitoring ongoing serviceability and authorising maintenance,
- review and authorise incorporation of OEM modifications,
- review and authorise incorporation of third party modifications,
- system performance monitoring, and
- authorise use of navigation databases and authorise navigation data base updates.

It is proposed that the CM function be executed by a formally approved organisation referred to as the Automated Vehicle entity (AVe).

As the AVe role is critical to the continued safety of the AV functions the AVe holds a significant degree of legal liability. For this reason, the AVe will need to be operated by people determined to be competent, operating within a defined process and having access to all the data necessary to perform the defined role. The nature of the AVe role suggests that the AVe organisation and the key personnel within the AVe organisation will need to be licensed or approved in some manner.

The closest existing function to the AVe within the Australian motor vehicle context would be the State based 'licensed motor vehicle testers'. There is no reason why AVe organisations could not be authorised in a similar manner to licensed vehicle testers although given the technical and process complexity of the role it is likely to be more cost effective for a single Australian entity to approve and oversee each AVe. There is the possibility of a single national entity providing a recommendation to each State that a given organisation is suitable to perform AVe functions, allowing each State to then approve the organisation using simple existing licensed vehicle tester style legislative instruments.

Part C2 – Technical Performance Monitoring

Given the nature of the technologies being discussed and considering in many cases approvals to operate will be based on a safety analysis that includes assumptions, it is highly likely that in-service performance monitoring will be required to confirm that AV functions are achieving required performance outcomes.

In keeping with other aspects of the SAS it is proposed that the data requirements for any given system are assessed and defined on a case-by-case basis. The SAS should not mandate particular data or data gathering methodologies. Rather the system should suggest a process. It is conceivable that the process would require an in-service DMP to be approved, as an aspect of initial safety assurance process, then past to the AVe to execute.

This part therefore becomes a place-holder in the generic structure.

Part C3 – Maintenance of Automated Systems

For the technical integrity to be maintained across a vehicle's life it will be essential that maintenance is performed correctly, in accordance with approved data by appropriately qualified maintainers.

This part of the SAS will provide the guidance on how maintenance organisations should be organised and how they should be approved for AV support on a case-by-case basis.

As with other aspects of the in-service safety assurance it is possible that a single national entity could be involved in the approval and ongoing audit of maintenance organisations then recommend to State authorities that a given maintenance organisation is suitable to support particular AV functions.

Part D1 – AV Specific Operator Approvals

As was noted in the previous chapter it is envisaged that an output from the initial technical safety assurance process will be a HPS that will define what, if any, specialist training is required.

It is envisaged that the initial technical safety assurance process will review and approve required training material and a definition of required competencies.

Training organisations could be approved by either a national entity or individual States in accordance with procedures used to approve driver-training organisations.

Given that States already are responsible for licensing it is likely that regardless of the entity that completes the training there will still need to be a State regulatory process to authorise the driver / operator.

Part D2 – Human Performance Monitoring

Given the nature of the technologies being discussed and considering in many cases approvals to operate will be based on a safety analysis that includes assumptions regarding operator performance, it is highly likely that in-service performance monitoring will be required to confirm that AV functions are achieving required performance outcomes.

In keeping with other aspects of the SAS it is proposed that the data requirements for any given system are assessed and defined on a case-by-case basis. The SAS should not mandate particular data or data gathering methodologies. Rather the system should suggest a process. It is conceivable that the process would require an in-service DMP to be approved as an aspect of initial safety assurance process then past to the AVe to execute.

This part therefore becomes a place-holder in the generic structure.

Part E3 – AV Environmental Approvals

As was noted in the previous chapter it is envisaged that an output from the initial technical safety assurance process will be an SOE that will define what operational environment that the design has assumed.

Given that States manage their own networks they will need to be responsible for taking the data contained within the SOE and then providing authorisation for operation on specific roads or road styles. It is envisaged that in many AV functions this ‘road approval’ will need to be loaded into the vehicle navigation system. This is likely to be a further AVe function.

Part E2 – AV Infrastructure

Over time it is assumed that National and International standards for infrastructure to support the operation of AVs will be developed.

If the attributes of a particular infrastructure are an input to the AV safety assessment, then those infrastructure attributes will need to be certified.

This part is a place-holder for the process of infrastructure initial certification and in-service maintenance / management of the infrastructure.

Part E1 – AV Navigation Data Bases

If a navigation database is relied upon to perform a safety related automated function then that data base must be managed such that:

- the configuration of the database is defined at all times
- a process exists to update the database without compromising the existing data
- updates to the database are approved by an entity authorised to assess and approve the changes
- there is a process to capture and correct database errors.

This part is a placeholder to ensure data base CM is understood to be a key part of the AV SAS.

This generic regulatory structure is based on the three pillars of the SAS proposed earlier in this report, together with the ideas developed regarding initial and in-service safety assurance.

The structure is generic in the sense that it is suggesting that the particular set of regulations of administrative functions will be required, without assigning those functions to any particular legislative of administrative construct.

Appendix B: High Level Plan

The aim of the plan is the timely establishment of a national AV SAS in Australia.

The report and this plan are intended for presentation to TISOC in March and to Council in May 2017. Subject to the necessary approvals, they will then be released for public comment.

The plan outlines administrative detail necessary for the initiation of the project and informs the implementation of the preferred option.

The Project Team responsible for the delivery of these products are:

- Project Manager, James Williams (NTC, Manager Policy – Compliance & Technology);
- Design Team Lead, Jim Kira (Nova Systems, Program Manager – Transport);
- Senior Systems Safety Engineer, Mitchell Lennard (Nova Systems, Technical Lead);
- Senior Systems Engineer, Dean Boyd-Clark (Nova Systems, Project Support); and
- Safety and Certification Technical Advisor, Brett Martin (Nova Systems, Capability Manager – Safety & Certification).

The preferred option proposed by Nova is attractive for several reasons including that it requires only minor amendments to existing State legislative instruments which, as a minimal interim measure, will mitigate the risk of unfit technology in-service, will cost significantly less and will produce the least amount of additional regulation. The plan does not avoid the prospect of major regulatory reform; it anticipates that after three years of operation the planned 2022 organisational review will be well placed to make any required changes in a way that is both clear and decisive.

This high-level plan, based on the report, sets out a timeline that could see the first AV certified in Australia under a new SAS from November 2019.

The plan is consistent with the NTC regulatory framework reform program for AVs in Australia; that its execution is both timely and responsible, meeting the momentum of technology change in AVs with an evolved regulatory framework that affords continuous improvement in safety, security and environmental features and simultaneously accommodating further innovation and competition.

The plan has four phases – concept, planning, preparatory, implementation – and culminates with a 'go live' milestone in November 2019 and roll-out of National legislation empowering safety governance within a National AV Safety Assurance System. The following is a more detailed view of the phases together with aligned concurrent projects in a work breakdown structure (WBS) scheduled to span 2017, 2018 and 2019.

NTC Automated Vehicle Safety Assurance System Project, WBS and Master Schedule

- **Concept Phase – AV SAS**
  - Regulatory reforms for automated road vehicles – Determination on Recommendation 5
  - NTC Commission Nova report on AV safety management incl. a proposed AV SAS
  - Nova draft proposal on AV safety assurance incl. governance and safety criteria and high level plan
  - Targeted stakeholder engagement and feedback
  - Nova report on a National AV SAS

- TISOC, Brief for noting – Nova proposal for a National AV SAS
- Council, Brief for noting – Nova proposal for a National AV SAS
- Concept Phase – COMPLETE
- Austroads program on Registration and Licensing
- Council approval of R&L project outcomes
- R&L Project – COMPLETE

- **Planning Phase – AV SAS**
  - Full public consultation on Nova report
  - Draft detailed AV project plan with costing
  - Austroads Brief to TISOC – report on Registration and Licensing Project
  - Brief TISOC for noting – detailed plan for National AV SAS
  - Brief Council for noting – detailed plan for National AV SAS
  - Council approval of direction and cost model
  - Planning Phase – COMPLETE
- **NTC Driver Reforms Project**
  - Develop Driver Reforms Regulatory Impact Statement (RIS)
  - Driver Reforms RIS approved by Council
  - Driver Reforms RIS Phase – COMPLETE
- **Preparatory Phase – National AV SAS**
  - Stand up AV Project Office
  - Preparations to develop proposed AV governance processes incl. nominal independent AV entity
  - Draft report on proposed independent AV entity to run SAS in Australia
  - Brief TISOC for noting – update on proposed independent AV entity scope and authority
  - Brief Council for noting – update on proposed independent AV entity scope and authority
  - Develop final report development on independent AV entity
  - Brief TISOC – final report on AV entity to run SAS in Australia
  - Brief Council – final report on AV entity to run SAS in Australia
  - Council approval of direction and funding
  - Preparatory Phase – COMPLETE
- **Implementation Phase – National AV SAS**
  - Stand up AV entity
  - Draft AV entity standard operating administrative procedures
  - Writing detailed technical processes
    - Part A top regulation and sub-processes
      - A1 Design Organisations
      - A2 Recognition of National Authorities
    - Part B sub-processes

        - B1 - B4 Use of Existing ADR
        - B5 Automated Vehicle – Safety Assurance
        - B6 Production Technical Assurance
    - Part C sub-processes
        - C1 Configuration Management
        - C2 Technical Performance Monitoring
        - C3 Maintenance of Automated Systems
        - C31 Maintainer Training and Approval
    - Part D sub-processes
        - D1 Automated Vehicle Specific Operator Approvals
        - D2 Human Performance Monitoring
    - Part E sub-processes
        - E1 Automated Vehicle Navigation Data Bases
        - E2 Automated Vehicle Infrastructure
        - E3 Automated Vehicle Environmental Approvals
  - Targeted stakeholder engagement and feedback on consistency with States Driver Licensing
  - Targeted stakeholder engagement and feedback on consistency with States Roadworthiness
  - Draft AV amendments for legislation
  - Targeted stakeholder engagement and feedback on consistency with States Operational Laws
  - Brief TISOC on National AV SAS implementation
  - Brief Council on National AV SAS implementation
  - Implementation Phase – COMPLETE
- **Go Live: National AV Safety Assurance System**
  - Approval for SAS to go live
  - Institute AV amendments in legislation
  - Support States with any guidance on amendment of traffic laws
  - After 3 years of initial operations conduct organisational review of goals and effectiveness

Scope of the high-level plan

This initial planning for a national AV SAS, being at a high level, focusses on some typical planning elements while others will not be covered or covered only superficially. The necessary work and timeline to achieve it are reasonably evident once the available options have been reduced to a single preferred option. Assignment of work and other resources and the associated costs are not documented at this time in this plan. Similarly, the project risks that can be imagined need to be based on the framework which has been determined for them to have any actual value.

Risks – technical and administrative

The risks, like the costs discussed in the following paragraphs, morph with the scale of actions in the planned regulation reform. This risk profile associated with the actions can have a perverse effect in obscuring the risk profile of inaction in regulation. The reliance on Australian Consumer Law as a default arbiter of safety and

controlling influence in the engineering revolution that is faced by the automotive industry should be analysed in the context of some recent testimony to the U.S. Senate. At the U.S. Senate hearing on AVs in March 2016, Professor Mary Cummings articulated the tip of the hazard potential when stating that "inadequate certification basis established as evidence-based tests for AV has been relatively lacking". The 'tip' is a reference to the Iceberg Principle which serves well as a model for many risks in design, logistics and costs; that is, there is often unseen threats below the surface that are of greater bulk.

Compounding the challenge is another piece of evidence she presented to the U.S. Senate hearing, that "AV performance information developed has often met with Regulatory agencies whose roles suffer from insufficient staffing".

There is a need to better identify and assess the threats of inaction in proportion to those associated with proposed actions in the regulatory reform program and this is the purpose of the second phase of the NTC program culminating in a more detailed, and strategic, plan.

This is then taken further by the establishment of a project office within NTC, in the preparation phase, dedicated to mitigating risks and preparing for the likely, and less likely, contingencies of new as well as in-service modified AV configurations.

Master Schedule

A summary schedule is shown in the full page that follows capturing detail from the WBS, shown before, and illustrating the phases, key milestones and parallel activities in related projects.

Costs

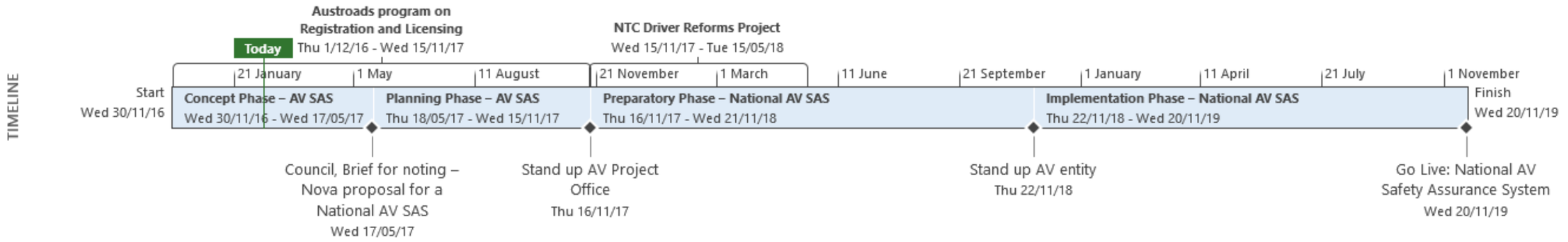
It is not possible to produce costing detail for the set up and sustainment of regulation functions applicable to AVs when the preferred option is yet to be down selected.

Even in instances where regulatory change had been announced with a chosen option there are still numerous examples, in Australia and overseas, of cost modelling being largely non-existent. All associated costs were basically absorbed by those falling under the new regulations in developing their compliance. For example, in Australia, the absence of cost modelling applied in the standing up of Director General Technical Airworthiness; similarly, Nova staff experienced the same in the UK in standing up the Military Aviation Authority following the Nimrod crash in 2007 – which was imbedded in 2010 with ~150 dedicated personnel – as well as the Defence Safety Authority (consolidating air, maritime, land, fire, environmental and nuclear authorities) in 2015 which was completed in just over a year.

Accordingly, Nova can provide budget factors not budget facts and there is no budgeting included at this time except in the drafting of technical processes in the *Implementation phase – Writing detailed technical processes*. For this suite of safety assurance processes, it is estimated that a staff of three specialists working full-time would require eight months to completion. This far range forecast is feasible based on the premise of a reasonably standard model of a modern safety assurance system ultimately being adopted.

It is estimated that 90% of the overall processes can be completed in this way as a standalone task within that eight-month period. These processes would form the bulk of the necessary technical instruments for the proper functioning and management of an AV-SAS in Australia. The residual 10% of processes involves tailoring of the final administrative arrangements for the AV entity.

Summary Schedule for Establishing an AV Safety Assurance System in Australia



GANTT CHART

	Task Name	Duration
1	**NTC Automated Vehicle Safety Assurance System Project, WBS and Master Schedule**	**776 days**
2	**Concept Phase – AV SAS**	**121 days**
11		
12	**Austroads program on Registration and Licensing**	**250 days**
15		
16	**Planning Phase – AV SAS**	**130 days**
24		
25	**NTC Driver Reforms Project**	**130 days**
29		
30	**Preparatory Phase – National AV SAS**	**265 days**
41		
42	**Implementation Phase – National AV SAS**	**260 days**
68		
69	**Go Live: National AV Safety Assurance System**	**0 days**

Appendix C: List of Stakeholders

Stakeholder	Attendees
Australian Government – Department of Infrastructure and Regional Development (DIRD)	• Donna Wieland • Andrew Hyles • Dr Andrew Dankers
Bosch	• Carl Liersch • Mounir Kiwan • Mark Jackman
Federal Chamber of Automotive Industries (FCAI)	• James Hurnall • Tony McDonald • Ashley Wells
Government of South Australia – Department of Planning and Infrastructure (DPTI)	• Phil Blake
Government of Western Australia – Main Roads Western Australia	• Kamal Weeratunga
Government of Western Australia – Department of Transport	• Simon Grieve • Fiona Tannock-Jones • Rebecca Poduti • Parik Lumb,
National Heavy Vehicle Regulator (NHVR)	• Daniel Elkins
National Transport Commission (NTC)	• James Williams • Marcus Burke • Natasha Bolsin • Geoff Allan
New South Wales Government – Transport for New South Wales (TfNSW)	• Cheryl Richey • Richard Fullalove • David Newman • David Wilson • Evan Walker • Dan Leavy • Dominique Win • Peter Boland • Claire Owens • Ralston Fernandes
New South Wales Government – Transport for New South Wales (TfNSW) – Centre for Road Safety	• Vanessa Vecovski
New South Wales Government – Roads and Maritime Services (NSW RMS)	• Norman Scheul • Andrew Mehaffey
Nova Systems	• Jim Kira • Dr Mitchell Lennard • Brett Martin • Dean Boyd-Clark
Queensland Government – Department of Transport and Main Roads (QLD TMR)	• Michael Skinner • Nicholas Mackay

Stakeholder	Attendees
RACV	• Brian Negus • Irene Christopher • Michael Case
VicRoads	• Stuart Ballingall • Chris Jones • Steven Huxtable
Volvo Australia	• David Pickett

Appendix D: Glossary

ABS	Automatic Braking System
ADR	Australian Design Rule
ADS	Automated Driving System
ALARP	As Low As Reasonable Practicable
AMC	Acceptable Means of Compliance
AMVS	Australian Motor Vehicle Standards
AV	Automated Vehicle
AVe	Automated Vehicle entity
CASA	Civil Aviation Safety Authority
CASR	Civil Aviation Safety Regulation
CM	Configuration Management
COAG	Council of Australian Governments
CP	Certification Plan
DDT	Dynamic Driving Task
DIRD	Department of Infrastructure and Regional Development
DMP	Data Monitoring Plan
DOT	United States Department of Transportation
DPTI	S.A. Department of Planning, Transport & infrastructure
EASA	European Aviation Safety Authority
FAA	Federal Aviation Authority
FAR	Federal Aviation Regulation
GNSS	Global Navigation Satellite System
HPS	Human Performance Statement
ISAe	Initial Safety Assurance entity
MVSA	Motor Vehicle Standards Act
NHTSA	United States National Highway Traffic Safety Authority
NSW	New South Wales
NTC	National Transport Commission
ODD	Operational Design Domain
OEM	Original Equipment Manufacturer
ONRSR	Office of the National Rail Safety Regulator
ORS	Operational Rules Statement
PSSA	Preliminary System Safety Assessment
QLD	Queensland
RMS	Roads and Maritime Services
RVCS	Road Vehicle Certification System
SAS	Safety Assurance System
SFAIRP	So Far As Is Reasonably Practicable
SOE	Statement of Operational Environment
SITI	Statement of Initial Technical Integrity
SMS	Safety Management System
TISOC	Transport and Infrastructure Senior Officials' Committee
TfNSW	Transport for New South Wales
TMR	Queensland Department of Transport and Main Roads
UAS	Unmanned Aerial System
UNECE	United Nations Economic Commission for Europe
US	United States of America
VASS	Vehicle Assessment Signatory Scheme
VSSB	Vehicle Standards Safety Branch
WA	Western Australia
WHS	Work, Health and Safety

Appendix E: Definitions

Term	Definition
As Low As Reasonably Practicable (ALARP)	For a safety risk to be ALARP it shall be possible to demonstrate that the cost involved in reducing the risk further would be grossly disproportionate to the benefit gained. For a risk to be accepted it shall be demonstrated to have been reduced to a level ALARP and shall be tolerable.
Assurance	A positive declaration intended to give confidence. In engineering References, it is the evidence that planned outcomes have been achieved, or the evidence of effective management of risk.
Automated Driving System (ADS) *SAE J3016J definition*	The hardware and software that are collectively capable of performing the entire DDT on a sustained basis, regardless of whether it is limited to a specific operational design domain (ODD); this term is used specifically to describe a level 3, 4, or 5 driving automation system.
Dynamic Driving Task (DDT) *SEA J3016 definition*	All of the real-time operational and tactical functions required to operate a vehicle in on-road traffic, excluding the strategic functions such as trip scheduling and selection of destinations and waypoints, and including without limitation: 1. Lateral vehicle motion control via steering (operational); 2. Longitudinal vehicle motion control via acceleration and deceleration (operational); 3. Monitoring the driving environment via object and event detection, recognition, classification, and response preparation (operational and tactical) 4. Object and event response execution (operational and tactical); 5. Manoeuver planning (tactical); and 6. Enhancing conspicuity via lighting, signalling and gesturing, etc. (tactical).
Operational Design Domain *SAE J3016 definition*	The specific conditions under which a given driving automation system or feature thereof is designed to function, including, but not limited to, driving modes. NOTE 1: An ODD may include geographic, roadway, environmental, traffic, speed, and/or temporal limitations. A given ADS may be designed to operate, for example, only within a geographically-defined military base, only under 25 mph, and/or only in daylight. NOTE 2: An ODD may include one or more driving modes. For example, a given ADS may be designed to operate a vehicle only on fully access-controlled freeways and in low-speed traffic, high-speed traffic, or in both of these driving modes. NOTE 3: In the previous version of this document, the term driving mode was used more extensively. In this updated version, ODD is the preferred term for many of these uses. NOTE 4: Section 6 discusses the significance of ODDs in the context of the levels of driving automation.

Term	Definition
Safety Assurance	A subset of Systems Assurance, the primary role of which is to demonstrate that all safety risks arising during or across any or all segments of the life cycle (design, construction, commissioning, operation, maintenance, decommissioning and disposal) of an asset have been identified, assessed and mitigated. The safety assurance process involves six stages and may include any or all of the following stages as appropriate: 1. Determining generic "Project Safety Management" requirements. 2. Reliability, Availability, Maintainability and Safety (RAMS). 3. Engineering Safety. 4. Governance. 5. Development of a Safety Assurance Report (or equivalent). 6. Independent validation[1]
Safety Management System	All plans and actions taken to identify hazards; assess and mitigate associated risks; and track, control, accept, and document risks encountered in the design, development, test, acquisition, use, and disposal of systems, subsystems, equipment, and infrastructure.
So Far As Is Reasonably Practicable (SFAIRP)	To achieve the best possible safety outcomes, to the extent that is 'reasonably practicable'.[2]
Systems Assurance	A positive declaration intended to give confidence. In engineering references, it is the evidence that planned outcomes have been achieved, or the evidence of effective management of risk The structured and systematic approach to ensuring the requirements related to reliability, availability, maintainability and safety are satisfied.
Systems Engineering	Systems engineering (SE) is an inter-disciplinary collaborative engineering methodology to derive, evolve and verify a successful transport system solution that satisfies stakeholders' requirements. It is an iterative problem-solving process, based on the cycle of analyse, synthesise, and evaluate. SE encompasses individual subsystems and their interactions to form an integrated system to meet stakeholder requirements.
Work, Health and Safety (WHS)	A generic term to cover all activities related to designers' and manufacturers' responsibilities in relation to the various WHS Acts. The WHS Acts provide a framework to protect the health, safety and welfare of all workers at work. They also protect the health, safety and welfare of all other people who might be affected by the work. All workers are protected by the applicable WHS Act, including employees and customers.

[1] TFNSW, *Safety Management System Overview*, http://www.transport.nsw.gov.au/sites/default/files/b2b/projects/tfnsw-safety-management-system-overview.pdf, p.9
[2] SFAIRP refers to the legal duty to manage safety whereas ALARP refers to the management of safety risk to the lowest reasonably practicable level.

Appendix F: SAE Levels of Driving Automation

SAE's levels of driving automation, as described in SAE J3016:2016, are descriptive and informative, rather than normative, and technical rather than legal. Elements indicate minimum rather than maximum capabilities for each level. In this table, "system" refers to the driving automation system or Automated Driving System (ADS), as appropriate.

Level	Name	Narrative Definition	DDT		DDT Fallback	ODD
			Sustained lateral and longitudinal vehicle motion control	OEDR		
Driver performs part or all of the *DDT*						
0	No Driving Automation	The performance by the *driver* of the entire *DDT*, even when enhanced by *active safety systems*.	*Driver*	*Driver*	*Driver*	n/a
1	Driver Assistance	The *sustained* and *ODD*-specific execution by a *driving automation system* of either the *lateral* or the *longitudinal vehicle motion control* subtask of the DDT (but not both simultaneously) with the expectation that the *driver* performs the remainder of the *DDT*.	*Driver* and *System*	*Driver*	*Driver*	Limited
2	Partial Driving Automation	The *sustained* and *ODD*-specific execution by a *driving automation system* of both the *lateral* and *longitudinal vehicle motion control* subtasks of the *DDT* with the expectation that the *driver* completes the *OEDR* subtask and *supervises* the *driving automation system*.	*System*	*Driver*	*Driver*	Limited
ADS ("*System*") performs the entire *DDT* (while engaged)			*System*	*System*	*Fallback-ready user (becomes the driver during fallback)*	Limited
3	Conditional Driving Automation	The *sustained* and *ODD*-specific performance by an *ADS* of the entire DDT with the expectation that the *DDT fallback-ready user* is *receptive* to *ADS*-issued *requests to intervene*, as well as to *DDT performance-relevant system failures* in other *vehicle* systems, and will respond appropriately.				
4	High Driving Automation	The *sustained* and *ODD*-specific performance by an *ADS* of the entire *DDT* and *DDT fallback* without any expectation that a *user* will respond to a *request to intervene*.	*System*	*System*	*System*	Limited
5	Full Driving Automation	The *sustained* and unconditional (i.e., not *ODD*-specific) performance by an *ADS* of the entire *DDT* and *DDT fallback* without any expectation that a *user* will respond to a *request to intervene*.	*System*	*System*	*System*	Unlimited

Appendix G: References

1. National Transport Commission, 'Regulatory barriers to more automated road and rail vehicles', ISBN 978-1-921604-85-0, February 2106
2. National Transport Commission, 'Regulatory options for automated vehicles', ISBN 978-1-921604-94-2, May 2016
3. National Transport Commission, 'Regulatory reforms for automated vehicles', ISBN 978-0-9946335-4-5, November 2016
4. SAE J3016, 'Taxonomy and Definitions for Terms Related to Driving Automated Systems for On-Road Motor Vehicles', September 2016
5. G. Rechnitzer, N. Haworth, N. Kowadlo 'The Effect of Vehicle Roadworthiness on Crash Incidence and Severity', Monash University, July 2000, ISBN 0 7326 1463 5
6. Australian Transport Council 2011, 'National Road Safety Strategy 2011-2020'
7. Department of Infrastructure and Regional Development 1989 – Motor Vehicle Standards Act 1989 – Australian Design Rules
8. The US Department of Transport – National Highway Traffic Safety Administration, 'Federal Automated Vehicles Policy – Accelerating the Next Revolution in Road Safety' September 2016
9. Commonwealth of Australia, Competition and Consumer Act 2010
10. Commonwealth of Australia, Privacy Act 1988
11. Commonwealth of Australia, Work Health and Safety Act 2011
12. SAE J2399, 'Adaptive Cruise Control (Acc) Operating Characteristics and User Interface', September 2016
13. Department of Infrastructure and Regional Development, Administrator of Vehicle Standards, Circular 0-1-2 'A Guide to the Certification of New Vehicles – Type Approval', August 2015
14. (82nd GRRF 2016) – UNCE Working Party 29 GRRF Secretariat, informal document GRRF-82-12-Rev 3, 20-23 September 2013
15. Department of Infrastructure and Regional Development, Administrator of Vehicle Standards, Circular 0-13-1 'Conformity of Production', 2015
16. VicRoads Vehicle Standards Information (26), 'Roadworthiness Requirements', December 2012
17. www.Volvocars.com – Automated Driving, accessed January 2017
18. SAE J2980, 'SAE Surface Vehicle Recommended Practice—Considerations for ISO 26262 ASIL Hazard Classification', May 2015
19. US Federal Aviation Regulation Part 25.1329, US Department of Transport
20. US Department of Transport, Federal Aviation Administration, Advisory Circular 25.1329, 'Approval of Flight Guidance Systems',
21. D. L. Parnas, A.J. van Schouwen, S. P. Kwan, 'Evaluation of Safety Critical Software', Communication of the ACM, Volume 33 Number 6 June 1990
22. Department of Infrastructure and Regional Development, Australian Motor Vehicle Certification Board – Administrator of Vehicle Standards, Circular 38-1-8 'Approval for Computer Simulation of ADR 38 Service Brake Effectiveness', September 2015
23. M. Maurer, J. Christian Gerdes, B. Lenz, H. Winner, 'Autonomous Driving – Technical, Legal and Social Aspects', Springer Open, ISBN 978-3-662-48847-8 (eBook), 2016
24. Australian Government, 'International Standards and Risk Assessment', Cutting Red Tape at website www.cuttingredtape.gov.au
25. Department of Industry, Innovation and Science 'Industry Growth Centres – Initiative Summary' at website www.industry.gov.au
26. Civil Aviation Safety Regulations 1998 at website www.legislation.gov.au/Details/F2017C00095
27. AS/NZS ISO 9001:2016, 'Quality Management Systems—Requirements', SAI Global at website https://infostore.saiglobal.com/preview/as/as9000/9000/9001-2016.pdf?sku=1845270
28. ISO 26262:2011, 'Road Vehicles – Functional Safety' at website www.infostore.saiglobal.com/en-au/Standards/ISO-26262-1-2011-1499990/
29. Australian Government, Department of Infrastructure and Regional Development, Federal Interstate Registration Scheme at website www.infrastructure.gov.au/roads/motor/firs/