Nova Systems

Melbourne Office
Level 2, 95 Coventry Street
South Melbourne, VIC 3205

Telephone: +61 3 9024 1851

Email: transport@novasystems.com
Web: www.novasystems.com

Nova Systems
Experience Knowledge Independence

Attn: Automated Vehicle Team
National Transport Commission
Level 15, 628 Bourke Street
Melbourne VIC 3000
Australia

9 July 2018

Dear Sir / Madam,

SAFETY ASSURANCE FOR AUTOMATED DRIVING SYSTEMS CONSULTATION REGULATORY IMPACT STATEMENT

On behalf of Nova Systems, I thank you for the opportunity to comment on this Regulatory Impact Statement (RIS).

In terms of regulatory options for automated vehicles, Nova Systems commends the NTC for the comprehensive and well researched consultation RIS. Nova generally endorses the recommendation for Option 4 Safety Assurance System, including a Primary Safety Duty. As well as answering the RIS consultation questions - comments, suggestions for improved clarity and additional references are offered to support substantiation and focus and further RIS development.

Nova Systems is a professional services provider established in 2000 by a former Royal Australian Air Force (RAAF) Test Pilot and a former Flight Test Engineer as a Test & Evaluation (T&E) specialist organisation for aerospace capabilities (i.e. military aircraft, aviation technologies and weapon systems). Today Nova Systems is the largest and pre-eminent test and trials organisation in the southern hemisphere, providing a whole range of systems-engineering services throughout a number of industries including Defence, Energy, Resources, Utilities, Civil Aviation, Satellite Communications and Transport.

Nova Systems has spent 15 years working within high-risk environments, dynamic regulatory frameworks and emerging technology domains. Nova Systems' comprehensive experience acquired across aerospace (aviation & space) and defence has been leveraged into commercial technology adoption programs, including several projects involving the introduction of automated vehicle systems, most notably, the BHP Billiton Autonomous Haul Production Trial (AHPT) program. Nova Systems is at the forefront of introducing unmanned systems into the Australian Defence Force and is a leading member of various Civil Aviation Safety Authority (CASA) Unmanned Aerial Systems (UAS) advisory panels. Nova Systems is also a current key contributor to the Singapore Standards Development Organisation for introduction of Level 4 and 5 AVs for land transport, in the area of safety.

The challenges and complexities faced by the aerospace sector (especially UASs) have many similarities to those that are currently being faced by the transport sector with respect to autonomous vehicles and Cooperative Intelligent Transportation Systems (C-ITS). As such, Nova Systems believes it has a wealth of knowledge and experience that could add value to the transport sector in general and the development and introduction of autonomous vehicle systems in particular.

Nova Systems' value proposition is its unique capability to provide independent, whole-of-systems T&E services that are necessary to verify that the new technology/capability satisfies design, legal, operation and safety regulations and standards (systems and safety assurance) and validates that the new technology/capability achieves the pre-defined functional and performance specifications, and

satisfies the user needs and operational concept. Thus, certifying that the technology is fit for purpose and safe to operate for a particular Operating Design Domain (ODD).

Additionally, Nova Systems can work with manufacturers, customers and other stakeholders early in a project life-cycle to assist with capability definition, operation concept definition, requirements capture etc. Otherwise, Nova Systems can provide third party governance and project management capabilities during the acquisition and delivery phase of the project and on-going logistics and asset management services.

Nova Systems' independence means that we are solutions agnostic, therefore we do not promote a particular manufacture's technology or capability. Our mission is to enable next generation transport systems through independent integration of intelligent, safe and effective solutions and through systemised approaches to innovation.

Further commentary around the specific questions posed by the NTC is enclosed.

Should you wish to discuss any aspect of this submission, require clarification of any matter raised, or would like Nova Systems to provide assistance in any capacity, feel free to contact me via the details identified below.

Sincerely,

JAMES KIRA
Nova Systems
Program Manager - Transport

T: (02) 9043 2512
M: 0409 690 329
E: jim.kira@novasystems.com

Enclosures:

1. Nova Systems' Response to the Safety Assurance for Automated Driving Systems Consultation Regulatory Impact Statement – May 2018

Nova Systems' Response to the Safety Assurance for Automated Driving Systems Consultation Regulatory Impact Statement – May 2018

1 GENERAL COMMENTS ON THE RIS

Other local examples of changing the regulatory framework

For years it was acknowledged that the aviation industry was over-regulated and the aviation regulations were very prescriptive, especially in Australia. This lead to a very safe system, but it was very expensive to maintain and didn't allow innovative approaches to safety. However, in recent years both the civil and defence aviation regulatory systems have been revamped using outcomes-based regulations based on International Civil Aviation Organization (ICAO) principles. There is a lot to be learned from this process. When assessing a vast array of alternate regulatory systems, the Australian Defence Aviation Safety Authority (DASA) used tools such as the one shown in Figure 1 below. This model assesses Product, Behavioural and Process integrity across the Design, Production and Maintenance domains to ensure that the Defence Aviation Safety Regulations (DASRs) ensured aircraft remained safe.

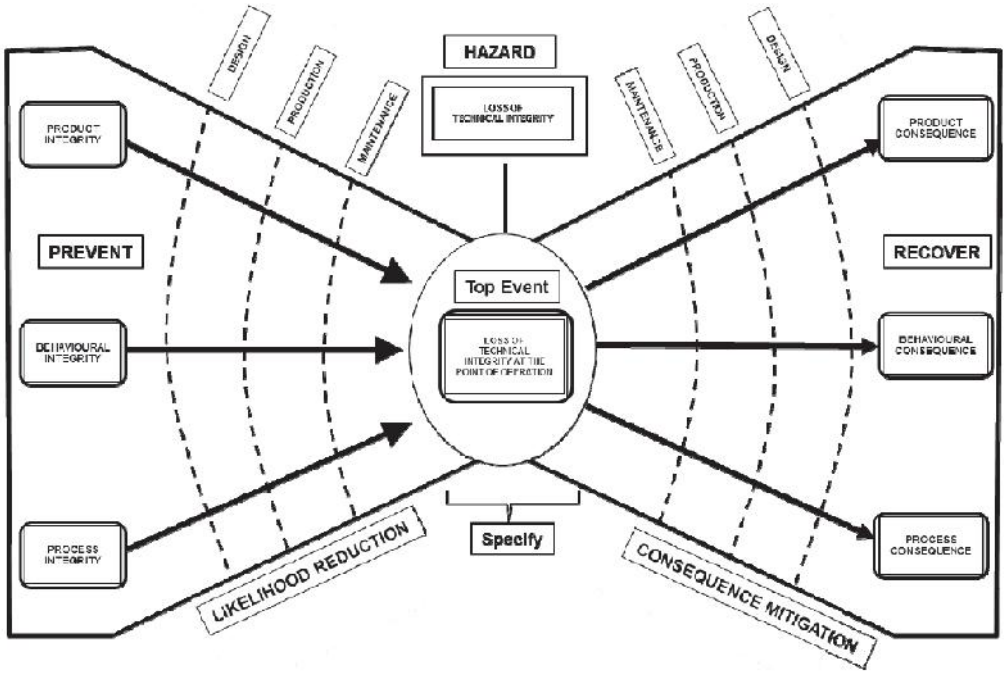


Figure 2. A composition of the bow-tie methodology overlapped with the technical integrity definition and technical item lifecycle, this framework is given the title the Product-Behaviour-Process (PBP) Bow-Tie. Importantly, this research is focused on preventative barriers of the PBP Bow-Tie (the lead up to the top event, shown on the left-hand side of the illustration).

Figure 1 – The Product-Behaviour-Process (PBP) Bow-Tie for Regulation Comparison
(Purton et al., 2016)[1]

This figure outlines the Likelihood barriers (layers of protection) within the Product, Behaviour and Process streams that are required to ensure technical integrity. The Regulatory Impact Statement

[1] PURTON, L., CLOTHIER, R., KOUROUSIS, K. & MASSEY, K. 2016. The PBP Bow-Tie framework for the systematic representation and comparison of military aviation regulatory frameworks. The Aeronautical Journal

(RIS) doesn't cover the aspects of Product, Behaviour or Process in great detail. However, these can be addressed in detail if either of the 'Legislative' options are selected.

Primary Safety Duty - expectations

The RIS doesn't provide a detailed definition of 'Primary Safety Duty' or the associated duties and responsibilities. Does it include all aspects of a Safety Management System (SMS)? As an example, the DASR guidance on SMSs is modelled on a civil aviation SMS and is outlined below:

- **Management Commitment and Responsibility**. Establish the safety policy and objectives.
- Safety Accountabilities:
    a. Define safety management responsibilities and accountabilities across relevant departments of the organisation.
    b. Establish an SMS/safety coordination mechanism/committees.
    c. Establish departmental/ divisional Safety Action Groups where applicable.
- **Emergency Response Planning**. Develop an Emergency Response Plan (ERP).
- **SMS Documentation**. Initiate progressive development of SMS documentation and other supporting documentation.
- **Hazard Identification**. Establish a voluntary hazard reporting procedure.
- **Safety Risk Management**. Establish safety risk management procedures.
- **Safety Performance Monitoring**. Establish occurrence reporting and investigation procedures.

(Defence Aviation Safety Authority, 2018)

Oversight

How do you 'assure' the government and the public that the vehicles are designed, produced and maintained:

- to appropriate standards;
- using appropriate procedures; and
- by qualified, competent personnel who follow the standards and procedures.

A key part of a regulatory system and cost of implementation is understanding the level of oversight that should be provided by authorities, based on an understand of risks, sources and exposure. The well recognised 'Swiss-Cheese' model proposed by Professor James Reason (1997)[2], to represent separation of threats by imperfect control barriers in organisational accidents, has long been a touch stone of regulatory frameworks in a variety of industries. Identifying and understanding the control barriers (slices) and their integrity (size of the holes) is fundamental.

[2] Reason, J. (1997) *Managing the Risk of Organizational Accidents*. Aldershot: Ashgate.

The options – first impressions

Option 1. Option 1 appears extremely unlikely to satisfy the goals outlined in the RIS. There appears to be a lot of potential for misunderstanding and subsequent misinterpretation by consumers, Automated Driving System Entities (ADSEs), registration bodies, law enforcement and litigators.

Option 2. As with Option 1, Option 2 does not have clear laws for consumers, ADSEs, registration bodies, law enforcement and litigators.

Option 3. Option 3 appears much clearer on responsibilities and would therefore make a good, minimum option for consideration. Option 3 would require effort to research and instate the appropriate laws but would be well worth the clarity. Even though Option 3 is a far more consistent basis for safe operation of Autonomous Vehicles (AVs), it doesn't yet provide much clarity on the level of regulatory interaction and oversight. The RIS has articulated the options and costs in Sections 3, 6.4 and 6.5 well, with good initial detail. However, details on the scope and powers of a Regulatory Agency are minimal; which could be broad ranging and is likely to contain the main cost drivers.

Option 4. Option 4 appears to be the safest option and Nova Systems agree with the NTCs preference for Option 4. It appears to have more clarity on expectations and responsibilities. It offers greater safety outcomes but is likely to be the most expensive to set up. Therefore, it will be imperative to assess, monitor and maintain the business case for AV introduction in terms human and financial savings, if this option is introduced. However, as with Option 3, this option does not provide much clarity on the level of regulation and oversight implied by the Primary Safety Duty.

The meaning of 'Primary Safety Duty'?

To determine the bounds of requirements covered by 'Primary Safety Duty' the investigating body should consult with other relevant Safety Agencies and/or other countries. Other industry regulators with comparable duties could include:

- Civil Aviation Safety Authority (CASA) / DASA – relatively recently reshaped to adopt international regulatory model from Europe (EASA);
- Office of the National Rail Safety Regulator (ONRSR) – relatively recently formed as a standardisation body between states following harmonised laws and informed by Europe/UK regulatory models; and
- Safework Australia – relatively recently boosted in influence by the Work, Health and Safety (WHS) Act 2012.

Mind Map of AV Safety Factors

In the process of developing this submission, Nova Systems produced an AV Safety Factors 'Mind Map'. This was produced as a quick tool to help determine if there were any gaps in the RIS proposal. This 'Mind Map' is provided in Annex A for information and can be used by the NTC if it is found to assist the arguments outlined in the NTC RIS.

2 ANSWERING THE SPECIFIC RIS QUESTIONS

RIS Question 1. To what extent has the consultation RIS fully and accurately described the problem to be addressed? Please provide detailed reasoning for your answer.

The three key issues noted in paragraph 2.1 of the RIS capture the community level risk issues associated with the introduction of Automated Driving Systems (ADS). The first point 'ADS may fail to deliver reasonable safety outcomes' would be improved by changing 'reasonable' to 'necessary'. The introduction of ADS technologies will come with an associated financial cost to the community and it is necessary for all of those costs (including externalities and, specifically in the case of this RIS, the System Safety Assessment process cost) to be balanced against a suitable increase in safety (and hence balancing cost reduction). 'Reasonable' is a qualitative descriptor usually associated with safety policy for 'reasonably practicable risk control'. Safety outcomes are measured in quantitative terms and targets, so 'necessary' or 'measurable' is better.

Section 2.2.2. Case Studies. The Section 2.2.2 case studies would benefit from stating the problem first, and then using the case study to relate the problem to a real scenario. If only a scenario is provided, without the correct context, then the reader can be easily convinced that by addressing the cause of that incident, the ADS is now safe. This may not be the case. Section 2.2.2 would be improved by asserting the safety risks in a more direct manner. The technologies used in ADS are not necessarily built to an industry code or standard – they can and will fail in specific circumstances. From a safety system engineering perspective, technical failure will result in loss of function that may or may not result in an unacceptable safety risk. The acceptability will depend on the barriers (e.g. redundant systems that stop the accident/incident occurring) and mitigators (e.g. Emergency braking, ABS, airbags etc.) inherent in the ADS/vehicle design. Technical failure in the ADS system technologies derive from the following general areas:

- High-level system design errors and requirements errors (including design assumptions);
- In-service configuration, role or environment does not match design assumptions;
- Hardware failures (sensors, effectors and processing elements);
- Software and complex hardware design errors; and
- Software execution errors and real time operating system failures.

The use of these case studies can be improved by redescribing the 'Design Risk' heading and outlining the risk as follows:

- Design Risk: Importation / Manufacturing becomes….. Risk: Limited / No objective evidence that the ADS design meets agreed safety criteria.
- Design Risk: Modification / Roadworthiness becomes….. Risk: ADS design does not meet users operating assumptions of operating environment.
- Organisational Risk: Modification / Roadworthiness becomes….. Risk: ADS safety is not assured during ongoing operation.
- Organisational Risk: Modification / Roadworthiness becomes….. Risk: ADS safety is compromised by poor maintenance practices or base vehicle configuration change.
- Operational / Use Risk: On-road operation becomes….. Risk: ADS design or configuration not compatible with operation environment and road regulations.

- Organisation Risk: Vehicle disposal/end of life becomes…..Risk: ADS does not have sufficient through life support.

There are also additional regulatory risks that have not been identified:

- The AV or ADS operational approval is provided based on assertions and substantiation by the ADSE. If the approval authority is not adequately skilled or the novel technologies are not independently certified, then there is a risk that an unsafe system could be approved for use beyond its capabilities.

- There is also a risk that the country of manufacture provides certifications of safety for the ADS design that is either not suitable for the Australian Operating Design Domain (ODD) or is not provided by a competent agency.

RIS Question 2. What other factors should be considered in the problem statement?

A further issue is the risk that ADS accidents involving death and significant injury may result in an increase in litigation cases which will increase community costs and will leave an indeterminate environment for ADS suppliers, since each new court ruling may change the requirements that suppliers have to address. If an effective Safety Assurance System is deployed, then this risk will be controlled by reducing exposure to deficient products and having a ready and robust evidence base for investigations and defences.

Other areas that could have been addressed in the RIS include:

- The key risk that the slow uptake of AVs will result in a continued 'High' road toll and the associated human, social and economic costs.

- Risk that government is not seen to have done all that is 'reasonably practicable' and therefore hasn't complied with its own WHS legislation.

- During the period of initial uptake, societal adjustments and industry and regulator immaturity – unanticipated behaviours may arise in interaction of the AV drivers and their technology, other traditional road vehicle users and pedestrians or cyclists on roads. Responses may include counter intuitive use cases not considered in design, malicious behaviour and mischievous 'bullying' of collision avoidance safety systems. Public acceptance and behaviour education programs as well as additional offences may need to be considered for interfering with safety systems.

- **Delayed Safety Assurance**. Insurance and legal liabilities are not effective mechanisms to assure safety to a 'socially acceptable level'. They are second order controls that rely on an incident/accident occurring, the ADSE being found guilty and liable, and the financial punishment being influential enough to change behaviours. The resulting safety outcome would not be realised until years after the hazard was first identified; possibly after dozens more incidents. There is no certainty for the community that the financial/punitive drivers associated with insurance or legal liability will be large enough to drive ADSEs to suitable safety outcomes. This is a risk success of market uptake and an argument for Option 4 and pro-active Safety Assurance.

- **Obtaining Public Buy-in**. An important follow-on program, once the regulations are in place, is selling the importance of 'Why AVs have their own regulations', and the benefits of AV regulation. This will ensure that the interest and uptake of AVs remains high, ensuring the social, community and economic benefits are realised. A number of studies and public commentaries have addressed this thinking. (see recent piece and supporting study at https://theconversation.com/driverless-cars-really-do-have-health-and-safety-benefits-if-only-people-knew-99370.

RIS Question 3. Has the consultation RIS provided sufficient evidence to support the case for government intervention? What else should be considered and why?

The case for government intervention is sufficiently covered by the existing NTC process as described by "Regulatory options to assure automated vehicle safety in Australia and the supporting submissions. The Nova Systems submission for the Safety Assurance Systems options was as developed by (Dr Lennard Mitchell Nova, 2017).

Perhaps greater evident comparisons to other regulated industries/sectors in Australia such as Rail, Heavy Vehicle and the Aviation industry, could be used to bolster the case for government intervention. Autonomous vehicles may have their greatest uptake as means of public transport or mobility enablers. In this respect the regulatory oversight should be commensurate with established approaches to those sectors where the risks dictate.

Other tools could also be used to explore the problem and substantiate analysis, such as the PBP Bow Tie outlined in Section 1, LOT Journey Maps for each option, or a SWOT Analysis for each option.

RIS Question 4. To what extent have the community and industry expectations of a regulatory response been accurately covered?

It is Nova Systems' view that the stakeholder engagement and consolation conducted to date by the overall process is sufficient to capture community and industry expectation and no further work is specifically required in the RIS. Volume's of current media coverage and academic studies indicate community sentiment, especially when an incident occurs. International comparisons and benchmarking have been addressed accurately. The RIS could provide a summary of previous work in the introduction and in section 2.5, thereby making it clearer that the case for intervention is not being re-addressed in the RIS, as it is covered by earlier work.

RIS Question 5. Are the four options clearly described? If not, please elaborate.

It is Nova Systems' view that Options 3 and 4 could be better described. Option 3 as presently described in 3.4.2, includes in-service safety management, which is supported.

Option 4 adds a further 'primary safety duty' which is characterised as an overarching 'catch all' requirement to ensure the identification of likely hazards and the mitigation of non-eliminated risks So Far As Is Reasonable Practicable (SFAIRP). This approach is understood and supported.

In section 3.5.3 'How it would work' it is suggested that the primary safety duty be 'triggered by and incident or near miss'. This description is considered insufficient and potentially misleading as it suggests that the primary safety duty is specific to the in-service aspects of the Safety Assurance System (SAS). It is thought that the primary safety duty concept as outlined in 3.5.1 and 3.5.2 is equally applicable to design (introduction to service) initial safety assessment as it is to in-service (continuing) safety. It is also considered beneficial to consider that the primary safety duty should aim to be pro-active as well: including 'Hazard Identification' and 'Safety Performance Monitoring', through defect and problem report investigation to pre-empt potential design Safety incidences.

It is recommended that the Option 3 and Option 4 descriptions be amended to make it clear that:

- both Option 3 and Option 4 address both initial safety and the in-service safety assurance phases;
- the additional primary safety duty concept introduced by Option 4 is to be applied in both the initial safety and the in-service safety assurance phases; and
- Option 4 includes pre-emptive safety measures, such as Hazard Identification in design.

As outlined in Section 1 of this response, this approach is fundamental to an aviation SMS. Further is implicit to SMS expectations under the WHS Act 2012.

RIS Question 6. Are the proposed safety criteria and obligations on ADSEs (detailed in chapter 4 and Appendix C) sufficient, appropriate and proportionate to manage the safety risk?

The principals-based safety criteria approach and detail is thought to be acceptable in general with the following detailed comments:

- **4.3.1.** Would recommend the wording be amended to 'why it chooses a particular design basis, design assurance philosophy and design compliance processes'. This is more in keeping with Systems Engineering language that is the basis of modern complex automotive design. As is 'Verification and Validation (or V&V)' vice "test and validation" as has been used by NTC in reports. It is noted that throughout the RIS there is continuing reference to 'test' as a crucial methodology. While testing is a necessary element of the design process - it is only one verification method alongside analysis, inspection, modelling and simulation. Further, test is unlikely to play a major role in the overall safety assurance processes of the designers in accordance with industry standards for functional safety such as ISO 26262. Thus, it is important not to over emphasise the role of testing, as this may be misleading to suppliers and approval agencies. The nature of software based technologies, and especially artificial intelligence and machine learning concepts, is that it cannot be exhaustively verified for every combination of scenarios and variables likely to be encountered in service. Instead, testing is supplemented by process quality practices and oversight, logical analysis and proofs of safety critical functions and architectural separation of non safety critical processes etc.
- This section should note that the applicant will need to demonstrate following a system safety engineering process (or Functional Safety and Safety of the Intended Functionality as now used in automotive electrical/electronic systems) in accordance with an applicant nominated, known industry standard, safety assurance process.
- The NTC may also consider how these criteria fulfil the structure of a 'Safety Case' basis for technical and operational approval of a new type approval or safety significant design change. This goal based concept and terminology is more prominent in the UK and European rail and industrial sectors, and not in the US (NHTSA) other than instances in the Oil and Gas production platforms.
- **4.3.2.** The ODD paragraph would be enhanced by clarifying that it includes all aspects of the vehicle Configuration, Role and Environment (CRE). The CRE model has been extremely useful in defence technical regulation for over 20 years to consider the scope of applicability of any prior certification to a new application and identifying potential risk sources from differences. A change in the vehicle configuration (extra sensors / improved software) could allow the expansion of the ODD, with the associated verification evidence provided.

- **4.3.3.** While dealt with later, the relationship between Human Machine Interface (HMI), education and training should be noted in this section. It is recommended that the last sentence becomes “the applicant must outline how the HMI has been designed, and outline the design assurance philosophy and the design compliance processes that have been used”. This is more in accordance with systems engineering language.

- It may also be identified that HMI takes on a different importance for SAE Level 1,2,3 where a driver is implicit party of the safety system, and Level 4/5 automation where the HMI relates to passengers, passenger safety systems and their level of service interaction with the ADS**.**

- **4.3.4.** It is suggested that breaking out compliance with relevant road rules as a separate topic may not be relevant at a principles level. Compliance with road rules and the ability to update systems when rules change is an aspect of any ADS design as a minor subset of 4.3.1 Safe System Design and the 4.3.2 ODD. It should also be noted that many existing road rules will not be suitable for ADS. For instance, in some Australian systems ‘undertaking’ is a legal manoeuvre that may not be able to be supported by an ADS. The relationship between the ADS safe operating design and road rules is complex and to suggest that simplistic compliance with existing road rules is a fundamental requirement to be placed on any vehicle system safety engineering design process both overestimates the contribution of road rules/traffic laws and oversimplifies the complexity of the design and assessment that must be demonstrated.

- **4.3.5.** It should probably be made clearer that the purpose of this requirement is purely for accident investigation and not for real time policing or emergency traffic management. Otherwise it is unclear how real time reporting of system state to police or emergency services contributes in any way to the safe operation of the ADS or why this function is included at such a high level in the assessment of the SAS.

- **4.3.6.** The minimum risk condition should also have a minimum equipment list outlining exactly which systems need to be operating correctly in order to achieve certain safe autonomous modes. Then if the minimum equipment list for that mode cannot be maintained, how does the system transition to the minimum risk condition. This is a principle used in aviation for release of aircraft for certain operations that require specific equipment for safety functions and assumptions to hold true.

- **4.3.7.** On road behavioural competency is a key design aspect that should be expanded upon as an element of 4.3.1 it is unclear why this attribute is broken out by the National Highway Traffic Safety Administration (NHTSA) and further investigation on this issue is warranted. See General notes on Appendix C.

- **4.3.9.** Recommend changing ‘testing for Australian road environment’ to ‘Designing for the Australian road environment’. As stated earlier, testing is just one method of verifying that a design has met a standard or requirement.

Nova agrees that outcomes-based criteria are superior to prescriptive criteria in such a dynamic technology field. It is also agreed that the high-level manner in which the criteria are used in section 4 as an example of how a SAS may assess an applicant’s proposal is useful. However, Nova suggests that there is additional work warranted to develop a robust set of assessment criteria by technology and safety specialists to be used once a choice is made between the high level organisational options presented in the RIS. It is suggested that the present criteria, as outlined in Appendix C, does not necessarily reflect current best practice in the execution of safety assurance in complex safety critical systems. The criteria could be better focussed and supported by guidance material on the risks of the technologies likely to be deployed or the failure methodologies associated with those technologies.

Nova recommends that section 4 be kept but noted as examples only and that the purpose of Appendix C be considered as heavily qualified “preliminary” or even removed from the RIS. It is clearly useful to explain current thinking and expectations on this journey for the stakeholders. However, not necessary to support decision-making on the regulatory structure. It is recommended

that the final set of guiding safety criteria be further developed along with the overall SAS once the RIS process nominates the higher-level approach. This approach also allows room for changes to evolve further and harmonise in the automotive producing countries and regions while the Australian SAS is drafted.

General comment on principles. 'Additional Principles' that may also guide the development of regulation, such as those outlined in the ''10 Ways to Better Aviation Regulation'[3], as outlined below:

- **Employ Hazard-Based Regulation**. Ensure regulatory obligations are only imposed to treat threats to aviation safety.
- **Maximise Outcome-Based Regulation**. Where possible, focus regulation on the outcomes needed to treat threats to safety and not the means of achieving those outcomes.
- **Take a Purposive Approach**. Express the purpose of the regulatory obligation simply and clearly and interpret and apply regulation with its purpose at the foremost of mind.
- **Utilise Compliance Proofs**. Define verification criteria against which to assess compliance.
- **Ensure Sufficient Prescription**. Decompose outcomes into constituent parts so that obligations are comprehensively specified and ambiguous principles are avoided.
- **Provide Comprehensive Explanation**. Implement a comprehensive and ongoing education program on aviation safety regulation.
- **Utilise Safety Indicators**. Utilise a wide-range of indicators to understand safety performance and drive continuous improvement.
- **Apply Risk-Based Oversight**. Use a robust risk-based assessment process to allocate finite oversight resources most effectively.
- **Take a Graduated Response**. Escalate enforcement remedies to elicit acceptable and compliant behaviour proportional to the observed behaviour and intent of the regulated entity.
- **Establish Genuine Engagement**. Aim to develop mutual respect, appreciating the natural tension between regulators and the regulated community. (Air Marshal Leo Davies, 2016)

RIS Question 7. Are there any additional criteria or other obligations that should be included?

As noted in the response to question 6 it is thought that a significant amount of further work is probably required to develop a final set of safety criteria to be used in the SAS. That said, there seems to be several notable exceptions at present, including:

- **Continued design integrity**. There appears to be limited detail in the RIS with respect to the in-service performance monitoring required / proposed to ensure ongoing safety for a given ADS functionality.

[3] Document used to shape the recent revolution in Defence Aviation regulatory approaches and language.
http://www.defence.gov.au/DASP/Docs/Manuals/BetterPracticeGuide/10WaystoBetterAviationRegulationSecondEdition2016.pdf

- **Safety Management System**. As outlined in our response to question 5, the RIS should include pro-active Hazard Identification and Safety Risk Management via defect and reliability data analysis aspects in greater detail.

RIS Question 8. Do you agree with the impact categories and assessment criteria? If not, what additional impact categories or assessment criteria should be included?

Road Safety. Would recommend adding another assessment criterion: 'Ensures safety of drivers and of other vulnerable road users'.

Uptake of Automated Vehicles. Would recommend adding the following assessment criteria: 'significantly contributes to a reduction of the road toll' and 'prevents an initial high incident rate that would halt automated vehicle uptake'.

Regulatory Cost to Industry. Because costs to industry are basically cost to consumers would recommend amending assessment criteria 'a. Results in low upfront ……' is edited to 'Results in market acceptable upfront....'. From a community perspective total cost of technology introduction, including regulatory costs, need to be less than the total cost savings that result from reduced accident rate, so the costs don't necessarily need to be low.

Regulatory Cost to Government. These assessment criteria are supported.

Flexibility and responsiveness. These assessment criteria are supported.

Safety Management System Principles. Organisational Accident risk management literature[4] would suggest comparisons can be made by assessing the threats and barriers to a top-level event, including:

- Number of barriers;
- Effectiveness of each barrier;
- Coverage across product, behaviour and process;
- Coverage across the initial design, continued integrity of the design and maintenance of individual vehicles; and
- Impartial assessment of the SMS.

As a follow-on from this RIS, it is Nova Systems' recommendation that a detailed safety assessment (such as a Bow-Tie Analysis) be conducted as part of developing any autonomous vehicle regulations.

[4] Ibid Reason, J. 1997

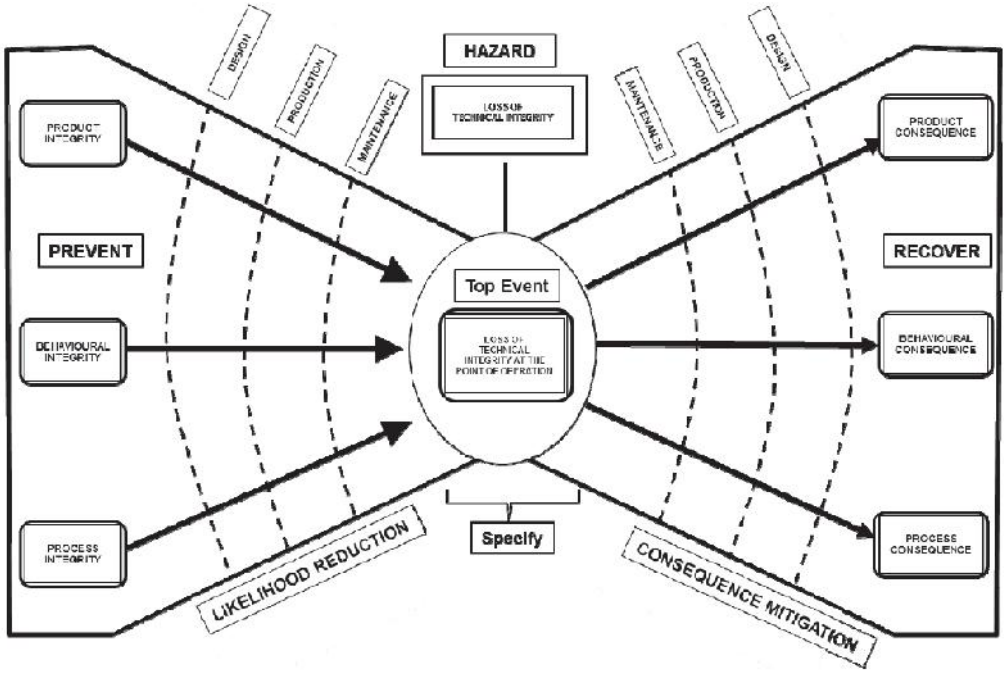


Figure 2. A composition of the bow-tie methodology overlapped with the technical integrity definition and technical item lifecycle, this framework is given the title the Product-Behaviour-Process (PBP) Bow-Tie. Importantly, this research is focused on preventative barriers of the PBP Bow-Tie (the lead up to the top event, shown on the left-hand side of the illustration).

Figure 2 – The Product-Behaviour-Process (PBP) Bow-Tie for Regulation Comparison
(Purton et al., 2016)

RIS Question 9. Has the consultation RIS captured the relevant individuals or groups who may be significantly affected by each of the options? Who else would you include and why?

Suggestions for additional stakeholder consideration:

Impact Category 1. Mechanics and 3rd party vehicle modifiers.

- Mechanics will need to understand what constitutes the certification basis of the vehicle to ensure that the safety assumptions made during the initial design, remain intact. Mechanics and 3rd party modifiers will likely incur additional training and certification costs as a result.

- Mechanics and vehicle modifiers may also incur additional costs due to the implementation of additional safety systems, which could include including organisational and individual certifications.

Impact Category 2. Uptake of Automated Vehicles … recommend including 'General Public (earlier reduced community cost due reduction in accidents)'.

Impact Category 3.

- **Infrastructure / 5G Network providers.** As the AVs achieve a higher level of automation, the amount of data they use across the 4G/5G network could significantly increase. This should be investigated with network providers.

- **Legal advice providers.** Until the regulations and laws around AVs are well understood there is a significant risk of confusion, which could slow progress, unless training is provided

Impact Category 5. Flexibility and Responsiveness …recommend including 'Manufacturers (where these are different from the ADSE)'.

RIS Question 10. Does our analysis accurately assess the road safety benefits for each reform option? Please provide any further information or data that may help to clearly describe or quantify the road safety benefits.

Nova Systems considers that the assessment correctly addresses the options.

Table 7 criteria e. If Option 3 includes an in-service monitoring function then emergent safety issues may still be identified. When an emergent safety issue is identified Option 3 is likely to produce the question 'what is the minimum we need to do to return the system to our service entry standard?'. Whereas Option 4 will ask the question 'what do we have to do to show we have reduced this emergent issue to an SFAIRP level.'

The RIS could also consider utilising some of the information outlined in the Waymo Trial example on Page 18 where the Virginia Tech Transport Institute found a 24% reduction in accidents, with the State of California DMV figures suggesting that only 1/25 may be attributable to the ADS. These figures are expected to get better with time, as the technology improves.

There are also several other areas that could see a significant reduction in accidents, including:

- Better adherence to the Road Rules;
- Better driver etiquette;
- Less tailgating;
- Reduced distracted drivers (phones etc);
- Reduced impaired drivers (drugs and alcohol);
- Less frustration on the roads; and
- Reduced Road Rage

RIS Question 11. What additional safety risks do you consider the primary safety duty in option 4 would address compared with option 3?

The advantage of Option 4 depends greatly on the level of regulation and oversight that is employed along with the 'primary safety duty'. The 'primary safety duty' should result in greater hazard identification and far more detailed root cause analysis, where the underlying problem is rectified,

rather than just replacing a defective piece of equipment. For example, if an ADS is found to have to have exceeded speed limits then, as part of Option 3, the ADSE would correct that specific issue. In Option 4 the ADSE would need to conduct a more comprehensive review of design processes, assumptions and identify any trends. Option 4 would require the ADSE to have a more comprehensive monitoring system to provide additional data around the lead-up to an event. Option 4 should significantly reduce the likelihood of an event re-occurring.

It would also be expected that maintenance standards should improve, due to the additional oversight provided by the ADSE.

RIS Question 12. Does our analysis accurately assess the uptake benefits for each reform option? Please provide any further information or data that may help to clearly describe or quantify the uptake benefits.

In general, the assessment provided in RIS 6.3 is agreed. An analysis of the reduction in the road toll would significantly strengthen the argument, however, it is acknowledged that reliable data is difficult to obtain at this point.

RIS Question 13. Does our analysis accurately assess the regulatory costs to industry for each reform option? Please provide any further information or data that may help to clearly describe or quantify the regulatory costs.

The comments in section 6.4.2 suggest that there may have been limited access to experience with technical certification processes. The use of the terminology ‘administrative cost’ and ‘delay costs’ is unclear and therefore the difference between Option 3 and Option 4 are not well outlined. The level of oversight and regulation activity and skills base applied can greatly influence the costs and benefits of an Option 4 system. For example, the Option 4 ‘primary safety duty’ could extend to having all personnel and organisations in the design and maintenance system assessed and approved by a regulatory body. The safety benefits of this additional regulation could be minimal if Option 4 focuses on efficient safety outcomes.

The context of the evolution of AV technology globally, is already impacting designers and manufacturers processes as well as regulatory thinking in producing countries. The approaches and safety criteria identified by the NTC are not out of step with those being addressed internationally. Therefore, options 3 and 4 should result in very similar initial certification costs. Given that Original Equipment Manufacturers (OEMs) will be re-using data that has previously been prepared for other national certification authorities the Australian specific certification cost should only involve addressing changes related to how the vehicle is operated in Australia and the unique Australian operating environment(s).

The in-service costs are not ‘administrative’ but involve supporting a comprehensive technical monitoring SMS. It is suggested that industry will have to ‘build’ internal processes and systems. For initial certification, the equipment OEMs should already be required to have these systems in place for certification in other markets and the Australian initial certification costs, especially if Australia establishes a system that is flexible enough to accommodate compliance finding artefacts in a non-prescriptive manner, should be a minor additional cost for a given product.

Sections 3.4.2 and 3.5.3 describe the expectation for how these options would work and implies aspects of functions within a national body that have not clearly been taken into account in the costing considerations. Such as:

- Option 3 in-service regulatory controls. The effectiveness of the proposed legislation would depend on a level of surveillance or investigation after some incident presumably reported by a fault finding body. Who would that body be and what data access, skills and knowledge would they require to identify these transgressions?

- Option 4 suggests the national body could investigate causes of incidents, near-misses or unsafe behaviour and then make findings with respect to ADS design deficiencies for unacceptable risk and whether technical solutions were reasonably practicable. This implies an ATSB like capacity with a detailed knowledge of ADS technologies. Nova would suggest this is beyond the current ATSB resources for other modes of transport and technical skill sets.

The in-service SMS cost will be far higher as they exist across the operational life of the product. The costs are associated with the operational monitoring, analysis and investigation systems. Costs are a function of the fleet size and risk sharing with the OEMs. However, in-service SMS infrastructure cost for an ADSE could be spread across multiple products. Systems do not have to be replicated for each new product. There is also potential for third-party organisations to provide the ADSE SMS services to a range of equipment vendors. The in-service SMS cost is likely to be passed on from the ADSE to customers / users as ongoing ADS running costs (analogous to maintenance support cost). Importantly these costs should be offset by reductions in insurance costs, both for vehicle damage and third party personal (TAC) costs, as accident rates reduce.

Option 4 provides the most definitive cost. For Option 3 the lack of an overarching 'primary safety duty' may actually result in greater long-term costs for the ADSE. The uncertainty around Option 3 should be highlighted in the RIS. Option 3 may leave ADSEs and equipment OEMs open to more undefined legal action and costs not incurred in more complete Option 4 processes.

RIS Question 14. Are there any specific regulatory costs to industry that we have not considered?

The analysis correctly identifies the two key costs as initial certification and ongoing in-service costs.

Other regulatory costs will depend on the level of regulatory oversight employed and its maturity. In a full compliance SAS that involves individual accreditation/certification and organisational accreditation of ADSEs (if not the OEM), then industry would have to fund additional training, certification and professional membership costs (e.g. CPEng for Engineers).

The likely nature of commercial relationships and risk sharing between ADSEs and the OEMs, may give rise to other cost factors associated with professional indemnity insurances.

RIS Question 15. Does our analysis accurately assess the costs to government for each reform option? Please provide any further information or data that may help to clearly describe or quantify the costs to government.

The general notion that Options 3 and 4 represent higher cost to Government than Options 1 and 2 is considered to be correct. The Appendix F costs to government are thought to be relatively low and should be benchmarked against similarly responsible agencies such as DASA and ONRSR.

As part of the Nova recommended consideration of regulatory risk barriers, there will be a realisation that trust in overseas authority certificates, and understanding the limitations and caveats of applicability to local needs, should have a basis of governance. This is typically achieved through

bilateral due diligence and agreements or international standardisation conformance audits. There will be a cost associated with establishing and maintaining this basis.

The RIS has notably struggled with detail on the additional costs to government. Nova Systems acknowledges that this will depend on the level of oversight and regulation that is outlined in the next phase. However, as a minimalist Rough Order of Magnitude (ROM), Nova Systems provides an estimate below based on experience in government regulation of defence aircraft. An initial estimate of a minimalist Vehicle Safety Agency could include:

- Developing regulation and staying abreast of current safety practice – 3 people (design, maintenance, operation/personnel).
- Initial product certification – 2 individuals.
- Initial organisational certification – 3 individuals (design, maintenance, operation/personnel).
- Ongoing Compliance Assurance – approx. 1 individual per 10 ADSEs. If the government plans to conduct oversight of maintenance organisations as well, then this number would be orders of magnitude higher.
- Accident investigators – 2-4 individuals.
- Data / Black Box assessments – several individuals.
- Section heads / task management – 3 individuals.
- Department head and admin staff – 4 individuals.
- Litigation?
- Total 25+ individuals.

This ROM estimate doesn't include any training or advisory aspects. It also doesn't include the manpower required to investigate and implement the initial set-up of a Vehicle Safety Agency.

RIS Question 16. Does our analysis accurately assess the flexibility and responsiveness for each reform option? Please provide any further information or data that may help to clearly describe or quantify the flexibility and responsiveness of the options.

The analysis is correct. Option 3 and Option 4 can be implemented in a 2020 timeframe if the safety assurance functions are executed outside existing government departments. It is thought that the 2020 timeframe would be extremely difficult to achieve if the transition was conducted on top of the core department duties. Subject Matter Experts (SMEs) could be engaged to assist in this process.

The regulatory system can stay abreast of international approaches if manpower is available to conduct this task. A regulatory agency can be flexible with outcomes-based regulation and empowerment within the agency. They can have legal powers to produce regulation, acceptable means of compliance and guidance materiel; such as CASA. Regulations can be updated on a regular basis (6/12 months) and an immediate ruling can be published within 24-48 hours.

RIS Question 17. Do you consider the relevant factors and conditions for government in choosing an option to be valid? Are there any factors and conditions you do not agree with?

The approach outlined in RIS 7.3 appears to be generally valid for Options 3 and 4 with some statements being more polarised than expected. However, it is recommended that the points to consider for Option 2 may fail to deliver on the promise. A cautious, incremental approach is believed to result in Australia lagging the rest of the world and not realising the vital safety improvements that are promised for AVs. It is believed that this would result in greater uncertainty for the public and manufacturers and would maintain a higher road toll for longer.

Option 3 point 6 is also unrealistic; requirements, offences and penalties will need to be updated when we learn more about the technology and how it is used.

RIS Question 18. Do you agree with our view on the relevant factors and conditions for government in choosing an option?

It is Nova Systems' view that the RIS Options choice and full development of the SAS could also benefit from a Risk Identification and Risk Management approach to the regulations outlined in Options 3 and 4. As discussed earlier, the Purton et.al (2016) comparative regulatory framework analysis technique could help substantiation. It could also be well worth conducting a Bow-Tie Analysis of a range of AV accident scenarios to provide a more detailed cross section of the likely hazards. Once the hazards have been identified a layered regulatory approach can provide safety assurance through appropriate barriers. Using this method, there is limited wasted effort in regulation that does not target a particular safety concern.

RIS Question 19. Has the consultation RIS used an appropriate analytical method for assessing the benefits and costs of the options? What else should be considered?

The benefits are well explained, and the main relevant benefits are clearly understood.

The cost for both industry (consumers) and government are not well understood or outlined in the RIS. The structure or outcomes required of a Vehicle Safety Regulator are not well articulated, which makes it extremely difficult to estimate the cost of a regulatory system. It is possible to investigate like technology / industry SASs to achieve an estimate of costs. The Appendix E benefit estimates are simplifications and would warrant external validation and academic sensitivity testing. Likewise, the Appendix F cost estimates warrant benchmarking against similar regulatory systems in Aviation and Rail, as the DIRDAC past experience has been in a vastly simpler administrative process based on internationally agreed standards and less complex integrated technologies with risks shared with the driving public.

The concept that the costs of any SAS will be significantly less (by orders of magnitude) than the savings from increased road safety is agreed and this thought to be the most important consideration.

The lack of fidelity in costs at this point in the RIS process is not crucial as the relative ranking of options is correct.

RIS Question 20. On balance, do you agree that the preferred option best addresses the identified problem? If not, which option do you support?

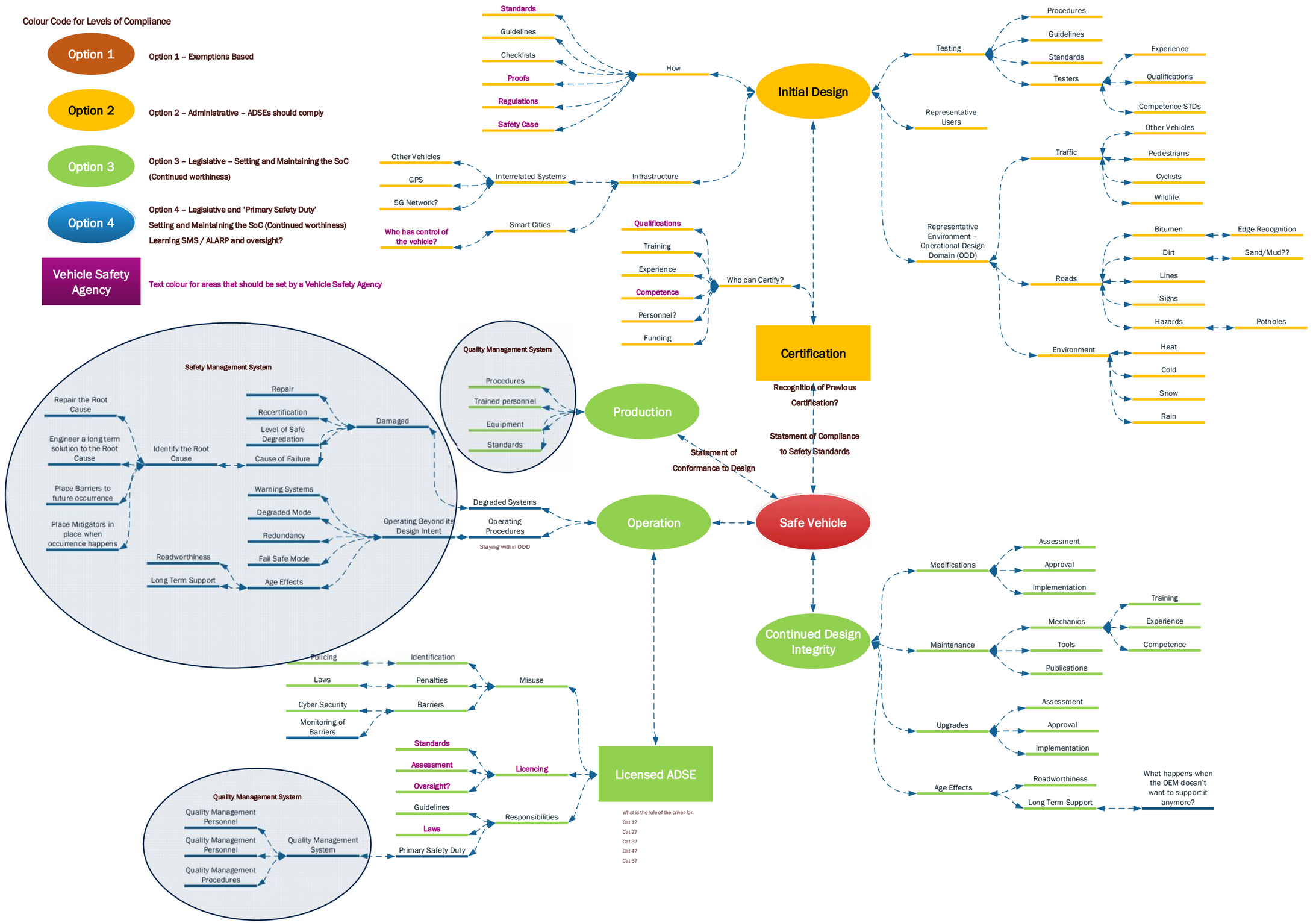
Nova Systems agrees that Option 4 is the best option.

RIS Question 21. How does your choice of option better address the problem than the preferred option?

Not applicable. Nova endorses the NTC choice of option.

3 ANNEXES

A. Mind Map of AV Safety Factors


Colour Code for Levels of Compliance
Option 1
Option 1 – Exemptions Based
Option 2
Option 2 – Administrative – ADSEs should comply
Option 3
Option 3 – Legislative – Setting and Maintaining the SoC (Continued worthiness)
Option 4
Option 4 – Legislative and 'Primary Safety Duty' Setting and Maintaining the SoC (Continued worthiness) Learning SMS / ALARP and oversight?
Vehicle Safety Agency
Text colour for areas that should be set by a Vehicle Safety Agency
Standards
Guidelines
Checklists
Proofs
Regulations
Safety Case
How
Initial Design
Other Vehicles
GPS
5G Network?
Who has control of the vehicle?
Interrelated Systems
Smart Cities
Infrastructure
Qualifications
Training
Experience
Competence
Personnel?
Funding
Who can Certify?
Certification
Recognition of Previous Certification?
Statement of Compliance to Safety Standards
Statement of Conformance to Design
Testing
Representative Users
Procedures
Guidelines
Standards
Testers
Experience
Qualifications
Competence STDs
Representative Environment – Operational Design Domain (ODD)
Traffic
Other Vehicles
Pedestrians
Cyclists
Wildlife
Roads
Bitumen
Edge Recognition
Dirt
Sand/Mud??
Lines
Signs
Hazards
Potholes
Environment
Heat
Cold
Snow
Rain
Safety Management System
Repair the Root Cause
Engineer a long term solution to the Root Cause
Place Barriers to future occurrence
Place Mitigators in place when occurrence happens
Identify the Root Cause
Repair
Recertification
Level of Safe Degredation
Cause of Failure
Damaged
Warning Systems
Degraded Mode
Redundancy
Fail Safe Mode
Age Effects
Roadworthiness
Long Term Support
Operating Beyond its Design Intent
Quality Management System
Procedures
Trained personnel
Equipment
Standards
Production
Degraded Systems
Operating Procedures
Staying within ODD
Operation
Safe Vehicle
Continued Design Integrity
Modifications
Assessment
Approval
Implementation
Maintenance
Mechanics
Training
Experience
Competence
Tools
Publications
Upgrades
Assessment
Approval
Implementation
Age Effects
Roadworthiness
Long Term Support
What happens when the OEM doesn't want to support it anymore?
Policing
Identification
Laws
Penalties
Cyber Security
Barriers
Monitoring of Barriers
Misuse
Standards
Assessment
Oversight?
Licencing
Guidelines
Laws
Responsibilities
Primary Safety Duty
Licensed ADSE
What is the role of the driver for:
Cat 1?
Cat 2?
Cat 3?
Cat 4?
Cat 5?
Quality Management System
Quality Management Personnel
Quality Management Personnel
Quality Management Procedures
Quality Management System