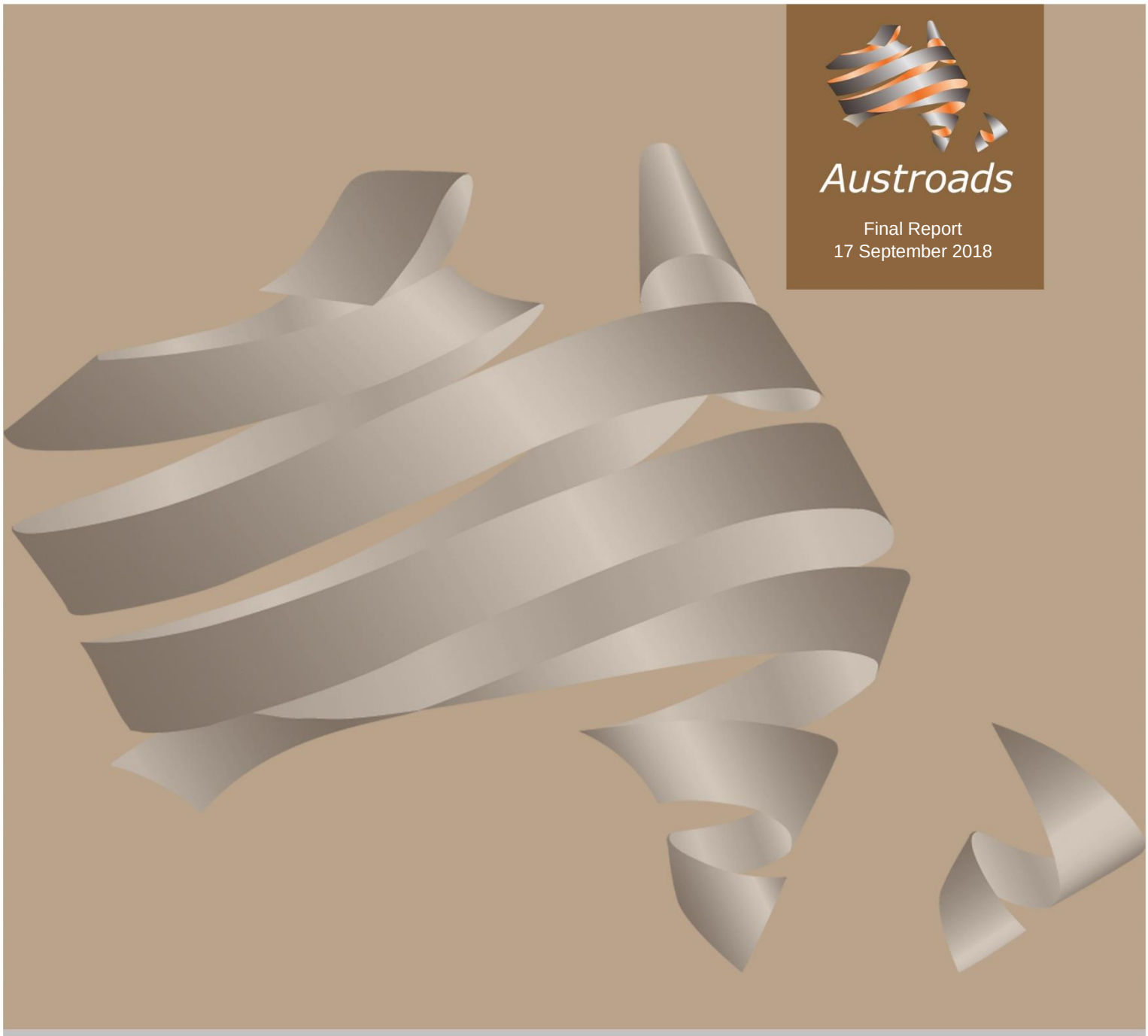


Austroads

Final Report
17 September 2018

C-ITS Compliance Assessment Framework for Australia and New Zealand

C-ITS Compliance Assessment Framework for Australia and New Zealand

Prepared by

Jesper Engdahl (Rapp Trans), Dr. Cornelie van Driel (Rapp Trans), David Green (ARRB)

Project Manager

Niko Limans

Publisher

Austroads Ltd.
Level 9, 287 Elizabeth Street
Sydney NSW 2000 Australia
Phone: +61 2 8265 3300
austroads@austroads.com.au
www.austroads.com.au

Abstract

This report on a compliance assessment framework (CAF) for cooperative intelligent transport systems (C-ITS) for Australia and New Zealand (ANZ) covers the key findings from a literature review and stakeholder consultations and describes the main CAF model options for C-ITS.

The C-ITS CAF options cover status quo, self-regulation, quasi-regulation and regulation, whereby the level of regulation and assurance by the government increases with each option.

The report sets out options for the development of a C-ITS CAF for ANZ, including the proposed approach based on hybrid model options and guidance relating to key topics, such as governance architecture and approval processes.

It provides recommendations for the main tasks to be undertaken in the further development and implementation of an ANZ C-ITS CAF.

Keywords

C-ITS, compliance assessment, market surveillance, certification, accreditation, type approval, mutual recognition principle and agreement, overseas approvals, governance architecture, standards and regulations, trust model, Security Credential Management System, Common Criteria

ISBN ANO to supply on publication

Austroads Project No. XXX

Austroads Publication No. ANO to supply on publication

Publication date ANO to supply on publication

Pages ANO to supply on publication

About Austroads

Austroads is the peak organisation of Australasian road transport and traffic agencies.

Austroads' purpose is to support our member organisations to deliver an improved Australasian road transport network. To succeed in this task, we undertake leading-edge road and transport research which underpins our input to policy development and published guidance on the design, construction and management of the road network and its associated infrastructure.

Austroads provides a collective approach that delivers value for money, encourages shared knowledge and drives consistency for road users.

Austroads is governed by a Board consisting of senior executive representatives from each of its eleven member organisations:

- Roads and Maritime Services New South Wales
- Roads Corporation Victoria
- Queensland Department of Transport and Main Roads
- Main Roads Western Australia
- Department of Planning, Transport and Infrastructure South Australia
- Department of State Growth Tasmania
- Department of Infrastructure, Planning and Logistics Northern Territory
- Transport Canberra and City Services Directorate, Australian Capital Territory
- Australian Government Department of Infrastructure and Regional Development
- Australian Local Government Association
- New Zealand Transport Agency.

Acknowledgements

This project team would like to acknowledge the contribution of the Austroads' project manager on C-ITS, Niko Limans. It would also like to acknowledge the contributions of the Project Reference Group and all stakeholders that participated in the stakeholder consultations. In addition, the project team would like to acknowledge the contributions of external experts for their inputs and guidance in the project: Robert Sykora (convenor of C-ITS standardisation in ISO/TC204/WG18 and CEN/TC278/WG16), Niels Peter Skov Andersen (general manager of C2C-CC and chairman of ETSI TC on ITS), Andrea Lorelli (technical officer of ETSI TC on ITS), Hans Johansson (chairman of ETSI ITS WG4 on media and medium related), Gerhard Menzel (DG Move policy officer C-ITS), Bernardo Martinez (DG Move, policy officer smart tachograph), Kevin Gay (USDOT ITS JPO), Jasja Tijink (C-ITS Platform, Kapsch) and Kerry Malone (C-ITS Platform, TNO).

Summary

Austroads is seeking to identify and assess options for an assurance compliance framework in the area of cooperative intelligent transport systems (C-ITS) that will ensure the safe operation of C-ITS in Australia and New Zealand (ANZ).

This report covers the key findings from a literature review and stakeholder consultations and describes and assesses the main compliance assessment framework (CAF) model options.

C-ITS deployment is in its infancy. Europe and the USA are leading the global developments, driven by the industry wanting to develop the automotive market by bringing voluntary C-ITS services quickly into the market. Policy makers try to create favourable market and regulatory conditions so that society can start to reap the benefits from the emerging C-ITS services. In ANZ, significant C-ITS research work has been undertaken. Moreover, both countries are proactively undertaking connected and automated vehicle trials.

The C-ITS CAF options cover status quo, self-regulation, quasi-regulation and regulation, whereby the level of regulation and assurance by the government increases with each option. The report sets out the options and discusses them in detail, including the proposed approach based on hybrid model options and guidance relating to key topics, such as governance architecture and approval processes.

The stakeholder consultations revealed that it is currently premature to determine the preferred CAF model(s), given the range of elements of C-ITS that are still in the development phase (e.g. evolving policies, use cases, standards, technologies).

The following main tasks are recommended to be undertaken in order to progress the development and implementation of C-ITS in ANZ:

1. **Set up an ANZ C-ITS Platform** in order to address the main barriers and enablers identified for deployment of C-ITS in ANZ
2. **Determine the overall objective, role and scope of the ANZ C-ITS CAF**: the C-ITS strategy including agreed Day 1 applications and associated use cases and message sets
3. **Set up the C-ITS governance model**
4. **Prepare the establishment of the Security Credential Management System**
5. **Determine the approval procedures and conformity assessment criteria** through adoption of relevant international standards and recognition of overseas approval procedures

The CAF should provide a framework in which the compliance model is linked to the risk of the application for which the compliance model is to apply. The CAF model required for the applications should be adaptable and reflect the risk and consequence of that application misbehaving. A ‘one size fits all’ approach is unlikely to provide a framework that is fit for purpose.

It is recommended to consider adopting a staged and hybrid approach, consisting of different models for different types of C-ITS stations and application areas, in the downstream work.

Contents

Tables

Figures

1. Introduction

Austroads is seeking to identify and assess options for an assurance compliance framework in the area of cooperative intelligent transport systems (C-ITS) that will ensure the safe operation of C-ITS in Australia and New Zealand (ANZ).

This project *C-ITS Compliance Assessment Framework* under the Austroads Program CAV2109 *Cooperative ITS Operational Framework* contributes to the development of a C-ITS compliance assessment framework (CAF) in ANZ, which will ensure that C-ITS stations comply with a range of agreed standards and specifications ensuring that these do not jeopardise safety, are fit for purpose, are interoperable, support an open vendor market and avoid vendor lock-in with proprietary solutions.

Two outputs will be produced:

1. A report setting out the options for the development of a C-ITS compliance assessment framework (C-ITS CAF), including potential governance and process models, technical performance requirements and validation. It is required to be fit for purpose.

2. A high-level project plan for achieving an ANZ C-ITS CAF, taking into account the time and methods by which such a framework might be implemented.

This report covers the key findings from a literature review and the stakeholder consultations, and describes the main CAF model options for the C-ITS CAF. The report sets out, in accordance with the agreed direction with the Project Reference Group, the options including the proposed approach based on hybrid model options and guidance relating to key topics, such as governance architecture and approval processes.

The structure of the report is as follows:

- Section 1: Introduction – introduces the report and the project.
- Section 2: Literature Review – provides details of the literature review undertaken along with key findings and implications for the project.
- Section 3: Development and Evaluation of ANZ C-ITS CAF Models – provides an overview of the main CAF models and an assessment of these models.
- Section 4: Stakeholder Consultations – provides details of the stakeholder consultations undertaken along with key findings and implications for the project.
- Section 5: Discussion – provides the main findings and considerations on future work.
- Section 6: Conclusions and recommendations – provides the conclusions and recommendations of this project.
- Appendices: Appendices provide supplementary information to that contained in the body of the report.

1.1 Project Background

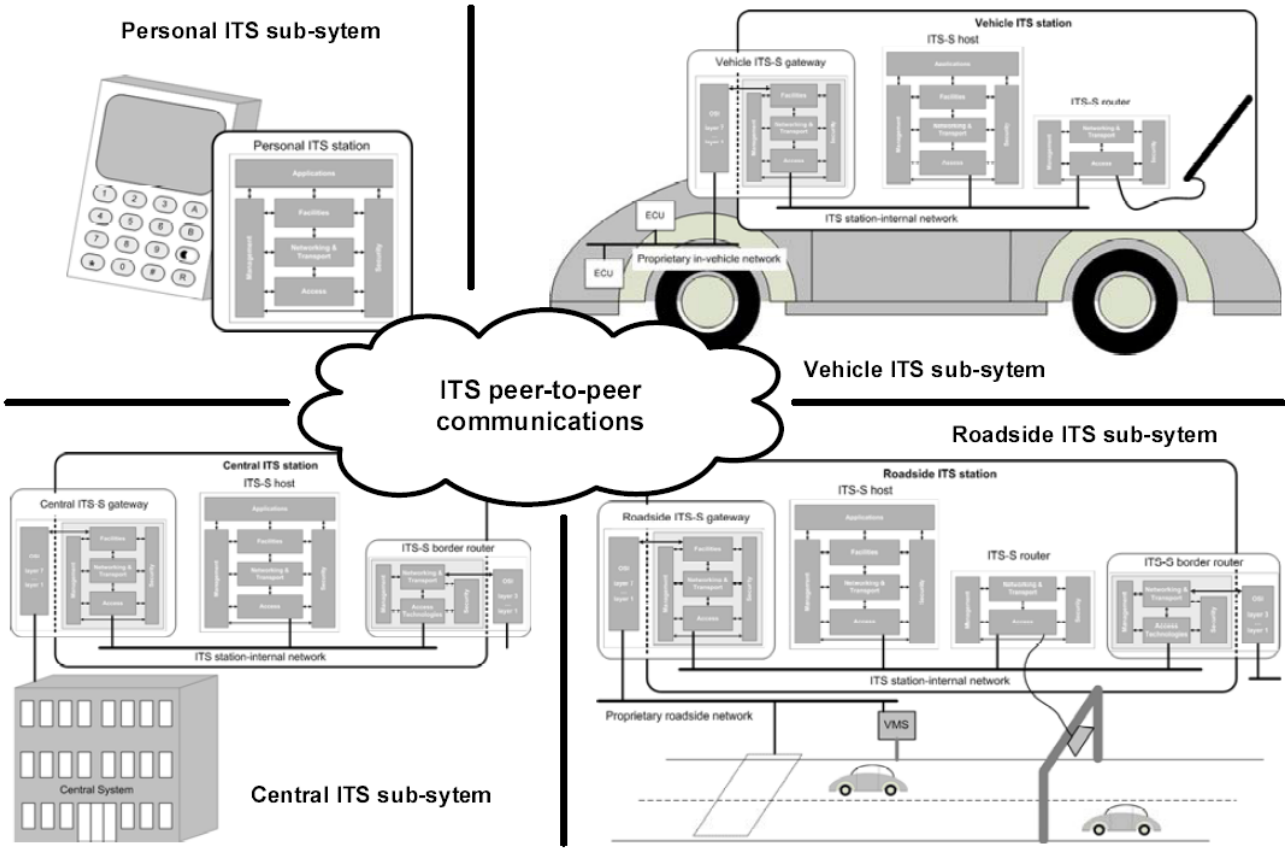
Cooperative ITS (C-ITS) are a subset of the broader suite of ITS which use wireless communications to share information between vehicles, roadside infrastructure, mobile devices and centres through so-called ITS stations. This will allow vehicle and transport applications to work together cooperatively to deliver outcomes that are beyond what is achievable with standalone ITS and vehicle applications.

1.1.1 ITS stations

Four types of ITS stations, being part of an ITS sub-system, can be identified (as illustrated in Figure 1.1):

- Personal ITS station (P-ITS-S): ITS station in a personal ITS sub-system, e.g. in hand-held devices, such as mobile phones
- Central ITS station (C-ITS-S): ITS station in a central ITS sub-system, e.g. in road authority offices or service providers' back offices
- Vehicle ITS station (V-ITS-S): ITS station in a vehicle ITS sub-system, e.g. in cars and trucks in motion or parked
- Roadside ITS station (R-ITS-S): ITS station in a roadside sub-system, e.g. on gantries, poles.

Figure 1.1: Illustration of ITS sub-systems



Source: ETSI EN 302 665.

C-ITS are expected to significantly improve road safety achieved by vehicle-to-vehicle (V2V) communications and traffic efficiency, traffic management and road safety by infrastructure -to-vehicle (I2V) communications. C-ITS also serve other purposes, like commercial services, and prepare the technology needed for self-driving vehicles.

1.1.2 C-ITS compliance assessment framework

The technology is rapidly evolving and the public and private sectors are investing substantial amounts into developing and testing C-ITS technologies. Industry has stated its intention to start large-scale deployment of C-ITS enabled vehicles in 2019. For this to happen, coordination is urgently needed.

One important element of coordination is the development of a C-ITS compliance assessment framework to ensure that only valid ITS stations are deployed in the field, i.e. ITS stations that:

- do not jeopardise safety
- are fit for purpose (including effective use and support for efficient use of the radio spectrum in order to avoid harmful interference)
- are interoperable
- support an open vendor market and avoid vendor lock-in with proprietary solutions.

A C-ITS compliance assessment framework can be defined as a series of processes, by which ITS stations are validated through a set of tests intended to assess the level of their compliance throughout their whole life cycle, whereby several stakeholders are involved or responsible for the different phases of the processes.

C-ITS, having a global context, make it crucial to view the C-ITS compliance assessment framework at an international level, also to identify areas where harmonisation is needed. For New Zealand this could mean seeking to align its C-ITS standards with those in Australia, but also seeking to share administrative and legal approaches with Australia – where sensible. At a higher international level, the work done within the Harmonisation Task Groups of Australia (TCA), the European Commission (EC) and the US Department of Transport is also relevant.

The term 'compliance' is generally used to describe the action of doing what is required. For example, an organisation 'complies' by making something conform or by fulfilling a regulatory requirement (ISO/IEC 17000). Related to this, the term 'conformity assessment' is the demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.

Overall, compliance/conformity assessment covers the following aspects:

- The conformity of a product is assessed before it is placed on the market.
- It needs to demonstrate that all (legislative) requirements are met.
- It includes testing, inspection and certification.
- The procedure for each product is specified in the applicable product specification/legislation.

Objectives of the conformity assessment procedure are:

- To demonstrate that a product being placed on the market complies with all requirements.
- To ensure confidence of consumers, public authorities and manufacturers regarding the conformity of products.
- To facilitate trade by the use of conformity assessment (e.g. mutual recognition principle) including the accreditation of conformity assessment bodies.

Conformity assessment must not be confused with market surveillance, which consists of controls by the (national) market surveillance authorities or bodies after the product has been placed on the market. However, both techniques are complementary and equally necessary to ensure the protection of the (public) interests at stake and the smooth functioning of the market.

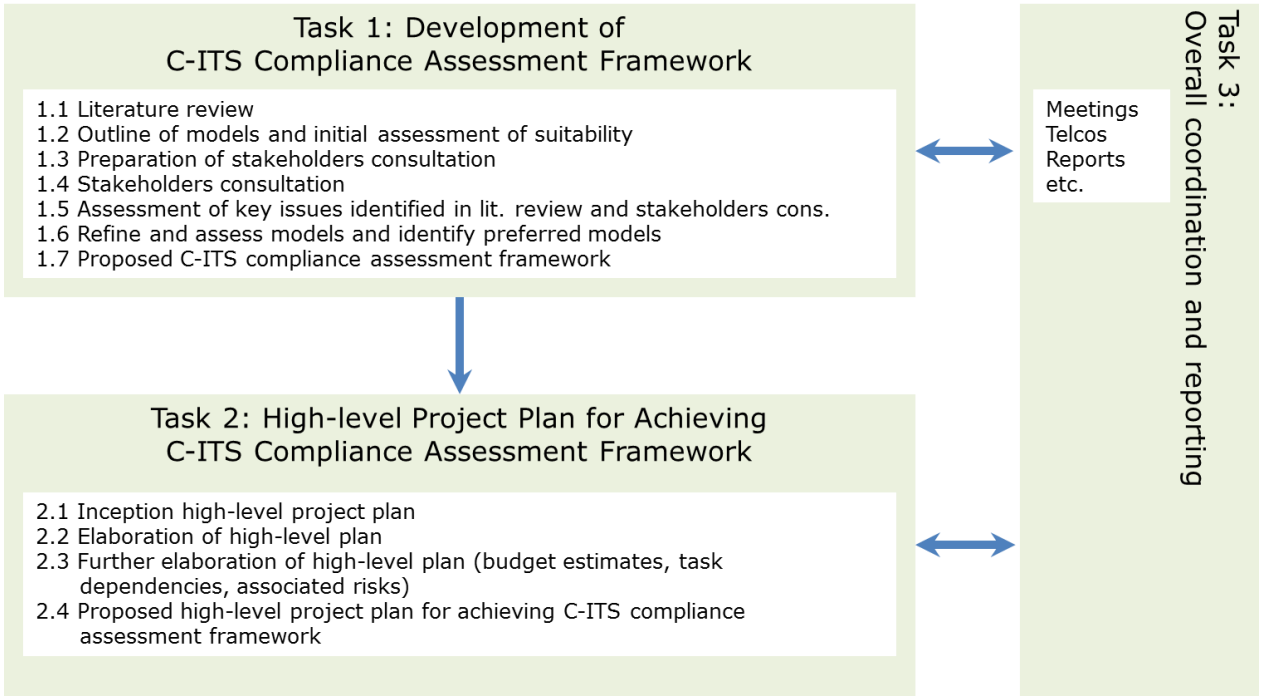
1.2 Project Overview

The two main outputs defined in Section 1 are being prepared through execution of two main tasks:

- Task 1: Development of C-ITS compliance assessment framework
- Task 2: High-level project plan for achieving C-ITS compliance assessment framework.

In addition, Task 3 provides the overall coordination of the activities as well as coordination with Austroads. Figure 1.2 gives an overview of the planned tasks.

Figure 1.2: Overview of the planned tasks



This project is delivered over several milestones as indicated in Figure 1.3 with timing and deliverables provided.

Figure 1.3: Project outline

2. Literature Review

2.1 Approach

The purpose of the literature review was to present an overview of the C-ITS context and state of play in ANZ as well as the global C-ITS developments, mainly in Europe and USA[1]. This section provides the high-level review of documentation deemed relevant to this project. More details of the literature review can be found in a Working Paper[2]. Appendix A presents a list with all reviewed documentation within the time frame of October 2017 until January 2018. Moreover, as part of the literature review the project team contacted relevant external experts[3] in Australia, Europe and USA to discuss and clarify certain ongoing developments.

At the end of this section is a list of the key findings derived from the literature review. These key findings were used to refine the scope of the development of the ANZ C-ITS CAF, especially for developing and evaluating possible models (see also Section 3) and drafting the Explanatory Note prepared for the stakeholder consultations (see also Section 4).

2.2 ANZ C-ITS Context and State of Play

Significant C-ITS research work has been undertaken in ANZ. However, both countries are investigating the regulatory and policy implications of connected and automated vehicles (CAV). No formalised ANZ C-ITS implementation road map is known to exist. Australia and New Zealand are both proactively undertaking CAV trials, representing the current status in ANZ in terms of initial C-ITS deployment. The following sections present the main elements for describing the ANZ C-ITS context and state of play.

2.2.1 Austroads C-ITS Program

Introduction

New and emerging technologies, such as C-ITS, will have a direct impact on the management of the road network (Austroads 2015a). C-ITS is part of the work streams of the Austroads Safety Program and Network Program. The C-ITS Task Force provides expert input to the work.

The Austroads Connected and Automated Vehicles (CAV) program is working closely with key government and industry stakeholders towards establishing the required supporting regulatory and operational frameworks. As well as automated vehicles (AV), C-ITS is one of the key focus areas in the CAV program.

In order to reach the key public objectives for the deployment of C-ITS, ANZ need to be prepared for the advent of C-ITS equipped vehicles. As described in the *Cooperative ITS Strategic Plan* (Austroads 2012b), ANZ started working towards this goal. The Transport and Infrastructure Senior Officials' Committee (TISOC) endorsed a summarised version of this strategic plan.

Austroads has been working on investigating C-ITS for potential deployment since 2008. One of the current projects is CAV2109 *Cooperative ITS – Operational Framework*, under which this assignment on *C-ITS Compliance Assessment Framework* is being undertaken. Relevant information from previous projects (e.g. *C-ITS Standards Assessment*), current projects (e.g. *Evaluation of the European C-ITS platform including a threat, vulnerability and risk analysis*) and current practices (e.g. the product acceptance process) is described below.

[1] Japan pursues the use of its VICS equipment, which operates at 5.8 GHz and is not interoperable with C-ITS.
[2] C-ITS Compliance Assessment Framework for Australia and New Zealand (16 February 2018), which can be obtained on request via Austroads' C-ITS Project Manager, Mr. Niko Limans (Niko.Z.Limans@tmr.qld.gov.au).
[3] In particular key stakeholders in the development of national C-ITS frameworks and strategies, ETSI / ISO CEN standardisation work and the C-ITS industry.

C-ITS Standards Assessment

The *C-ITS Standards Assessment* report (Austroads 2015b) contains the outcomes of an analysis of 160 C-ITS standards, including:

- EU scenario: 55 high-priority standards
- US scenario: 7 high-priority standards.

The report may be used to provide an understanding of the standards and provide guidance for determining which standards should be adopted locally.

Standards are important for C-ITS as they enable two or more entities within the C-ITS environment to interact in an interoperable and safe manner.

Compliance of products and services in the ANZ market with standards is normally voluntary, unless they are regulated by government. Regulation may be considered if the standard for the products and services relates to safety or addresses environmental or consumer protection issues. Certification refers to confirmation that certain characteristics of a product or service, as defined by standards or some other mechanism, are complied with. Therefore, certifying a product or service gives the purchaser or user assurance that it complies with the standards defining its use.

Australian Standards define the strategies for assessing conformity. In line with this, it is considered that certification for C-ITS standards may be undertaken by three levels as outlined below:

- Third-party certification: Involves an independent assessment of compliance by an accredited body.
- Second-party certification: An association or group provides assurance of compliance. For example, the Traveller Information Service Association (TISA) certifies traffic message channel (TMC) location tables for use in TMC traveller information services.
- First-party certification: An individual or organisation providing the product offers assurance that it complies. For example, the USA requires vehicle manufacturers to 'self-certify' that their products meet the Federal Motor Vehicle Safety Standards (FMVSS).

The types of certification considered relevant to C-ITS include:

- Individual inspection: Each individual product is assessed. For example the Registered Automotive Workshop Scheme (RAWS) requires each vehicle to be inspected that is a low-volume import, before it can be registered.
- Type approval: This is granted to a type of product that meets a set of requirements (i.e. inspect/assess one and therefore approve all of the same type). This is usually required before a type of product can be sold in a particular market. Evidence of compliance generally needs to be submitted to a governing body to assess and grant type approval (also known as homologation) (e.g. the Australian Design Rules, ADRs). Some type approval systems do not require evidence to be submitted prior to product release, but that it is available if requested (e.g. as of 2013, the single regulatory compliance mark (RCM) administered by the Australian Communication Media Authority (ACMA) and the Radio Spectrum Management in New Zealand).
- Audit/surveillance: This is used to verify that a product is complying with the requirements when in service/operation (e.g. vehicle roadworthiness inspections).[4]

For those C-ITS standards that are determined to need compliance, it will be necessary to decide whether compliance should be regulated and what level and type of certification is most appropriate. The report recommends that comprehensive conformance test suites should be developed for the various core standards. While mandating C-ITS functionality in vehicles is not currently being considered in Australia or New Zealand, voluntary compliance with the C-ITS standards that are associated with voluntary C-ITS functions may be required or optional.

[4] For example, the VW Dieselgate was detected through a US Environmental Protection Agency (EPA) check of in-service emissions vs expected performance.

The report discusses considerations regarding the EU vs the US scenario:

- Australia traditionally follows Europe's vehicle regulations. For example, where possible, Australia harmonises with the United Nations Economic Commission for Europe (UNECE) vehicle regulations. On the other hand, the USA follows the Federal Motor Vehicle Safety Standards (FMVSS).
- Australian communication standards (beyond C-ITS) traditionally follow Europe.
- The Federal Chamber of Automotive Industries (FCAI) has indicated a desire to follow European standards for C-ITS.

Conclusions of the report include:

- Need for a minimum set of standards for early deployment
- Need to pick a scenario.

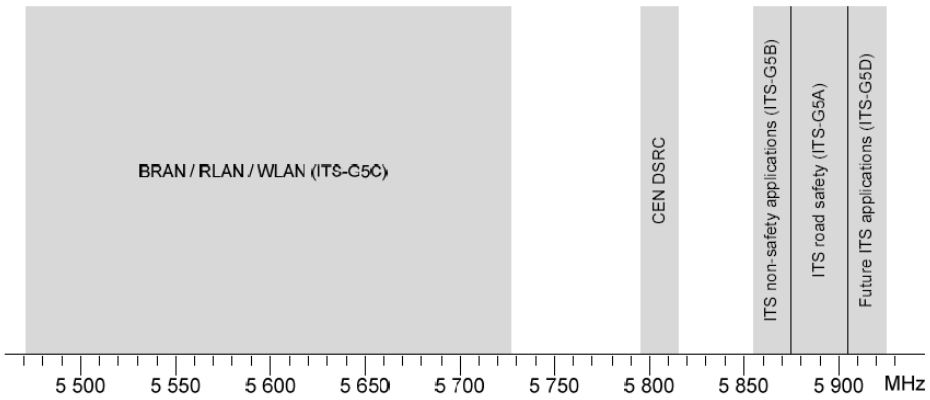
C-ITS spectrum management and device licensing regime

The *C-ITS 5.9 GHz Spectrum Management and Device Licensing Regime* report (Austroads 2012a) identified that the Australian Communication and Media Authority (ACMA) had three licence regimes for the licencing of communications devices wishing to communicate on radio spectrum.

Austroads has been working with ACMA to secure the 5.9 GHz spectrum for C-ITS and to put the licencing regime in place. ACMA's *Radiocommunications (ITS) Class Licence 2017* came into effect on 6 January 2018 and authorises the operation of transmitters used for V2V, V2I and vehicle-to-person communications.

Australia has adopted the European frequency allocation for C-ITS (Figure 2.1) concerning the ITS-G5A, B and D bands (based on ETSI EN 302 571 standard, not ITS-G5C), with the similar protection of the 5875-5905 MHz band for ITS road-safety-related applications as in Europe.

Figure 2.1: Channel allocation for the 5 GHz frequency within the European Union



Source: ETSI EN 302 663.

Figure 2.1 illustrates the channel allocation in the 5 GHz range for C-ITS within the European Union. It also shows the European bands for dedicated short-range communication (DSRC, so called CEN DSRC) used for electronic toll collection.

Equipment complying with the EU C-ITS RF regulation (i.e. Radio Equipment Directive and ETSI EN 302 571) would meet Australian licensing conditions, whereas US-complying equipment may not. The ACMA ITS Class Licence requires evidence of compliance (with ETSI EN 302 571) to be held by the supplier of the radiocommunications device, but does not need to be submitted to ACMA (unless ACMA asks for it as part of an audit or investigation).

New Zealand has a similar radio licencing regime but has not yet made a formal decision to allocate 5.9 GHz spectrum for C-ITS use. A decision is expected to be taken after the 2019 World Radiocommunication Conference. However, NZ has reserved the 5.9 GHz spectrum for use by C-ITS.

Operationalising the ITS product acceptance process

The *Operationalising Austroads' Product Acceptance Process* report (Austroads 2016) proposes a detailed governance framework.

It includes an analysis of nine cases studies[5] and a selection of the most suitable operational model. It recommends that ITS products that fall under the following principal criteria should be type approved according to the proposed national ITS type approval process (NIPTAP):

- regulatory devices or devices with legislation requirements
- devices which have significant failure impacts on road network operation and safety (i.e. suitably high-risk profile)
- devices which require a high level of interoperability and compatibility with existing traffic management systems
- devices which have reasonable volume and regular/reasonable frequency of demand.

It proposes a hybrid model with a harmonised type approval governance process endorsed by all Australian state and territory road agencies following a seven-step pre-market approval process:

- Step 0: Accept type approval application
- Step 1: Determine performance requirements
- Step 2: Perform preliminary product assessment
- Step 3: Conduct desktop audit
- Step 4: Conduct laboratory tests
- Step 5: Perform field tests
- Step 6: Report and enter into the national type approved ITS product register.

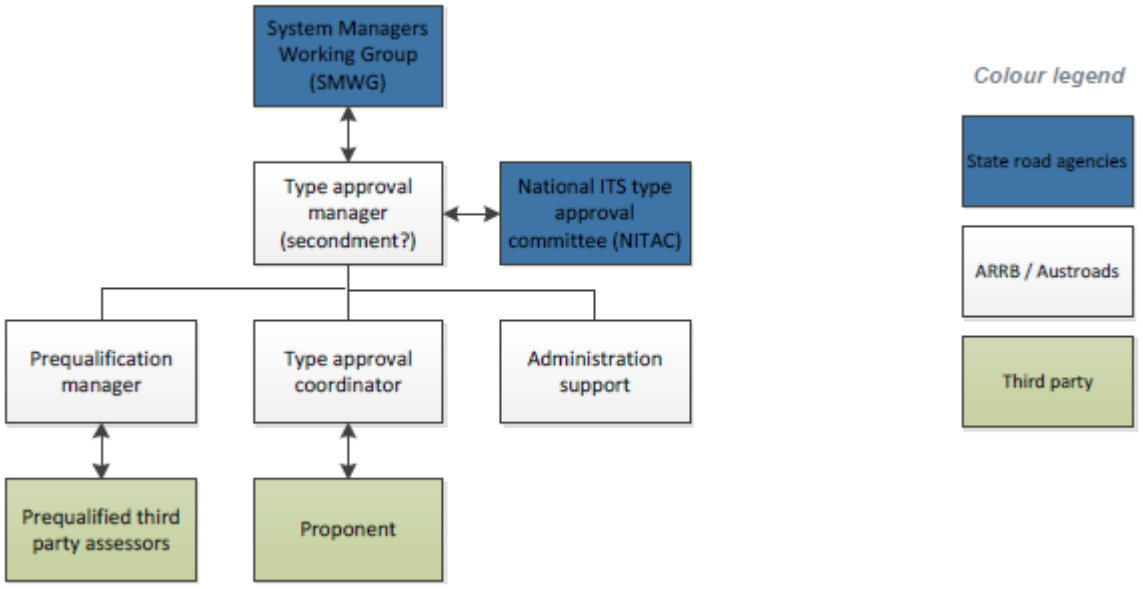
It proposes a governance framework (Figure 2.2), for which it recommends the establishment of a national ITS type approval committee (NITAC) (under the authority of the road agencies), to review product testing results, and approve products.

A single nationwide type approval certificate with acceptance conditions will be issued for successful ITS products. The process will be administrated from a central office with the product assessment outsourced to prequalified third parties. The approval process workflow and results would be managed and maintained through a web register, which would also provide centralised access management and an information-sharing mechanism for both road agencies and industry stakeholders.

It should be noted that the model is conceptual and that no decision has been made to implement it.

[5] The report includes the three case studies (RMS, VicRoads and TMR) in the preceding report on product acceptance techniques for road network devices (Austroads 2015d), which recommended a quasi-identical six-step pre-market approval process.

Figure 2.2: Governance model



Source: Austroads 2016.

Harmonisation Task Groups

C-ITS, having an international context, make it crucial to view the C-ITS compliance assessment framework at an international level, and also to identify areas where harmonisation is needed. At the highest international level, the work done within the Harmonisation Tasks Groups (HTGs) of the European Commission, the US Department of Transport, and Australia (TCA) is of high importance - especially HTG7 on standards to enable first stage deployments of C-ITS, and HTG6 on a cooperative-ITS security policy framework.

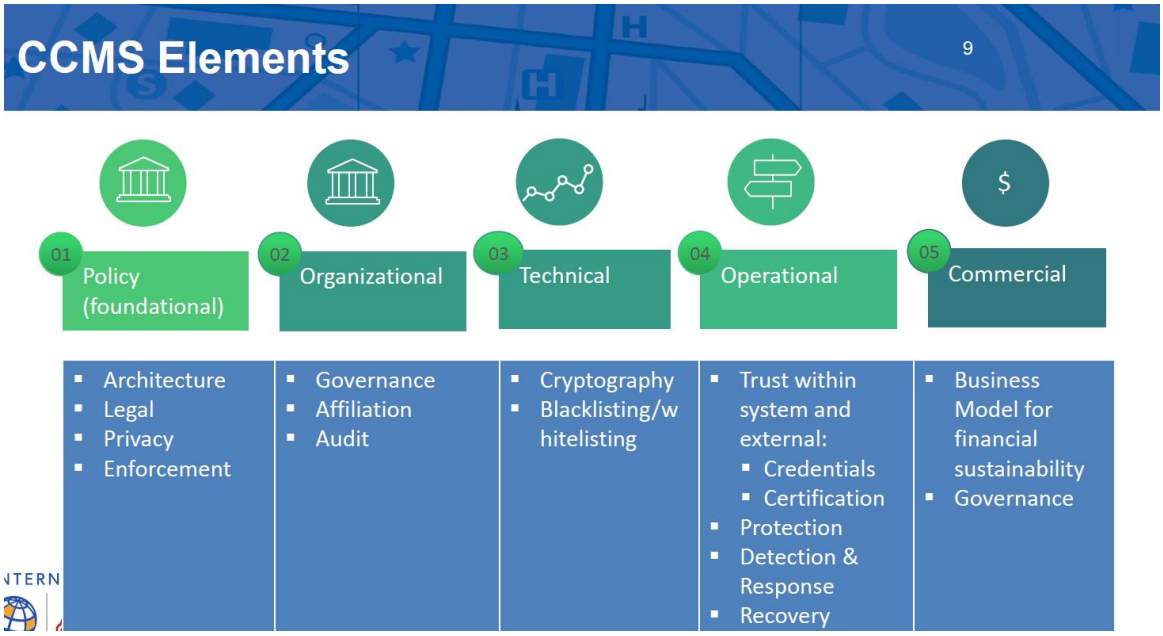
Japan (Highway Industry Development Organization, HIDO) started to participate in HTG only recently; it also joined the September 2017 meeting of HTG7 to discuss ongoing international collaboration on identifying and prioritising areas for alignment and harmonisation of C-ITS standards[6]. The Task Group reviewed Japanese C-ITS architecture and standards, successfully integrating Japanese service packages into the online Harmonised Architecture Reference for Technical Standards (HARTS) database, and further evolved HTG7's standards gap analysis.

C-ITS Credential Management System (CCMS)/Security Credential Management System (SCMS)

One of the key outcomes of HTG6 was designating a generic term for the operational and security framework for a C-ITS environment, the so-called C-ITS Credential Management System (CCMS) currently known as security trust models, and the Security Credential Management System (SCMS) (Harmonisation Task Group 6 2015a). An SCMS is based on a public key infrastructure (PKI), which consists of cryptographic technologies, standards, organisational and policy controls and procedures to provide security for exchanges of sensitive data. Figure 2.3 shows the main elements of a SCMS.

[6] TCA Quarterly Briefing, November 2017.

Figure 2.3: Main elements of a CCMS/SCMS



Source: Harmonisation Task Group 6 2017.

A comparative analysis of four security architectures yielded a common understanding of the fundamental elements of a CCMS (Harmonisation Task Group 6 2015b).

A SCMS is complex and has many components that have security requirements. The core components include certificate authorities (CAs), registration authorities (RAs), and ceremony rooms:

- Certificate authority (CA): Derives its authority from the trust anchor for the PKI, designated as the 'Root CA', and issues security certificates to other credential management entities in the SCMS in accordance with system policies and procedures.
- Registration authority (RA): Checks that requests for security certificates come from entities that are entitled to them and processes the requests.
- Ceremony room management/entity credential: The ceremony room is used for signing and verification of root certificates.

Public Key Infrastructure

C-ITS security is based on public key infrastructure (PKI) which provides security to address communications (the medium, messages/data, certificates, etc.), devices and structure (organisational, operational, and physical) (Harmonisation Task Group 6 2017). PKI can be implemented in varying ways to achieve different levels of security for data confidentiality, data integrity, authentication, non-repudiation and authorisation.

Each device has a credential that it cryptographically binds to a message (Harmonisation Task Group 6 2015a). Device and application certification processes, whatever they may be, are linked with credential management, and as such must be considered concurrently with the design of security management systems and procedures.

International SCMS harmonisation

An important consideration is international SCMS harmonisation. In a multi-SCMS world that supports a global transportation marketplace, trust will need to be defined beyond jurisdictional boundaries. The HTG6 team found a need for an international association, or federation, of SCMS managers for tasks related to international harmonisation.

High-priority areas for harmonisation include:

- cryptographic material
- SCMS components (e.g. CA, RA, ceremony rooms)
- organisational trust (e.g. intra-SCMS, inter-SCMS)
- additional privacy and security protections (e.g. certification).

Especially cross-border issues and harmonisation of trust constitute remaining challenges.

Europe and the USA are under way to define their SCMS and build their PKI (see also Section 2.3). Australian participants are considering options for a SCMS. A SCMS will be used in the Ipswich-based Cooperative and Automated Vehicle Initiative (CAVI) C-ITS pilot project developed by Queensland's Department of Transport and Main Roads[7]. Its readiness, safety role, governance, placement and administrative overhead on government and private industry will be studied through this project. The project is intended to:

- Analyse the impact that the introduction of an SCMS has on:
  - Australian transport authorities (organisational, operational and governance implications)
  - vehicle safety and security
  - Australian and state privacy legislation, and the implications and protections required thereof
  - C-ITS system performance.
- Prepare a research platform in order to inform future standards development for connected vehicle security threat detection and prevention (being performed in a separate though related iMOVE[8] project).

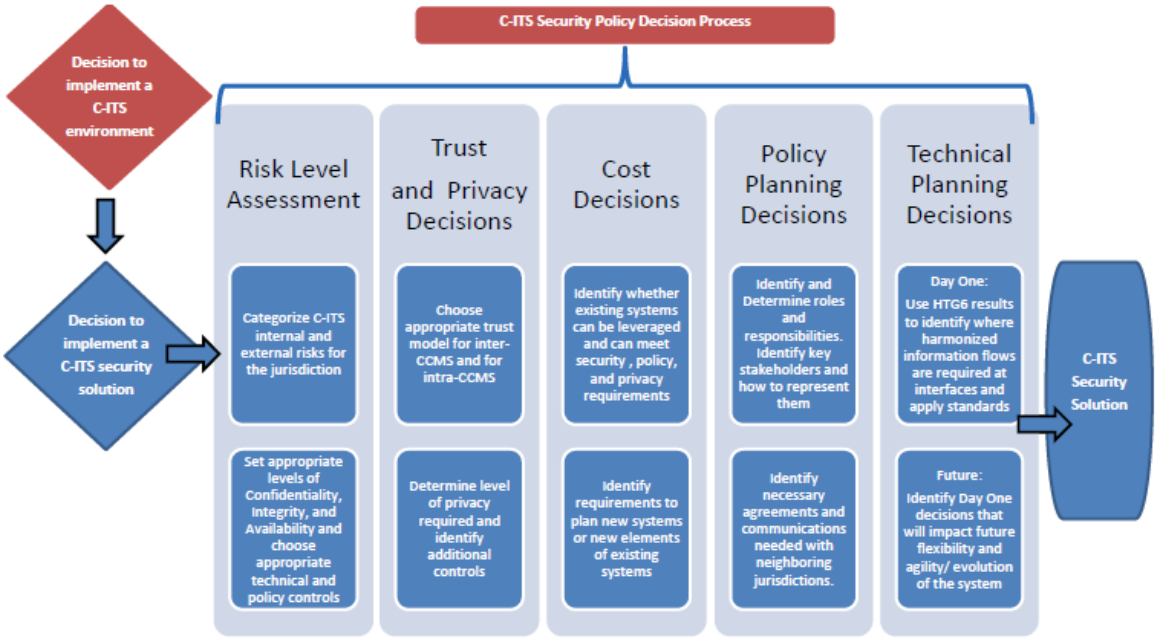
Other states (including New South Wales, Victoria and South Australia), at the time of writing of this report in July 2018, support Queensland in piloting an SCMS, rather than undertaking separate initiatives for their own C-ITS projects.

C-ITS Security Policy Decision Process

The HTG6 team identified a decision process that supports policy and decision makers in the early stages of planning for C-ITS security implementation (Figure 2.4).

[7] https://imovecrc.com/project/c-its-pilot-security-credential-management-system/
(visited 26 June 2018).
[8] The iMOVE Cooperative Research Centre (CRC) is a consortium of 44 industry, government, and research partners engaged in a concerted 10-year effort to improve Australia's transport systems through collaborative R&D projects.

Figure 2.4: C-ITS security policy decision process



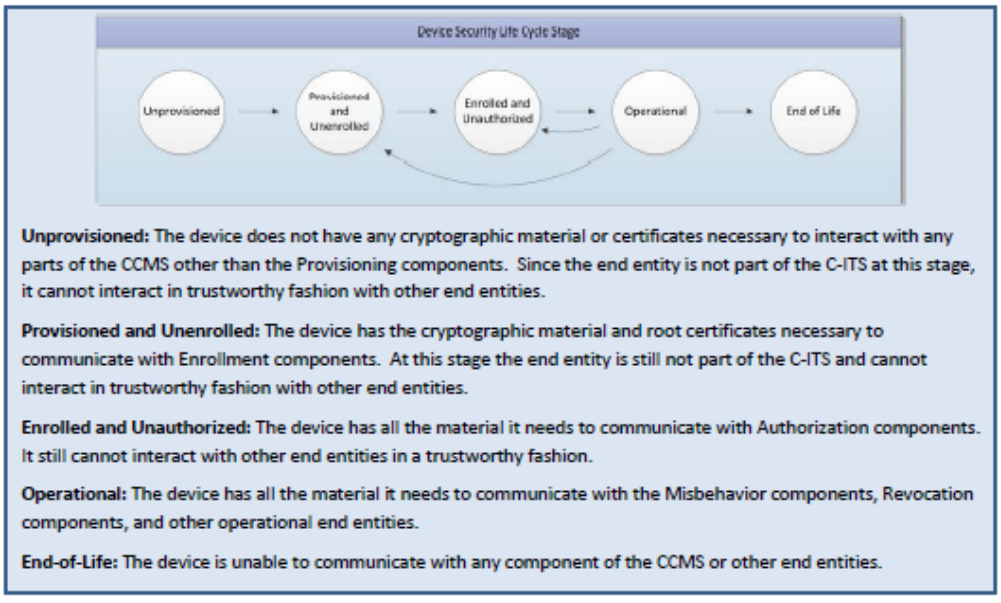
Source: Harmonisation Task Group 6 2015a.

C-ITS Life-cycle Aspects

C-ITS life-cycle aspects were raised in the security work of HTG[9].

Life-cycle requirements – both for the SCMS and the end-entity devices – must be brought into alignment, to support ongoing trust and interoperability. Applications and devices have a changing set of relationships with the CCMS depending on the life-cycle stage. A simplified version of the end-entity security life-cycle is depicted in Figure 2.5.

Figure 2.5: Simplified version of the end-entity security life cycle



Source: Harmonisation Task Group 6 2015a.

[9] C-ITS life cycle stages are being standardised in ETSI's ITS Security – Trust and Privacy Management (revision of TS 102 941).

Evaluation of the EU C-ITS platform related to security, privacy and data protection

In parallel with this project, Austroads is also undertaking a project titled *Evaluation of the European C-ITS Platform including a Threat, Vulnerability and Risk Analysis (TVRA).*

The key objectives of Austroads TVRA project are to:

- understand and evaluate the ETSI TVRA for the European C-ITS platform and put into the Austroads endorsed (Australian and New Zealand) context
- identify areas of Austroads interest that were not covered in the ETSI TVRA and provide high-level overview of the following:
  - central ITS stations
  - personal ITS stations
  - cellular communications
- identify areas of Austroads interest where further detailed examinations are required
- from an Austroads context and from both a technical and business perspective, outline the
  - G5 limitations of the EU TVRA
  - Institute of Electrical and Electronics Engineers (IEEE) / US aspects
  - developments since EU TVRA
  - hybrid communications paradigm and especially long-term evolution (LTE) considerations for broadband cellular network technologies (including 4G and upcoming 5G)
  - conformity assessment/certificate policy implications
  - expectations associated with the deployment and operation of European C-ITS.

For the CAF project, key findings of the TVRA project to date include:

- ANZ to follow formal and structured methods in analysis and testing.
- Recommendation is to follow HTG6 proposals identified in the literature review.
- Security should be a fundamental part of the architecture, and not an add-on.
- From a data ownership, safety and security perspective, extended vehicle (ExVe[10]) should not be the basis for critical ANZ ITS services.
- 5G is a new paradigm that could potentially be used to deliver C-ITS in the future.
- ANZ can accept European recommendations and continue to represent an example of a Europe-like solution.
- For the central ITS-S the role of core systems support needs to be considered and its paradigm determined politically.

2.2.2 C-ITS Trials and Pilots in ANZ

ANZ are both proactively undertaking connected and automated vehicle trials, representing the ANZ state of the art in terms of initial C-ITS deployment. As outlined on the Austroads website (Austroads 2017) the trials extend right across ANZ.

[10] Extending beyond the physical boundaries of the road vehicle and consists of the road vehicle, off-board systems, external interfaces and the data communication between the road vehicle and the off-board systems, as defined by ISO 20077-1:2017

Examples of current C-ITS trials include:

- Cooperative and Automated Vehicle Initiative (CAVI) in Queensland
- Cooperative Intelligent Transport Initiative (CITI) freight signal priority, public transport information and priority systems in New South Wales
- Australian Integrated Multimodal EcoSystem (AIMES) and ITS grant projects in Victoria.

A brief overview of some of the trials being undertaken in ANZ is outlined in Appendix B. Many of the trials focus on testing and demonstrating technologies, validating impacts and benefits, and increasing public awareness of C-ITS. No explicit information regarding conformity assessment of the ITS-stations to be used was found in publicly available information.

Austroads is an associate partner of C-Roads in Europe (cf. Section 2.3.1), and ANZ trials will seek to leverage this.

2.2.3 Safety Assurance System for Automated Vehicles

The National Transport Commission (NTC) works to ensure the best productivity and safety outcomes from rapidly evolving technology in the field of C-ITS policy implementation and automated vehicles (AVs) (National Transport Commission 2017b). The NTC policy paper on assuring the safety of automated vehicles (National Transport Commission 2017a) represents an input to the development of the C-ITS CAF in ANZ due to (a) a large overlap of stakeholders and (b) similar questions to be answered in the process of the high-level design.

The policy paper (National Transport Commission 2017a) evaluated the following four safety assurance regulatory options for AVs in Australia:

1. Continue current approach
2. Self-certification
3. Pre-market approval
4. Accreditation.

It sets out the high-level design of a safety assurance system for automated vehicles in Australia by recommending that it is based on mandatory self-certification until the development of international standards for AV systems (see also Table 2.1). It identifies key steps to implement the safety assurance system by 2020, including legislative and registration changes and the development of administrative functions.

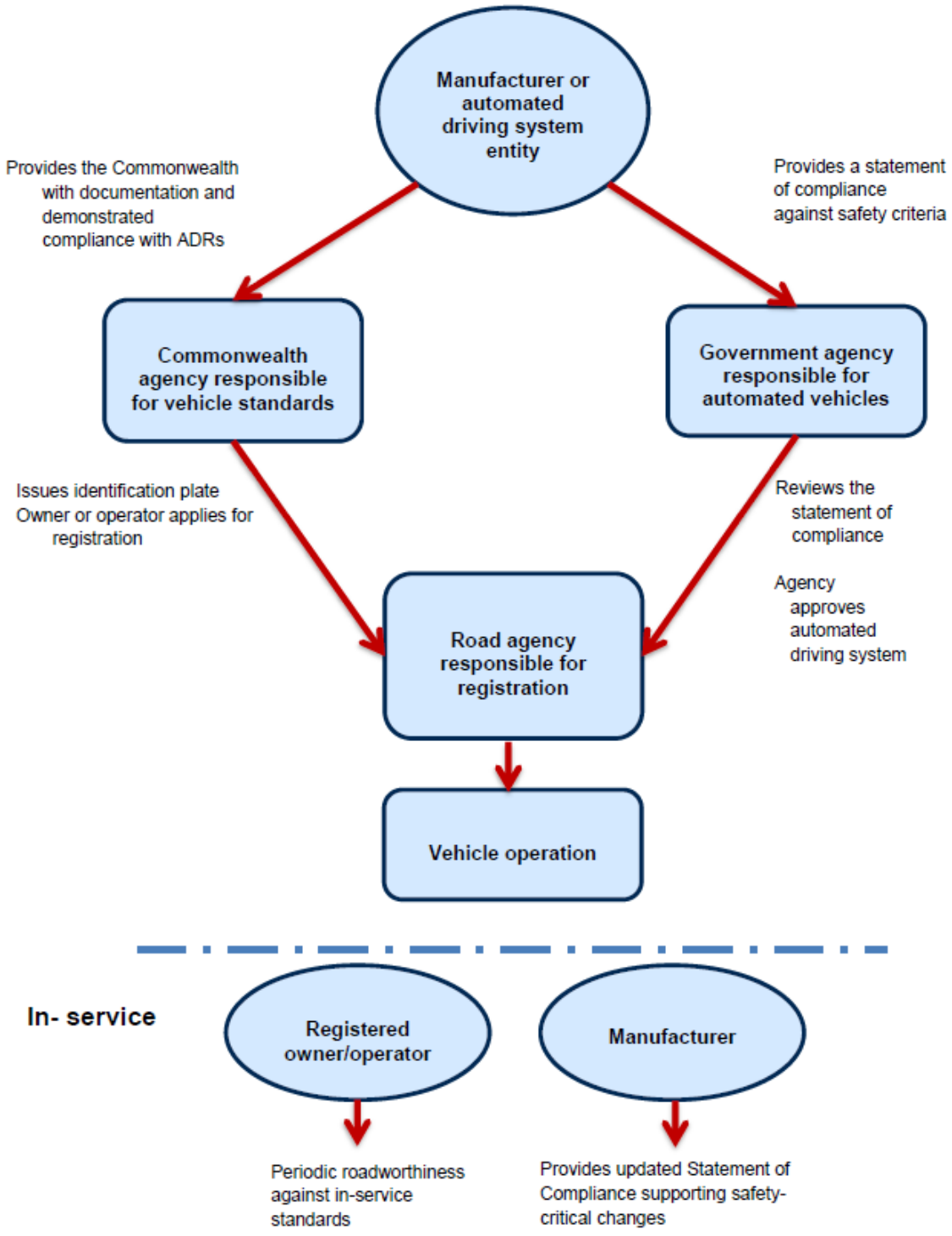
Table 2.1: Design features of the proposed safety assurance system

1. The safety assurance system will be administered by a government authority, preferably on a national basis. Approval decisions may be made on the advice of a single national government panel consisting of the Commonwealth, states and territories, the NTC, the National Heavy Vehicle Regulator (NHVR) and Austroads.
2. The safety assurance system will manage principles-based safety criteria that capture key safety risks associated with automated vehicles. The safety criteria should include matters relating to:
    i. the safe operational design domain of the vehicle
    ii. the human–machine interface
    iii. on-road behavioural competency, including compliance with traffic law, interaction with vulnerable road users
    iv. cybersecurity
    v. driver training
    vi. the provision of data, including interaction with enforcement agencies.
3. Automated driving system entities (such as manufacturers) will be required to submit a Statement of Compliance that demonstrates how each of the agreed safety criteria has been managed. A Statement of Compliance must be submitted and approved before the relevant automated driving system or function can be introduced into the market.
4. The automated driving system entity remains responsible for testing and validating the safety of the automated driving system or function. The role of government in the safety assurance system is to satisfy itself that the applicant has processes in place to identify and manage the safety risks. It is not envisaged that the safety assurance process will conduct independent testing or validation activities.
5. To support national consistency and cross-border travel, state and territory road managers will be notified of a safety assurance outcome, but approval of a road manager should not be required for the automated driving system to operate unless the automated driving system forms part of a vehicle that would otherwise require a permit or exemption to access the road network. This is consistent with the current arrangements for new light vehicles.
6. All in-service modifications to the automated driving system that have a **significant** impact on safety performance or material compliance with the original safety assurance system approval, including over-the-air software updates of the vehicle, are anticipated to require approval by the safety assurance system before that **significant** modification is introduced into the market.

Source: National Transport Commission 2017a.

Figure 2.6 illustrates in a simplified way how the safety assurance could interact with existing regulatory mechanisms, but the finalised process will depend on the legislative option that is adopted.

Figure 2.6: How the safety assurance system for automated vehicles could work



Source: National Transport Commission 2017a.

Under mandatory self-certification, industry, rather than government, will be responsible for testing and validating the safety of the automated driving system and documenting these processes. The role of the government would be to satisfy itself that the applicant has the processes in place to identify and manage safety risks. In this proposal, it is not envisaged that the safety assurance process will conduct independent testing or validation activities.

Australia's approach to a safety assurance system for automated vehicles is the subject of a Consultation Regulation Impact Statement (RIS), which opened for public consultation on 15 May 2018 (National Transport Commission 2018). Submissions for the RIS could be made until Monday 9 July 2018. The RIS seeks feedback on what role Australian governments will play in assuring the safety of automated driving systems, and what form a safety assurance system would take. The RIS has proposed 11 safety criteria that automated driving system entities would need to self-certify against, which include among others aspects of safety system design, compliance with road traffic laws, requirements around system upgrades, testing for the Australian road environment, and cyber security. Following consultation, the NTC is now preparing a Decision RIS for consideration by Australia's transport ministers in November 2018. The NTC is aiming to develop end-to-end regulation to support the safe commercial deployment of automated vehicles in Australia by 2020.

2.2.4 Vehicle Standards and Regulations in ANZ

Australia is involved in the World Forum for Harmonisation of Vehicle Regulations (UNECE WP.29), including development of new and updated vehicles standards. Cybersecurity and data protection are being addressed within WP.29 primarily under the broader intelligent transport systems and automated driving discussions.

The Australian Design Rules (ADRs, Australian Government 2017a) are Australia's national technical standards for vehicle safety under the responsibility of Commonwealth Department of Infrastructure, Regional Development and Cities (DIRDC).

The Australian Government's policy is to harmonise the national vehicle safety standards with international regulations where possible and consideration is given to the adoption of the international regulations of the United Nations Economic Commission for Europe (UNECE). Australia is a signatory to the *UNECE 1958 Agreement* and the *1998 Agreement* (UNECE 1998).

The ADRs are largely based on the European (ECE) vehicle regulations promulgated by the World Forum (WP.29). The ADRs include conformity of production requirements and audits of evidence. The Australian certification system for new vehicles is a type approval, wherein a vehicle design representing a make-model (the 'type' of vehicle) undergoes tests to demonstrate compliance with the safety and emissions standard. However, the Government does not test vehicles for certification purposes. The manufacturer is responsible for ensuring compliance with the ADRs. The Australian certification process allows the vehicle manufacturer to conduct the various ADR tests locally and also accepts tests conducted under the ECE system of type approval. The manufacturer certifies that its vehicle and regulated vehicle components comply with all applicable provisions of applicable ADRs in effect at the date of manufacture.

In this context it should be pointed out that the ADRs govern only some technical aspects of vehicle design, whereas many are left to the vehicle manufacturer to ensure safe design. The ADRs also include conformity of production requirements, and audits of evidence. So, while they have an element of self-certification, there are also elements of government certification. Safety-related defects are covered by recall provisions that can require a product to be removed from the market and fixed if it is not safe for use in transport. This is supported by a code from the Federal Chamber of Automotive Industry (FCAI) on how it supports the recall of vehicles.

Overall, a direction towards further harmonisation of international vehicle standards and the move towards 'international whole vehicle type approval' where a vehicle is approved as complying with an agreed set of regulations can be noticed. The new Commonwealth vehicle importation legislation (*Road Vehicle Standards Bill*) will also allow for overseas approval of vehicles to Australian standards.

The *Compliance and Enforcement Strategy* of the *Motorway Vehicles Standards Act 1989* (December 2017, Australian Government 2017b) outlines how Australia will conduct compliance and enforcement activities to fulfil their role of regulating the first supply of road vehicles in Australia.

The compliance and enforcement activities are undertaken in accordance with the principles shown in Table 2.2.

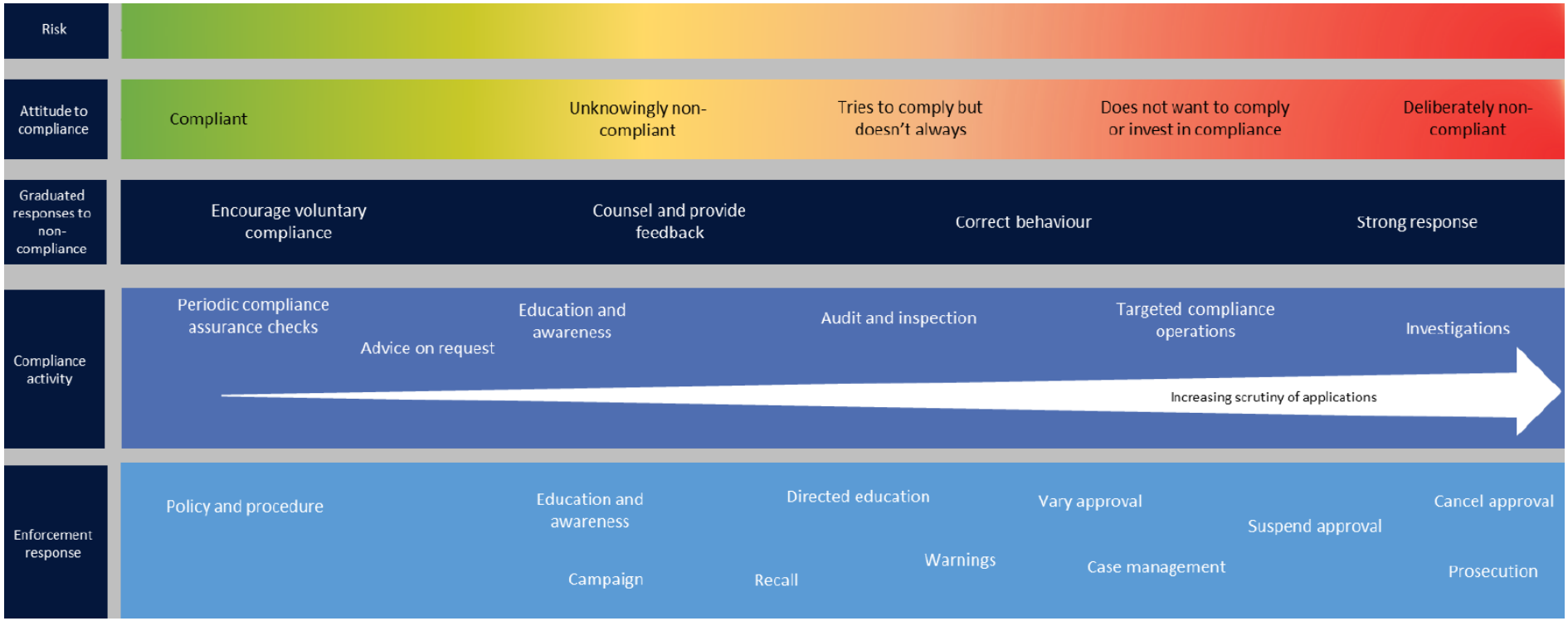
Table 2.2: Compliance and enforcement principles

Risk-based	Our compliance activities will be risk-based to ensure resources are effectively allocated towards addressing the most serious and systemic risks
Proportionate	Our compliance activities and enforcement responses will be proportionate to the risk being managed
Outcomes focussed	Our compliance and enforcement activities will be outcomes focussed, prioritising resources towards the greatest potential risks to regulatory outcomes with a view to improving overall compliance
Consistent	Our compliance activities and administrative decision making will be consistent and in accordance with documented procedures
Fair and transparent	We will be fair, open and transparent in relation to our decisions and compliance activities and will communicate with regulated entities in a clear, and effective manner
Voluntary compliance	We will promote and encourage a culture of voluntary compliance amongst regulated entities
Efficient	Our compliance activities will be streamlined and coordinated to reduce unnecessary impost on regulated entities and the department

Source: Australian Government 2017b.

The compliance continuum reflects a range of activities and enforcement responses to achieve and enforce compliance ranging from light touch (such as education) to a stronger approach (e.g. investigations and prosecution) (Figure 2.7).

Figure 2.7: Compliance and enforcement continuum



Source: Australian Government 2017b.

The New Zealand Transport Agency sets out requirements to control the entry of vehicles into, and operation of vehicles in, the land transport system in *Land Transport Rule: Vehicle Standards Compliance 2002* (NZ Transport Agency 2002). It is noted that the regulations are based on a type approval issued by a relevant authorised certification organisation in accordance with the approved vehicle standards. Although NZ accepts Australian standards and will usually follow the ADRs, it also accepts vehicles built to Japanese, European and US standards.

2.2.5 Linkage to Other Initiatives in ANZ

ANZ Approach to regulation

The Australian Government has issued a *Guide to Regulation* (Australian Government 2014) 'that is intended to be read by every member of the Australian Public Service involved in policy marking – from the most junior member of the policy team to the departmental secretary. It provides the context for regulation and encourages policy makers to think about regulatory impacts early in the policy process.'

New regulation is to be considered as a last resort; policy makers are encouraged to develop and make use of alternative instruments in shaping the rules of the market.

Compliance of products and services in the ANZ market with standards is normally voluntary. Regulation may be considered if the associated standard relates to safety or addresses environmental or consumer protection issues.

The Guide contains seven options for regulatory approaches:

1. The most important policy option: the no-regulation option
2. Better enforcement of existing regulation
3. Light-touch regulation
4. Self-regulation
5. Quasi-regulation
6. Co-regulation
7. Explicit government regulation.

It also highlights alternative instruments that might be used to address the problem or the issue that a regulatory approach is supposed to resolve:

- no specific action – that is, relying on the market in conjunction with existing general liability laws (e.g. negligence or breach of contract) and insurance laws
- information and education campaigns, including product labelling or media campaigns
- pre-market assessment schemes, such as listing, certification and licensing
- post-market exclusions like bans and recalls
- service charters
- standards, which may be voluntary, compulsory or performance-based
- other mechanisms like public registers, mandatory audits and quality assurance schemes.

It includes ten principles for Australian Government policy makers, including the need to underpin the legislative option by means of a regulation impact statement (RIS).

The Government of New Zealand has issued *Government Expectations for Good Regulatory Practice* (Government of New Zealand 2017). The guide includes general rules of thumb about what makes a good regulatory system and what is good stewardship practice for a regulatory agency. The Government expects any regulatory system to be an asset for New Zealanders, not a liability. Hence, a regulatory system should deliver, over time, a stream of benefits or positive outcomes in excess of its costs or negative outcomes.

ANZ National policy frameworks for land transport

- *National Policy Framework for Land Transport Technology – Action Plan: 2016-2019* (Transport and Infrastructure Council 2016)

This document outlines in detail Australia's approach to emerging transport technologies (including ITS) for the timeframe 2016-2019 and builds on previous work by the Council in its 2011 *Policy Framework for Intelligent Transport Systems in Australia* (Transport and Infrastructure Council 2011*)*. Regarding C-ITS, it states that 'this technology has an exciting potential to improve safety by providing drivers with warnings of imminent collisions or dangerous conditions ahead'. Australian governments are preparing for the introduction of C-ITS equipped vehicles in Australia (including addressing security and geo-positioning requirements).

The document also includes the *National Transport Technology Action Plan (2016-2019)*, which outlines Australia's national priorities for implementing new transport technologies identified and agreed through discussions between Australian governments and with industry. It includes the following action items relevant to C-ITS:

- develop a connected vehicle (cooperative ITS) infrastructure road map (TISOC)
- publish a connected vehicle (cooperative ITS) statement of intent on standards and deployment models (TISOC/Commonwealth)
- develop a nationally agreed deployment plan for the security management of connected and automated vehicles (TISOC/Austroads).

- *Intelligent Transport System Technology Action Plan 2014-2018* (New Zealand Government 2014)

This plan sets out the government's proposed work program on ITS for the timeframe 2014-2018. Regarding C-ITS, it emphasises the desire for government to set timely standards that ensure industry can plan for ITS implementation. Incompatibility between standards for ITS, especially for C-ITS, may have great implications for New Zealand, as for the past decade roughly half the vehicles entering the fleet have been built to European standards and half to Japanese standards (with a few percent from the USA as well). An example of a standard to be set in law is the communication frequency used in C-ITS (see also Section 2.2.1). Australia has adopted the 5.9 GHz range allocated in the EU, so there is good reason for New Zealand to adopt the same C-ITS frequency range. Proposed government actions on transport standards include, among others, taking part in international standard development processes (e.g. ISO TC 204) and promoting harmonisation and open standards and interoperability of technologies at an international level.

The New Zealand Ministry of Transport is currently updating the government's technology and innovation work program. This will include the production of a CAV road map.

Overall, C-ITS, having an international context, makes it crucial to view the C-ITS compliance assessment framework at an international level, and also to identify areas where harmonisation is needed. For New Zealand this could mean seeking to align its C-ITS standards with those in Australia, but also seeking to share administrative and legal approaches with Australia – where sensible.

Regulatory Compliance Mark and associated requirements

The regulatory compliance mark (RCM) process sets out the compliance requirements for electronic and electrical equipment (Comtest Laboratories 2017). Testing, test reports, standards, approvals, compliance levels and declarations of compliance are mandatory requirements as per previous arrangements for electrical safety approvals and Australian Communications and Media Authority (ACMA) requirements.

The RCM system is based on a common national database used by the Electrical Regulatory Authority Council (ERAC) and the ACMA in Australia, and Radio Spectrum Management (RSM) in NZ for the purpose of registration.

The RCM is a visible indication (Figure 2.8) of a product's compliance with all applicable ACMA regulatory arrangements, including all technical and record-keeping requirements. ACMA's regulatory requirements cover electrical safety, electromagnetic compatibility (EMC), and electromagnetic energy (EME) requirements.

Figure 2.8: RCM mark

Source: ACMA 2017b.

Product labelling (ACMA 2017b)

The final step to product compliance involves labelling the product. Steps to compliance are:

1. Identify the applicable labelling notice.

2. Identify the applicable technical standards (prescribed in the relevant labelling notice) and the testing requirements.

3. Demonstrate product compliance.

4. Complete a declaration of conformity (DoC) and maintain compliance records.

5. Register as a 'responsible supplier'.

6. Label the product.

The RCM must not be applied to a product until the supplier has registered on the national database and complied with all other regulatory requirements.

The ACMA regulatory arrangements require a supplier to apply a compliance label to a product **before** the product is supplied to the Australian market. When all steps to compliance are complete, the product may be supplied to the Australian market. New Zealand has a similar regime.

The ACMA takes a risk-based approach to product compliance. If non-compliance of a product is identified, the ACMA may conduct targeted auditing and may seek to examine a supplier's compliance records.

The RCM system has some noticeable differences compared with the European EC mark. The RCM system requires that **only** Australian or New Zealand importers and manufacturers have the authority to sign the 'Supplier Declaration of Conformity' and can authorise the placement of the RCM logo onto products (Comtest Laboratories 2017).

Overall, the RCM is deemed relevant for ITS stations in ANZ with regard to electrical safety, electromagnetic compatibility (EMC), electromagnetic energy (EME) requirements.

Equipment compliance and labelling requirements related to EMC, radiocommunications and electromagnetic radiation – ACMA and FCAI agreements

ACMA has granted members of the FCAI, that comply with the FCAI's "Voluntary Code of Practice for Electromagnetic Compatibility (EMC)", exemptions from both the ACMA's equipment compliance and compliance labelling requirements. This exemption is included in Schedule 2 of the *Radiocommunications Labelling (Electromagnetic Compatibility) Notice 2017* (ACMA 2017c). However, if an FCAI member choses not comply with the FCAI's "Voluntary Code of Practice for Electromagnetic Compatibility (EMC)", it **must** comply with the ACMA's equipment compliance and compliance labelling requirements.

In addition to the above EMC exemption, the ACMA has also exempted FCAI members from the ACMA's compliance labelling requirements, but **not** the compliance requirements included in;

- *The Radiocommunications Devices (Compliance Labelling) Notice 2014* (ACMA 2014a) - provided that the device complies with the requirements of the applicable ACMA mandated radiocommunications standard and addresses any applicable radiocommunications licencing requirements. In the case of high and medium risk radiocommunications devices, the requirement to establish compliance records, included in this notice, must be complied with – no compliance records are required for low risk devices, and
- The *Radiocommunications (Compliance Labelling - Electromagnetic Radiation) Labelling Notice 2014* (ACMA 2014b) - provided that the device complies with the requirements of the applicable ACMA mandated electromagnetic radiation standard. The requirement to establish compliance records, included in this notice, must be complied with.

FCAI members are **not exempt** from the equipment compliance and compliance labelling requirements included in the *Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2015* (ACMA 2015).

ANZ Security Frameworks

The following frameworks and guidance documents reflect security-related best practice in ANZ:

- the Common Criteria Recognition Arrangement (CCRA) based on the evaluation criteria for IT security based on the ISO/IEC 15408 series (also known as the Common Criteria)
- the ISO/IEC 27000 standards series on information security management systems
- the public key infrastructure (PKI) gatekeeper framework, under the responsibility of the Australian Digital Transformation Office (https://www.dta.gov.au/standard/design-guides/authentication-frameworks/gatekeeper-public-key-infrastructure-framework/), intended as a key enabler of online government services.

In particular the first two appear to be more broadly adopted by the ANZ stakeholders in C-ITS.

Common Criteria Recognition Arrangement (Common Criteria Portal 2017)

The participants in this arrangement share the following objectives:

- 'to ensure that evaluations of information technology (IT) products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles
- to improve the availability of evaluated, security-enhanced IT products and protection profiles
- to eliminate the burden of duplicating evaluations of IT products and protection profiles
- to continuously improve the efficiency and cost-effectiveness of the evaluation and certification/validation process for IT products and protection profiles.'

The purpose of this arrangement is to advance the objectives by bringing about a situation in which IT products and protection profiles which earn a Common Criteria certificate can be procured or used without the need for further evaluation. It seeks to provide grounds for confidence in the reliability of the judgements on which the original certificate was based by requiring that a certification/validation body (CB) issuing Common Criteria certificates should meet high and consistent standards.

The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that:

- 'products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance
- supporting documents are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies
- the certification of the security properties of an evaluated product can be issued by a number of certificate authorising schemes, with this certification being based on the result of their evaluation
- these certificates are recognised by all the signatories of the CCRA.'

The CC is the driving force for the widest available mutual recognition of secure IT products. The CC web portal is available to support the information on the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news and events.

The certificate authorising members include Australia's Signals Directorate and New Zealand's Defence Signals Directorate (www.asd.gov.au/infosec/aisep).

Common Criteria licensed laboratories, including Australian ones, can also be found on the CC web portal (https://www.commoncriteriaportal.org/labs/).

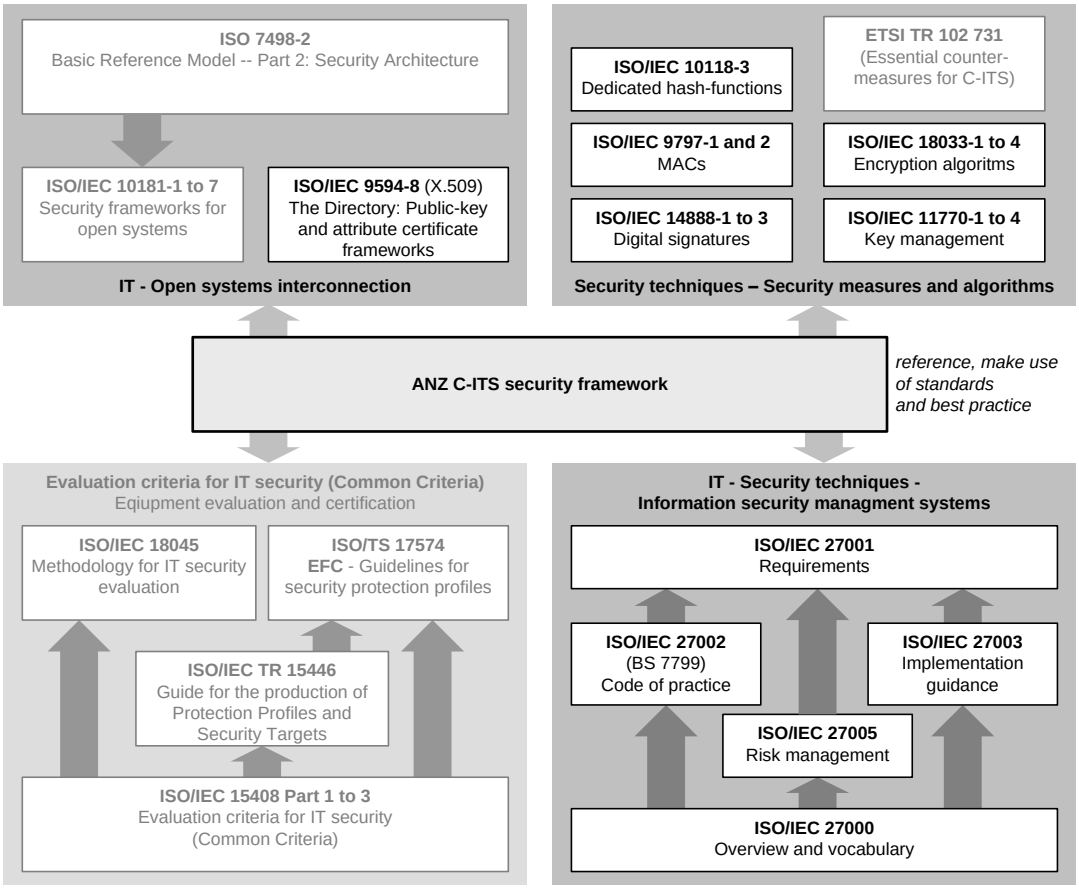
ISO/IEC 27000 standards series

The ISO/IEC 27000 series define requirements and guidelines for the implementation of security management systems for all types of organisation. The standards are particularly relevant for the security solutions of central systems and other fixed or installed equipment including the software of (C-)ITS systems.

Security-related standards and general development path for security-related documents

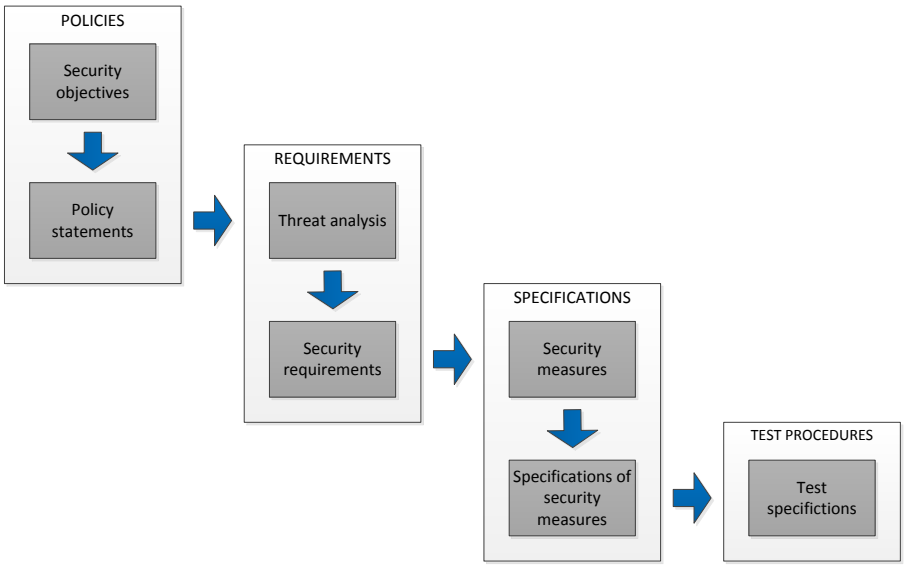
Figure 2.9 illustrates potentially relevant security-related standards and their relationship to a C-ITS security framework, whereas Figure 2.10 shows a general road map for developing security-related documents.

Figure 2.9: Potentially relevant standards and their relation to a C-ITS security framework



Source: Modified Figure 4 in ISO/TS 19299:2015.

Figure 2.10:General development path for security-related documents



Source: ISO/TS 19299:2015.

Federal Chamber of Automotive Industries

The Federal Chamber of Automotive Industries (FCAI), comprising vehicle manufacturers and importers, has indicated a desire to follow European standards for C-ITS (Section 4.3.2 in Austroads 2015b) as have the NZ equivalent for vehicle importers (the Motor Industry Association Inc and Imported Motor Vehicle Industry Association Inc).

It is also important to note FCAI's *Code on Guiding Principles for Privacy and Cooperative Intelligent Transport (C-ITS) Systems* which have been set out to give consumers confidence that their privacy is properly protected (FCAI 2017).

Moreover, FCAI has a voluntary code of practice for EMC, which includes an agreement with ACMA that FCAI members are exempt from ACMA compliance labelling requirements. It addition to the EMC exemption, the ACMA has also exempted FCAI members from the ACMA's compliance labelling requirements related to radiocommunications and electromagnetic radiation. See *Equipment compliance and labelling requirements related to EMC, radiocommunications and electromagnetic radiation – ACMA and FCAI agreements* above for further details.

2.3 Global C-ITS Developments

Overall, C-ITS deployment is in its infancy with Europe and the USA leading the developments, pushed by the industry. Policy makers try to create favourable market and regulatory conditions, so that society can start to reap the benefits from the emerging C-ITS services. Large-scale C-ITS trials and early deployments are being implemented and put into service. Europe and the USA have come relatively far in defining their SCMS, which are essential enablers for large-scale deployment. The following sections present the main elements for describing the C-ITS state of play in Europe and the USA.

2.3.1 EU C-ITS State of Play

European framework and rules for placing of products on the EU market

To improve the internal market for goods and strengthen the conditions for placing a wide range of products on the EU market, the new legislative framework (NLF) was adopted in 2008[11]. It is a package of measures that aim to improve market surveillance (including the revision of the safeguard clause procedures) and boost the quality of conformity assessments. It also clarifies the use of CE marking and creates a toolbox of measures and a template for use in product legislation. It includes definitions of terms commonly used in product legislation, and procedures to allow future sectorial legislation to become more consistent and easier to implement.

A main objective of the European Commission is to achieve a better alignment of product legislation across different sectors. There are currently some 20 different directives and regulations that have been aligned with the NLF approach[12], including the Radio Equipment and Low Voltage Directives (RED and LVD). The operation of EU harmonisation legislation under the NLF approach requires harmonised standards to offer a guaranteed level of protection with regard to the essential requirements established by the legislation.

The principle of reliance on standards in technical regulations has been adopted by the World Trade Organisation (WTO). In its *Agreement on Technical Barriers to Trade* (TBT), it promotes the use of international standards[13].

Mutual recognition agreements (MRAs) promote international trade in goods and facilitate market access[14]. They are bilateral agreements and aim to benefit industry by providing easier access to conformity assessment. These agreements lay down the conditions under which one party will accept conformity assessment results (e.g. testing or certification) performed by the other party's designated conformity assessment bodies (CABs) to show compliance with the first party's (non-member country) requirements and vice versa.

Two important elements of every legislative act covering products are:

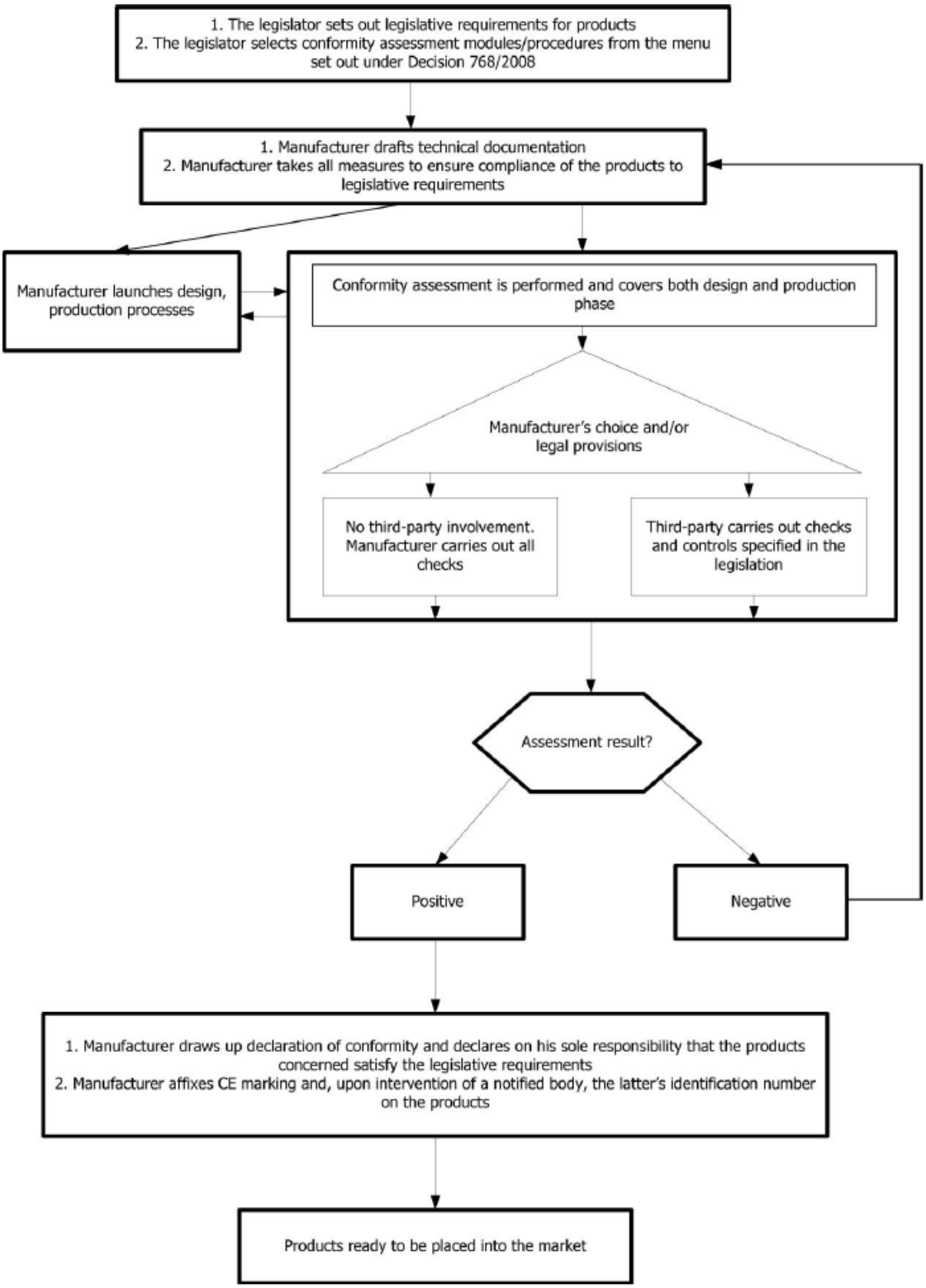
- the legislative requirements governing the characteristics of the products covered
- the conformity assessment procedures the manufacturer carries out in order to demonstrate that a product, before it is placed on the market, conforms to these legislative requirements. A product is subjected to conformity assessment both during the design and in the product phase.

[11] It consists of a) Regulation (EC) 765/2008 setting out the requirements for accreditation and the market surveillance of products, b) Decision 768/2008 on a common framework for the marketing of products, which includes reference provisions to be incorporated whenever product legislation is revised, and c) Regulation (EC) 764/2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another EU country.
[12] http://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en.
[13] 2.4 of the WTO TBT Agreement.
[14] http://ec.europa.eu/growth/single-market/goods/international-aspects/mutual-recognition-agreements/. The agreements between ANZ and the EU include e.g. automotive products, EMC and low voltage equipment.

Conformity assessment flowchart and principles

Figure 2.11 illustrates the position of conformity assessment in the supply chain when placing equipment on the EU market.

Figure 2.11: Conformity assessment flowchart for placing of equipment on the market



Source: European Commission 2016b.

Conformity assessment principles for placing of equipment on the EU market include:

- Legislation should be limited to the essential requirements.
- Harmonised standards for products meeting the essential requires can be applied alongside the legislation.
- The application of harmonised standards is voluntary but has the advantage of giving 'presumption of conformity'.
- A conformity assessment involving a notified body shall be used, if such harmonised standards are partially applied or not applied or do not exist.
- Compliance is assessed with regard to the legal requirements applicable at the time of the first making available.

Conformity assessment vs market surveillance

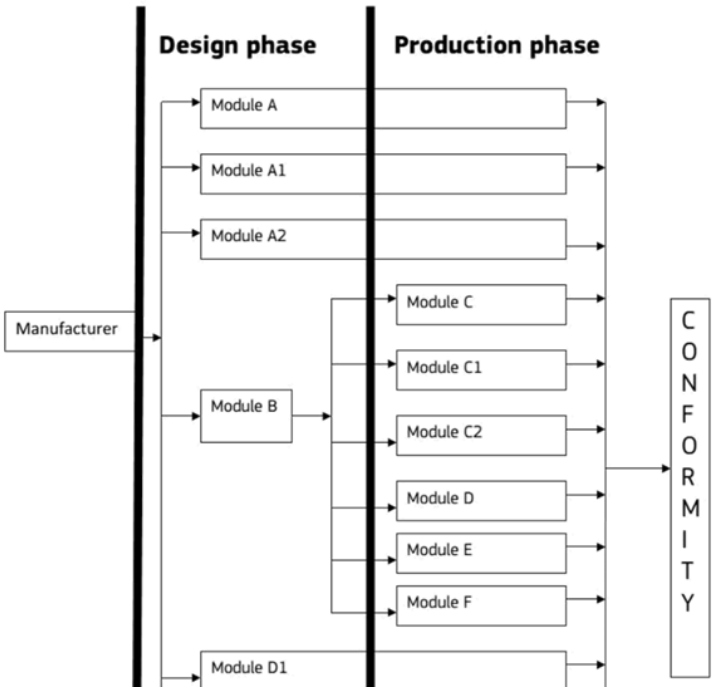
The most important change brought about by the NLF to the legislative environment of the EU was the introduction of a comprehensive policy on market surveillance. This has considerably changed the balance of EU legislative provisions from being fundamentally oriented at setting product-related requirements to be met when products are placed on the market to an equal emphasis on enforcement aspects during the whole life-cycle of products.

Conformity assessment is the responsibility of the manufacturer and must not be confused with market surveillance, which consists of controls by the national market surveillance authorities after the product has been placed on the market. Both techniques are complementary and equally necessary to ensure the protection of the public interests at stake and the smooth functioning of the internal market.

Two-step Procedure: Design and Production

In EU harmonisation legislation, conformity assessment procedures cover both design and production phases (Figure 2.12). They are composed of one or two modules. Some modules cover both phases. In other cases, distinct modules are used for each phase.

Figure 2.12: Overview of the conformity assessment modules



Source: Extract from p. 71 in European Commission 2016b.

The conformity assessment procedure may be in the following two steps (EU-type examination), deemed particularly relevant for C-ITS stations in view of the expected volume involved:

- examination of the conformity of a specimen or the design of the concerned product (i.e. type approval)
- determination of the conformity of the manufactured products against the approved specimen (e.g. by means of production control, product check at random intervals).

In cases where there is no EU-type examination, the conformity assessment procedure is composed of one two-phase (design and production) module (e.g. conformity based on unit verification).

The rationale for selection of the appropriate modules is:

- The legislator should avoid modules too onerous for the objectives of the EU harmonisation legislation concerned, without however compromising the protection of the public interest.
- The complexity of the modules selected should be proportional to the risk (impact on public interest, health, safety, and environment) of the product, its design complexity, the nature of its production (large series vs small series, custom-made, simple vs complex production mechanism etc.).

EC C-ITS strategy and preparation of an EU delegated regulation on C-ITS

The European Commission (EC) in 2016 released a European strategy on C-ITS, a milestone towards cooperative, connected and automated mobility (European Commission 2016a). This C-ITS strategy is seen as an important milestone for cooperative, connected and automated vehicles.

Following the recommendations of the C-ITS Platform, the EC has identified issues which should be tackled at EU level to ensure coordinated deployment of C-ITS services in 2019:

- priorities for deployment of C-ITS services (i.e. Day 1 ‘hazardous location notifications’ and ‘signage applications’ and Day 1.5 C-ITS services including vulnerable road user protection)
- security of C-ITS communications (including trust model, certificate policy and governance model)
- privacy and data protection safeguards
- communication technologies and frequencies (hybrid communication approach, e.g. ITS-G5 and LTE-V2X)
- interoperability at all levels (C-Roads platform for testing, validation and ensuring interoperability of Day 1 C-ITS services)
- compliance assessment (for Day 1 C-ITS services), legal framework, international cooperation (promoting international standardisation e.g. vehicle regulation and traffic rules in UNECE)
- legal framework.

Day 1 C-ITS services:

Hazardous location notifications:

  - slow or stationary vehicle(s) and traffic ahead warning
  - roadworks warning
  - weather conditions
  - emergency brake light
  - emergency vehicle approaching
  - other hazards.

Signage applications:

- In-vehicle signage
- In-vehicle speed limits
- Signal violation/intersection safety
- Traffic signal priority request by designated vehicles
- Green light optimal speed advisory
- Probe vehicle data
- Shockwave damping (falls under European Telecommunication Standards Institute (ETSI) category 'local hazard warning').

Day 1.5 C-ITS services:

- Information on fuelling and charging stations for alternative-fuel vehicles
- Vulnerable road user protection
- On-street parking management and information
- Off-street parking information
- Park and ride information
- Connected and cooperative navigation into and out of the city (first and last mile, parking, route advice, coordinated traffic lights)
- Traffic information and smart routing.

C-ITS Platform

The Platform for the Deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS Platform), launched by the EC in July 2014, was created with the clear intention to support the emergence of a common vision, provide an operational instrument for dialogue, exchange of technical knowledge and cooperation on technical, legal, organisational, administrative and governing aspects.

The C-ITS Platform represents all the key stakeholders along the value chain including the EC, public stakeholders from member states and local or regional authorities, road operators, vehicle manufacturers and suppliers, service providers, and telecommunications companies. The objective of the C-ITS platform is to identify and agree on how to ensure interoperability of C-ITS across borders and along the whole value chain. The objective is also to identify the most likely and suitable deployment scenario(s), including e.g. the first V2V and V2I services to be deployed across the EU.

A first phase of the C-ITS Platform (Phase I) led to the adoption of the *C-ITS Platform* report in January 2016 (C-ITS Platform 2016) with policy recommendations and proposals for action for both the EC and other relevant actors along the C-ITS value chain.

Nine topics were further analysed and discussed in the second phase of the Platform (Phase II, from July 2016 to September 2017) in corresponding working groups, gathering around 200 experts, on a monthly basis.

A third phase of the C-ITS Platform is not planned, although many topics are still in progress.

Recent and upcoming EC activities related to C-ITS

In the beginning of September 2017, the EC conducted a stakeholder workshop on the 5.9 GHz band discussions. In October 2017 the Radio Spectrum Committee had adopted a new mandate for the European Conference of Postal and Telecommunications Administrations (CEPT[15]) to study the 5.9 GHz band for road-safety-related ITS services. The mandate has been adopted by the member states. CEPT will study the co-existence issues in the 5.9 GHz band, based on the four guiding principles that the EC has formulated and recognising all the activities that are currently already being deployed in Europe.

In relation to C-ITS security, the EC has published Release 1 of the *Common European Certificate Policy* (available on the DG MOVE website[16]) as a guidance document in June 2017[17]. The security policy Release 1 was published in December 2017. The EC will operate a four-year pilot phase of a C-ITS Security Credential Management System (CCMS, including operational Trust List Manager, Central Point of Contact and an EU Root CA) open to all stakeholders. The activities started in January 2018 and will be carried out by the EC. In this context, close cooperation with the European standards organisations (ESOs) will be needed to ensure an effective set-up of these security elements for the EU. The EC stresses the importance of a timely update of ETSI TS 102 941 (*Trust and Privacy Management*) ensuring compliance with the certificate policy and consistency with ETSI TS 103 097 (*Security Header and Certificate Formats*) for a revision of the certificate policy.

The focus lies on the development of a delegated regulation on C-ITS, which is in preparation. It was preceded by public consultation, which closed in January 2018[18].

The delegated regulation on C-ITS is intended to cover the following aspects:

- ensuring continuity of C-ITS services
- laying down rules to ensure security of C-ITS communications
- ensuring the practical implementation of the general data protection regulations in the area of C-ITS
- ensuring a forward-looking hybrid communication approach
- laying down rules on interoperability
- laying down rules on the compliance assessment processes.

C-ITS Platform II: compliance assessment and security approach

Current scope of Europe's compliance assessment framework (CAF)

Three levels can be distinguished in the supply chain of a C-ITS system (Figure 2.13):

- The C-ITS components starting with the provision of key integrated circuits (chips) such as the C-ITS HSM (hardware security module) and C-ITS modems which are then integrated in C-ITS boards (printed circuits) and then packaged in C-ITS units. Antennas, cables and HMI will be added to constitute a complete C-ITS station[19].
- The C-ITS station which can be sold on the after sales/retrofit market and be mounted by accredited agents in vehicles or roadside units being already in-service. But, in most cases, the C-ITS station will be directly embedded in new types of vehicles/roadside units (RSUs) by original equipment manufacturers (OEMs).
- The complete C-ITS system which is composed of many C-ITS stations which are cooperating and are supported by C-ITS servers especially for the system security management (PKI) and the delivery of customer services.

[15] https://www.cept.org/ecc.
[16] https://ec.europa.eu/transport/themes/its/c-its_en.
[17] Meanwhile an updated release has been published in June 2018.
[18] https://ec.europa.eu/transport/content/public-consultation-specifications-cooperative-intelligent-transport-systems_en.
[19] C-ITS station is a synonym for ITS station, which is defined as a functional entity specified by the ITS-S reference architecture (from ETSI EN 302 665).

Figure 2.13: C-ITS components, stations and system

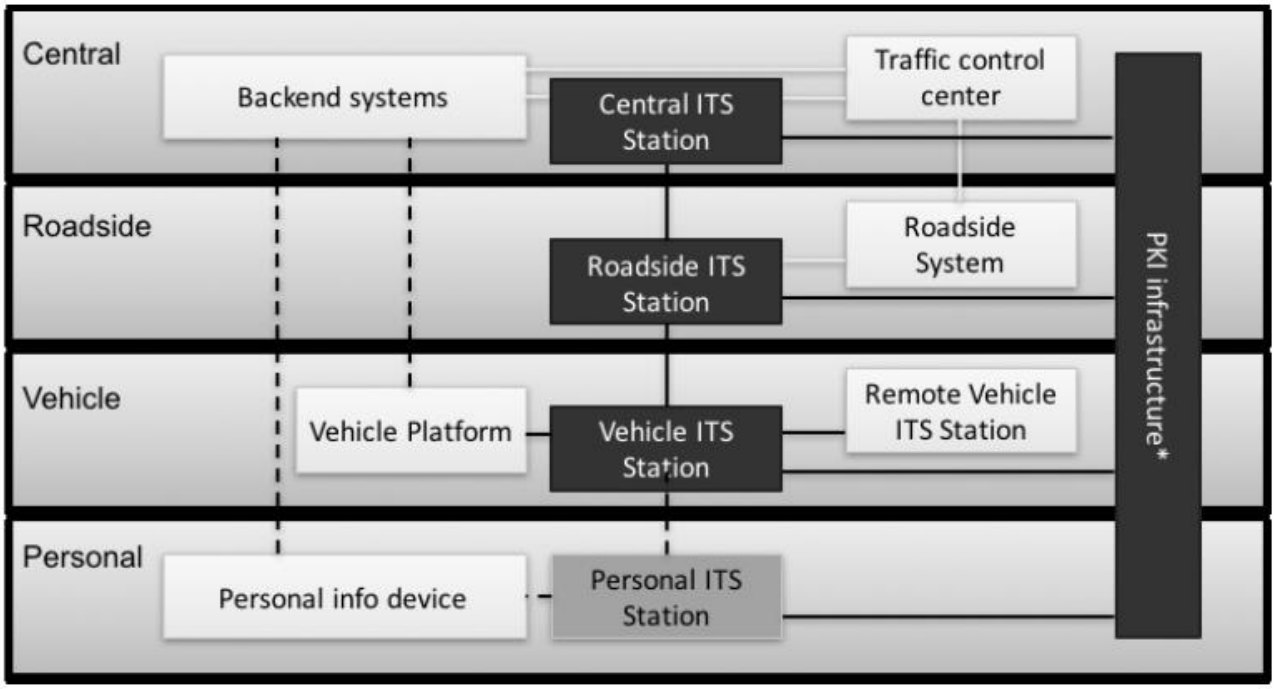
Source: C-ITS Platform Phase II 2017b.

The scope of the C-ITS compliance assessment process is only considering the C-ITS station level including isolated C-ITS stations for the after sales and retrofit markets, and C-ITS stations being embedded in vehicles and RSU.

However, this does not mean that C-ITS components and systems will not be validated, but their compliance assessment is out of scope of the proposed organisation and is left to the private industries and member states.

Figure 2.14 presents the current scope of the CAF, i.e. the black boxes and lines (grey boxes and dashed lines are currently out of scope but could be added in future). The main focus is on the interfaces between V-ITS stations and on the interface between a V-ITS station and an R-ITS station. P-ITS stations and cellular communication are currently out of scope of the conformance assessment.

Figure 2.14: Current scope of CAF in Europe



Source: C-ITS Platform Phase II 2017b.

Results of the Working Group on Compliance Assessment

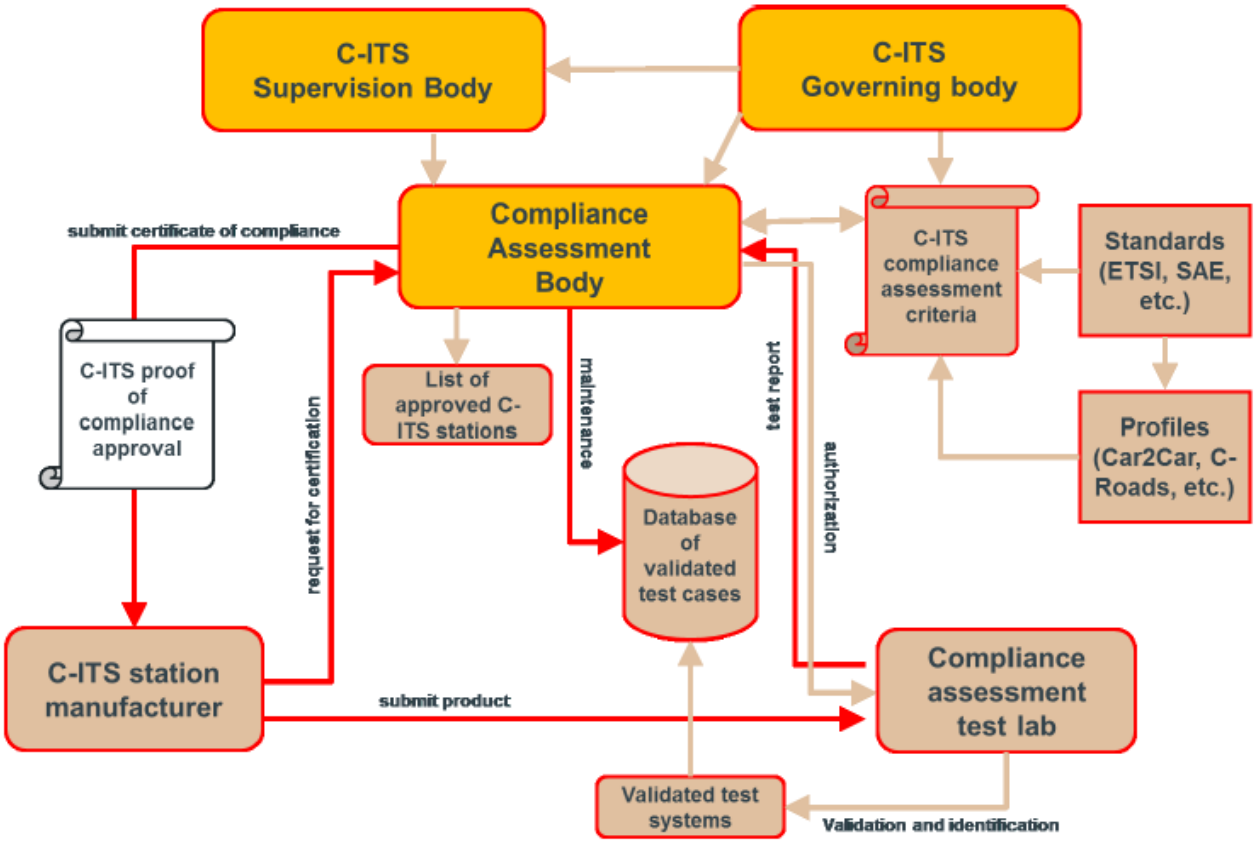
The aim of the report of the Working Group Compliance Assessment was to define a top-level approach and methodology for testing and validation. This includes evaluating and issuing recommendations on how this compliance assessment can be achieved, with a specific focus on ITS stations, and on the necessary legal and organisational frameworks for the set-up and the operational phase of the C-ITS network.

The following recommendations and follow-up actions were presented in the final report of the Working Group (C-ITS Platform Phase II 2017b):

- Need to set up an appropriate common EU legal and technical framework defining the functional, technical and organisational provisions to implement the proposed roles and compliance assessment requirements and process, which is summarised in Figure 2.15.
- Main roles in relation to C-ITS compliance assessment are governance (C-ITS governing body), operation (compliance assessment body) and supervision (C-ITS supervision body). The main decision body is the C-ITS governing body.
- Any new C-ITS station must fulfil the compliance assessment criteria to be part of the C-ITS security trust model.
- Considering the challenging time schedule of setting up a final organisation as described by the Compliance Assessment Working Group, progressive development of this organisation should allow for deployment in a relatively short timeframe (2019).
- After 2019, the proposed compliance assessment organisation should be able to also address and ensure interoperability of existing services and future C-ITS service extensions and technology deployments.
- The proposed organisation shall be capable of introducing new services or/and new technologies in a backward compatibility manner with already deployed services.
- Need to finalise by the second half of 2018 the standards and profiles necessary to support the compliance assessment process for Day 1 services.

- Need to maintain consistency with other validation frameworks having an impact on connected and automated vehicles and road infrastructure, e.g. in the future, evolution of data quality requirements may be needed for higher levels of automated vehicles.
- Further work is needed to elaborate a common EU framework to cover the roles defined by all working groups (in particular compliance assessment, privacy/data protection, and security).

Figure 2.15: Overview of the compliance assessment process



Source: C-ITS Platform Phase II 2017b.

C-ITS Compliance Assessment Reference Framework

Initially, a C-ITS compliance assessment reference framework is developed by the C-ITS governing body which includes all relevant C-ITS stakeholders. This reference framework includes:

- C-ITS assessment criteria which shall be used during the compliance assessment process by testing laboratories and other assessment organisations.
- C-ITS reference specifications, including basic and test standards, which shall be used during the different steps of the assessment process.
- C-ITS system profiles, which are the selections of particular options or parts of standards to be used.

This C-ITS reference framework shall be used by the compliance assessment body and all compliance assessment laboratories and assessment environments as a reference for testing and assessing against it the conformity of C-ITS stations.

When a C-ITS station (e.g. vehicle, RSU) is ready for the validation against the released C-ITS reference framework, the manufacturer shall issue a request for compliance approval firstly to the compliance assessment body and then select the necessary authorised test laboratories and assessment organisation which have the capability to cover all the required assessment criteria. A supplier organisation may itself operate the required test/assessment if authorised.

C-ITS stations shall be provided to selected test laboratories and assessment organisations when a request for compliance approval is sent to the compliance assessment body. Each selected test laboratory, assessment body sends to the compliance assessment body its test/assessment report. A station can only be put on the market once this report is positive.

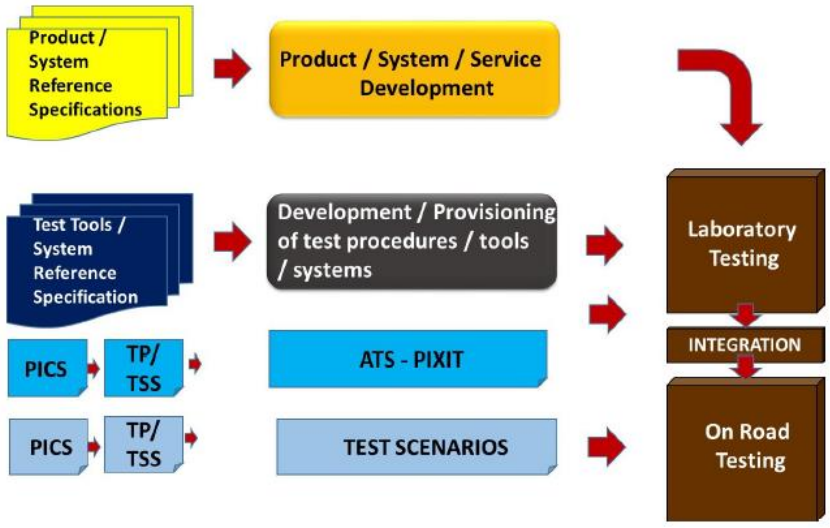
Once the compliance assessment body has received all required test/assessment reports, it shall analyse all the results and consolidate a global decision to deliver or not a certificate of compliance to the requesting supplier. In case of a negative response from the compliance assessment body, it shall provide the rationale for its opinion.

When the compliance assessment body is delivering a C-ITS proof of compliance approval, the approved station is added in the list of C-ITS stations and the supplier shall ask to be part of the security framework.

General compliance assessment methodology

The general compliance assessment methodology is represented in Figure 2.16.

Figure 2.16: General compliance assessment methodology in Europe



Source: C-ITS Platform Phase II 2017b.

Conformance to product specifications can, in large part, be achieved in test laboratories. Performance of a C-ITS system shall be tested in a closed environment between implemented C-ITS stations, before being assessed in an open environment.

The set of test cases that is to be passed by a C-ITS station might vary depending on the type of C-ITS station (vehicle, roadside unit, etc.) and on the services the C-ITS station supports.

Reference specifications

A part of the reference specifications is identical for different types of C-ITS stations. This fact will be used to define test cases independent of the type of C-ITS station. Typical examples are the geonetworking specifications that are identical for vehicle and roadside C-ITS stations, and the message definitions.

Note that some messages are only transmitted by R-ITS stations (e.g. road topology 'map' (MAP), 'signal phase and time' (SPaT) and 'in-vehicle information' (IVI) messages), and only received by V-ITS stations. So, although the messages are the same for both stations, a minimal conformance assessment process could limit the conformance testing to only encoding or only decoding of those messages, respectively.

Especially on the application layer, the various C-ITS station types are expected to implement different reference specifications, and therefore the test cases will need to be defined separately for the C-ITS station types.

Minimum requirements for all C-ITS stations (applicable to mature technologies for which profiles of standards are being adopted) include:

- Physical and access layer (e.g. ETSI EN 302 571, a harmonised standard covering essential requirements of the European radio equipment directive)
- Networking (e.g. ETSI EN 302 636 parts 1 to 6)
- Facilities (e.g. cooperative awareness message (CAM), decentralized environmental notification message (DENM) and SPaT and the associated standards)
- Applications (e.g. ETSI TS 102 965 on ITS application object identifier).

Minimum performance requirements are particularly important for road safety applications and in particular collision avoidance (human or automated), e.g. maximum latency time, data element accuracy, level of trust in received data. However, until now, the first priority of standardisation bodies was on interoperability and conformance testing, not on defining minimum performance requirements.

Since V-ITS and R-ITS stations have a long life cycle (V at least 10 years, R usually significantly longer than 10 years), there is also a need for minimum scalability requirements, e.g. capacity to adapt to new standard versions and to sustain a system load increase.

In the relatively near future, requirements regarding emerging technologies, e.g. cloud-based and LTE-based solutions, are expected as well. Compliance of emerging technologies is assumed to be covered by radio equipment directive (RED) and/or global certification forum (GCF[20]) certification schemes (Carabin 2017, slide 20).

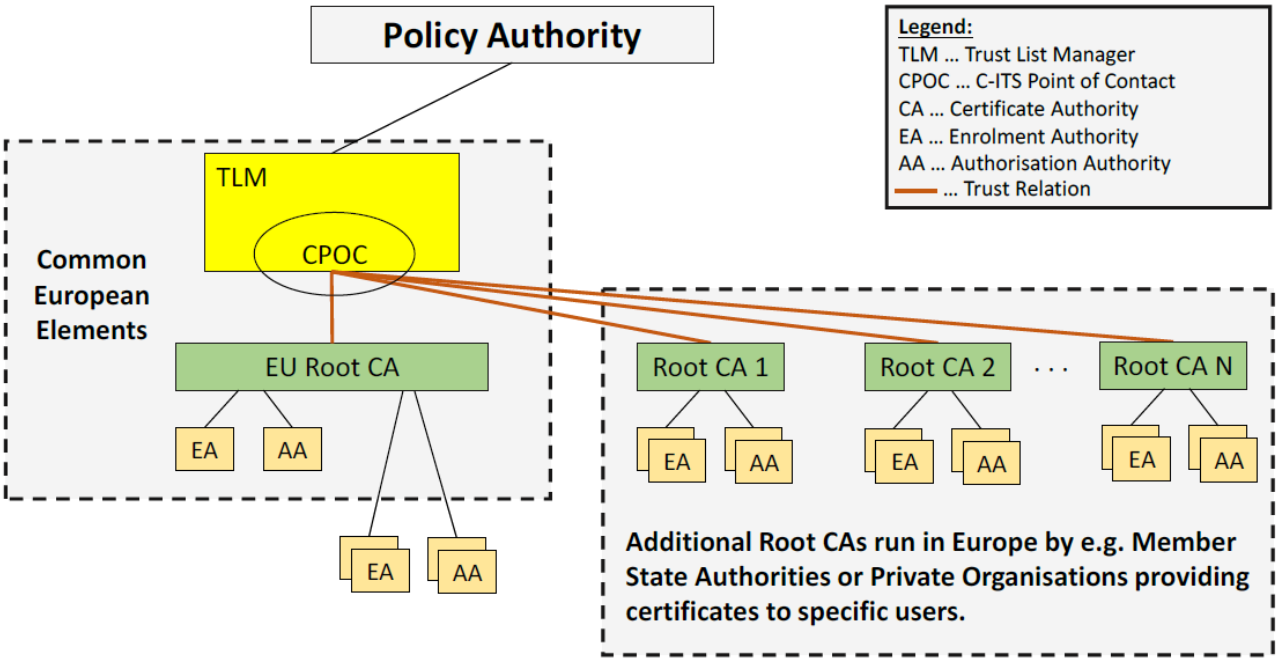
SCMS: Europe's C-ITS trust model

The compliance assessment regimes adopted for C-ITS will have to work hand in hand with the SCMS, and the SCMS will have an active role in ensuring that permissions/certificates are issued to C-ITS stations on the basis that they are compliant with compliance assessment regimes.

The *Certificate Policy for Deployment and Operation of European C-ITS* (C-ITS Platform Phase II 2017a) presents the European C-ITS trust model, based on public key infrastructure (PKI) (Figure 2.17). It defines legal and technical requirements for the management of public key certificates for C-ITS applications by issuing entities and their usage by end-entities in Europe.

[20] https://www.globalcertificationforum.org/.

Figure 2.17: The European C-ITS trust model



Source: C-ITS Platform Phase II 2017a.

The C-ITS trust model is based on a multiple Root CA architecture, where the Root CA certificates are transmitted periodically to the central point of contact (CPOC) through a secure protocol (e.g. link certificates), which is defined by the CPOC. The C-ITS trust model elements shall use physical security controls in compliance with ISO 27001 and ISO 27005.

It should be highlighted that Europe's trust model is a federated and multi-SCMS solution, with central administration and coordination undertaken by the EC. Member states and private organisations will have their own Root CAs (with the EC's Joint Research Centre operating an EU Root CA). Root CAs are added into the system and audited by the EC. In this sense, member states and private organisations will be responsible for operating 'modularised' SCMS, which together form a European-wide SCMS with a public entity providing oversight and coordination.

PKI roles and information flows

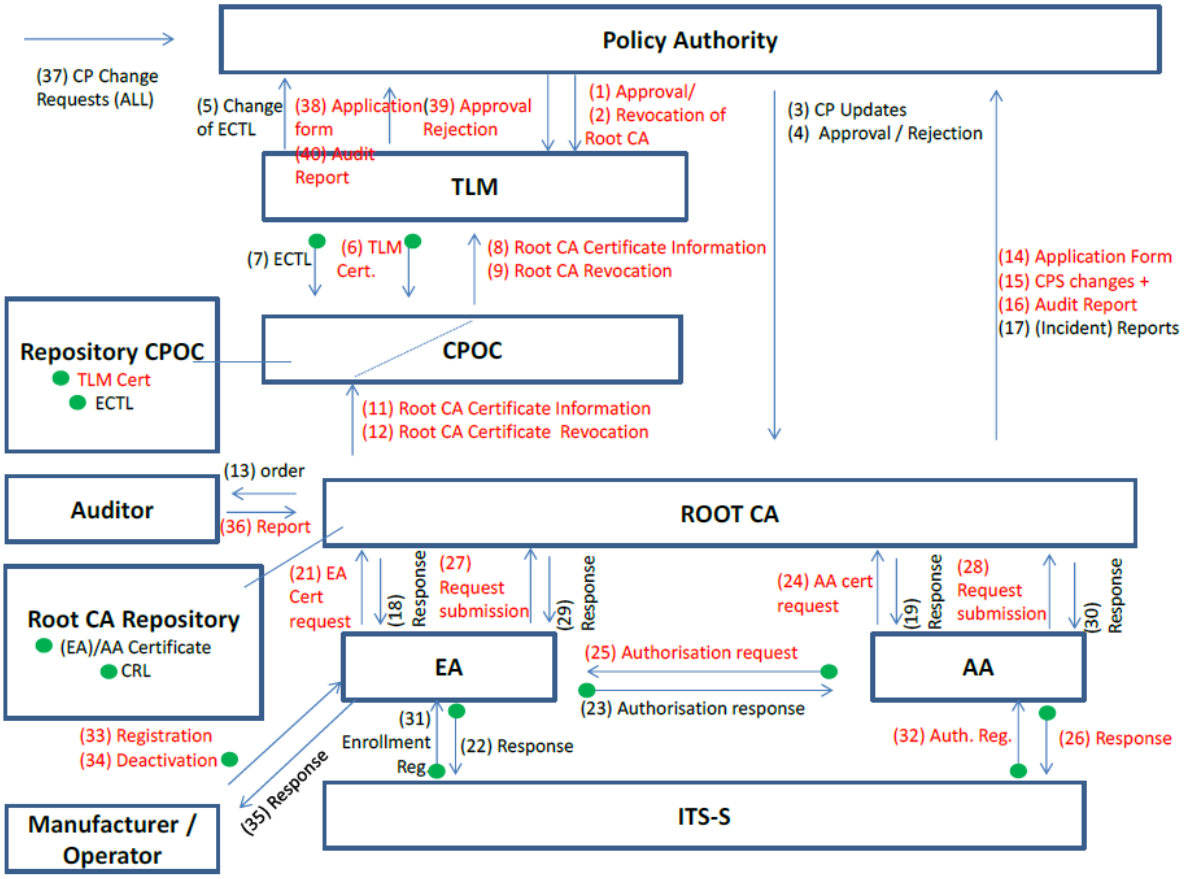
Figure 2.18 provides an overview of the information flows between the PKI participants. The green dots indicate flows that necessarily require machine-to-machine communications. The information flows in red have defined security requirements.

PKI roles are distinguished in:

- Authoritative roles, i.e. each role is uniquely represented:
  - policy authority: a role composed by the representatives of public and private stakeholders (e.g. member states, vehicle manufacturers, etc.) participating in the C-ITS trust model. The policy authority is responsible for two-sub roles: certificate policy management and PKI authorisation management.
  - trust list manager (TLM)
  - accredited auditor
  - C-ITS point of contact (CPOC).
- Operational roles, i.e. roles which can be represented by one or more entities:
  - Root certification authority (Root CA)

- enrolment Authority (EA)
- authorisation authority (AA)
- sending ITS-S
- relaying ITS-S (forwarding ITS-S)
- receiving ITS-S
- manufacturer
- operator.

Figure 2.18: Information flows between PKI participants



Source: C-ITS Platform Phase II 2017a.

Stakeholders: C2C CC and C-Roads

The CAR 2 CAR Communication Consortium (C2C CC) and C-Roads are two important stakeholders in Europe. Substantial development of C-ITS in Europe has been driven by the C2C CC (see also Car 2 Car Communication Consortium 2017).

The general approach and current priorities of C2C CC can be described as follows[21]:

- To enable competition by design and innovation (specification of the 'minimum requirements').
- To develop the automotive market by bringing voluntary C-ITS related services quickly onto the market.

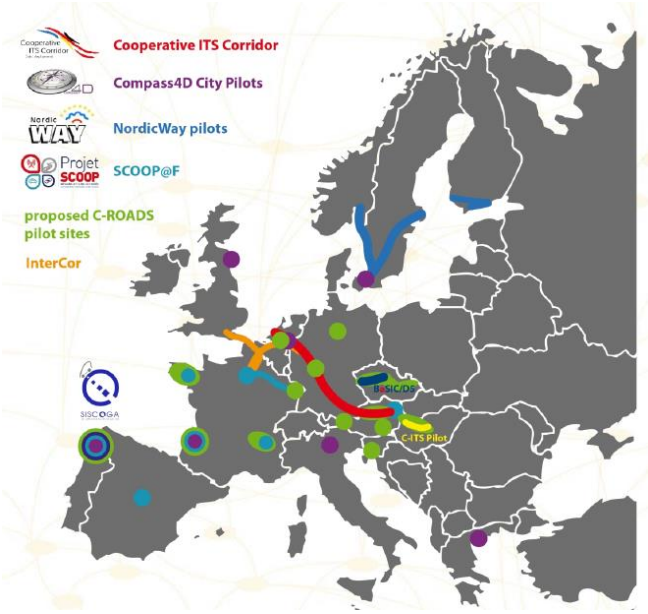
[21] Based on a telephone conversation on 13 November 2017 with Mr. Niels Peter Skov Andersen, general manager of C2C CC and chairman of ETSI's Technical Committee on ITS.

- The focus will initially typically be on C-ITS driver safety support applications/messages (such as emergency electronic brake light, emergency vehicle approaching, stationary vehicle warning, slow vehicle warning, active queue assisting); it should be left to the receiving entity (typically the V-ITS-S) to decide if and how to process the received data.
- V-ITS-S is generally seen as a milestone towards AVs. Eventually the conformity assessment of V-ITS-S should become part of the vehicle type approval, i.e. part of the UNECE type approval regulation.
- The PKI framework will provide the needed trust in C-ITS messages.
- C2C CC has defined 90-95% of the relevant test cases, which are currently not in the public domain – but should be released in the public domain at a later stage. (It is not clear whether these need to be followed up with more detailed test specifications that define the procedures, test parameters and criteria); ETSI has done more on test specifications for C-ITS than ISO/CEN (whose progress and results to date have been rather modest).
- The *General Data Protection Regulation* (European Union 2016), which appears to have been designed with peer-to-peer applications in mind, is generally considered as a 'nightmare' and its implications for C-ITS are unclear. For example, is it permissible or not for the users to opt out to relay relevant safety-related information.
- Concerning the approach related to conformity assessment aspects:
  - radiofrequency parameters: demonstrate compliance by use of harmonised standards covering essential requirements in the radio equipment directive and in line with the new legislative framework (NLF) approach (see Figure 2.11). European industry is generally in favour of self-assessment and declaration, based on harmonised standards, rather than having to use an in-house or external conformity assessment body (i.e. the other two alternatives according to the European NLF approach)
  - security-related aspects – C-ITS trust model and the evaluation of product according to the Common Criteria
  - the quality of the data: the focus is on the quality of the transmitted data (i.e. the triggering event and the latency of the transmitted data, in accordance with the standardised format) – the emergency braking message needs to be trustworthy, in particular if the vehicle, at a later stage of development, is to take actions autonomously.
  - human machine interface (HMI) aspects: whereas some general HMI principles need to be respected and assessed (as part of the general vehicle type approval criteria), the HMI aspects are outside the scope of the C-ITS conformity assessment; it is important to seek to minimise overlap between sector-specific legislation
  - V-ITS-S and R-ITS-S are the focus for Days 1-3
  - C-ITS-S and P-ITS-S are not the focus for the next 5-10 years. The automotive industry generally considers C-ITS information stemming from P stations to be ‘noise’ (as the P station’s position is typically not accurate enough and should be accurate to 10-30 cm). Hence, information from P stations will typically not be taken into account by V-ITS-S. C-ITS-S will form part of deployed service but will not be the focus of conformity assessment activities in coming next years.

In 2016, member states and the EC launched the C-Roads Platform (https://www.c-roads.eu/platform.html) to link C-ITS deployment activities, jointly develop and share technical specifications and to verify interoperability through cross-site testing. Initially created for C-ITS deployment initiatives co-funded by the EU, C-Roads is open to all deployment activities for interoperability testing.

Overall, C2C CC and C-Roads will play an important role in the coming years in the early deployment, validation and profiling of standards, so that these become fit for purpose and provide a suitable basis for interoperability specifications/regulations. Figure 2.19 shows main current C-ITS pilots and deployments at European level.

Figure 2.19: Main current C-ITS pilots and deployments in Europe



Source: Geissler 2017.

2.3.2 US C-ITS State of Play

USDOT

The USDOT Intelligent Transportation Systems Joint Program Office (ITS JPO) fosters the development and future deployment of connected vehicle technologies. The focus of the ITS JPO is on research to push the boundaries of what is possible, spur technology innovation, and reduce the risks of moving from the laboratory to the real world. Connected vehicle research involves all agencies within the USDOT including the National Highway Traffic Safety Administration (NHTSA), Federal Highway Administration (FHWA), Federal Motor Carrier Safety Administration, Federal Transit Administration, and the Federal Railroad Administration.

USDOT ITS Strategic Plan

Connected vehicles is one of the program areas of the USDOT *ITS Strategic Plan 2015-2019* (ITS JPO 2014). The USDOT is working, with its public and private partners, to address the technical, safety and policy challenges, and helping to create the standards and the wireless architecture that will be the backbone of the system.

NHTSA Notice of Proposed Rulemaking

Citing the benefits associated with connected vehicle technologies, the NHTSA issued in December 2016 a Notice of Proposed Rulemaking that would enable V2V communication technology on all light vehicles (NHTSA 2016). The proposed rule would require automakers to include V2V technologies in all new light-duty vehicles and require V2V devices to 'speak the same language' through standardised messaging. The NHTSA received many (negative) comments; a regulatory review seems still ongoing[22]. Several media reports state that it is far too early to mandate this technology for light vehicles[23].

[22] https://arstechnica.com/cars/2017/11/trump-administration-reportedly-kills-vehicle-to-vehicle-safety-mandate/ (dated 1 November 2017, viewed 15 December 2017).
[23] https://www.mercatus.org/publications/department-transportation-v2v-technology-mandate (dated 14 April 2017, viewed 15 December 2017).

USDOT Automated Driving Systems 2.0: A Vision for Safety

The USDOT recently released *A Vision for Safety* to promote improvements in safety, mobility, and efficiency through automated driving systems (ADSs) (USDOT 2017a). *A Vision for Safety* replaces the *Federal Automated Vehicle Policy* released in 2016. This updated policy framework does not explicitly mention V2V technologies to be used and offers a path forward for the safe deployment of automated vehicles by:

- encouraging new entrants and ideas that deliver safer vehicles
- making department regulatory processes more nimble to help match the pace of private sector innovation
- supporting industry innovation and encouraging open communication with the public and with stakeholders.

FHWA V2I Guidance

As a complement to the proposed V2V rule, the Federal Highway Administration (FHWA announced in January 2017 the V2I guidance to assist transportation system owners/operators as they deploy V2I technology (USDOT 2017d). The guidance can help transportation agencies and tollway authorities understand what a decision to deploy V2I technology could mean to their region, prepare for emerging V2I/V2V technologies and leverage federal-aid funds to deploy them.

USDOT Connected Vehicle and Connected Vehicle Certification Programs

With basic technical feasibility determined, the USDOT initiated in 2014 the Connected Vehicle Program to address the following key strategic challenges:

- 'to resolve remaining technical, policy, institutional, and funding challenges
- to conduct testing to determine the actual benefits of applications
- to determine whether overall benefits are sufficient to warrant implementation and, if so, how the systems would be implemented
- to address issues of public acceptance such as maintaining user privacy and whether systems in vehicles are effective, safe, and easy to use.'

Connected vehicle certification is a key research program of ITS JPO (USDOT 2016). Certification is defined as the process of ensuring that system components, manufactured according to program requirements, perform as intended. Certification will ensure that users can trust that the components will work within the system.

Research goals of the certification program are:

- 'to work with industry to define certification needs and develop supporting test methods and tools
- to develop a future plan that will make certification activities self-sustaining through fees for testing shaped by the organisations seeking those requirements.'

Two major questions in the research program were the ultimate form that a certifying entity would take and the potential role of the Federal Government in oversight and enforcement of certification requirements.

USDOT has recently completed its initial phase of C-ITS certification research and development[24]. A major outcome of this research is that the OmniAir Consortium (see also below) is now offering certification services for connected vehicle functionality. Moreover, it appears that USDOT is contemplating work on a regulation for minimum requirements.

[24] Source: E-Mail by Kevin Gay, Chief – Policy, Architecture, & Knowledge Transfer of ITS JPO.

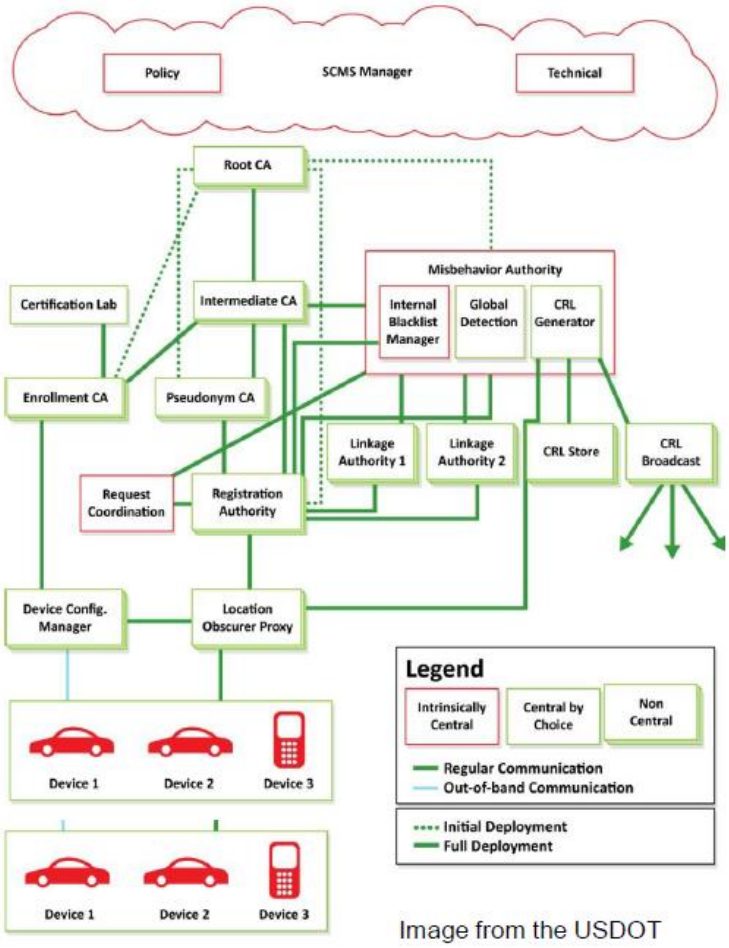
USDOT SCMS presentation

Vehicle and infrastructure messages must be trusted for the system to work. The security credentials management system (SCMS) is the entity that issues, distributes, and revokes security credentials for devices operating in the system. The USA is pursing one centralised SCMS solution, with the USDOT also operating the root certificate authority component.

In 2012, the USDOT made available the first prototype of the SCMS for use in the safety pilot model deployment and by others performing research, and development and testing activities that required security certificates. Together with the automotive industry and industry security experts through the Crash Avoidance Metrics Partnership (CAMP), a state-of-the-art security system that enables users to have confidence in one another and the system as a whole was developed (USDOT 2017e). Figure 2.20 shows the USDOT SCMS.

The SCMS provides the security infrastructure to issue and manage the security certificates that form the basis of trust for V2V and V2I communication. Connected vehicle devices enrol into the SCMS, obtain security certificates from certificate authorities (CAs), and attach those certificates to their messages as part of a digital signature. The certificates prove the device is a trusted actor in the system. Misbehaviour detection and reporting allow the system to identify bad actors and revoke message privileges, when necessary.

Figure 2.20: USDOT SCMS



Source: Harmonisation Task Group 6 2017.

Lessons learnt about the role of the SCMS

The connected vehicle pilots, smart cities, and other research deployments, that derive funding from the USDOT, are able to interact with the current prototype national-level SCMS (SCMS POC[25]) to ensure the security and privacy of their messages. From September 2017, the SCMS operational environment (production-ready) is available to coincide with the full-scale deployment of devices at the connected vehicle pilot sites. The policies, procedures, and lessons learnt from using the SCMS POC (e.g. USDOT 2017b) will eventually be shared with connected vehicle stakeholders to support the establishment of the national SCMS.

The OmniAir Connected Vehicle Certification Program

In October 2017, the OmniAir Consortium™ announced its independent, third-party testing and certification program for V2X-DSRC connected vehicle products.

The OmniAir Consortium is a leading industry association promoting interoperability and certification in connected vehicles, ITS, and transportation payment systems. Membership includes public agencies, private companies, research institutions, independent test laboratories, test equipment/software providers, cybersecurity experts, engineering firms, tolling agencies, and ITS deployment organisations.

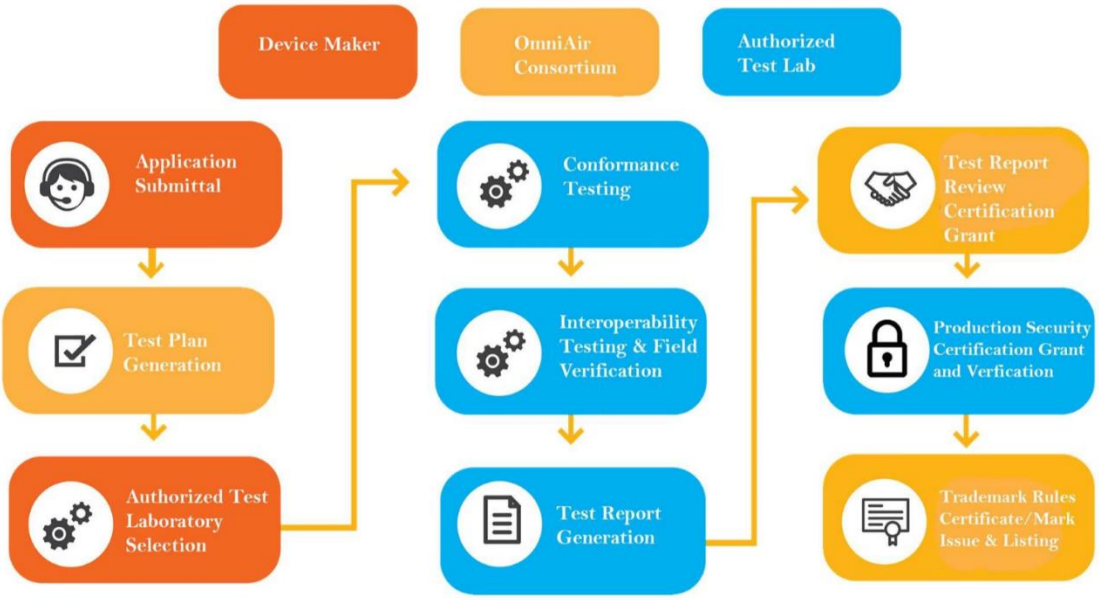
Connected Vehicle Certification

The OmniAir certification program for connected vehicle devices allows members to measure compliance and ensure interoperability among products and services that support OmniAir specifications (OmniAir Consortium 2017b).

The certification program includes testing for 5.9 GHz DSRC-enabled devices (OBU, RSU, modules, software stakes and test systems). Test specifications cover IEEE 802.11p, IEEE 1609.3, IEEE 1609.4, SAE J2945/1 and upcoming IEEE 1609.2 security/certificates. In the future, OmniAir will add certifications of other emerging technologies for transportation communications connectivity.

Figure 2.21 shows the certification process.

Figure 2.21: OmniAir certification process



Source: Based on OmniAir Consortium 2017a.

[25] POC = Proof of Concept

Certification is optional. OmniAir encourages device makers to test their products for conforming and interoperability readiness before certification by participating in OmniAir industry plugfests[26]. One reason to certify products is that federal, state and local agencies are requiring device certification in their request for proposals.

Certification is a partnership between the device maker and OmniAir. The manufacturer applies to OmniAir first by selecting the device category, connect vehicle certification or tolling certification and fills out a form that describes the device, system or unit under test (UUT).

Each form varies slightly as to the protocol and the requirements against which the UUT is being tested. The applicants remit a flat fee for each certification program they want to participate in. For example, they might submit multiple devices that differ only in the form factor to the OmniAir 5.9 GHz DSRC test program. The application fee is the same for one, two, up to arbitrary number of devices.

After OmniAir receives the fee – to set up the applicant in the database – applicants are asked to send the product directly to an OmniAir-accredited test laboratory. Once the laboratory test is completed, the laboratory sends the report to OmniAir for review. If warranted the device will receive an OmniAir-certificate with a number and be entered into the publicly available OmniAir-certified online database. Companies completing certification may display the OmniAir® certified logo.

Accredited Laboratories and Qualified Test Equipment

Only OmniAir Consortium members will be selected to serve as an OmniAir authorised test laboratory (OATL). OATLs follow ISO standards for laboratory auditing and accreditation and must use OmniAir qualified test equipment (OQTE), systems and test tools to ensure accuracy and consistency of test results.

OmniAir will assess and qualify the test equipment, systems and test tools used in industry. Only those items that undergo this rigorous investigation become an OQTE product and are eligible for use by the OATLs for the purpose of device certification.

Connected Vehicle Pilots

The Connected Vehicle Safety Pilot (2011-2012) was the main scientific research initiative to collect the data needed to understand the safety benefits of connected vehicle core technologies. It was critical to supporting the 2014 NHTSA decision on the deployment of these technologies for light vehicles (USDOT 2014).

Since then, testing, development and data collection activities have continued. For example, in Ann Arbor (in the state of Michigan), where the Safety Pilot Model Deployment research left off, the Connected Vehicle Test Environment project continues with research and development.

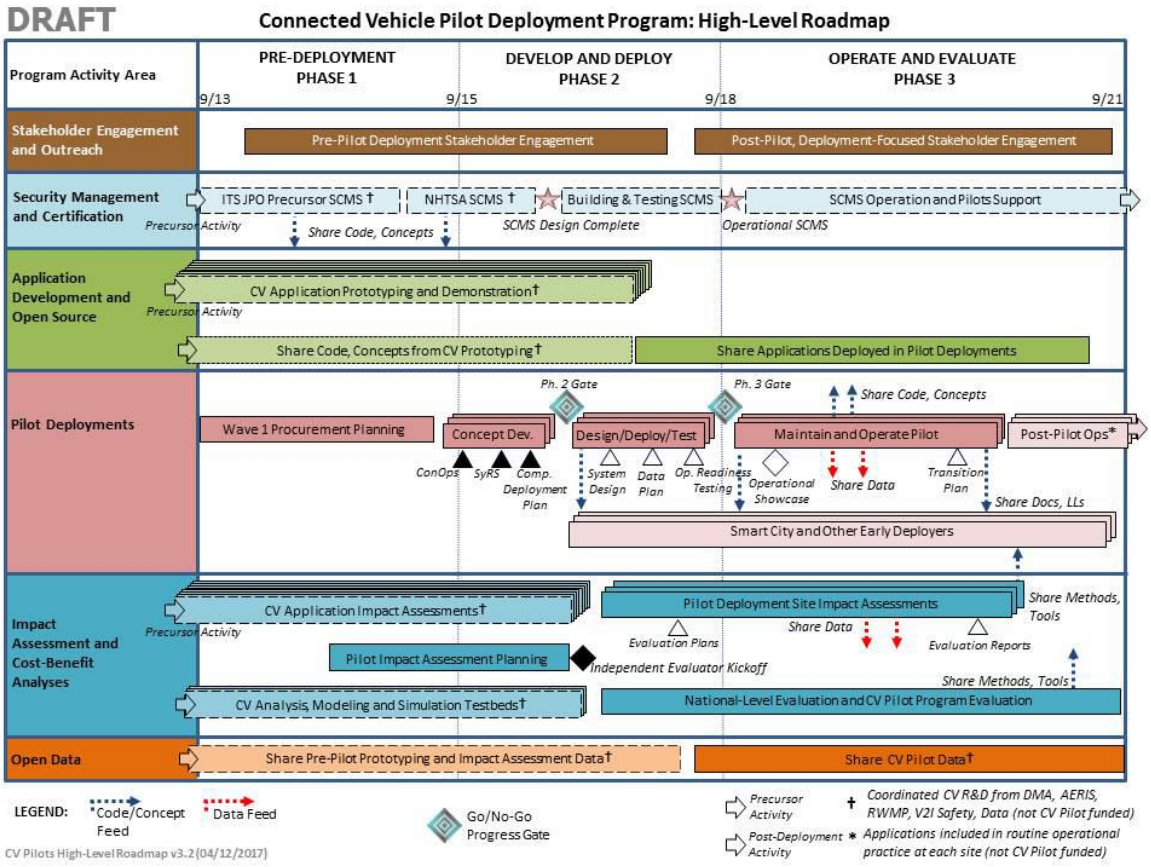
Moreover, the USDOT Connected Vehicle Pilot Deployment program kicked-off in September of 2015 with the following three pilots (USDOT 2017c):

- New York City DOT Pilot
- Tampa-Hillsborough Expressway Authority Pilot
- Wyoming DOT Pilot.

Figure 2.22 presents the high-level road map of the Connected Vehicle Pilot Deployment program.

[26] Where the designers of equipment or software test the interoperability of their products or designs with those of other manufacturers and according to the OmniAir specifications.

Figure 2.22:High-level road map of the Connected Vehicle Pilot Deployment Program



Source: USDOT 2017c.

2.4 Key Findings

This section lists the key findings derived from the literature review, which were used in the refinement of the scope of the development of a C-ITS CAF for ANZ, especially for developing and evaluating possible models (see Section 3) and drafting the Explanatory Note prepared for the stakeholder consultations (see Section 4).

ANZ C-ITS context and state of play

- Significant C-ITS research work has been undertaken, in particular by Austroads.
- No formalised ANZ C-ITS implementation road map, e.g. defining priority (Day 1) services or specific actions in order to lay down the rules and conditions for initial large-scale deployment of C-ITS, is known to exist. It would be beneficial for the ANZ C-ITS CAF if the TVRA project (or beyond) would describe the systems on offer and their vulnerabilities, determine the impact of these vulnerabilities and what mitigation is required to bring these down to an acceptable level. Some of the mitigation may be compliance.
- In ANZ, significant C-ITS research work has been undertaken. Moreover, both countries are proactively undertaking connected and automated vehicle trial, representing the state of the art in terms of initial C-ITS deployment. The trials focus is especially on testing and demonstrating technologies, validating impacts and benefits, and increasing public awareness of C-ITS. The trials require that C-ITS devices comply with certain requirements (e.g. from a contractual perspective), but compliance in the sense of how C-ITS will need to address compliance when ultimately deployed is not their focus.
- Pending a more elaborated ANZ C-ITS policy to be developed and approved, the current working assumption is that ANZ favour adoption of the EU C-ITS scenario. Australia is now considering its options for a SCMS. Input is expected from C-ITS trials in ANZ, where a SMCS will be used.

- The Australian Government's approach to regulation is to introduce new regulation as a 'last resort'. Policy makers must seek practical solutions, balancing risk with the need for a regulatory framework. They are encouraged to develop and make use of alternative instruments in shaping the rules of the market, including for example pre-market assessment schemes. Compliance of products and services in the Australian and New Zealand market with standards is normally voluntary, unless they are regulated by government. Regulation may be considered if the standard for the products and services relates to safety (in particular safety-critical services) or addresses environmental or consumer protection issues.
- The *Operationalising Austroads' Product Acceptance Process* report (Austroads 2016) proposes a detailed governance framework to support the national ITS product approval process. It is based on a hybrid model and a pre-market approval model involving a seven-step approval process. It proposes a governance framework, for which it recommends the establishment of a national ITS type approval committee (NITAC, under the road agencies' authority), to review product testing results, and approve products. The final pre-market approval step is reporting and entering the result into the national type approved ITS product register. Although the proposed model is conceptual and no decision has been made to implement it, it is relevant to consider as a potential compliance assessment model for R-ITS-S.
- NTC policy paper on *NTC Assuring the safety of automated vehicles* (NTC 2017a) provides a relevant input to the development of a C-ITS CAF for ANZ. It presents the policy direction related to an SAS for AVs, taking into account the needs of the relevant stakeholders. It sets out the high-level design of a safety assurance system for automated vehicles in Australia by recommending that it is based on mandatory self-certification until the development of international standards for AV systems. A consultation regulation impact statement (RIS) was released in May 2018; a decision RIS for consideration by Australia's transport ministers is expected in November 2018. A key objective of many of the AV stakeholders is the adoption of a consistent approach to the approval of products on the Australian market – this appears particularly relevant for adjacent market sectors like AVs and C-ITS.

Global C-ITS developments

- C-ITS deployment is in its infancy. Europe and the USA are leading the global developments, driven by the industry wanting to develop the automotive market by bringing voluntary C-ITS services quickly into the market. Policy makers try to create favourable market and regulatory conditions so that society can start to reap the benefits from the emerging C-ITS services, increased road safety, increased capacity of the road infrastructure, reduced traffic congestion and without negative impact on the environment.
- Large-scale C-ITS trials and early C-ITS deployments are being implemented and put into service. In Europe, the C2C CC and C-Roads are expected to play an important role in the coming years in the early deployment, validation and profiling of standards. In the USA, the connected vehicle pilots are being undertaking with test beds in New York City, Tampa and Wyoming.
- Europe is about to launch the preparation of a delegated regulation on C-ITS. It is intended to pave the way for large-scale deployment of C-ITS (Day 1 services) by laying the needed rules, e.g. on the compliance assessment processes. An overarching governance architecture incorporates the compliance assessment process including the description of roles and actors.
- European C-ITS conformity assessment activities are focusing on the V-ITS and the R-ITS stations (as opposed to components and systems); no significant work on conformity assessment is expected on C-ITS and P-ITS stations in the next five years.
- USDOT has recently completed its initial phase of C-ITS certification research and development. A major outcome of this research is that the OmniAir Consortium is now offering voluntary certification services for connected vehicle functionality.
- Europe and the USA have come relatively far in defining their security trust models and security credential management system (SCMS), which are essential enablers for large-scale deployment. Where the USA is pursing one centralised SCMS solution, with the USDOT also operating the root certificate authority component, Europe's trust model can be seen as a federated, multi-SCMS solution, with central administration and coordination by the EC. The EC will operate a four-year pilot phase of the European SCMS, as of January 2018. The activities will be carried out in close cooperation with the European Standards Organisations (ESOs, i.e. CEN/TC278 and ETSI TC on ITS).

- An important consideration is international SCMS harmonisation. In a multi-SCMS world that supports a global transportation marketplace, trust will need to be defined beyond jurisdictional boundaries. High-priority areas for harmonisation include: SCMS components, organisational trust (e.g. intra-SCMS, inter-SCMS), additional privacy and security protections (e.g. security certificate).

The findings from the literature review have provided a healthy basis for the further work on the design of a C-ITS CAF for ANZ, especially regarding input for:

- the basic assumptions made regarding the ANZ C-ITS CAF, which form the foundation for the elaboration of the C-ITS CAF model options
- the differentiation of the four main high-level policy options for compliance assessment of C-ITS, with illustration of how the type approval process can be implemented based on ITS CAF best practice models
- the outline of an overarching C-ITS governance architecture
- the assessment of the four C-ITS CAF models, based on a set of proposed evaluation criteria
- the Explanatory Note to foster a common basic understanding of C-ITS compliance assessment among stakeholders and to assist stakeholders in taking positions on relevant issues, as part of the preparation for the stakeholder consultations.

3. Development and Evaluation of ANZ C-ITS CAF Models

3.1 Basic Assumptions towards an ANZ C-ITS CAF

A number of basic questions will need to be answered in the process of designing the ANZ C-ITS CAF, such as:

- What is the overall objective and role of the CAF? Why is a CAF needed and what are the current weaknesses? How is the 5.9 GHz band protected from threats that impact its intended use and design?
- What is the overall scope of the assessment framework? What is driving the extent of the restrictions?
- Who defines what is to be assessed? Who determines the compliance assessment criteria?
- What are the requirements (with or without references to technical specifications or standards)?
- What are the test cases and test procedures (ditto)?
- Who examines the product against the requirements?
- Who makes the overall appraisal of a product's conformity? Is a certificate granted and by whom, or does the supplier or its representative deliver a declaration of conformity upon successful demonstration of compliance (cf. ITS Class Licence)?
- Is a list of type approved models to be kept? If so, kept by and accessible by whom?
- Who finances the set-up and operations of the CAF?
- Who performs the market surveillance?
- What is the definition of life-cycle stages of C-ITS stations? How long is a type approval certificate valid and can a C-ITS type approval be prematurely withdrawn in case of detection of a non-compliance?

All these questions need not initially have definitive answers. This section seeks to initially address all the above questions.

The basic assumptions in this section are proposed to form the basis for the further elaboration of the C-ITS CAF model options in the following discussion.

What is the overall objective and role of the CAF?

The overall objective and role of the ANZ C-ITS CAF was described in the project plan and scoping document – a framework 'which will ensure that C-ITS stations (that are being placed on the market or in service for safety-related, regulated, or commercial services) comply with a range of agreed standards and specification ensuring that these

- do not jeopardise safety
- are fit for purpose (including effective use and support for efficient use of radio spectrum in order to avoid harmful interference)
- are interoperable
- support an open vendor market and avoid vendor lock-in with proprietary solutions'[27].

[27] In general a compliance assessment framework can be used as a means to promote free trade or on the contrary as a means to trade protectionism.

What is the overall scope of the assessment framework?

It is essential to clarify the overall scope of the ANZ C-ITS CAF, including what types of products that would fall under this framework, in order to elaborate suitable options.

Generally, the market distinguishes between C-ITS stations, C-ITS components and C-ITS systems. The international developments of C-ITS CAFs focus on the C-ITS station, noting that these can relatively easily be matched with standards (existing or under development), which are essential pillars that underpin the frameworks. It is further noted e.g. that C-ITS stations are 'standalone' products for after sales and retrofit in e.g. vehicles or roadside units or embedment in equipment. Hence, it is assumed that C-ITS stations constitute the scope of the ANZ C-ITS CAF (as opposed to C-ITS components or systems[28]), in line with the project plan and scoping document.

Further, for efficiency it is strived to ensure consistency with existing legislation and best practice. It seems sensible to seek to minimise the overlap with existing legislation and codes of practice, and in the C-ITS CAF only include the C-ITS-specific aspects.

Below are some thoughts on the overall scope and aspects that are covered by existing regulations and codes of practice and which are C-ITS-specific aspects that potentially would form the scope of the ANZ C-ITS CAF:

- **General aspects** that are covered by provisions in **existing** regulations and codes of practice:
  - **Health and safety** protection related to products placed on the ANZ market covered in provisions of the consumer protection laws in ANZ as defined in Australia's *Competition and Consumer Act 2010* (which includes the Australian Consumer Law; Australian Government 2015) and New Zealand's *Consumer Guarantees Act 1993* (New Zealand Government 2017a)
  - **Electrical safety, electromagnetic compatibility and electromagnetic energy** requirements covered in the provision of the Regulatory Compliance Mark for ANZ
  - **Environmental protection** laws[29]
  - **General data protection** as defined in the *Australian Government's Privacy Act 1988* (Australian Government 2013) and *New Zealand Government's Privacy Act 1993* (New Zealand Government 2017b)
  - **Human machine interface** design principles.[30]
- **C-ITS-specific aspects** that are potentially part of the scope of the conformity assessment:
  - **C-ITS radio frequency** conformity assessment. C-ITS stations in Australia must comply with the ACMA ITS Class Licence (ACMA 2017a[31]), whereas the requirements are not yet established for New Zealand.
  - **C-ITS applications**, noting that at present these requirements are not defined. The main candidate applications to form part of the framework are regulatory, safety critical and safety-related, enhanced user protection (e.g. vulnerable road user protection) and enhanced environmental protection (e.g. geo-fencing of high-consequence dangerous goods in tunnels or in urban areas).

C-ITS security-related requirements, noting these are currently not established. The C-ITS security-related requirements and associated test procedures can for example be developed according to the process illustrated in Figure 2.10. The evaluation of a C-ITS station can be done according to the Common Criteria Recognition Arrangement.

[28] C-ITS components and systems also need to be assessed for their conformity to specifications, but this is outside the proposed scope of the ANZ C-ITS CAF and left to the private sector.
[29] Similar to EU laws on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RHoS, Directive 2011/65/EU on) and waste of electrical and electronic equipment (WEEE, Directive 2012/19/EU). Environmental and energy management systems requirements based on ISO 14001 and ISO 50001.
[30] Similar to the European Commission's recommendation on safe and efficient in-vehicle information and communication systems: update of the European Statement of Principles on human machine interface (2007/78/EC).
[31] ETSI EN 302 571 in general, and Annex A in particular, regarding the C-ITS radiofrequency conformity assessment criteria.

– **C-ITS data protection** conformity assessment, in case specific principles[32] would be added on top of the ANZ privacy acts.

Hence, it is proposed to seek to align the C-ITS CAF with the existing regulations or codes of practice in ANZ, and only to include in the C-ITS CAF aspects which are C-ITS-specific or not adequately dealt with in the existing regulations and codes of practice.

Further basic assumptions

The framework should cover compliance assessment for placing of C-ITS stations on the market (design and manufacturing) and C-ITS stations being in service.

It is assumed that the compliance is assessed with regard to the C-ITS CAF requirements applicable at the time of the first making available of the C-ITS station on the market[33].

It is assumed that the onus remains throughout the lifetime with the manufacturer (or its representative) to demonstrate compliance with the C-ITS CAF requirements.

It is assumed that the conformity assessment procedure at the time of placing of the C-ITS stations on the market is in two steps, in view of the expected volume involved:

- first examination of the conformity of a specimen or the design of the concerned product (i.e. type approval)
- then, determination of the conformity of the manufactured products against the approved specimen (e.g. by means of production control, product check at random intervals, see modules and their variants in Section 2.3.1).

In case the manufacturer makes a significant change to the product in service, it is assumed that it is responsible for reassessing and ensuring that the product complies with C-ITS CAF requirements before the modified product is introduced into the market. It is the manufacturer's duty to provide an updated certificate or statement of compliance (in case of self-assessment) supporting safety-critical changes.

A C-ITS station is assumed to be subject to the following events (consistent with the simplified version of the end-security life cycle as illustrated in Figure 2.5):

- placing on the market (i.e. ‘Operational’ in Figure 2.5): a product is placed on the market when it is made available for the first time on the (ANZ) market. It includes the necessary security certificate, which is a prerequisite for being part of the C-ITS trust model and to be recognised as a trustworthy entity
- withdrawal from the market (i.e. ‘Unenrolled’ or ‘End-of-life’ in Figure 2.5), either at the end of the certification period (e.g. expiry of the security certificate), prompted prematurely by the market surveillance authorities due to non-compliance (e.g. by withdrawal of security certificate) or prematurely by the user.

The expected commercial lifetime of a V-ITS-S is generally around 10 years. The lifetime of an R-ITS-S is usually (significantly) longer. The definition of the life-cycle stages, including the time limitation of certificates and the management of imposed withdrawal of type approvals will need attention during the downstream stakeholder consultation and beyond.

It is assumed that the ANZ CAF will endeavour to be consistent with and leveraging off best practice related to placing of products on the ANZ market and ongoing developments of international C-ITS CAFs, notably in the EU.

[32] E.g. based on FCAI 2017.

[33] Consistent with the EU Blue Guide (European Commission 2016b) and the guiding principle that more recent products need to ensure backwards compatibility with older ones.

It is noted that part of Australian's best practice in compliance assessment includes registration and dissemination of approved product types via web registers. It is expected that a web-based register[34] of type approved C-ITS stations will form part of the CAF model. A product that has successfully been subject to conformity assessment may potentially be affixed with a product label, an essential element to enable effective market surveillance and control of the production process[35], and also a 'C-ITS' mark.

It is assumed that ANZ in C-ITS initially will largely follow the EU C-ITS approach, i.e. to initially focus on C-ITS driver safety support messages and in terms of specification and conformity assessment concentrate on the quality of the transmitted data (i.e. the triggering event and the latency of the transmitted data in accordance with the standardised format and defined security mechanisms).

The compliance assessment activities will focus on the vehicle and roadside types of C-ITS stations. In this respect, it is worth noting that the Commonwealth has an established position of harmonising Australian Design Rules with the UNECE (European) standards for vehicles.

Central and personal ITS-stations are currently outside of the scope, but should be able to be included in a future extension of the ANZ C-ITS CAF.

Further, it is assumed that the ANZ CAF that will be implemented initially will need to be adjusted over time in view of experiences in early deployment of C-ITS in ANZ, new C-ITS technologies (e.g. LTE-V2X) and international downstream developments in order to remain fit for purpose.

Conformity assessment vs market surveillance and safeguards

Conformity assessment is the responsibility of the manufacturer.

Conformity assessment must not be confused with market surveillance, which consists of controls by the market surveillance authorities or bodies after the product has been placed on the market. However, both techniques are complementary and equally necessary to ensure the protection of the (public) interests at stake and the smooth functioning of the market.

Why are market surveillance and safeguards needed?

Market surveillance authorities or bodies have to take appropriate (proactive or reactive) measures to deter or prevent the making available on the market and use of non-compliant products. Market surveillance activities are directed towards the protection of health and safety. Additionally, they may also be undertaken with the aim of ensuring fairness and to eliminate unfair competition.

To be able to monitor products on the market, market surveillance authorities or bodies must have the required auditing and enforcement powers, competence and resources, and if appropriate:

- to organise periodic, random and spot checks
- to take samples of products, and to subject them to examination and testing
- to require, upon reasoned request, all necessary information
- to require, upon detection of non-compliant products, the manufacturer to undertake corrective measures, withdrawals or recalls. The measures need to be effective, proportionate to the seriousness of the offence and dissuasive and may be increased if the relevant economic operator has previously committed a similar infringement. In addition to the corrective measures, they may include product bans, penalties and criminal sanctions (such as fines and imprisonment) wherever necessary and possible.

A higher degree of regulatory intervention enables a stronger embedment in the institutional set-up, and hence generally greater inspection, auditing and enforcement powers.

[34] Similar to the Regulatory compliance mark register (https://www.acma.gov.au/Industry/Suppliers/Product-supply-and-compliance/Steps-to-compliance/supplier-registration) and the EU Digital Tachograph (https://dtc.jrc.ec.europa.eu/dtc_vehicle_units_status.php).
[35] Chapter 4.2 on Traceability requirements in the EU Blue Guide (European Commission 2016b).

3.2 Models to be Considered for an ANZ C-ITS CAF

Based on the literature review, the following three high-level policy options for compliance assessment of C-ITS can be differentiated, based on:

- industry certification (e.g. OmniAir in the USA)
- public sector certification[36]
- C-ITS regulation.

These three policy options are among the range of options listed in the *Australian Government Guide to Regulation* (Australian Government 2014). Following the guide, these policy options were complemented by the option of continuity of the current regulatory approach and policy as a (status quo) benchmark.

Hence, the following four policy models form the starting point for elaborating ANZ C-ITS CAF options:

1. Continue current approach ('do nothing' type of option)
2. Industry certification[37]
3. Public sector certification
4. C-ITS regulation.

There is a need to first agree on the main 'pure' models and their main characteristics, whilst recognising the possibility to adopt a hybrid approach of the proposed model options, and to adopt different models for different types of C-ITS stations. The result of the initial evaluation of the main 'pure' model is used as input when elaborating hybrid model options (i.e. refining the options) for consideration of the future work (see also Section 5.2).

In the project brief, it was underlined that the project should strive to adopt a consistent approach to approval of ITS-related products on the ANZ market. In this context, NTC's recent policy paper *Assuring the Safety of Automated Vehicles* (National Transport Commission 2017a) is relevant, considering the large overlap of stakeholders and the similarity of the high-level questions to be addressed in the process of designing an appropriate level of regulatory intervention. Like the high-level options in the NTC's paper (which ranged from continue current approach to accreditation), the level of regulation and assurance by the government increases with each C-ITS CAF option. The options cover the status quo, self-regulation, quasi-regulation and regulation. Generally, a (perceived) low risk or a high appetite for risk tends to lead to a low degree of assurance and level of regulatory intervention (e.g. continue current approach). A low appetite for risk generally tends to lead to a higher degree of assurance and level of regulatory intervention.

These four models are described in the following sections, including illustrations of how the type approval process can be implemented using C-ITS CAF best practice models as examples. Thereafter an outline of a C-ITS CAF in an overarching architecture applicable for the latter three models is presented, followed by an overview of the characteristics of the four models.

The described models were reviewed by and discussed with stakeholders. The results of the stakeholder consultations are presented in Section 4.

3.2.1 Continue current approach

This ('do nothing') model is based on the continuity of the policy and the regulations for placing of products (i.e. C-ITS stations) on the ANZ market, i.e. in accordance with existing road safety laws and consumer laws in Australia and New Zealand as well as the radio spectrum allocated for the use of C-ITS.

[36] Inspired by Austroads proposed *Operationalising ITS product acceptance process* (Austroads 2016), which describes a conceptual model that focussed on ITS in general and not specifically on C-ITS. It should also be noted that no decision has been made to implement this model.

[37] This model was referred to as 'Voluntary industry association certification' in previous working drafts of this report.

An example of this model is the current approval of new and imported vehicles and their operation under the *Motor Vehicle Standards Act 1989*. Safety would be managed through existing safeguards (such as road rules and the *Australian Consumer Law*) without additional regulatory oversight.

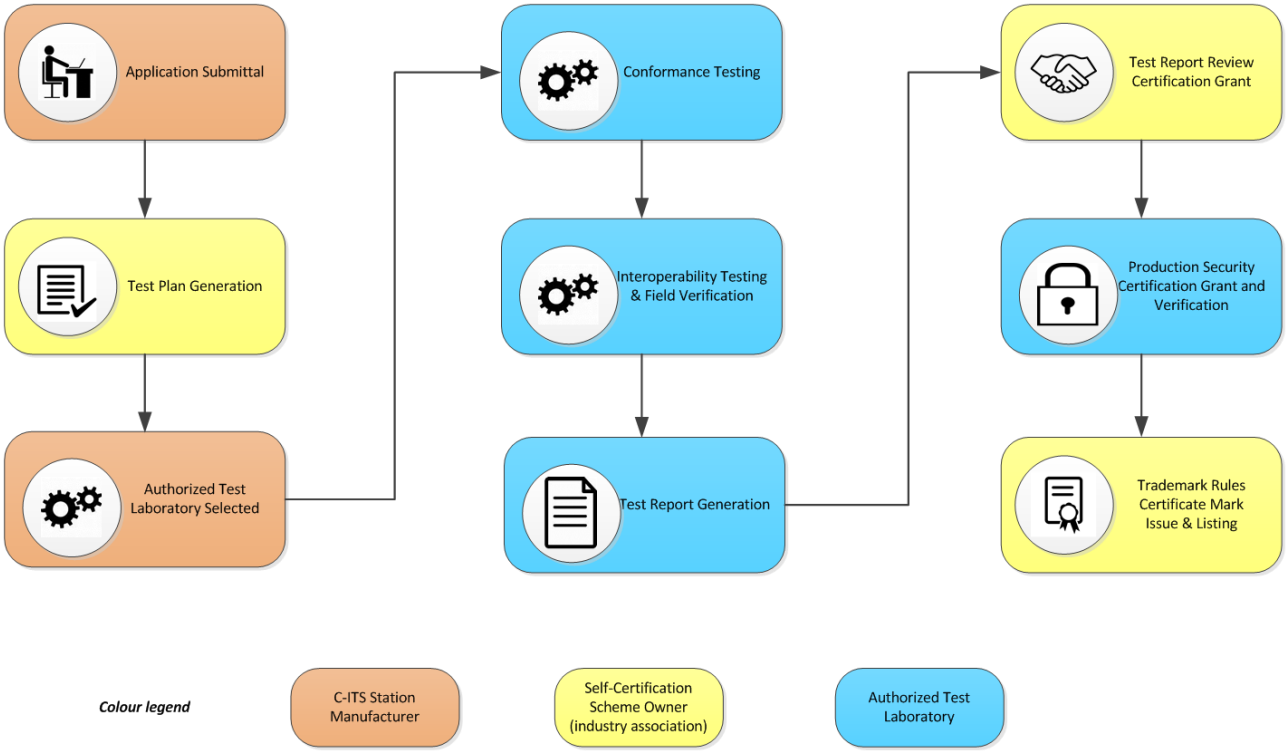
3.2.2 Industry certification

This model assumes that the C-ITS industry in ANZ is responsible for setting the scope of compliance assessment and determining the requirements and test cases/procedures. C-ITS station manufacturers can voluntarily certify their products according to the industry's defined compliance assessment criteria.

Further, the model can be implemented as follows. The manufacturer applies for certification at the industry association and sends its device to one of the authorised test laboratories, accredited by the industry association. This test laboratory performs the testing. The industry association reviews the test results and, if warranted, issues the type approval certificate and enters it into a web-based register.

An example of this model is the OmniAir connected vehicle certification program in the USA, which type approval process is illustrated in Figure 3.1.

Figure 3.1: Main steps of the compliance assessment model based on industry specifications



The main steps of the OmniAir type approval process can be described as follows:

- application submittal by proponent
- test plan generation by C-ITS industry association
- authorised test laboratory selection by manufacturer
- conformance testing by authorised laboratory
- interoperability testing and field verification by authorised laboratory
- test report generation by authorised laboratory
- test report review – certification grant by C-ITS industry association

- production security certification grant and verification by authorised laboratory
- trademark rules certificate, mark issue and listing by C-ITS industry association.

3.2.3 Public sector certification

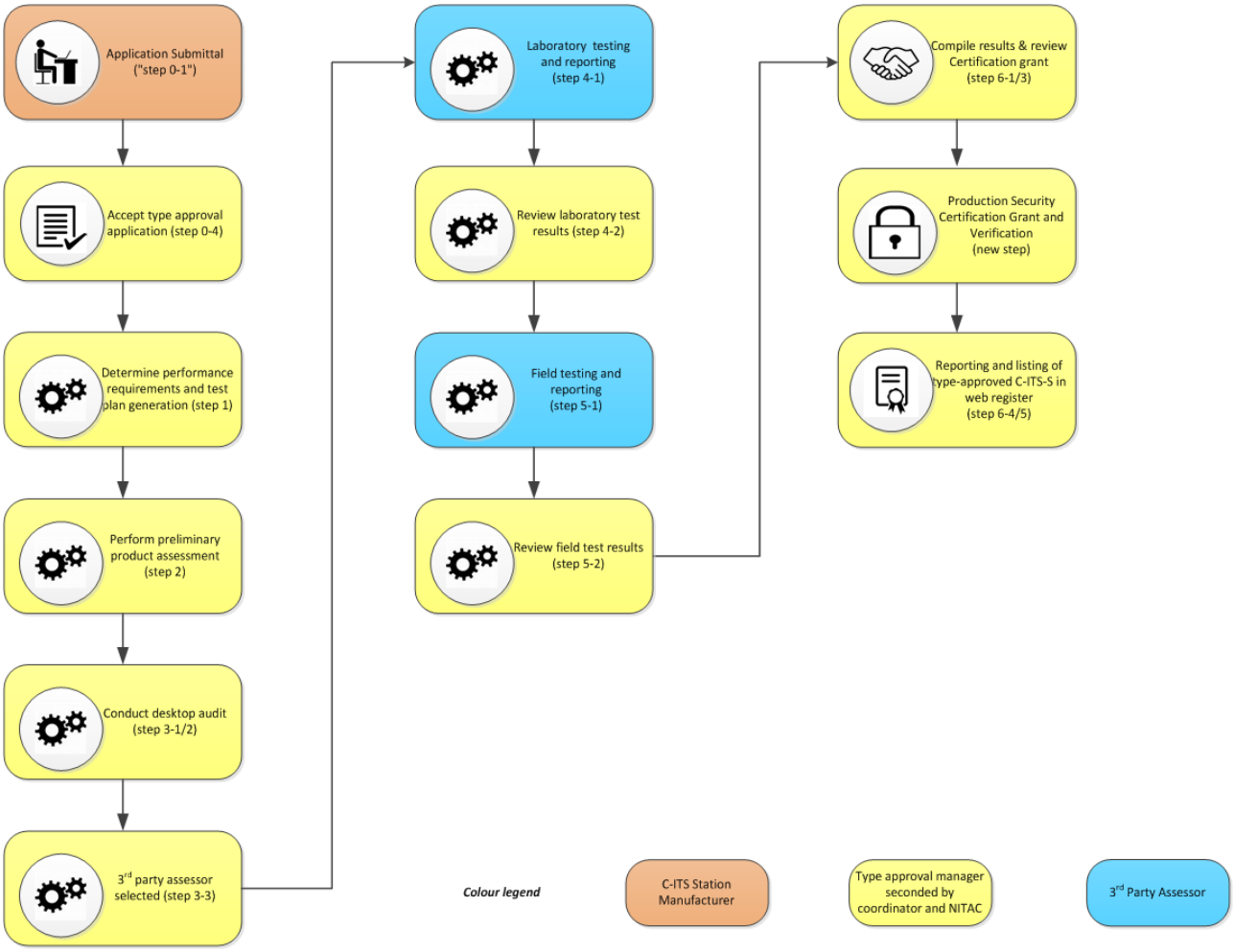
The public sector certification model assumes that a government agency or a group of public authorities is responsible for setting the scope of compliance assessment and determining the requirements and test cases/procedures. It would be mandatory to obtain a C-ITS certificate in order to place C-ITS stations on the public sector market (in particular relevant for R-ITS-S), and virtually also a pre-requisite for placing these on the private sector market ('guarantee to proper functioning with R-ITS-S').

A national C-ITS working group would be responsible for all strategic decisions. A national C-ITS type approval committee (NITAC, under road agency authority) would be responsible for defining the compliance assessment criteria, reviewing the test results and, if warranted, issuing the type approval certificate and entering it into a web-based register. Prequalified third-party assessors would be engaged to carry out testing of C-ITS stations in laboratory tests and field tests.

This model is expected, in view of the commitment by the public sector, to be implemented with a high degree of consistency and underpinned by references to standards, and therefore expected to provide a high level of consumer trust and confidence.

Figure 3.2 shows the main steps of the type approval process, based on Austroads proposed ITS product acceptance process (Austroads 2016).

Figure 3.2: Main steps of the compliance assessment model based on public sector specifications



The main steps of the type approval process can be described as follows:

- Step 0: Accept type approval application
- Step 1: Determine performance requirements
- Step 2: Perform preliminary product assessment
- Step 3: Conduct desktop audit
- Step 4: Conduct laboratory tests by third-party assessor
- Step 5: Perform field tests by third-party assessor
- New step: Production security certification grant and verification
- Step 6: Report and enter into the national type-approved C-ITS stations register.

3.2.4 C-ITS regulation

This model assumes preparation and promulgation of a new or several new C-ITS regulations. Hence, the government is responsible for setting the scope of compliance assessment and determining the requirements and test cases/procedures, potentially by means of regulatory instruments. It would be mandatory to obtain a C-ITS certificate in order to place C-ITS stations on the ANZ market.

It is assumed that the compliance would be assessed predominantly by accredited third parties, which have formally demonstrated their competence to carry out specific conformity assessment tasks (as defined in the ISO/IEC 17000 series of standards; see 0 for an overview), or by the manufacturer in case of the existence of harmonised standards (cf. Figure 2.11).

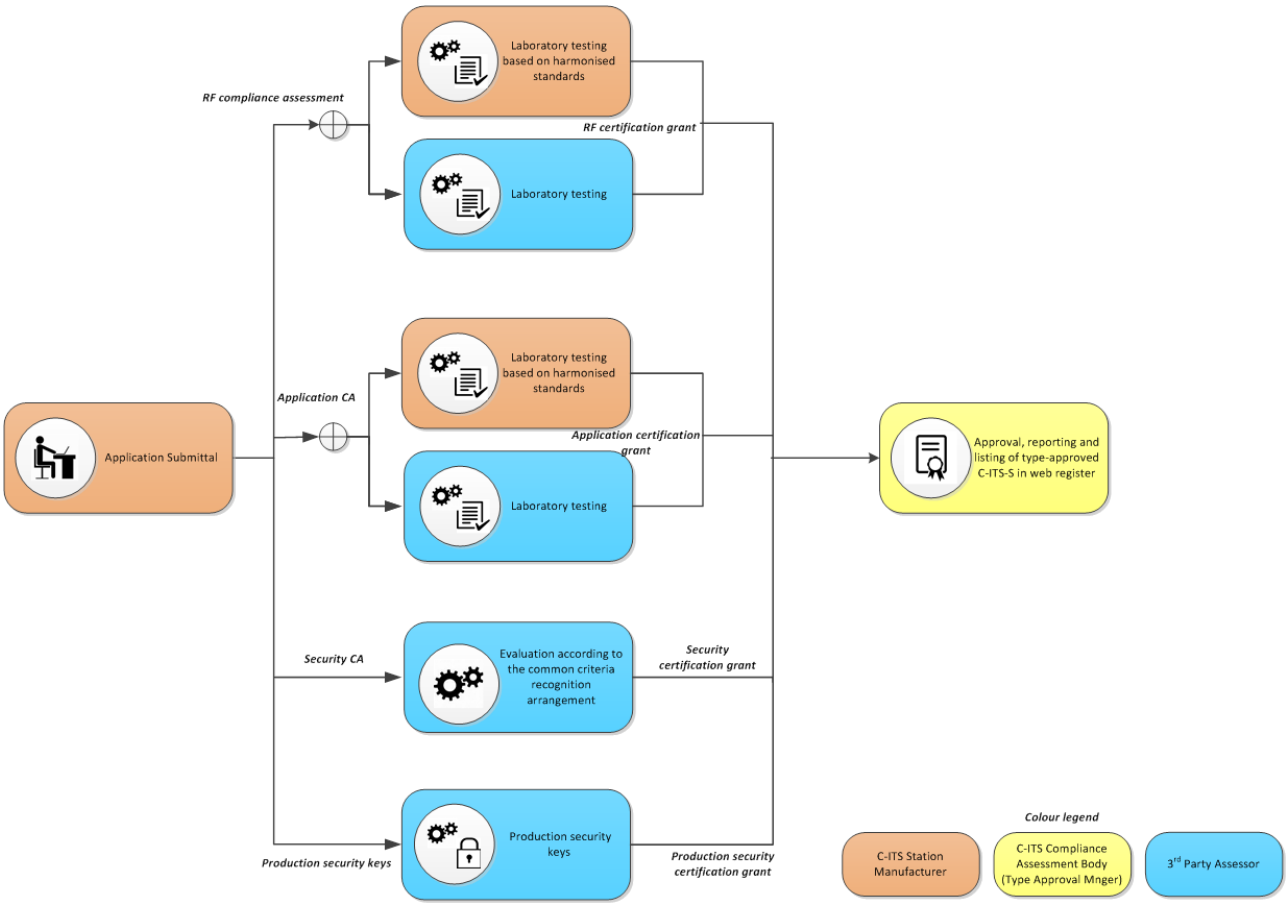
An example of this model is EU's draft C-ITS compliance assessment framework. It foresees the set-up of an appropriate legal and technical framework to implement the proposed roles and compliance assessment requirements and process. A so-called C-ITS compliance assessment body would be established as the central operational body in the compliance assessment process. This body oversees the overall process and manages the day-to-day compliance assessment operation. It defines the governing rules and procedures for the compliance assessment tests and procedures, approves testing results, issues the C-ITS proof of compliance approval and maintains the list of approved C-ITS stations. C-ITS station manufacturers will apply to the C-ITS compliance assessment body and send their device to one of the selected test laboratories and assessment organisations for testing. Optionally they may perform parts of the compliance assessment of radio frequency and application themselves (if authorised).

This model has the potential to be firmly embedded in the institutional set-up, in which authorities potentially could be assigned significant auditing and enforcement powers.

Whereas this model, based on a regulation, potentially could provide the highest level of consumer trust and confidence, a key challenge for the legislator is to safeguard the public interests at stake whilst not stifling innovation and keeping it fit for purpose over time.

Figure 3.3 shows the main steps of the type approval process associated with the new C-ITS regulation. These steps are based on EU's draft C-ITS CAF and its smart tachograph regulation.

Figure 3.3: Main steps of the compliance assessment model based on new regulation



The main steps of the type approval process can be described as follows:

- Conformity assessment of C-ITS stations according to harmonised specifications defined by the compliance assessment body (e.g. NITAC) related to radio frequency matters[38] and transmitted C-ITS messages, with or without the use of third-party assessors (assuming use of harmonised standards such as ETSI EN 302 571); successful assessment yields a functional certificate.
- Evaluation to security protection profiles defined or recognised by the compliance assessment body (e.g. NITAC), by a certified CC assessor; successful assessment yields a security certificate.
- Interoperability certificate, distribution of key and interoperability field test, issued or recognised by the compliance assessment body (e.g. NITAC).
- Successfully completed overall accreditation yields approval of the C-ITS station type and recording in the national type-approved C-ITS stations list through the web register.

3.2.5 C-ITS CAF in an overarching governance architecture

Figure 3.4 outlines how the C-ITS CAF models described in Sections 3.2.2 to 3.2.4 fit into an overarching governance architecture. It should be noted that it is based on EU work that will feed into a proposal for an EU delegated regulation on C-ITS. It incorporates the compliance assessment process described in Figure 2.15. It is important to note that this process description can be used to describe the processes associated with the three models discussed in Sections 3.2.2 to 3.2.4, be it that the identified roles are assumed by different actors and that the range of the functional elements is slightly different.

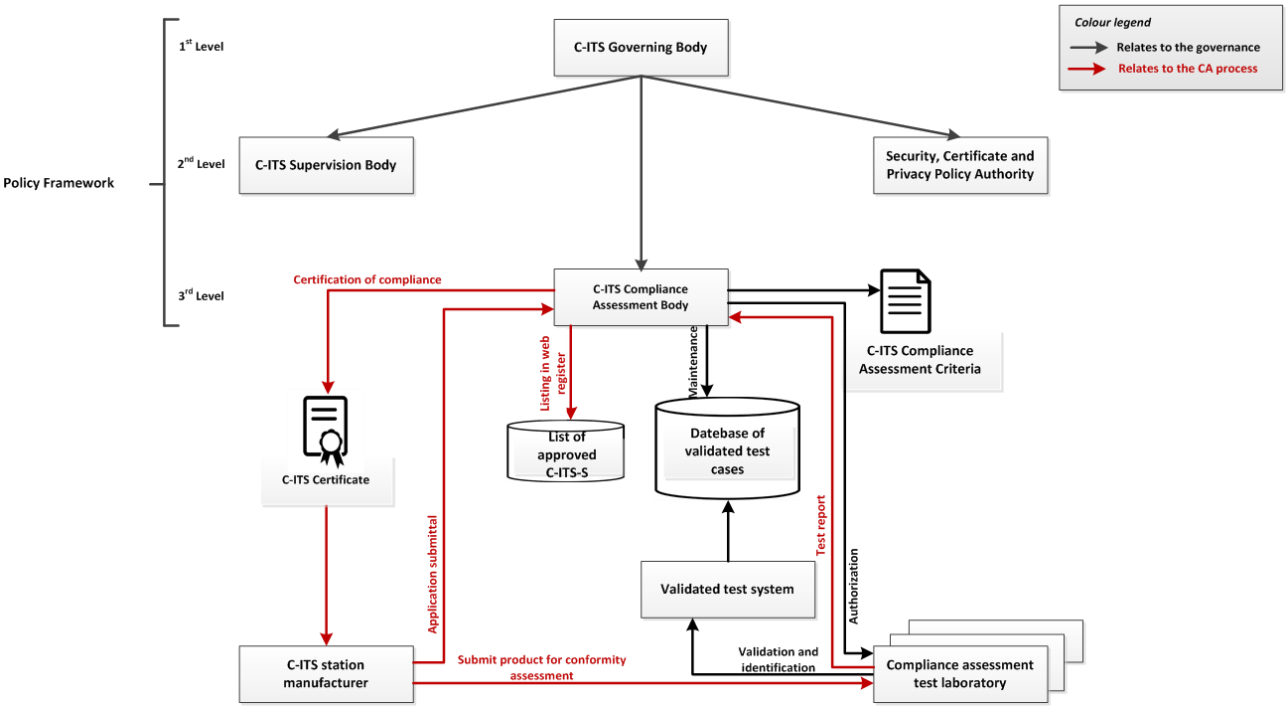
[38] E.g. based on the European harmonised standard ETSI EN 302 571.

The proposed overarching architecture distinguishes policy on the following three different levels:

- First level: The C-ITS governing body is responsible for taking all strategic decisions for the C-ITS scheme.
- Second level: The second level comprises the C-ITS supervision body and the 'C-ITS security, certificate and privacy policy authority'. The C-ITS supervision body is responsible for organising the market surveillance and for detection of problems in the deployment phase (its attitude can range from a proactive to a reactive stance). The C-ITS security, certificate and privacy policy authority is responsible for proposing policy on security, certificate and privacy-related matters for endorsement by the C-ITS governing body.
- Third level: The C-ITS compliance assessment body reports primarily to the C-ITS governing body and is responsible for:
  - overseeing the overall process and management of compliance assessment operation
  - proposing the governing rules and procedures for the compliance assessment tests and procedures, for endorsement by the C-ITS governing body
  - issuing the C-ITS proof-of-compliance approval
  - maintaining the list of approved ITS station models.

In Figure 3.4 the arrows and the associated text in black correspond to the governance. The arrows and associated text in red correspond to the conformity assessment process, as described in Sections 3.2.2 to 3.2.4.

Figure 3.4: C-ITS CAF in an overarching governance architecture



3.2.6 Overview of the C-ITS CAF model options

Table 3.1 provides an overview of main properties of the four model options.

Table 3.1: Overview of the C-ITS CAF model options

Characteristics	Continue current approach	Industry certification	Public sector certification	C-ITS regulation
Level of regulatory intervention	Status quo	Self-regulation Trademark rules and commercial conditions governed by the industry	Quasi-regulation C-ITS certificate virtually a pre-requisite for placing of C-ITS stations on the ANZ market	Regulation Mandatory to obtain a C-ITS certificate in order to place C-ITS stations on the ANZ market
Who defines the compliance assessment criteria?	No separate compliance assessment of C-ITS stations Safety of C-ITS stations managed through existing safeguards (e.g. road safety laws, consumer protection laws in ANZ) No additional regulatory oversight or reporting to government No explicit protections relating to after-market modification of C-ITS stations	Industry, but noting that currently the majority of original suppliers come from overseas, which may limit the influence of the industry in ANZ With or without references to standards Could potentially be supported by government and road agencies	Public sector, e.g. the government agency together with the road agencies With references to relevant standards Government responsible for defining major technical decisions, such as determining requirements (e.g. national C-ITS committee) – but with no legal recognition Government responsible for defining test cases and test procedures (e.g. national C-ITS committee) – again without no legal recognition	Government With references to relevant standards Government responsible for setting up technical framework with legislative requirements for products, such as assessment criteria, reference specifications and system profiles (e.g. C-ITS governing body; framework to be used by C-ITS operation body and third-party assessors) Government responsible for defining conformity assessment procedures (e.g. C-ITS governing body; framework to be used by C-ITS operation body and third-party assessors)
Who examines the product against the requirements?	N/A	Third-party assessor prequalified by the industry (association) The manufacturer could potentially carry out part of the assessment based on test specifications recognised by the industry (i.e. mimicking the status of harmonised standards in European legislation)	Third-party assessor prequalified by the public sector The manufacturer could potentially carry out part of the assessment based on test standards recognised by the public sector (i.e. mimicking the status of harmonised standards in European legislation)	Accredited third-party assessor, which has formally demonstrated its competence to carry out specific conformity assessment tasks (as defined in ISO/IEC 17000; see Appendix C) The manufacturer could potentially carry out part of the assessment based on test standards recognised in the C-ITS regulation (i.e. mimicking the status of harmonised standards in European legislation)
Who makes the overall appraisal of a product's conformity and grants the certificate?	N/A	Industry association (C-ITS type approval manager)	C-ITS type approval manager, on behalf of national C-ITS committee	Accredited third-party assessor

Characteristics	Continue current approach	Industry certification	Public sector certification	C-ITS regulation
Who performs the market surveillance?	Current public oversight of road safety laws and consumer protection laws in ANZ	Current public oversight of road safety laws and consumer protection laws in ANZ In addition, industry association surveillance within the framework of private law Weak auditing and enforcement power	Current public oversight of road safety laws and consumer protection laws in ANZ In addition, public sector surveillance Enhanced auditing powers conceivable	Current public oversight of road safety laws and consumer protection laws in ANZ Strong embedment of governmental power to audit or enforce use of compliant C-ITS stations in institutional arrangement (mandated in law)
Dissemination of C-ITS type approved products	N/A	C-ITS register, operated by the industry (association)	C-ITS register, operated by the public sector	C-ITS register, operated by the government or on its behalf
Example of how the operations of the compliance assessment may be financed N.B. each model will have sub-options for funding	N/A	Set-up: membership fees Ongoing: fees paid by applicants	Set-up: funding by the public sector (government and road agencies) Ongoing: fixed costs covered by the public sector, certification fees paid by applicants	Set-up: government funding Ongoing: fixed costs covered through government funding, fees paid by applicants
Overall characteristics	Legal requirements fall well behind industry operating standard, insufficient safety assurance	Requirements keep pace with industry operating standard but perceived and actual independence issues arise	Independence assured, sufficient regulatory agility to accommodate industry innovation, safety ensured	Industry impeded and innovation held back due to cumbersome full-regulatory processes

3.3 Evaluation Criteria

The proposed evaluation criteria in Table 3.2 take into account the input in the project brief and are augmented with criteria stemming from the NTC policy paper.

Table 3.2: Proposed evaluation criteria for the C-ITS CAF model options

Criteria	Description
1. Safety, environmental and user protection	• The model should support C-ITS safety including ongoing safety over the lifespan of the C-ITS station. • The model should allow for specific issues to be addressed including security, user data protection and environmental protection over the lifespan of the C-ITS station.
2. Innovation, flexibility and responsiveness	• The model should be technology-neutral and allow innovative solutions. • The model should allow government to respond and adapt to the changing market and evolving technology.
3. Accountability and probity	• The model should ensure the decision-making process is transparent, accountable and, where appropriate, appealable. • The model should provide certainty about who is responsible and legally accountable for the C-ITS station throughout its lifespan.
4. Regulatory efficiency	• The model should be as efficient as possible and result in the least cost for industry and government, proportionate to the risk. • The model should minimise structural organisational and regulatory change necessary to implement the model. • Effects on industry are minimised where possible.
5.International and domestic consistency	• The model should support a single national approach, or state-based approaches that are nationally consistent. • The model should support consistency with the EU C–ITS approval processes and international standards should be recognisable.
6. Other policy objectives	• The model should be able to support non-safety policy objectives such as traffic management and the provision of data for enforcement purposes.
7. Timeliness	• The model should be able to be implemented and operational within two years when the technology is ready.

3.4 Assessment of the C-ITS CAF Models

The assessment of the models in Table 3.3 served as a support and so as to spark critical reviews by and discussions with the stakeholders. The results of the consultations related to the evaluation of the models are presented in Section 4.2.3.

Table 3.3: Assessment of the C-ITS CAF model options against the proposed evaluation criteria

	Fully meets the evaluation criterion
	Partially meets the evaluation criterion
	Unlikely to meet the evaluation criterion

Criteria	Continue current approach	Industry certification	Public sector certification	C-ITS regulation
1. Safety, environment and consumer protection	Continuity of policy and relevant regulations Outdated regulations – may potentially expose road users to unknown C-ITS road safety risks (in particular related to after-market modification) and increased risk of C-ITS non-interoperability	Specifications/standards known by all those involved in the industry Not its primary role to elaborate and govern rules that safeguard the public interests	Part of its primary role is to safeguard the public interests Expected high degree of consistency in the definition of the compliance assessment criteria, underpinned by references to standards[39]	Part of its primary role
2. Innovation, flexibility and responsiveness	Would support innovation by not constraining manufacturers, but the lack of explicit regulation or policy guidelines could create uncertainty	Would support evolving technology and a changing market; the room for innovation would reflect the needs of the industry (association) Would reflect the interests and technologies promoted by the industry (association)	Would require the public sector to implement and govern an overarching C-ITS architecture Framework can relatively easily be updated and improved over time Would require the public sector to build up and maintain expertise in C-ITS technologies	Would be a major challenge to adopt timely legislation and keeping it fit for purpose over time.
3. Accountability and probity	Safety managed through existing safeguards in road safety and consumer protection laws Would not ensure that it is always clear who is legally responsible for C-ITS induced road safety risks	Some risks would potentially be reduced through enhanced management of unwanted signals and messages Self-regulation does not provide the governments with certainty that safety risks are being managed	Some risks would potentially be reduced through enhanced management of unwanted signals and messages	Some risks would potentially be reduced through enhanced management of unwanted signals and messages Expected clarification of the legal accountability for C-ITS in the new C-ITS regulation
4. Regulatory efficiency	Would not require regulatory change but safety-related risks not appropriately managed (e.g. due to lack of appropriate protection against harmful radio interference)	Potentially reduced safety-related risks Set-up costs financed by membership fees Ongoing: fees paid by applicants	Reduced safety-related risks Set-up costs financed by the public sector Ongoing: fixed costs covered by the public sector, certification fees paid by applicants	Minimised safety-related risks at the lowest cost. Preparatory and set-up costs financed the government Ongoing: fixed costs covered through government funding, fees paid by applicants
5.International and domestic	Lack of explicit regulation	Would allow for	Would allow for	Would allow for

[39] Potentially complemented by so-called public top-up specifications, in case the underlying relevant standards are too broad and not sufficiently profiled for ANZ's context or purposes.

Criteria	Continue current approach	Industry certification	Public sector certification	C-ITS regulation
consistency	or policy guidelines could create uncertainty regarding which approach to follow Mutual recognition would most likely not be possible ANZ C-ITS stations will need to comply with the anticipated EU C-ITS regulation if placed on the EU market: EU C-ITS stations could potentially be placed on the ANZ market	consistency with the EU approach The degree of consistency, use of standards and the quality of the governance are uncertain Some degree of mutual recognition is likely Potentially some of the compliance assessment criteria would be common and based on (EU) harmonised standards, and not be subject to reassessment	consistency with the EU approach Expected high degree of consistency, extensive use of standards and an appropriate governance Some of the compliance assessment criteria would be common and based on (EU) harmonised standards, and not be subject to reassessment	consistency with the EU approach Likely that some or all compliance assessment criteria could be common and form part of a mutual recognition agreement with the EU
6. Other policy objectives	Would not provide opportunities to support other policy objectives	Would provide a light-touch mechanism to support other policy objectives, such as traffic management	Would provide a mechanism to support other policy objectives, including traffic management	Could support other policy objectives, but the primary C-ITS regulatory policy objectives would be the focus
7. Timeliness	Continuity of policy and relevant regulations	Initial CAF may potentially be implemented within two years	Initial CAF may potentially be implemented within two years	Very unlikely to be implemented within two years[40] It generally takes more time to prepare and adopt primary and secondary legislation

[40] It is unlikely to be able to make nationally consistent legislation in under five years using any of the various ways this can happen such as Commonwealth law, model law or applied law. Even just negotiating the content and form across eight or nine jurisdictions takes a long time.

4. Stakeholder Consultation

4.1 Approach, stakeholders and questions

The stakeholder consultations were undertaken to seek feedback on the proposed overall scope and assumptions for the ANZ C-ITS CAF, outlined models and on the evaluation, in the endeavour to identify a model that is fit for purpose or the direction for the future work.

An Explanatory Note on the C-ITS compliance assessment framework (16 February 2018) was used as the main support for the stakeholder consultation. The note, prepared by the project team, was intended to foster a common basic understanding of the C-ITS compliance assessment and to assist stakeholders in reflecting and taking position on relevant issues, as part of the preparation for the consultation. It was used as a basis for the discussion on the following key themes:

- overall scope of the C-ITS CAF (Section 6 in the note and in particular questions 1 to 5, as outlined in Table 4.3)
- model options (Section 7 in the note and in particular questions 6 to 10, as outlined in Table 4.3)
- evaluation criteria and evaluation of the models (Section 8 in the note and in particular questions 11 to 15, as outlined in Table 4.3).

For especially interested stakeholders, the project team had also made available the C-ITS CAF Elaborated Findings working paper (16 February 2018), which provided more detailed information and also included different type approval processes elaborated by the project team.

The process involved consultation with 84 stakeholders ranging across 42 organisations. The consultations were undertaken via the following three main formats:

- High-level workshop with key decision makers on the afternoon of 14 March 2018 in Melbourne. Attendees of the high-level workshop are outlined in Table 4.1.
- High-level discussion with selected agencies in five separate meetings from 12 to 16 March 2018. The agencies consulted and their representatives are outlined in Table 4.2.
- Invitation to the stakeholders to provide written comments to the questions contained in the note.

Table 4.1: High-level workshop attendees

Type	Name	Organisation
Austroads	Niko Limans	Austroads
	Chris Jones	Austroads
Road agencies	Richard Zhou	VicRoads
	Wayne Harvey	VicRoads
	Malith Nanayakkara	VicRoads
	Steven Shaw	Roads and Maritime Services
	Noel Peters	Transport and Main Roads
	Geoffrey McDonald	Transport and Main Roads
	Stuart Allen-Keeling	Transport and Main Roads
	Kamal Weeratunga	Main Roads Western Australia
National Government	Sharon Ronald	Department of Infrastructure and Regional Development

	Scott Martin	Department of Infrastructure and Regional Development
NTC	Marcus Burke	National Transport Commission
ACMA	Gabriel Phillips	ACMA
ARRB	Dickson Leow	ARRB
Industry	Anto Komarica	Kapsch TrafficCom
	Rodrigo Perez	Kapsch TrafficCom
	Ian Oxworth	ConnectEast
	Carl Liersch	Bosch Australia
	Alan Koncar	Bosch Australia
	Matthew Banks	Cohda Wireless
	Fabien Cure	Cohda Wireless
	Peter Girgis	2SG Bigmate
	Holger Arends	Telstra
	Jamie Smith	Telstra
	Todd Essery	Telstra
	David Ross	Telstra
	Lance Brand	Q-Free
	Rory Stott	Transurban
	Jonathan Ball	Tomtom
	Mike Hammer	GM Holden/FCAI
	Jason Gomes	Toyota Australia
	Mario Filipovic	Toyota Australia
	Brett Hyland	NATA
	Philip Lloyd	TCA
	Simona Mihaita	Data61/CSIRO
	Peter Chalmers	Transmax
	Scott Benjamin	WSP
Project Team	Jesper Engdahl	Rapp Trans
	David Green	ARRB

Table 4.2: High-level discussion with selected agencies

Meeting	Organisation	Representative
TMR	Transport and Main Roads	Geoffrey McDonald
	ditto	Jason Venz
	ditto	Melissa Perkins
	ditto	David Jones
	ditto	Kym Eldridge
	ditto	Stuart Allen-Keeling

	ditto	Lilanthi A Balasingham
RMS and TfNSW	Roads and Maritime Services	Steven Shaw
	ditto	Sharon Kindleysides
	ditto	Farzad Naziri
	Transport for New South Wales	John Wall
DIRDC	Department of Infrastructure, Regional Development and Cities	Sally Todd
	ditto	Sharon Ronald
	ditto	Scott Martin
	ditto	Andrew Dankers
VicRoads	VicRoads	Wayne Harvey
	ditto	Richard Zhou
	ditto	Chris Jones
	ditto	Blake Harris
NZ MoT and NZTA	New Zealand Ministry of Transport	Lee McKenzie
	New Zealand Transport Agency	Dirk Van Der Walt
	ditto	Mark Rounthwaite
	ditto	Michael Cummins
	ditto	Steve Penman
	ditto	Bruce Currie
	ditto	Glen Bunting
	ditto	Deryk Whyte

The individual consultations were based around the 15 questions outlined in Table 4.3. However, consultation was somewhat fluid and not rigid so it focussed of different aspects related to compliance and determined by the discussions.

For the workshop, the background of the literature review was presented before delving into the questions outlined in Table 4.3.

Table 4.3 outlines the stakeholder consultation questions. The questions should be read within the context of the Explanatory Note[41] for a full understanding. A brief contextual preamble is given to the questions in the rightmost column in the table, whenever necessary, in order to allow for a basic understanding of the questions without the need to read the note.

Table 4.3: Outline of stakeholder consultation questions

Theme	Question number	Question
Overall C-ITS CAF scope and basic assumptions	1	**Framework scope** C-ITS stations (as opposed to C-ITS components or systems) Follow largely the EU C-ITS approach Initially focus on vehicle and roadside types of C-ITS stations Central and personal ITS-stations should be able to be included in a future extension

[41] C-ITS Compliance Assessment Framework – Explanatory Note can be obtained via Austroads C-ITS Project Manager, Mr. Niko Limans (Niko.Z.Limans@tmr.qld.gov.au).

		Do you agree with the assumptions above? If not, how should these be modified?
	2	**Application scope** Minimise the overlap with existing legislation and codes of practice – C-ITS CAF only includes the C-ITS-specific aspects Should so-called safety-related C-ITS applications (e.g. flooded road warning) be part of the CAF as well?
	3	**Legislative interactions** C-ITS-specific aspects • C-ITS radiofrequency conformity assessment. C-ITS stations in Australia must comply with ACMA ITS Class Licence. Requirements are not yet established for New Zealand • C-ITS applications, noting that at present these are requirements not defined. The main candidate applications to form part of the framework are: – regulatory – safety critical (e.g. red light violation) – enhanced user protection (e.g. vulnerable road user protection) – enhanced environmental protection (e.g. geo-fencing of high-consequence dangerous goods in tunnels or in urban areas) – C-ITS security-related requirements, noting these are currently not established – C-ITS data protection conformity assessment, in case specific principles would be added on top of the ANZ privacy acts Do you agree with the assumptions above? If not, how should these be modified?
	4	**Life-cycle management** C-ITS station life-cycle stages include: • placing on the market: a product is placed on the market when it is made available for the first time on the ANZ market, with the necessary security certificate • withdrawal from the market: either at the end of the certification period, prompted prematurely by the market surveillance authorities due to non-compliance or prematurely by the user What would be a suitable definition of the life-cycle stages of a C-ITS station for the CAF, including the time limitation of certificates and the management of imposed withdrawal of type approvals?
	5	**Further basic assumptions** Placement of C-ITS stations on the market and in service Conformity assessment procedures at the time of placing on the market in two steps (incl. type approval) In case the manufacturer (or representative) makes a significant change of the product in service, the entity is responsible for reassessing and ensuring that the product complies with C-ITS CAF requirements before the modified product is introduced into the market Registration and dissemination of approved product types via web registers, compliant C-ITS stations affixed with a product label and potentially also with a 'C-ITS' mark CAF will need to be adjusted over time in view of experiences in early deployment of C-ITS, new C-ITS technologies (e.g. LTE-V2X) and international downstream developments in order to remain fit for purpose Do you agree with the assumptions above? If not, how should these be modified?
Main models and overarching governance architecture	6	**Relationship between C-ITS CAF and AV SAS** What is your view on the relation between the C-ITS compliance assessment framework V-ITS-S and the proposed safety assurance system for automated vehicles? For example, should both processes (in the future) be merged?
	7	**Compliance assessment policy options** C-ITS CAF high-level model options • continue current approach

		• industry certification[42] • public sector certification • C-ITS regulation Any other policy options that ought to be considered?
	8	**CAF model options** Do you agree with the description of the models? If not, how should it be modified?
	9	**International harmonisation of C-ITS CAF** Should there be an agreement for accepting international approvals of C-ITS stations (in particular V-ITS-S)?
	10	**CAF governance architecture** Outline of the C-ITS governance architecture – distinguish policy at three levels • 1st level: C-ITS governing body: takes all strategic decisions for the C-ITS scheme • 2nd level: C-ITS supervision body and certificate and privacy policy authority • 3rd level: C-ITS compliance assessment body Do you agree that an overarching C-ITS governance model is needed for ANZ and with the outlined model? If not, what is your vision regarding a suitable C-ITS governance model for ANZ?
Evaluation criteria and evaluation of the models	11	**Evaluation criteria** Proposed evaluation criteria: 1. Safety, environmental and user protection 2. Innovation, flexibility and responsiveness 3. Accountability and probity 4. Regulatory efficiency 5. International and domestic consistency 6. Other policy objectives 7. Timeliness Are the proposed criteria for the assessment of the identified models suitable and sufficient to decide on the best compliance assessment model for C-ITS in ANZ?
	12	**Evaluation criteria priorities** Which criteria are deemed most important?
	13	**General CAF model assessment feedback** What is your general feedback on the assessment?
	14	**Preferred CAF model(s)** Which of the models do you prefer and what are the main reasons?
	15	**Transitional considerations** Should the government adopt a transitional approach to the development of compliance assessment of C-ITS?

4.2 Key Findings

Appendix D provides the key comments noted in the stakeholder consultation high-level workshop and in the high-level discussion meetings with selected agencies, as well as for the six sets of written comments received.

The overall key findings from the stakeholder consultations are summarised in the next section.

[42] Referred to as 'Voluntary industry association certification' in the Explanatory Note and in previous working drafts of this report.

4.2.1 Overall scope and basic assumptions

Framework scope: The proposed initial scope and the need to adjust it over time were essentially endorsed. Hence, the current focus of the CAF is on V- ITS-S and R-ITS-S, whereas C-ITS-S and P-ITS-S should be able to be included in a future extension of the framework. Moreover, it is recommended to consider the following adjustments and clarifications of the overall scope:

- Restrict the scope to C-ITS using 5.9 GHz, i.e. leave regulatory telematics and communications on existing cellular to traffic management centre/data portals out of the scope. It should be noted that the latter is already deployed. Leaving the latter outside the scope would be consistent with the endeavour to align the C-ITS CAF with existing regulations and codes of practice.
- Consider the potential inclusion, in a later stage, of in-vehicle device environmental requirements and associated conformity assessment criteria as part of the scope, noting that ANZ experience environmental challenges (e.g. dust, vibration, ranges of temperature and humidity) that can adversely affect the reliability of V-ITS-S. The potential future extension could be considered after the initial setting up of the CAF (by the governing body).

Application scope: The stakeholders endorse the focus of the conformity assessment on communication protocols and application messages. The CAF should provide a framework in which the compliance model ties back to the risk of the application in which the compliance model is to apply. The CAF model required for the applications should be adaptable, reflecting the risk and consequence of that application misbehaving. It is recommended to consider grouping the types of applications into the following four areas:

1. Regulatory (e.g. red light violation) – CAF required, e.g. legislation
2. Warning (e.g. debris on the road, blackspot) – CAF required, e.g. self-compliance
3. Traffic operation (e.g. management of intersections and green corridors) – CAF required, e.g. some compliance required
4. Advisory – no CAF required, no compliance required.

Compliance assessment for the latter can be left out of the CAF and to the industry to sort out.

- **Legislative interactions**: The comments received endorse the proposed approach to seek to align the CAF with existing regulations and codes of practice in ANZ and to include the C-ITS security-related requirements. It is recommended to explicitly highlight the scope of the CAF and that other legal applicable regulations will need to be adhered to in the terms of reference for the CAF and to the applicants.
- **Life-cycle management**: The stakeholders generally support the five life-cycle stages as defined in HTG and ETSI TS 102 941. Support was expressed for the proposed base premise (i.e. ‘once approved, always approved’ status assuming no product update, even in the event of the CAF requirements being subsequently revised) and the approach for how to deal with technology provider self-motivated product updates, namely:
  - It is recommended to consider a mechanism to mandate forced reassessment or withdrawal when, for example, a critical security exploit is discovered that could threaten community safety, and thus results in a mandatory update of the CAF requirements.
  - The importance of seeking to ensure backwards compatibility was underlined and it is recommended to form part of the guiding principles to be duly considered in the governance of the C-ITS CAF (by the governing body).
- **Further basic assumptions**: It is agreed that best practice compliance assessment models include the registration and dissemination of approved product types via public registers, and that a web-based register of type-approved C-ITS stations should form part of the CAF model. Further, the importance of including market surveillance in the overall framework is underlined.

4.2.2 Main models and overarching governance architecture

- **Relationship between C-ITS CAF and AV SAS**: It is recommended to consider a CAF for ANZ with regard to the convergence of connected and automated vehicles, either by clearly articulating the boundaries of what is envisioned as two separate frameworks, or by scoping a more holistic framework. It is recommended to seek adoption of a consistent and whenever sensible a common approach, e.g. a coordinated approach in ANZ for evaluation of security-related requirements for C-ITS, connected and automated vehicles.
- **Compliance assessment policy options**: The four options put forward capture the four distinct options that are relevant to consider. They were intentionally 'pure' model options, with the aim of achieving a common view on the main pure model options and their main characteristics. The possibility to adopt a hybrid approach of the proposed model options and to adopt different models for different types of C-ITS stations needs to be highlighted. Looking ahead, the development of the preferred model will almost certainly be a hybrid model, with a mix of multiple options.
- **CAF model options**: The description and the high-level characteristics provided for the four main models are supported. Continuation of the current approach (option 1) generally appears to be the least attractive of the four main options. A CAF purely based on one of the three remaining options, may not be fit for purpose. Comments offer some advice where these are deemed suitable, largely endorsing the guidance given in the Explanatory Note.

  The stakeholders underlined that the C-ITS regulation (option 4) would only be warranted in rare cases where a very high level of assurance is required over the standards, policies and processes used. They generally agree with the Austroads summary of this option. 'Whereas this model potentially could provide the highest level of consumer trust and confidence, a key challenge is to timely deliver the regulation and keep it fit for purpose over time'. That is certainly the biggest hazard with this option.

  Stakeholders concur with the proposed basic principle that it is the manufacturer that is responsible for demonstrating compliance, which depending on the risk may indeed include the option to undertake this through self-assessment.
- **International harmonisation of C-ITS CAF**: The feedback received underlines the importance to embrace the mutual recognition principle. It is recommended to adopt relevant international standards and recognise overseas type approval procedures, even if only applicable for a fraction of the ANZ CAF requirements and compliance assessment criteria.
- **Overarching C-ITS governance**: The feedback received confirms the need and the importance to set up an overall governance model for C-ITS, which includes notably the governing body and the security, certificate and privacy policy authority. It is recommended to seek to leverage off the existing vehicle governance model (i.e. existing ADR model, processes and procedures), and to consider setting up either the proposed model or a combined and lighter governance model for C-ITS/connected and automated vehicles.

4.2.3 Evaluation criteria and evaluation of the models

- **Evaluation criteria**: The proposed evaluation criteria in the Explanatory Note are broadly supported by the stakeholders and considered adequate.

  However, it is should be noted that there was no full consensus regarding criterion 2 'Innovation, flexibility and responsiveness'. The differences of opinion stem from the tension between the need to not stifle innovation (part of criterion 2) and the need for stability for C-ITS to be developed and largely deployed. Indeed, stakeholders expressed fundamentally different views regarding their relative importance. A few stakeholders stress that technology-neutrality may result in proprietary solutions and that this fragmentation may conflict with interoperability, industry stability and minimising barriers to entry. It is feared that innovation, especially based on the principle of technology-neutrality, may lead to undesirable variability which may 'kill C-ITS deployment'. However, the majority of stakeholders underline that the evolving nature of standards, technologies, use cases, etc. mean that innovation, flexibility and responsiveness are crucial to the early part of C-ITS deployment.

- **Evaluation criteria priorities**: The criteria that appear to be the highest ranked ones are: safety, environmental and user protection (criterion 1), international and domestic consistency (criterion 5), flexibility and responsiveness (amended criterion 2) and timeliness (criterion 3). Whereas it is probably difficult and not essential to establish a broadly agreed ranking of the criteria from highest-to-the-lowest priority, it could make sense to assign the criteria into two (or three) overall bands. The cited criteria would in that case fall in the high-priority band.
- **General CAF model assessment feedback**: The outcome of the assessment is broadly endorsed.
- **Preferred CAF model(s)**: Stakeholders generally appear to favour the adoption of a hybrid approach and potentially different models for the V-ITS-S and R-ITS-S, predominantly favouring a public-sector certification approach for the latter. However, several stakeholders note that it is premature at this stage to choose the model(s), given the necessary desirable prerequisites are not in place. It is recommended to fill these gaps before deciding on which model(s) to adopt (see Section 5 for considerations on the future and on what the mix could look like).

  Further, some elements may over time need to be hardened into legislation, for example, to support a regulatory use case, but this should not be an initial position while so much of the underlying frameworks are in flux, and the deployment use cases are unclear.
- **Transitional considerations**: As with any significant initiative, a transitional approach is of benefit to government, industry and those appointed to oversight the compliance assessment model introduced. The risks associated with a 'big bang' introduction typically far outweigh any perceived benefits of concurrent universal adoption. It is recommended to use transition arrangements and a staged adoption of an ANZ CAF, e.g. along geographical lines or by vehicle type. It is recommended to consider preparation of an initial guidance note, similar to the Austroads/NTC guidelines for trials of automated vehicles, ideally prepared jointly with the FCAI/Truck Industry Council.

5. Discussion on Future Work and Main Findings

The stakeholders' views are particularly important in the design of an ANZ C-ITS CAF. Based on the outcome of the stakeholder consultation, several options and open issues around the development of the ANZ C-ITS CAF were drafted and discussed with the Project Reference Group in a telephone conference on 7 June 2018 to identify the preferred direction. The next sections present considerations on the future work and on the hybrid model options, taking into account the guidance of the Project Reference Group.

5.1 Considerations on the future work

The main findings from the stakeholder consultation revealed that it is currently premature to choose the CAF model, given the range of elements of C-ITS that are still in the development phase (evolving policies, use cases, standards, technologies, SCMS). This section offers guidance on the future work, so that an informed decision on the preferred CAF model can be made and so as to progress its development.

1. **Set up an ANZ C-ITS Platform**

   The platform, mirroring Europe's C-ITS platform, will address the main barriers and enablers identified for deployment of C-ITS in ANZ.

2. **Determine the overall objective, role and scope of the ANZ C-ITS CAF**

   There is a need for a C-ITS strategy/policy, ideally developed jointly by Australia and New Zealand. Also, Day 1 applications, C-ITS use cases and the associated message sets need to be defined and assigned to an application area (see Section 4.2.1), noting that this would provide a more solid basis for the further development of the C-ITS CAF.

   In parallel, it is recommended to consider a CAF for ANZ with regard to the convergence of connected and automated vehicles, either by clearly articulating the boundaries of what is envisioned as two separate frameworks, or by scoping a more holistic framework. It is recommended to seek adoption of a consistent and whenever sensible a common approach, e.g. a coordinated approach in ANZ for evaluation of security-related requirements for C-ITS, connected and automated vehicles.

3. **Set up the C-ITS governance model**

   Thereafter, there is a need to refine and select the CAF model(s) and set up an overarching governance model for C-ITS, which includes notably the governing body and the security, certificate and privacy policy authority. The governing body needs to be tasked and given the mandate to outline a high-level implementation plan, based on a staged approach for the development and deployment of the C-ITS CAF in ANZ. The financing of the set-up and (trial) operations of the CAF need to be answered. It is recommended to seek to leverage off the existing vehicle governance model (i.e. the existing ADR model, processes and procedures), and to consider setting up either the proposed model or a combined and lighter governance model for C-ITS/connected and automated vehicles.

4. **Prepare the establishment of the SCMS**

   Progress and prepare the establishment of an SCMS for ANZ, whilst seeking to leverage off existing relevant security-related frameworks (e.g. the Common Criteria Recognition Agreement based on ISO/IEC 15408 CC series and the ISO/IEC 27000 ISMS) and exploring the adoption of a common approach with connected and automated vehicles.

   This work should ideally involve DIRDC and the Signals Directorates in Australia and New Zealand.

5. Determine the approval procedures and conformity assessment criteria

Thereafter, one should seek to identify the relevant requirements and test standards, and any profiling needs within these standards, when determining the conformity assessment criteria. It is recommended to adopt relevant international standards and recognise overseas approval procedures, even if only applicable for a fraction of the ANZ CAF requirements and compliance assessment criteria.

In parallel with these main tasks, there is a need to pursue the following:

- the Australian (DIRDC) involvement in UNECE WP.29, notably related to intelligent transport systems and automated driving, and in particular related to cybersecurity and data protection
- the Austroads C-ITS/connected vehicle program
- the Australian involvement in the Harmonisation Task Group, as part of the activities to foster the exchange and adoption of best practice in C-ITS
- Learn from the C-ITS trials and pilots impact assessments: description of the use cases, systems, their vulnerabilities and risks and required mitigation to bring down these to an acceptable level. Some of the mitigation might be compliance assessment.

5.2 Considerations on hybrid model options

Below are some reflections on the hybrid model options, given the main findings from the stakeholder consultation, for consideration in the future work.

The model options are proposed to be designed from the type of application and stations, which reflect the risk and consequence of them misbehaving, as outlined in Table 5.1. As can be seen in the table, R-ITS-S and V-ITS-S are distinguished. A further distinction is made between V-ITS-S OEM and aftermarket devices, whilst noting that the latter are generally perceived as less trustworthy.

Table 5.1: Outline of hybrid model options

Application area	R-ITS-S	V-ITS-S OEM	V-ITS-S aftermarket
Regulatory	C-ITS Regulation (option 4)		
Warning	Public sector certification (option 3)	Industry certification (option 2)	Industry certification (option 2) or Public sector certification (option 3)
Traffic operation	Public sector guidelines or Public sector certification	Public sector guidelines or Public-private guidelines or Industry certification	Public sector guidelines or Public-private guidelines or Industry certification

Regulatory: C-ITS regulation (option 4) should only be warranted in rare cases where a very high level of assurance is required over the policies, standards and processes used (e.g. red light violation, speed violation applications).

Warning: For safety-related messages (e.g. debris on the road, road damage, flash flooding, blackspot, single vehicle), different certification models could apply for the different types of devices. A public sector certification is the predominant approach for the R-ITS-S, an industry certification approach for V-ITS-S OEM, whereas either industry or public sector certification for the V-ITS-S aftermarket devices.

Traffic operation: For traffic-operation-related messages, the appropriate approach could either be based on guidelines, public/industry certification.

For clarity, it is recommended in all cases to adopt relevant international standards and recognise overseas approval procedures, even if only applicable for a fraction of the ANZ CAF requirements and compliance assessment criteria. It is also recommended in general to recognise self-assessment, given that the applicable conformity assessment criteria are based on international standards.

Further, it is in general recommended to use transition arrangements and a staged adoption of a CAF for ANZ, e.g. along geographical lines or by vehicle type. It is recommended to consider preparation of an initial guidance note, similar to the Austroads/NTC guidelines for trials of automated vehicles, ideally prepared jointly with the FCAI/Truck Industry Council.

Finally, the tension between providing flexibility and adequately ensuring interoperability and managing safety risks should be noted (see Section 4.2.3). One way of managing this tension is to adopt a staged transitional approach, e.g. by agreeing on the Day 1 use cases in ANZ, elaborating on initial guidelines for C-ITS trials, deployment and evaluation of trials, and potentially hardening the guidelines into industry/public sector certification or legislation (presumably limited to a small set of use cases).

6. Conclusions and Recommendations

6.1 Conclusions

Austroads is seeking to identify and assess options for an assurance compliance framework in the area of cooperative intelligent transport systems (C-ITS) that will ensure the safe operation of C-ITS in Australia and New Zealand.

This report covers the key findings from a literature review and the stakeholder consultation, describes and assesses the main CAF model options. It sets out the options for the development of an ANZ C-ITS CAF, including the proposed approach based on hybrid model options and guidance relating to key topics, such as governance architecture and approval processes.

The purpose of the literature review, conducted between October 2017 and January 2018, was to present an overview of the C-ITS context and state of play in ANZ as well as the global C-ITS developments, mainly driven by Europe and the USA. The findings from the literature review provided a healthy basis for the further work on the design of the ANZ C-ITS CAF, especially for:

- the basic assumptions which form the foundation for the elaboration of the C-ITS CAF model options
- the description of the main properties and the differentiation of the four main high-level policy options for compliance assessment of C-ITS, covering status quo, self-regulation, quasi-regulation and regulation; the level of regulation and assurance by the government increases with each C-ITS CAF option
- the illustrations of how the type approval process may be implemented
- the outline of an overarching C-ITS governance architecture
- the assessment of the four C-ITS CAF models, based on a set of proposed evaluation criteria.

The stakeholder consultations were undertaken to seek feedback on the proposed overall scope and assumptions for the ANZ C-ITS CAF, outlined models and on the evaluation, in the endeavour to identify a model that is fit for purpose and the direction for the future work.

An Explanatory Note *C-ITS Compliance Assessment Framework*[43] was used as the main support for the consultation. The note, prepared by the project team, was intended to foster a common basic understanding of the C-ITS compliance assessment and to assist stakeholders in taking a position on relevant issues. It was used as a basis for the discussion on the following key themes:

- overall scope of the C-ITS CAF
- model options and overarching governance architecture
- evaluation criteria and evaluation of the models.

The consultations involved discussions with 84 stakeholders ranging across 42 organisations. The consultations were undertaken via the following three main formats:

- high-level workshop with key decision makers on the afternoon of 14 March 2018 in Melbourne
- high-level discussion with selected agencies in five separate meetings from 12 to 16 March 2018
- invitation to the stakeholders to provide written comments to the questions contained in the note.

[43] C-ITS Compliance Assessment Framework – Explanatory Note (16 February 2018) can be obtained via Austroads C-ITS Project Manager, Mr. Niko Limans (Niko.Z.Limans@tmr.qld.gov.au).

The findings from the consultations show that the basic assumptions for an ANZ C-ITS CAF as well as the four 'pure' models to be considered are broadly supported by the stakeholders. Also, the proposed evaluation criteria and the outcome of the assessment are broadly endorsed. However, the main findings revealed that it is currently premature to choose the CAF model, given the range of elements of C-ITS that are still in the development phase (e.g. evolving policies, use cases, standards, technologies, SCMS).

6.2 Recommendations

The following main tasks are recommended to be undertaken in order to progress the development and implementation of a C-ITS CAF for ANZ:

1. **Set up an ANZ C-ITS Platform**, in order to address the main barriers and enablers identified for deployment of C-ITS in ANZ.
2. **Determine the overall objective, role and scope of the ANZ C-ITS CAF**: there is a need for a C-ITS strategy, ideally developed jointly by Australia and New Zealand, also laying down agreed Day 1 applications and associated use cases and message sets.
3. **Set up the C-ITS governance model**: there is a need to refine and select the CAF model(s) and set up an overall governance model for C-ITS.
4. **Prepare the establishment of the SCMS**: there is a need to pursue the earlier work on a SCMS for ANZ, whilst seeking to leverage off existing relevant security-related frameworks and exploring the adoption of a common approach with connected and automated vehicles. This work should ideally involve DIRDC and the Signals Directorates in Australia and New Zealand.
5. **Determine the approval procedures and conformity assessment criteria,** through adoption of relevant international standards and recognition of overseas approval procedures.

The findings form the stakeholder consultation also underlined that the compliance model should be linked to the risk of the application to which the compliance model is to apply. The CAF model required for the applications should be adaptable and reflect the risk and consequence of that application misbehaving. A 'one size fits all' approach is unlikely to provide a framework that is fit for purpose.

It is recommended to consider adopting a staged and hybrid approach, consisting of different models for different types of C-ITS stations and application areas (see 5.2 for further details), in the downstream work.

References

ACMA 2014a, *Radiocommunications (Compliance Labelling – Devices) Notice 2014*, Compilation No. 3, Compilation date 27 October 2017, Australian Communications and Media Authority.

ACMA 2014b, *Radiocommunications (Compliance Labelling – Electromagnetic Radiation) Notice 2014*, Compilation No. 1, Compilation date 27 October 2017, Australian Communications and Media Authority.

ACMA 2015, *Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2015*, 17 February 2015, Australian Communications and Media Authority.

ACMA 2017a, *Radiocommunications (Intelligent Transport Systems) Class Licence 2017*, Australian Communications and Media Authority.

ACMA 2017b, *Product labelling*, ACMA, viewed 22 November 2017, https://www.acma.gov.au/Industry/Suppliers/Product-supply-and-compliance/Steps-to-compliance/product-labelling, Australian Communications and Media Authority.

ACMA 2017c, *Radiocommunications Labelling (Electromagnetic Compatibility) Notice 2017*, Dated 18 December 2017, Australian Communications and Media Authority.

ACMA 2017b, Product labelling, ACMA, viewed 22 November 2017, https://www.acma.gov.au/Industry/Suppliers/Product-supply-and-compliance/Steps-to-compliance/product-labelling, Australian Communications and Media Authority.

Australian Government 2013, *Australian Government's Privacy Act 1988* (no. 119, 1998 as amended, includes amendments up to Act No. 13, 2013), https://www.legislation.gov.au/Details/C2014C00076, viewed 18 December 2017, Australian Government, Canberra, ACT.

Australian Government 2014, *The Australian Government Guide to Regulation*, Australian Government, Canberra, ACT.

Australian Government 2015, *Competition and Consumer Act 2010* (No. 51, 1974, Compilation No. 100, Includes amendments up to Act Mp. 38, 2015), https://www.legislation.gov.au/Details/C2015C00327, viewed 11 January 2018, Australian Government, Canberra, ACT.

Australian Government 2017a, *Australian Design Rules*, Department of Infrastructure and Regional Development, https://infrastructure.gov.au/roads/motor/design/, viewed 14 December 2017, Australian Government, Canberra, ACT.

Australian Government 2017b, *Motorway Vehicles Standards Act 1989, Compliance and Enforcement Strategy,* Australian Government, Canberra, ACT.

Austroads 2012a, *C-ITS 5.9 GHz Spectrum Management and Device Licensing Regime Report*, AP-R414-12, Austroads, Sydney, NSW.

Austroads 2012b, *Cooperative ITS Strategic Plan, AP-R413-12,* Austroads, Sydney, NSW.

Austroads 2015a, *Austroads Strategic Plan 2016-2020*, Repositioning for a sustainable future, AP-C29-15, Austroads, Sydney, NSW.

Austroads 2015b, *Cooperative Intelligent Transport Systems (C-ITS) Standards Assessment*, AP-R474-15, Austroads, Sydney, NSW.

Austroads 2015c, *Development of Product Acceptance Techniques for Road Network Devices*, AP-R471-15, Austroads, Sydney, NSW.

Austroads 2016, *Operationalising Austroads' Product Acceptance Process*, AP-R524-16, Austroads, Sydney, NSW.

Austroads 2017, *Connected and Automated Vehicle Trials*, Austroads, viewed 30 November 2017, http://www.austroads.com.au/drivers-vehicles/connected-and-automated-vehicles/trials.

Austroads 2018, *Evaluation of the European C-ITS platform including TVRA: Literature Review and Stakeholder Consultation Section* – Working paper (V3), March 2018.

Carabin, G. (2017) *WG Compliance assessment*, Presentation at C-ITS Plenary Meeting at DG Move on 20 September 2017 in Brussels, Belgium.

Car 2 Car Communication Consortium 2017, *Mission & Objectives*, C2C CC, viewed 30 November 2017, https://www.car-2-car.org/index.php?id=5.

C-ITS Platform 2016, *C-ITS Platform, Final report*, January 2016.

C-ITS Platform Phase II 2017a, *Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)*, Release 1, June 2017.

C-ITS Platform Phase II 2017b, *Working Group Compliance Assessment – Final Report*, 12 July 2017.

Common Criteria Portal 2017, *Common Criteria Recognition Arrangement*, Common Criteria Portal, viewed 22 November 2017, https://www.commoncriteriaportal.org/.

Comtest Laboratories 2017, *The Regulatory Compliance Mark (RCM)*, Comtest Laboratories, viewed 22 November 2017, http://www.comtest.com.au/compliance/the-regulatory-compliance-mark-rcm.

ETSI EN 302 571 V2.1.1 (2017-02), Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU.

ETSI EN 302 636, *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking;*

302 636-1 V1.2.1 (2014-04), *Part 1: Requirements*

302 636-2 V1.2.1 (2013-11), *Part 2: Scenarios*

302 636-3 V1.2.1 (2014-12), *Part 3: Network Architecture*

302 636-4-1 V1.3.1 (2017-08), *Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality*

302 636-5-1 V2.1.1 (2017-08), *Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol*

302 636-6-1 V1.2.1 (2014-05), *Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols*

ETSI EN 302 663 V1.2.1 (2013-07), *Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band*.

ETSI EN 302 665 V1.1.1 (2010-09), *Intelligent Transport Systems (ITS); Communications Architecture*.

ETSI TS 102 941 V1.2.1 (2018-05), *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*.

ETSI TS 102 965 V1.3.1 (2016-11), *Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration*.

ETSI TS 103 097 V1.3.1 (2017-10), *Intelligent Transport Systems (ITS); Security; Security header and certificate formats*.

European Commission 2016a, *A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*, COM(2016) 766 final.

European Commission 2016b, *The 'Blue Guide' on the implementation of EU product rules 2016*, C(2016) 1958 final.

European Union 2016, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*.

FCAI 2017, *Code on Guiding principles for privacy and cooperative intelligent transport (C-ITS) systems*, https://www.fcai.com.au/news/codes-of-practice/index/year/all/month/all/publication/87, viewed 14 December 2017.

Geissler, T. 2017, *C-ITS Deployment is underway – Workshop Introduction*, Presentation at third public workshop of the Amsterdam Group and CODECS, 14 February 2017, Amsterdam.

Government of New Zealand 2017, *Government Expectations for Good Regulatory Practice*, Government of New Zealand, Wellington, NZ.

Harmonisation Task Group 6 2015a, *Cooperative-ITS Security Policy Framework: Summary of Results*, Document HTG6-2, EU-US ITS Task Force, Standards Harmonisation Working Group, Harmonisation Task Group 6.

Harmonisation Task Group 6 2015b, *Public Key Infrastructure (PKI) Architecture Analysis and Recommendations for Harmonization*, Document HTG6-3, EU-US ITS Task Force, Standards Harmonisation Working Group, Harmonisation Task Group 6.

Harmonisation Task Group 6 2017, *End-to-End Technical and Organisation Security Policy Framework*, Presentation held at TCA's Connected Vehicle Security & Standards Industry Event, 30 May 2017, RACV Club Melbourne, VIC.

IEEE 802.11p, *IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*.

IEEE 1609.2, *IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages.*

IEEE 1609.3, *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Networking Services.*

IEEE 1609.4, *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Multi-channel Operation.*

ISO 14001:2015, *Environmental management systems -- Requirements with guidance for use*.

ISO 20077-1:2017, *Road Vehicles — Extended vehicle (ExVe) methodology — Part 1: General information*.

ISO 50001:2011, *Energy management systems – Requirements with guidance for use*.

ISO/IEC 9594-8:2017, *Information technology -- Open Systems Interconnection -- The Directory -- Part 8: Public-key and attribute certificate frameworks*.

ISO/IEC 9797, *Information technology -- Security techniques -- Message Authentication Codes (MACs)*

ISO/IEC 9797-1:2011, *Part 1: Mechanisms using a block cipher*.

ISO/IEC 9797-2:2011, *Part 2: Mechanisms using a dedicated hash-function*.

ISO/IEC 10118-3:2004, I*nformation technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions* (a new edition is under preparation).

ISO/IEC 11770, *Information technology -- Security techniques -- Key management*

ISO/IEC 11770-1:2010, *Part 1: Framework*.

ISO/IEC 11770-2:2008, *Part 2: Mechanisms using symmetric techniques*.

ISO/IEC 11770-3:2015, *Part 3: Mechanisms using asymmetric techniques*.

ISO/IEC 11770-4:2017, *Part 4: Mechanisms based on weak secrets*.

ISO/IEC 15408, *Information technology -- Security techniques -- Evaluation criteria for IT security*

ISO/IEC 15408-1:2009, *Part 1: Introduction and general model*.

ISO/IEC 15408-2:2008, *Part 2: Security functional components*.

ISO/IEC 15408-3:2008, *Part 3: Security assurance components*.

ISO/IEC AWI 15408-4, *Part 4: Framework for the specification of evaluation methods and activities*.

ISO/IEC 17000:2004, *Conformity assessment -- Vocabulary and general principles*.

ISO/IEC 17011:2017, *Conformity assessment -- Requirements for accreditation bodies accrediting conformity assessment bodies*.

ISO/IEC 17020:2012, *Conformity assessment -- Requirements for the operation of various types of bodies performing inspection*.

ISO/IEC 17021, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*:

ISO/IEC 17021-1:2015, *Part 1: Requirements*.

ISO/IEC 17021-3:2013, *Part 3: Competence requirements for auditing and certification of quality management systems*.

ISO/IEC TS 17021-7:2014, *Part 7: Competence requirements for auditing and certification of road traffic safety management system*.

ISO/IEC 18033, *Information technology -- Security techniques -- Encryption algorithms*

ISO/IEC 18033-1:2015, *Part 1: General*.

ISO/IEC 18033-2:2006, *Part 2: Asymmetric ciphers*.

ISO/IEC 18033-3:2010, *Part 3: Block ciphers*.

ISO/IEC 18033-4:2011, *Part 4: Stream ciphers*.

ISO/IEC 27000:2016, *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*.

ISO/IEC 27001:2013, *Information technology -- Security techniques -- Information security management systems – Requirements*.

ISO/IEC 27002:2013, *Information technology -- Security techniques -- Code of practice for information security controls*.

ISO/IEC 27003:2017, *Information technology -- Security techniques -- Information security management systems – Guidance*.

ISO/IEC 27005:2011, *Information technology -- Security techniques -- Information security risk management*.

ISO/TS 19299:2015, *Electronic fee collection -- Security framework*.

ITS JPO 2014, *USDOT's Intelligent Transportation Systems (ITS) ITS Strategic Plan 2015-2019*, FHWA-JPO-14-145, Washington, DC.

National Transport Commission 2017a, *Assuring the safety of automated vehicles*, Policy Paper, National Transport Commission, Melbourne, VIC.

National Transport Commission 2017b, *Cooperative Intelligent Transport Systems policy implementation*, National Transport Commission, viewed 6 December 2017, http://www.ntc.gov.au/current-projects/cooperative-intelligent-transport-systems-policy-implementation/?modeId=1064&topicId=1166.

National Transport Commission 2018, *NTC seeks feedback on a safety assurance system for automated vehicles*, National Transport Commission, viewed 26 June 2018, https://www.ntc.gov.au/about-ntc/news/media-releases/ntc-seeks-feedback-on-a-safety-assurance-system-for-automated-vehicles/.

New Zealand Government 2014, *Intelligent Transport System Technology Action Plan 2014-2018*, New Zealand Government, Wellington.

New Zealand Government 2017a, *Consumer Guarantees Act 1993* (Public Act 1993 No 91, Reprint as at 1 September 2017), viewed 11 January 2018, http://www.legislation.govt.nz/act/public/1993/0091/latest/DLM311053.html.

New Zealand Government 2017b, *New Zealand Government's Privacy Act 1993* (Public Act 1993 No 28, Reprint as at 28 September 2017), viewed 18 December 2017, http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

NHTSA 2016, *U.S. DOT advances deployment of Connected Vehicle Technology to prevent hundreds of thousands of crashes* (Notice of Proposed Rulemaking), NHTSA, viewed 1 December 2017, https://www.nhtsa.gov/press-releases/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands.

NZ Transport Agency 2002, *Land Transport Rule: Vehicle Standards Compliance 2002*, NZ Transport Agency, viewed 12 December 2017, https://www.nzta.govt.nz/resources/rules/vehicle-standards-compliance-2002-index/.

OmniAir Consortium 2017a, *Conformance & Interoperability for Trusted Device Communications* (slide 9), Presentation at the ISO/TC204 plenary meeting, ISOTC204 N4023, San Antonio, USA, 22-27 October 2017.

OmniAir Consortium 2017b, *Connected Vehicle Certification*, viewed 1 December 2017, https://omniair.org/services/connected-vehicle-certification/.

Queensland Government 2017, *CAVI: Cooperative and Automated Vehicle Initiative*, Queensland Government, viewed 30 November 2017, https://www.qld.gov.au/transport/projects/cavi.

SAE J2945/1, *On-Board System Requirements for V2V Safety Communications*.

Transport and Infrastructure Council 2011, *Policy Framework for Intelligent Transport Systems in Australia*, Transport and Infrastructure Council, Canberra, ACT.

Transport and Infrastructure Council 2016, *National Policy Framework for Land Transport Technology – Action Plan: 2016-2019*, Transport and Infrastructure Council, Canberra, ACT.

Transport for NSW 2017, *Cooperative Intelligent Transport Initiative*, Transport for NSW, viewed 30 November 2017, http://roadsafety.transport.nsw.gov.au/research/roadsafetytechnology/cits/citi/index.html.

UNECE 1998, *Text of the 1998 Agreement on UN Global Technical Regulations (UN GTRs), incl ECE/TRANBS/132 – Global technical regulations for wheeled vehicles, equipment and parts which can be fitted/or be used on wheeled vehicles*; viewed 14 December 2017, http://www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29glob.html.

USDOT 2014, *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*, USDOT, DOT HS 812 014.

USDOT 2016, *Connected Vehicle Certification Program*, Factsheet, V5.5.1, USDOT.

USDOT 2017a, *Automated Driving Systems 2.0: A Vision for Safety*, USDOT.

USDOT 2017b, *Connected Vehicle Pilot Deployment Program Phase 1 – Lessons Learned*, USDOT, Final Report, FHWA-JPO-17-504.

USDOT 2017c, *CV Pilots News & Events*, USDOT, viewed 1 December 2017, https://www.its.dot.gov/pilots/index.htm.

USDOT 2017d, *FHWA Announces Vehicle-to-Infrastructure Guidance* (V2I Guidance), USDOT, viewed 1 December 2017, https://www.transportation.gov/briefing-room/fhwa0317.

USDOT 2017e, *Security Credential Management System (SCMS) Proof of Concept (POC)*, Factsheet, USDOT.

Appendix A Literature List

Table A 1 lists the sources for the literature review presented in Section 2. A first version, based on a preliminary list was discussed, enhanced and agreed upon at the project inception meeting (27 November 2017). Since the developments regarding C-ITS are ongoing, the list has since then been enhanced with (mostly) very recent documentation. Note that the literature review was conducted between October 2017 and January 2018.

Table A 1: Literature list – basis of literature review

Documentation
Harmonization Task Groups, e.g.:
HTG6: Findings and Recommendations, TCA, October 2015
HTG6: End-to-End Technical and Organization Security Policy Framework, Presentation at Connected Vehicle Security & Standards Industry Event, 30 May 2017 at TCA
HTG6-1 Exec Sum
HTG6-2 Summary of Results
HTG6-3 Architecture
HTG6-4 Functional Decomposition Analysis
HTG7: Progress Report: To October 2015, TCA, February 2016
HTG7 Presentations at Connected Vehicle Security & Standards Industry Event, 30 May 2017, Melbourne:
Presentation-20170530-CVSS-CCMS
Presentation-20170530-CVSS-EUSTATUS
Presentation-20170530-CVSS-HARTS
Presentation-20170530-CVSS-HTG7
Presentation-20170530-CVSS-USSTATUS
C-ITS Platform (EU):
Phase II, Final Report, September 2017
Phase II, Final Report, Annex I, Compliance Assessment, 12 July 2017
Phase II, Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1, June 2017
Phase I, Final Report, January 2016
WG5: Security & Certification, Final Report, ANNEX 4: Compliance assessment in Cooperative ITS (C-ITS), 2015
Menzel (2017) European Framework for C-ITS Deployment, presentation of DG MOVE at the Third public workshop of the Amsterdam Group and CODECS, 14 February 2017, Amsterdam
Menzel (2017) C-ITS Deployment in Europe: Common Security and Certificate Policy, presentation of DG MOVE at the Third public workshop of the Amsterdam Group and CODECS, 14 February 2017, Amsterdam
Carabin (2017) WG Compliance assessment, presentation of DG MOVE at C-ITS Plenary Meeting, 20 September 2017, Brussels
Other documentation EU:
A European strategy on C-ITS, a milestone towards cooperative, connected and automated mobility
The 'Blue Guide' on the implementation of EU product rules 2016, Commission Notice C(2016) 1958
The RED Guide – Guide to the Radio Equipment Directive 2014/53/EU, Version of 19th May 2017

Engdahl (2017) ETSI EN 300 674-2-x in the context of the European Radio Equipment Directive – State of Play, Prepared for CEN/TC278/WG1 & ISO/TC204/WG5 – Electronic Fee Collection, 6 April 2017
ENCC Study: Study on the Implementation of a European Network of Certification Centres (ENCC) for the purpose of the Single European Service of Electronic Fee Collection Final Report, Release 2007-10-16, for the EC DG Energy & Transport
European Commission Whole Vehicle Type Approval – ECWVTA
Regulation (EU) 2016/679 General Data Protection Regulation
Geissler (2017) C-ITS Deployment is Underway, presentation at the Third public workshop of the Amsterdam Group and CODECS, 14 February 2017, Amsterdam
Car 2 Car Communication: https://www.car-2-car.org/
C-Roads Platform and Pilots: https://www.c-roads.eu/
Documentation ANZ:
Transport Certification Australia 2018, Key Decisions to Progress Australian Deployment of a SCMS, Document Number TCA-B067
NTC (2017-11) NTC Assuring the safety of automated vehicles - Policy paper
NTC (2017-06) Regulatory options to assure automated vehicle safety in Australia, Discussion paper - superseded
Nova Systems (2017-02) Safety Assurance System for Automated Vehicles in Australia - superseded
Rapp (2011) Feasibility Study: Heavy Vehicle Charging in Australia, Austroads Research Report AP-R384/11
Docs on CAVI: Cooperative and Automated Vehicle Initiative: https://www.qld.gov.au/transport/projects/cavi
Cooperative Intelligent Transport Initiative, Transport for NSW, 2017
Connected and Automated Vehicle Trials in ANZ: http://www.austroads.com.au/drivers-vehicles/connected-and-automated-vehicles/trials
Austroads reports relating to ITS/C-ITS:
AP-R479-15 Concept of Operations for C-ITS core Functions
AP-R474-15 C-ITS Standards Assessment
IR-252-16 Harmonised ITS Specifications
AP-R471-15 Product acceptance technique for road network devices (Section 2.2.2: first review of jurisdictional type approval processes in 2014)
AP-R524-16 Operationalising Austroads product acceptance process (Section 5 and Appendix A: review of latest processes regarding jurisdictional type approval processes)
AP-R414-12 C-ITS 5.9 GHz Spectrum Management and Device Licensing Regime Report
AP-C29-15 Austroads Strategic Plan 2016-2020
Examples of already existing compliance schemes (e.g. other areas of transport industry):
ARRB (2015) Transport Infrastructure Product Evaluation Scheme (TIPES) - TIPES Governance and Risk Management Framework
TCA (2014) Telematics In-Vehicle Unit (IVU) - Guideline for type-approval
TCA: certification of devices associated with Australia's IAP: https://tca.gov.au/
Australian Signals Directorate (ASD): Evaluated Products List (EPL): https://www.asd.gov.au/infosec/epl/index.php
Australian Design Rules for vehicles: https://infrastructure.gov.au/roads/motor/design/
NZ vehicle standard compliance: http://www.nzta.govt.nz/assets/resources/rules/docs/vehicle-standards-compliance-amendment-2013-2.pdf and https://www.nzta.govt.nz/resources/rules/vehicle-standards-compliance-amendment-2011-qa.html
Ministry of Business, Innovation and Employment: http://www.mbie.govt.nz/about/our-work/compliance-and-enforcement
The Regulatory Compliance Mark (RCM), Comtest Laboratories
ACMA: Australian Communications and Media Authority, e.g. Class Licence, Product Labelling
FCAI: Code on Guiding principles for privacy and cooperative intelligent transport systems

Relevant acts, e.g. Australian Government's Privacy Act 1988, Competition and Consumer Act 2010, Motorway Vehicles Standards Act 1989, New Zealand Government's Consumer Guarantees Act 1993, Privacy Act 1993
The Australian Government Guide to Regulation (2014)
TCA (2018) Key Decisions to Progress Australian Deployment of an SCMS: Full Report and Executive Companion
Documentation USA:
Connected Vehicle Certification Program - ITS Research Fact Sheet
USDOT: Andersen / Fehr (2015) Device Certification - PPT for ITS World Congress, Bordeaux, France
OmniAir™ Launches World's First V2X Connected Vehicle Certification Program (info from Mr. Kevin Gay, USDOT: https://www.prnewswire.com/news-releases/omniair-launches-worlds-first-v2x-connected-vehicle-certification-program-300540272.html?tc=eml_cleartime, https://omniair.org)
OmniAir Consortium: Connected Vehicle Certification: https://omniair.org/services/connected-vehicle-certification/
Smith (2012) Qualifying products and streamlining implementation of new technologies, AASHTO Paper prepared for 25th ARRB Conference, Perth, Australia
NHTSA: Notice of Proposed Rulemaking; FHWA: V2I Guidance
USDOT: Readiness of V2V Technology for Application
USDOT: Automated Driving Systems 2.0: A Vision for Safety
USDOT: SCMS; CV Pilot Deployment Program Phase 1 - Lessons Learned
USDOT: CV Pilots: https://www.its.dot.gov/pilots/index.htm
International and regional standards, e.g.:
ISO 21217:2014, Intelligent transport systems -- Communications access for land mobiles (CALM) – Architecture
ISO/DIS 17419:2017, Intelligent transport systems -- Cooperative systems -- Globally unique identification
ISO/IEC 17000: Conformity assessment — Vocabulary and general principles
ISO/IEC 17011, Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies
ISO/IEC 17020, General criteria for the operation of various types of bodies performing inspection
ISO/IEC 17021 series on "Conformity assessment. Requirements for bodies providing audit and certification of management systems"
ISO/IEC 17024, Conformity Assessment. General requirements for bodies operating certification of persons
ISO/IEC 17025, General requirements for the competence of testing and calibration laboratories
ISO/IEC 17065 Conformity assessment — Requirements for bodies certifying products, processes and services
ISO/IEC 17067, Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes
ISO 9000:2015, Quality management systems -- Fundamentals and vocabulary 9001
ISO 9001:2015, Quality management systems -- Requirements
ISO/IEC 9797, Information technology -- Security techniques -- Message Authentication Codes (MACs) – Parts 1 and 2
ISO/IEC 11770, Information technology -- Security techniques -- Key management – Parts 1 to 4
ISO/IEC 15408, Information technology -- Security techniques -- Evaluation criteria for IT security – Parts 1 to 4
ISO/IEC 18033, Information technology -- Security techniques -- Encryption algorithms – Parts 1 to 4
ISO/IEC 27000 standards series on Information technology -- Security techniques -- Information security management systems
ETSI TR 102 893:2017-03 (V1.2.1), Intelligent Transport Systems (ITS) - Security - Threat, Vulnerability and Risk Analysis (TVRA)
ETSI EN 302 636, Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking – Parts 1 to 6
ETSI EN 302 571 V2.1.138 (2017-02), Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
ETSI EN 302 663 V1.2.1 (2013-07), Intelligent Transport Systems (ITS); Access layer specification for Intelligent

Transport Systems operating in the 5 GHz frequency band
ETSI EN 302 665 V1.1.1 (2010-09), Intelligent Transport Systems (ITS); Communications Architecture
ETSI TS 102 940 V1.3.1 (2018-04), Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
ETSI TS 102 941 V1.2.1 (2018-05), Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
ETSI TS 102 965 V1.3.1 (2016-11), Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration
ETSI TS 103 097 V1.3.1 (2017-10), Intelligent Transport Systems (ITS); Security; Security header and certificate formats
UNECE 1998, Text of the 1998 Agreement on UN Global Technical Regulations (UN GTRs)
Common Criteria Portal: https://www.commoncriteriaportal.org/
National ITS/C-ITS programs:
Austroads Cooperative ITS Strategic Plan, 2012
Transport and Infrastructure Council's National Policy Framework for Land Transport Technology – Action Plan: 2016-2019, Commonwealth of Australia 2016
Cooperative Intelligent Transport Systems, Final policy paper, NTC, 2013
New Zealand Government's Intelligent Transport System Technology Action Plan 2014-2018, NZTA, November 2013
NZ Transport Agency position statement on intelligent transport systems, Responding to the opportunities, 2014
A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility, COM (2016) 766
USDOT Intelligent Transportation Systems (ITS) ITS Strategic Plan 2015-2019, Report FHWA-JPO-14-145
MLIT's White paper on Land, Infrastructure, Transport and Tourism in Japan, 2015
Makino (2016) C-ITS development "ETC 2.0" in Japan, ITS Congress, 10-14 October 2016, Melbourne

Appendix B C-ITS Trials/Pilots in ANZ

Note that the most recent information on the trials described below can be found on the Austroads website: http://www.austroads.com.au/drivers-vehicles/connected-and-automated-vehicles/trials.

B.1 Queensland

The Cooperative and Automated Vehicle Initiative (CAVI) project in Queensland runs from 2017 to 2021 and consists of four components (Queensland Government 2017):

1. Cooperative intelligent transport systems (C-ITS) pilot – eight C-ITS safety use cases
2. Cooperative and highly automated driving (CHAD) pilot
3. Vulnerable road user pilot
4. Change management.

The objectives of the CAVI project are to:

- validate the impacts and benefits, and user perceptions
- demonstrate technologies and build public awareness and uptake
- grow the Department of Transport and Main Roads technical and organisational readiness
- encourage partnerships and build capability in private and public sectors.

CAVI consists of four components with the C-ITS pilot being the largest component. It constitutes the (to this date) largest on-road testing trial in Australia of cooperative vehicles and infrastructure. From 2019, around 500 public and fleet vehicles will be retro-fitted with C-ITS technologies, and roadside C-ITS devices installed on arterial and motorways in and around the City of Ipswich. These devices allow vehicles and infrastructure to talk to each other to share real-time information about the road and to generate safety-related warning messages for drivers.

The C-ITS pilot will run for up to one year, and will test and analyse a number of C-ITS safety use-case applications:

- emergency braking warning (V2V)
- in-vehicle speed warning (V2I)
- turning warning for bicycle riders and pedestrians (V2V)
- roadworks warning (V2I)
- back-of-queue warning (V2I)
- red light violator warning (V2I/V2V)
- red light warning (V2I)
- stopped or slow vehicle warning (V2V)
- hazard warning (V2I).

In terms of compliance assessment, the following was noted based on a telephone discussion on 6 December 2017 with Stuart Allen-Keeling who is the Principal Advisor on Security for the CAVI project:

- The CAVI trial is not yet looking at compliance in the sense of how C-ITS will need to address compliance when ultimately deployed. The CAVI trial will require that C-ITS devices comply with certain requirements, but that is from a contractual perspective for the purpose of undertaking the trial.
- The CAVI trial will look to other projects, such as the Austroads compliance assessment framework project to help guide what compliance techniques need to be put in place for C-ITS. It is felt that knowledge from the CAVI trial will help ANZ develop and refine the compliance assessment framework required for C-ITS deployment by identifying what elements of C-ITS need to be complied with.
- In terms of the compliance assessment framework, it is felt that what is needed is a definition of the different compliance models and their impacts so that educated decisions can be made on the compliance models to adopt.

B.2 New South Wales

The following trials are being undertaken in NSW:

- Cooperative Intelligent Transport Initiative (CITI) trial of heavy vehicle safety applications using cooperative ITS (Transport for NSW 2017, see next point).
- Heavy Vehicle Priority Project trial of applications to provide heavy vehicle priority at signalised intersections using a 5.9 GHz US DSRC unit.

CITI (from 2013 onwards)

CITI is a testing facility for C-ITS and incorporates a trial of heavy vehicle safety applications using C-ITS. Based in the Illawarra region, it is the largest C-ITS test facility in the Southern Hemisphere, covering 2,300 km of the NSW road network.

The main features of the CITI testbed are:

- 60 trucks and 11 buses have been fitted with CITS so far.
- Three intersections are equipped with C-ITS to provide red traffic signal information.
- More than 1 billion records have been collected for analysis.
- A roadside transmission station broadcasts speed limit information to heavy vehicles about the 40 km/h truck and bus zone down the Mount Ousley descent.
- A licence has been provided by the Australian Communications and Media Authority to broadcast on the 5.9 GHz radio spectrum.

Drivers in participating vehicles will receive via V2V and/or V2I safety messages about upcoming hazards that could cause a crash. These safety broadcasts include:

- intersection collision warning
- heavy braking ahead warning
- traffic signal phase information
- speed limit information.

The Centre for Road Safety is expanding CITI to also include light vehicles. To investigate the potential safety benefits and user friendliness of the system, 55 cars from the Wollongong area will be fitted with C-ITS.

In terms of compliance assessment, it was noted in a telephone discussion on 6 December 2017 with Vanessa Vecovski (Project Manager, Road Safety Technology) that the CITI project is primarily focussed on:

- trialling the applications

- understanding the benefits of the applications
- understanding the requirements for the applications to function effectively (e.g. positioning).

The CITI project will look to other projects (e.g. Austroads projects) to provide guidance on security and compliance.

B.3 Victoria

The following trials are being undertaken in Victoria:

- A trial of automated vehicles, including their integration with roadside infrastructure, undertaken by ARRB, Connect East and La Trobe University.
- A trial of two connected technologies that can give trams priority at signalised intersections, undertaken by Yarra Trams, ARRB and La Trobe University.
- Development and trial of connected vehicle applications that interface with signalised intersections and managed motorway systems, undertaken by Intelematics.
- A trial of a driverless shuttle bus in the context of university students' mobility requirements.
- Bosch Highly Automated Driving Vehicle partnership with the Transport Accident Commission (TAC) and VicRoads.
- A consortium of stakeholders, led by the University of Melbourne, is developing an urban testbed that involves connectivity across multiple transport modes.

B.4 South Australia

The following trials are being undertaken in South Australia:

- A trial of a driverless shuttle at the Adelaide airport long-term car park.
- A trial of an automated cargo pod for the Tonsley Innovation precinct. This includes funding to construct pods for the trial.
- A trial of driverless shuttles for Flinders University.
- Cohda wireless on-road trial of two automated vehicles, including development of V2X capability.
- A test by Cohda Wireless and Telstra of vehicle-to-pedestrian technology over mobile networks in Adelaide. The technology provides an early-warning collision detection to the driver and alerts the pedestrian or cyclist via an application on their mobile phones.

B.5 Western Australia

The following trials are being undertaken in Western Australia:

- A trial of a fully driverless, fully electric shuttle bus in South Perth.
- Main Roads WA is partnering with industry to launch a trial of autonomous heavy vehicle platooning.

B.6 Australian Capital Territory

The ACT Government is supporting a two-year trial that will include testing a driver monitoring system on 40 residents with the residents driving semi-automated vehicles for up to two weeks at a time. The trial will look at how drivers behave when operating the vehicles in both manual and partially automated driving modes.

B.7 Northern Territory

The NT Government announced a six-month trial of an EasyMile shuttle bus at the Darwin Waterfront during 2017.

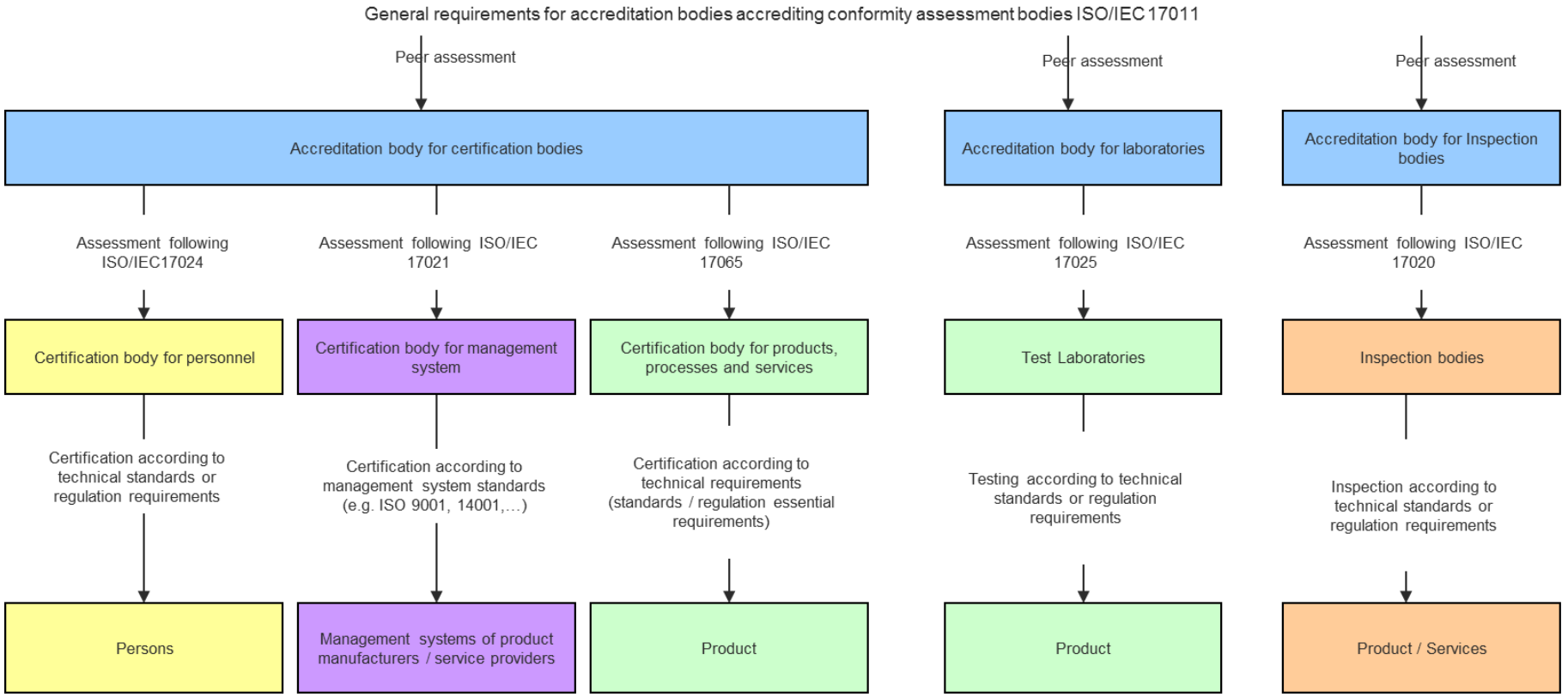
B.8 New Zealand

In September 2017, the New Zealand company HMI Technologies launched the Ohmio Hop Shuttle, which is a self-driving, connected and autonomous vehicle. The Ohmio vehicle uses connected vehicle technology to enable it to move more efficiently and safely in a convoy or platooning formation. Four Ohmio models which range in size from small to large shuttles and light commercial vehicles are planned for production in the next 12 months.

Appendix C ISO/IEC 17000 Series

Publicly governed certification structures often follow the general requirements for accreditation that are laid down in the ISO/IEC 17000 series of standards, for which Figure C 1 provides an overview.

Figure C 1: Overview of the ISO/IEC 17000 series



Appendix D Stakeholder Consultation Comments

Appendix D provides the key comments noted in the stakeholder consultation high-level workshop and in the high-level discussion meetings with selected agencies, as well as for the received written comments (including the project team's response).

D.1 Key points noted in the high-level workshop and in the meetings

D.1.1 Key points noted in the high-level workshop

The following key points were noted in the high-level workshop on 14 March 2018 in Melbourne:

- Ian Oxworth clarified that he can provide details to the group on a register of 5.8 GHz tolling stations, for the purpose of operating ITS-G5 stations (or other radio technologies in the 5.8 GHz band) in restricted mode in the DSRC protected zones in order not to cause harmful interference to DSRC stations.[44]
- Ministers approved self-regulation for automated vehicles (AVs). NTC is preparing a draft regulatory impact statement, which is expected to be released for consultation in April 2018. The high-level design is based on mandatory self-certification until the development of international standards for AVs. All significant modifications (e.g. SW updates) to the automated driving system must also be approved before being introduced into the market. The automated driving system entity, rather than government, will be responsible for testing and validating the safety of the automated driving system.
- Australia follows the European C-ITS approach. It was noted that the ACMA ITS Class Licence, which came into effect in January 2018, is based on the European ETSI standard. Equipment complying with EU C-ITS RF regulation (i.e. Radio Equipment Directive and EN 302 571) would meet Australian licensing conditions.
- It was clarified that the personal and central ITS-S are not yet defined, so difficult to comment on how these will work in the CAF. The central and personal ITS-S should be in the overall scope of the CAF but not in scope of the project to verify the appropriate compliance model for central and personal ITS-S.
- Concerns were raised as to whether having multiple root certification authorities (CAs) for Australia as per the EU model was appropriate for ANZ. Participants are happy with EU model but it was noted that the architecture and structure of the SCMS needs to be established for ANZ. Supply and vendors will influence the architecture. It is likely that there will be a need for one Root CA only for Australia.
- There may be one central ITS-S for each jurisdiction. However, as a vehicle crosses a border it should be able to communicate with the applicable central ITS-S. Central ITS-S are unlikely to need to be regulated.
- Policy options for CAF should consider the life-cycle management as cannot choose upfront entry models without considering life-cycle management.
- The four main compliance model options presented in the Explanatory Note are the main ones to consider.
- The compliance model required should tie back to the risk of the application in which the compliance model is to apply.
- The overall CAF should be set up to ensure that the CAF is not over-burdening or requires a CAF for each individual application.
- There are several gaps in the current approach to the compliance modal. As such the least attractive model is the current approach.

[44] ASECAP has prepared a geolocation database of DSRC installations in Europe to support coexistence between DSRC and ITS in the 5 GHz frequency range. The content of the database can be accessed upon registration at https://www.asecap-pzdb.com.

- A potential issue with the industry association compliance model is that it can lead to entry barriers for other suppliers not part of the industry association, in particular for small and medium-sized enterprises.
- C-ITS work to date has been largely based on technical and operations issues. There is a need for policy inputs. This will help drive the required CAF as it will define what ANZ is hoping to achieve with C-ITS. Need an overarching ANZ C-ITS strategy/policy.
- The overarching ANZ C-ITS strategy/policy should define the Day 1 applications and associated use cases and help define the type of applications ANZ is interested in deploying. The CAF will then help to define the type of compliance models required for the various types of applications based on the risk and consequence.
- It was noted that a device cannot be stopped from broadcasting with or without regulation. However, enforcement and sanctions can be more effectively performed based on an appropriate regulation being in place, which may also have a deterrent effect.
- CAF should recognise that ANZ are both large geographical areas and that once products are out there that it is difficult to manage their use.
- It is not clear if regulation is required, therefore it is difficult to discuss the governance architecture. Conformity assessment (CA) and market surveillance are complementary and equally necessary to ensure the protection of the public interests at stake. It is important to take a holistic view and consider not only CA but also market surveillance aspects.
- The proposed evaluation criteria in the Explanatory Note appear to be reasonable. The most relevant ones are probably
  - Criterion 1 Safety, environment (electromagnetic emissions or geofencing of dangerous goods on certain roads or areas) and consumer protection
  - Criterion 2 Innovation, flexibility and responsiveness
  - Criterion 3 Timeliness
  - Criterion 5 International and domestic consistency.
- Roadside ITS-S for road agencies could be managed through type approval or public-sector certification rather than through C-ITS regulation. Road agencies would like standards to ensure that what they say meets their needs.
- The C-ITS regulation model option is unlikely to be adopted in a timely manner and might be difficult to keep fit for purpose over time.

D.1.2 Key points from the high-level discussion meeting with TMR

The following key points were noted in the high-level discussion meeting with Transport and Main Roads (TMR) on 12 March 2018 in Brisbane:

- The CAF should be based on the Day 1, 1.5 and 2 applications and use cases, which still need to be developed and agreed among the Australian stakeholders. CAM and DENM form part of the C-ITS messages that trigger Day 1 use cases.
- Seems reasonable to adopt the European scope and approach for the C-TS CAF. Some adaptation (additions and omissions) will most likely be needed to reflect the Australian context and needs.
- RCM applies to all types of C-ITS stations. Telecommunication and cyber acts have to be included as part of the existing legislation.
- The ADRs cover also the HMI design rules related to V-ITS-S for Australia.
- Safety-related application should also form part of the C-ITS CAF scope.
- Road traffic risks induced by C-ITS need to be managed. All has to be certified like applications to be put in the Apple store. Integrity of the system is paramount.

- Confirms that the main compliance model options are the ones presented in the Explanatory Note.
- Proposed evaluation criteria in the Explanatory Note appear to be relevant. The most relevant ones are probably
  - Criterion 1 Safety and consumer protection
  - Criterion 5 International (i.e. European) and domestic consistency
  - Criterion 2 Innovation, flexibility and responsiveness.
- The current approach model is not deemed suitable.
- The voluntary industry association certification model[45] is not preferred.
- The preferred modes are the public-sector certification and the C-ITS regulation, potentially a combination of the two, or a transition from the former to the latter one. It is noted that a regulatory impact statement is needed to justify any new regulation in Australia.

D.1.3 Key points from the high-level discussion meeting with RMS and TfNSW

The following key points were noted in the high-level discussion meeting with Roads and Maritime Services (RMS) and Transport for New South Wales (TfNSW) on 13 March 2018 in Sydney:

- RMS focus is on aligning the traffic system to fit in with C-ITS to make the traffic system perform at a level that is deemed acceptable. For example, how can the Sydney Coordinated Adaptive Traffic System (SCATS) manage the network better with C-ITS, to improve traffic safety and traffic management.
- RMS is interested in testing the system to see what is required at the back end (e.g. security).
- RMS is following Austroads direction.
- RMS is interested in what data sets are required for the traffic system to work in an optimised manner with C-ITS. This would help to specify the data set requirements that should be specified for C-ITS equipped vehicles.
- Barriers to access the vehicle data (IPs, ownership and privacy issues) prevent RMS from making better use of vehicle information (e.g. number of passengers, truck's actual weight and loads).
- TfNSW has the largest HV C-ITS trial in the world with 71 HV equipped, 11 of which are buses. TfNSW is dealing with the certificate issue manually rather than in a manner in which it would need to be dealt with if deployed.
- A Frame architecture is purchased by Austroads. This is considered as endorsement to follow Europe, as the FRAME architecture is the European ITS architecture.
- Trust and security of the C-ITS system is paramount.
- As TMR is dealing with a large-scale deployment (500 vehicles), it is envisaged that there will be good information from it as TMR deals with issues like managing certificates for 500 vehicles.
- It is felt that 5G can solve many of issues associated with security of C-ITS communications as 5G does not get communications directly from the vehicle (peer-to-peer). Instead communications are going through the telecommunication network. Perhaps a hybrid communication approach will evolve and prove viable, in order to also support the V2V safety-related (low latency) use cases.
- Some basic decisions need to be made with respect to C-ITS before moving forward as it will govern the type of C-ITS applications and therefore the compliance models required. Need to know how the GNSS in ANZ is going to be provided and to what level of position accuracy. Need to know what data is going be available from vehicles equipped with C-ITS.

[45] Now referred to as „Industry certification model“

- Local government (as the biggest road manager) needs to be involved. For example, if C-ITS applications require detailed mapping of roads, is local government going to do this? Do they have the resources?
- It is seen that ANZ do not have the expertise to run and design a complex compliance assessment framework for C-ITS.
- The compliance assessment framework (CAF) chosen needs to balance the benefits versus costs of the complexity of the CAF.
- The CAF needs to be flexible. Keep it simple. Be flexible. The CAF option to introduce C-ITS regulation is not preferred, as it is likely to be too complex and lengthy. Also a challenge to keep abreast with a changing market and evolving technology.
- The CAF should be based on the type of applications and use cases that will operate on C-ITS. The latter still need to be developed and agreed among the Australian stakeholders.
- Need to identify where certification is a must and what are the type of applications where compliance is required and at what level.
- TfNSW is about to do testing on Satellite-Based Augmentation Systems (SBAS) for Australia.

D.1.4 Key points from the high-level discussion meeting with DIRDC

The following key points were noted in the high-level discussion meeting with the Department of Infrastructure, Regional Development and Cities (DIRDC) on 13 March 2018 in Canberra:

- CAF needs to be extendable, scalable and adaptable to the changing market and evolving technology. A prescriptive CAF written now probably will not fit what may be required in the future.
- Would like to see legislation minimised not extended, as real challenge to provide timely regulations and keep these keep fit for purpose over time.
- There is regulatory impact statement process. If pushing for regulation this can create a drawn-out process.
- CAF needs to be designed to fit the use cases, which are yet to be worked out and agreed by the Australian stakeholders.
- Public sector focuses on the safety-critical and related applications, which fall within its primary role of responsibilities.
- EU vehicles are checked for compliance for electrical communications.
- Compliance models for C-ITS and AVs should be linked but not merged. The AV is unknown at this stage.
- The four main compliance model options presented in the Explanatory Note are probably the main ones.
- Compliance models may not be federally funded. Replace 'federal funding' with 'government funding'. Cost-recovery-based model is preferred for the on-going financing of the C-ITS CAF scheme.
- No necessarily required to adopt the same CAF model for the V-ITS-S and the R-ITS-S. Road agencies should be able to look after their own compliance issues for R-ITS-S. Instead the CAF should focus on the vehicle side of things.
- The manufacturer indeed certifies that its vehicle and regulated vehicle components comply with all applicable provisions of applicable ADRs in effect of the date of the manufacture.
- The ADRs cover also the HMI design rules related to V-ITS-S for Australia.
- For new ADRs to be implemented. There needs to be evidence. Need benefit-cost ratio to implement.
- For large uptake of C-ITS there needs to be a clear benefit. Unlikely to drive uptake through regulation.

- The main evaluation criteria of interest to DIRDC are criteria 1 (safety and consumer protection), 2 (innovation, flexibility and responsiveness) and 5 (international and domestic consistency).
- At a policy level DIRDC is interested in national consistency. National consistency is the main issue.
- There are several gaps in the current approach compliance model. As such the least attractive model is the current approach.
- One problem with industry association compliance models is that it can lead to barriers of entry for other suppliers not part of the industry association, in particular for small and medium-sized enterprises. This risk could potentially be reduced through involvement in the association by the public sector (e.g. road agencies).
- The CAF should avoid focusing too much on legislation in a prescriptive manner. Legislation can potentially be difficult to change at a later date. Regulatory approach might be very difficult to implement and keep fit for purpose over time.
- The area of most interest is the security aspects. The Commonwealth could help road agencies deal with security, but this will likely be at the advice level. It is quite possible that Australia's Signals Directorate also would like to assume a support and advisory role related to security aspects.
- The Commonwealth is involved in the SCMS for TMR as part of its CAVI project.

D.1.5 Key points from the high-level discussion meeting with VicRoads

The following key points were noted in the high-level discussion meeting with VicRoads on 15 March 2018 in Melbourne:

- Agree that applications would determine the compliance model but not so worried about the technology.
- Do not want to lock into a technology. CAF needs to be adaptable to the changing market and evolving technology.
- Road agencies need a data standard in place in order to consume data from vehicles to assist the operation of their ITS systems. Barriers to access the vehicle data include IPs, ownership and privacy issues, noting that the vehicle manufacturers are unlikely to give these away for free. These barriers prevent VicRoads from making better use of vehicle data.
- Quality and integrity needs to be determined for messages from various different vehicles.
- Austroads has a project on harmonisation of specifications.
- There is a need for an ANZ C-ITS strategy/policy defining what ANZ wants to achieve from C-ITS, including broadly adopted C-ITS use cases by Australian stakeholders.
- The compliance model required for the applications should be adaptable and be based on the type of application and the risk and consequence of that application misbehaving. The types of applications could be grouped into the following four areas:
    1. Regulatory – Major concern as legislation. Compliance required (e.g. truck journey, monitoring of dangerous goods)
    2. Warning – Minor concern, but self-compliance should be sufficient (e.g. debris on the road, road damage, flash flooding, blackspot, single vehicle)
    3. Traffic operation – Some concern (e.g. management of intersections and green corridors)
    4. Advisory – Not a concern no compliance required.
- CAF for the latter can be left to the industry to sort out.
- CAF could take what is available now and apply the following:
    - public sector certification for R-ITS-S
    - industry association certification for V-ITS-S

  - ACMA looks after the class licence.
- The major issue is how to deal with the aftermarket devices.
- SCMS may need to manage the issue of aftermarket devices. Perhaps those that are retrofitted may be less trusted.
- The CAF should be simple and flexible. Do not want to come up with an over-complicated system. However, continuation of the current approach is not deemed as a viable model.
- The more regulations and tighter a CAF is, the more prone to disruption it becomes and the greater the disruption as a result.
- EU might develop a CAF in five-year period. Does Australia need to do anything in the meantime? Can Australia just adopt what is available now and adapt it to suit?
- CAF should be a gradual step process.
- Need an ITS architecture, including an overarching governance in place, that also covers C-ITS. In terms of Figure 7.1 of the Explanatory Note, it was felt that the top three bodies are required (C-ITS governing body, C-ITS supervision body and security, certificate and privacy policy authority).
- Security framework is the major gap that needs to be addressed. Do not want to let anything into the vehicle that could attack the network.
- It will be difficult to certify individual applications. The CAF should aim to certify type of applications. Therefore, just need to know the type of the application.

D.1.6 Key points from the high-level discussion meeting with New Zealand Ministry of Transport and Transport Agency

The following key points were noted in the high-level discussion meeting with the New Zealand Ministry of Transport and New Zealand Transport Agency on 16 March 2018 in Wellington:

- NZ Land Transport Act is the existing legislation.
- The NZ ITS action plan is being revised. Road safety, slow forms of mobility, public transport and sustainable mobility form part of the high-priority actions.
- NZTA does not have a road map for C-ITS deployment. C-ITS trials are currently being undertaken.
- The road traffic enforcement policing program is being revisited, also to create an enabling environment for automated vehicles.
- Electronic log books allowed; compliance assessment by accredited 3rd parties.
- HV-distance-based road user charging scheme is in operation; conformity assessment by accredited 3rd parties.
- Motor vehicle standards and regulations: mutual recognition agreements in place (i.e. recognition of certification from the country where the vehicle was manufactured).
- The average lifetime of a vehicle is 14 years (in addition to the time of the foreign owner, if applicable).
- Motor vehicle inspection is performed periodically by accredited 3rd parties. It would not be easy to extend their services to include certain type approval activities related to V-ITS-S, due to lack of training and equipment etc.
- NZ agrees that the CAF should be based on a risk framework that is based on the types of C-ITS applications.
- NZ legislation can change pretty quickly. NZ legislation can be applied quickly. Different to Australia.

- NZ accepts vehicles that meet the local vehicle market from which they are imported. A future issue is expected with Japanese imported vehicles; 760 MHz VICS OBE need to be switched off when entering NZ.
- NZ can apply legislation that vehicles require a feature that NZ has legislated.
- NZ is inclined to follow the Australian approach for C-ITS CAF.
- NZ may need a different compliance body to Australia but would prefer not to. Only would want to do it where it is required. Most likely for regulated applications.
- Retrofit of C-CITS stations should be part of the scope of C-ITS CAF.
- There is a need for NZ C-ITS strategy/policy defining what NZ wants to achieve from C-ITS, including broadly adopted C-ITS use cases by the stakeholders.
- The compliance model required for the applications should be adaptable and be based on the type of application and the risk and consequence of that application misbehaving. The types of applications could be grouped into the following four areas:
    1. Regulatory – Major concern as legislation. Compliance required (e.g. truck journey, monitoring of dangerous goods)
    2. Warning – Minor concern, but self-compliance should be sufficient (e.g. debris on the road, road damage, flash flooding, blackspot, single vehicle)
    3. Traffic operation – Some concern (e.g. management of intersections and green corridors)
    4. Advisory – Not a concern no compliance required.
- CAF for the latter can be left to the industry to sort out.
- NZTA would be inclined to favour CAF model option 3 (i.e. public-sector certification), as this model is consistent with the approach being adopted for AVs.
- The current approach is deemed as a not suitable model, noting that C-ITS and connected vehicles ultimately associated with, possibly unprecedented, road traffic safety issues.
- All proposed evaluation criteria in the Explanatory Note appear to be relevant. The most relevant ones are probably:
    - Criterion 1 Safety, environment and consumer protection
    - Criterion 5 International and domestic consistency
    - Criterion 2 Innovation, flexibility and responsiveness.

D.2 Written comments received from stakeholders

Appendix D.2 presents the six sets of written comments received on the Explanatory Note and the project team's response to these. The comments are presented in:

- Table D 1 – General comments
- Table D 2 – Comments related to the overall proposed scope and basic assumptions
- Table D 3 – Comments related to the main models and overarching architecture
- Table D 4 – Comments related to the proposed evaluation criteria and the initial evaluation.

The comments have been edited minimally so as to ensure that neither the names nor the organisations are revealed in order not to link any points raised to particular individuals or organisations, in accordance with the invitation to provide written feedback on the questions in the note.

Table D 1: General comments

Comment no.	Comment	Project team response to comment
1	We welcome the opportunity to contribute to the consultation process for the development of a CAF for C-ITS to ensure the safe operation of C-ITS in ANZ. End-users of C-ITS, like any other public digital environment, inherently assume and expect that their safety and security will be protected. For connected and automated vehicles, the stakes are higher because digital security and physical safety become one and the same. A commercially sustainable global market for C-ITS will not be possible without security; and neither will safety nor true connectivity. Secure systems (be they human or technology-based) require participants to be verified as trustworthy prior to inclusion into that system. One of the major roles of a CAF is therefore to examine the credentials and evidence of potential participants (against trust requirements) prior to inclusion, and to ensure that trustworthiness is maintained throughout the lifecycle of participation. Cooperative, connected and automated vehicles are developing at different rates but will ultimately be interdependent. As one writer puts it, 'Automated vehicles that aren't connected to each other is a bit like gathering together the smartest people in the world but not letting them talk to each other.'[46]	This comment provides a concise description of the C-ITS CAF context.

[46] Huei, P. 2016. Saving lives by letting cars talk to each other. The Conversation. Available at https://theconversation.com/saving-lives-by-letting-cars-talk-to-each-other-59221.

Comment no.	Comment	Project team response to comment
	Connectivity in vehicles, infrastructure and mobile devices will create a truly connected environment, inclusive of information services providing regional road-use policy, up-to-date road network operational information, and the digital distribution of traffic regulations. It is vital that, rather than creating a competing ecosystem, automated vehicles are integrated into the C-ITS environment to receive strategic and tactical information that vehicle sensors cannot determine directly, to achieve safe, effective and efficient use of the road network. Connected and automated vehicles will fundamentally challenge our understanding of what qualifies as an 'in-service' product, and the associated impact of in-service system updates on type-approval, certification and compliance assurance, and where responsibilities fall. Managing the risks introduced through such connectivity lies at the very heart of the CAF.	
2	We are supportive of Austroad's project to develop a C-ITS Compliance Assessment Framework to support the deployment of C-ITS systems within Australia. The work that Austroads coordinated with the Australian Communications and Media Authority to establish a class licence to support C-ITS applications was a vital precondition to getting to this stage in C-ITS deployment. C-ITS systems have the capacity to be used for a range of purposes, from safety critical systems such as vehicle to vehicle collision avoidance, information services to drivers, such as availability of parking, to regulatory or commercial systems. One of the challenges to our response is that it is not clear what range of use cases the states and territories are anticipating in early C-ITS deployment. We are aware of a number of trials underway that may inform decision-making on this issue. In our view the Commonwealth's interest in contributing to this work is in terms of its national leadership role, specifically: • a role in participating in international regulatory bodies on behalf of Australian interests. • a strong policy interest in ensuring that frameworks and investments are, to the greatest extent, internationally and nationally consistent. • an interest in ensuring any legislative frameworks are harmonised across state and territory jurisdictions. • a role in investing in productivity-enhancing, land transport infrastructure. Finally, while we understand the enormous technical and operational challenges of the implementation of C-ITS, we believe the CAF development would benefit from greater input from state and territory policy departments. There is a lack of understanding of the policy complexity and the range of options available to achieve nationally consistency, which makes proposals based on a European model problematic.	The opening remarks are supportive of Austroads project to develop a C-ITS CAF and express understanding for the technical and operational challenges of the implementation of C-ITS.

Table D 2: Comments related to the overall proposed scope and basic assumptions

Question no	Comment no	Comment	Project team response to comment
1	1	**Framework scope** Agrees that it is essential to clarify the overall scope of the ANZ C-ITS CAF, including what types of products that would fall under this framework, to elaborate suitable options. An approach that considers the C-ITS station (rather than C-ITS components or systems) is most consistent with international (notably EU) approaches, while allowing compliance assessment criteria to be most easily developed from established international standards. This also allows those criteria to be performance-based, with the outcomes achieved by the C-ITS station considered, rather than potentially limiting innovation by considering assumed components or system designs. This is a crucial element for an effective CAF. From a commercial perspective, technology providers are expected to predominantly offer C-ITS products and services based on mobile and roadside units (i.e. C-ITS stations) which further reinforces the C-ITS station as the appropriate level of granularity for compliance assessment. While we agree that it is important for initial compliance assessment criteria to focus on the quality of the transmitted data (i.e. the triggering event and the latency of transmitted data in accordance with the standardised format and defined security mechanisms), our experience suggests that reliability of devices is also highly important. ANZ experiences some of the harshest vehicle environmental challenges in the world with respect to ranges of temperature and humidity, dust, insects, vibration and other factors that in-vehicle devices are subject to. Being able to reliably sustain the quality of transmitted data throughout the lifecycle of a C-ITS station is essential, and historically many internationally sourced in-vehicle devices are simply not designed for the harshness of ANZ conditions. Lastly, it is accepted that central and personal C-ITS stations are to be excluded from the initial C-ITS compliance assessment activities (for the reasons given in the Austroads report) but we strongly recommend that the principles of the CAF be developed with the future inclusion of such station types in mind.	This comment endorses the need to clarify the framework scope, the proposed overall scope and initial focus. Whereas it agrees with the initial focus for the initial compliance assessment criteria, it suggests to include also in-vehicle device environmental requirements and associated conformity assessment criteria as part of the overall scope. This will be highlighted as a potential future extension of the scope to be considered by the C-ITS governing body, after the initial setting up of the CAF.
1	2a	There are 3 key assumptions in the scope statement: 1. “focus on the vehicle and roadside types of C-ITS stations.” - Agree 2. “concentrate on the quality of the transmitted data” – Agree 3. “initially focus on C-ITS safety driver support messages” – I would like to have further discussion on this. If the intents of the CAF includes:	This comment suggests that the overall scope should make extended provisions for other types of C-ITS messages in order to achieve interoperability. The project team recommends, in line with stakeholder feedback, a staged approach and

Question no	Comment no	Comment	Project team response to comment
		– are fit for purpose (including effective use and support for efficient use of radio spectrum in order to avoid harmful interference), – are interoperable, – support an open vendor market and avoid vendor lock-in with proprietary solutions. Then only focusing on “safety driver support messages” will not achieve the intents above. To achieve interoperability, other types of C-ITS messages need to be considered as well.	initially to focus on C-ITS driver safety support messages. The focus/scope of CAF can be extended and adapted over time (see also the discussion on the proposed types of applications with regard to the CAF scoping).
1	2b	One of the assumptions is that we will follow the EU approach for C-ITS , which is fairly well set already - but, to add some weight to it, it is worth noting that the Commonwealth has an established position of harmonising Australian Design Rules with the UNECE (European) standards for vehicles.	It is noted that the ADRs are largely based on the European standards for vehicles. It will be highlighted also in the basic assumption section for clarity.
1	2c	I just think it should be anything wanting to use 5.9 GHz. That way you remove regulatory telematics, or comms on existing cellular to TMCs/data portals from the equation. We already have that now, and I can’t see any need to regulate it. Also, agree that personal devices should be out of scope. But then I think this raises the point, how do you ensure they don’t use 5.9 GHz until they’re capable of producing useful messages. So perhaps should be included as a note. This should be for anything that we need to ensure high levels of trust, and to ensure the band is available for safety/important messages.	This comment suggests restricting the scope to C-ITS using 5.9 GHz, and leaving out regulatory telematics, and communications on existing cellular to TMCs/data portals from the scope. This is in line with the proposed initial focus but goes beyond it, as it proposes that the latter issues (definitively) are outside the overall scope. The project team is also in favour of seeking to align the CAF with existing general regulations and codes of practice. Hence, it will be proposed to the project reference group to adopt this comment. This comment agrees that personal devices should be out of the scope, and contemplates on the possibility to include a note that personal devices should not use the 5.9 GHz for transmitting messages until they are capable of producing useful and trustworthy messages. Such a clarification could be included in the terms of reference for the CAF and conveyed to applicants. It might also be worthwhile to seek

Question no	Comment no	Comment	Project team response to comment
			ACMA's views on whether such a note (or conditions) can be added to ACMA's Radiocommunications (ITS) Class Licence.
1	3	In general we agree. We would like to make the statement In clause 5 of the explanatory note document more precise, interoperability only is not sufficient, also backwards compatibility i.e. interoperability through time and compatibility in general are key aspects.	This comment highlights the importance to also ensure backwards compatibility of legacy compliant devices. The project team supports this as a guiding principle to be duly considered by the C-ITS CAF governing body. See also comment no. 17, concerning the base premise (i.e. 'once approved, always approved' status) and approach for how to deal with technology provider self-motivated product updates.
1	4	• **Agree** that **C-ITS stations** constitute the scope of the ANZ C-ITS CAF, as opposed to C-ITS components or systems. • **Agree** that ANZ initially will largely **follow the EU C-ITS approach**, i.e. to initially focus on C-ITS safety driver support messages and in terms of specification and conformity assessment concentrate on the quality of the transmitted data (i.e. the triggering event and the latency of the transmitted data in accordance with the standardised format and defined security mechanisms). • **Agree** that compliance assessment activities will focus on the **vehicle and roadside types of C-ITS stations**. Agree that central and personal ITS-stations are currently outside of scope, but should be able to be included in a future extension of the ANZ C-ITS CAF.	This comment endorses the proposed overall scope.
1	5	We understand the priority in focussing on C-ITS stations, as opposed to components (sub-elements of stations) or systems, which are likely to be managed by road agencies in the early instances. We also note that, while we understand there has been no definitive decision, the preference from most stakeholders is to align Australian standards with the EU C-ITS approach. It may be useful for TCA to provide some information on the progress of its participation in Harmonisation Task Group 7, which we understand is an international group that has been looking at harmonising C-ITS standards across the several major world groupings.	This comment endorses the proposed overall scope. A wish for more information by TCA on its work in HTG7 is mentioned.
2	6	**Application scope**	Several stakeholders expressed the need to

Question no	Comment no	Comment	Project team response to comment
		The question is posed whether so-called “safety-related” C-ITS applications (e.g. flooded road warning) should be part of the CAF. We recommend that, while an appreciation of the intended use of data exchanged between vehicles and/or infrastructure within the context of an application is important when considering the associated risk, the compliance assessment criteria developed should be application-neutral and thus able to support a range of known and future applications. Therefore, if established international standards define the underlying interaction (event, latency, format and security mechanisms) used to achieve these so-called “safety-related” applications, then they should form part of the CAF. The marginal cost of doing so is expected to be negligible. This approach best supports future innovations to develop new applications that reuse data exchanges, rather than hard-wiring compliance assessment criteria to known applications. The established international standards describe these data exchanges, not applications. However, it is acknowledged that some international standards are currently underdeveloped in their definition of such performance criteria; this will continue to improve over time.	develop and agree on a common ANZ C-ITS strategy and types of applications, to identify the ones that would fall within ANZ C-ITS CAF scope. These, followed by the definition of the use cases and associated C-ITS messages, would form a more solid basis for the further development of the C-ITS. So whereas it is not intended to foster the development of compliance assessment criteria tightly tied to applications, these have been derived from the types of applications and use cases. Some of these requirements and assessment criteria are indeed expected to apply to several applications (i.e. ‘application-neutral’). It is not believed that an approach to define the application scope driven by the supply of international standards (cf. C-ITS Standards Assessment, Section 2.2.1), if this is what is suggested, but it is recognised that the lack of standards can indeed be a barrier for C-ITS implementation and deployment.
2	7	See comment 2a.3 above	
2	8	Yes. What is meant by 'Safety Warning'. Safety critical could be for applications such as red light violation. Safety related could be for traveller information that relate to a safety aspect (e.g. flood warning). Use safety related as opposed to safety warning.	This comment is in line with feedback from other stakeholders. Safety-related C-ITS messages are included as part of the C-ITS CAF application scope.
2	9	Interoperability can only be reached when all messages are conform. Messages that are not tested are useless. Here we shall be careful again between system and station view. Complete RWW solution CAF will require that C-ITS and/or RW trailer are also subject to CAF, in Q1 we consider that we apply CAF to R-ITS and V-ITS i.e. protocol and message conformance would be sufficient,	This comment considers that it is sufficient to assess the protocol and message conformance. The comment is in line with the proposed scope of the C-ITS-specific aspects to form part of the CAF.
2	10	Yes, they are generally in a reasonably mature state (being high on the ‘needs’ list in terms of journey reliability and safety management) and therefore could be integrated with minimal risk. This also means there is strong public/user expectation/demand for this	This comment is in line with feedback from other stakeholders. Safety-related C-ITS messages are included as part of the C-ITS CAF application

Question no	Comment no	Comment	Project team response to comment
		level of information/functionality from C-ITS – right from the outset.	scope. This comment should also be taken into account when defining the D1 C-ITS applications.
2	11	This question comes back to the question of use cases and the underlying policy intent of ITS deployment. Given the potential contribution that C-ITS can make to safety outcomes and road productivity, among other outcomes, it is difficult to establish what Day 1 services you are designing to accommodate, or how quickly you may want to start to deploy Day 2 services.	This comment discusses the difficulty of defining Day 1 and Day 2 services, e.g. related to the currently unknown contribution of such services to safety outcomes or road productivity.
3	12	**Legislative Interactions** We endorse an approach that seeks to align the CAF with existing general regulations in ANZ, to avoid simultaneous application of two or more (legislative) acts, and therefore only include in the CAF aspects which are C-ITS specific or not appropriately dealt with in the more general regulations and codes of practice. It is therefore appropriate for the CAF and its compliance assessment criteria to not duplicate established health and safety, electrical safety, electromagnetic compatibility and energy, general data privacy protection and other requirements. For avoidance of doubt, these should be explicitly noted in the terms of reference for the CAF and conveyed to applicants as being separate from, but in addition to, the compliance assessment criteria. We consider the inclusion of C-ITS security-related requirements (as proposed by Austroads) to be fundamental to the CAF. As discussed earlier, the entire value proposition of vehicle connectivity is predicated on the safety and security of end-users being protected. This will necessarily require the inclusion of C-ITS specific compliance assessment criteria associated with: • C-ITS device hardware and software security-by-design • Interactions with security credential management policies and practices (including C-ITS Security Policy and C-ITS Certificate Policy) • C-ITS application permission requirements and standards	The comment endorses the proposed approach to seek to align the CAF with existing general regulations in ANZ and to include the C-ITS security-related requirements. It is indeed a good idea to explicitly note in the terms of reference for the CAF and convey to applicants that other legal applicable regulations in addition to the C-ITS CAF will need to be adhered to.
3	13	Would this assumption only be applicable if the “ITS regulation” approach is chosen for the CAF?	It is essential to clarify the assumptions for the overall scope of the ANZ C-ITS. The proposed assumptions would largely apply to all model options, whilst noting that some adjustments might be needed depending on specific model options and expected to be done in the downstream works once the preferred model or direction for the future work has been agreed.

Question no	Comment no	Comment	Project team response to comment
3	14	we see the assumptions reasonable.	This comment considers the proposed overall scope of the CAF and legislative interactions reasonable.
3	15	Agree to minimise overlap with existing legislation by recognising and aligning to existing regulations and codes of practice across: • H&S and Consumer Guarantees • Electrical safety, electromagnetic compatibility and energy • Environmental protection • General data protection • HMI	The comment endorses the proposed approach.
3	16	We agree it may not be beneficial to have the CAF replicate existing requirements or regulatory systems, where these adequately deal with subsets of C-ITS systems.	The comment endorses the proposed approach.
4	17	**Lifecycle Management** We consider the proposed lifecycle stages of a C-ITS station to be adequate currently but wishes to highlight one related consideration. The base premise is that compliance is assessed against the CAF requirements applicable at the time of the first making available the C-ITS station on the market. Such an approach is commercially appropriate, as it does not subject an established product in the market to ongoing reassessment against evolving compliance assessment criteria. Assuming no product updates are ever made, this imparts a “once approved, always approved” status, even in the event of the CAF requirements being subsequently revised. However, a mechanism to mandate forced reassessment/withdrawal needs to be considered when, for example, a critical security exploit is discovered that could threaten community safety, and thus results in a mandatory update of the CAF requirements. In the case where a technology provider is self-motivated to make product updates, it is reasonable that appropriate steps be undertaken to demonstrate continued compliance with the CAF requirements. However, it is strongly recommended that for significant changes to in-service products that this assessment occurs against the CAF requirements applicable at the time of the first making available the updated C-ITS station on the market. Care must therefore be taken with respect to clear, consistent criteria for the determination of what constitutes a significant change. Such criteria should be performance-based against the risks under management, rather than based on	This comment supports the proposed life-cycle stages, the base premise (i.e. ‘once approved, always approved’ status) and approach for how to deal with technology provider self-motivated product updates. The need to consider a mechanism to mandate forced reassessment or withdrawal will be highlighted when, for example, a critical security exploit is discovered that could threaten community safety, and thus results in a mandatory update of the CAF requirements.

<table>
<tr><th>Question no</th><th>Comment no</th><th>Comment</th><th>Project team response to comment</th></tr>
<tr><td></td><td></td><td>technology or assumed system design.

Lastly, on the issue of withdrawal from the market, commercial forces (based on features, cost, etc) will typically drive such outcomes irrespective of CAF requirements and policy. In an open technology market, consumers should be free to elect to stay with older but still adequate products, or to upgrade to benefit from newer product capabilities.</td><td></td></tr>
<tr><td>4</td><td>18a</td><td>It mentions that the expected commercial life of a V-ITS-S is 10 years. The average vehicle age in Australia is 10.1 years, and around 40% of vehicles are greater than 10 years old. It is challenging, but should we be expecting a longer life from a V-ITS-S? Vehicle life is likely to be disrupted in the future by different ownership models.

The life cycle should consider potential in-service updates to a system that may affect its approval status.</td><td>The comment provides further nuances related to the average vehicle age in Australia, which will be taken into account.

The comment also highlights that the vehicle life is likely to be disrupted in the future by different ownership models. The CAF model indeed needs to be improved and adapted over time in order to remain fit for purpose.

Regarding the in-service updates, see comment no. 17.</td></tr>
<tr><td>4</td><td>18b</td><td>For both road side and vehicle units, life cycle stages should include:
New device
On going use in service
Modification in service
Withdrawal from service
It may not be necessary to have the same compliance process at each point, but need to consider options at each point.</td><td>This comment is noted and should be taken into account in the downstream works.

Regarding the in-service updates, see comment no. 17.</td></tr>
<tr><td>4</td><td>18c</td><td><table>
<tr><th>Lifecycle stage</th><th>Definition</th><th>Comment</th></tr>
<tr><td>Product evaluation and certification</td><td>Product has undergone and evaluation / certification process</td><td>This may be conducted by EU/US regulatory body or third party bodies.
List the product on the evaluated product list(EPL)</td></tr>
<tr><td>Placing on the market</td><td>A product is placed on the market when it is made available for the first time on the (ANZ) market.</td><td>Assume ANZ adopts Evaluated products from EU/US EPLs</td></tr>
<tr><td>Procurement and Provision</td><td>Product is provisioned with the necessary security certificate, which is a prerequisite for being part of the C-ITS trust model and to be</td><td></td></tr>
</table></td><td>This comment is noted and should be taken into account in the downstream works.

It is noted that some of the assumptions contained in the comment might need to be challenged in the downstream works, e.g. the adoption of US EPLs (cf. C-ITS spectrum management and C-ITS standards assessment, see Section 2.2.1).

It is noted that ETSI TS 102 941 on ITS Security, Trust and Privacy Management (which is currently being revised) defines the C-ITS life-</td></tr>
</table>

Question no	Comment no	Comment			Project team response to comment
		(enrolment)	recognised as a trustworthy entity.		cycle stages. It should also be taken into account in the downstream works.
		Monitor and Manage	Product is kept up to date with necessary updates.		
		Deprovisioning	Either at the end of the certification period (e.g. expiry of the security certificate), prompted prematurely by the market surveillance authorities due to non-compliance (e.g. by withdrawal of security certificate) or prematurely by the user		
		Withdrawal from the market	Product is no longer available for procurement.	Example End of life of the product	
4	19	The 5 stages identified in TCA's Security Standards and Options for Compliance Assurance (TCA 2018, Figure 4).			This comment is noted and should be taken into account in the downstream works. It is noted that ETSI TS 102 941 uses different terms but essentially defines the same stages.
4	20	min. >10 years; and min. +10 years after introduction of a new technology with significantly different functional capabilities to preserve user investment and backwards compatibility			This comment underlines the importance to preserve user investments, ensure backwards compatibility, and the typical transition timeframe involved to introduce a new technology. The project team supports these as guiding principles to be duly considered by the C-ITS CAF governing body.
4	21	We agree that the life stages should include product commencement in the market and withdrawal, whether from expiry of the certification period, voluntary withdrawal from the market, or exit from the market due to non-compliance.			This comment supports the proposed life-cycle stages.
5	22	**Further Basic assumptions** We agree that best-practice compliance assessment models include the registration and dissemination of approved product types via public registers, and that a web-based register of type-approved C-ITS stations should form part of the CAF model. While it is also therefore considered informative to the market and appropriate for approved C-ITS stations to be affixed with a product label (or an equivalent kind of "C-ITS" mark), our experience is that careful measures, including strong legal provisions, need to exist to ensure that only approved C-ITS stations be allowed to carry this label or			This comment agrees with the further basic assumptions, including the registration and dissemination of approved product types via public registers, and the need to put in place a C-ITS CAF governance structure. It stresses the importance to include market surveillance in the overall framework, including strong legal provisions (auditing/enforcement powers and resources).

Question no	Comment no	Comment	Project team response to comment
		mark. False claims of compliance create damaging distortions in the market. As a result, the maintenance of public registers, the issuing of product labels or marks, and the market surveillance to ensure only approved C-ITS stations carry a label or mark should be conducted by an independent party and be included within the scope of the CAF. Lastly, we agree with Austroads' assertion that the CAF (inclusive of its governance structure, requirements and compliance assessment criteria) should be managed as a dynamic system requiring ongoing review and adjustment in line with changes to policy, technology, international standards and market forces. As such, the CAF needs to be established as a sustainable initiative, resourced according to the associated policy directives defining the risks under management and the level of assurance being sought by government.	This comment should be taken into account in the downstream works.
5	23	If there is an onus on the manufacturer to ensure ongoing compliance with the CAF requirements then it should be acknowledged that there may be a resulting onus on the CAF to not alter the requirements in a manner that affects compliance/backwards compatibility of legacy devices.	This comment states that the resulting onus on the CAF is to ensure backwards compatibility of legacy compliant devices. The project team supports this as a guiding principle to be duly considered by the C-ITS CAF governing body. See also comment no. 17 regarding the base premise (i.e. 'once approved, always approved' status) and approach for how to deal with technology provider self-motivated product updates.
5	24	Compatibility and interoperability must be the main aspect when adjustments over time are done. C-ITS will have very long lifecycles, because market penetration is of essence to utilize real benefit; new technologies have to be always compatible and interoperable for safety reasons.	The comment highlights that compatibility and interoperability need to be duly considered in the governance of the C-ITS framework. See also comments above.
5	25	• Agree compliance to be assessed before first entry to the market • Agree on-going lifetime compliance must be on the manufacturer • Agree conformity assessment should be two steps based on typical 'type approval' method: 1. Product testing, 2. Conformity of production • Agree that manufacturer must be responsible for manufacturer controlled changes to products in-service and that there must be a manufacturer's duty to provide evidence of updated compliance before modified product re-introduced on the market.	This comment agrees with the further basic assumptions.

Question no	Comment no	Comment	Project team response to comment
5	26	We do not have a view on the model. This is a more relevant question for the states and territories who are likely to be managing the central and roadside stations. We certainly agree that the design and needs of the C-ITS system will need to be capable of changing over time, with factors for change including developments in the underlying technology and technical standards, evolution of use cases, the unknowns in terms of V2X needs of higher level automated vehicles, changes in the communications landscape, including developments in cellular technology, and changes in the security threat environment, among others.	This comment stresses the importance of the input from states and territories who are likely to be managing the C-ITS-S and R-ITS-S. This comment also stresses that the design and needs of the C-ITS system will need to be capable of changing over time.

Table D 3: Comments related to the main models and overarching architecture

Question no	Comment no	Comment	Project team response to comment
6	1	**Relationship Between C-ITS CAF and AV SAS** We recommend that consideration of a CAF for ANZ would absolutely benefit from a more nuanced approach with regards to the convergence of connected and automated vehicles. We largely subscribe to the European Commission's view that there are key aspects of connected and automated vehicles that 'should be approached horizontally' – most notably, those related to security and connectivity. In principle, we believe that adopting a holistic approach would be both beneficial, and greatly align with developments overseas. Furthermore, if/when the NTC's Safety Assurance System (SAS) proposed for automated vehicles progresses towards implementation, Austroads must consider how these 'horizontal' issues will be managed by what may then be parallel policy, regulatory and compliance frameworks for connected vehicles. It may be beneficial for Austroads to take this opportunity to bring some much-needed attention to what will be coexisting and potentially overlapping concerns from regulatory, governance and compliance assurance perspectives; either by clearly articulating the boundaries of what is envisioned as two separate regulatory frameworks, or by scoping (or by noting, with a view to the future) a more holistic framework. We are pleased to note the inclusion of cybersecurity within the NTC's proposed assessment criteria for the design of the SAS. We do suggest that the matter is less a 'non-safety' or 'other policy' objective, as was recently put forward by the NTC Connected and automated vehicles will have different security requirements – different risks, threats and vulnerabilities that will need to be considered and managed. However, many of these threats and vulnerabilities will overlap, suggesting significant potential	This comment stresses the need to adopt a nuanced approach with regard to the convergence of connected and automated vehicles, either by clearly articulating the boundaries of what is envisioned as two regulatory frameworks, or by scoping (or by noting, with a view to the future) a more holistic framework. The adoption of a consistent and whenever sensible a common approach is promoted, e.g. through a coordinated approach for evaluation of security-related requirements. The Common Criteria Recognition Agreement based on the ISO/IEC 15408 CC series and the ISO/IEC 27000 ISMS are two security-related frameworks that appear to be broadly adopted by the ANZ stakeholders in C-ITS and AV, and hence ought to be considered in the downstream works of C-ITS, connected and automated vehicles.

Question no	Comment no	Comment	Project team response to comment
		advantages and efficiencies may be achieved through coordinated security requirements and techniques.	
6	2a	There will also be non-AV's with C-ITS which will need to be included in a CAF if that is the direction that we go in.	The scenario contained in this comment is supported.
6	2b	I can't see how the SAS should apply at all. This is a technology that could be added to a 20 year old vehicle. The SAS design principles are worth considering though	See also comment no. 1.
6	3	Not merged but could be linked. Safety assurance system needs to focus on AV. Whatever entity is administering the AV could administer the CAF.	See comment no. 1 and comment no. 23.
6	4	This is a hypothetic question we recommend to keep it separate and monitor the experience. A vehicle utilizing a V-ITS-S doesn't necessarily to be an automated vehicle where an automated vehicle may require to have a V-ITS-S.	The comment recommends, for the time being, separate approaches to compliance assessment for C-ITS and AVs. On the other hand it recognises that an AV may require the usage of V-ITS-S.
6	5	Many V-ITS-S and AV technologies are currently independent and therefore independent compliance assessment appears the more appropriate over the short to medium term. Looking further ahead there will be greater overall transport efficiency and safety advantages in highly integrated V-ITS-S and AV technologies. With this increasing integration (and interdependence) there could therefore be potential for a common assessment framework (or at least common elements).	This comment highlights that many V-ITS-S and AV technologies are currently independent and therefore independent compliance assessment appears the more appropriate over the short to medium term. Looking further ahead, with increasing integration (and interdependence) there could be potential for a common assessment framework (or at least common elements). See comment no. 1.
6	6	There are obviously intersections between C-ITS V-ITS-S compliance needs and the work that may be done by a Safety Assurance System for automated vehicles, the latter of which is under development led by the National Transport Commission. It seems premature to strongly link these two projects at this time. It is likely that most C-ITS deployments within vehicles in the next 5-8 years will be in either post-market fitment of vehicle stations, or will come pre-fit in vehicles at lower levels of automation, and thus will not fall under the proposed Safety Assurance System for higher level automated vehicles. Further, there appears to be debate within the vehicle and automated driving system	This comment highlights the intersections between C-ITS CAF for V-ITS-S and SAS for AV. At the same time it is stated that it may be premature to strongly link both projects at this moment. Nevertheless, it is recommended to have a similar approach in terms of the role of the manufacturer vs the role of the regulator.

Question no	Comment no	Comment	Project team response to comment
		industries about the extent to which higher level automated vehicle driving systems will be dependent upon V2X, as opposed to relying upon information from other sources and their own sensors. There are a wide range of views represented in the debate. The capacity to manage cyber security risks is a factor in these debates, as is the desire to build vehicles that are capable of operating in a wide range of world markets with varying underlying infrastructure deployments. It would be beneficial to have a similar approach to the SAS in terms of the role of the manufacturer vs the role of the regulator, which at this stage, is tending towards industry self-certification with some form of assurance by the SAS regulator/s. Nevertheless, we are open to consider a range of models.	
7	7	**Compliance Assessment Policy Options** Best-practice dictates that regulatory options should reflect the *risk appetite* of community and industry, and how the optimum role of government is perceived and understood by them. However, gauging the community's risk appetite and translating it into regulatory options may be difficult in this case. Industry and governments are familiar with identifying the boundaries of regulations, roles and responsibilities, and are skilled at making careful distinctions between technologies, even when the same device relies on multiple technologies. Unfortunately, the community does not often share these skills. Users of these systems will not view connected and automated vehicles (or C-ITS stations embedded within vehicles and infrastructure) as distinct technologies – they will expect a *truly connected and cooperative experience* integrated across the transportation network. Additionally, daily events demonstrate that community awareness of cybersecurity risks and vulnerabilities is low, despite an assumption and expectation that the safety and security of connected and automated vehicles will be inherent. In short, there is every reason for the 'risk appetites' of communities, industry and governments to substantially differ in this case; as such their understandings and hence thresholds will be different. We appreciate that the four options put forward by Austroads are intentionally 'pure': they capture high-level approaches, and sketch out some of the potential advantages, disadvantages, and implementation challenges. In this sense they successfully capture four distinct options on a spectrum. Austroads has taken care to include in-service updates in the consideration of options – a concern similarly registered by the European Commission. In-service compliance will be one of the most challenging aspects of the regulatory program. Indeed, it will challenge long-held assumptions about what in-service and ongoing compliance mean for the vehicle industry, and for all parties in the regulatory	The four options put forward, according to the comment, successfully capture four distinct options. The four high-level compliance options as presented in the Explanatory Note raise a concern as they seem to imply that only one model can be selected, which was not the intention as also explained orally during the stakeholder consultation meetings. At the high-level workshop, the need to first agree on the main 'pure' models and their main characteristics was emphasised, whilst recognising the possibility to adopt a hybrid approach to the proposed model options, and to adopt different models for different types of C-ITS stations. This was clarified in the amended description of the model options and in the outline of the main options to be considered for the future work.

Question no	Comment no	Comment	Project team response to comment
		environment. Certification and re-certification processes for connected and automated vehicles requiring updates will need careful consideration. Our biggest concern with the four high-level compliance options presented is that they imply that only one model can be selected, and that a single model is appropriate to all risks under management and the level of assurance being sought by government. Based on our experience in administering regulatory telematics programs within Australia, it is asserted that a '*one size fits all'* approach will not work. A key consideration should be the benefits of adopting a risk-driven approach that both manages safety and compliance concerns, while at the same time remaining flexible (as not all changes carry the same risk or require the same level of assurance), so that the CAF *encourages* innovation. We suggest that, looking ahead, optimisation of the outcomes being sought will require a hybrid of two or more of the proposed options, applied according to the associated risk	
7	8a	Combination of those options, different options apply to different type of C-ITS stations.	See comment no. 7.
7	8b	I've listed the main options as I see them, but you could consider some in combination (e.g. 2+3) Road side units: 1. Do nothing 2. New guideline to specify standards for RSUs (could be a new Austroads guide). Could be called up in NITAC or state based ITS contracts. 3. A voluntary certification program (ominaware) 4. Restrict RSUs to only competent entities such as state road authorities or those delegated by declaring as a major traffic control item 5. Regulate standards for RSUs in appropriate Act/Regulations 6. Add new offences/penalties for unauthorised installation Vehicle units: 1. Do nothing 2. New guidelines to specify standards for OBUs (could be a FCAI code of practice) 3. A voluntary certification program (ominaware) 4. Restrict voluntary supply of RSUs to only competent entities such as OEMs. Other	See comment no. 7. In addition, it is noted that the 'do nothing' option is covered by (Continue current approach, CAF Model Option 1). Also, CA should not be confused with market surveillance including auditing and enforcement powers (i.e. option 6, according to the comment). Both techniques are complementary and equally necessary to ensure the protection of the public interests at stake and the smooth functioning of the market. See also Section 3.1. Option 2, according to the comment, is indeed a variant of the pure model 1 but largely does not address the gaps of model 1. However, this variant will be mentioned in the description of CAF models. It is recommended not to include it as one of the main high-level options, in order to avoid presentation of an unnecessarily complex and cluttered range of main options.

Question no	Comment no	Comment	Project team response to comment
		devices need specific public sector approval as they could be higher risk 5. ADRs mandate specific standards 6. Add new offences and penalties for unauthorised installation	
7	9	Not sure this is already covered in any other option, ANZ recognize (adopt) the EU/US evaluated C-ITS stations (or sub set of stations based on a criteria that suits ANZ). In this model ANZ does not need to heavily focus on C-ITS station evaluation aspects of the compliance framework.	The support of the mutual recognition agreement is not considered as a CAF model option, but as a key feature of a CAF model. Indeed, the approach to support consistency with the EU C-ITS approval processes and international standards is recognised as a model evaluation criterion. The model's capability and aptitude to provide this feature were also described. Regarding the adoption of US EPLs (cf. C-ITS spectrum management and C-ITS standards assessment), see Section 2.2.1.
7	10	Non, at least for the time being.	Noted.
7	11	We are comfortable that the four options set out represent the range of policy option. We note that some sort of hybrid may be appropriate, with different parts of the CAF being regulatory (for example, privacy issues regulated under the existing laws), while others could be managed by other policy options such as public sector certification.	This comment endorses the four main policy options. Some sort of hybrid seems to be appropriate.
8	12	**CAF Model Options** We agree with the descriptions and high-level characteristics provided for the four models. Based on our experiences, we offer the following recommendations: Option 1, *Continue Current Approach*, is the least attractive of the four options, given that it would give significant power to suppliers through narrow focus on commercial risk, and any damage/loss, injury or death arising would need to be legally proven as arising from 'unsafe' behaviour of the connected vehicle, and thus culpability of the supplier. A compliance assessment framework based purely on one of the three remaining options, however, may not be fit for purpose. The CAF needs to be flexible enough to balance the traditional objectives of an approval process, but also be responsive to what will be one of the biggest changes – providing assurances for in-service operation and corresponding re-approval processes. The level of assurance provided by Option 3, *Public Sector Certification* – that is, utilising	This comment supports the description and the high-level characteristics provided for the four main models. It also states, what appears to be the general opinion by ANZ stakeholders, that option 1 (continue current approach) is the least attractive of the four main options. It highlights that a CAF purely based on one of the three remaining options, may not be fit for purpose. It further offers some advice where these may be suitable, largely endorsing the guidance given in the Explanatory Note. It also endorses the basic principle that it is the manufacturer that is responsible for demonstrating compliance, including through self-assessment (depending on the risk). The latter is a possibility indeed explicitly described in

Question no	Comment no	Comment	Project team response to comment
		the expertise of a third party – will be necessary in some cases. Changes to core functionality, cybersecurity requirements, or changes that could have unintended impacts on system integrity or other functionality may necessitate a more in-depth re-approval process. There will certainly be many cases where Option 2, *Industry Certification*, in the interests of efficiency and managing low-risk profiles, is most appropriate. For these cases, the following principles can be used to inform whether such an approach provides an adequate level of assurance for the end-users of the system: • Documenting the purpose and scope of proposed changes and updates • Appreciating and analysing the extent to which updates may unintentionally impact other performance aspects, and • Factoring in the historical performance and compliance of the organisation proposing to make the update. *As a point of note*, when comparing what is proposed for ANZ against models proposed or implemented internationally, it is important to look below the surface. For example, in the United States 'self-certification' often entails something very different to what would typically be expected in Australia and Europe. Establishing what 'self-certification' means in a different compliance culture is an important consideration – it would almost certainly require an assessment of what may potentially be broader differences in the underpinning legal and litigation frameworks. Finally, Option 4, C-ITS Regulation, would only be warranted in rare cases where a very high level of assurance is required over the standards, policies and processes used. We concur with Austroads' summary of this option, "Whereas this model, based on a regulation, potentially could provide the highest level of consumer trust and confidence, a key challenge for the legislator is to safeguard the public interests at stake whilst not stifling innovation and keeping it fit for purpose over time." That is certainly the biggest hazard with this option. It should also be explicitly recognised that not all evidence for meeting C-ITS compliance assessment criteria requires a C-ITS station manufacturer to engage the services of a compliance assessment test laboratory. This should be risk-based, and only necessary for high-risk considerations that justify the complexity and expense of third-party assessment, or where the manufacturer is not equipped to adequately undertake their own assessment. This reinforces the principle that compliance *assessment is not about testing*. Testing is the responsibility of manufacturers (through self-assessment, third-party assessment, etc according to risk, complexity and/or commercial drivers), such that the oversighting body exists only to coordinate and validate that a contemporary, robust approach has been	the Explanatory Note (Table 7.1 for options 2-4) and in the outlined type approval processes in the Elaborated findings working document (Figure 4.3), which were made available to the stakeholders in preparation for the high-high level workshop. This comment will be taken into account when seeking to improve the presentation of the CAF model options.

Question no	Comment no	Comment	Project team response to comment
		followed, addressing all established compliance assessment criteria.	
8	13	Not sure you can say the EU framework is an example of regulation More appropriate example is Vehicle Regulation Vehicle recall is an example of industry led compliance to address vehicle issues without regulation. It is noted that road agencies cannot make people hand back vehicles at recall. This shows an example of a hybrid model. industry certification: Code of practice for things fitted to vehicles. For RSU it could be similar to Austroads type approval for ITS. It might not be one association, but an association for vehicle and an association for roadside units. The respective association will unlikely want to deal with the other. Public sector certification: Point out that Austroads type approval for ITS could apply to RSU.	The European Commission intends (according to an e-mail from an official at DG Move, 16 November 2017 and public presentations of DG Move[47]) to make use of its mandate under the ITS Directive to adopt a delegated act by 2018, including laying down the rules on compliance assessment processes. Several tasks are on-going to progress this initiative, but it is true that the overall process is still in a relatively early phase. The project team agrees that the vehicle regulation is a good example to mention. The vehicle recall is a good example of a hybrid model. The reflections on approach are related to the V-ITS-S and R-ITS-S. These will be taken into account in the guidance on the direction of the future work and considerations on what the mix could look like. The relevance of Austroads type approval for ITS (Austroads 2016) is highlighted in Section 2.2.1 and in the Elaborated findings working paper.
8	14	A reasonable combination of "Public sector certification" and "C-ITS regulation" may make sense. As a guideline could be that the process is not so bureaucratic but well defined and legally binding.	This comment advocates a hybrid approach and predominantly-favouring a public-sector certification/regulatory approach. The project team notes that a hybrid approach predominantly-favouring a public-sector certification, in particular for the R-ITS-S, appears to enjoy broad support by ANZ stakeholders. See further the other comments and responses to question no. 10.
8	15	Agree, they align the NTC AV SAS approach.	This comment is noted including the highlighting

[47] For example: Menzel (2017) *European Framework for C-ITS Deployment* and Menzel (2017) *C-ITS Deployment in Europe: Common Security and Certificate Policy* – two presentations of DG MOVE at the Third public workshop of the Amsterdam Group and CODECS, 14 February 2017, Amsterdam

Question no	Comment no	Comment	Project team response to comment
		• Continue current approach: Legal requirements fall well behind industry operating standard, insufficient safety assurance • Industry certification: Requirements keep pace with industry operating standard but perceived and actual independence issues arise • Public sector certification: Independence assured, sufficient regulatory agility to accommodate industry innovation, safety ensured • C-ITS regulation: Industry impeded and innovation held back due to cumbersome full-regulatory processes	of associated key characteristics of the model options. The latter has been added to Table 3.1, in order to complement the description of the key characteristics of the models.
8	16	We do not accept the assumption that the Commonwealth would fund the establishment or operation of C-ITS in either the public sector certification or regulation models. We are generally comfortable with the descriptions of the models. We have a strong interest in nationally consistency and interoperability of C-ITS applications across Australia. We note that if the Commonwealth were to consider whether it was to become involved in a regulatory or quasi-regulatory activity, it must first undertake an analysis of the regulatory impact, including whether the problem can be solved with a non-regulatory solution[48]. Further, when the Commonwealth undertakes new activities such as regulatory activities, it applies the Australian Government Charging Framework[49], which supports government entities to design, implement and review government charging. Under the Charging Framework, regulatory and quasi-regulatory work is likely to be undertaken under full cost recovery. In terms of funding models for infrastructure deployment, we would need to see how this work develops over time and how it reflects a range of principles, including efficiency, identifying who the beneficiaries would be, and its sustainability.	This comment stresses important steps to be taken in case of a regulatory policy option and with respect to the issue of funding in all outlined policy options.
9	17	Do not agree that government regulation is needed to ensure compliance. Only a small reason for government to legislate. Do not want to assume regulation is the only way to ensure compliance.	It is agreed that regulation is not the only way to ensure compliance. This option is one of four main high-level options identified by the project team. See also comment no. 12 regarding the CAF model options. This comment appears to have been triggered by the last sentence on page 5 in the Explanatory Note; 'A higher degree of regulatory intervention

[48] See https://www.pmc.gov.au/regulation/developing-regulation-impact-statement
[49] See: https://www.finance.gov.au/resource-management/charging-framework/

Question no	Comment no	Comment	Project team response to comment
			enables a stronger embedment in the institutional set up, and hence generally greater inspection, auditing and enforcement powers.' The project team still believes this is a correct statement. Further, Section 2.2.5 highlights the Australian Government's approach to regulation; new regulation is to be considered as a 'last resort'; policy makers are encouraged to develop and make use of alternative instruments in shaping the rules of the market. *The Australian Government Guide to Regulation* (Australian Government 2014) contains seven options to regulatory approaches (see Section 2.2.5 for further details).
9	18	**International harmonisation of C-ITS** Safety assurance and compliance assessment activities for connected vehicles are being progressed internationally, and with high levels of cooperation and harmonisation. With technical and standards work now well progressed, attention is shifting more concretely towards the same issues currently being addressed by Austroads – that is, towards regulatory and compliance assurance frameworks, and determining their governance. It is our opinion that, for regions utilising the same underlying C-ITS standards, international harmonisation of core CAF requirements and compliance assessment criteria is possible, providing the open technology market with reduced compliance costs, lower trade barriers and improved time-to-market for innovation. Even if only a fraction of ANZ CAF requirements and compliance assessment criteria were pre-met through international co-recognition, significant benefits could still be achieved.	The comment underlines the importance to embrace the mutual recognition principle. The project team also recognises the importance to seek the adoption of relevant international standards and recognise overseas type approval procedures, even if only applicable for a fraction of the ANZ CAF requirements and compliance assessment criteria.
8-9	19	There should be an agreement for accepting international approvals, particularly for vehicles. Vehicle standards are moving this way with further harmonisation and a move towards 'International Whole Vehicle Type Approval' where a vehicle is approved as complying with an agreed set of regulations and is therefore suitable for approval in the contracted jurisdictions. The new Commonwealth vehicle importation legislation (Road Vehicle Standards Bill) will also allow for overseas approval of vehicles to Australian Standards.	See comment no. 12. Further, today it is very difficult to fully recognise US or Japanese C-ITS EPLs (different from 'international whole vehicle type'), as the USA and Japan have different requirements compared with Australia (see cf. C-ITS spectrum management and C-ITS standards assessment, see Section 2.2.1). The direction of the further harmonisation and

Question no	Comment no	Comment	Project team response to comment
			the move towards 'international whole vehicle type approval' are highlighted in the section on ANZ standards and regulations (Section 2.2.4).
9	20	Yes, when they are applicable definitely means in different geographies different standard profiles may be needed and different rules may be existing.	This comment endorses the mutual recognition principle, even if only applicable for a fraction of the ANZ CAF requirements and compliance assessment criteria. See comment no. 18.
9	21	In theory, yes, but local context needs to be taken into account and it remains to be seen what this might bring up e.g. retention of diverse vehicle source markets (NZ accepts EU, Aus, US, Jap)	This comment endorses the mutual recognition principle but underlines the importance to duly take into account the local context needs. See comment no. 18.
9	22	Generally, we are supportive of utilising international approvals where they are fit for purpose in the Australian environment. Thus we would be comfortable with considering overseas approvals assuming they were able to satisfy Australian requirements, including those relating to cyber security.	This comment endorses the mutual recognition principle, including for cyber security.
10	23	**CAF Governance Architecture** While we appreciate the principles by which the roles within the governance model have been assigned (providing appropriate separation of strategic/operational responsibility and delegation of powers to avoid market manipulation), the proposed model is thought to be too 'heavy-weight' for Australia, for the following reasons: • Overlap between C-ITS/connected vehicle, automated vehicle, and vehicle cybersecurity strategic governance – there would be significant savings and benefits to be achieved through combining the strategic-level bodies across these three areas, with the C-ITS Governing Body effectively becoming a CAV Governing Body. • Potential to establish a single Security, Certificate and Privacy Policy Authority for CAVs – there would similarly be significant savings and benefits through coordination and consistency if there were a single Security, Certificate and Privacy Policy Expert Body for all cooperative, connected and automated vehicle systems (and supporting infrastructure) for road transport. This holistic approach would align with international developments and enable the delivery of an all-inclusive vehicle cybersecurity framework for ANZ. • Potential to collapse the C-ITS Supervision Body into the C-ITS Compliance Assessment Body – given the relatively small ANZ population and budget available,	This comment confirms the need and importance to set up an overall governance model for C-ITS, and appreciates the proposed separation of strategic/operational responsibility and delegation of powers to avoid market manipulation. It considers the outlined model too 'heavy-weight' for Australia, and outlines a combined and lighter governance model for C-ITS/connected and automated vehicles (CAV): • CAV governing body • CAV security, certificate and privacy policy authority for CA • CAV compliance assessment body, including market surveillance. The proposed model has many merits and needs to be discussed and endorsed by the 'CAV body'. The project team will present the outlined

Question no	Comment no	Comment	Project team response to comment
		there is sufficient potential synergy and efficiency (without meaningful loss of governance protection) in merging the responsibilities of the C-ITS Supervision Body into the C-ITS Compliance Assessment Body. We currently provide this dual-role for the management of regulatory telematics programs, with evident efficiency and coordination/consistency benefits. Given the federated nature of Australian government, and with the proposals above applied, it is recommended that: • the CAV Governing Body consist of senior strategic representatives from each State and Territory road and transport agency, and the Commonwealth department • the Security, Certificate and Privacy Policy Expert Body consist of security expert representatives from those same agencies (where they exist) in partnership with industry • the C-ITS Compliance Assessment Body be a jointly-owned (by those same State, Territory and Commonwealth agencies) national body empowered to implement agreed policy on behalf of government and industry.	alternative model to the project reference group and Austroads for guidance whether one of the models or both should be considered in the downstream works. This comment is also related to the relationship between C-ITS CAF and AV SAS (question no. 6), see especially comment no. 1 on two separate frameworks vs a more holistic framework.
10	24	We see the need of the "CITS Governing Body" and the "Security, Certification and Privacy Policy Authority". But not sure the function of the "CITS Supervision Body", may need further elaboration.	This comment confirms the need to set up an overall governance model for C-ITS, and notably the • governing body • security, certificate and privacy policy authority. See also comment no. 23.
10	25	Yes. Give appropriate consideration to where to leverage off existing assurance requirements. May need to come up with a clear diagram to show how it links with the vehicle governance model.	This comment confirms the need to set up an overall governance model for C-ITS, and recommends to seek to leverage off existing assurance requirements (e.g. vehicle governance model). See comment no. 23.
10	26	It seems to be reasonable, the objective should be to keep it simple or not to make it more complex than necessary	This comment considers the outlined model reasonable and highlights the importance to keep it simple and fit for purpose.
10	27	We are not sure if the model translates from the EU, where it is based, to the Australian environment. For example, the role of the C-ITS Supervision Body is not clear from the material supplied. We understand that this role is taken by nation state regulators in the	This comment questions whether the model translates to the Australian environment. Input on who should (or would like to) play an active role

Question no	Comment no	Comment	Project team response to comment
		EU deployment to enable nation states to have a direct role in the framework. If the Commonwealth does not see itself having an active role in managing the C-ITS CAF, it would not necessarily have a role in managing the C-ITS Governing Body, which is a European Commission role in the diagram. If this model was going to be implemented, the states and territories would need to agree amongst themselves as to how they manage the various roles. In our view the main area of Commonwealth interests are in a possible contribution to the security policy aspects of the model and in ensuring a nationally consistent outcome, whether this comes from a legislative or non-legislative solution.	is necessary for the further development of the C-ITS governance architecture.

Table D 4: Comments related to the proposed evaluation criteria and the initial evaluation

Question no	Comment No	Comment	Project team response to comment
11	1	**Evaluation Criteria** We consider the proposed evaluation criteria for the CAF Model Options to be adequate.	This comment agrees with the proposed evaluation criteria.
11	2	Detail of the C-ITS messages (or use cases) with the CAF scope is also required to make the decision.	This comment highlights the importance to elaborate and agree on (Day 1 applications and associated use cases and) C-ITS messages in ANZ, in order to be in position to make an informed decision on the preferred CAF model or direction for the future work (see the main findings of the stakeholder consultation, Section 4.2).
11	3	In our view, innovation is not really important, instead compatibility and interoperability of future enhancements must be part of the criteria. Innovation i.e. new technologies in this respect shall take the pre-conditions in consideration for being real innovation, i.e leveraging the status quo.	This comment suggests to delete and replace '*innovation*' with '*compatibility and interoperability*'. The project team notes that there is indeed some tension between *innovation* and needed *stability* for C-ITS to be developed and largely deployed. However, several stakeholders have underlined the need for the CAF to allow for innovative solutions and not to stifle innovation. Further, it is considered that 'compatibility and interoperability' are means to an end, i.e. to enhance road safety

Question no	Comment No	Comment	Project team response to comment
			and user protection. It appears that the ANZ stakeholders in general consider that the proposed evaluation criteria to be relevant, as noted at the high-level workshop (see Appendix D.1.1).
11	4	yes	This comment agrees with the proposed evaluation criteria.
11	5	We are comfortable with the proposed criteria.	This comment agrees with the proposed evaluation criteria.
12	6	**Evaluation Criteria Priorities** Based on our experience in administering regulatory telematics programs within Australia, the following priorities are suggested, from highest-to-lowest priority: 1. Safety, environmental and user protection 2. Accountability and probity 3. International and domestic consistency 4. Innovation, flexibility and responsiveness 5. Regulatory efficiency 6. Timeliness 7. Other policy objectives It is noted that these seven ranked criteria effectively fall into three overall bands, where the priorities within those bands are somewhat less distinct: • 1-3 provide the core principles stated by Austroads for the CAF (safety, integrity, consistency) • 4-6 provide collective contributions to efficiency and somewhat overlap (flexibility promotes efficiency, efficiency promotes timeliness, etc), and • 7 provides latent potential once initial objectives are met.	This comment largely confirms the priorities of the other ANZ stakeholders. It may make sense to present the evaluation criteria in two or three overall bands, to be explored further with the project reference group.
12	7	1. Safety; 5. Consistency; 7 Timeliness; 2 Innovation	This comment largely confirms the priorities of the other ANZ stakeholders.
12	8	Let us say, innovation is the most unimportant one. All others are important. Compatibility and interoperability over time and continental regions where vehicles drive through seamless without geographical interruption is the main important criteria. Because the quantity of users create the quality.	See comment no. 3. It appears that the ANZ stakeholders in general consider that the most relevant criteria are the ones listed in Appendix D.1.1, noted at the high-

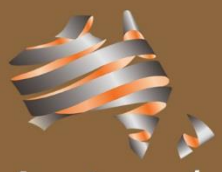
Question no	Comment No	Comment	Project team response to comment
		Provision of data for enforcement could be a sensitive objective counterproductive for acceptance by the users.	level workshop, whilst noting these are not unanimously supported.
12	9	There was a brief discussion on the relative ranking of the criteria which was not concluded. If this approach (ranking is to be used then in effect weighting factors need to be added to derive a final weighted result from Table 8.2 in the Explanatory Note [editor's remark, i.e. Table 4.3 in this document]. This would look to be the preferred approach given 'safety', for instance, is currently treated equally to 'other policy objectives' and 'timeliness' which does not seem right. Suggestions for ranking – most to least important (but not weighting): • Safety • Accountability • Innovation • International and domestic consistency • Regulatory efficiency • Other policy • Timeliness	See comments no. 3 and no. 8.
12	10	We consider that all of the criteria, taken together, represent an appropriate assessment framework and that particular criteria should not be considered in isolation from the others. We consider criteria 1 - safety, environmental and user protection, 2 – innovation, flexibility and responsiveness, and 5 – international and domestic consistency to be the more important criteria. In relation to criteria 1, safety, security and data protection will be crucial to community acceptance and managing risks inherent in C-ITS deployment. The evolving nature of standards, technologies, use cases, etc mean that innovation, flexibility and responsiveness are crucial to the early part of C-ITS deployment. We note the tension between providing flexibility and adequately managing safety and security risks. This may go to use cases deployed in the early C-ITS deployment. One way of managing this tension is to focus on early use cases that are not safety critical, enabling a model to be deployed with a reasonable degree of flexibility without creating unmanageable risks. International consistency calls to the need to align with international developments. For example, it is likely that vehicles arriving in the Australian market over the next 5 years will have vehicle stations pre-fit. It would be advantageous if these units could be used as supplied. In terms of national consistency, it seems likely that the heavy vehicle industry will be an	This comment largely confirms the priorities of the other ANZ stakeholders, taking notice of the remark that particular criteria should not be considered in isolation of others. This comment highlights important considerations with respect to the criteria, for example, the tension between providing flexibility and adequately managing safety and security risks. The suggestion to manage this tension by focusing on early-use cases that are not safety critical is duly noted.

Question no	Comment No	Comment	Project team response to comment
		early user of C-ITS systems, and this can be seen from the selection of heavy vehicles in a range of the Australian C-ITS trials. While individual state or territory road agencies may have their own use cases that they want to implement, for example, aimed at road productivity improvement, it would be wasteful and frustrating if a lack of national consistency made it difficult for interstate heavy vehicles to use C-ITS systems in a seamless way across state and territory borders. The same argument follows for all vehicle classes, but particularly apply to heavy vehicles in early deployment. In relation to criteria 4 - regulatory efficiency, cost and industry burden, we reiterate the points made in relation to question 8 in terms of the Commonwealth's policies on assessing regulatory burden and on cost recovery of government activities.	
13-14	11	**General CAF Model Assessment Feedback - Preferred CAF Model(s)** Our general feedback on the assessment of CAF Model Options provided by Austroads is to largely agree with the outcome – the predominantly-favoured approach (catering for the majority of anticipated risks managed at the level of assurance being sought by government) being Public Sector Certification. However, as expressed earlier, our experience suggests (cf comment no 6 in Table D 3) that a single model fails to provide potential efficiencies by requiring all compliance assessment activities to conform to a single process. A stratification of compliance assessment activities across Industry Certification, Public Sector Certification, and C-ITS Regulation – according to an assessment of risk linked to the specific compliance assessment criteria, and the historical performance and compliance of the organisation in question – is recommended as the best-practice approach.	This comment is consistent with the key points noted at the high-level workshop, i.e. a hybrid model approach, and predominantly favouring a public-sector certification approach (for the R-ITS-S).
13	12	There is a real-risk that if Australia goes ahead with something that makes compliance too hard, then (unless it is made mandatory) we will be put in the too-hard basket and won't receive vehicles with C-ITS and the benefits that come with them. Another challenge here will be that over-regulation in this space has the potential to stifle innovation.	This comment points out the risks associated with over-regulation, i.e. notably with model option 4. See also the main findings of the stakeholder consultation (Section 4.2).
13	13	Is a good and useful assessment.	This comment endorses the assessment.
13	14	We consider it a useful introduction to the policy issues developing the CAF raises. We believe a number of the questions it raises will become clearer going forward, with the further discussion, the experience gained from trials including overseas trials, and the development of international standards and systems.	This comment endorses the assessment being a useful introduction to the policy issues that developing the CAF raises.

Question no	Comment No	Comment	Project team response to comment
14	15a	The assessment method (Table 8) could be further find tuned. E.g. Against different type of C-ITS station, the result could be different; and could be further break down for "partially meet", meeting 10% and 90% are quite different.	This comment contemplates the benefits of adding further nuances to the assessment method (assuming that Table 8.2: Assessment of the C-ITS CAF model options against the proposed evaluation criteria in the Explanatory Note is meant here). The project team can see the benefit in the downstream works to separate the evaluation of the models for the V-ITS-S and R-ITS-S, noting that it would be beneficial, not to say necessary, to first agree on a common ANZ C-ITS strategy, agreed Day 1 applications and associated use cases and C-ITS messages. The project team would think that it sufficies to distinguish between three quantitative results per evaluation criteria accompanied with their qualitative rationale.
14	15b	Suggest other options are considered. E.g. I don't think industry certification is purely just the omniaware model. Could include just having industry agreed standards.	This comment suggests that other (main high-level) options should be considered, but it is not clear which other models ought to be considered noting: • The voluntary industry association certification is not purely the OmniAir model; the assumed key features (self-regulation, voluntary, governed by an industry association…) are described in the overview of the CAF model options (see Section 3.2.2 and Table 3.1). • See Table D 3/comment no. 12.
14	15c	I don't have a firm position yet, however I would keen to consider a combination of the options. E.g. industry certification for OEM V-ITS-S, Public sector certification for R-ITS-S and C-ITS Regulation for aftermarket V-ITS-S.	This comment is in line with the main findings, noting the importance to progress the adoption of a common C-ITS strategy, agreed Day 1 applications, and associated use cases and C-ITS messages.
14	16	We should not fall into the trap of ranking or prioritising the 4 options listed in the paper. It will almost certainly be a hybrid model that is established, with a mix of multiple options, and any government regulation will likely be minimal. Hopefully this will be highlighted in	This comment is overall in line with the main findings, i.e. a hybrid model is likely to be the favoured model and potentially different models

Question no	Comment No	Comment	Project team response to comment
		the final report, including some guidance/options on what the mix could look like.	for the V-ITS-S and R-ITS-S. It is premature at this stage to choose the model(s), given the necessary desirable prerequisites are not in place (see comment no. 2). The project team will propose guidance on the direction of the future work and considerations on what the mix could look like.
14	17	A reasonable combination of “Public sector certification” and “C-ITS regulation” may make sense. As a guideline could be that the process is not so bureaucratic but well defined and legally binding. Other best practices e.g. European experience and approach could be considered.	This comment advocates a hybrid approach and predominantly-favouring a public-sector certification/regulatory approach, and to seek adoption of the European C-ITS approach. See comment no. 16.
14	18	Public sector certification	This comment considers the public-sector certification to be the preferred model (see further this stakeholder's comments on the model options in Table D 3/comment no. 15).
14	19	Given the range of elements of C-ITS systems that are still in a development phase (as discussed in response to question 12), if the policy intention is to get C-ITS up and running reasonably quickly to enable use-cases to come forward, then third party or public sector certification seem reasonable compromise solutions. It may be possible that, over time, some elements may need to be hardened into legislation, for example, to support a regulatory use case, of for security reasons, but this should not be an initial position while so much of the underlying frameworks are in flux, and the deployment uses cases and funding models are unclear.	This comment stresses the importance of third-party or public-sector certification to get C-ITS up and running reasonably quickly and points out the possibility to harden some elements into legislation at a later stage.
15	20	**Transitional Considerations** As with any significant initiative, a transitional approach is of benefit to government, industry and those appointed to oversight the compliance assessment model introduced. The risks associated with a ‘big bang’ introduction typically far outweigh any perceived benefits of concurrent universal adoption. Such policies, requirements and criteria require time to mature and incremental improvement during the early stages of adoption to optimise the outcomes being sought. We recommend the use of transitional arrangements and the staged adoption of a CAF for ANZ. Such stages could be along geographical lines, by vehicle type or other manageable segmentation.	This comment recommends the use of transitional arrangements and a staged adoption of a CAF for ANZ. Such stages could be along geographical lines, by vehicle type or other manageable segmentation. The recommendation will be taken into account in the outline of the forward plan, which initially will be discussed with the project reference group.

Question no	Comment No	Comment	Project team response to comment
15	21a	Would this question only be applicable if the “ITS regulation” approach is chosen for the CAF? And if this is the case, yes, a transitional approach should be adopted, but consider this is a new area and there are relatively small numbers of ITS-S vendors, the transition period could be shorter than usual.	The question is applicable for model options 2-4 and combinations thereof. See also comment no. 16.
15	21b	I think an interim arrangement is needed now as devices can already be brought to market with the ITS class license. There is a real risk to me that some small projects go off and do their own thing and don’t understand what they’re doing. We want to avoid a patchwork of devices later on. The document produced should be similar to the Austroads/NTC guidelines for trials of automated vehicles. Should consider both RSUs and VSUs. Suggest we go to FCAI/Truck Industry Council to seek support in developing one. I think the CAF2109 project should consider developing that right now, even before this project is complete. Initial guidance would be light, but develop in time as we develop standards.	This comment recommends the use of transition agreements, including an initial guidance note ideally prepared jointly with the FCAI/Truck Industry Council. See further comment no. 20.
15	22	A transition from "Current Approach" to a reasonable combination of "Public sector certification" and "C-ITS regulation" in a well-defined time of 2-5 years would definitely accelerate the deployment process and the acceptance.	This comment suggests implementation of a hybrid approach based on a mix of public sector certification/C-ITS regulation within two to five years. See comment no. 16.
15	23	Yes, as discussed above. Over time, the initial scheme may prove to be capable of the modification necessary, or it may be decided to move to another model.	This comment agrees with adopting a transitional approach, where over time the initial scheme may be modified or be replaced by another model.



Austroads

Level 9, 287 Elizabeth Street
Sydney NSW 2000 Australia

Phone: +61 2 8265 3300

austroads@austroads.com.au
www.austroads.com.au