Austroads

Research Report
AP-R479-15

Concept of Operations for C-ITS Core Functions

Concept of Operations for C-ITS Core Functions

Prepared by

Freek Faber and David Green

Project Manager

Stuart Ballingall

Publisher

Austroads Ltd.
Level 9, 287 Elizabeth Street
Sydney NSW 2000 Australia
Phone: +61 2 9264 7088
austroads@austroads.com.au
www.austroads.com.au

Abstract

This document defines the core functions of the C-ITS platform including their objectives and capabilities. It identifies user needs and describes how the system will operate.

The Concept of Operations is intended to be an input to future decision making and system engineering documents, including system requirements and design documentation.

Keywords

Cooperative ITS, C-ITS, Concept of Operations, ConOps, core system, core functions.

ISBN 978-1-925294-13-2

Austroads Project No. NT1785

Austroads Publication No. AP-R479-15

Publication date March 2015

Pages 124

About Austroads

Austroads' purpose is to:

- promote improved Australian and New Zealand transport outcomes
- provide expert technical input to national policy development on road and road transport issues
- promote improved practice and capability by road agencies
- promote consistency in road and road agency operations.

Austroads membership comprises the six state and two territory road transport and traffic authorities, the Commonwealth Department of Infrastructure and Regional Development, the Australian Local Government Association, and NZ Transport Agency. Austroads is governed by a Board consisting of the chief executive officer (or an alternative senior executive officer) of each of its eleven member organisations:

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

The success of Austroads is derived from the collaboration of member organisations and others in the road industry. It aims to be the Australasian leader in providing high quality information, advice and fostering research in the road transport sector.

Acknowledgements

The authors would like to thank Stuart Ballingall, Austroads C-ITS Project Director, for his valuable and detailed input throughout the project and Jacobs for its review and feedback.

This report has been prepared for Austroads as part of its work to promote improved Australian and New Zealand transport outcomes by providing expert technical input on road and road transport issues.

Individual road agencies will determine their response to this report following consideration of their legislative or administrative arrangements, available funding, as well as local circumstances and priorities.

Austroads believes this publication to be correct at the time of printing and does not accept responsibility for any consequences arising from the use of information herein. Readers should rely on their own skill and judgement to apply information to particular issues.

Preface

Cooperative intelligent transport systems (C-ITS) can be defined as a subset of the broader suite of ITS that use a range of wireless communications to share information between vehicles, roadside infrastructure, mobile devices and centres. This will allow vehicle and transport applications to cooperatively work together to deliver safety, efficiency and environmental outcomes that are beyond what is achievable with standalone ITS and vehicle applications.

Austroads is taking a lead role in establishing an operational framework that will enable emerging C-ITS to be deployed in Australia and New Zealand. It has been decided to take a Systems Engineering approach of which a Concept of Operations is a key document. ARRB Group was engaged by Austroads to compile the document.

The purpose of the document is to define the C-ITS platform core functions including their objectives and capabilities, identify user needs and describe how the system will operate. The Concept of Operations is intended to be an input to future decision making and System Engineering documents, including system requirements and design documentation.

Inputs include the *Policy Framework for Intelligent Transport Systems in Australia*, the *C-ITS Strategic Plan*, the Austroads *National ITS Architecture* project (NS1696), the FRAME ITS architecture and a range of consultations and reviews.

The intended audience is all stakeholders that may be involved in the deployment of C-ITS in Australia and New Zealand. These include different user groups (such as fleet managers, drivers, travellers, motoring organisations, emergency services), road agencies, toll operators, rail operators, vehicle manufacturers, original equipment manufacturers, dealers, mobile device manufacturers, telecommunication operators, ITS infrastructure manufacturers, C-ITS service and content providers, representative organisation such as the motorist organisations, the Federal Chamber of Automotive Industries and the Motor Industry Association, the Truck Industry Council and the Road Transport Forum, standardisation organisations, certification organisations, regulators such as communications and media authorities, industry-specific regulators, national competition authorities, policy makers and the national and state privacy commissioners.

The development of a Concept of Operations is an iterative and evolutionary process. This is considered to be version 1.0 of the Concept of Operations for C-ITS core functions, which is based on the current understanding and stakeholder inputs on what is an evolving system. As local and international consensus is achieved, it is intended to update the Concept of Operations as appropriate.

Contents

Tables

Figures

1. Scope

1.1 Identification

This document describes a proposed 'Concept of Operations', which is intended as an input to the planning and elaboration of core functions that will support the deployment of cooperative intelligent transport systems (C-ITS) within Australia and New Zealand[1].

The document is the deliverable of the project *Cooperative ITS (Stage 2b): Development of a Concept of Operations for Cooperative ITS* (NS1785), and is part of the Austroads Cooperative ITS project.

1.2 Document Overview

This section describes the objective of the document, the applied methodology and the structure of the document.

1.2.1 Purpose

The purpose of the Concept of Operations document is to provide clear guidance for the development of C-ITS in Australia and New Zealand and facilitate discussion with key stakeholders. The Concept of Operations is intended to be an input to future decision making and System Engineering documents, including system requirements and design documentation.

It is important to understand that the Concept of Operations relates to the provision of 'core functions' that are necessary in order to facilitate and enable C-ITS service provision. The document does not provide a Concept of Operations for any particular C-ITS application.

Additionally, the report intends to capture the views of stakeholders and includes these in a reflection on the findings and recommendations for future decision making.

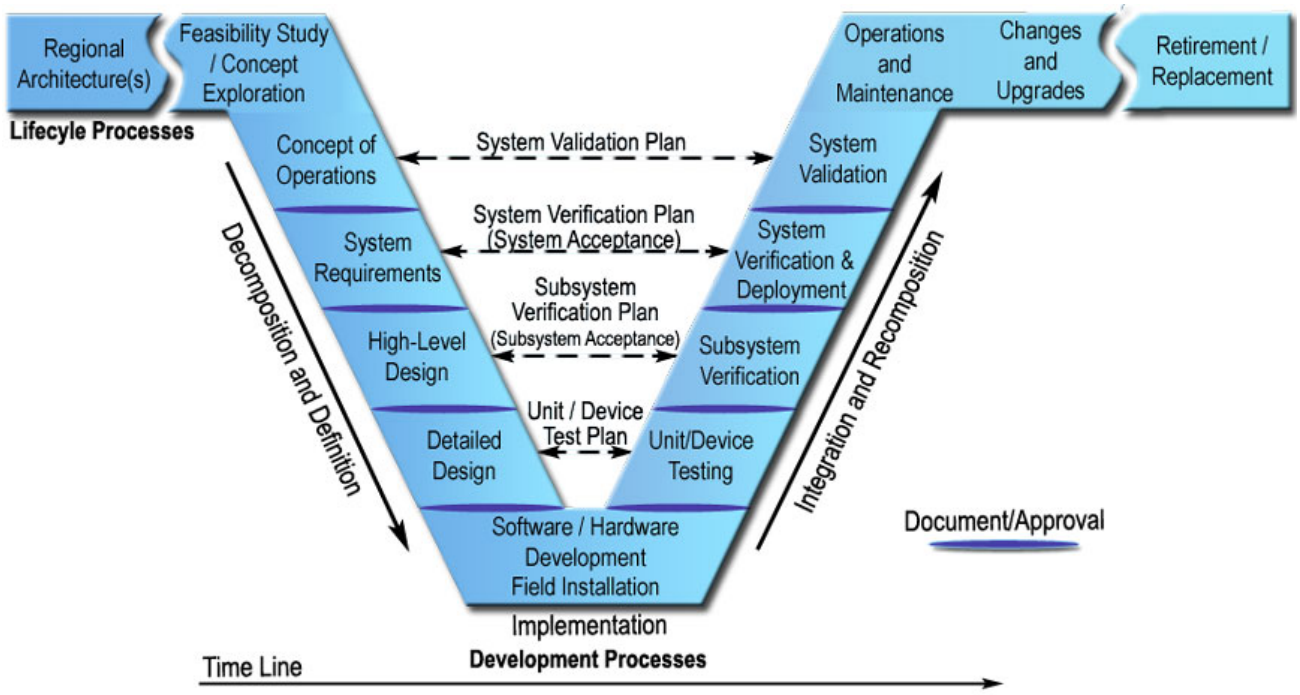
1.2.2 Methodology

It was decided to take a Systems Engineering approach and to develop a Concept of Operations document as described in the Institute of Electrical and Electronic Engineers (IEEE) 1362 standard (IEEE 1362-1998: 2007).

Systems Engineering is an interdisciplinary approach and a means to enable the realisation of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem (Federal Highway Administration 2007). The Systems Engineering V-model, as illustrated in Figure 1.1, describes the role of a Concept of Operations document in the Systems Engineering approach and in the ITS design process.

[1] The concepts are generally applicable to both the Australian and New Zealand context, although there are differences that need attention in respect of each national environment. In these cases, a reference is made to the specific national issues. The main differences are that the issue of having state-level jurisdictions is not relevant to New Zealand and the import into New Zealand of significant numbers of second-hand vehicles from the Japanese market.

Figure 1.1: Systems Engineering V-diagram



Source: Intelligent Transportation Systems Joint Program Office (2013).

A 'Concept of Operations' is a user-oriented document that describes system characteristics for a proposed system from the users' viewpoint. This describes C-ITS stakeholders, their roles and responsibilities, an overview of the emerging system design, a high-level description of how the system will operate, and it should highlight identified issues with the operational framework that will need to be addressed.

The Concept of Operations is part of the initial phase of the Systems Engineering process and includes:

- an overview of the existing ITS system
- a justification for a C-ITS core
- a description of the proposed core functions
- the system's stakeholders, their roles and responsibilities.

This lays the foundations for the system requirements for the C-ITS core functions and consequently the high-level and detailed design. It defines the boundaries of these systems and provides an understanding of who the stakeholders are and identifies their needs.

The steps taken in the development of a Concept of Operations can be summarised as follows:

- review relevant projects, initiatives and research
- consult with key system stakeholders
- develop the Concept of Operations document.

A review of international sources including European and US literature related to concepts of operation and system specifications was performed as part of this project in 2012[2]. This review included the US *C-ITS Core System: Concept of Operations* document (Research and Innovative Technology Administration 2011) as an example of a Concept of Operations for a C-ITS core system. Other European and US documents that were used as key inputs are COMeSafety (2010), ISO 21217, Shulman (2012), and a technical policy analysis of the US Core System (Federal Highway Administration 2012).

The inputs to the Concept of Operations in the Systems Engineering approach are the Regional Architecture, a Feasibility Study/Concept Exploration, a Needs Assessment and a Systems Engineering Management Plan. These inputs were not available. The required information from these input documents has either been obtained from other sources or assumptions have been made.

The Australian ITS architecture is currently being developed in Austroads project NS1696 – National ITS Architecture. As part of this project, international ITS architectures were reviewed and it was recommended that the European FRAME Architecture be used as the basis for the Australian and New Zealand ITS architecture. For example, the classification of service domains from the FRAME architecture was used in this Concept of Operations. This was guided by the decision in NS1696 to use the FRAME architecture as a basis. Where needed, this document has made assumptions on the ITS architecture based on the FRAME architecture and the Austroads *C-ITS Strategic Plan* (Austroads 2012).

Stakeholder needs were obtained as part of the project. A stakeholder consultation was performed in collaboration with the University of South Australia and Queensland University of Technology. Twenty-five consultations were undertaken with stakeholders from industry and road agencies in Australia and New Zealand, as well as international C-ITS experts. Stakeholders were consulted about their view of C-ITS, core capabilities, user needs, and roles and responsibilities. The key findings from the stakeholder consultation can be found in Appendix A. Additionally, the US Core System needs have been assessed in the context of Australia and New Zealand based on the stakeholder consultations as shown in Appendix B.

The selection of which standards are to be used for the C-ITS core functions for Australia or New Zealand is to be assessed in the subsequent stages of the Systems Engineering approach. A review of C-ITS standards titled *Cooperative Intelligent Transport Systems (C-ITS) Standards Assessment* (Austroads 2015) is being performed as part of the current project NS1785 – Cooperative ITS Project (Stage 2c) as well.

This C-ITS core functions Concept of Operations proposes core functions on a conceptual level. The internationally emerging platforms as described in Section 3.3.4 are however an important input to this work.

The intended audience for the Concept of Operations is the stakeholders involved in deploying C-ITS as described in Section 1.3.4.

1.2.3 Structure of the Document

In line with the Concept of Operations format, the document is structured differently from a typical research or policy report. The structure largely follows the outline of a Concept of Operations as defined in the *IEEE Guide for Information Technology – System Definition – Concept of Operations* (IEEE 1362).

The document describes the scope of the work, and lists the referenced documents. It describes the situation with the current ITS systems, and the justifications for and nature of changes. This leads to a description of the proposed core functions and operational scenarios. The impacts are also described and an analysis of the proposed system is provided. The document structure is:

- Section 1: Scope
- Section 2: References

[2] C-ITS Concept of Operations Discussion Paper 1 (Draft – 17 December 2012) by Greg Hood, David Green and Charles Karl – not published.

- Section 3: The Current System or Situation
- Section 4: Justification for and Nature of Changes
- Section 5: Concepts for the Proposed System
- Section 6: Operational Scenarios
- Section 7: Summary of Impacts
- Section 8: Analysis of the Proposed System.

The development of C-ITS and the C-ITS core functions involves multiple systems that need to work together which will be developed and managed by many different stakeholders (rather than a single complex technical system developed by a single organisation). This means that there is not one engineering task, but several independent engineering tasks by different organisations. To better describe how multiple engineering tasks by different stakeholders result in the complex system of systems, this document has diverged slightly from the standard IEEE Concept of Operations format. Additionally, content has been added to cover the absent inputs from the upstream documents describing a Regional Architecture, a Feasibility Study/Concept Exploration, a Needs Assessment and a Systems Engineering Management Plan.

Also most Concepts of Operations propose modifications of an existing system. In this case, no C-ITS core currently exists. As suggested in the IEEE standard, alternative to describing the current systems, the document describes the current situation. This made three of the sub-section from the IEEE standard redundant, being *'3.4 Modes of Operation for the Current System or Situation', '3.5 User Classes and Other Involved Personnel'* and '*3.6 Support Environment'*. These sections have therefore not been included in this document.

Diversions from the IEEE standard are:

- inclusion of user needs assessment and stakeholder consultations (Appendix A and Appendix B)
- exclusion of three sections on the current system
  - 3.4 Modes of Operation for the Current System or Situation
  - 3.5 User Classes and Other Involved Personnel
  - 3.6 Support Environment.

Appendix D shows the mapping of the document structure to the standard document structure for Concept of Operation documents, which is the IEEE 1362-1998:2007 standard. The structure of the US C-ITS core Concept of Operations is shown in the table as well.

1.3 System Overview

This section introduces the purpose of the proposed core functions to which the Concept of Operations applies. It first describes the emerging C-ITS, including a high-level description of how it fits within the broader ITS environment. The core functions will be necessary to support this emerging cooperative intelligent transport environment

1.3.1 Cooperative Intelligent Transport Systems

A nation's road transport system is critical not only to its economy, but also to its social and environmental well-being. It includes numerous modes of transport, including passenger vehicles, buses and trucks, and vulnerable road users such as pedestrians, bicycle riders and motorcycles. It also is increasingly integrated and interfacing with other non-road-transport modes, such as trains.

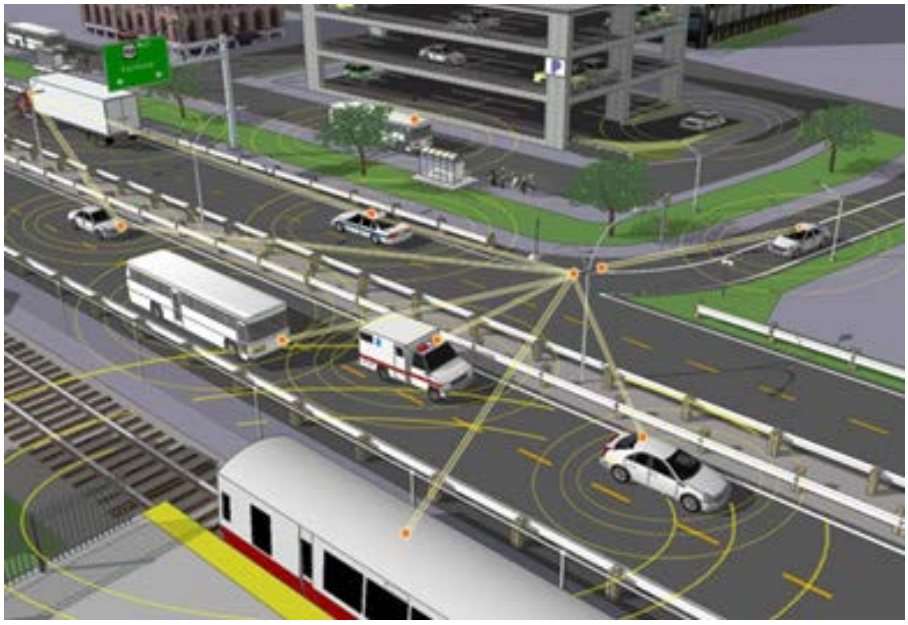
Australian and international transport authorities and their stakeholders are faced with three main transport challenges of improving safety, improving mobility and reducing the environmental impact of transport. ITS, which can be defined as the use of Information and Communication Technologies (ICT) within the transport network, have progressively assisted in meeting these challenges.

Cooperative ITS (C-ITS) is a subset of the broader suite of ITS which use wireless communications to share information between vehicles, roadside infrastructure, mobile devices and centres. 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.

The key public objectives for the deployment of C-ITS in Australia and New Zealand as described in the Austroads *Cooperative ITS Strategic Plan* include a reduction in the number of fatalities and serious casualties caused by road crashes, a reduction of the costs associated with road trauma, a reduction in traffic congestion, an improvement of the productivity in road infrastructure use and a reduction in the environmental impacts of road transport, through less emissions and fuel use (Austroads 2012).

The C-ITS that are evolving will have wireless connections between the actors in road transport, and the deployment will be multimodal, as shown in Figure 1.2.

Figure 1.2: Multimodal cooperative intelligent transport systems



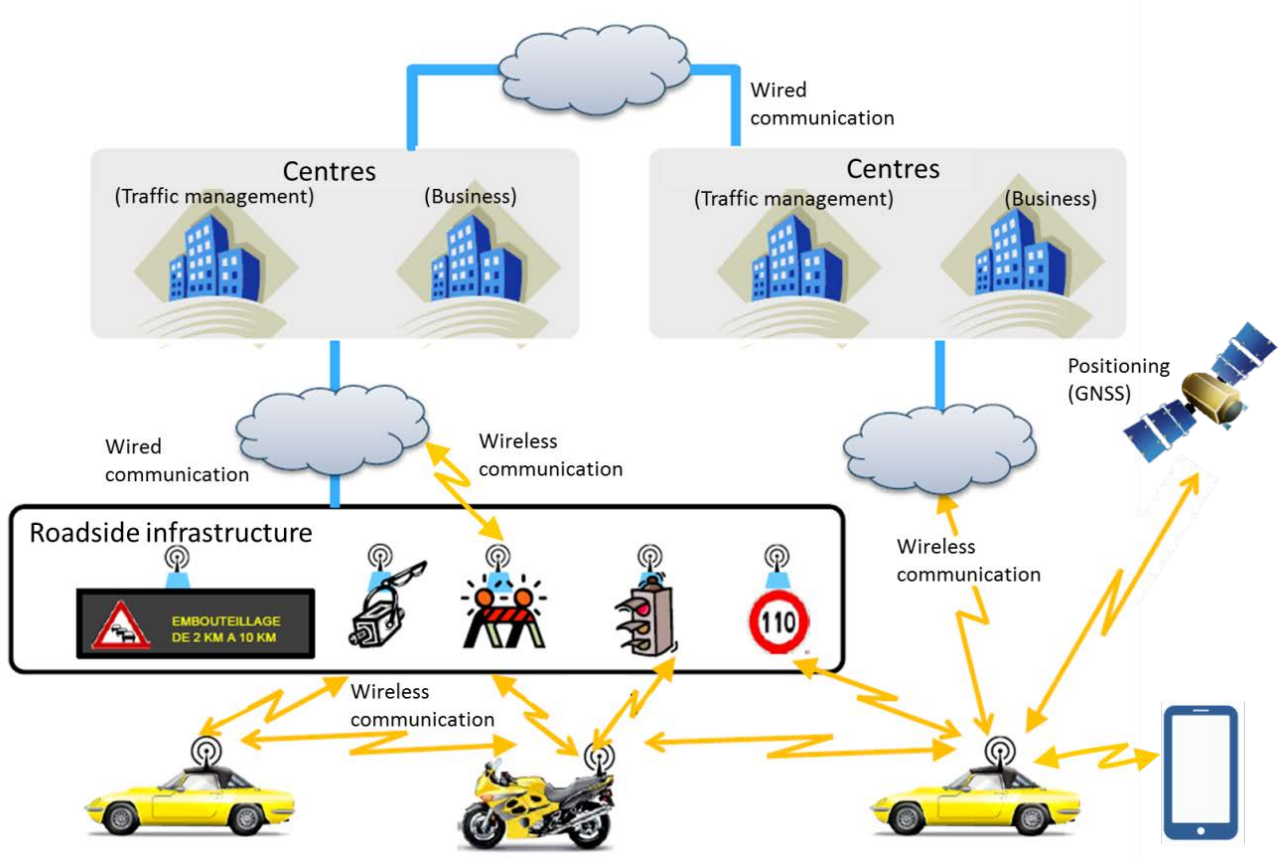
Source: Andersen and McKeever (2011).

The emerging C-ITS will involve connections between:

- vehicles – equipped with built-in, aftermarket or nomadic C-ITS devices
- infrastructure – ITS roadside infrastructure connected through C-ITS
- centres – traffic management centres and service providers' back office centres
- mobile devices – e.g. smart phones and other nomadic devices focussed on assisting vulnerable road users (e.g. bicycle riders, pedestrians) or other road users.

In addition, many C-ITS applications and services will also require a connection with Global Navigation Satellite Systems (GNSS) for positioning, navigation and timing data. The connections between the various actors in the cooperative intelligent transport environment are illustrated in Figure 1.3.

Figure 1.3: Cooperative intelligent transport systems



Source: Modified from Lan (2013).

C-ITS applications and services

The emerging C-ITS will provide a platform on which service providers can use their initiative to develop and deploy a wide range of applications and services[3]. Appendix C provides a list of potential applications and use cases that European Telecommunication Standards Institute (ETSI) considers as deployable after a first complete set of C-ITS standards is available. While it may be difficult to predict the full range of applications that may be seen in future, it is possible to categorise the types of applications that are currently under development.

A typical categorisation is by policy impact area, distinguishing safety, traffic efficiency and environmental impacts. However, there are several ways to categorise C-ITS applications and services, for example by:

- policy impact area: traffic safety, traffic efficiency or environmental impacts
- communication latency requirements: time-critical or non-time-critical, or the possible value range in ISO/TS 17423 on ITS application requirement for selection of communication profiles (smaller than 1 ms, 10 ms, 1s, 10 s, 1 min, 10 min or 1 h)
- positioning accuracy requirements
- safety-of-life and property risk: safety critical and non-safety critical
- level of guidance: informing, warning or automated

[3] The difference between an application and a service is that an application is a specific implementation of a service in terms of hardware and software. Since these specific implementations are to be determined, the two terms can be used interchangeably. The terms are used interchangeably in the document.

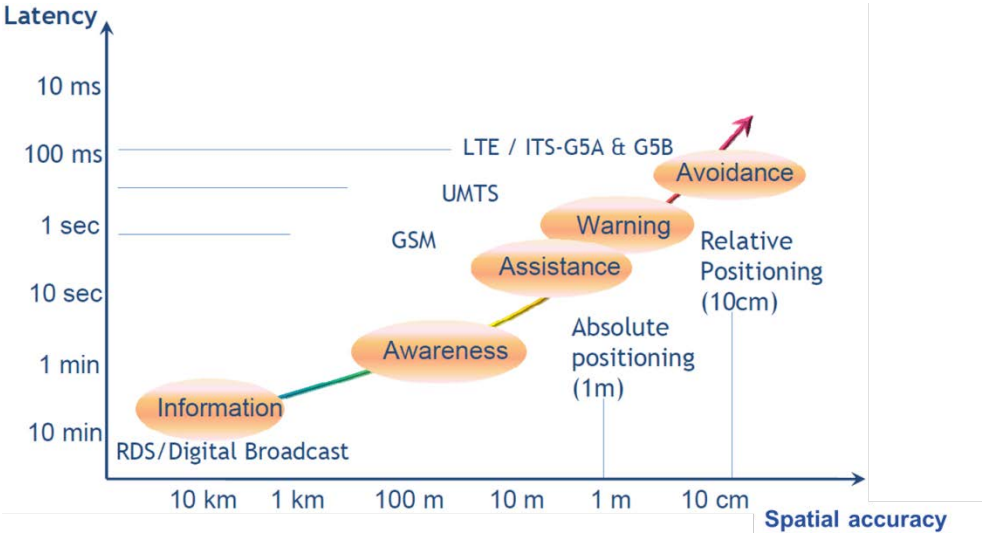
- driving task: strategic driving tasks (navigation, trip planning), tactical driving tasks (lane choice, speed choice) or operational driving tasks (steering, braking)
- type of user: fleet management, traffic management or consumer market applications.

A common categorisation used by ERTICO and other stakeholders is based on the applications' influence on the driving task. These categories include:

- information – e.g. travel time services
- awareness – e.g. road works warning
- assistance – e.g. intelligent speed adaptation
- warning – e.g. collision warning
- avoidance – e.g. electronic brake assist
- automated – e.g. cooperative adaptive cruise control.

Figure 1.4 shows a modified version of a diagram from ERTICO, which plots these application categories on a graph based on their latency and spatial accuracy requirements. While this is a useful representation, it is noted that there may be some types of application that do not fit neatly in this categorisation.

Figure 1.4: Types of C-ITS by latency and spatial accuracy



Source: Modified from ERTICO (2011).

Communication technologies

As per the earlier definition, C-ITS refers to the use of wireless communications to share information between vehicles (V2V) and between vehicles and infrastructure (V2I/I2V). C-ITS will involve a range of communication technologies, and many C-ITS applications will likely use a hybrid communications approach. That is, an application may use several communication mediums, and not necessarily rely on one type.

Communication technologies have different characteristics and attributes and are suited to different types of applications. Table 1.1 shows the categories of communication technologies and their attributes.

Table 1.1: Wireless communication technologies and attributes

Category	Communication technologies	Attributes
Short range communications	Examples include: • 5.9 GHz DSRC • Wireless LAN (e.g. WiFi) • Bluetooth • Infra-red	• Short range • Low to very low latency • Two-way communications
Long range communications	Examples include: • Cellular networks, including: – UMTS (3G) – LTE (4G)	• Long range • Medium to low latency • Two-way communications
Wide area broadcast	Examples include: • Digital radio (e.g. DAB+) • Analogue radio	• Long range • Medium to high latency • One-way

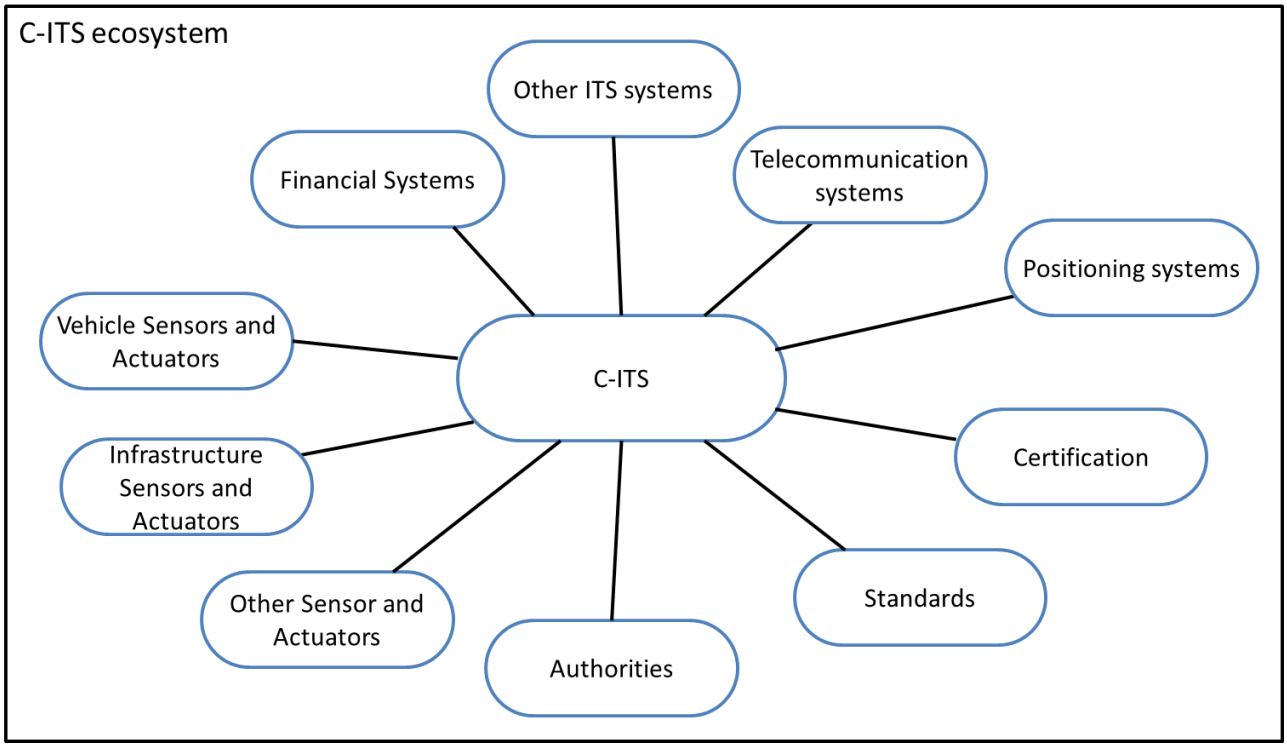
These communication technologies and their current use are described further in Section 3.3.3.

1.3.2 System of Systems

C-ITS comprise a dynamic, distributed computing environment with computing units in vehicles, roadside infrastructure, mobile devices and central systems. C-ITS can be described as a 'system of interoperable systems'. Some of the external systems, as shown in Figure 1.5, that make up the C-ITS community include:

- telecommunication systems – C-ITS require communication systems to provide connectivity
- positioning systems – in order to determine the position of a C-ITS entity, positioning is required, which can then be paired with mapping to create knowledge of the surroundings of an entity
- certification bodies – to be able to certify devices and applications to ensure their operation is appropriate with respect to the system environment
- standards – to provide specifications and conformance tests to ensure devices and applications can interoperate and their ability to interoperate can be assessed
- authorities – to oversee C-ITS, ensure compliance with standards, and ensure that its deployment and uptake has benefits to the road users and does not result in a negative impact on the road environment
- other sensors and actuators – to obtain external input of the road environment from central systems
- infrastructure sensors and actuators – to obtain external input of the road environment from infrastructure installed along or within the road
- vehicle sensors and actuators – to obtain input on vehicle status from sensors within the vehicles
- financial systems – in order to support financial transactions associated with C-ITS (e.g. tolling)
- other ITS systems – C-ITS are one part of a broader ITS.

Figure 1.5: External systems that make up the C-ITS community



Source: Modified from ISO 17427.

1.3.3 C-ITS Core Functions

This Concept of Operations aims to identify those core functions that are required to enable C-ITS applications to be deployed and positive transport and societal outcomes to be realised.

The following aspects are to understanding the roles of, and therefore the Concept of Operations for, core functions:

- Some processes relate to the provision of a specific application service (external processes, objects and data).
- Some processes are required to enable services but are not specifically part of that service provision (internal processes, objects and data).
- Different transactions require different levels of security.
- Different transactions require different levels of latency.

Systems that require a high level of trust, and in many cases, systems that require low latency have to be managed both during and before operation, which can only be achieved by measures such as certification, verification and prioritisation of resources. This requires support from 'central' services, such as user permissions management, user trust management, data distribution, misbehaviour management, network services, service monitoring and time synchronisation.

Based on an assessment of international C-ITS developments, and an assessment of the current local situation, it is proposed that the core functions required to support C-ITS in Australia and New Zealand are the following:

- secure exchange of data between users and applications
- trust in and integrity of data
- assurance of privacy between users and from third parties
- facilitation of a platform for sharing of data and efficient use of resources
- assurance of national interoperability and nationally consistent service access.

These core functions are often part of a physical system, or several physical systems, such as a C-ITS device in a vehicle or in several vehicles, centres, roadside infrastructure and mobile devices.

The core functions are adapted from the functions of the US core system by the Federal Highway Administration (2012) and the features of C-ITS summarised by Schade (2012a) based on the definitions of C-ITS by the standardisation organisations ISO, CEN and ETSI.

The Federal Highway Administration (2012) has summarised the functions for the US core system as follows:

- secure exchange of trusted data between users and applications without pre-existing relationship or entering into a permanent relationship
- assurance of privacy between users and from third parties
- more efficient data collection from various sources and distribution to many users.

Additionally, the features of C-ITS described by Schade (2012a) from the combined definitions from ISO, CEN and ETSI provide core functions for a C-ITS are:

- a common reference architecture
- the sharing of information between C-ITS devices (e.g. in-vehicle, roadside, central and mobile C-ITS equipment), in a peer-to-peer environment
- the sharing of information between multiple applications in a single C-ITS device
- the sharing of resources (communication, positioning, security, etc.) by multiple applications in a single C-ITS device
- the authorised use of information for purposes other than the original intent
- the support of multiple applications running simultaneously.

There is overlap between these two sets of core functions, so a set of core functions for Australia and New Zealand is defined based on these two sources.

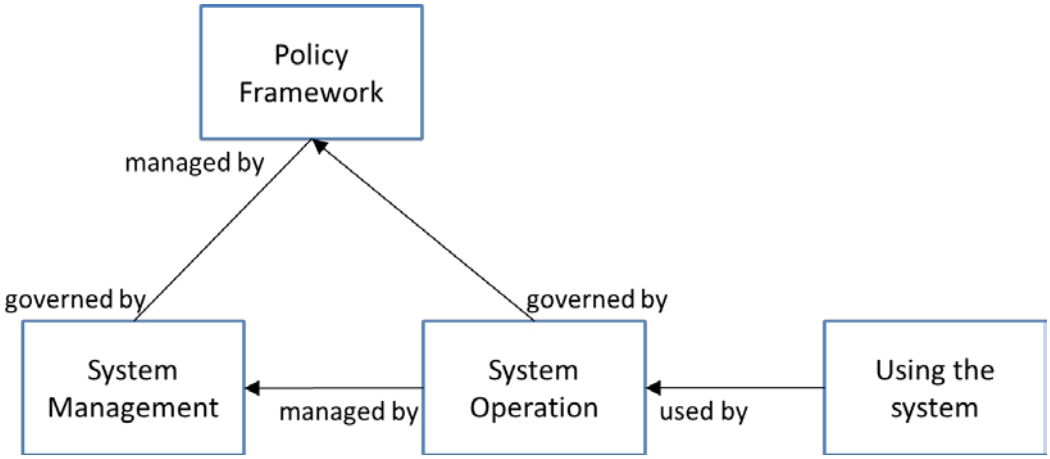
1.3.4 Roles and Stakeholders

This section gives an overview of the main stakeholders and the roles with regard to C-ITS. Further detail on the roles and responsibilities specific to the proposed C-ITS core functions are described in Section 4.5.

Roles

A role is a set of activities or functions that are logically performed together. The ISO standard about roles and responsibilities in the context of cooperative ITS (ISO 17427) identifies four major roles, illustrated using a generic view of the organisational architecture (Figure 1.6).

Figure 1.6: High-level description of organisational architecture



Source: ISO 17427-1.

This categorisation of roles will be used in various sections of the document. The following provides a brief description for each of these roles:

- **Policy framework** – responsible for all governing and institutional activities in the system. This includes governing the system management and system operation roles. Responsibilities within this role include:
  - defining the regulatory and non-regulatory policies relevant to C-ITS
  - defining the standards and guidelines relevant to C-ITS
  - ensuring that standards, guidelines, laws and regulations are followed and applied.
- **System management** – responsible for the management activities within the system. This role is governed by the policy framework role, and provides direct management and support to the system operation role. Responsibilities within this role include:
  - designing, testing and deploying C-ITS
  - managing maintenance and support services for C-ITS
  - managing availability and capacity of C-ITS
  - managing access, security, confidentiality and integrity for C-ITS
  - managing configuration, changes, and updates for C-ITS
  - enabling communications within and between C-ITS devices
  - maintaining the implemented C-ITS architecture.
- **System operation** – responsible for activities related to the operation of the system. This role is supported by the system management role, and provides services directly to the end users. Responsibilities with this role include:
  - provision of content, which could include any type of data
  - provision of services, which include processing content to create the end service
  - presentation of the service results to the end user.

- **End user** – responsible for requesting, receiving and using the end C-ITS application or service, (in some use cases the service may be imposed by the jurisdiction, or perhaps an insurer, or by a third party contracted to provide a service to the recipient. In terms of functionality, however, these are grouped as 'end user' operations). This role has a close relationship with the system operation role. Responsibilities within the role include:
  - issuing a service request, and fulfilling any obligations (e.g. subscription conditions)
  - recognition of service result presentation (which could be visual, audible, etc.)
  - judging the need for reaction, and react accordingly.

These roles are in agreement with those as performed in the operation of telematics applications like the electronic work diary (TCA 2013).

Stakeholders

A stakeholder is a person or an organisation that has an interest in or can impact C-ITS. This document generally refers to stakeholder groups rather than individual stakeholders, even though individual stakeholders can have unique and specific characteristics. Based on the stakeholder consultation (Appendix A, key finding 1.4); the following stakeholder types and sub-types are provided that are relevant in the Australian and New Zealand context:

- users: freight and fleet managers, drivers, travellers, motoring organisations, emergency services, road agencies
- road agencies: state and territory road agencies, local councils
- operators: tolling operators, rail operators
- vehicle manufacturers, original equipment manufacturers (OEMs), dealers, and their representative organisation such as the Federal Chamber of Automotive Industries and the Motor Industry Association, the Truck Industry Council and the Road Transport Forum
- mobile device manufacturers: smartphone manufacturers, personal navigation device manufacturers
- telecommunication operators
- ITS infrastructure manufacturers
- service and content providers: radio stations, app developers, app stores, aftermarket service providers, tolling operators, positioning and mapping industry, car manufacturers, traffic data providers
- standardisation organisations: international and national standardisation organisations
- certification organisations: transport certification organisations, mapping certification organisations, sector specific certification organisations
- regulators: communications and media authorities, industry specific regulators, national competition authorities
- policy makers: Departments of Infrastructure and Regional Development, ministries, policy advisory committees
- other: national and state privacy commissioners, ITS industry representatives.

These stakeholders are expected to play a role in the deployment of C-ITS. It is important to note that stakeholders can perform several roles, and roles can be performed by more than one stakeholder.

2. References

Amsterdam Group 2013, *Roadmap between automotive industry and infrastructure organisations on initial deployment of Cooperative ITS in Europe*, version 1.0, The Netherlands.

Andersen, C & McKeever, B 2011, *V2I for safety: roadmap, accomplishments and constraints*, PowerPoint presentation, US Department of Transportation, Washington, DC, USA, viewed 30 September 2014, <http://www.its.dot.gov/presentations/L_V2I_Safety2011_files/frame.htm>.

Australian Bureau of Statistics 2014, *9309.0: Motor vehicle census, Australia, 31 Jan 2013*, viewed 23 July 2014, <http://www.abs.gov.au/ausstats/abs@.nsf/mf/9309.0>.

Austroads n.d., *Austroads strategic plan 2012-2016*, Austroads, Sydney, NSW.

Austroads 2010, *Defining applicability of international standards for intelligent transport systems (ITS): final report*, AP-R368-10, Austroads, Sydney, NSW.

Austroads 2012, *Cooperative ITS strategic plan*, AP-R413-12, Austroads, Sydney, NSW.

Austroads 2014, *National ITS Architecture: Context and Vision*, AP-R467-14, Austroads, Sydney, NSW.

Austroads 2015, *Cooperative intelligent transport systems (C-ITS) standards assessment*, AP-R474-15, Austroads, Sydney, NSW.

Budapest University of Technology and Economics 2013, *CEN/TC278: PT1604: LDM for C-ITS*, PowerPoint presentation, BME, Budapest, Hungary, viewed 16 December 2014, <http://www.hit.bme.hu/~buttyan/atnc/20130918_Fischer2.pdf>.

Briggs, V 2012, *Connected vehicle implementation and institutional issues,* PowerPoint presentation to the ITS Program Advisory Committee, Ann Arbor, Michigan, USA, viewed 4 September 2014, <http://www.its.dot.gov/itspac/october2012/PDF/Implementation.pdf>.

CALM 2012, *Communications in cooperative intelligent transport systems: CALM for C-ITS,* webpage, CALM, European Union, Brussels, Belgium, viewed 14 September 2014, <http://calm.its-standards.info/>.

COMeSafety 2010, *D31 v3.0 European ITS communication architecture: overall framework: proof of concept implementation,* COMeSafety, Munich, Germany.

Council of the European Union 2010, *Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of intelligent transport systems in the field of road transport and for interfaces with other modes of transport: text with EEA relevance,* official journal L 207, European Parliament, Belgium, Brussels, viewed 16 September 2010, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do? uri=CELEX:32010L0040:EN:HTML>.

CSIRO 2011, *What trust and security really mean*, webpage, CSIRO, Clayton South, Vic, viewed 16 December 2014, <http://www.csiro.au/Outcomes/ICT-and-Services/Security-And-Trust.aspx>.

Dar, K, Bakhouya, M, Gaber, J, Wack, M & Lorenz, P 2010, 'Wireless communication technologies for ITS applications', *IEEE Communications Magazine*, vol. 48, no. 5, pp. 156-62.

Delgrossi, L 2013, *The future of the automobile*, presentation, Stanford University, Stanford, CA, USA, April 2013, < http://web.stanford.edu/class/me302/PreviousTerms/2013-04-01%20VSC%20Lecture%2001.pdf>.

Department of Communications 2014, *Mobile phones*, Department of Communications website, Canberra, ACT, viewed 17 December 2014, < http://www.communications.gov.au/mobile_services/mobile_phones>.

Digital Radio Plus 2013, *Coverage*, webpage, viewed 2 September 2014, <http://www.digitalradioplus.com.au/index.cfm?page_id=1003>.

DRIVE C2X 2013, *Standards*, webpage, viewed 2 September 2014, <http://www.drive-c2x.eu/standards>.

Economic Commission for Europe 2012, W*orld forum for harmonization of vehicle regulations (wp.29): how it works, how to join it*, 3rd edn, UNECE, Geneva, Switzerland.

ERTICO 2011, *How standardisation supports Intelligent Transport Systems, World Standards Day 2011: competitiveness through standardisation*, presentation, ERTICO, Brussels, Belgium.

ETSI 2012, *Intelligent transport systems*, web article, viewed 6 December 2014, ETSI, Sophia-Antipolis, France, <http://www.etsi.org/technologies-clusters/technologies/intelligent-transport>.

EU-US harmonisation task force 2012a, *Overview of harmonisation task groups 1&3*, EU-US ITS Task Force Standards Harmonisation Work Group, document HTG1&3-1, European Commission, Brussels, Belgium.

EU-US Harmonisation Task Force 2012b, *Status of ITS security standards*, EU-US ITS Task Force Standards Harmonisation Work Group, document HTG-1, European Commission, Brussels, Belgium.

European Commission 2013, *Progress and findings in the harmonisation of EU-US security and communications standards in the field of cooperative systems: EU-US Task Force: reports from HTG1 and HTG3*, European Commission, Brussels, Belgium, viewed 17 December 2014, <http://ec.europa.eu/digital-agenda/en/news/progress-and-findings-harmonisation-eu-us-security-and-communications-standards-field>.

European Committee for Standardisation (CEN) & International Organisation for Standardisation (ISO) 2013, *C-ITS Release 1 list of standards: N196*, CEN/ISO, viewed 20 May 2014, <http://release1.its-standards.eu/CEN_ISOrelease1/N196_C-ITS%20Release%201_CEN-ISO%20standards%20list_v2.pdf>.

Federal Highway Administration 2007, *Systems engineering for Intelligent Transportation Systems: an introduction for transportation professionals*, FHWA, Washington, DC, USA, viewed 17 December 2014, <http://www.ops.fhwa.dot.gov/publications/seitsguide/seguide.pdf>.

Federal Highway Administration 2012, *Technical policy analysis: core systems*, Chicago Safety Workshop, FHWA, Washington, DC, USA, viewed 26 September 2014, <http://www.its.dot.gov/presentations/CV_Safety_sept2012/Day2_System_Analysis_files/frame.htm>.

FRAME 2011a, *The FRAME model*, webpage, viewed 8 May 2014, <http://www.frame-online.net/architecture/about-architecture/08-frame-model.html>.

FRAME 2011b, *The FRAME architecture: its contents*, D15 FRAME architecture part 1, version V1.0, viewed 8 May 2013, webpage, <http://www.frame-online.net/sites/default/files/the-architecture/Articles/The%20FRAME%20Architecture%20-%20Contents.pdf>.

FOT-NET 2011, *Category: cooperative systems*, wiki, viewed 1 July 2014, <http://wiki.fot-net.eu/index.php?title=Category:Cooperative_Systems>.

GSMA 2013, *Connected car forecast: global connected car market to grow threefold within five years*, version 1.0, viewed 28 February 2014, <http://www.gsma.com/connectedliving/wp-content/uploads/2013/06/cl_ma_forecast_06_13.pdf>.

Harmonization Task Group 6 2013, *Candidate harmonized policies for cooperative ITS security implementation*, EU-US harmonisation task force, HTG-6 work item description (WID), viewed 10 September 2014, <www.its.dot.gov/connected_vehicle/pdf/HTG6_WorkItemDesc.pdf>.

Honey Access 2014, *Bluetooth range*, webpage, Warsaw, Poland, viewed 16 December 2014, <http://www.bluair.pl/bluetooth-range>.

Intelligent Transportation Systems Joint Program Office 2013, *Request for information connected vehicle: next stage certification environment*, Federal Highway Administration, Washington, DC, USA.

Jesty, PH & Bossom, RAP 2011, 'Using the FRAME architecture for planning integrated intelligent transport systems', *IEEE forum on integrated and sustainable transportation systems*, *June 29 – July 1 2011*, *Vienna*, Institute of Electrical and Electronics Engineers, New York, NY, USA, pp. 370-5.

Kanazawa, F, Tanaka, Y & Tsukiji, T 2013, 'Research on location planning of ITS spots for using probe data in travel speed survey', *ITS world congress, 20th, 2013, Tokyo, Japan,* ITS Japan, 10 pp.

Koichi, S 2013, 'Recent research activities on ITS spot in Japan', *ITS world congress, 20th, 2013, Tokyo, Japan,* ITS Japan.

Lan, L 2013, *ETSI G5 technology: the European approach*, PowerPoint presentation, DRIVE C2X, viewed 13th June 2014, <http://www.drive-c2x.eu/tl_files/publications/3rd%20Test%20Site%20Event%20TSS/1%20DRIVE%20C2X%203rd%20Test%20site%20event_Lan%20Lin_Technology_20130613.pdf>.

Lee, T 2011, 'ACMA to plug gap in wireless spectrum', *The Australian*, 4 May 2011, viewed 17 December 2014, <http://www.theaustralian.com.au/business/push-to-plug-the-gap-in-wireless-spectrum/story-e6frg8zx-1226049450443>.

Ministry of Transport 2014a, *Intelligent Transport Systems trial*, Ministry of Transport, Wellington, New Zealand, viewed 17 December 2014, <http://www.transport.govt.nz/ourwork/intelligenttransportsystems/itstrial/>.

Ministry of Transport 2014b, *Intelligent Transport Systems technology action plan 2014-18*, Ministry of Transport, Wellington, New Zealand, viewed 17 December 2014, <http://www.transport.govt.nz/ourwork/intelligenttransportsystems/itsystems-technology-action-plan/>.

National Highway Traffic Safety Administration 2014a, *Federal motor vehicle safety standards: vehicle-to-vehicle (V2V) communications*, NHTSA, Washington, DC, USA, viewed 20 August, 2014, <http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/V2V-ANPRM_081514.pdf>.

National Highway Traffic Safety Administration 2014b, *Vehicle-to-vehicle communications: readiness of V2V technology for application*, DOT HS 812 014, NHTSA, Washington, DC, USA.

National Transport Commission 2013, *Cooperative Intelligent Transport systems: final policy paper*, NTC, Melbourne, Vic, viewed December 2013, <http://www.ntc.gov.au/Media/Reports/(55AFE902-73F4-073B-E6ED-AE684E3BE595).pdf>.

PRESERVE 2013, *About the project*, web article, viewed 30 January 2014, <http://www.preserve-project.eu/about>.

Research and Innovative Technology Administration 2011, *Core system: concept of operations (ConOps)*, RITA, Washington, DC, USA, viewed 16 November 2014, <http://www.its.dot.gov/docs/CoreSystemConOpsRevE2.pdf>.

Research and Innovative Technology Administration 2012, *National ITS architecture: executive summary*, RITA, Washington, DC, USA, viewed 7 September 2014, <http://www.iteris.com/itsarch/documents/execsum/execsum.pdf>.

Research and Innovative Technology Administration 2013, *Request for information connected vehicle: next stage certification environment*, RITA, Washington, DC, USA, viewed 27 May 2014, <http://www.its.dot.gov/press/2013/connected_vehicle_cert.htm>.

Schade, HJ 2012a, *CEN/TC278 and M/453: progress of C-ITS standards*, webinar, COMeSafety2, viewed 4 September 2014, <http://www.comesafety.org/fileadmin/user_upload/PDFs/Status_C-ITS_at_CEN_TC_278.pdf>.

Schade, HJ 2012b, 'Status report on European Commission standardization mandate M/453', COMeSafety2, Munich, Germany.

Schade, HJ 2013, *What is next in C-ITS standardization in Europe? To offer some ideas from CEN/TC278 and ISO/TC204*, PowerPoint presentation, ETSI workshop, Vienna, 5 February 2013.

Shulman, M 2012, *V2V Communications security project update: ITS Advisory Committee update*, presentation, CAMP Vehicle Safety Communication 3 consortium, viewed 11 October 2014, <http://www.its.dot.gov/itspac/october2012/PDF/V2V%20Security%20Research%20Update%20-%20MShulman%20-Oct%202012.pdf>.

Society of Automotive Engineers 2014, *Information report on candidate improvements to Dedicated Short Range Communications (DSRC) message set dictionary [SAE J2735] using systems engineering methods*, SAE International, Washington, DC, USA.

Sprouffske, S 2013, *V2X Cooperative systems: what is it all about?* ITS America 23rd annual meeting & exposition, 2013, viewed 17 December 2014, <http://itswc.confex.com/itswc/AM2013/webprogram/ExtendedAbstract/Paper11511/20130402_Kapsch_V2X_ITSAPaper_FINAL.pdf>.

Standing Council on Transport and Infrastructure 2012, *Policy framework for intelligent transport systems in Australia*, SCOTI, Canberra, ACT.

Transport Certification Australia 2013, *Final report: operational pilot of electronic work diaries and speed monitoring systems*, prepared for NSW Roads and Maritime Services, TCA, Melbourne, Vic, viewed 17 December 2014, <http://roadsafety.transport.nsw.gov.au/stayingsafe/drivers/heavyvehicledrvers/electronic_work_diaries_oct2013.pdf>.

Transport Certification Australia 2014, *TCA national telematics framework*, Transport Certification Australia, Melbourne, Vic, viewed 21 July 2014, <http://www.tca.gov.au/tca/tca-national-telematics-framework>.

Telstra 2013, *Our coverage: maximise your coverage*, webpage, Telstra, Sydney, NSW, viewed 2 September 2014, <http://www.telstra.com.au/mobile-phones/coverage-networks/our-coverage/>.

Toyota 2013, *Toyota to launch advanced driving support system using automated driving technologies in mid-2010s*, Toyota City, Japan, viewed 11 October 2014, <http://www2.toyota.co.jp/en/news/13/10/1011_1.html>.

Transportation Research Centre 2012, *SAFETYPILOT: what is the Safety Pilot Model Deployment?*, UMTRI, Ann Arbor, MI, USA, viewed 17 December 2014, <http://safetypilot.umtri.umich.edu/>.

Standards

ETSI EN 302 665 V1.1.1 (2010-09), *Intelligent Transport Systems (ITS): communications architecture*.

ETSI TS 102 637-1 V1.1.1 (2010-09), *Intelligent Transport Systems (ITS): vehicular communications: basic set of applications: part 1: functional requirements*.

ETSI TS 102 637-2 V1.2.1 (2011-03), *Intelligent Transport Systems (ITS): vehicular communications: basic set of applications: part 2: specification of cooperative awareness basic service*.

ETSI TS 102 637-3 V1.1.1 (2010-09), *Intelligent Transport Systems (ITS): vehicular communications: basic set of applications: part 3: specifications of decentralized environmental notification basic service*.

IEEE 1362-1998 2007, *IEEE guide for information technology: system definition: concept of operations (ConOps) document*.

IEEE 802.11 2012, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.*

IEEE P1609.0 2013, *Guide for Wireless Access in Vehicular Environments (WAVE): architecture*.

ISO 15638:2012, *Intelligent transport systems -- Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV).*

ISO 21217:2010, *Intelligent transport systems: communications access for land mobiles (CALM): architecture*.

ISO 17427:2013, *Intelligent Transport Systems (ITS): co-operative systems: roles and responsibilities in the context of co-operative ITS based on architecture(s) for co-operative systems*.

ISO/TS 17419:2014, *Intelligent Transport Systems: cooperative systems: classification and management of ITS applications in a global context*.

ISO/TS 17423:2014, *Intelligent Transport Systems: cooperative systems: ITS application requirements and objectives for selection of communication profiles*.

ISO/IEC 27000:2009, *Information technology: security techniques: information security management systems: overview and vocabulary*.

SAE J2735 2014, *Dedicated short range communications (DSRC) message set dictionary*.

3. Current Situation

This section describes the current ITS environment in Australia and New Zealand, and provides an overview of existing ITS and communication services. It also includes a subsection on the ongoing establishment of a regulatory and operational framework for C-ITS. Finally, it includes a subsection on the key international initiatives to enable and establish C-ITS.

3.1 Background

A safe and efficient transport network is essential to a nation's economy and the wellbeing of its people. Across Australia and New Zealand, the combined road network is over 900 000 kilometres (Austroads n.d.), with over 17 million vehicles registered in Australia in 2013 (Australian Bureau of Statistics 2014) and over 3 million vehicles registered in New Zealand (Ministry of Transport 2014b).

ITS encompass the application of information and communications technologies to land transport, which enable efficient and safe use of this asset. ITS include stand-alone infrastructure applications such as traffic management systems, as well as C-ITS. These technologies cover private and public transport by road and rail, as well as cycling and walking, together with applications for cross-modal transport and transport hubs.

While governments and industry may work together to deploy systems to users, the systems developed and implemented in most cases currently do not interact with one another, or where they do, the interaction is limited. For example, governments may use ITS-like traffic signals, ramp metering, or traveller information systems to operate the network and to achieve its objectives. Vehicle manufacturers may use advanced driver assistance systems (ADAS) and other in-vehicle technologies to improve safety and convenience. These systems do not necessarily interact with one another either across classifications (i.e. between governments, industry and users) or within classifications (i.e. between government-run systems or industry built systems). Essentially, for the most part, entities of the road system are not fully connected. This is discussed in further detail in Section 4.1.3.

The current local ITS environment already includes a first generation of C-ITS applications using existing cellular communication and radio broadcast technology. These include traveller information systems, vehicle monitoring systems and, increasingly, local dynamic hazard warnings.

Commercial fleet management systems use cellular communications widely in regions where cellular coverage is available. Feedback from industry is that cellular-based connected applications will become more common over the next 12 to 24 months using both embedded SIM cards in the vehicle and tethering to mobile phones.

Additionally, car manufacturers are currently working with their suppliers towards equipping their new models with the next generation C-ITS technology in the next few years. Twelve automakers have signed a memorandum of understanding to begin including 5.9 GHz Dedicated Short Range Communication (DSRC) C-ITS devices as early as the 2015 model year for the European market (Harmonization Task Group 6 2013; Sprouffske 2013). In the USA, the National Highway Traffic Safety Administration (NHTSA) in August 2014 released an advance notice of proposed rulemaking which commences the process to consult on and draft a proposed regulation requiring V2V equipment in new light vehicles (NHTSA 2014a).

However, the current ITS environment in Australia and New Zealand does not provide mechanisms for registration of C-ITS applications and devices, and secure and private communication between vehicles, roadside ITS and centres (it does provide security and privacy arrangements for mobile devices through telecom operators and mobile device manufacturers, but this does not suffice for all desired transport applications and raises issues of driver distraction). Neither does the current ITS environment adequately support time-critical safety C-ITS applications. These will require a secure and trusted low-latency data exchange that current cellular and broadcast technologies cannot provide. To deploy emerging C-ITS, a platform needs to be put in place that facilitates security, privacy and registration for a range of applications.

3.2 Policies

The *Policy Framework for Intelligent Transport Systems in Australia* was endorsed by Australia's transport ministers at the inaugural Standing Council of Transport and Infrastructure (SCOTI) meeting in November 2011(Standing Council on Transport and Infrastructure 2012). This policy framework provides a robust framework for ITS, and identifies policy principles and foundation actions for guiding the development and implementation of ITS in Australia. It identifies C-ITS as a priority action area and nominates Austroads as the body responsible for developing a national C-ITS strategy.

The Co-operative ITS Strategic Plan (Austroads 2012) sets the direction for the local deployment of C-ITS. It outlines the mission, vision, objectives and guiding principles with respect to the local deployment of a C-ITS platform with a key theme being the need to harmonise with international standards and best practice.

With regard to radio communications, Australia is a signatory to the International Telecommunication Union (ITU) Convention. In line with this agreement, the ACMA gives appropriate consideration to harmonising with the international radio regulations and other international agreements when considering local spectrum allocations and conditions.

With regard to the automotive industry, Australia is a signatory to both the 1958 and the 1998 United Nations Economic Commission for Europe (UNECE) agreements regarding harmonised vehicle regulations. As part of these agreements, Australia is actively involved in and supports the World Forum for Harmonisation of Vehicle Regulations (Working Party 29). In addition to this, the *Motor Vehicle Standards Act 1989* states that Australian Design Rules may be harmonised with UNECE vehicle regulations.

Australia and New Zealand are signatories of the World Trade Organisation's Treaty on Technical Barriers to Trade, which requires the use of relevant international technical regulations where they exist or are imminent.

The majority of technical requirements for C-ITS to be deployed locally will not be unique to Australia or New Zealand. Also, much of the C-ITS hardware, applications and services will either be developed overseas, or at least be developed for an international market. It is therefore critical that the technical requirements for the local C-ITS framework are informed and guided by international developments and, where possible, harmonised with international standards and best practice.

For the above reasons Australia and New Zealand are positioning themselves to be adopters and adapters of C-ITS technology developed internationally, with the principal aim being that any platform deployed locally will be harmonised with an international platform. This is not just for the purpose of complying with international agreements but to maximise the benefits of the technology. Harmonising with an international platform will assist in:

- maximising market penetration: vehicles in Australia and New Zealand come from local and international markets and hence market penetration will be assisted by ensuring that local platforms are harmonised with international platforms
- maximising applications: being part of an international platform with various international investment and resources will assist in establishing a broader set of applications.

There are still open questions regarding possibly crucial constraints, for example whether and how the use of a core system will be incentivised or mandated and for which types of services and applications. For example, the NTC *Cooperative Intelligent Transport Systems: Final Policy Paper* (NTC 2013) flags, amongst others, privacy and liability issues. These and other policy issues that will directly affect the system architecture are reflected in assumptions or constraints as described in Section 4.5.

3.3 Description of the Current Situation

This section presents an overview of the current ITS environment in Australia and New Zealand, and the currently emerging C-ITS platforms internationally. It describes how the equivalents of C-ITS core functions are achieved today and addresses:

- ITS in Australia and New Zealand
- national ITS architecture for Australia and New Zealand
- telematics services
- international C-ITS developments.

3.3.1 ITS in Australia and New Zealand

There is a wide range of ITS currently operating in Australia and New Zealand. Road operators have a large number of existing ITS assets including traffic signal management systems, vehicle detection systems, dynamic traffic information systems and traffic management centres. Private service providers are also increasingly deploying ITS, particularly traveller information systems and telematics services. Table 3.1 shows a the ITS currently implemented in Australia and New Zealand that span across the nine functional groups as defined by FRAME (2011b) with some examples outlined.

Table 3.1: Currently implemented ITS

FRAME functional groups	Currently implemented ITS	Stakeholder responsible
Provide electronic payment facilities	Free-flow tolling equipment (based on 5.8 GHz DSRC)	Toll operator
Provide safety and emergency facilities	Vehicle activated signs (including speed activated signs)	Road operator
	Pedestrian detection (e.g. puffin crossing)	Road operator
	Ice detection and warning stations	Road operator
	Emergency vehicle signal pre-emption systems interfaced with the traffic signal controller	Road operator
	Railway level crossing warning	Service provider
Manage traffic	Traffic signals and traffic signal controllers (including SCATS/STEAMS regional computers)	Road operator
	Ramp metering (coordinated, e.g. based on HERO)	Road operator
	Traffic sensing loops, traffic counting loops and data station	Road operator
	Bluetooth travel time	Road operator
	CCTV camera equipment	Road operator
	Video incident detection cameras	Road operator
	Electronic speed limit signs (including variable speed limits, school zones and weather-based speed limits)	Road operator
	Overhead lane controls (including tidal flows)	Road operator
	Moveable medians	Road operator
	In-pavement lights	Road operator
	Signalised railway crossings	Train operator
Manage public transport operations	Real-time bus monitoring	Bus operator
	Real-time bus priority including public transport signal priority systems interfaced with the traffic signal controller	Road operator
	Bus-lane cameras	Road operator
	Smart-bus signs	Road operator

FRAME functional groups	Currently implemented ITS	Stakeholder responsible
Provide advanced driving assistance systems	Intelligent speed assist	Car owner
	Forward collision warning with brake support	Car owner
	Lane departure warning	Car owner
	Blind spot assist	Car owner
	Active park assist	Car owner
	Reverse assist	Car owner
Provide traveller journey assistance	Electronic signs (i.e. variable message, changeable message and electronic information)	Road operator
	The provision of routing and congestion information via cellular communication and RDS-TMC into in-vehicle and mobile devices	Service provider
	The provision of routing and congestion information via web-portal	Service provider
Provide support for law enforcement	Red light cameras	Road operator
	Speed cameras	Road operator
Manage freight and fleet operations	Height gauges	Road operator
	Weigh-in-motion	Road operator
	Truck noise cameras – enforcement of noise emissions from trucks	Road operator
	Intelligent Access Program	Transport Certification Australia
	Private fleet management systems	Business user
Support for cooperative systems	No current systems	No current systems

In addition, an increasing number of vehicles are being equipped with an advanced driver assistance system (ADAS). These systems predominantly use sensors that are part of the vehicle and do not require communication to systems external to the vehicle. The systems provide advice to drivers based on inputs received from sensors like cameras and/or radar technology. C-ITS will provide another input into the vehicle's ADAS by being connected to systems operated by other vehicles and with ITS operated by road agencies.

While the greater majority of vehicles on Australian and New Zealand roads do not have system that connect with field infrastructure or centres, the proportion of vehicles with such wireless connections continues to increase. This includes in-vehicle telematics applications as listed above, such as the intelligent access program (IAP), routing and congestion traveller information, electronic toll collection and private fleet management systems. These in-vehicle telematics applications enable information exchange between vehicles and infrastructure.

The implementation of ITS has generally been undertaken on an 'as required' basis resulting in many proprietary based systems that are not interoperable with one another. Initiatives such as the national ITS architecture would enable ITS to be deployed across both Australia and New Zealand in nationally consistent and interoperable ways for the benefit of ITS users and suppliers.

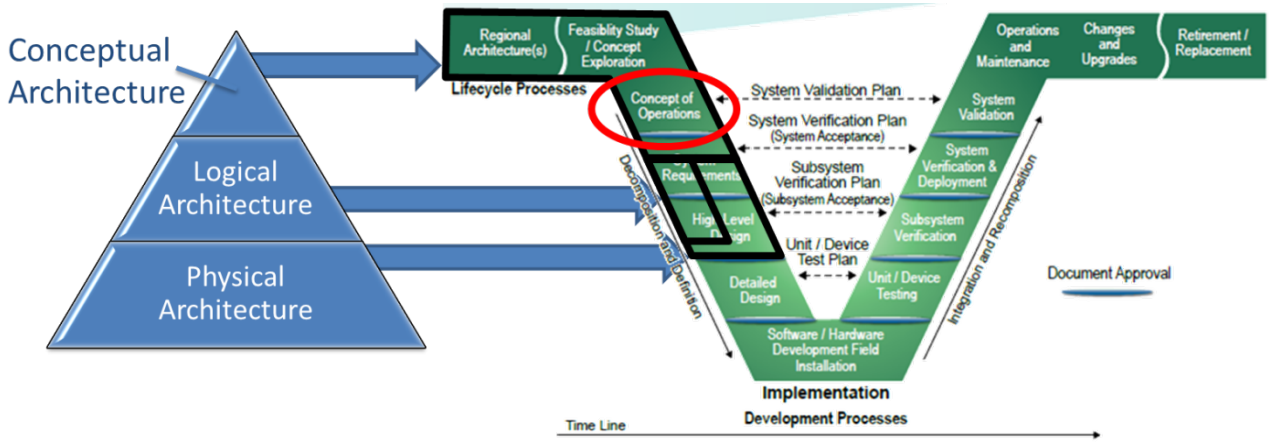
3.3.2 National ITS Architecture for Australia and New Zealand

An ITS architecture is the conceptual design that defines the structure and/or behaviour of an integrated ITS. An ITS architecture helps to ensure that the ITS deployments can be planned in a logical manner, integrate successfully with other systems, meet the desired performance levels and have the desired behaviour (FRAME 2011).

As shown in Figure 1.1, architecture is used as an input to the system engineering design process. Austroads, through project NS1696 – *National ITS Architecture*, is currently progressing the development of the conceptual architecture[4]. Currently C-ITS functions and applications are included in the draft logical architecture to a limited extent, which is similar to the FRAME architecture on which it is based. Figure 3.1 shows the relation between an ITS architecture and a Concept of Operations. A conceptual architecture is an input to a Concept of Operations.

Because the conceptual ITS architecture for Australia and New Zealand was still work in progress at the time of writing, and because it is based on the FRAME reference architecture, the FRAME reference architecture has been used as an input to this document. Assumptions have been made based on the Austroads ITS strategic plan, where needed. Assumptions and constraints are described in Section 4.5.

Figure 3.1: C-ITS core Concept of Operations in relation to ITS architecture



Source: Modified from Austroads (2014).

New Zealand is currently developing a local consensus on ITS. This includes a draft strategic framework for ITS, which the Transport Agency has been progressing. This work will confirm ITS benefits and highlight issues that might be particular to New Zealand conditions and requirements. Where possible, New Zealand aims to align with approaches set by Austroads and this includes the probable adoption of a common reference architecture such as FRAME, but this will be confirmed at a later time.

Currently C-ITS functions and applications are included in the draft logical architecture to a limited extent. C-ITS are likely to become a substantial part of ITS. It is recommended that C-ITS functions are integrated into ITS architectures.

[4] At the time of writing, the Austroads National ITS Architecture project NS1696 was developing an ITS business architecture.

3.3.3 Vehicle Telematics Services

The term *telematics* has different meanings in different contexts, and there are various definitions of the term. Some definitions are very similar to that for C-ITS, while others are more specific to the services involving road vehicles only. Drawing on the *Telematics Applications for Regulated Commercial Freight Vehicles* (TARV) standards (ISO 15638), telematics could be defined as *an in-vehicle device that forms part of a system that captures and sends information electronically*. As such, it could be considered a subset of C-ITS with a focus on services provided to and from vehicles.

A range of telematics services are currently provided to users by commercial service providers, for both private and commercial end users. These are sometimes referred to as vehicle-to-business (V2B) services and currently do not involve vehicle-to-vehicle or vehicle-to-infrastructure (roadside unit) services.

Traveller information services are available in Australia and New Zealand, primarily broadcast on analogue FM radio using the RDS-TMC protocol. Industry feedback suggests more value-added services may also be broadcast over digital radio using the TPEG protocol in the future. In addition to these, vehicles and road users are becoming increasing connected through the use of cellular communications, and this will enable an increase in traveller information and other commercial telematics offerings.

User based insurance is also emerging as a telematics service, where data captured by vehicles will be transmitted to insurance companies and used to determine risk factors and subsequent insurance premiums for vehicle owners. User based insurance has taken off in some international markets, but is yet to become a mainstream product offering locally.

A number of regulated telematics applications and services are also provided by service providers. These include the i*ntelligent access program* for monitoring compliance with heavy vehicle road access permits, and *intelligent speed compliance* for monitoring compliance with regulated speed zones. Transport Certification Australia (TCA) administers these services, including the service-level agreements with the providers of these services to the end users. TCA manages these telematics services in line with the policy framework for ITS in Australia and with its TCA national telematics framework.

With the exception of the traveller information services that are broadcast using one-way communications (e.g. analogue radio broadcast), essentially all other telematics services that are currently provided require the user to opt in to the service. This means the user has entered into an agreement to receive the service, whether it is paid for or not. By opting in, the user is often consenting for some of the data captured by the vehicle to be used by the service provider for a variety of services.

There are equivalents of C-ITS core functions in today's telematics services. The regulated telematics applications run in a context (on a platform) that has many of the C-ITS core functions in place. The other telematics applications have no mechanism to ensure the core functions are in place, so it is up to the service provider whether and how the core functions are included.

For the current regulated telematics applications the equivalent of the core functions are as follows:

- Secure exchange of trusted data between users and applications is realised through a public key infrastructure based security system. The requirements are specified by TCA and systems are certified by TCA.
- Assurance of privacy between users and from third parties is ensured by enabling the service providers to anonymise data and provide aggregated anonymised data to governments for legal enforcement based on requirements defined and audited by TCA.
- A platform for sharing of data and efficient use of resources is created by allowing service providers to offer other commercial applications on the same devices used for the applications providing regulatory information on, for example, legal speed limits.
- National interoperability is ensured for the provision of regulatory information to governments. National interoperability and nationally consistent service access are in practice provided by service providers.

3.3.4 Wireless Communication Technologies

The emerging cooperative intelligent transport environment will involve a range of communications technologies. GSM/UMTS (cellular 2G and 3G) is widely deployed across the more populated areas of Australia and New Zealand, with the rollout of LTE (4G) proceeding apace. However, in rural areas network coverage can be patchy, and in the outback the only communications options in many places are satellite communications or short wave radio. In addition to existing communication technologies, digital short range communication (DSRC) is a new technology that has been developed specifically for communication between vehicles.

Table 3.2 shows five categories of communication technologies and some of their attributes. These are detailed further in the following sections.

Table 3.2: Communication technologies and attributes

Category	Communication technologies	Range	Attributes
Short range communications –very low latency	Examples include: • 5.9 GHz DSRC • Infra-red	• 250 – 1000 metres • Up to 100 metres	• Very low latency • Two-way communications
Short range communications – low latency	Examples include: • Wireless LAN (e.g. WiFi) • Bluetooth • Mobile wireless broadband	• Up to 100 metres • Up to 30 metres • Up to 1000 metres	• Short range • Low latency • Two-way communications
Long range communications (up to around 35 km) – medium latency	Examples include: • Cellular networks, including • UMTS (3G) • LTE (4G)	Apparent ‘seamless’ connectivity across cells	• Long range-seamless across cell network coverage • Medium latency • Two-way communications
Very long range communications – medium to high latency	• Satellite telephony • Satellite broadcasting	Can communicate in areas not covered by land-based networks	• Very long range • Access areas not available to land-based networks
Wide area broadcast	Examples include: • Digital radio (e.g. DAB+) • Analogue radio	Communication distance varies greatly and depends on many factors including noise and sending power	• Long range • Large latency • One-way communications

Short range communication

Examples of short range communication technologies include dedicated short range communications (DSRC) and wireless LAN. Short range communication technologies will generally communicate over distances of up to 250–1000 metres, dependant on topology and atmospheric conditions. Bluetooth offers a range of up to 100 metres (Honey Access 2014).

DSRC is short- to medium-range wireless communication technology specifically designed for automotive use. It can be used for one-way and two-way communication. Currently, DSRC is used for electronic toll collection in the 5.8 GHz band. Globally DSRC-based C-ITS have been developed and tested extensively in pilots and early deployments, mainly in the 5.9 GHz band. It has the benefits of having low latency, high mobility and, currently, no communication connection charges. Limitations are that data communication rates are typically lower than via 3G or 4G LTE and that DSRC units have not yet been deployed so there is no network coverage. There was currently an embargo on the 5.9 GHz frequency band in Australia. However it should be noted that, at the time of writing, there is international lobbying in USA and Europe to open up the 5.9 GHz band, including those frequencies currently reserved for automotive safety applications, for general wireless broadband use.

Bluetooth technology is the global wireless standard for the exchange of data over short distances using radio transmissions in the 2.4 to 2.485 GHz band. Bluetooth is available in many of the current mobile devices like smartphones or car kits. The communication range varies by Bluetooth specification, but typically the effective range varies from a few metres to about 30 metres (Honey Access 2014). Bluetooth is used by some road agencies for traffic monitoring. In Brisbane it is currently used as permanent traffic monitoring equipment. In New Zealand several Bluetooth systems are operational, both temporary and permanent, for example the *Intelligent transport systems trial* (Ministry of Transport 2014a).

A wireless local area network (WLAN) links two or more devices using some wireless distribution methods, and generally provides a connection to the Internet. This allows users to move around within a local coverage area and still be connected to the network and Internet. Many modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.

The range of a WLAN 802.11 network depends on the number of routers but is generally linked to a building and its direct surroundings. Wireless 802.11 LANs are not suitable for ‘fast’ moving C-ITS devices, but they could be used for exchange of data in stationary situations; for example, the download of security certificates or for services at service stations like exchanging information about the type of vehicle to determine the required tyre pressure.

Long range communication

For the purpose of this document, long range communications are considered to include those media that enable two-way, unique communication connections over many kilometres. Current long range communication technologies include cellular network and satellite communication.

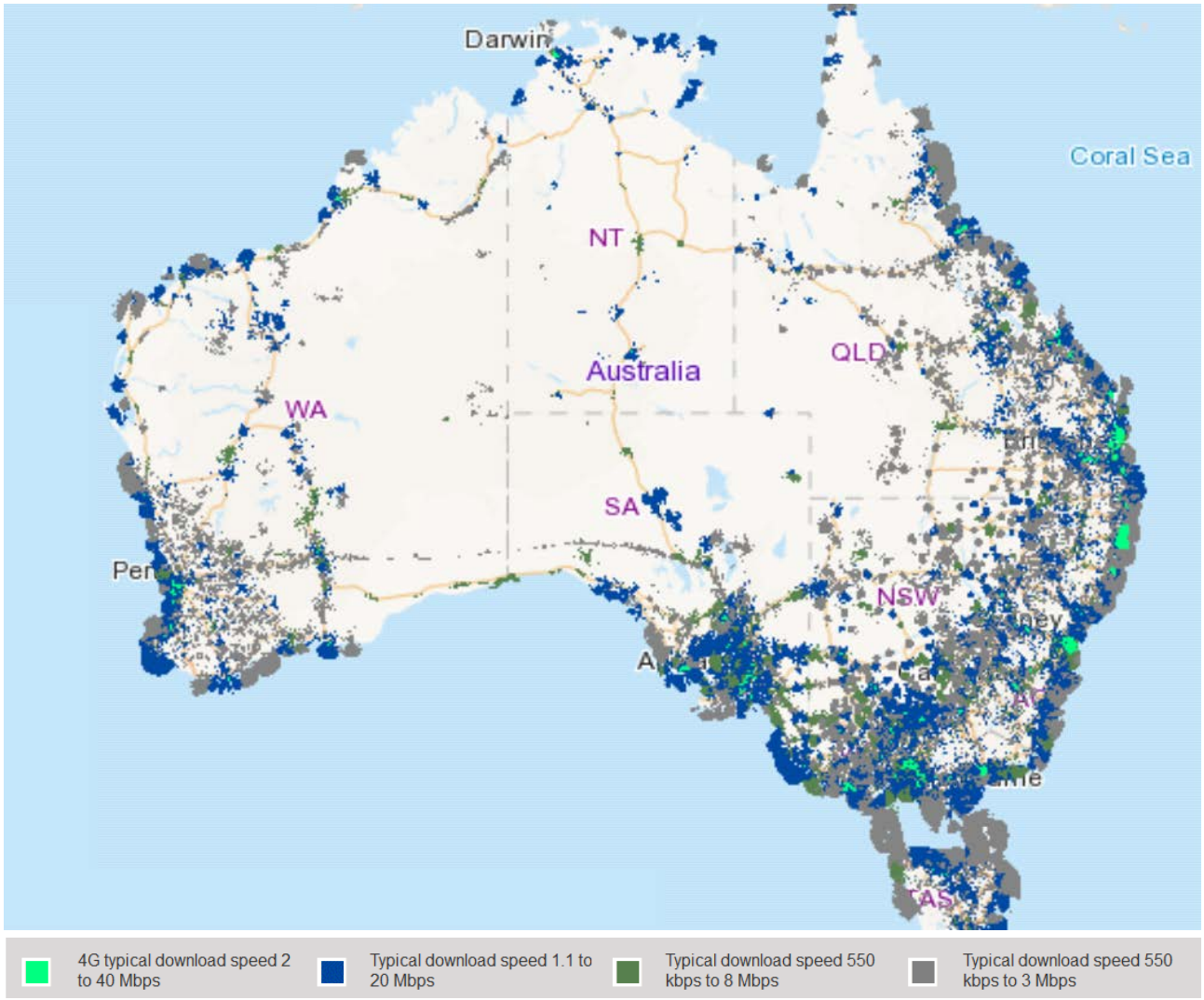
Cellular communications networks offer apparent ‘seamless’ communication sessions across the cells of the network. Mobile phone services based on cellular communication are available in urban areas, many regional areas and along a number of national and regional highways. They use parts of the spectrum between 700 MHz to 2500 MHz (Lee 2011). Mobile phone services currently reach 99% of the Australian population where people live. However, coverage is only available to around 25% of the Australian landmass (Department of Communications 2014). This is similar to New Zealand. Figure 3.2 shows an example of the coverage of one of the cellular communication providers, where the different colours indicate the different download speeds.

Cellular communication technologies like UMTS/3G, LTE/4G and WiMAX/4G have the advantage of providing high bandwidth, wide coverage and high mobility. Disadvantages of UMTS/3G are the relatively high latency, and the required communication costs. LTE/4G has a much lower latency, and is comparable to that of DSRC (Delgrossi 2013). It is as yet unclear to what extent time-critical safety applications can use LTE. From a deployment point of view, it is an advantage that cellular communication infrastructure already has significant coverage, and offers cell-to-cell transfer of ongoing communication sessions.

The connectivity of cars is expected to grow rapidly over the next few years. Vehicles can be connected to cellular communication networks via systems embedded in the vehicle, via smartphones or via tethering. Tethered systems use applications embedded into the car, but use the owner's mobile phone for connectivity. GSMA's Connected Car Forum is an example of a platform of automakers and mobile operators launching joint cross-industry activities to accelerate the development and take-up of telematics and infotainment services. Connected Car Forum global sales target figures for new vehicles include (GSMA 2013):

- over 20% of global vehicle sales in 2015 to include embedded connectivity solutions
- over 50% of global vehicles sales in 2015 to be connected (either by embedded tethered or smartphone integration).

Figure 3.2: Cellular coverage of Telstra 3G and 4G communication networks



Source: Telstra (2013).

Satellite communications is conducted via a satellite sent to space for the purpose of telecommunications. Satellite communications could be used in remote areas, for example using digital radio technology. Satellite communications can be used to broadcast data to equipped vehicles. As with cellular communication, using satellite communication requires a subscription with a provider. An example of the current use of satellite communications is an implementation of an intelligent access program application using satellite communication to cover areas where no cellular coverage is available. While vehicle manufacturers are progressively introducing cellular communication into vehicles, this is not the case for satellite communication.

It must be noted that not all satellite communications telephony options offer 24/7 coverage, and depend on the number and orbit of available satellites. Geostationary orbit-based systems offer coverage.

Wide area broadcast

For the purpose of this report, wide area broadcast is considered to include one-way communication that involves messages to be broadcast over areas of many kilometres.

RDS-TMC is widely used to broadcast traffic information messages on conventional FM radio broadcasts. Traffic message channel (TMC) is a technology for delivering traffic and travel information to motor vehicle drivers. It is digitally coded, using the Radio data system (RDS).

Currently digital radio is being rolled out in Australia using the DAB+ standard. As a broadcast technology it can be used for one-way communication. Digital radio is now available in the five capital cities of Sydney, Melbourne, Brisbane, Adelaide and Perth. Trial broadcast services are currently available in Canberra and Darwin (Digital Radio Plus 2013). In Australia digital radio is currently not used for broadcasting traffic or traveller information.

3.3.5 Positioning Services

Global navigation satellite services (GNSS) refers to constellations of satellites that broadcast positioning, navigation and timing data that receivers on earth can receive and use for various applications. GNSS is offered by satellite navigation systems of USA (GPS), Russia (GLONASS) and China (COMPASS). In addition Europe is in the process of rolling out its high-precision GALILEO system (expected to be fully operational around 2020) and Japan is progressing its regional system called QZSS (expected to be operational in 2018). The primary positioning service used for transport applications across Australia and New Zealand is the US GPS.

A standalone GPS receiver typically achieves a spatial accuracy of 10–20 metres. Increasingly, there is a trend towards using a multi-GNSS approach where other GNSS constellations (e.g. the Russian GLONASS) are used to supplement GPS. This approach can improve spatial accuracy and integrity, and has been demonstrated to achieve a spatial accuracy in the range 5–10 metres.

However, many safety-critical C-ITS applications emerging internationally require a spatial accuracy of less than 1 metre, and also require high integrity, availability and timeliness. Standalone GNSS and multi-GNSS receivers cannot repeatedly achieve this, although multi-GNSS including GALILEO may come close to these accuracies.

International C-ITS developments are using wide-area augmented GNSS, where the positioning signals from a satellite constellation are augmented with correction signals, which are transmitted from satellites and/or ground stations. This is further supplemented by relative positioning measurements from on-board vehicle sensors to achieve the stringent positioning requirements. Safety-critical systems are most likely to use multiple technologies in order to improve system robustness and reliability.

Australia and New Zealand do not currently have access to an augmented GNSS. Geoscience Australia is working with key stakeholders to develop a national positioning infrastructure plan for Australia, which is intended to provide strategic guidance in this area. However, at the time of writing, the plan had not been released.

3.3.6 International Developments

This section discusses the current international C-ITS environment and developments. The equipment and applications for the Australian cooperative intelligent transport ecosystem are currently being developed for a global market. These components are part of emerging C-ITS platforms primarily in the United States, Europe and Japan. They are being developed in trials like DRIVE C2X (2013), model deployments like the Safety Pilot (Transportation Research Centre 2012) and deployments like the ITS Spot program (Koichi 2013) and the Corridor Initiative (Amsterdam Group 2013). In parallel, several international standardisation organisations are developing partly harmonised sets of standards for C-ITS. The limited size of the Australian market for C-ITS equipment justifies minimal customisation, if any, for the Australian market. From an interoperability and efficiency perspective, one of the Australian policy principles is to adopt and adapt international standards and best practices as much as possible.

International C-ITS developments by region

Over the past five to ten years, significant advancements have been made internationally in the development of C-ITS, especially in Europe, the USA, Japan and South Korea. C-ITS using cellular and radio broadcasts are already deployed and used for V2I/I2V. Significant effort has also been invested in developing C-ITS using low latency communication technologies for time-critical safety V2V and V2I/I2V applications. C-ITS developments in different regions are discussed below.

Europe

Europe has been undertaking a large and focused effort in C-ITS since around 2006. In 2010, the European Commission prepared the ITS Action Plan and Directive 2010/40/EU (Council of the European Union 2010) that encompasses C-ITS and has also defined a timeframe under the European Commission Mandate M/453 to develop a set of standards, specifications and guidelines to support European community-wide implementation and deployment of C-ITS.

The C-ITS effort in Europe has been largely delivered through a variety of projects funded by individual European countries, European vehicle manufacturers, the European Commission and other relevant organisations interested in C-ITS. Examples of large joint public-private research projects in the European Union's research programs are CVIS, SAFESPOT, Coopers, SIMTD, TeleFOT, Cooperative Cruise Control, PRE-DRIVE C2X, and currently DRIVE C2X and SCOREF (FOT-NET 2011).

The technology used in the DRIVE C2X pilot project is largely based on European standards developed by ETSI. DRIVE C2X verifies the feasibility of implementing the standards in a multi-vendor environment. Additionally, the project supports standardisation activities by participating in standardisation meetings (e.g. working groups, technical committees and workshops) and making active contributions to standardisation documents (DRIVE C2X 2013).

Recently, some of the vehicle OEMs industry and some road authorities have developed a joint C-ITS roadmap, aiming for deployment of basic safety warning services in 2015 and committing to the deployment of C-ITS equipped vehicles and roadside infrastructure (Amsterdam Group 2013).

The CEN *Technical Committee for Intelligent Transport Systems* (CEN TC278) has merged its work (WG16) with that of ISO TC204 (WG18) to provide coordinated standards for C-ITS. In communications terms these are closely aligned with IEEE802.11/IEEE1609.

Although there is a level of cooperation between ISO/CEN and ETSI, and although there are many common C-ITS standards, there are significant technical differences between the communications and data approaches for C-ITS.

USA

The US developments are largely government driven. The US Department of Transportation is working towards the deployment of C-ITS vehicles between 2016 and 2020. The National Highway Traffic Safety Administration (NHTSA) in August 2014 released an advance notice of proposed rulemaking (ANPRM) which commences the process to consult on and draft a proposed regulation requiring V2V equipment in new light vehicles (NHTSA 2014a). This has been supported by a research report on vehicle-to-vehicle (V2V) communications technology which includes the analysis of research findings in several key areas including technical feasibility, privacy and security, and preliminary estimates on costs and safety benefits (NHTSA 2014b).

A large-scale safety pilot involving approximately 3000 vehicles was recently undertaken as a major input to the decision as to mandate C-ITS applications, mainly in light vehicles.

The US Federal Government through the Intelligent Transport Systems (ITS), Joint Program Office of the US Department of Transportation, Research and Innovation Technology Administration (RITA) (Research and Innovation Technology Administration 2012) has been working on C-ITS in collaboration with the vehicle manufacturers and other key industry players and organisations, as well as state and local road authorities for some time prior to 2011. In 2003, the US Department of Transportation (US DOT) launched the program currently known as the Connected Vehicle program (formerly Intellidrive and prior to that known as the Vehicle Infrastructure Integration (VII) Program) to define and undertake tasks to implement the full suite of applications that comprise the program.

A *Core System: Concept of Operations* was developed by RITA (Research and Innovation Technology Administration 2011). The security aspects have been developed further by a consortium of car manufacturers since then in the Crash Avoidance Metrics Partnership (CAMP) (Shulman 2012).

US standardisation organisations have released standards frequently used in C-ITS, for example the Institute of Electrical and Electronics Engineers (IEEE) has developed the IEEE 802.11 standard for DSRC and the IEEE 1609 WAVE (Wireless Access in Vehicular Environments) series of communication standards. The Society of Automotive Engineers (SAE) has developed the SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary. These standards were used in the US safety pilot deployment.

Japan

Japan has begun deploying C-ITS safety systems across its network. Evidence of this is through the deployment of the SmartWay project using 5.8 GHz DSRC, which commenced in 2007. The SmartWay project is a cooperative vehicle-highway system primarily using V2I technology (or vehicle to road (V2R) as referred to in Japan) to communicate a situation to a vehicle using an ITS roadside device. Applications as part of the SmartWay project include back-of-queue warning, curve-speed warnings, information to assist vehicles in carrying out merging on an expressway, and traffic condition information.

Japan also has a Driving Safety Support System (DSSS) deployment delivering safety initiatives to urban roads via I2V. Applications as part of the DSSS include stop-sign support, merge assist, red-light violation avoidance, and right-turn assistance. Over 1600 ITS Spot roadside units are deployed across Japan and ITS Spot services are currently operational (Kanazawa et al. 2013). ITS Spot has been deployed since 2011 and now has many tens of thousands of vehicles equipped, both new and with aftermarket devices.

In Japan, both the 5.8 GHz and 700 MHz frequency bands will be used for C-ITS. Toyota (2013) announced cooperative-adaptive cruise control using 700-MHz band vehicle-to-vehicle ITS communications to transmit acceleration and deceleration data of preceding vehicles so that following vehicles can adjust their speeds accordingly.

South Korea

Considerable work and development has also been undertaken in South Korea with the development of the concept of the Green Intelli Travel Society (G-ITS) model. The G-ITS model somewhat mirrors other C-ITS international business directions. However, it has a strong focus on the need to maintain multimodal connectivity and identifies the use of the personal (wireless) devices as being the key to the future. The model sees the public and private sectors playing significant roles in providing benefits and services to the users.

Emerging platforms compared

Throughout the world, different C-ITS platforms are currently being developed to facilitate C-ITS applications. A platform is a group of technologies that are used as a base upon which other applications, processes or technologies are developed. Examples of platforms are a Windows operating system as a platform for personal computing software, or an iPhone and iOS mobile operating system as a platform for apps. Internationally emerging C-ITS platforms have differences and similarities. On a conceptual level, platforms have strong similarities. The detailed design and implementation have differences.

The platforms in the USA and Europe are described as relevant examples for the Australian and New Zealand C-ITS developments. This is partly because these regions have allocated the 5.9 GHz band for C-ITS, whereas Japan has not. It is also because Australia's Design Rules for new vehicles are largely harmonised with European UNECE regulations (and to a lesser degree the US FMVSS). However, an issue for New Zealand is that it currently allows the import of a large volume of used cars that meet vehicle regulations other than just the UNECE regulations, including vehicles that meet the Japanese specifications. This will need to be considered when establishing the New Zealand C-ITS platform.

The description of the two most relevant platforms is an interpretation of complex systems that are currently still being developed and concepts are still changing. Even more so, the emerging European platform could be considered a set of emerging national platforms that might be different for different countries. However, to support the discussion on the core functions for Australia and New Zealand, Table 3.3 compares some typical aspects of the emerging US and European platforms.

Table 3.3: Emerging platforms from the United States and the Europe

	United States	European
Paradigm	• Planned deployment, government driven platform (core system) • National Highway Traffic and Safety Administration (NHTSA) released an advance notice of proposed rulemaking (ANPRM) in August 2014 which commences the process to consult on and draft a proposed regulation requiring V2V equipment in new light vehicles (NHTSA 2014a)	• Organic deployment based on standards • Led by 'front runner' countries and industry • Common industry and government deployment roadmap (Amsterdam Group) • Initial deployment of day-one apps announced for 2015 by Amsterdam Group partners
Focus	• Focus on time-critical safety applications • C-ITS core (security, privacy assurance and data collection and distribution functions)	• All applications • Day-one applications: simple 'basic warning services'
Architecture	• Based on OSI • Limited to 5.9 GHz DSRC	• Based on OSI and ITS-station Reference Architecture (ISO 21217)
Communication media	• Currently focused on 5.9 GHz DSRC • Applications other than time-critical safety applications can use other media	• Communication technology agnostic platform (CALM), including 5.9 GHz DSRC, UMTS and LTE

	United States	European
Security and privacy	• Public key infrastructure for 5.9 GHz communication • Include misbehaviour management and certificate revocation • As proposed by CAMP	• Public key infrastructure • Include misbehaviour management and certificate revocation • Details to be confirmed
System management/certification	• Currently under development • Vehicle standards typically through self-certification • Integration of time-critical safety applications and other applications not clear	• Currently under development • Vehicle standards typically through type approval certification • Possibly following proposed global certification in CEN/ISO TS 17419. Certification on platform and on application level
Standards	• Primarily based on IEEE and SAE standards • Limited number of standards	• Primarily based on ETSI and CEN/ ISO. Some standards are based on the IEEE standards (e.g. IEEE 802.11) • Large number of standards

The paradigms are different in the sense that the USA uses a government-led Systems Engineering approach to develop a C-ITS core system for time-critical safety applications, using 5.9 GHz DSRC. The European paradigm is a more organic public-private cooperation, with a number of public-private initiatives, such as the *Cooperative ITS Corridor* project and the *Amsterdam Group*. Formal cohesion is the referencing of regulations and research and development projects to the European Union's ITS Directive (directive 2010/40/EU). There is not yet any planned mandated introduction, as is being envisaged in the USA.

However, most concepts used in these emerging C-ITS platform are similar. Both acknowledge the concept of an ITS-station, separating the platform functions from the applications. Both platforms allow for the use of different communication technologies, although the US core system and the US platform remain focussed on 5.9 GHz DSRC communication and time-critical safety applications, and an impending requirement for cars to support 5.9 GHz DSRC communications. At the present time, in Europe, apart from the *Cooperative ITS Corridor* project, in terms of core system support, it is being left to individual states, and apart from the *Cooperative ITS Corridor* project, is still in the R&D phase. There are, as yet, no advanced plans to require 5.9 GHz DSRC support in vehicles in Europe.

But both platforms propose to use a security credential management system based on public key infrastructure and separation of authorities. In the USA, car manufacturers have specified the security system in the proposal by the CAMP consortium; whereas Europe relies on standards using the same concept of a security credential management system. These standards however do not yet cover all aspects yet and need to be completed and consolidated.

System management for the US core system is envisaged to be performed by state road authorities for operational management, and certification is proposed on a system level (Research and Innovative Technology Administration 2013). System management of the European platform has yet to be determined. System management might be performed through global certification processes as suggested in a draft CEN/ISO standard (ISO TS 17419).

Emerging platforms will have different detailed designs and implementations. This means that C-ITS devices developed for one platform will not be interoperable with C-ITS devices developed for another platform, unless a device is developed to be interoperable with several platforms.

A review of C-ITS standards is out of scope for this Concept of Operations but can be found in the Austroads report titled *Assessment of International C-ITS Standards* currently being written as part of the Austroads project *NS1785 – Cooperative ITS Project (Stage 2c).*

Emerging C-ITS message formats

C-ITS message formats are developed as part of the C-ITS developments described above. These data message types will be specified in international C-ITS message set standards. At the time of writing there was still debate regarding the exact content of such messages. However, the primary message types are likely to include the following, or some internationally agreed variant thereof:

- BSM: basic safety message

  One of the messages outlined in the SAE J2735 standard. The BSM message is used to communicate safety messages from vehicles to vehicles and infrastructure (i.e. V2V and V2I), and from infrastructure to vehicles (I2V). BSM is the SAE equivalent of the CAM and DENM message. The EU-US harmonisation task force has demonstrated a level of harmonisation between the BSM and the CAM and DENM message sets.

- CAM: cooperative awareness message

  The CAM message is a periodically transmitted message containing transient data on the vehicle status. The CAM message is designed primarily for communication from vehicles to vehicles and infrastructure (i.e. V2V and V2I), but may also be sent from infrastructure to vehicles (I2V). The CAM message is defined by the ETSI standard TS 102 637-2.

- DENM: decentralised environmental notification message

  A DENM messages is an event-triggered message which is generated upon detecting an event and contains information about the event. DENM messages are typically relevant for a defined geographic area. The DENM is sent from vehicles to vehicles (V2V), vehicles to infrastructure (V2I), and from infrastructure to vehicles (I2V). DENM is defined by the ETSI standard TS 102 637-3.

- RSA: roadside alert message

  One of the messages outlined in the SAE J2735 standard. The RSA message is used to communicate traveller information applications from roadside infrastructure.

- PVM: probe vehicle message

  One of the messages outlined in the SAE J2735 standard. The PVM message is used to communicate probe information obtained from the vehicle to roadside infrastructure.

- PVD: probe vehicle data

  PVD is used to communicate the status of a vehicle to the roadside ITS-station to allow the collection of information about vehicle movements along a segment of road.

- PDM: probe data management

  PDM is used to control the type of data collected and sent by the vehicle to the roadside ITS-station. PDM is sent from the roadside ITS-station to the vehicle.

- Map: geometric intersection description

  A message containing geometric details of the road such that the vehicle can cross-reference information contained in other messages sent from the roadside ITS-station against the map message to determine how to apply the message (i.e. determine if the message applies to the lane the vehicle is currently in).

- SPaT: signal phasing and timing

  A SPaT message contains information about the signal phasing and timing including current phase and time remaining so that it can be used by a vehicle to provide warnings about potential red light violations or advice on optimal speed. The SPaT message is sent from a roadside ITS-station integrated with a traffic signal.

- SRM: signal request message

  SRM is sent by a vehicle to a roadside ITS-station at a signalised intersection (or central system). It is used for either a priority signal request or a pre-emption signal request depending on the way the message flag is set. In either case, the vehicle identifies itself, its current speed, heading and location, and makes a specific request for service as well as an anticipated time of service.

- SSM: signal status message

  SSM is sent by a roadside ITS-station at a signalised intersection (or central system). It is used to relate the current signal status of the signal and any collection of pending or active pre-emption or priority events acknowledged by the controller. The data contained in this message allows other users to determine their 'ranking' for any request they have made.

- IVI: in-vehicle information

  The data structure of the in-vehicle information (IVI) message format specifies which data needs to be transmitted between ITS-stations (I2V) in order to deliver in-vehicle signage associated with various ITS services (e.g. contextual speed, roadwork warning, vehicle restrictions, lane restrictions, road hazard warning and re-routing). The information will be specified in terms such as content/data elements and data structures. A technical standard is being developed that will specify a general data structure that is future proof, extensible and communications agnostic.

International harmonisation

Although the C-ITS platforms in Europe, the USA and Japan have differences, there are initiatives to improve the level of harmonisation worldwide, e.g. through the EU-US Task Force (Japan, Korea and Australia participate in some of its working groups as well). Different task groups cover security, safety, GeoNetworking, HMI and harmonisation of standards (European Commission 2013).

As Australia and New Zealand have a fleet with a wide range of vehicles and transport systems from different parts of the world, harmonisation between C-ITS developments in these regions is very much in their interest. There is a great benefit to be informed and involved in these harmonisation activities.

Despite these initiatives to improve harmonisation internationally, it appears that Australia and New Zealand will still need to make decisions regarding which standards for C-ITS to adopt as part of the core functions.

4. Justification for and Nature of Changes

This section justifies the need to introduce changes to the current ITS environment that will enable the emerging C-ITS to be progressively deployed in Australia and New Zealand. It describes the vision and objectives, the nature of these changes, and considers constraints and assumptions.

4.1 Justification for Changes

4.1.1 Vision, Drivers and Objectives

The *Policy Framework for ITS in Australia* identifies foundation actions for guiding the development and implementation of ITS in Australia. It identifies C-ITS as a priority action area. One of the foundation actions was for Austroads to develop a national strategic plan for C-ITS.

The *Cooperative ITS Strategic Plan* was developed by Austroads in close consultation with key Government and industry stakeholders, and was published in August 2012. The plan provides an overview of C-ITS technologies, the benefits, vision, objectives, policy challenges, and the priority actions that will be required. The following vision, drivers and objectives are based on the plan.

Vision

The vision for C-ITS in Australia and New Zealand is:

> *To achieve a transport system that utilises C-ITS through a nationally harmonised platform, and thus provides a safer, more productive, efficient and cost effective road-based transport system, and enables enhanced road user and road operator services and information.*

Drivers and objectives

The key drivers for the deployment of C-ITS in Australia and New Zealand are:

- Improved road safety – road crashes cause over 1200 deaths and 32 000 serious injuries in Australia every year, with an estimated annual cost to the national economy of $27 billion. The Australian *National Road Safety Strategy 2011–20*, which aims to reduce annual road fatalities and serious injuries by 30% by 2020, specifically refers to C-ITS as an emerging technology that can contribute towards these road safety targets (Austroads 2012).
- Increased transport efficiency and productivity – the avoidable cost of traffic congestion in Australia was estimated at $9.4 billion in 2005, and predicted to rise to $20.4 billion in 2020. Congestion also has a social cost, as it impacts on people and their social activities. C-ITS will enable in-vehicle applications and adaptive traffic management systems that could deliver improved efficiency and productivity to the road transport system (Austroads 2012).
- Reduced environmental impacts – transport is a significant contributor to Australia's total greenhouse house gas emissions, accounting for approximately 16% of total emissions, of which road transport makes up over 85%. C-ITS technologies have been shown to improve traffic and vehicle efficiency, thus reducing fuel use and emissions (Austroads 2012).
- Provision of services – While the principal driver for C-ITS by public organisations is to achieve the outcomes outlined above, it is unlikely that C-ITS will evolve in an environment separate to the provision of infotainment applications, which are increasingly dependent on communication technology. As the market is prepared to pay for infotainment systems and vehicle manufacturers are catering for their use in vehicles, infotainment systems may provide a vehicle for early C-ITS to roll out into the marketplace much earlier than would occur naturally.

The key public objectives for the deployment of C-ITS in Australia and New Zealand as described in the Austroads *Cooperative ITS Strategic Plan* (Austroads 2012) include:

- Road safety objectives
  - reduce the number of fatalities and serious casualties caused by road crashes,
  - reduce the costs associated with road trauma.
- Transport efficiency and productivity objectives
  - reduce traffic congestion, including reduced delay times and vehicle operating costs,
  - improve the productivity of road infrastructure use.
- Environmental impacts
  - reduce the environmental impacts of road transport, through less emissions and fuel use.

Other goals expressed by stakeholders and in policy documents are:

- Adopt international standards – This constraint is based on the policy principles and confirmed by the stakeholder consultation (Appendix A, key findings 2.1 and 4.2). For New Zealand the import of used vehicles with Japanese vehicle specifications is a special consideration. Note that standards are part of a coherent set (release) and C-ITS core functions should use either one set or another. A combination of standards from different sets could cause significant issues. The emerging sets of standards use similar concepts. The choice of a specific set of standards should be made at a more detailed design level.
- Technology agnostic – The core functions should be technology agnostic and have to be able to facilitate different communication technologies. This constraint is based on the on the policy principles and confirmed by the stakeholder consultation (Appendix A, key findings 6.1 and 6.2). Cooperative applications are likely to seamlessly switch between different available communication technologies.
- Facilitate nationally interoperable C-ITS – The core functions should enable that the same applications to work everywhere and in the same way in all parts of the country.
- Meet national and state privacy requirements – The core functions should be able to meet the privacy and, where relevant, surveillance requirements set by national and state privacy, legislation and regulations. This constraint is based on the policy principles and confirmed by the stakeholders identifying privacy as a critical function (Appendix A, key finding 5.2).

4.1.2 Limitations of the Current Situation

There are a number of limitations that prevent emerging C-ITS to be deployed and the significant safety, efficiency and environmental benefits that a fully connected cooperative intelligent transport environment can provide. These limitations are based on an analysis of C-ITS core functions and the current situation and summarised as follows:

- Secure exchange of trusted data between users and applications
  - No framework established yet to support 5.9 GHz DSRC deployment in Australia or New Zealand.
  - No agreed governance or management arrangements for security certificates.
  - Lack of agreed international standards for C-ITS security (differences exist in the approaches for security certificates and the PKI architecture).
  - Lack of agreed international standards to provide trustable C-ITS.
  - No consistent mechanism to authorise sending/receiving messages.
  - No consistent mechanism to ensure integrity of messages.

- Assurance of privacy between users and from third parties
  - No agreed, nationally consistent interpretation of privacy and surveillance legislation with regard to the use of unique identifiers and other personal data. NTC (2013) found that Commonwealth and state legislation correlates reasonably well, but there have been instances of different interpretation between and within jurisdictions. A national C-ITS platform would require a single national interpretation.
  - Lack of agreed international standards for C-ITS privacy, and/or an agreed 'privacy-by-design' approach.
- Facilitate a platform for sharing of data and efficient use of resources
  - No mechanism to subscribe to probe data for emerging C-ITS applications. Certain proprietary types of probe data messages are currently commercially available. This is mainly limited to real-time travel speeds, used for real-time route planning and navigation applications in vehicles. No such mechanisms are available for subscribing to one or several message types appearing in emerging C-ITS such as the in-vehicle information (IVI) message or the signal request message (SRM). International standardisation initiatives by ISO to address this by developing a probe data management message have not yet been included in the latest release 1 (European Committee for Standardisation (CEN) & International Organisation for Standardisation (ISO) 2013). Subscription is an issue for uni-cast and multi-cast communication only, and not for data that is broadcast, such as the heartbeat messages CAM or BSM.
  - No arrangements for data ownership on an open technology agnostic platform. Currently only proprietary telematics solutions have mechanisms for data sharing between their own users.
  - No mechanism to authorise the distribution of probe data.
  - Lack of consistent access to authoritative and trusted road operator data.
- Assurance of national interoperability and nationally consistent service access
  - No agreement to a minimum set of C-ITS standards (e.g. no consensus between the IEEE/SAE approach for BSM (basic safety message) and the ETSI approach of CAM/DENM (cooperative awareness message/decentralised environmental notification message).
  - No internationally harmonised set of standards.
  - No mechanism to ensure initial (certification) or ongoing (audit) compliance with standards for both devices and services.

Other limitations preventing deployment of certain applications are:

- Limitations to GNSS positioning with high accuracy and integrity, as required for time-critical safety applications (see Section 3.3.5 for more detail).
- Limitations to detailed mapping data available as required for critical safety applications in terms of required accuracy, integrity and timeliness (see Section 5.1.1 for more detail).
- Limited availability of wireless communication networks in rural areas.

Table 4.1 compares the capabilities of C-ITS as it would develop without the identified core functions and C-ITS with core functions (Federal Highway Administration 2012). By providing interoperability, security, trust and privacy, core functions enable C-ITS applications that would not be feasible without them. Some critical C-ITS safety applications like red-light violation warning will not be possible without core functions in the foreseeable future. Other applications are likely to be implemented at a slower pace. This justifies the change from a scenario without core functions to a scenario with core functions. These core functions will better realise the potential benefits of C-ITS.

Demand and take-up of C-ITS enabled applications could be limited by similar applications that rely on on-board sensors (not cooperative), as these have started to be deployed in the market and are showing benefit, without the need for the core functions required by C-ITS. However, in scenarios where approaching vehicles are not within line of sight (e.g. because they are hidden behind other vehicles or corners), DSRC-based applications would be able to detect them while current on-board sensors would not.

Table 4.1: C-ITS capabilities with and without the identified core functions

Capabilities of fully market driven C-ITS deployment (no core)	C-ITS capabilities with core functions
• Separate agreements to access data from organisations • Applications navigate to organisations individually to find accessible data – slow • Island solutions – no easy data exchange • Gains still possible but some capabilities and functionalities will remain out of reach	• Can request any data without having a relationship to the data provider – no need for existing contracts or agreements • Data is readily accessible and trusted from multiple sources; rapid access in real-time; and of consistent format/quality

Source: Federal Highway Administration (2012).

To realise fully-connected C-ITS, a nationally harmonised platform incorporating appropriate privacy controls and security is required. This requires centrally coordinated functions, called the core functions, which were introduced in Section 1.3.3 and are further described in Section 4.5.

4.1.3 Need for Core Functions

The US *Core System: Concept of Operations* (Research and Innovative Technology Administration 2011) has identified user needs or core needs based on stakeholders consultations.

The priority for each of the core needs has been assessed from the Australian and New Zealand perspective based on the limitations and required changes in Section 4.1.2 and Section 4.3. This assessment can be found in Appendix A. Generally, the rationale of the US priority is applicable to the Australian and New Zealand situation as well. As such, most priorities are the same. The needs describe the functionality that is required while avoiding specifics on how to implement them. Each need is identified uniquely and contains a description and a rationale.

Generally, the rationales can be summarised as follows:

- The essential needs are mainly related to secure exchange of trusted data, e.g.:
  - the trust-related needs dealing with identification of C-ITS devices
  - authorisation dealing with access rights to C-ITS services
  - misbehaviour management.
- The desirable outcomes are mainly related to **efficient data collection and distribution.**
- Only one specific **privacy** need is included, which is not prioritised in the US Concept of Operations. Even though the description of this need is not very explicit, it has been rated essential for the Australian and New Zealand C-ITS. This should be interpreted in the sense that it is essential that privacy guidelines and regulations are being met.
- The main difference between the core needs for Australia and New Zealand and that for the USA is that the US Core System needs to facilitate different states having policy frameworks. This is the reason for introducing the concept of multiple cores in the US Concept of Operations (Research and Innovative Technology Administration 2011). Based on the ITS vision and objectives and the C-ITS policy principles in Australia and New Zealand, a single national policy framework is a more obvious advantageous situation. The needs related to interaction between different core systems are then not applicable since the proposed system for Australia and New Zealand can be a single national C-ITS platform. (Note that a single national C-ITS platform does not mean a single central back office. In the example of the internet, there is a single policy framework defining identification through IP-addresses and rules for routing, but the system implementation is very much decentralised. There are limitations to the comparison between C-ITS and the internet, especially in the role of government).

4.2 Description of the Desired Changes

This section summarises new or modified capabilities, functions, processes and other changes needed to respond to the limitations identified in Section 4.1. These desired changes are translated into the needs for core functions.

There are a large number of changes that will be required in order to address the current limitations identified in Section 4.1.2, and thus enable the emerging C-ITS to be deployed. Table 4.2 summarises the desired changes that have been identified, categorised by the core functions.

Table 4.2: Required changes

Limitation	Required changes
Secure exchange of data between users and applications	
No framework established yet to support 5.9 GHz DSRC deployment in Australia or New Zealand	• Formal allocation of the 5.9 GHz band and spectrum management arrangements including reasonably priced device licensing
Incomplete set of international standards for C-ITS security	• Standardisation organisations need to further develop and specify security standards and harmonise internationally
No agreed governance or management arrangements for security certificates	• Establish a security certificate authority and provide it with the mandate to issue security certificates for certified C-ITS devices and applications • The security certificate authority then needs to implement security certificate distribution systems and procedures
Provide trust in data	
Lack of agreed international standards for integrity for C-ITS	• Standardisation organisations need to further develop standards specifying a system for ensuring integrity of C-ITS messages and release them in a complete set internationally • As data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle it encompasses more than secure communication, but also includes standards about data formats and consistent system requirements and compliance assurance of C-ITS devices creating and sending messages • Current releases of set of standards lack a consistent set of message formats and are still under development, e.g. probe data related standards are still under development • Some elements of trust are realised by other means that standardisation. Assuring compliance with standards (e.g. through certification) contributes to, and is required for ensuring integrity
No consistent mechanism to ensure integrity of messages	• Define integrity requirements, including integrity checks, security and privacy requirements. These are likely to be defined by international standardisation organisations • Establish a compliance authority (e.g. certification) and provide it with the mandate to assess compliance with the requirements (e.g. by means of certification or type approval) • The compliance authority then needs to implement compliance ensuring (test)systems and procedures/processes • Establish a security certificate authority (as above) • Implement security certificate distribution systems and procedures (as above) • Establish a registration authority (as above) • Implement registration systems and procedures (as above)
No consistent mechanism to authorise sending/receiving messages	• Establish a registration authority and provide it with the mandate to register C-ITS devices and applications for use by end users • The registration authority then needs to implement registration systems and procedures

Limitation	Required changes
Assurance of privacy between users and from third parties	
No agreed, nationally consistent privacy and surveillance legislation and interpretation of that legislation with regard to the use of unique identifiers and other personal data	• Agree nationally on the interpretation of privacy and surveillance legislation with regard to the use of unique identifiers and other personal data. This might require changes in legislation
Lack of agreed international standards for C-ITS privacy, and/or an agreed 'privacy-by-design' approach	• Develop and agree on privacy standards internationally or agree on a 'privacy-by-design' approach nationally
Facilitate a platform for sharing of data and efficient use of resources	
No mechanism to subscribe to probe data	• Establish a registration authority (as above) • Implement registration systems and procedures (as above) • Rules for the possibility to opt in or opt out on C-ITS applications need to be defined • Implement publish-subscribe mechanism for probe data that keeps track of who subscribed (opted in or opted out) to which application
No arrangements for data ownership and no mechanism to authorise the distribution of probe data	• Agree on arrangement for data ownership • Rules for the possibility to opt in or opt out on C-ITS applications need to be defined • Establish a registration authority (as above) • Implement registration systems and procedures (as above)
Lack of access to consistent authoritative and trusted road operator data for service providers	• Road operators need to disclose data in standardised data formats • Road operators and service providers need to agree on the conditions for access to this data
A mechanism is needed to create a communication technology agnostic platform. None of the available communication technologies can facilitate the full range of communication requirements	• Establish requirements and compliance assurance for a communication technology agnostic platform
Assurance of national interoperability and nationally consistent service access	
No national agreement to a minimum set of C-ITS standards for day one deployment	• Agree nationally on day-one applications, amongst road operators for the deployment of C-ITS I2V applications and amongst industry for V2V applications • Agree nationally on standards for the C-ITS platform and for day one
No complete international set of standards	• Standardisation organisations need to further develop and harmonise C-ITS standards internationally and provide 'releases' that offer feasible ways forward
No mechanism to ensure initial (certification) or ongoing (audit) compliance with standards	• Establish a compliance authority (as above) • Implement compliance ensuring (test)systems and procedures (as above) • Establish a security certificate authority (as above) • Implement security certificate distribution systems and procedures (as above) • Establish a registration authority (as above) • Implement registration systems and procedures (as above)

Identifying these required changes will help to locate any interdependencies and define timelines as well as the responsible entities who will undertake the required changes.

4.3 Priorities Among Changes

This section identifies priorities among the desired changes. Since there is no existing system on which to base changes, this section classifies and prioritises the needs/required features of the proposed system. Each need is classified as essential, desirable, or optional. Desirable and optional changes are prioritised within their classes:

- *Essential features/needs* shall be provided by the proposed system.
- *Desirable features/needs* should be provided by the proposed system.
- *Optional features/needs* might be provided by the proposed system.

Classifying the desired changes and new features into essential, desirable, and optional categories guides the decision-making process during development of the proposed system. This information is also helpful in cases of budget or schedule cuts or overruns, since it permits determination of which features must be finished, and which ones can be delayed or omitted.

The description of the needs and most of the rationale is from the US *Core System: Concept of Operations* (Research and Innovative Technology Administration 2011) and is explained in detail in Appendix A.

Table 4.3 provides a list of the core needs and their priority for the Australian and New Zealand context. The rationale is based on the limitations of the current Australian and New Zealand situation as described in Section 4.1.2. Generally, the rationale for the Australian and New Zealand context is the same as for the US *Core System: Concept of Operations*, however some of the US core needs is not applicable. The rationale is described in Appendix A.3 of Appendix A.

Table 4.3: Core needs and rationale for AUS/NZ priorities

Number	Core need	Priority AUS/NZ
Trust and security-related needs		
1	Data protection	Essential
2	Core trust	Essential
3	System user trust	Essential
4	Core trust revocation	Essential
5	System user trust revocation	Essential
6	Authorisation management	Essential
7	Authorisation verification	Essential
8	Misbehaviour management	Essential
Data exchange and support-services-related needs		
9	Time base	Essential
10	Data request	Desirable
11	Data provision	Desirable
12	Data forward	Desirable
13	Network connectivity	Essential
14	Geographic broadcast	Desirable
15	Core system service status	Desirable
16	System integrity protection	Essential

Number	Core need	Priority AUS/NZ
17	System availability	Essential
18	System operational performance monitoring	Essential
Core-to-core-related needs		
19	Core system independence	Not Applicable
20	Core system interoperability	Not Applicable
21	Core system interdependence	Not Applicable
Privacy-related and other needs		
22	Core system data protection	Essential
23	Anonymity preservation	Essential
24	Private network connectivity	Essential
25	Private network routing	Optional

4.4 Changes Considered but not Included

The following features were considered as core functions but were not included:

- **Message prioritisation:** Core functions are to enable secure and trusted communication. Prioritisation of messages may be different for different applications. A general message prioritisation is therefore not included in the proposed Concept of Operations.
- **Warning prioritisation:** Different applications may compete with each other for the attention of the road user. The prioritisation of warnings from different applications is considered to be the responsibility of the HMI developer of the device applications. It is not included in the proposed Concept of Operations. This also applies to the amount and timing of warning messages.
- **Software updates:** Mechanism for software updates already exist. Updates of the software on C-ITS devices are the responsibility of the C-ITS service provider. The C-ITS service provider has to make sure that updates are recertified if required. Any changes in the requirements to the core functions have to be updated by the C-ITS service provider.
- **Map data:** Map data is not considered a core function, because different C-ITS devices might be using different mapping data for the same application. The internal map that the C-ITS devices use to represent the environment of the vehicle, does not necessarily have the same level of detail for different C-ITS devices. There might be a need to define map data requirements and ensure compliance for critical safety applications.
- **Positioning services:** Positioning services are not considered core functions. The reason is that two C-ITS devices might both realise the required positional accuracy for the messages and therefore be interoperable, but they could have implemented positioning in different ways. There may be a need to certify positioning services for some applications.

4.5 Constraints and Assumptions

This section describes constraints and assumptions applicable to the changes and new features.

4.5.1 Constraints

A constraint is a factor that lies outside, but has a direct impact on, a system design effort. Constraints may relate to laws and regulations, or technological, socio-political, financial, or operational factors. The following are constraints to realising the core functions as part of a C-ITS platform:

- **Funding and resources:** The implementation of core functions is likely to have budget constraints. Core functions will be implemented in different C-ITS components by different stakeholders, including C-ITS developers, a security certificate issuing organisation, and certification organisations. The budgeting mechanisms in these organisations will be different. Decisions on budgeting will be required for both capital and operational expenditure.
- **International standards:** Current policy in relation to C-ITS is to align with international developments and to use international standards. Although a Concept of Operations proposes system operation on a conceptual level, some of the current C-ITS architectural standards have been used as guidance.
- **Vehicle regulations:** Vehicle regulations are a potential future constraint. Currently, Australia harmonises primarily with the UNECE vehicle regulations which have not yet adopted C-ITS-related regulations.

Additionally, there are constraints to the performance of certain C-ITS applications, which include:

- **Funding and resources:** As with the funding and resources constraint for the core functions, the deployment of specific C-ITS applications is likely to be constrained by funding and other resources as well.
- **Positioning:** Certain critical safety applications may not be useable directly in Australia and New Zealand if they have been developed internationally under the assumption that GNSS positioning will meet accuracy and integrity requirements achieved elsewhere. Australia and New Zealand currently do not have access to a wide area augmented GNSS.
- **Availability of wireless communication services:** Another local limitation in rural regions is that the demand for wireless communication services is likely to be too low to deploy wireless communication infrastructure similar to that in other areas. Most applications will be developed for conditions where wireless communication infrastructure is available. Some might not work, or not work well in remote areas where this communication infrastructure is absent. Therefore the number of available C-ITS applications or their functionality is likely to be limited in these areas, or applications might need to be adapted to function under the available communication services.

4.5.2 Assumptions

An assumption is a judgment about unknown factors and the future, which is made in analysing alternative courses of action. The proposed core functions are based on the following assumptions[5]:

- **National policy framework:** It is assumed that a national policy framework for C-ITS will be developed, allowing a consistent deployment of cooperative applications in every state and territory. This assumption is based on the policy principles and the stakeholder consultation (Appendix A, key findings 2.2 and 4.2).

[5] New Zealand is independently considering these assumptions.

- **Allocation and management of the 5.9 GHz spectrum:** It is assumed that the Australian Communication and Media Authority (ACMA) will formally allocate the 5.9 GHz spectrum band for ITS use, with a licensing regime that enables DSRC units to be introduced to vehicles and ITS roadside equipment. It is assumed that challenges to the use of the 5.9 GHz band internationally will be resolved.
- **Introduction of C-ITS vehicles:** It is assumed that the automotive industry will introduce vehicles to the Australian and New Zealand vehicle fleets with C-ITS capability, including cellular and DSRC technology.
- **Increased automated driver assistance:** It is assumed that vehicles will increasingly have automated controls based on in-vehicle sensors. These will converge with C-ITS.
- **Availability of standards:** It is assumed that international standardisation organisations will continue to develop a complete set of standards for C-ITS in the next few years. This will result in different sets of C-ITS standards that will be partly harmonised.
- **The current liability framework suffices:** The National Transport Commission (NTC) recommends no changes are needed to the current laws and approaches around liability in Australia for the implementation of C-ITS when used for advisory applications (NTC 2013). Note that liability issues will need to be reassessed in the context of vehicle automation. It is assumed that current laws and approaches around liability will not withhold stakeholders from deploying C-ITS.
- **Business model and business cases:** It is assumed that business models will be developed, or evolve, for a range of C-ITS solutions, which will support positive business cases for the stakeholders involved.
- **Voluntary C-ITS applications:** In the USA a decision whether to mandate basic safety messages is being considered. There are no clear indications that any C-ITS functionality would be legally mandated in Australia or New Zealand in the near future. For this Concept of Operations it is assumed that there will be no legal mandate for C-ITS functionality or a C-ITS platform.
- **Willingness to provide probe data anonymously:** It is assumed that most travellers are willing to share data collected by their vehicles and mobile devices provided that they will be anonymised. The type, amount, quality and frequency of data will vary depending on vehicle capabilities and operator settings.
- **Sharing of data:** It is assumed that most travellers are willing to anonymously make probe data available to application providers, under conditions that are to be determined. Stakeholders have different views on business models for data ownership (Appendix A, key finding 3.1).

5. Concepts for the Proposed System

This section describes the concepts for the proposed C-ITS core functions that will enable the emerging C-ITS to be deployed and operated.

5.1 Background, Objectives and Scope

5.1.1 Background

As a background to describing the operation of the proposed C-ITS core functions, the section describes the operation of C-ITS as currently emerging in the form of pilots, initial deployment and standards.

C-ITS involve the use of wireless communications to share information between vehicles, roadside infrastructure, mobile devices and centres so that vehicle and transport applications can deliver safety, mobility and environmental outcomes for the road transport system that are beyond what is achievable with standalone applications.

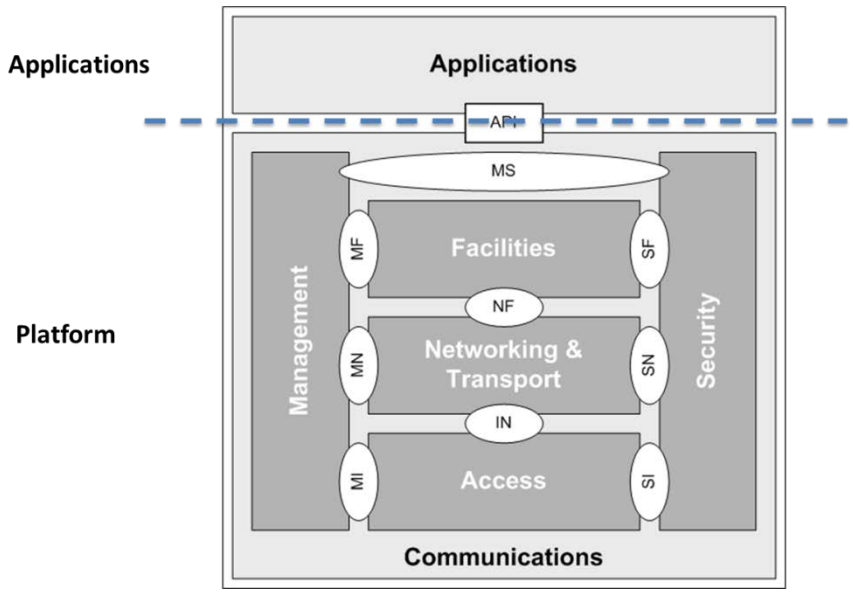
C-ITS form a distributed and dynamic computing environment. As such, C-ITS can be described as a system of interoperable systems, which will consist of a platform on which service providers can develop and deploy a wide range of applications and services.

ITS-station

The four main physical components of C-ITS are vehicles, roadside equipment, mobile devices and centres. Communication networks will connect these physical components. To enable the interaction, the different components need work in a certain coordinated way. This functional structure is described in the ITS-station architecture.

The ITS-station distinguishes applications from the platform on which the applications run. A platform can be defined as a group of technologies that are used as a base upon which other applications, processes or technologies are developed. ISO defines a C-ITS platform as the ITS-S layers with the exception of the applications layer (ISO 17419), as indicated in Figure 5.1.

Figure 5.1: Simplified ITS-station reference architecture



Source: Modified from simplified ITS-station reference architecture: ISO 21217 draft international standard.

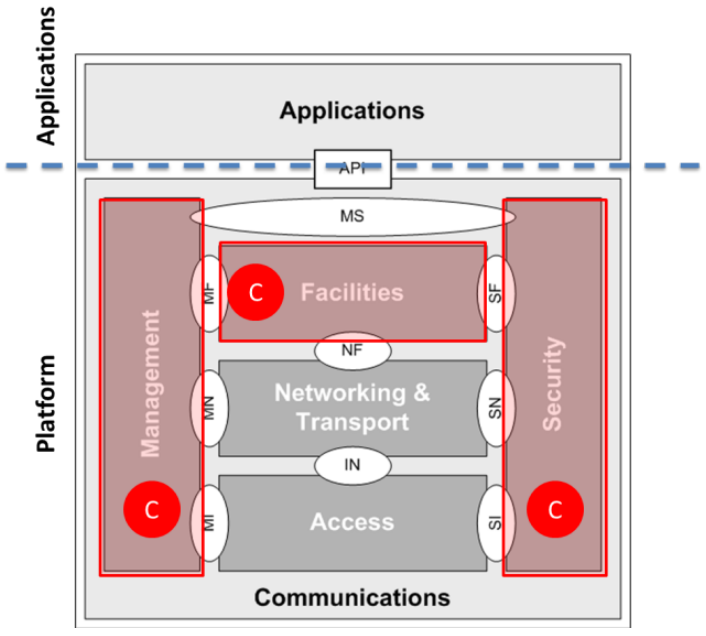
The ITS-station reference architecture, defined by the International Standardisation Organisation (ISO 21217) is also commonly used, accepted and referenced, by other standardisation organisations like ETSI and IEEE (ETSI EN 302 665, IEEE P1609.0). While the IEEE references and acknowledges the ITS-station, the commonly used architecture model in the USA is the IEEE WAVE protocol architecture. The main difference from the ITS-station architecture is that the WAVE protocol architecture is limited to the WAVE protocol stack and does not include the facilities and applications layers.

The layers in the ITS-station reference architecture are based on the open systems interconnection (OSI) model for layered communications protocols, and can be described as follows:

- Applications – contains the ITS applications. These applications make use of the underlying facilities and communications capacities within the ITS-station.
- Facilities – a middleware layer that provides support functions, information or services to the appropriate ITS applications. An example is managing the local dynamic map.
- Network and transport – contains various functions including routing of data between the communications technology and the appropriate function, managing data congestion, checking integrity of data packets and ensuring data is in the correct format.
- Access – contains the communications technologies that enable ITS-stations to wirelessly exchange data messages. These technologies can include any type of communications medium (e.g. cellular, DSRC, digital radio, etc.).
- Management – provides management functions for the C-ITS device and its applications. Examples are the storage of management data, subscribing to services and the selection of a communication technology for communication flows.
- Security – provides security functions such as encryption and decryption, a firewall and authentication and authorisation.

Figure 5.2 maps the core functions to the ITS-station reference architecture layers of management, facilities and security. It shows the supportive nature of the core functions. For example, the core functions will enable trusted and secure communications for those C-ITS applications that require this, however the ITS access technologies themselves and the network and transport layer protocols are not part of the core functions. Note that this figure is indicative and that the proposed core functions do not all exactly cover the components of the ITS-station reference architecture.

Figure 5.2: Core functions mapped to ITS-station reference architecture

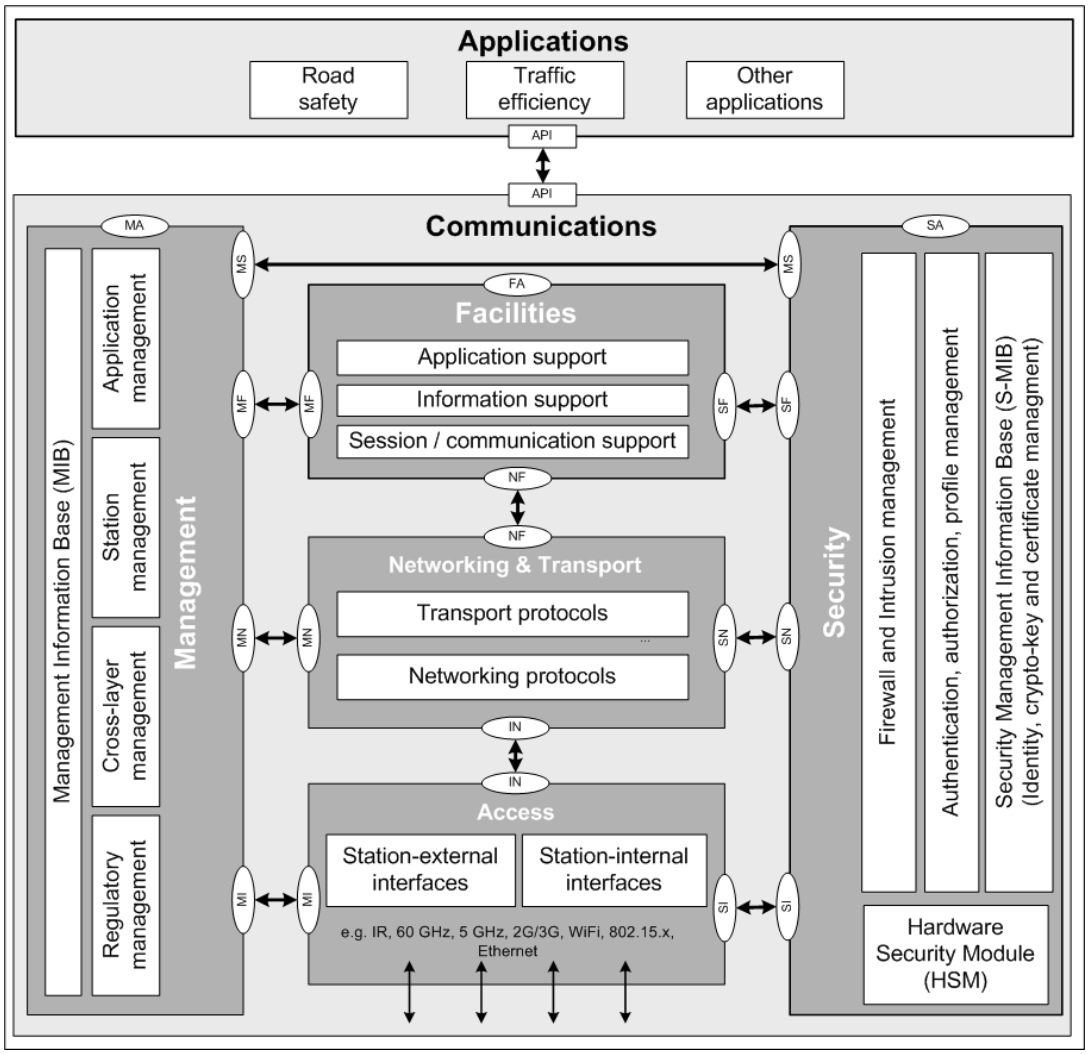


Source: Simplified ITS-station reference architecture: ISO 21217 draft international standard.

The same physical systems (C-ITS devices) that may be used to run an application and process application data, may also be used to run a core function and process core data messages. This does not include sensors and positioning. It does include C-ITS devices in vehicles, mobile or nomadic C-ITS devices, C-ITS devices in ITS roadside infrastructure and those computer systems in centres that are involved in core functions such as issuing security certificates or certificate revocation.

The simplified reference architecture for an ITS-station shows the functional components of C-ITS devices. The detailed ITS-station reference architecture (Figure 5.3) shows the interfaces between these components and subcomponents.

Figure 5.3: ITS-station reference architecture



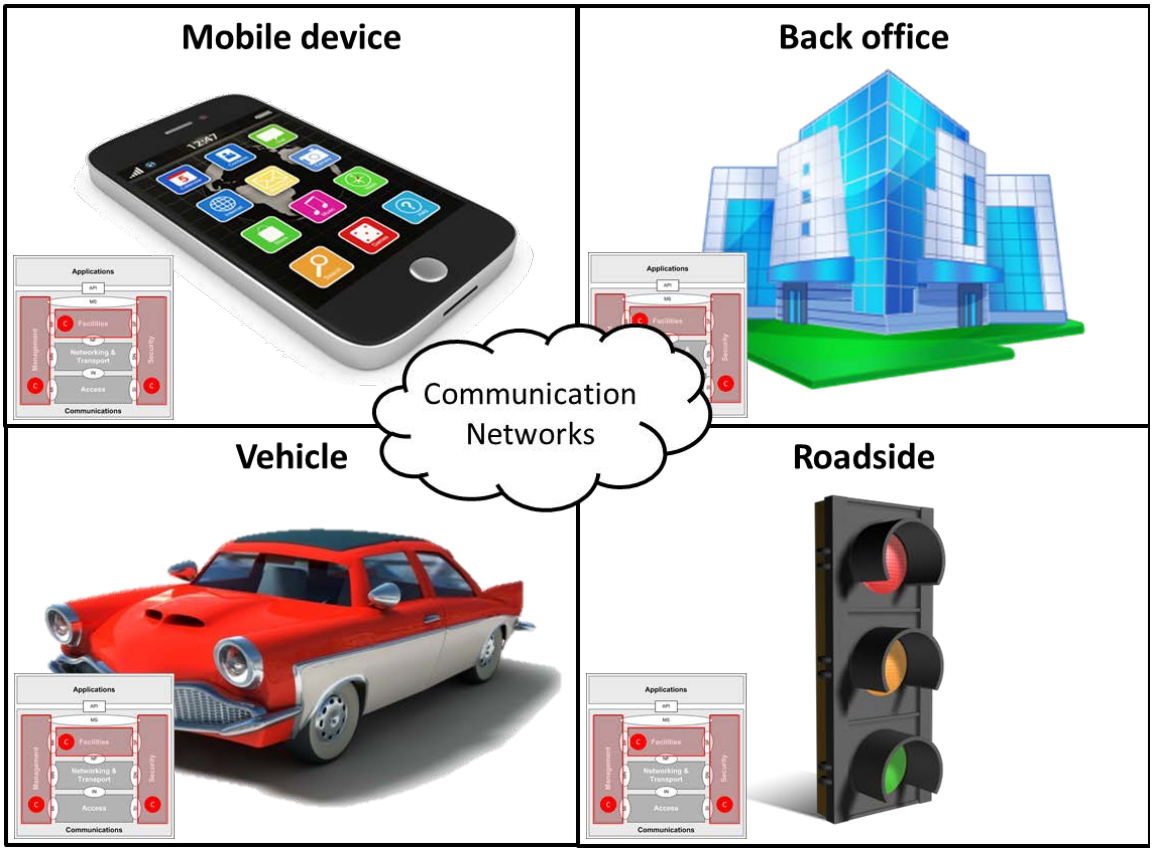
Source: ISO 21217.

Physical view

The core functions should be considered as functionality rather than a physical piece of equipment. For example, a vehicle equipped with an in-vehicle C-ITS device, which will house or connect to sensors and equipment in the vehicle, and possibly access to the vehicle CAN-bus, will also comprise core functions. Similarly, ITS-connected roadside equipment, ITS-connected portable devices, and control centres will have systems that connect to/control equipment and sensors and will include core functions.

Core functions are executed in each of these four types of physical ITS-stations, as a set of functions and rules embedded in software or software components, or even hardwired in a chip. Figure 5.4 shows the physical locations of core components. No core functions are found in the communication networks.

Figure 5.4: Physical locations of core components



Communication

Many emerging C-ITS applications will likely use a hybrid communications approach, dynamically selecting different communication technologies for different types of content, depending on the local availability of communication networks. Different communication technologies have different characteristics and attributes and are suited to different communication requirements. This section explains the hybrid communication approach.

C-ITS applications that use a hybrid communication approach may use several communication mediums, and not rely on one type. Different communication technologies have their strengths and weaknesses. None of the available communication technologies can facilitate the full range of communication requirements from C-ITS applications. For example time-critical safety warnings usually require low latency communication. Currently, the only communication technology that meets this latency requirement is 5.9 GHz dedicated short range communication (DSRC), although as LTE (4G) rolls out, where supported, it will provide an alternative for all but very low latency services. Snow, ice and most obstacle alerts, even train alerts can be delivered within a second, or two by most of the communication technologies – and are perfectly adequate for purpose. By comparison collision avoidance, ramp access control etc. need bi-directional communication and message completion within milliseconds, which requires very low latency communication. Many traveller information services require a long range communication connection and more bandwidth, which can be adequately offered by cellular communication technologies. DSRC would not be suitable for this type of application. Some messages, for example a roadworks warning message, could be sent via different communication technologies.

Even a single application, for example an intersection collision avoidance application, is likely to have different communication flows with different communication requirements. Messages that involve vehicular control (collision avoidance, ramp access control etc.) will need very low latency. The communication of detailed mapping data on the layout of the intersection may have less latency requirements. The same application might also have other requirements for the download of new security certificates; this type of communication flow does not have a low latency requirement, but it does require bandwidth. These communication flows, and probably others, might all be needed for this application to function. A hybrid communication approach allows for a more efficient and more robust C-ITS as vehicles can choose the best available communication channel dynamically.

Which communication technology is selected by an application is obviously also subject to the local availability of the communication technologies and the minimum communication requirements. The ISO 'release one' (European Committee for Standardisation (CEN) & International Organisation for Standardisation (ISO) 2013) includes a standard on communication access for land mobiles (ISO 21217), which provides the mechanism for this hybrid communication approach. The future availability and coverage of communication technologies throughout the network is currently hard to predict and will depend on the local conditions, the demand for communication and allocation of frequencies.

The hybrid approach is of significant importance in Australia and New Zealand because of large areas of low population where only limited choices of communications options may be available, and the optimum medium available may vary from one location to another.

Ad hoc V2V communication (Vehicular Ad hoc NETworks – VANETs), are most likely to use 5.9 GHz DSRC as a prime communication technology for the foreseeable future. The role of LTE (4G) for V2V communications is as yet unknown and unproven, but will in all probability also have an important role in the future for non-time-critical networking.

The hybrid communication approach is supported by the concept for communication management is described in the communication access for land mobiles (CALM) standards. The CALM standards are part of the ITS *Networking and Transport* component and the *Access* component (ISO 21210). Through the ITS-station architecture (ISO 21217), the CALM standards separate, as far as possible, the service provision applications from the wireless communications technology; and in most cases service provision can (similar to many application services available over the Internet) be totally agnostic in respect of the communications carrier technology. This allows for flexible use of the C-ITS platform to support a range of applications and will make the system of systems scalable and flexible in adopting for future technological developments.

Data messages

There will be a number of different types of data messages in C-ITS. They are categorised in two main categories, being application data messages and support data messages:

- Application data messages

  Data used by applications to provide a service to the end user. Some data message types will be used by more than one application. These universally used messages are being standardised. Some of the emerging standards for commonly used application data messages are described below.

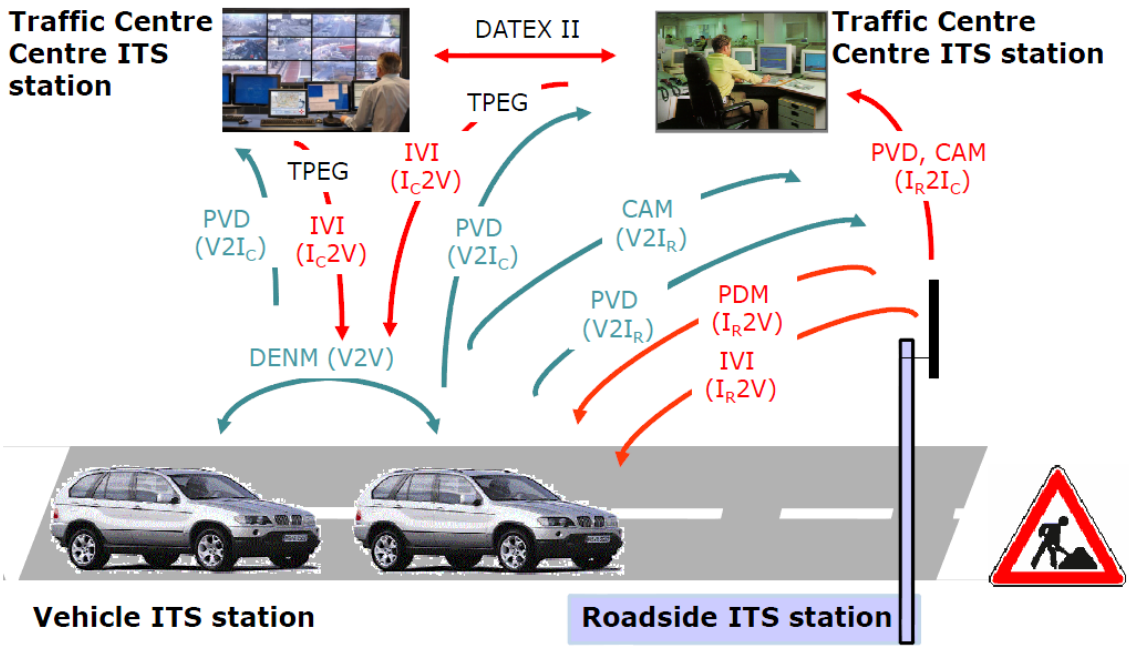
- Support data messages

  To enable C-ITS, support of core functions will be provided that is not directly related to the application data but are essential to enable the service provision to take place in a secure reliable and successful way. These services may generally be categorised as user permissions management, user trust management, data distribution, misbehaviour management, network services, service monitoring and time synchronisation. Data messages related to these functions are called support data messages and are part of the core functions discussed in Section 5.3.

Figure 5.5 shows the application data messages that could be involved in a roadwork warning use case, in this example being the decentralised environmental notification message (DENM), probe vehicle data (PVD), in-vehicle information (IVI) data message, TPEG data messages, the cooperative awareness message (CAM), and the probe data management (PDM) message.

For each message type it is indicated between brackets if the message is communicated between the vehicles and the traffic centre infrastructure (I_C) or the roadside infrastructure (I_R).

Figure 5.5: Messages involved in a roadwork warning use case in Europe



Source: Schade (2013).

Data messages and protocols for other ITS domains, such as for centre-to-centre and centre-to-infrastructure communication, include DATEX II and NTCIP.

The data message types used in this use case example are generated and used in the *Facilities* and *Applications* layer of the ITS-station. In the lower layers they are packaged into other data formats suitable for communication such as segments, IPv6 packets, data frames and bits.

In the *Applications* layer the roadwork warning application will translate the data messages described in Figure 5.5 in a roadwork warning message that will be 'communicated' to the user via a visual or audio warning on a human machine interface such as a screen or speakers.

5.1.1 Objectives

As stated in section 4.1.1, the key public objectives for the deployment of C-ITS in Australia and New Zealand as described in the Austroads *Cooperative ITS Strategic Plan* (Austroads 2012) are:

- Road safety objectives:
  - reduce the number of fatalities and serious casualties caused by road crashes
  - reduce the costs associated with road trauma.
- Transport efficiency and productivity objectives:
  - reduce traffic congestion, including reduced delay times and vehicle operating costs
  - improve the productivity of road infrastructure use.
- Environmental impacts:
  - reduce the environmental impacts of road transport, through less emissions and fuel use.

The use of ITS is progressively delivering improvements in each of these three areas, while also facilitating the provision of value-added services to road users. C-ITS represents the next generation of ITS, which will enable applications to cooperatively work together to achieve more optimised outcomes in each of these areas.

A cooperative intelligent transport environment is continuing to evolve locally, utilising existing ITS, communication technologies, mobile devices and in-vehicle systems. This is enabling a range of ITS and vehicle telematics applications to be deployed. However, many of the next generation of C-ITS applications will have requirements that the current environment cannot support. The limitations of the current situation have been described in Section 4. A key objective therefore is to address the identified limitations by establishing the core functions required to support the deployment and operation of emerging C-ITS.

Significant progress has been made internationally with the development of C-ITS technologies and services. While there are differences in some standards developed in different regions, there are efforts to progressively work towards harmonised standards and best practices for C-ITS. It is critical that a localised C-ITS platform is harmonised where possible with agreed international standards and best practices, so as to enable interoperability, to achieve cost-efficiencies, and to remove barriers for the global adoption and deployment of C-ITS technologies and services.

Ultimately the goal is to realise C-ITS that enable applications and services that benefit end users and optimise public purpose outcomes.

The proposed core functions that have been identified as necessary to address the objectives of C-ITS are as follows:

- secure exchange of data between users and applications
- support trust in and integrity of data
- assurance of privacy between users and from third parties
- facilitation of a platform for sharing of data and efficient use of resources
- assurance of national interoperability and nationally consistent service access.

5.1.2 Scope

The scope of the proposed system of core functions is indicated in terms of the functions of the ITS-station.

This Concept of Operations relates to the provision of core functions that are necessary in order to facilitate and enable C-ITS service provision. This document does not provide a Concept of Operations for any particular C-ITS application, but for the support functions required for such C-ITS applications.

The definition of core function extends to functions distributed over all four types of C-ITS devices, being vehicles, roadside infrastructure, mobile devices and centres. This differs from other documents that define core functions as those performed in centres, for example the SAE report on candidate improvements to DSRC message set dictionary (Society of Automotive Engineers 2014).

In scope

The five identified core functions are in scope, with the following requirements:

- Functions that provide security for the exchange of data between users and applications.
- Functions that provide trust in the exchange of data messages, including certificate revocation, misbehaviour management and integrity checks.
- Functions that assure privacy between users and from third parties. To ensure an appropriate level of protection for personal data, and to assure compliance with relevant privacy and surveillance requirements.

- Functions that provide efficient data collection from various sources and distribution to many users. These include functions that enable the efficient capture of data from a range of sources, and appropriate data management, storage and distribution to facilitate applications and services.
- Functions that assure national interoperability and nationally consistent services. These include functions that enable a consistent platform that facilitates efficient development and deployment by service providers, and achieves consistency in services for end users.

Out of scope

The following are considered out of scope:

- C-ITS applications and services – these will be developed and deployed primarily by service providers. The proposed core functions are simply intended to enable these applications and services to be developed and deployed. For example, assuring that a safety-critical application complies with required standards may be in scope, but developing and managing an application is not.
- Data supply chains and content for C-ITS – the data supply chains required to capture, validate, store, format, value-add and distribute content for consumption by C-ITS applications and services are out of scope. However, where it is necessary for data to meet a level of trust/integrity (e.g. position accuracy for a safety-critical application), the process for achieving trusted data may need to interface with the relevant core function.
- Systems that interface with the core functions – while the interfaces with other systems within the cooperative intelligent transport environment are obviously important, the systems themselves are not in scope. Examples include traffic management, in-vehicle and satellite positioning systems, etc.

Use of core functions

Not all C-ITS applications and devices will necessarily need to implement the core functions as proposed in this Concept of Operations. Trust and security are more crucial for safety-critical applications than for travel information applications.

For some communication technologies, some of the core functions might already be provided by the communication network provider. For example, cellular networks might already provide sufficient security and privacy functions for some C-ITS applications, such as road condition alerts.

The decision on what core functions are needed will very likely be determined for each application or for each message type case-by-case, based on a requirements and risk assessment. In the case of safety messages and actions, in order to limit liability, multiple sources and types of data will likely be used wherever possible. So for example, a collision avoidance system will likely use a combination of vehicle sensors, and DSRC communications from and to other vehicles, in order to perform the collision avoidance service. The risk assessment should include all inputs to the application including performance of the C-ITS platform/device and the sensors.

Where an application is deemed to be safety-critical, such as collision avoidance applications, there may potentially be a regulated requirement for the relevant core functions to be used. There may also be a need for assurance of compliance with agreed standards for such applications.

There is currently no clear categorisation of applications and platform devices by risk for the purpose of assessing the required level of compliance assurance. These classifications should preferably be developed as part of international standards. To facilitate the decision making on which applications should use the core functions, applications may need to be classified. For example, classification could be by:

- The time-criticality of information exchanges and management functions – for example, collision avoidance has a high time-criticality, whereas traveller information may have a low time-criticality, and road condition alerts (ice, obstacles, potholes etc.) have some time sensitivity, but not time-criticality in the same way as, say, collision avoidance or ramp access control.

- The safety risk of an application related to the level of automation – for example, an erroneous warning application is less likely to cause a problem than an erroneous autonomous breaking assist application.
- The security risk in relation to either safety or privacy – for example, communications that could be maliciously hacked and used to cause a safety incident, or could be used to compromise an individual's privacy.

A policy on the requirements for the use of core functions for different applications may be needed. Currently there is no international standardisation activity in progress addressing such a classification.

5.2 Operational Policies and Constraints

This section describes operational policies and constraints that apply to the proposed system. Operational policies are predetermined management decisions regarding the operation of the new core functions, normally in the form of general statements or understandings that guide decision-making activities. As stated in Section 4.5.2, it is assumed that a national C-ITS policy framework will be developed, which will specify many of these guiding statements. Some of the current regulations and policies affecting the operations of the C-ITS core functions are the following:

ITS

- The *Policy Framework for Intelligent Transport Systems in Australia* (Standing Council on Transport and Infrastructure 2012) was endorsed by transport ministers at the inaugural Standing Council of Transport and Infrastructure (SCOTI) meeting in November 2011. This provides a robust framework for ITS, and identifies policy principles and foundation actions for guiding the development and implementation of ITS in Australia. It identifies C-ITS as a priority action area.
- The New Zealand *Intelligent Transport Systems Technology Action Plan 2014–18* (Ministry of Transport 2014b) was released for public consultation. It summarises the strategic context guiding investment decision in ITS. It also proposes government actions. A proposed action specifically related to C-ITS is the allocation of radio spectrum for C-ITS by the Ministry of Business, Innovation and Employment, following the spectrum allocation in leading countries and regions from which most of the vehicles are imported into New Zealand.
- The *Cooperative ITS Strategic Plan* (Austroads 2012) sets the direction for the local deployment of C-ITS. It outlines the mission, vision, objectives and guiding principles with respect to the local deployment of a C-ITS platform, with a key theme being the need to harmonise with international standards and best practice.
- The *TCA National Telematics Framework* (Transport Certification Australia 2014) comprises four elements and provides a nationally agreed and industry compatible and sustainable policy and regulatory framework, a functional and technical platform, an operating environment and a commercial setting for telematics applications.
- Road authorities – Policies for type approval of ITS equipment do not set operational constraints to the C-ITS core functions. Rather, the C-ITS roadside devices are likely to create additional requirements for type approval of certain ITS roadside equipment.

ICT

- Radio communication licensing – The regime for radio communication licensing for the 5.9 GHz frequency band still has to be determined by the Australian Communication and Media Authority (ACMA) in Australia, and by the Ministry of Business, Innovation and Employment (MBIE) in New Zealand. This is likely to create operational constraints for the operational licensing processes.

- Privacy – Legislative privacy and surveillance requirements have been assessed by the National Transport Commission (NTC). The NTC has developed a *Final Policy Paper*, which includes a range of findings and recommendations which were endorsed by SCOTI at its meeting in November 2013. In summary, the Final Policy Paper does not recommend any significant changes to current legislation or policy, as it has been assessed that the current frameworks for privacy, liability, driver distraction, and compliance and enforcement should suffice. Recommendations are made that a privacy assessment are performed, that Australian ministers explicitly consider privacy impacts on drivers in any decision relating to institutional arrangements for C-ITS and that in the event that individuals can be reasonably identified from the safety data message broadcast by C-ITS devices, specific legislative protections are developed to define in what circumstances organisations that are exempt from compliance with privacy principles, including enforcement agencies, may access C-ITS personal information (NTC 2013).
- Security – Current IT security policies might set constraints to the publicly developed subsystems. The international developments of the security system for C-ITS are likely to determine the operational constraints in Australia, so these international developments have been taken as guidance in the Concept of Operations. It is noted that the Australian Government's *Gatekeeper PKI Framework* provided guidance to the PKI approach used for the Intelligent Access Program (IAP), and while not mandatory, should be given consideration with C-ITS also.
- Open data – Jurisdictions have different policies relating to access to government data (e.g. open data policies). These need to be considered when establishing data management and data distribution functions.
- System support – Some jurisdictions have policies relating to the support of ICT systems. For example, some states encourage or require a level of compliance with the information technology infrastructure library (ITIL).

Vehicles

- The *Australian Motor Vehicles Standards Act 1989* – for vehicle regulations on safety, security and the environment, states that Australian Design Rules (ADRs) may be harmonised with the United Nations Economic Commission for Europe (UNECE) agreements regarding harmonised vehicle regulations (Economic Commission for Europe 2012). This requires type approval for new vehicles and puts restrictions on the import of used cars. Currently the UNECE has not yet adopted C-ITS related regulations.
- ADRs – State jurisdictions have largely based their in-service vehicle roadworthy requirements on the ADRs, but with some differences. In particular some jurisdictions require annual evidence of compliance while others only require evidence at transfer of vehicle ownership. This will create requirements for the support environment (compliance assurance), but not for the system operations.
- Regulatory compliance mark (RCM) – The RCM indicates a device's compliance with all applicable ACMA technical standards and associated record-keeping (including testing) arrangements, and with applicable state and territory electrical equipment safety requirements. The ACMA has an agreement with the Federal Chamber of Automotive Industries (FCAI) for manufacturers listed under the FCAI *Code of Practice for Electromagnetic Compatibility*. FCAI members are bound by this code of practice, which applies to new vehicles registrable for use on the road.

Standards/general

- Harmonisation – Australia and New Zealand are signatories of the World Trade Organisation's *Treaty on Technical Barriers to Trade* (WTOTBT), which requires the use of relevant international technical regulations where they exist or are imminent. With regard to the automotive industry, Australia and New Zealand are signatories to both the 1958 and the 1998 United Nations Economic Commission for Europe (UNECE) agreements regarding harmonised vehicle regulations (Economic Commission For Europe 2012). As part of these agreements, Australia is actively involved in and supports the World Forum for Harmonisation of Vehicle Regulations (Working Party 29). In addition, it is general Australian Government policy to harmonise where possible with international vehicle safety regulations developed through Working Party 29. Currently these do not provide any constraints to the C-ITS core functions. Possibly in future they might include requirements related to C-ITS.

- Compliance – As a general rule, compliance with standards is voluntary, unless written into regulation. This may be considered for C-ITS where there are implications for safety, security, environment, or consumer protection.

5.3 Description of Proposed System

This section provides a description of the C-ITS core functions. As described in Section 1.3.2, C-ITS will be a system of systems, comprising a dynamic, distributed computing environment with computing units in vehicles, roadside infrastructure, mobile devices and centres.

Using different types of communication C-ITS will enable a range of vehicle and transport applications to be deployed that can deliver safety, mobility and environmental outcomes for the road transport system that are beyond what is achievable with standalone applications. For any data messages communicated that could be used by applications that are safety-critical (e.g. collision warning or intersection assistance), or are for a regulatory purpose (e.g. monitoring permitted road access) then it will be important that these communications occur in a way that does not compromise the operation or effectiveness of the applications.

Depending on the message being communicated and the application using the message, the following core functions may be necessary:

- secure exchange of data between users and applications
- support trust in and integrity of data
- assurance of privacy between users and from third parties
- facilitation of a platform for sharing of data and efficient use of resources
- assurance of national interoperability and nationally consistent service access.

The following sections provide further detail on these proposed core functions, which are part of C-ITS. The core functions are defined in terms of several functional subsystems, described in Section 5.3.6.

5.3.1 Secure Exchange of Data Between Users and Applications

The core functionality described is specifically to enable a secure connection between ITS-stations and the security of the systems that constitute C-ITS.

The EU-US Harmonisation Task Force (2012a) identified different communication scenarios for exchanging data including:

- vehicle-originated broadcast (one-directional communication from a single vehicle to any receiver)
- infrastructure-originated broadcast (one-directional communication from a roadside unit to any receiving vehicle)
- infrastructure-vehicle-unicast (bi-directional communication between a single vehicle and a single roadside unit).

These and other communication scenarios are detailed in Section 6.

It is important to define the meaning of security in the context of C-ITS communications. Security relates to the information being exchanged and the system used to interact. Information is secure if it cannot be intercepted, understood if intercepted, altered or faked. System resources are considered secure if they are free from unauthorised access, change and destruction. Both trust and security also extend beyond an interaction. Information is only secure if it is not released after the interaction (CSIRO 2011).

As defined in the ISO standard *Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary,* information security is the 'preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved' (ISO/IEC 27000:2009). EU-US Harmonisation Task Force security task group (HTG6) refers to:

- confidentiality (protection of personal information)
- integrity (trust in the message)
- authenticity (trust in the sender).

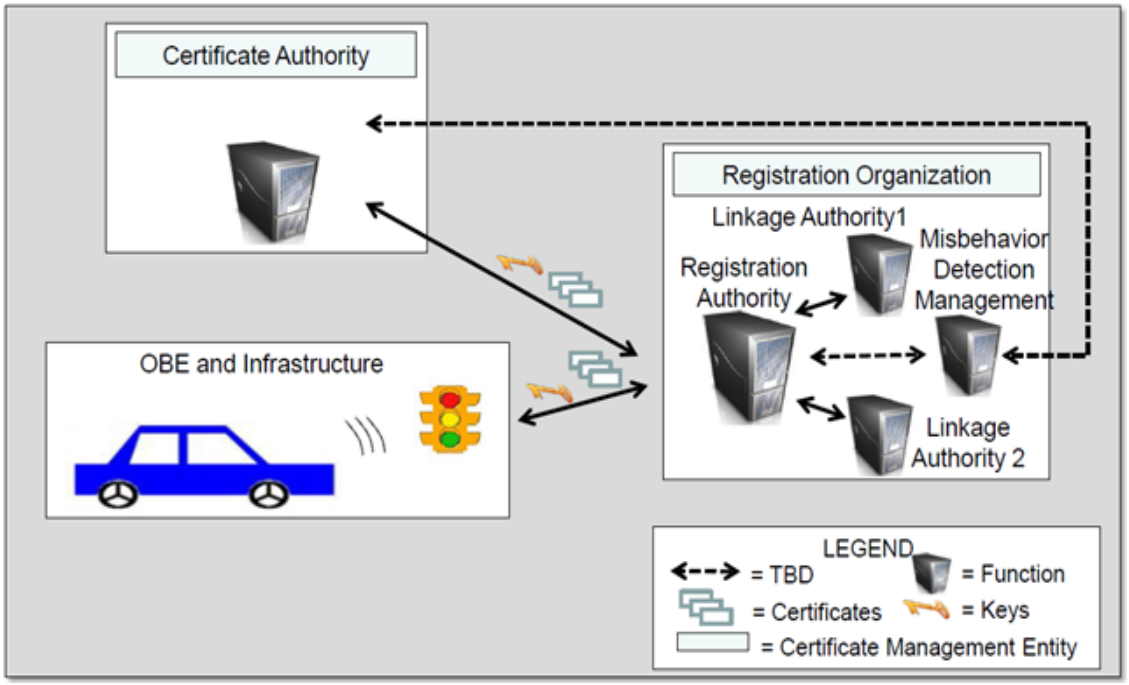
People are an integral part of any secure system. Therefore technological solutions on their own are not sufficient in guaranteeing security. A complete solution must also include legal and social regulations (CSIRO 2011), called the institutional context. An institutional context is proposed in this Concept of Operations based on the concept of public key encryption and a security credential management system (SCMS).

Security credential management system (SCMS)

An SCMS refers to a system that aims to achieve the security goals related to establishing trust among users in a communication network. The SCMS provides for a digital certificate that can identify a C-ITS device and provides directory services that can store and, when necessary, revokes the certificates. Figure 5.6 shows a SCMS, which includes the in-vehicle C-ITS device (OBE) and the roadside infrastructure, as well as the certificate authority, registration authority and linking authority. The systems of these certification management entities are called external support systems. The SCMS includes support systems that are part of the support environment and provide digital certificates to be used in the operation of C-ITS.

The certificates need to be provided to the vehicles, roadside units, mobile devices and centres before they can engage in the operation of C-ITS applications. Certificates probably will have to be renewed during the lifetime of the C-ITS equipment, and certificates may have to be revoked. This means that during the operational life of C-ITS equipment, it has to interact with the support systems.

Figure 5.6: Security credential management system



Source: Briggs (2012).

For the SCMS to meet the security needs of the emerging C-ITS ecosystem, the various functions must work together to exchange information securely and efficiently. There are two types of functions, pseudonym functions and bootleg functions:

- Pseudonym functions are responsible for creating the short-term certificates used by C-ITS devices. The term ‘pseudonym’ is used to indicate that short-term certificates contain no information about users, but still allow users to participate in the connected vehicle system, in essence allowing use of a pseudonym. Pseudonym functions create, manage, distribute, monitor, and revoke short-term certificates.
- Bootstrap functions establish the initial connection between ITS-stations and the SCMS. This process is characterized by its chief component, the enrolment certificate authority, which is responsible for assigning an enrolment certificate to each C-ITS device.

The European project PRESERVE intends to design, implement, and test a secure and scalable V2X security subsystem for realistic deployment scenarios (PRESERVE 2013). Figure 5.6 reflects the CAMP architecture rather than the PRESERVE architecture, but the two are very similar (EU-US harmonisation task force 2012b).

Public key infrastructure

A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. It enables users of a public network to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

PKI uses cryptography to provide authentication, integrity and confidentiality when sending messages between different users. There are two types of cryptography that CAMP has proposed for use by the SCMS: asymmetric and symmetric:

- Asymmetric – uses two keys and works in such a way that what is encrypted with one key can be decrypted with the other. Although the keys are mathematically linked, it is extremely difficult to derive one key based on knowledge of the other. This property allows one key, the ‘public key’, to be widely distributed while the other key, the ‘private key’, is held only by the owner. When asymmetric cryptography is used, the PKI provides the assurance that the public key is valid by putting the public key in a certificate signed by the PKI. In this way, a sender and a receiver do not need to have any prior interaction to securely send and receive messages and trust that the messages are authentic.
- Symmetric – uses a single key to encrypt and decrypt, which poses a challenge when controlling key distribution because it is important that only the required parties have the correct keys. Asymmetric cryptographic operations (encryption and decryption) are computationally harder than operations using symmetric cryptography.

Different types of messages or types of communication can use different encryption. Important factors for these design choices are processing speed and costs related to hardware and power use. The design choices will be made in later stages so they can align with international developments.

The PKI used with the SCMS can have a hierarchy with one or more tiers. In a single tier (non-hierarchical) PKI environment there is only one certificate authority, which will be the root certificate authority (as in the simplified Figure 5.6). If there are more tiers the root certificate authority will issue subordinate certificate authority certificates below the root. Users can request certificates from the subordinate certificate authority. All trust for system components and subscribers is inherited and delegated from the root certificate authority through certificate issuance. Once trust has been established with the root certificate authority, each relying party can validate PKI certificates issued under the root certificate authority cryptographically against the root certificate authority’s public key and certificate revocation list.

5.3.2 Support Trust in and Integrity of Data

The core functionality described in this section specifically aims to realise that the messages communicated can be trusted.

Trust relates to participants in an interaction (they are who they say they are), the information that is exchanged and the system used to interact. Something can be trusted when it can be unambiguously identified, operates exactly as designed and expected, does not do anything it was not designed to do (fit-for-purpose) and operates without interruption. Naturally, the longer the system works as expected, the more users are likely to trust it (CSIRO 2011).

In C-ITS there will be frequent encounters between vehicles that have never interacted before. A support system is needed that allows a sender and a receiver who did not have any prior interaction to securely send and receive messages and trust that the messages are authentic. Budapest University of Technology and Economics (2013) states that trust in C-ITS requires:

- globally unique identifiers
- related registries
- certification labs
- trust authorities
- public key infrastructure.

These are provided by a security credential management system (SCMS), which was described in detail in Section 5.3.1. The SCMS plays a key role in achieving trust in the sender of a message.

In addition to having trust in the sender of the message (authenticity), many applications will also need trust in the message itself (integrity). That is, that the contents of the message are accurate, timely, and generally are fit-for-purpose.

As highlighted in Figure 5.6, a key function under *Content Processing* is a quality or integrity check. For safety-critical applications, it will be a key requirement that these applications can trust various data messages and attributes that they are using. For example, if the position of a vehicle in a basic safety message is out by 10 metres, if the speed zone data in an IVI message is 20 km/h above the correct limit, or the red light timing in a SPaT message is wrong by even a second, the lack of integrity with these messages could cause road crashes, not avoid them. Thus, trust in the integrity of the data messages in these cases is critical.

Work is being progressed internationally on determining which data messages and attributes should have integrity checking, and how these integrity checks should operate. Australia and New Zealand will need to follow this as it progresses, and ensure that it is appropriately captured in future system requirement documents.

5.3.3 Assurance of Privacy

The core functionality described in this section is specifically to enable an appropriate level of privacy assurance.

Due to the potential of some of the C-ITS data to be linked to an individual, the issue of privacy is a real concern that will need to be appropriately addressed. Where required, elements of C-ITS will need to demonstrate compliance with the relevant privacy acts, surveillance acts and privacy principles, at both national and state level.

Further to this, it is proposed that a privacy-by-design approach be taken with all elements of C-ITS and the system as whole. This is an approach to systems engineering which takes privacy into account throughout the whole engineering process. This includes building privacy protection into the information and communications technologies, the business processes, and the physical systems. The NTC Final policy paper (National Transport Commission 2013) on its review into C-ITS regulatory policy issues, which was endorsed by SCOTI in November 2013, recommended that a privacy-by-design approach be taken in the development of the local C-ITS operational framework.

Key elements of C-ITS for which privacy will need particular attention are described below.

Data messages

As detailed in Section 3.3.6, there will be a wide range of standardised data messages transmitted and received within the C-ITS environment. Many of these messages will contain data attributes that could potentially be used to identify an individual. For example, the standard basic safety message that is proposed to be transmitted by C-ITS equipped vehicles up to ten times per second will likely contain:

- a temporary ID number
- time
- position
- speed
- heading
- acceleration
- vehicle size.

Also, the messages will be accompanied by a certificate which will be encrypted.

According to recent amendments to the *Privacy Act 1988* and associated privacy principles in Australia, personally identifiable information (PII) includes not just data that contains data that could reasonably identify an individual, but also data that could reasonably be joined with other readily accessible data to then identify an individual.

While the final design of how data messages will be handled and the SCMS have not yet been finalised internationally, there are a number of concepts that have been developed and trialled that are intended to address privacy concerns with the data messages. These include:

- the PKI approach using short-term pseudonym certificates
- the unique ID being a rolling ID that changes over time
- data messages captured by another ITS-station only being maintained for as long as they are still serving the intended purpose
- consent or opt in being required from vehicle owners for those authorities and service providers that wish to capture historic data from vehicles to use for various purposes.

A primary enabler of privacy is the PKI approach using short-term pseudonymity certificates. Similar to a rolling ID, frequently changing pseudonym certificates ensure that outsiders cannot monitor a device for a period longer than that for which the short-term pseudonym certificate is used. This period has not been determined but initial plans suggest between five minutes and a week (Schulman 2012). The other reason why a PKI ensures privacy is that it separates registration and certificate issuing in different authorities and different systems. This means that no single authority will be able to link personal data with the constantly changing ID and certificates.

Data management (including capture, storage and access)

A significant amount of data will be created by C-ITS. With data being created and potentially accessible from a large range of road users, much of which previously did not exist or was not accessible, the resultant scenario could be described as *big data*. The term refers to a collection of data that is so large and complex that it becomes very difficult for traditional relational database tools to be of much use.

While the creation of more data may appear to provide significant opportunities for service providers and authorities to create value-added services and improved outcomes, there are potential privacy concerns that will need to be considered with the management of this data.

Depending on the jurisdiction, there may be a relevant Surveillance Act which could restrict what data can be collected, particularly if it has the potential to identify and track an individual's location. Further to this, relevant privacy legislation and privacy principles may then restrict what any captured data can be used for.

In Australia, amendments to the *Privacy Act 1988* and the Australian privacy principles came into effect in March 2014. Implications from these instruments that are relevant to the management of C-ITS data include the following:

- Personally identifiable information (PII) includes not just data that can reasonably identify an individual, but also data can be used in concert with other reasonable accessible data to then identify an individual.
- Consent should be sought prior to capturing PII data, and users must be notified of the intended purpose of collecting the PII data at the point it is collected.
- Consent must be kept up to date, and users must be informed of when their data may be used for a different purpose to what was communicated when it was collected.
- PII data should be destroyed or de-identified once it has outlived the stated purpose for which it was collected.
- Individuals must have the option of dealing with an organisation anonymously or pseudonymously, unless identification is required by law or where it is impractical to deal with the individual this way.

The NTC final policy paper (National Transport Commission 2013) recommended that specific legislative protections for C-ITS may need to be considered, in the event that it is deemed that individuals can be reasonably identified by the data created and managed with C-ITS. Further progress with the data message and data management standards for C-ITS will need to occur before this decision can be made.

The paper also recommended that, with regard to the institutional arrangements for C-ITS, any entity that manages and stores unique identifiers of C-ITS devices is a separate entity to those that hold driver licensing and vehicle registration data.

5.3.4 Facilitate a Platform for Sharing of Information and Efficient Use of Resources

C-ITS share information between applications in a single C-ITS device and those running in different C-ITS devices and include, amongst others, the following features (Schade 2012b):

- information between any C-ITS device (vehicle, roadside, central and mobile)
- information between applications in a single C-ITS device
- resources (communication, positioning, security) by applications in a C-ITS device.

The objectives of this function are to realise better C-ITS services in a more efficient way. This requires the following functions:

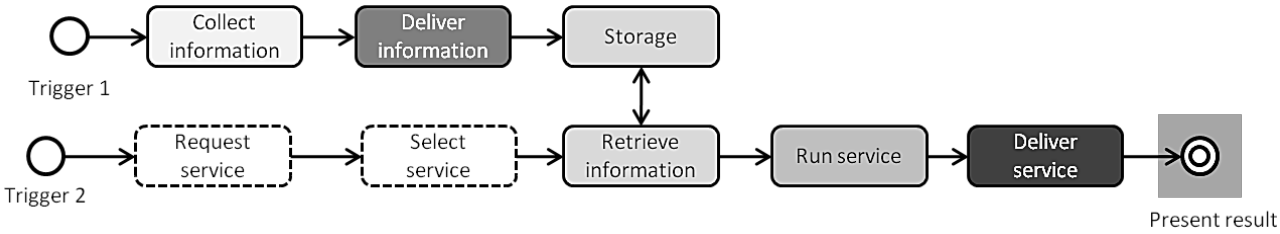
- a publish-subscribe function with a registration of which devices subscribe to which services that enables more efficient targeted communication
- an opt in/opt out function that enables C-ITS users to indicate which information they would like to share.

There are a number of issues which need to be solved. For data capturing and storage, rules on what can be captured and stored need to be agreed, both from a business model and a privacy perspective. Other than some commercial telematics services, there is currently no process for a user to opt in or out of a C-ITS service. There is currently no process to authorise the use of information for purposes other than the original intent. Anonymising data will therefore play an important part of C-ITS service provision. Either way, a system will be required to facilitate the subscription to C-ITS services (publish-subscribe) and the subscription to sharing data (opt in/opt out).

The sharing of information also requires several other functions including communication, data storage, processing/aggregation and data communication/service delivery. These are not core functions and therefore not part of the scope as they can be performed independently and do not need coordination between stakeholders. The core functions are those that require coordination between different system components.

ISO 17427 Co-Operative Systems — Roles and Responsibilities in the Context of Co-Operative ITS Based on Architecture(S) for Co-Operative Systems provides the 'sequential process' architectural perspective of the use of data in C-ITS service delivery as shown in Figure 5.7. The traditional life cycle for data services consists of a single chain going from data collection to data processing to information delivery. In C-ITS the service delivery is triggered by a service request.

Figure 5.7: Sequential process description

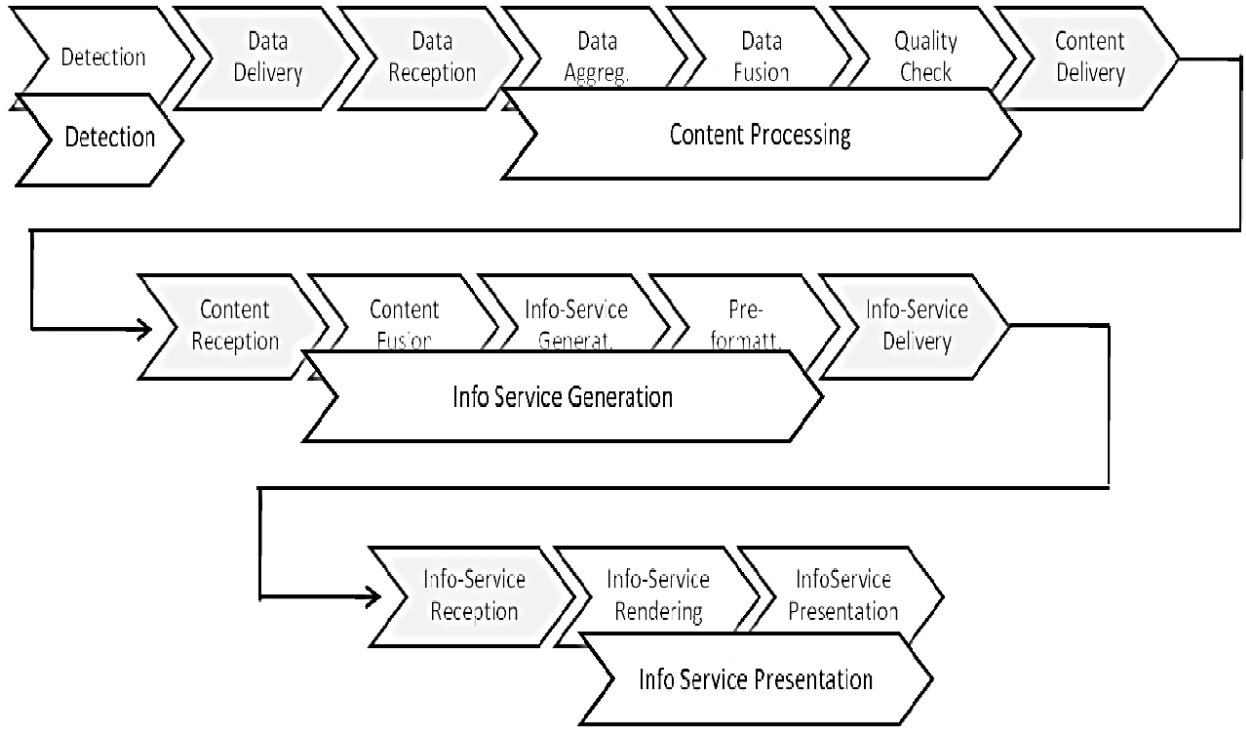


Source: ISO 17427.

The current data collection and distribution value chain is described in Figure 5.8. The chain includes mechanisms to ensure trust, but also the application. Some potential changes are

- Functions such as data aggregation and data fusion, part of the content processing in Figure 5.8, might be extended from the back office (centre) into the vehicle.
- Functions for ensuring integrity and trust such as quality checks, part of the content processing in Figure 5.8, might be extended from the back office (centre) into the vehicle.
- Functions such as content fusion and information service generation, part of the information service generation in Figure 5.8, might be extended from the back office (centre) into the vehicle.

Figure 5.8: General life-cycle process description



Source: ISO 17427.

5.3.5 National Interoperability and Consistency

The core functionality described in this section is specifically to enable a nationally interoperable platform that facilitates nationally consistent service availability and quality for end users.

National interoperability means that C-ITS applications and devices are able to communicate (technical interoperability), use the same data formats (syntactic interoperability) and understand the meaning of each other's communication (semantic interoperability). Additionally, different organisational processes need to be in place to enable different organisations to cooperate (organisational interoperability).

Consistency of service means that:

- the same services are available throughout different states and territories
- an application works and behaves in the same way under similar conditions throughout different states and territories.

This requires specifying how an application should operate. It might also require a national set of rules about which information is shared under which conditions. Standards are important for C-ITS as they can provide these specifications and enable two or more entities within the C-ITS environment to interact in an interoperable manner. However, the standards alone do not ensure interoperability between two or more entities unless the required standards are complied with. For those standards deemed critical to enable C-ITS, evidence of compliance with the relevant standards will likely be required.

Compliance of products and services in the Australian and New Zealand market with standards is normally voluntary, unless they are regulated. Regulation by government may be considered if the standards for the products and services relate to safety or address environmental or consumer protection. Other factors may also warrant regulation by government.

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 provides the purchaser or user assurance that the product or service complies with the relevant standards defining its use. As outlined in National Transport Commission (2013), Australian Standards (AS 1700 series and the related HB 68 series of handbooks) 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:

1. Third party certification: involves an independent assessment of compliance by an accredited body. For example, the United Nations Economic Commission for Europe (UNECE) regulations requires third party certification of vehicles (tested or witnessed by). The Australian Design Rules (ADRs) for vehicles also follow this model.
2. 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.
3. 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 country. Evidence of compliance generally needs to be submitted to a governing body to assess and grant type approval (also known as homologation) (e.g. ADRs).
- Audit/surveillance: to verify that a product is complying with the requirements when in service/operation (e.g. vehicle roadworthiness inspections).

Compliance assurance for C-ITS might be on several levels, being the application level, the core or platform level and the physical device level. The draft ISO standard *Classification and Management of ITS Applications in a Global Context* (ISO TS 17419), proposes certification on two levels, being the C-ITS application level and the platform level. The platform consists of the physical devices and the ITS-S platform functions, which include the proposed core functions.

Some components of C-ITS devices are in existence already, like the current telecommunication equipment, and will be tested as currently being done. Other components might need additional testing requirements and procedures. As C-ITS are frequently safety-critical, highly dynamic and complex systems and built on subsystems from different organisations working together, an organisation that is responsible for both the platform and working applications at the end-to-end level is recommended, as proposed in ISO TS 17419.

Which standards will be applicable to the core functions, the C-ITS platform in general, and to C-ITS applications is to be determined in later stages of the systems engineering design process.

5.3.6 Functional Subsystems

The core functions have been grouped into seven functional subsystems, all performing sub-functions that contribute the C-ITS core functions. The functional subsystems are the following:

- data distribution
- misbehaviour management
- network services
- service monitor
- time synchronisation

- user permissions
- user trust management.

These subsystems are described briefly below. The definition of the functional subsystems is based on the US C-ITS core Concept of Operations (Research and Innovative Technology Administration 2011), however other internationally emerging platforms use similar concepts and similar functions (see Figure 5.9 for a mapping of the functional subsystems to the detailed ITS-station reference architecture).

All functional subsystems will be present in each individual C-ITS device, whether an in-vehicle, a mobile, or roadside device or a centre. Most functions will be implemented differently in the different types of ITS devices. For example, when comparing the misbehaviour management functions in a vehicle ITS-station and a centre ITS-station, the misbehaviour management in a single vehicle might be limited to basic checks for misbehaviour based on the messages that the vehicle receives, plus forwarding suspicious messages to a centre. The centre can detect misbehaviour by comparing messages and misbehaviour notifications from several vehicles. Even though the detailed design will have to determine more precisely how these centralised or decentralised sub-functions will be implemented, all functional subsystems will likely be present to some extent in all four types of ITS-stations.

Data distribution

The data distribution subsystem has centralised and decentralised components. It maintains a registry recording which service each device has subscribed to. Each device, e.g. a roadside C-ITS unit can then send data to vehicles in their communication range that subscribed to it. It thus supports multiple distribution mechanisms, including source-to-points and publish-subscribe. This means it has to manage anonymising and be able to repackage the data it receives from data providers, stripping away the source header information while maintaining the message payload. It then sends the repackaged payload data to subscribers of that data.

Misbehaviour management

The misbehaviour management subsystem analyses messages in each ITS device and sends suspicious messages to a central system which can then identify if users operate outside of their assigned permissions. It identifies suspicious requests and maintains a record of users that provide false or misleading data, impede other users, or operate outside of their authorised scope. It will determine when to revoke credentials from such reported misbehaving users. How the misbehaviour checks will be implemented is not clear yet, and neither is the extent to which these checks will be decentralised (in vehicles, mobiles or roadside units) or centralised (in centres).

Network services

The network services subsystem provides management for communication layer resources. Each C-ITS device makes decisions about which communication medium to use when more than one is available following the hybrid communication concept, which means that service provision on the roads and in the vehicles will rely on different communication technologies (ISO 21217; Amsterdam Group 2013). The network services subsystem is also responsible for protecting the system from cyber threats.

Service monitor

The service monitor subsystem monitors the status of core functions, interfaces, and communications networks. Monitoring is likely to have both decentralised and centralised components. Status information provided by service monitoring functions can inform travellers of the availability and reliability of the C-ITS services and application being used.

Time synchronisation

This subsystem makes a time base available to services on each C-ITS device. This function will be provided by the GNSS. No additional subsystem needs to be developed.

User permissions

This subsystem verifies whether a system user is authorised to perform the action requested in the message payload. It therefore maintains the status of system users and operators, maintains their allowed behaviours (publish, subscribe, actions allowed to request, administrate, etc.). A central system also accepts and acts upon user permission change requests provided by misbehaviour management. This subsystem also performs encryption-related functions such as encrypting and decrypting messages and management and storage of keys.

User trust management

The user trust management subsystem manages trust between and among system users and the core by providing digital certificates that system users can use to demonstrate that they are legitimate users. It provides digital certificates to qualified users and accepts notification of misbehaving users from the misbehaviour management and revokes the certificates of misbehaving users. It also maintains the certificate revocation list (CRL).

Most of the sub-functions contribute to several of the core functions. Table 5.1 shows which sub-functions contribute to each core function.

Table 5.1: Functional subsystems used for each core function

		Functional subsystems						
		Data distribution	Misbehaviour management	Network services	Service monitor	Time synchronisation	User permissions	User trust management
Core functions	Secure data exchange					✓	✓	
	Provide trust		✓		✓	✓		✓
	Assurance of privacy		✓				✓	✓
	Facilitate a platform	✓		✓				
	Assurance of national interoperability						✓	

Table 5.2 shows the relationship between the subsystems and the needs defined in Section 4.1.3. In most cases, a subsystem will satisfy multiple needs and in some cases needs may be satisfied in multiple subsystems.

Table 5.2: Subsystem to needs traceability matrix

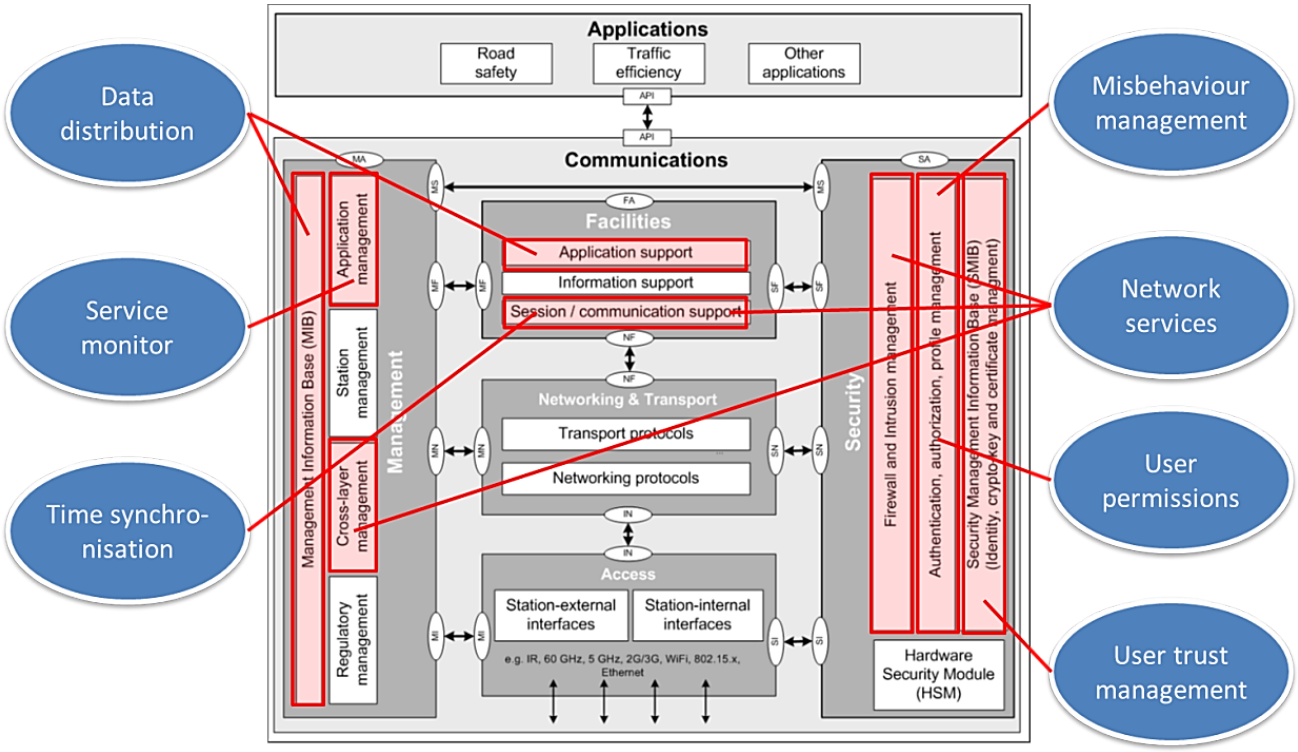
Subsystem	Needs
Data distribution	Data request, data provision, data forward, geographic broadcast, anonymity preservation
Misbehaviour management	Misbehaviour management, core trust revocation, system user trust revocation
Network services	Network connectivity, core data protection, private network connectivity, private network routing
Service monitor	Core service status, system integrity protection, system availability, system operational performance monitoring, core data protection
Time synchronisation	Time base
User permissions	Authorisation verification, authorisation management, core data protection, anonymity preservation
User trust management	Data protection, core trust, system user trust, core trust revocation, system user trust revocation, core data protection

A breakdown of the functional components into more specific functions of the detailed ITS-station reference architecture is set out in Figure 5.9. This shows a mapping of the functional subsystems to the functions of the detailed ITS-station reference architecture as follows:

- The *data distribution* functions are equivalent to the *management information base* functions and the *application support* functions in the ITS-station reference architecture.
- The misbehaviour management functions are part of the authentication, authorisation and profile management functions.
- The *network services* include *firewall and intrusion management* and the selection of the communication medium. The *selection of the communication medium functions* are part of the cross layer management in the ITS-station reference architecture. Communication profiles for applications are defined as part of the *session/communication support* in the facilities layer.
- The *service monitor* functions are part of the *application management* functions.
- The *time synchronisation* functions are part of the *application support* functions.
- The user permissions functions are part of the authentication, authorisation and profile management functions.
- And the user trust management functions are part of the security management information base functions.

This provides an indication of the interfacing between the core and the other parts of C-ITS. The detailed implementation will be further specified in the detailed design phase.

Figure 5.9: Core subsystems mapped to detailed ITS-station reference architecture



Source: Modified from ISO 21217 draft international standard.

5.3.7 Core Data

Some of the data messages used to perform the core functions are the following. Many of these messages are still being developed:

- Security certificates

  Security certificates are used in the public key infrastructure by C-ITS devices and services to sign messages so the receiver knows that the message is from a trustworthy source. Security certificates are uploaded onto C-ITS devices by a certificate authority once the device is tested for compliance with the appropriate standards and requirements and has been registered. Different applications and services may have different security certificates. Certificates are valid for a limited amount of time (e.g. 5 minutes or a day) and vehicles will have several simultaneously valid certificates, which makes it difficult to track a vehicle by following its trail of certificates.

  The exact form of the security certificates is still being developed and tested. Two security standards are currently being developed, one by IEEE and one by ETSI, each with a different format. Harmonisation of these standards is currently being discussed, but the outcome is still to be determined.

- Certificate revocation lists

  Certificate revocation lists are used for misbehaviour management to expel misbehaving C-ITS devices for the secure bounded managed domain. The emerging US and EU platforms are only starting to determine how to implement misbehaviour management. It is not clear if certificate revocation lists will be sent to vehicles as a core data message. The large size of the certificate revocation lists could create communication capacity issues.

- Misbehaviour report

  Misbehaviour reports are used to identify misbehaving C-ITS. The emerging US and the EU platforms are only starting to determine how to implement misbehaviour management. It is not clear what the reports will look like and whether they will be sent to a centre for centralised management or to C-ITS devices in vehicles or roadside ITS equipment for decentralised misbehaviour management.

- Service announcement messages

  Permission requests and permission confirmation messages are authorisation mechanisms to define roles, responsibilities and permissions for other connected vehicle applications. This allows application administrators to establish operational environments where different connected vehicle system users may have different capabilities. For instance, some emergency services may be authorised to request signal priority, or some traffic management centres may be permitted to use the geographic broadcast service, while those without the permissions would not.

  An example of a standards specifying this type of message is the service announcement messages (SAM) which provides a list of locally available and activated services and the communication profile being used to access and execute each service.

5.4 Modes of Operation

Typically, engineered systems have various modes of operation, such as operational, degraded, maintenance, emergency, active, and idle modes.

The proposed C-ITS core functions operate on different devices as part of the system of systems. These individual devices will have different modes of operation. Even though individual devices may stop working (permanently or temporarily), the C-ITS 'ecosystem' will keep operating as a system of systems. This is similar to how the internet operates consistently, even though a single server or cluster of servers does not function or is in a non-standard mode of operation.

Consideration will need to be given to the following:

- Secure exchange of data – the security credential management system (SMSC), providing security certificates, has to be designed for different operating modes. C-ITS devices are likely to have certificates stored for a period of time, so a temporarily failing SMSC will not directly have critical consequences for the operation of C-ITS services. Additionally there is likely to be redundancy in the form of independent servers providing certificates, so the system will not depend on one individual server.
- Trust and integrity of data – while C-ITS roadside infrastructure (as part of e.g. traffic signal systems, variable speed limit signs, lane use management systems) is likely to have a very high operational availability, there will be times when services are not available. Applications using this data will not be able to provide the service for this location and will likely develop ways of indicating this to the end user. This is part of the application and its interface with the user.
- Assurance of privacy – those systems that will manage personally identifiable information need to be designed in line with privacy guidelines for all modes of operation.
- Facilitation of a platform for sharing and efficient use of resources – requests for opt in or opt-out of information sharing and registration of services can be expected anytime. Systems for opt in or op-out of information sharing and registration of services need to be designed for all their modes of operation.
- National interoperability and consistency – the systems and processes for compliance assurance with standards are unlikely to be as dynamic and time-critical as those described above. However, the modes of operation will still need to be considered in the design phase.

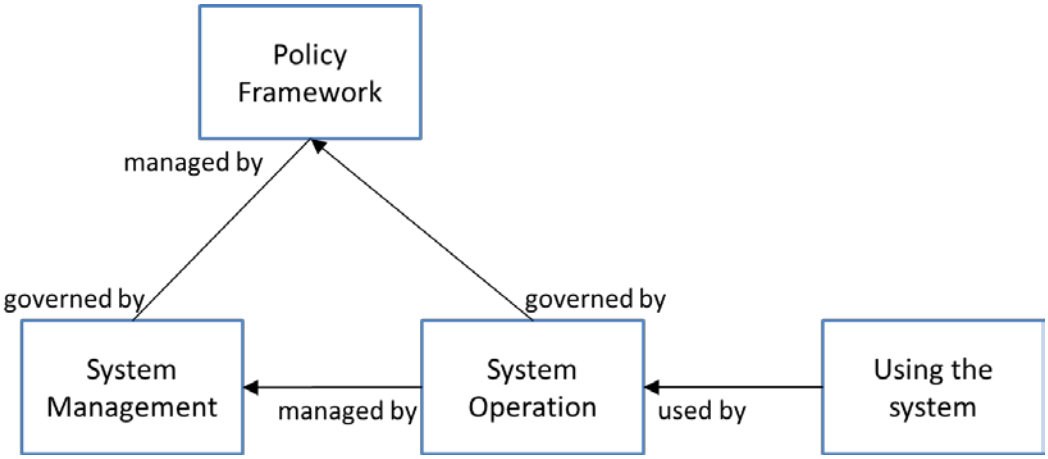
As system requirements are still evolving, detailed consideration of the modes of operation will be developed for individual devices and subsystems in their development.

5.5 Organisational Structure

This section describes the likely organisational approach to the governance and management of the core functions, and includes an overview of the stakeholder types that will be involved and their proposed roles and responsibilities. A list of stakeholders can be found in Section 1.3.4.

The high-level organisational architecture defined ISO 17427 *Roles and Responsibilities in the Context of Co-Operative ITS Based on Architecture(s) for Co-Operative Systems*, has been a reference and guide for the details in this section. Figure 5.10 shows the high-level roles as defined in the draft ISO standard.

Figure 5.10: High-level organisational architecture



Source: Modified from ISO 17427.

Section 1.3.4 provided detail on these four categories of roles. The following provides a summarised description of each:

- **Policy framework** – responsible for all governing and institutional activities in the system. This includes governing the system management and system operation roles. Responsibilities within this role include defining the regulatory and non-regulatory policies, defining the standards and guidelines, and ensuring that standards, guidelines, laws and regulations are followed and applied.
- **System management** – responsible for the management activities within the system. This role is governed by the policy framework role, and provides direct management and support to the system operation role. Responsibilities within this role include designing, testing, deploying, maintenance, support, access, security, confidentiality, integrity, configuration, update and change management activities for C-ITS.
- **System operation** – responsible for activities related to the operation of the system. This role is supported by the system management role, and provides services directly to the end users. Responsibilities with this role include provision of content, provision of services, and presentation of the service results to the end user.
- **End user** – responsible for requesting, receiving and using the end C-ITS application or service. This role has a close relationship with the system operation role. Responsibilities within the role include issuing a service request, recognition of service result presentation, and judging the need for reaction and reacting accordingly.

It is important to note that stakeholders can perform several roles across these categories, and that roles can be performed by more than one stakeholder.

A suggested approach to defining potential roles and responsibilities with regard to the core C-ITS functions is summarised in Table 5.3. This has been guided in part by the ISO 17427 standard on roles and responsibilities. Also, consultations were held with a range of local and international stakeholders regarding the potential roles and responsibilities within the emerging cooperative intelligent transport environment. Feedback received from these stakeholder consultations has also been used as an input to Table 5.3.

Table 5.3: Stakeholders and responsibilities regarding the C-ITS core functions

Role	Description	Possible responsible stakeholders
Policy framework		
Establish government policies relevant to C-ITS	Potential need to establish policies relating to: • safety-critical applications • privacy and surveillance with C-ITS data • security • roles and responsibilities • use of C-ITS core functions by service providers.	Government departments and agencies
Establish regulation, legislation, and/or industry code	Potential need to establish or make changes relating to: • privacy and surveillance laws • tele- or radio communication rules • a specific C-ITS industry code.	Government departments and agencies Industry associations
Define standards and guidelines requiring compliance	Need to determine a minimum set of agreed standards and guidelines with which C-ITS should comply including which regional standards to harmonise with.	Government departments and agencies Standards organisations Industry associations
Establish policy, governance and management frameworks for assuring compliance with standards and guidelines	Need to determine and establish policy, governance and management frameworks for assuring compliance with agreed standards and guidelines. This will then govern the system management functions relating to the certification and potential audit of devices, applications and services.	Government departments and agencies Standards organisations Industry associations Centralised management entity (TBD)
System management		
Establish operational rules and processes for assuring compliance with standards and guidelines	Establish operational rules, processes and responsibilities for ensuring compliance with standards and guidelines. This may include certification of devices, applications and services at deployment, and possibly also in-service audits.	Government departments and agencies Austroads Industry association Centralised management entity (TBD)
Managing ITS use of 5.9 GHz DSRC communication	Need to determine and establish management and operational rules for the use of ITS in the 5.9 GHz band, including for: • rules for use of ITS in 5.9 GHz band • licensing of 5.9 GHz DSRC devices • coordination and auditing of roadside units • referral and escalation point for coexistence criteria and interference issues.	Centralised management entity (TBD) Austroads (interim)
Enabling other communication (non 5.9 GHz DSRC) between ITS-stations	Establish technical and operational arrangements that will support a hybrid communication approach within an ITS-station.	Telecommunication companies Equipment manufacturers Service providers
Establish operational rules and processes for registration of C-ITS devices (registration organisation)	Establish operational rules and processes for registration of C-ITS devices. The responsible stakeholder should be a different entity than the security certificate authority.	Government departments and agencies Austroads Industry association Centralised management entity (TBD)

Role	Description	Possible responsible stakeholders
Security credential management	Need to design, establish and operate a security management system, which supports 5.9 GHz DSRC and other communication technologies. Functions may include managing and issuing security certificates.	Certificate authority Centralised management entity (TBD)
Misbehaviour detection management	Detect misbehaviour and revoke certificates.	Dedicated misbehaviour detection management entity Centralised management entity (TBD)
Provide linkage values to the registration authority	To prevent any SCMS component from tracking non-revoked vehicles, linkage values (that are used as revocation values) and certificate IDs are generated by different entities (linkage authorities).	Linkage authority Centralised management entity (TBD)
Development of C-ITS devices, applications and services	Includes design, development, testing and deployment of C-ITS devices, applications and services.	Equipment manufacturers Software companies Service providers Automotive companies Road operators Telecommunication companies
Maintenance and support of C-ITS devices, applications and services	This role is intended to support the system operator and the end user of a C-ITS device, application or service. It could include scheduled and unscheduled maintenance and fixes, technical support, etc.	Service providers Automotive companies Road operators Telecommunication companies
System operation		
Provision of content	Content may include data about road traffic conditions, speed zones, intersection geometry, signal phase and timing, etc. For some data, there may be a requirement to improve trust (e.g. safety-critical data attributes). Some data will likely be provided by road agencies and other data (probe data) by traveller opted in to certain services.	Service providers Road operators Traveller/ end user
Provision of applications and services	Includes the processing of content and the operation of applications to create a service for the end user.	Service providers Road operators Automotive companies
Presentation of results to end users	Refers to how the end service is presented to the user. This will include determining if to use a visual HMI, audible warning, or a haptic response (or a combination of these). Some responses may be automated.	Service providers Road operators Automotive companies
End user		
Use of C-ITS applications and services	This refers to the end users of C-ITS. Responsibilities limited to potentially issuing a service request, recognition of service result presentation, and judging the need for reaction and reacting accordingly. Opting in to the use of certain services may come with the obligation to share data.	Road users Road operators Fleet managers

5.6 Support Environment

This section describes the support concepts and support environment for the proposed core functions.

These typically include the support agency or agencies; facilities; equipment; support software; repair or replacement criteria; maintenance levels and cycles; and storage, distribution, and supply methods (IEEE 1362).

As some of the concepts and requirements for the core functions are still emerging internationally, it is considered too early at this stage to be able to determine much detail on the support environment. However, the following provides a high-level overview of some of the key systems and entities that will need to be considered:

- SCMS – will play a critical role in enabling the core functions, particularly the secure exchange of data, trust in data, and privacy assurance. While the conceptual model for the SCMS is still evolving, it is very likely that the system support activities will align with an internationally recognised system management framework, such as ITIL v3. The system management role detailed in ISO 17427, and discussed briefly in Section 5.5, is based on ITIL v3. Also, the outputs of the EU-US Harmonisation Task Group 6 on security policy should also be used to guide the required support environment.
- Assurance of compliance – compliance with standards that enable interoperability and ensure safety is maintained will be critical. Work is progressing internationally on determining those standards that will require compliance, and what level and type of compliance may be necessary. Austroads is also finalising an assessment on international C-ITS standards that will assist with local decision making. Once established, licensing, certification and audit systems will be critical in enabling the C-ITS core functions. As with the SCMS, it will be important that these systems have an appropriate support environment, aligned with a recognised system management framework.
- ITS managed by road operators – these ITS will play a critical role as inputs to, and support of emerging C-ITS applications. For those ITS that will be relied upon by other C-ITS entities, such as ITS infrastructure for broadcasting SPaT and IVI messages (e.g. speed zone), road operators will need to ensure they have appropriate procurement, maintenance and support processes in place. Similar to what is proposed for the SCMS, consideration may need to be given to aligning with a recognised system management framework, such as ITIL v3, for these support activities.
- Vehicle systems – the maintenance and support of vehicle systems, including not only their C-ITS equipment but also other associated sensors and systems, will need to be considered. The vehicle servicing programs set by OEMs, and also the periodic roadworthy regimes overseen by government agencies, may need to be modified to ensure that the C-ITS-related vehicle systems are appropriately maintained and supported.
- Communication equipment and providers – given a hybrid approach to C-ITS is proposed, it will be important for not just communication equipment vendors, but also communication providers to ensure that their support environments are appropriate for C-ITS.
- Global navigation satellite services (GNSS) – these systems are considered out of scope for the C-ITS core functions, they will play a critical support role in providing absolute positioning (latitude, longitude, altitude) and timing (UTC) data that many C-ITS applications will rely upon. Thus, consideration will need to be given to the levels of support that GNSS providers have, and also to any authentication and integrity check functions that are established locally.

6. Operational Scenarios

The core functions, which are in the scope of this Concept of Operations, are intended to facilitate secure and trusted communication between ITS-stations, and ultimately to enable emerging C-ITS applications to be deployed and to operate effectively.

The operational scenarios that are in focus are therefore the different conceptual communication scenarios that are emerging. The end-user applications that are enabled by these scenarios are not in scope, but may be used as appropriate to explain communication scenarios.

This section describes typical communication scenarios (Section 6.2) and how the core functions are applied as part of C-ITS communication in two of the operational scenarios (Section 6.2 to Section 6.6).

6.1 Communication Scenarios

The EU-US harmonisation task force (2012a) has categorised communication systems as shown below. This highlights the range of communication characteristics that need to be considered.

Table 6.1: Communication characteristics

Communication characteristics	Classification
Traffic pattern	• Broadcast (one-way communication from a sender to any receiver in range) • Unicast (communication session connecting a single sender and a single receiver) • Geocast (one-way communication from a sender to any receiver in a certain geographical area)
Network mode	• Single-hop • Multi-hop
Time-criticality	• Critical • High • Low
Transaction size	• Small (single message) • Medium (multiple messages but transaction can be completed in the time it takes two vehicles to pass at high speed) • Large (larger than medium)
Transaction frequency	• Frequent (multiple times a second, generally a broadcast such as CAM/BSM) • Infrequent (once a second or less)
Endpoints	• V2V • V2I/I2V • V2C (vehicle to remote infrastructure, reached over a backhaul network)
Session*	• Individual messages • Unicast local session • Unicast session with a server remote over the network • Unicast session with a server remote over the network, which must be maintained across several V2I communication sessions
Protocol type	• Messaging • IP

** A session is a semi-permanent interactive information interchange or dialogues between two communication devices.*

Source: EU-US Harmonisation Task Force (2012a).

Communication scenarios are defined as combinations of these characteristics in their supporting communication systems. The EU-US Harmonisation Task Force (2012a) identified five communication scenarios:

- vehicle-originated broadcast
- infrastructure-originated broadcast
- infrastructure-vehicle-unicast
- local time-critical sessions
- local non-time-critical sessions
- multi-roadside unit sessions.

A communication scenario involving geocast or multi-hop was not considered by the EU-US Harmonisation Task Force. The emerging US platform does not facilitate geocast or multi-hop. The EU does have standards for geocast and multi-hop, but there is some debate as to whether they will be part of initial C-ITS deployments in Europe. Therefore, this Concept of Operations has not considered them, but there may be a need to revisit this in future.

The different C- ITS use cases and applications will require different communication scenarios. Typical communication scenarios for a number of C-ITS applications are defined by the EU-US Harmonisation Task Force (2012a). Note that a single application could use several communication scenarios depending on the conditions and availability of these scenarios.

Table 6.2: Examples of C-ITS applications and typical communication scenarios

Applications	Communication scenario	Examples
Safety applications		
V2V cooperative collision warning	Vehicle-originating broadcast	Forward collision warning, blind-spot warning, electronic emergency brake light warning, emergency vehicle approach warning, overtaking (do not pass) warning
I2V cooperative collision warning	Infrastructure-originating broadcast	Intersection collision/violation warning, vulnerable road user presence warning
Roadwork (work zone) warning	Infrastructure-originating broadcast	Low time-criticality, but safety critical
Mayday/SOS	Vehicle-originating broadcast	Also stolen vehicle alerts
Mobility applications		
Cooperative adaptive cruise control	Vehicle-originating broadcast	Extensions could include platooning
Multi-lane toll collection	Local time-critical session	
Probe data upload	Local non-time-critical session	
Local traffic data download	Local non-time-critical session	Also route guidance, point of interest info
In-vehicle signing	Infrastructure-originating broadcast	Static or slow-changing contents
Signal priority or pre-emption	Infrastructure-vehicle unicast	
Local access control	Infrastructure-vehicle unicast	Parking, loading zone mgt., tolling with barriers
Efficiency/sustainability applications		
Basic efficiency improvement	Infrastructure-originating broadcast	Broadcast SPaT, then vehicles determine speed profiles
Interactive efficiency improvement	Local non-time-critical session	

Applications	Communication scenario	Examples
Comfort/convenience/commercial applications		
Personal data synchronisation	Local non-time-critical session	Synch car computer to home PC
Customer relationship management	Local non-time-critical session	Include remote diagnosis, software updates
Fleet management	Local non-time-critical session	
Large media download	Multi-roadside unit session	
Web surfing	Multi-roadside unit session	(For passengers rather than drivers)
Concierge services	Multi-roadside unit session	

Source: EU-US Harmonisation Task Force (2012a).

The focus of the scenarios by the EU-US Harmonisation Task Force is on 5.9 GHz communication. The proposed hybrid approach will include cellular (3G/4G) based scenarios as well.

6.2 Vehicle-originated Broadcast

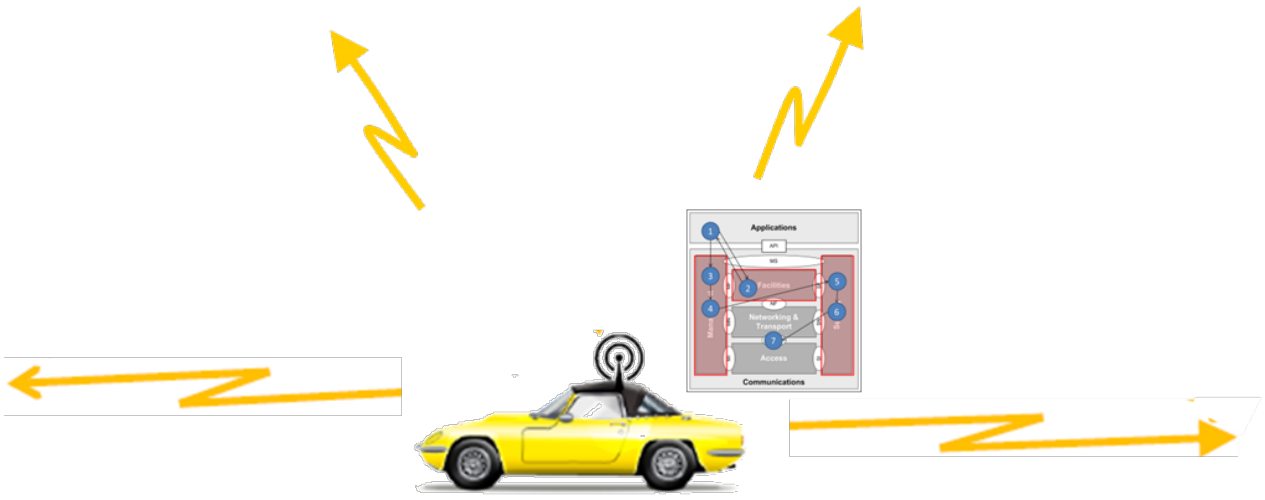
Vehicles broadcast information about their movements and safety-related attributes frequently to make sure that this information is available to other vehicles so that they can identify potentially hazardous situations or in support of other applications. Typical examples are the broadcast of time-critical safety related messages like:

- basic safety messages (BSM),
- cooperative awareness messages (CAM) and
- decentralised environmental notification message (DENM).

These are individual single-hop broadcast V2V or V2I messages, with the highest time-criticality and small but frequent transactions (EU-US Harmonisation Task Force 2012a).

Figure 6.1 shows the ITS-station of a vehicle broadcasting to other ITS-stations that are in range.

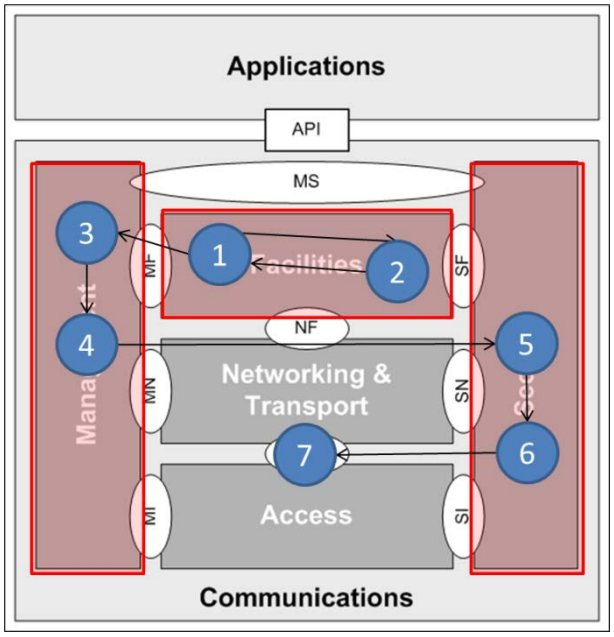
Figure 6.1: Vehicle-originated broadcast scenario (sending)



The scenario shows the steps for a C-ITS device in a vehicle to generate a message and broadcast it, and then for another C-ITS device to receive and use it. The scenario focusses on those steps performed by the core functions using the BSM as a use case. Note that the BSM message is generated in the *Facilities* layer. Messages can also be generated by applications in the application layer.

Figure 6.2 shows the path that the message takes from being created in the application layer (step1) to being physically sent through the antenna (typically 5.9 GHz DSRC) (step 7).

Figure 6.2: Vehicle-originated broadcast scenario (sending) – core functions



Source: Modified from ISO 21217 draft international standard.

The steps can be described as follows. The functional subsystem that performs the function is added in brackets:

1. Create a message, e.g. a BSM.
2. Include time stamp (time synchronisation).
3. Monitor the status of communication technologies (service monitor).
4. Select communication technology (network services).
5. Confirm if allowed to broadcast BSM (user permissions).
6. Add security certificate (user trust management).
7. Send message.

Note that not all subsystems are used in this scenario. The data distribution subsystem is not used because this is a broadcast scenario so there is no need to check if any of the possible receivers have subscribed to this type of message.

The misbehaviour management subsystem is not used either. This is only used for received messages.

After the message has been broadcast, it might be received by other C-ITS devices including in other vehicles or roadside infrastructure.

Figure 6.3 shows a vehicle receiving a message broadcast by another vehicle.

Figure 6.3: Vehicle-originated broadcast scenario (receiving)

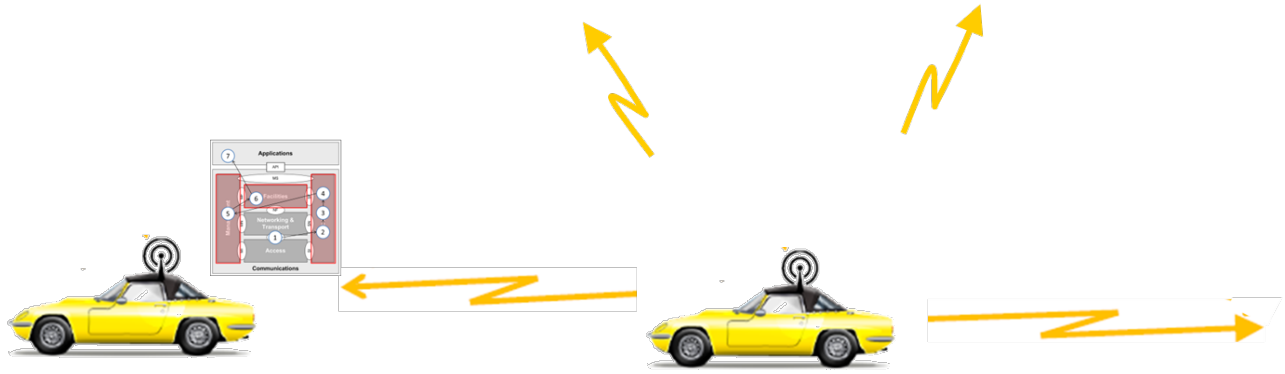
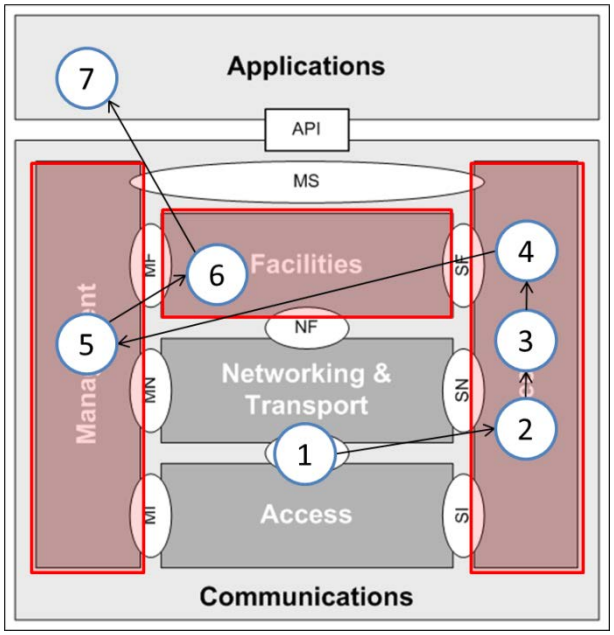


Figure 6.4 shows the path that the message takes from being received through the antenna (typically 5.9 GHz DSRC) (step1) to the usage of the message content in an application (step 7).

Figure 6.4: Vehicle-originated broadcast scenario (receiving) – core functions



Source: Modified from ISO 21217 draft international standard.

The steps can be described as follows. The functional subsystem that performs the function is added in brackets:

1. Receive message.
2. Check security certificate (user trust management).
3. Confirm if allowed to use BSM (user permissions).
4. Check for consistency, possibly forward to central management system (misbehaviour management).
5. Check if subscribed to this message type (data distribution).
6. Check timeliness (time synchronisation).
7. Use BSM.

Note that the network services subsystem is not used. The network services subsystem selects the communication technology, which is not part of the scenario of receiving a message. Also the service monitor subsystem was not used as no service availability needs to be checked to receive and use messages.

Examples of applications that could then use the BSM (as highlighted in Table 6.2) could include:

- V2V collision warning
- electronic emergency brake light
- overtaking (do not pass) warning
- mayday/SOS applications
- an advanced detection mechanism for traffic management systems
- cooperative adaptive cruise control.

6.3 Infrastructure-originated Broadcast

Infrastructure-originated broadcasts are used to disseminate data that are relevant to all vehicles in the vicinity of a specific road infrastructure location where a roadside unit is installed. Typical examples are the broadcast of time-critical safety related messages such as:

- signal phase and timing (SPaT)
- roadside alert (RSA)
- geometric intersection data (MAP)
- in-vehicle information (IVI).

These messages are individual, single-hop I2V messages, involving small transactions, with frequent transmission (EU-US Harmonisation Task Force 2012a).

The scenario shows the steps for a C-ITS roadside unit to generate a message and broadcast it, and then for an in-vehicle or mobile C-ITS device to receive and use it. The scenario focusses on those steps performed by the core functions using a Signal Phase and Timing (SPaT) message as a use case.

Figure 6.5 shows a roadside unit connected to a traffic signal broadcasting to other ITS-stations that are in range.

Figure 6.5: Infrastructure-originated broadcast scenario (sending)

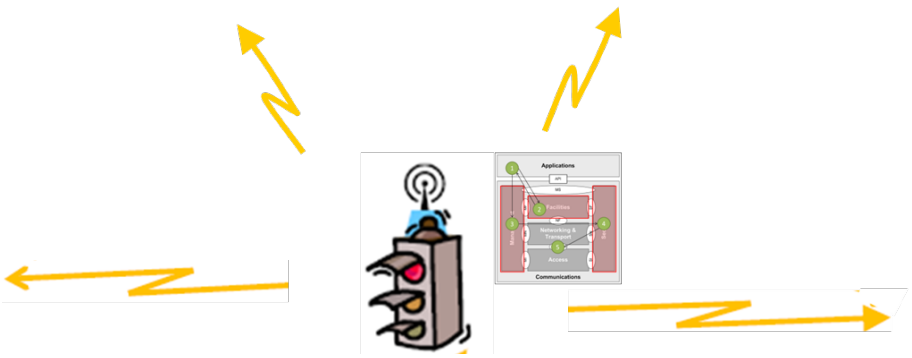
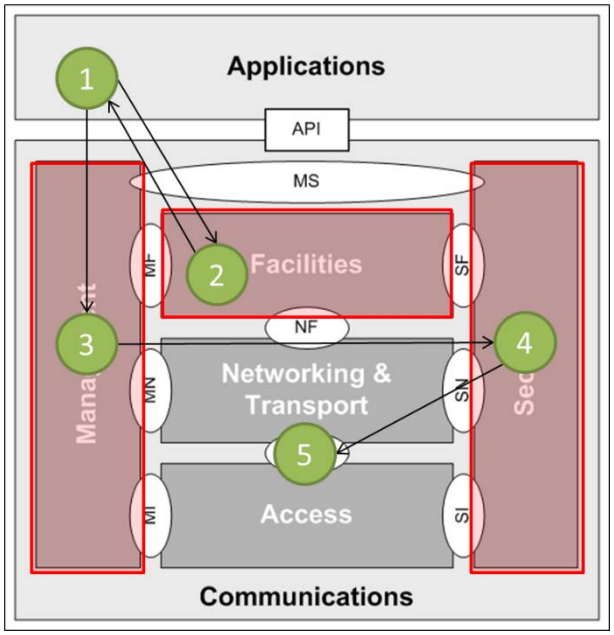


Figure 6.6 shows the path that the message takes from being created in the application layer (step1) to being physically sent through the antenna (typically 5.9 GHz DSRC) (step 5).

Figure 6.6: Infrastructure-originated broadcast scenario (sending) – core functions



Source: Modified from ISO 21217 draft international standard.

The steps can be described as follows. The functional subsystem that performs this function is added in brackets.

1. Create message, e.g. a SPaT message.
2. Include time stamp (time synchronisation).
3. Select communication technology (network services).
4. Add security certificate (user trust management).
5. Send message.

Note that not all subsystems are used in this scenario. The data distribution subsystem is not used because this is a broadcast scenario so there is no need to check if the any of possible receivers have subscribed to this type of message.

Also, steps 3 (*monitor the status of communication technologies*) and 4 (*select communication technology*) of the infrastructure-originated broadcast scenario may not be needed because most roadside units are likely to use only 5.9 GHz DSRC communication and no other technologies such as cellular communication.

The misbehaviour management subsystem is not used either. This is only used for received messages.

After the message has been broadcast, it might be received by in-vehicle or mobile C-ITS devices.

Figure 6.7 shows a vehicle receiving a message broadcast by a roadside unit.

Figure 6.7: Infrastructure-originated broadcast scenario (receiving)

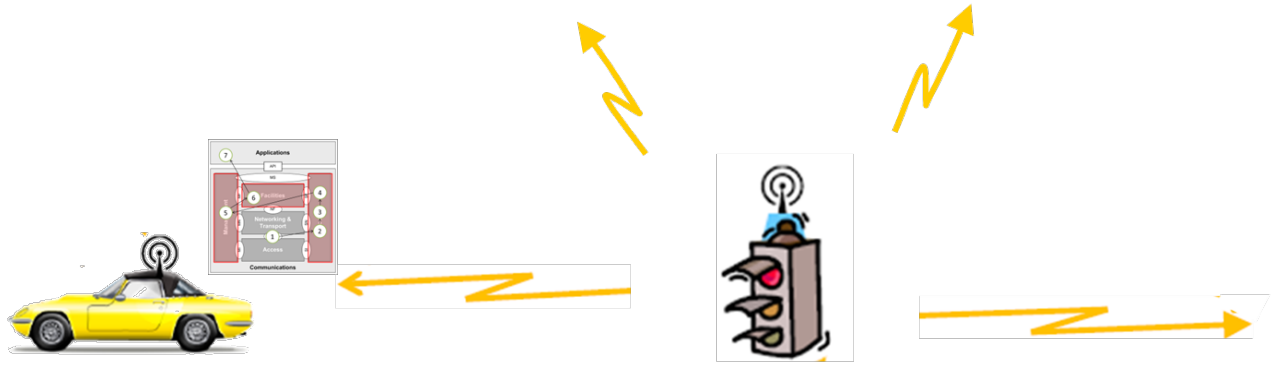
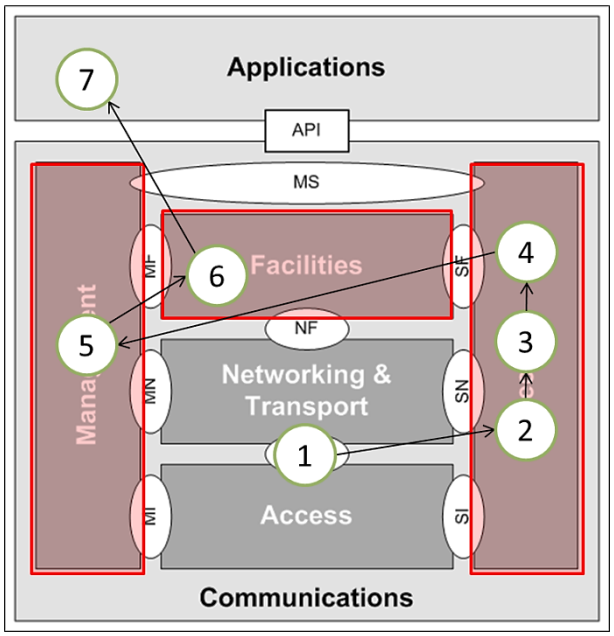


Figure 6.8 shows the path that the message takes from being received through the antenna (typically 5.9 GHz DSRC) (step1) to the usage of the message content in an application (step 7).

Figure 6.8: Infrastructure-originated broadcast scenario (receiving) – core functions



Source: Modified from ISO 21217 draft international standard.

The steps are the same as when a vehicle receives a message broadcast from another vehicle (Section 6.2) and can be described as follows. The functional subsystem that performs this function is added in brackets:

1. Receive message.
2. Check security certificate (user trust management).
3. Confirm if infrastructure was allowed to send SPaT message (user permissions).
4. Check for consistency, possibly forward to central management system (misbehaviour management).
5. Check if subscribed to this message type (data distribution).
6. Check timeliness (time synchronisation).
7. Use SPaT Message.

Note that the network services subsystem is not used. The network services subsystem selects the communication technology, which is not part of the scenario of receiving a message. Also the service monitor subsystem is not used as no service availability needs to be checked to receive and use messages.

Examples of applications that could then use the SPaT (as highlighted earlier in Table 6.2) could include:

- red-light violation warning
- intersection movement assistance
- eco-driving support.

6.4 Infrastructure-vehicle-unicast

Infrastructure-vehicle-unicast messages are individual transactions between a vehicle requesting a service from the infrastructure and the infrastructure responding to that vehicle about whether it can provide that service. Typical examples of these services are:

- traffic signal priority or pre-emption (vehicle sends an SRM, infrastructure responds with an SSM)
- access to a location such as a private parking facility
- potentially vehicle probe data (for example infrastructure sends a PDM, vehicle responds with PVD).

These messages are generally unicast local sessions with low time-criticality, low transaction frequency and small transactions (EU-US Harmonisation Task Force 2012a).

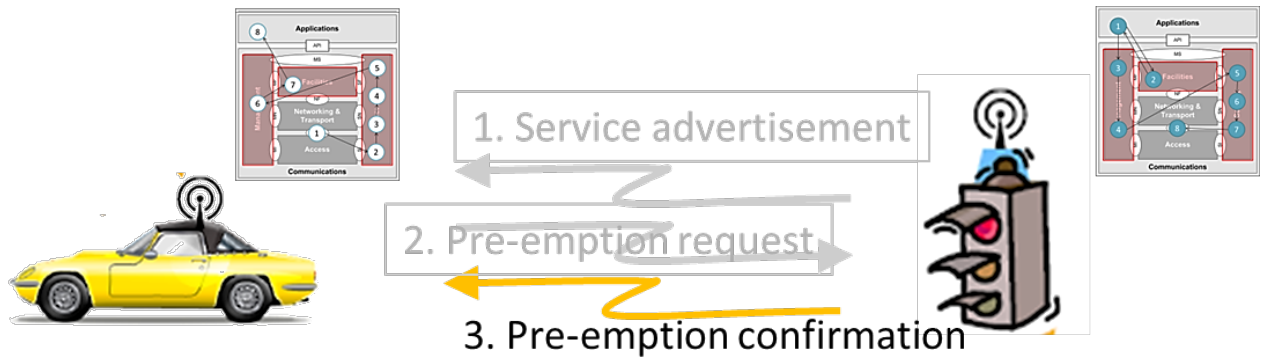
From a security point of view there are three ways to implement this type of communication scenario (EU-US Harmonisation Task Force 2012b):

- Messages from both sender and receiver are protected using security mechanisms for broadcast.
- The first message from the C-ITS device in the vehicle is protected using security mechanisms for broadcast, subsequent messages are protected using security mechanisms for a session.
- All messages are protected using security mechanisms for sessions with pre-arranged keys.

This scenario describes the exchange of messages protected using security mechanisms for a session. This means that messages are encrypted.

Figure 6.9 shows a traffic signal roadside unit sending a pre-emption confirmation to a vehicle. The unicast message is part of a series of messages and follows a service advertisement and a pre-emption request message.

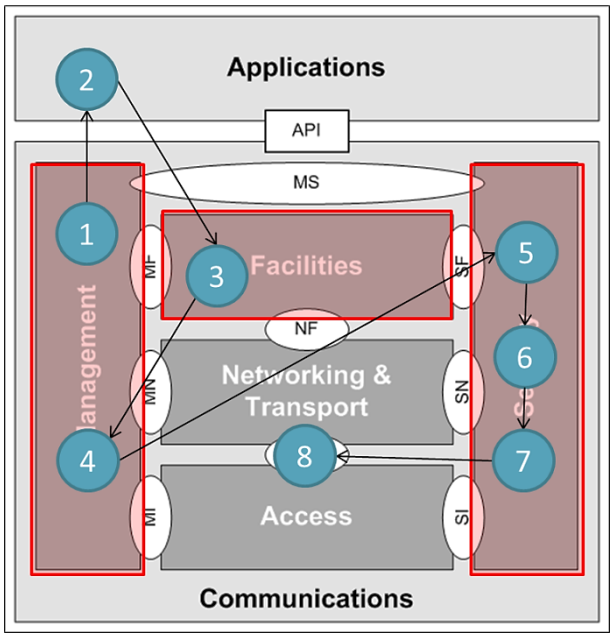
Figure 6.9: Infrastructure-vehicle-unicast scenario (sending)



This scenario shows the exchange of the third step in a traffic signal pre-emption use case, being the pre-emption confirmation. The scenario shows the steps for a C-ITS-equipped signal controller to generate the pre-emption confirmation message and send it to a specific vehicle, and then for the C-ITS device in this vehicle to receive and use it. This assumes that step one and step two of the traffic signal pre-emption use case have been completed. The combinations of all three unicast message exchanges would be called a local time-critical session (see Section 6.5).

Figure 6.10 shows the path that the message takes from being created in the application layer (step1) to being physically sent through the antenna (typically 5.9 GHz DSRC) (step 9).

Figure 6.10: Infrastructure-vehicle-unicast scenario (sending) – core functions



Source: Modified from ISO 21217 draft international standard.

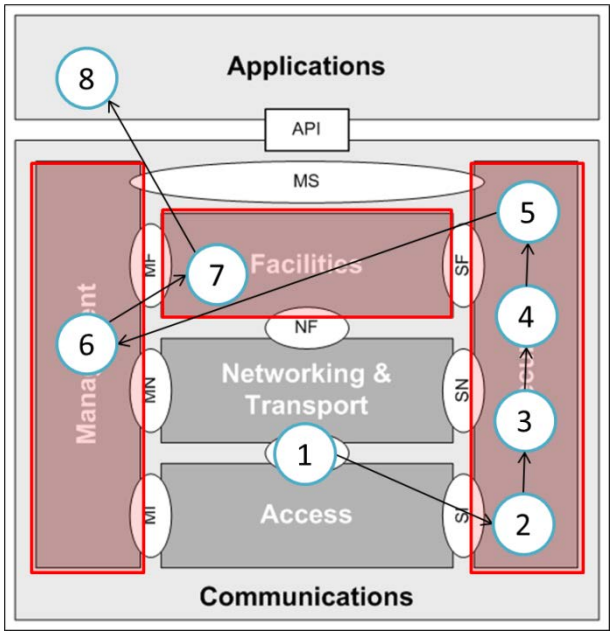
The steps can be described as follows. The functional subsystem that performs this function is added in brackets:

1. Check if receiving vehicle subscribed to this message/application type (data distribution).
2. Create message, e.g. a traffic signal priority message to confirm pre-emption for an approaching vehicle.
3. Include time stamp (time synchronisation).
4. Monitor the status of communication technologies (service monitor).
5. Select communication technology (network services).
6. Confirm if allowed to broadcast pre-emption confirmation message (user permissions).
7. Encrypt message (user trust management).
8. Add security certificate (user trust management).
9. Send message.

Note that, as with the vehicle-originated broadcast scenario, the misbehaviour management subsystem is not used when sending messages. This is only used for received messages.

After the message has been sent, it might be received by the C-ITS devices from addressed vehicles. Figure 6.11 shows the path that the message takes from being received through the antenna (typically 5.9 GHz DSRC) (step1) to the usage of the message content in an application (step 8).

Figure 6.11: Infrastructure-vehicle-unicast scenario (receiving) – core functions



Source: Modified from ISO 21217 draft international standard.

The steps can be described as follows. The functional subsystem that performs this function is added in brackets:

1. Receive message.
2. Decrypt message (user trust management).
3. Check security certificate (user trust management).
4. Confirm if allowed to use message (user permissions).
5. Check for consistency, possibly forward to central management system (misbehaviour mananagement).
6. Check if subscribed to this message type (data distribution).
7. Check timeliness (time synchronisation).
8. Use message.

Note that, as with the vehicle-originated broadcast scenario, the network services subsystem is not used. The network services subsystem selects the communication technology, which is not part of the scenario of receiving a message. Also, the service monitor subsystem is not used as no service availability needs to be checked to receive and use messages.

Examples of applications that could then use the SSM (as highlighted in Table 6.2) could include:

- traffic signal priority
- traffic signal pre-emption
- road access
- parking management.

6.5 Local (Non-) Time-critical Sessions

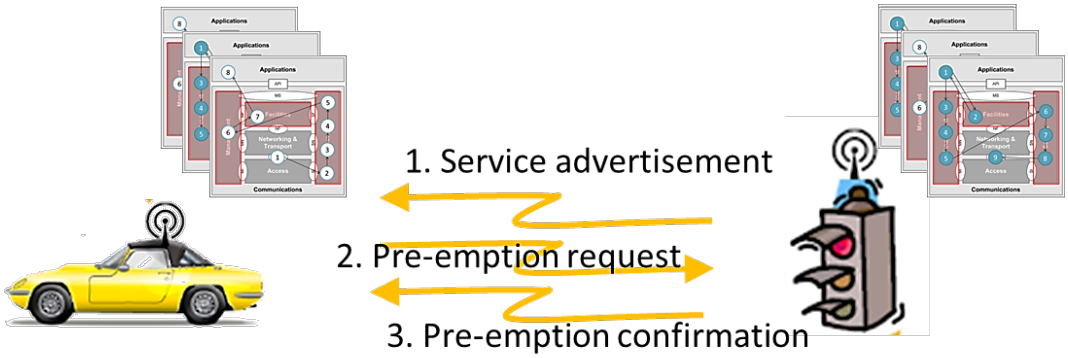
Local sessions are combinations of multiple V2I and I2V unicast messages. There are two types of local sessions, local time-critical sessions and local non-time-critical.

Local time-critical sessions support small and time-critical transactions. These could be advertised services or financial transactions such as multi-lane open-road electronic toll collection. Advertised services refer to services where a roadside C-ITS device of a service provider sends out a message of a particular type advertising that the service is being provided, and a C-ITS device of the user with the corresponding user application connects to the service.

Local non-time-critical sessions support non-time-critical transactions, with small- to moderate-size transactions at low frequency, probably using IP. These could be advertised services, such as uploading probe vehicle data, downloading moderate amounts of data such as local or regional traffic conditions, or fleet management or customer relationship management services. For these transactions, multiple frames would be transmitted while a moving vehicle is within range of one roadside device.

Figure 6.12 shows an example of a local non-time-critical session as part of a signal pre-emption service, starting with a service advertisement message from the traffic signal roadside unit, followed by a pre-emption request from a vehicle and concluded with a pre-emption confirmation message from the traffic signal roadside unit to the vehicle.

Figure 6.12: Local Non-Time-Critical Session as part of a signal pre-emption service



As local sessions are combinations of multiple V2I and I2V unicast messages, the steps in this scenario are the same as for the unicast scenario and are explained in the infrastructure-vehicle-unicast scenario in Section 6.4.

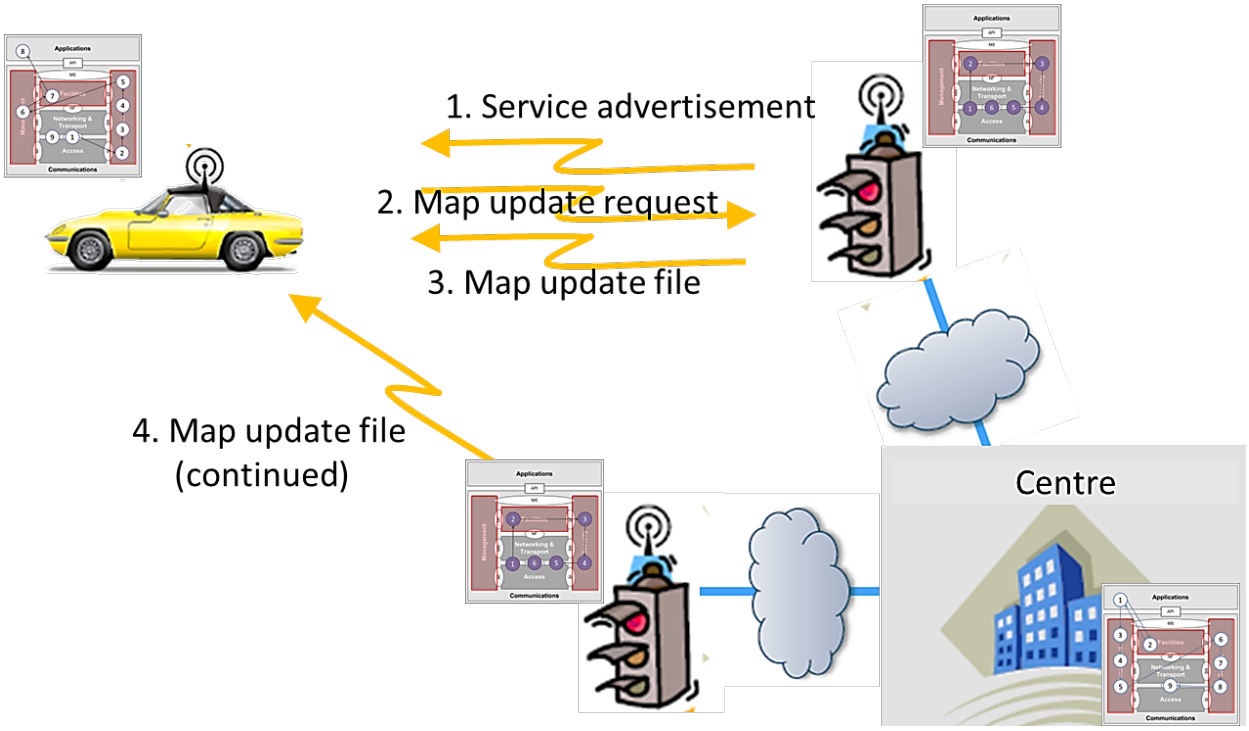
6.6 Multi-roadside Unit Sessions

Multi-roadside unit sessions with hand-offs are needed to transfer large quantities of data or to execute transactions that take considerable time, which cannot be accommodated within a single encounter between a moving vehicle and one roadside ITS-station, but must be maintained across several V2I/I2V unicast communication sessions with a remote server in a centre. These transactions include single-hop, low time-criticality with large and low frequency transactions. This service involves connecting with a service provider across a network, but the logical communication session needs to persist across multiple ‘touches’ between the in-vehicle device and a series of roadside units offering access to the backhaul.

Figure 6.13 shows a scenario where a centre ITS-station provides a map update to a vehicle via several roadside units. The following operations are described:

- centre sending to roadside units via wired connection
- roadside units sending to vehicle
- vehicle receiving.

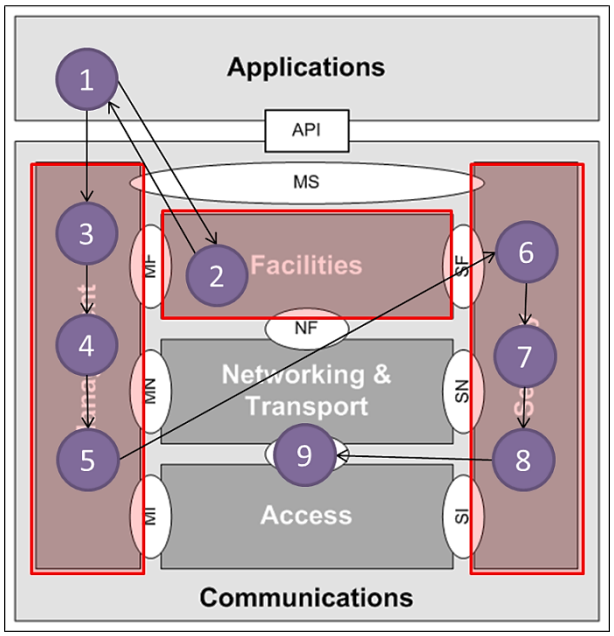
Figure 6.13: Multi-roadside unit session



The scenario assumes that the communication session has already been setup. The scenario focusses on those steps performed by the core functions.

Figure 6.14 shows the path that the message takes from being created at a centre in the application layer (step1) to being physically sent through the typically wired connection (step 9). Note that this first part of the multi-roadside unit section does not use DSRC.

Figure 6.14: Multi-roadside unit session (centre to roadside unit) – core functions



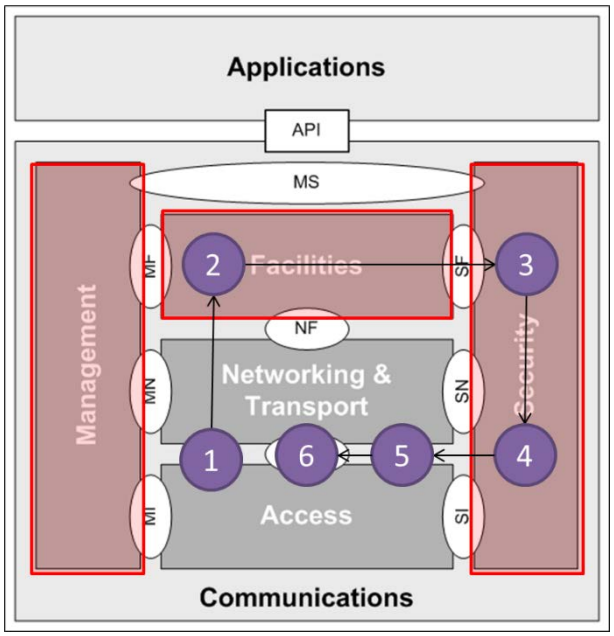
Source: Modified from ISO 21217 draft international standard.

The steps for the first part of the communication (from centre to roadside unit) can be described as follows. The functional subsystem that performs this function is added in brackets:

1. Centre provides a map update/infotainment files.
2. Include time stamp (time synchronisation).
3. Check if receiving vehicle subscribed to this message/application type (data distribution).
4. Monitor the status of communication technologies (service monitor).
5. Select communication scenario (network services).
6. Confirm if allowed to communicate content (user permissions).
7. Encrypt message (user trust management).
8. Add security certificate (user trust management).
9. Send message to roadside unit via wired connection.

After the data has been sent to a roadside unit, this roadside unit will forward the data to the receiving vehicle. Figure 6.15 shows the path that the message takes from being received by the roadside unit and sent to the vehicle.

Figure 6.15: Multi-roadside unit session (roadside unit receiving and sending)



Source: Modified from ISO 21217 draft international standard.

The steps performed by the roadside unit can be describes as follows. The functional subsystem that performs this function is added in brackets:

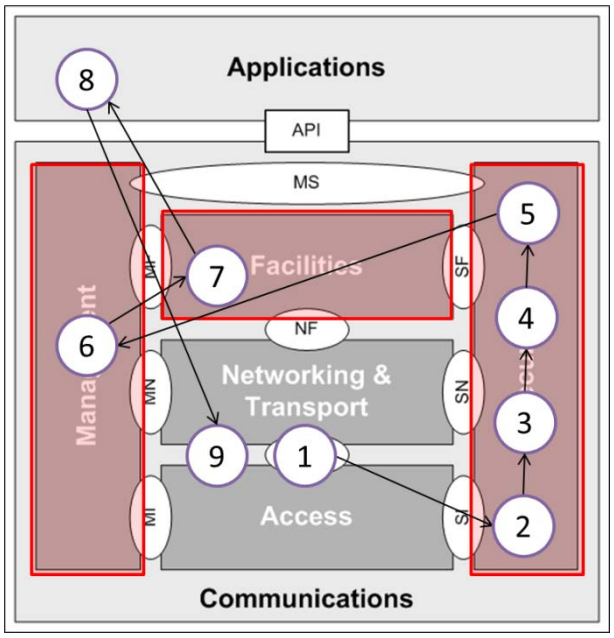
1. Receive data via from centre.
2. Include time stamp (time synchronisation).
3. Encrypt message (user trust management).
4. Add security certificate (user trust management).
5. Forwards data via unicast to vehicle.
6. Hand-off vehicle to other roadside unit.

Note that, as with to the vehicle-originated broadcast scenario, the network services subsystem is not used. The network services subsystem selects the communication technology, which is not part of the scenario of receiving a message. Also the service monitor subsystem is not used as no service availability needs to be checked to receive and use messages.

The hand-off to another roadside unit has not been described by the EU-US Harmonisation Task Force (2012a) and is here depicted as a single step, but might in practice consist of several steps.

Figure 6.16 shows the path that the message takes after the message has been sent to the receiving vehicle.

Figure 6.16: Multi-roadside unit session (vehicle receiving) – core functions



Source: Modified from ISO 21217 draft international standard.

The steps performed by the receiving vehicle can be described as follows. The functional subsystem that performs this function is added in brackets:

1. Receive, e.g. a vehicle receiving a map update.
2. Decrypt message (user trust management).
3. Check security certificate (user trust management).
4. Confirm if allowed to use message (user permissions).
5. Check for consistency, possibly forward to central management system (misbehaviour management).
6. Check if subscribed to this message type (data distribution).
7. Check timeliness (time synchronisation).
8. Use message.
9. Hand-off to other roadside unit.

The steps are the same as receiving a broadcast message with the addition of the hand-off. The hand-off has not been described by the EU-US Harmonisation Task Force (2012a) and is here depicted as a single step, but might in practice consist of several steps.

7. Summary of Impacts

This section provides a summary of impacts that should be considered when planning for the deployment of C-ITS and the proposed core functions. This includes the potential impacts on operations, organisations, and during system development.

7.1 Operational Impacts

Operational impacts can be defined as the impacts caused by the introduction of a new system on current operational activities. This could include impacts (positive or negative) on operational processes, products, service levels, standards, technologies, etc. Potential operational impacts have been assessed and categorised into the four key roles identified in the organisational architecture, as defined in Section 1.3.

Policy

Table 7.1: Policy impacts

Impact	Description
Policy keeping pace with technology	Given the dynamic nature of the emerging C-ITS, it will be important that policy is developed in a way that enables new technologies in future, and does not easily become obsolete or a barrier to innovation.
Agreement to standards	Achieving agreement across key stakeholders with those standards necessary to support consistent C-ITS deployment and enable interoperability will be critical.
Assurance of compliance with standards (at time of deployment)	There is a need to determine what assurance of compliance will be necessary for the agreed standards in terms of the level of compliance (e.g. third, second or first party certification. Third party certification involves an independent assessment by an accredited body. Second party certification involves an assessment by an association or group. First party certification involves an individual or organisation providing the assurance that it complies) and the types of compliance (e.g. individual inspection, type approval or audit/surveillance).
Assurance of compliance with standards (in-service)	There may be a need to assure continued compliance for some standards during operation (e.g. some critical sensors may degrade or go out of calibration over time). Consideration will need to be given as to the options for this, which could include periodic audits or regular integrity checks.
Licensing of 5.9 GHz devices	Decisions will be required on what type of radio communication license (e.g. class, apparatus) is appropriate for 5.9 GHz devices, what the conditions are (e.g. what level of protection is afforded from interference), and how this device licensing should be administered.
Security	In establishing a security credential management system (SCMS), a number of policy decisions will likely need to be made, including which entity should be the SCMS manager/administrator, and what the role of government and the private sector should be with regard to the other roles in the agreed SCMS model.
Privacy	While the NTC regulatory policy review found that the current privacy framework should suffice, there remains some concern regarding whether the use of unique identifiers with C-ITS communication complies with relevant privacy and surveillance legislation.
Liability	While the NTC regulatory policy review found that the current legal framework for liability should suffice, this will remain an important issue for all providers of equipment, services and data to consider with their operations. Also, further consideration of liability will be necessary for automated controls.
Driver distraction	The NTC regulatory policy review found that the current rules around driver distraction should suffice. However, rules about this issue continue to evolve internationally, and it will be important for service providers to be cognisant of this when developing and deploying C-ITS solutions.

System management

Table 7.2: System management impacts

Impact	Description
Management of new systems	There will likely be a need for a new system to enable secure and trusted communication between C-ITS devices, including a system for managing security certificates and systems for registration of C-ITS equipment and services. The new systems will need to be designed, developed, integrated, tested, deployed, maintained and supported.
System monitoring and support	Any new C-ITS will need to have the appropriate system management, monitoring and support processes established, and these ideally should be in compliance where appropriate with the Information technology infrastructure library (ITIL) service management framework. Maintenance and support is likely to be managed in a decentralised way on a subsystem level (e.g. for support on my non-functioning in-car device I go to my local dealer. For support on a C-ITS roadside unit a road agency goes to this supplier, etc.).
Security management	Some applications, which carry low security risk, will be able to function using the normal wireless communication security (cellular, IP security or similar). However, other applications will require higher levels of security. In order to enable secure communication, an appropriate security credential management system (SCMS) and supporting processes will need to be in place. For 5.9 GHz DSRC, this will likely be based on a PKI using security certificates to achieve the required authentication. The emerging PKI model is still to be finalised, so system management requirements for the SCMS are not yet known.
Trust management	To ensure trust, there will be a need to establish processes to ensure the globally unique identifiers, related registries, certification labs, trust authorities and a public key infrastructure.
Compliance with standards	There will likely be standards (and possibly other specifications) that require assurance of compliance, both at the time of deployment, and during operation. In these cases, there will be a need to establish processes to determine if compliance is being achieved (e.g. type approval, individual inspections, audit processes, in-service checks, etc.).
Misbehaviour detection and revocation	Depending on the application and the communication medium, there will be a need to identify when a malicious activity or erroneous behaviour is occurring. There would also then be a need to establish processes for how the offending device or service is revoked, so that it cannot affect other C-ITS devices or services in the system.
Updating software and hardware	To enable C-ITS equipment to evolve, and to be maintained or fixed, there is a need to establish processes that will enable both software and hardware to be updated. This could include both physical and remote (wireless) software updates.

System operation

Table 7.3: System operation impacts

Impact	Description
Provision of new applications and services	The emerging C-ITS, and the core functions that support it, should enable service providers to develop and deploy new applications and services, some of which are not envisioned, and probably not yet even technically possible.
Integrity of content	There will be an increasing demand for content, including attribution, geographic coverage, accuracy, timeliness, etc. This may require integrity check processes to be established for different data sources to ensure the data can be trusted and is fit for purpose.
Roadside infrastructure	For some communication media, such as 5.9 GHz DSRC, there will be a need for communication infrastructure to be deployed in the field. This will have an impact on asset management processes, including maintenance and operations.
Data messaging	Some C-ITS applications will require data messages to be transmitted to them from roadside infrastructure to enable them to operate. Examples include signal phase and timing (SPaT) and intersection map data (MAP). Road operators will need to establish processes to create, maintain and transmit these messages, in compliance with agreed standards.

Impact	Description
Hybrid communication approach	There will likely be a trend towards C-ITS applications that enable several communication media (i.e. not just dedicated to one media). The operations of some service providers will be affected by this hybrid approach, and it will be critical that messages are consistent and interoperable.
Systems integration, including interfacing with legacy ITS	To enable integration with other ITS in the broader system, interoperability will need to be considered at four levels (technical, syntactical, semantic, organisational). This will likely be a particular challenge with legacy systems, using older communication technology and data protocols.
New sources of traffic data	C-ITS will enable traffic data to be accessed from new sources, which may include floating car data directly from C-ITS-equipped vehicles. This will provide opportunities for road operators to better optimise their road network operations. It may also provide opportunities to reduce the number of road sensors and other ITS infrastructure assets across their road networks.
Data management	The emerging C-ITS will create significantly more data than is currently created in the transport system. Rules will need to be established regarding what data is captured, how privacy and security is assured, what data is made accessible. This could include making road network data accessible to other service providers for their C-ITS services.
Positioning and timing	Some safety-critical applications will have stringent positioning and timing requirements, some of which cannot be met with currently available services (e.g. standalone GNSS receivers do not meet emerging requirements). Positioning and timing services may also need to be authenticated and checked for integrity.

Users

Table 7.4: User impacts

Impact	Description
Access to new apps and services	End users will over time increasingly have access to new applications and services as C-ITS evolve, and they will experience positive safety, mobility and/or environmental outcomes from these.
Potential reliance upon C-ITS	Road users could potentially develop some level of reliance on C-ITS applications in future. While initial C-ITS apps are likely to focus on advice and warnings, in the longer term the trend will be towards enabling automation of driver controls. It will be important to consider this, balanced with the current road rule requirement that the driver should be in control of a vehicle at all times.
In-service compliance with standards	End-users may have to take on some responsibility for ensuring that C-ITS equipment that they own and operate continues to comply with relevant standards. For example, vehicle owners currently have a responsibility to ensure their vehicle is in a roadworthy condition. Some C-ITS potentially could be included within this requirement in future.
Opt in and opt out for end-user applications and services	Some C-ITS applications and services will be continually operational in a vehicle, whereas for others the driver will either have to opt in (e.g. pay for a commercial service), or opt out (e.g. choose not to receive a service). The user will need to understand these options and make an informed decision.

7.2 Organisational Impacts

Organisational impacts can be defined as the impacts caused by the introduction of a new system on current organisations. This could include impacts (positive or negative) on organisational structures, roles, responsibilities, governance arrangements, policy, strategy, resourcing, capabilities, budgeting, etc. Potential organisational impacts have been assessed and categorised into the four key roles identified in the organisational architecture, as defined in Section 1.3.

Policy

Table 7.5: Organisational policy impacts

Impact	Description
National policy framework	The policies that guide decisions regarding C-ITS should preferably be part of a national framework, and not be state-based. This should ensure national consistency in policy direction and organisational decisions. The governance and responsibilities around such a policy framework will need to be determined.
Spectrum management and device licensing	For 5.9 GHz devices, there will be a need for a centralised entity, working closely with the Australian Communication and Media Authority, to coordinate the use of ITS in the 5.9 GHz band and the administration of device licences. A policy decision on which entity should take on this role is yet to be determined. The result of the current international lobbying to open up the 5.9 GHz spectrum for wireless mobile broadband may impact the allocation decision and licensing regime.
Assurance of compliance with standards	It is likely that some standards will be deemed to be critical for C-ITS. To assure compliance with critical standards, there may be a need for certification and auditing processes to be established. If it is determined that this is necessary, it would be wise to be consistent with international practice, and to leverage existing processes where possible. For those standards that become UN vehicle regulations, these will come under the current ADR processes that are overseen by DIRD (in Australia). For other standards, there may be a need for a centralised entity to administer certification processes. This may require a policy decision.
Security management	In establishing a security credential management system (SCMS), a number of policy decisions will likely need to be made, including which entity should be the SCMS manager/administrator, and what the role of government and the private sector should be with regard to the other roles in the agreed SCMS model.
Industry guidance	Consideration should be given to developing a national industry code or industry guidelines for C-ITS. This could be effective in ensuring a consistent and appropriate approach to issues such as privacy, security, data ownership, data access and licensing, data message integrity, etc.
Funding/business model	The implementation of core functions identified in this Concept of Operations will need to be funded. This implementation will be part of the development of C-ITS equipment to be used in vehicles, in roadside ITS infrastructure, in mobile devices and in centres. Different stakeholders will fund these implementations. Public and private stakeholders are likely to have different funding mechanisms. The business models are yet to be determined, however, some core functions, particularly those required for 5.9 GHz DSRC, may require government funding and coordination. This will have implications for current budgeting, and may require a business model to be established that supports the required initial and ongoing investment.
National Positioning Infrastructure	Although positioning services are not part of the proposed core functions, the wide-area positioning services currently available locally (e.g. GPS) do not meet the requirements of many emerging safety-critical applications. A National Positioning Infrastructure (NPI) has been proposed by spatial stakeholders. While an NPI might be considered an input to C-ITS (i.e. not within it), it is worth noting that establishing an NPI will likely require funding and resources that have not been committed today.
Capability development	C-ITS include a wide range of technologies and services that continue to evolve at a rapid rate. Stakeholders who have a role with C-ITS will need to consider how they source, develop and maintain an appropriate level of capability. Some of the required capabilities will likely not be accessible today.

System Management

Table 7.6: Organisational system management impacts

Impact	Description
Spectrum management and device licensing	To effectively manage the use of the 5.9 GHz band, including the licensing of DSRC devices and coordination with other users of and near the band, there will likely be a number of systems and processes that will need to be established. Which entity (or entities) undertakes these functions will need to be determined.
Security management	To enable secure communication, an appropriate security credential management system and supporting processes will need to be in place. For 5.9 GHz DSRC, this will likely be based on a PKI using security certificates to achieve the required authentication. It is recommended that the role of the SCMS manager/administrator is undertaken by a centralised entity. Also, in line with the NTC regulatory policy review, it is recommended that any entity that manages security certificates should be a separate entity to those that hold registration and licensing data.
Compliance with standards	There will likely be some technical standards that require assurance of compliance, both at the time of deployment, and during operation. For those standards that become UN vehicle regulations, these will be administered as part of the ADR process at market entry, and the state and territory roadworthiness processes for in-service (in Australia). For other standards, decisions will need to be made as to whether compliance is necessary, and if so, what level and type of certification may be required. Consideration should be given to a centralised entity overseeing such certification processes.
Capability development	C-ITS include a wide range of technologies and services that continue to evolve at a rapid rate. Stakeholders who have a role with C-ITS management will need to consider how they source, develop and maintain an appropriate level of capability.

System Operation

Table 7.7: Organisational system operation impacts

Impact	Description
Authentication and integrity of data and services	There will be an increasing demand for content, including greater attribution, geographic coverage, accuracy, timeliness, etc. This may require authentication and integrity checking by means of the proposed core functions to ensure data from different sources can be trusted and is fit for purpose. Depending on the application, these functions might need to be centralised, or could be done by separate entities.
Roadside infrastructure	For some communication media, such as 5.9 GHz DSRC, there will be a need for communication infrastructure to be deployed in the field. This will have an impact on asset management and maintenance, which will have funding and resource implications. This will be particularly relevant to road operators looking to use DSRC devices.
Data messaging	Some C-ITS applications will require data messages to be transmitted to them from roadside infrastructure to enable them to operate. Examples include signal phase and timing (SPaT) and intersection map data (MAP). Road operators in particular will need to give consideration to funding and resource implications for this.
Systems integration	To enable integration with other ITS in the broader ITS domain, interoperability will need to be considered at four levels, including organisational.
Data management	C-ITS will create significantly more data than is currently created in the transport system. Organisations will need to consider what data is captured, how privacy and security is assured, what data is made accessible, etc. This will likely have resource and funding implications for some organisations.
Support services	New C-ITS services will need support to end users, dependent on the type of application and service. This may have resource and funding implications for some organisations.

Impact	Description
Service level agreements with system operation entities	Given that cooperative intelligent transport systems are a system of connected systems, there may be a need for different organisations to enter into formal agreements for the exchange of data and other services. Ideally there should be consistency in the type of service level agreements across the domain, to facilitate consistency and interoperability in the way data aggregators engage with those who provide access to data, and those who include it in end products.
Capability development	C-ITS include a wide range of technologies and services that continue to evolve at a rapid rate. Stakeholders who have a role with C-ITS operation will need to consider how they source, develop and maintain an appropriate level of capability.

Users

Table 7.8: Organisational user impacts

Impact	Description
Vehicle fleets	Where a single entity owns and operates a number of C-ITS-equipped vehicles (e.g. commercial fleets), there is potential that these entities could be taking on additional responsibility, depending on the type of application (e.g. will differ if it is a regulatory application or a traveller information service).

7.3 Impacts During Development

The impacts described in this section can be defined as the anticipated impacts caused during the development phase of the proposed system.

The development of C-ITS are likely to be of an evolutionary nature. The following possible stages have been defined an indication of the impact during development:

- the piloting stage: temporary partial deployments
- day-one deployments: initial permanent deployment of a limited number of simple applications on limited geographical locations. Not all core functions are necessarily implemented
- 3–5 years: take-up of more and more complex applications and services, on a larger geographical scale, most core functions are implemented, initial C-ITS platform (or several) start to emerge.
- 5+ years: C-ITS start to mature, most C-ITS applications and services use a platform shared with other applications. The proposed core functions are deployed as part of the available platform or platforms.

Potential impacts during development have been assessed and categorised into the four key roles identified in the organisational architecture, as defined in Section 1.3.

Policy

Table 7.9: Policy impacts during development

Impact	Description
Analysis, research and planning	Due to the evolutionary nature of C-ITS, work on analysis, research and planning for future C-ITS will continue, and should be informed where appropriate during development activities.
Regulatory and policy instruments	While every effort will be made to ensure that an appropriate regulatory and operational framework is in place prior to deployment, it is possible that some regulatory and policy instruments may need to be further reviewed or modified based on additional learnings from C-ITS initiatives.

Impact	Description
Standards and assurance of compliance	It is anticipated that achieving agreement to a minimum set of standards could progress for some time, and relevant decisions may be made following the different development stages. Also, some standards may not be finalised prior to initial deployment commencing. Further, agreement on the level of assurance of compliance may also take some time, and may change with the development stages. Much of this is due to the evolutionary nature of C-ITS, so will need to be given appropriate consideration.
Licensing for trials and testing	C-ITS devices will require licensing to operate during trials and testing. The licensing regime will need to give appropriate consideration to how best to licence these devices (e.g. possibly a scientific license could be most appropriate, but will need to be determined).

System management

Table 7.10: System management impacts during development

Impact	Description
Develop core functions	The core functions identified in this Concept of Operations will need to be established by the different stakeholders so as to support the development of new C-ITS applications and services.
System management	During all development stages the system management role will need to be implemented.
Maintenance and support	Maintenance and support is likely to be managed in a decentralised way on a subsystem level (e.g. for support on a non-functioning in-car device go to the local dealer. For support on a C-ITS roadside unit a road agency goes to this supplier, etc.).
Testing and validation	Testing and validation of C-ITS core functions during the development phase should follow a robust process. Which core functions are required in which stage of the development of C-ITS and how compliance should be ensured will have to be determined during the development based on risks and the overall system performance.
Architecture	Development work should be done in compliance with the internationally agreed ITS-station architecture. Also, any variations to the ITS architecture that are identified during the development phase should be highlighted and appropriate changes made.

System operation

Table 7.11: System operation impacts during development

Impact	Description
Interfacing with legacy ITS applications and services	To enable integration with other ITS, interoperability will need to be considered at four levels (technical, syntactical, semantic, organisational). This will likely be a particular challenge with legacy systems, using older communication technology and data protocols. Any changes to legacy ITS could affect cost, resource and timing of the development phase.
Effect on existing ITS application and services in operation	Some C-ITS developments may require existing ITS in operation to be affected. An example would be a C-ITS application that needs to interface with and/or make a change to a traffic signal system. It will be critical that appropriate system management (as described under Section 5.4) and change management processes are followed to mitigate any risks to road operations.

Users

Table 7.12: User impacts during development

Impact	Description
Involvement in trials and testing	Some users, including vehicle owners and system operators, could be involved in the trialling and testing of C-ITS developments. Appropriate agreements and processes may be put in place with those users that opt in to minimise any detrimental impacts.

8. Analysis of the Proposed System

This section provides an analysis of the proposed C-ITS core functions, which comprise the changes required to deployed the core functions.

The analysis considers the four key roles identified in the organisational architecture defined in Section 1.

8.1 Summary of Improvements

The improvements that will be enabled in C-ITS due to the introduction of the proposed core functions are summarised in Table 8.1 to Table 8.8.

Policy

Table 8.1: Policy improvements

Improvement	Description
Realise societal benefits	The core functions will facilitate a range of applications that would not exist otherwise. Therefore the core functions help to make a tangible contribution towards solving key transport challenges (e.g. road safety, efficiency and environmental).
Efficient transport system	The core functions define a platform that supports the sharing of information between different C-ITS devices, independent of the mode of transport. Therefore the core functions enable services, coordination and interoperability between various modes of transport.
Assurance of compliance with agreed standards for devices and services	The proposed core functions are based on commonly accepted concepts defined in standards from international standards development organisations. Part of the core functions are the procedures, rules and regulations that define standards and ensure compliance with these standards.
Ensuring safety and security	The core functions are designed to provide a secure and trusted platform for C-ITS applications and to mitigate the risk of cyber threats and malicious acts. This includes the proposed institutional context that can ensure compliance with performance and security standards and rules. This allows for safety-critical applications to provide safety benefits for road users where security risks are controlled.
Privacy assurance	The core functions will be designed to manage the privacy of users of C-ITS by ensuring that personal data created in C-ITS is effectively managed in compliance with relevant legislation, privacy principles and other rules as appropriate. A separation of roles, responsibilities and technical systems as proposed enable the deployment of C-ITS and at the same time respecting privacy. The proposed core functions and management structure are concrete proposals for the deployment of C-ITS which can and will be subjected to a privacy impact assessment. However, there is currently no nationally consistent interpretation of privacy and surveillance legislation with regard to the use of unique identifiers and other personal data.
International harmonisation	International harmonisation will result in reduced barriers to trade and interoperability. Harmonisation with international standards and best practice will realise a range of benefits including interoperability, nationally consistent services and services levels and the ability to adopt internationally developed technology and export nationally developed technology.
Use of the 5.9 GHz spectrum band	The core functions will enable the use of the 5.9 GHz spectrum band for a safer and more efficient transport system by facilitating safety-critical applications that could not exist without the core functions.

System management

Table 8.2: System management improvements

Improvement	Description
Assurance of compliance with standards and guidelines (for devices, apps, services)	The proposed core functions and institutional changes enable standards to be used and compliance with these standards to be ensured. This is the main improvement allowing a nationally interoperable system aligned with international developments.
Security management system to enable security and trust	The proposed public key infrastructure and security credential managements system as part of the core function enable security and trust in C-ITS devices and services.
Public key infrastructure to provide privacy by design	The proposed public key infrastructure does not only provide security and trust, it also provides privacy by design. The separation of authorities separates personal information from data generated by C-ITS. The proposed rotating IDs and short-term certificates support privacy by providing barriers to monitor vehicles throughout the network over time.
Licensing and management role to enable the use of the 5.9 GHz band for C-ITS	The proposed licensing and management role to enable 5.9 GHz DSRC based critical safety applications to be deployed and provide safety benefits to travellers.
Facilitation of improved interoperability and data sharing	The proposed core functions facilitate the sharing of information between applications on a single C-ITS device and between different C-ITS devices.

System operation

Table 8.3: System operation improvements

Improvement	Description
Enable emerging C-ITS to be deployed	The core functions facilitate the sharing of information and resources between vehicles, roadside infrastructure, mobile devices and centres. They also enable secure and trusted communication required for safety-critical applications.
Access to probe data	Anonymised data from vehicle sensors can be made available to other vehicles and traffic managers. Content providers will specialise in collecting and processing these data to generate useful information for different users.
Open platform, based on standards, allows service providers to develop and deploy while sharing resources	The core functions define a platform that supports the sharing of information between different applications over different communication channels. They facilitate the deployment and operation of all types of C-ITS applications and services (for example safety, mobility, and environmental), and thus contribute to an extendible service.
Hybrid communication, leveraging of existing and emerging communication networks	The advantage of the proposed hybrid communication approach (technology agnostic platform) is that enabling several technologies will allow for a more flexible and organic development of C-ITS. The existing communication networks like 3G and 4G/LTE already provide coverage for large parts of the populated areas and can be used for a variety of C-ITS services to accelerate the deployment and adoption of C-ITS. 5.9 GHz can be used by VANETs without infrastructure, and at key points, a new communication infrastructure using 5.9 GHz DSRC can be rolled out additionally to supplement and benefit from its unique communication characteristics.(e.g. accident black spots, ramp access, etc.).

Users

Table 8.4: User improvements

Improvement	Description
Benefits in terms of road safety, mobility and comfort	The core functions will facilitate a range of applications that would not exist otherwise. Road users will benefit from these applications. Additionally, the core functions enable different applications on a single platform and a single coordinated human machine interface.
Assurance of secure and trusted communication	The core functions assure the user that the communication is secure and trusted.
Confidence that privacy is ensured	The core functions and management structure ensure privacy-by-design principles are applied and that privacy guidelines are followed. This will ensure that data created by C-ITS will not be used in ways that breach the privacy of individuals.

8.2 Disadvantages and Limitations

This section describes disadvantages and limitations of the proposed core functions. Disadvantages might include the need to retrain personnel, rearrange work spaces, or change to a new style of user interface; limitations might include features desired by users but not included, degradation of existing capabilities to gain new capabilities, or greater-than-desired response time for certain complex operations.

Policy

Table 8.5: Policy disadvantages and limitations

Disadvantages and limitations	Description
National-level policy framework required	A possible disadvantage of nationally consistent C-ITS services is that this limits the states in their autonomy. Although each state can choose which services or applications to provide or incentivise, the way in which any applications or services work should be nationally consistent. This requires national requirements for C-ITS (applications and core functions) which need to be based on a single national policy framework. The states, along with key stakeholders, will have to agree on a national C-ITS policy framework.
International standards and best practice are still incomplete	A policy principle is to align C-ITS in Australia and New Zealand with international standards and best practice. The proposed core functions are in line with the concepts that are being established for C-ITS internationally. This alignment is limited to the current progress made internationally in developing C-ITS and standards.

System management

Table 8.6: System management disadvantages and limitations

Disadvantages and limitations	Description
Standards development still in progress	A disadvantage to following internationally emerging C-ITS is that these developments create an uncertainty for decision-making locally. Some standards for system management are still under development. Several standardisation bodies have released partly complete sets of standards suitable for day-one deployments. Although initial deployments and pilots are currently based on the available standards, the detailed design of the core functions would benefit from having more complete and mature standards available.
Hybrid approach to communication is still evolving	While a hybrid approach to utilising a suite of wireless communication technologies is desirable, each is at a different point with deployment. Cellular and analogue radio broadcast are well established. Digital radio is still emerging and 5.9 GHz DSRC has not yet been deployed. 4G/LTE is starting to be rolled out, and is rolling out much more rapidly than any infrastructure-based implementation of 5.9 GHz may be expected to do. The integration of different modes is still evolving which creates uncertainty in decision making.
Mechanism for software updates to be defined	The core functions are limited and do not include mechanisms for software updates. For example questions like how many software updates would be needed to keep ensuring secure and trusted operation, and who controls the rate at which software updates are done that address newly identified security risks? Experience with large scale deployment will answer these questions over time.
There are limitations of the security system with regard to the speed to process and communicate authenticated messages	There are challenges in exchanging authenticated messaging ten times a second in a physical world of fast moving parts, and this is still a topic of research and development in the international C-ITS community.
Management of non-interoperable used imported vehicles to be defined	Imported used vehicles, especially in the case of New Zealand importing vehicles with different regional specifications, might have incompatible C-ITS. The interoperability or possible interference needs to be managed when this becomes an issue.
Prioritisation of messages to be defined	The proposed core functions and management structure facilitate that messages can be prioritised; however a prioritisation has yet to be defined.

System operation

Table 8.7: System operation disadvantages and limitations

Disadvantages and limitations	Description
Limited operational capacity management	C-ITS will be a distributed system with little or no centralised operational capacity management. Capacity management will possibly be managed through standards and performance requirements and compliance procedures, with many different stakeholders being responsible for decentralised operational components.
Big data	The amount of data that is generated through C-ITS will be too large to store, both in the backend and in the vehicles or nomadic devices. This means that useful information will have to be extracted from vehicles in (near) real-time.

Users

Table 8.8: User disadvantages and limitations

Disadvantages and limitations	Description
Data plan could be affected (depending on the app)	A possible disadvantage is that data plans by users could be affected. This is left to the market, as an incentive to service providers to provide services that minimise data rates. The extent to which this is an issue depends on the development of pricing schemes for data communication for different technologies.
Safety benefits cannot easily be experienced	Safety benefits cannot easily be experienced, so any safety improvements might go unnoticed by users. This makes it a challenge for services providers to show the added value.
Possibility to opt in or opt out is not specified	The proposed core functions are possibly going to be implemented in many of the C-ITS platforms that will be deployed. A C-ITS platform that is registered and capable of sending messages might come as an extra with new vehicles without user being aware. The core functions do not specify procedure for user to opt in or opt out on the use of a C-ITS platform that comes with their vehicle.

8.3 Alternatives and Trade-offs Considered

During the creation of this Concept of Operations, several rounds of consultations and discussion have highlighted that views on a C-ITS platform are still evolving. The following alternatives and trade-offs were identified in the process.

8.3.1 Alternatives

Do-nothing scenario

If the market would continue to evolve without the proposed core functions, some applications would not be feasible. Time-critical safety applications which require low latency, trusted and secure data exchange, like intersection safety applications will not be possible without the identified core functions in the foreseeable future. Additionally, many C-ITS applications would be island solutions. C-ITS service providers would deploy their own platform and devices, based on existing communication technologies like cellular networks, and there would be no or minimal data exchange between applications from different services providers. C-ITS equipment in imported cars may need to be turned off for the Australian and New Zealand markets.

The choice of (i) technology agnostic core functions enabling all types of applications or (ii) 5.9 GHz communication for time-critical safety applications

The Concept of Operations proposes communication technology agnostic core functions, supporting all types of applications. This so-called ‘hybrid communication approach’ means that C-ITS applications that implement the core functions can, given any minimum communication requirements, seamlessly switch to the best available communication technology. An advantage of this concept is that the system optimally uses the available communication infrastructures, which may include DAB+, UMTS, LTE, WiMAX, Bluetooth, Wi-Fi and 5.9 GHz DSRC.

If core functions were implemented that facilitate 5.9 GHz communication only and support time-critical safety applications only, similar island solutions would occur as in the do-nothing scenario. C-ITS service providers would deploy their own platform and devices, and there would be no or minimal data exchange between applications from different services providers.

Core functions that support all types of communication have two main advantages. The first advantage is that C-ITS applications will be able to choose the communication technology that best meets the communication requirements for that application. Even a single application is likely to have different communication requirements for different processes. A hybrid approach means that applications can use communication technologies that are fit for purpose, and therefore are more efficient. The second advantage is that enabling several technologies will allow for a more flexible and organic development of C-ITS. The existing communication networks like 3G and 4G/LTE already provide coverage for large parts of the populated areas and can be used for a variety of C-ITS services to accelerate the deployment and adoption of C-ITS.

Most stakeholders consulted strongly advised in favour of technology agnostic core functions. Over the last few years, international developments in Europe and the USA have been moving from a strong focus on 5.9 GHz communication to a hybrid approach that includes several communication technologies.

National or state level policy framework

Another important conceptual design choice is that between having a single national policy framework or having different policy frameworks at the state and territory level. A policy framework defines which applications and messages are regulated, which applications and services must use which core functions, and how compliance will be managed.

It is proposed to have one national Australian platform using the same core functions based on a single national policy framework as opposed to allowing multiple platforms based on different state or territory policy frameworks. Based on the ITS vision and objective and the C-ITS policy principles in Australia, a single national policy framework is a more obvious advantageous situation. This was acknowledged broadly by stakeholders.

The advantage is that the same requirements apply to C-ITS applications in all parts of the country so they can work everywhere and in the same way, using one national policy; for example which available applications should be supported by the core functions. Additionally, the core functions can be managed and operated nationally. Each state can, depending on its specific key drivers, choose which services or applications to provide or incentivise. However, the way in which any particular application or service works should be nationally consistent. This requires national requirements for C-ITS (applications and core functions) which need to be based on a single national policy framework. This would provide guidance on the required level of security or privacy for certain (types of) applications. The states, along with key stakeholders, will have to agree on this national C-ITS policy framework.

A possible disadvantage is that this requires road agencies throughout Australia to agree on a common policy and common system management.

For New Zealand, it is proposed to have one national platform using the same core functions based on a single policy framework. Although the policy framework will be similar in structure to Australia, there might be differences regarding which C-ITS devices are authorised to send what types of messages and how this is enforced. In the case of different policy frameworks in Australian and New Zealand, C-ITS devices might have to be certified in both countries for them to work in both countries.

8.3.2 Trade-offs

As described in Section 4.4, the following features were considered as core functions were but not included:

- Updates of the software on C-ITS devices are the responsibility of the C-ITS service provider. Mechanisms for software updates already exist. Updates of the core functions have to be updated by the C-ITS service provider.
- The trade-off here is the amount of control of a system management entity to solve security risks against the control of service providers like vehicle manufacturers over their software updates.

- Map data is not considered a core function, because different C-ITS devices might be using different map data for the same application. The internal map that the C-ITS devices use to represent the environment of the vehicle does not necessarily have the same level of detail for different C-ITS devices. There might be a need to define map data requirements and ensure compliance for safety-critical applications.
- The trade-off is the freedom for commercial C-ITS developers to distinguish themselves against central control over mapping performance.
- Positioning services are not considered core functions. The reason is that two C-ITS devices might both realise the required positional accuracy for the messages and therefore be interoperable, but they could have implemented positioning in different ways. There may be a need to certify positioning services for some applications.
- The trade-off is the freedom for commercial C-ITS developers to distinguish themselves against central control over positioning accuracy. Control is proposed at the level of services and devices, rather than individual components.

Appendix A Stakeholder Consultation

Stakeholder consultation was performed in collaboration with the University of South Australia and Queensland University of Technology. Twenty-two of the main stakeholders were consulted about their views on C-ITS, the core function capabilities, user needs, and roles and responsibilities. This appendix describes the key findings, the method and an example of the online questionnaire used in the consultations.

A more detailed report of the consultations with each stakeholder is produced as an internal working paper titled *C-ITS Concept of Operations: Consultations with Key Stakeholders*.

A.1 Key Findings

This section outlines the key findings. They are grouped by topic area as follows:

1. Role
2. Certification
3. Data
4. Scenarios
5. Application
6. Communication
7. Core.

A.1.1 Role

Key findings related to roles are outlined in Table A 1.

Table A 1: Key findings from consultations with respect to roles

No.	Area	Finding
1.1	Organisational preparation for C-ITS	Stakeholders' organisations were preparing for C-ITS to varying degrees. Preparation by their organisation differed between organisations (e.g. road agencies may be undertaking trials, industry may be working on hardware/software, research institutions may be conducting research etc.).
1.2	Role for your organisation	Stakeholders' views of the role of their type of organisation (e.g. road agency) differed between stakeholders.
1.3	Roles for actors	Stakeholders' views of the role of various actors differed between stakeholders. In particular, certification of standards was identified to be the role of various actors both by the same stakeholder and across stakeholders.
1.4	Missing actors	Various additional actors were identified by the stakeholders including TMC, emergency services, positioning and mapping, ITS Australia, vehicle repair organisations, aftermarket equipment suppliers, mining, ports, infrastructure/civil planning, finance, national e-tolling, ARRB, universities and research bodies. All missing actor categories are added to the stakeholder list.
1.5	Role of government	Stakeholders noted that there will likely be a distinction between the roles of state and federal governments, with harmonisation and cooperation between them. Further, stakeholders saw the role of governments as establishing policy and encouraging infrastructure deployment.
1.6	Administering 5.9 GHz	Stakeholders in the application and communication layer identified that a government or semi-government body should be responsible for administering 5.9 GHz. Austroads was identified as one such body by stakeholders in both the application and communication layer.
1.7	Maintenance responsibilities	Stakeholders generally felt that the owner of the C-ITS device should be responsible for its maintenance.
1.8	Critical operational policy areas for the maintenance and operation of the core	Responses varied with respect to the critical operational policy areas for the maintenance and operation of the core, with some stakeholders noting market intervention to maximise public benefit, providing access to areas the market cannot (e.g. 5.9 GHz) and establishing a body that sits under a federal umbrella and consists of a mix of industry, road agency representatives and standards bodies.

No.	Area	Finding
1.9	Management of digital certificates	Stakeholders across the application and communication layer felt that digital certificates should be managed by a government or semi-government body.
1.10	Critical aspects of security management	Various critical aspects of security management were identified. These included secure roadside communication protocols and standards testing, EMC compliance, PCI compliance impacts, direct encryption of tolling and enforcement, spoofing of network addresses, generating false alerts and data storage security.
1.11	Role of your organisation to ensure secure operation	The roles of application stakeholders to ensure secure operations ranged from providing technical input, assisting in standards definition, undertaking testing, implementing standards and implementing systems.
1.12	Nationwide consistency	It was generally felt that C-ITS should be centrally managed by a country.
1.13	Extent of system to monitor devices	The need to monitor malfunctioning devices was identified by some stakeholders in the user and communication layers.
1.14	Separation of responsibilities (e.g. certification authority from certificate issuing body)	Stakeholders in the application and communication layer, who had an opinion on the separation of responsibilities (e.g. certification authority from certificate issuing body) felt that the certification authority and certificate issuing body should be kept independent of one another. Reasons cited included to increase security.
1.15	Centralised management entity	While some stakeholders questioned whether a centralised management entity is required, stakeholders in the communication and application layer recognised the common role of the management entity as ensuring system integrity.
1.16	Critical operational policy areas from an organisation viewpoint	Stakeholders' views of the critical operational policy areas differed between stakeholders based on their background.

A.1.2 Certification

Key findings related to certification are outlined in Table A 2.

Table A 2: Key findings from consultations with respect to certification

No.	Area	Finding
2.1	Certification required	Views on certification were varied. However, one common theme was that Australia and New Zealand should follow the lead of international regions (e.g. EU and USA) on certification. Also the need to keep the certifying authority separate from the certificate issuing body was identified. It is noted that a concern was raised about the cost incurred as a result of incorporating the certification process into the core system.
2.2	Certification management	The general view on who would be best suited to manage certification was a national authority.
2.3	Management of digital certificates	Stakeholders across the application and communication layer did not have a clear view on who should manage digital certificates, however some noted that digital certificates should be managed by a government or semi-government body.

A.1.3 Data

Key findings related to data are outlined in Table A 3.

Table A 3: Key findings from consultations with respect to data

No.	Area	Finding
3.1	Data storage and access management responsibility	Both the application and communication layer stakeholders noted that the body responsible for data storage would be dependent on the application and therefore could be any body within C-ITS.
3.2	Data ownership conflicts	Data ownership was seen as a critical issue that was closely related to privacy and security.
3.3	Data – private or open	Stakeholders across the user, application and communication layer felt that data that can be used to identify users should be kept private. Further, it was noted that private agencies may want to keep their data private to preserve the investment they may have put into the collection of the data.

A.1.4 Scenarios

Key findings that are related to scenarios are outlined in Table A 4.

Table A 4: Key findings from consultations with respect to scenarios

No.	Area	Finding
4.1	Uptake and market deployment – incentives	Stakeholders felt that incentives were needed for users to provide data, but that in many instances the provision of better services (e.g. safety and traveller information) that C-ITS can provide could be a sufficient incentive.
4.2	Geographical extent	Stakeholders across the application and communication layer felt that C-ITS should be seen as an ecosystem rather than just a system and therefore its geographical extent should ultimately be national if not international.
4.3	Operational scenarios	Stakeholders provided a range of views on the inputs, enablers, control and outputs of the various operational scenarios presented.
4.4	Other operational scenarios	Various additional operational scenarios were presented by the stakeholders; however no common themes were identified.
4.5	Miscellaneous comments	There should be coordination between C-ITS and the Heavy Vehicle Charging and Investment Reform project.

A.1.5 Application

Key findings related to applications are outlined in Table A 5.

Table A 5: Key findings from consultations with respect to applications

No.	Area	Finding
5.1	Critical applications	The focus should be on 'theme' applications rather than specific applications with safety and traffic management identified as the key themes by stakeholders across the user, application and communication layers.
5.2	Critical functions	Privacy, security and reliability were common critical functions of C-ITS that were identified by stakeholders across the user, application and communication layers.
5.3	User needs	Ease of use was a common user need identified with cost being a potential concern of the users.

A.1.6 Communication

Key findings related to communication are outlined in Table A 6.

Table A 6: Key findings from consultations with respect to communication

No.	Area	Finding
6.1	Communication technologies	Stakeholders in the application and communication layer identified that C-ITS should consider the use of all available communication technologies (i.e. communication technology agnostic).
6.2	Specific communication technologies of interest	Stakeholders felt that the system should be open to any standardised communication technology.
6.3	Early entrant technologies	5.9 GHz, 3G and 4G were identified as communication technologies of interest for early C-ITS applications.

A.1.7 Core

Key findings from international C-ITS experts with respect to the C-ITS core and Concept of Operations are outlined in Table A 7.

Table A 7: Key finding from discussions with international C-ITS experts with respect to the C-ITS core

No.	Area	Finding
7.1	C-ITS core Concept of Operations	The Concept of Operations should be technology agnostic and define the impacts of the core in terms of high-level test specifications.
7.2	C-ITS core	The C-ITS core should include basic interoperability requirements such as security, certifications and standards.
7.3	Security management	Security should be managed by a public body.
7.4	Security management in US trials	Public key infrastructure security certificate management is being used in the US trials to enable trust management of messages. Its use is still evolving in the US. However it is based on IEEE 1609.2 and is exploring the use of providing an OBE (on board equipment) with three years' worth of certificates and assuming the existence of nationwide communication infrastructure to obtain updated certificates.
7.5	OBE and trusting messages	The functions that the OBE would perform in order to be granted and maintain trust are not part of the US core Concept of Operations documentation. Experts noted that in order for the OBE to use core services it must have the requisite functionality.
7.6	OBE and prioritising messages	The OBE must have the means to prioritise messages according to the interfaces.
7.7	Single or multiple cores	A single national C-ITS platform simplifies things and eliminates the need for a core2core subsystem, however it requires consistent policy. Where consistent policy cannot be achieved multiple cores may be required.
7.8	Data distribution	Data distribution was seen to be largely an application-layer function. Keeping data distribution elsewhere keeps basic connectivity and security methods isolated from the application-level functions.
7.9	FRAME architecture	ISO TC 204 standards do not directly relate to FRAME because the architecture is too high level for standards. Further, the need for and identity of relevant standards becomes clear as you move from a system structure to system design phase.

A.2 Method

This section outlines the method used to undertake the consultations.

Queensland University of Technology (QUT) and the University of South Australia (UniSA) were engaged to assist with the consultations.

Consultations were undertaken with stakeholders that were categorised into the following four groups. This was based on the following four components of C-ITS:

1. User layer: use of the system in order to obtain improved safety, mobility and environmental conditions.
2. Applications layer: provides functionality needed to improve safety, mobility and the environment.
3. Communication layer: provides access and/or connectivity between users through wireless communication.
4. Core system layer: provides functionality that facilitates secure exchange of trusted data, privacy and efficient data distribution.

The stakeholders consulted are outlined in Table A 8. The consultations were performed by UniSA, QUT and ARRB.

Table A 8: Stakeholders consulted

Group	Organisation and contact	UniSA, QUT or ARRB	Date and time of interview
User layer	DPTI SA: Phillip Blake and Mark Shotton	UniSA	Thursday 04/07/2013 9:30am–11:15am
User layer	RMS NSW: Victor Shapilsky	QUT	Tuesday 09/07/2013 10:00am–11:00am

Group	Organisation and contact	UniSA, QUT or ARRB	Date and time of interview
User layer	Qld TMR: Geoff McDonald	QUT	Thursday 04/07/2013 3:00pm–4:00pm
User layer	NZTA: Iain McAuley	QUT	Questionnaire response only
User layer	Australian Automobile Association: Craig Newland	UniSA	Friday 05/07/2013 10:00am–11:15am
User layer	Ministry of transport NZ: Iain McGlinchy	QUT	Thursday 04/07/2013 1:00pm–2:00pm
User layer	Truck Industry Council: Simon Humphries	UniSA	Tuesday 02/07/2013 9:30am–10:30am
User layer	Federal Chamber of Automotive Industries (FCAI): James Hurnall	UniSA	Wednesday 17/07/2013 2:30pm–3:30pm
User layer	National Road Safety Executive Group: John Wall	QUT	Thursday 04/07/2013 3:00pm–4:00pm
User layer	VicRoads: James Holgate	UniSA	Tuesday 09/07/2013 9:30am–10:30am
User layer	Office of Road Safety MRWA: Linley Cracknel	ARRB	Wednesday 24/07/2013 11:30am–12:30pm AEST
Applications/facilities layer	Intellimatics: Adam Game	UniSA	Questionnaire response only
Applications/facilities layer	Codha Wireless: Paul Gray	UniSA	Wednesday 03/07/2013 10:00am–10:45am
Applications/facilities layer	NeTC: Ian Oxworth of Connect East	UniSA	Monday 08/07/2013 3:30pm–4:30pm
Applications/facilities layer	Transmax: Jason Wagstaff	QUT	Tuesday 09/07/2013 3:15pm–4:15pm
Applications/facilities layer	Transport Certification Australia: Gavin Hill, Chris Koniditsiotis and Peter Girgis	QUT	Thursday 25/07/2013 1:00pm–2:00pm
Communication/ access layer	NICTA: Glenn Geers	QUT	Monday 08/07/2013 3:30pm–4:30pm
Communication/ access layer	UniSA: Alex Grant	UniSA	Monday 15/07/2013 11:00am–11:50am
Core layer	US DOT (various)	ARRB	Tuesday 04/06/2013 4:30pm–5:30pm AEST Followed by email correspondence throughout June 2013
Core layer	American Association of State Highway and Transportation Officials (AASHTO): James Wright	ARRB	Friday 31/05/2013 7:30am–8:30am AEST
Core layer	FRAME: Richard Bossom	ARRB	Tuesday 04/06/2013 5:30pm–6:30pm AEST Follow by email exchange
Core layer	Q-Free: Knut Evenson	ARRB	Tuesday 11/06/2013 4:30pm–5:30pm AEST

Consultations were undertaken by various means but generally commenced with an online questionnaire followed by a telephone and/or Skype conversation where further details/feedback were obtained.

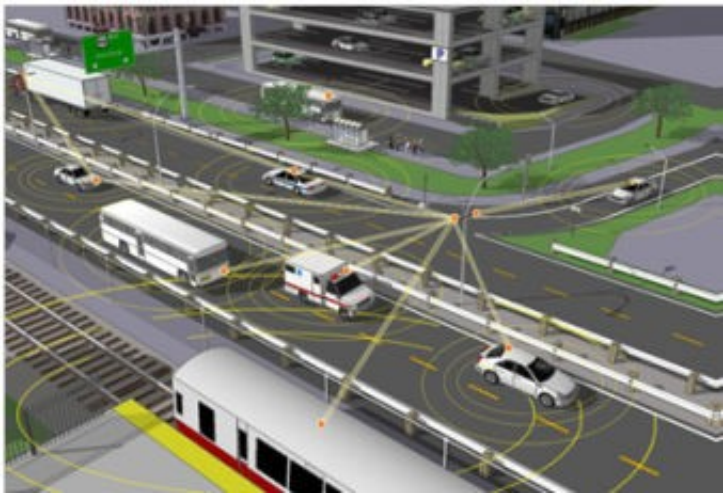
A.3 Questionnaires

This section contains the online questionnaire for the stakeholders from the user layer utilised during the consultations. Questionnaires for the other stakeholder groups were similar. Some questions were tailored to the specific user groups.

A.3.1 Questions (User Layer)

Introduction

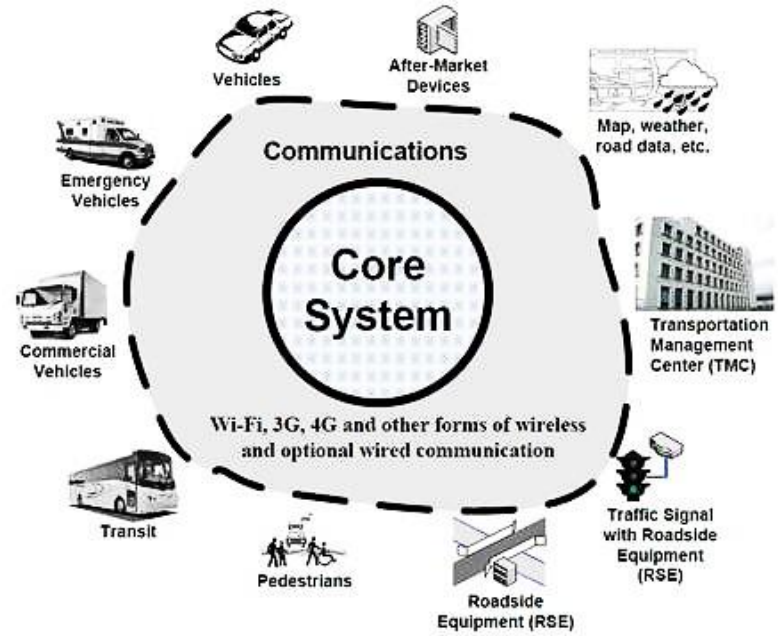
Cooperative intelligent transport systems (C-ITS) refers to real-time information sharing between vehicles and roadside infrastructure, and a new generation of applications that cooperatively work together to improve safety, productivity, efficiency and environmental outcomes for our transport system.

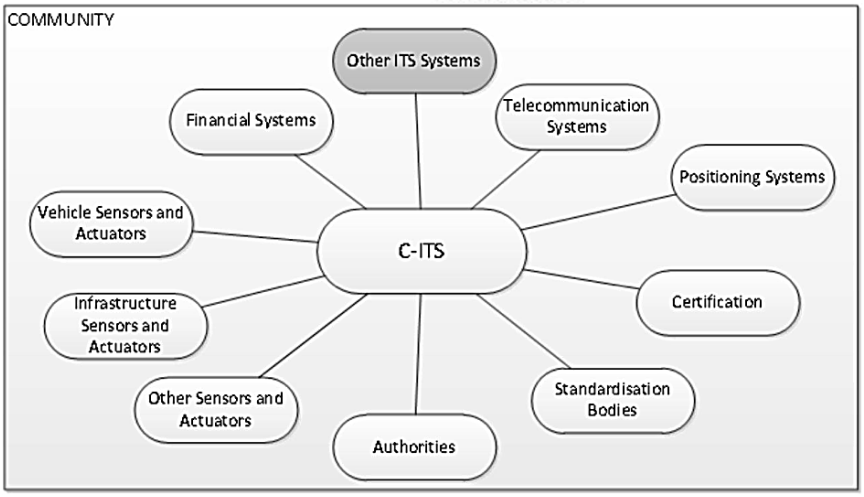


C-ITS involves vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication to enable cooperation between vehicles, and between vehicles and roadside infrastructure (as illustrated in the above figure). The goal is to create a ubiquitous wireless communication link that allows them to ‘talk’ to each other.

C-ITS technology comprises computer and wireless network components in vehicles and roadside infrastructure, supported by backend systems to coordinate information and manage system integrity. Significant design and development activities internationally with respect to C-ITS have delivered working prototype solutions that have been successfully trialled. The technology has reached a stage in its maturity cycle that allows for practical consideration of a broader adoption strategy.

As can be appreciated the C-ITS is a complex system with various interactions between vehicles, field infrastructure and centres as shown in the following figures:

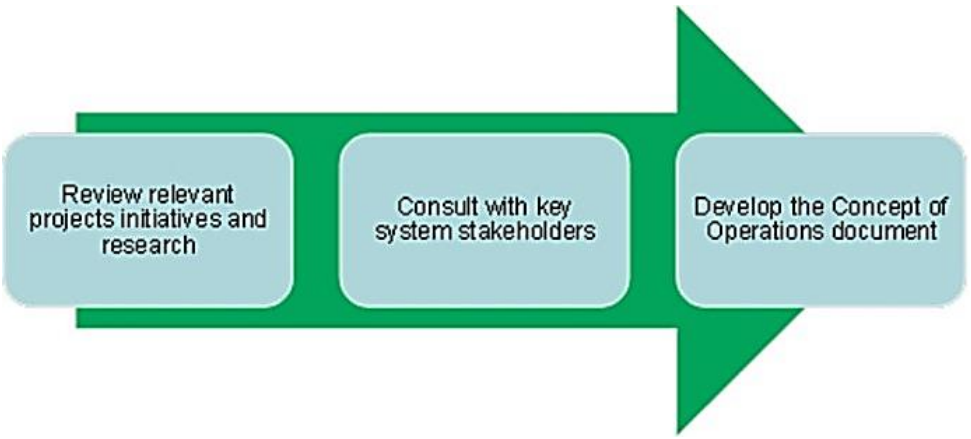




As such Austroads is looking to develop a Concept of Operations document that where possible will be closely aligned with international developments for C-ITS and will technically define a high-level view of the overall system to be developed in a context that each stakeholder can understand, such that it can be used to guide future activities around system requirements and design. As such it is the aim of Concept of Operations that it will:

- define the system's actors, their roles and responsibilities
- provide an overview of the emerging system design
- provide a high level description of how the system will operate
- identify issues with the operational framework.

The Concept of Operations is being developed over a three step process as shown in the figure below. The first step included a review of international documentation such as the US Core System Concept of Operations and European CVIS architecture and system specifications documents. The second step involves consultations. A key objective of the consultations is to obtain feedback from key stakeholders regarding who they see as the key actors in the proposed C-ITS environment, what role they think their organisation will play, and to explore other roles and issues that they think are critical to the successful operation of C-ITS locally.



In preparation for your discussion with UniSA, QUT or ARRB staff on C-ITS Core System Concept of Operations, please fill in the following questionnaire to the best of your ability. The topics and questions that follow will be the focus these later conversations:

- I. About you
  - 1. Your name
  - 2. Current position
  - 3. Organisation
  - 4. Respondent's field of expertise
- II. General view of C-ITS
  - 5. Which applications do you see being the critical ones for Australia and New Zealand?
  - 6. For these applications to function what do you see as the three most important functions of C-ITS (e.g. privacy, security etc.)?
    - 1.
    - 2.
    - 3.
  - 7. What would be the user needs? Rank them by priority/importance
    - 1.
    - 2.
    - 3.
  - 8. Is your organization preparing for the deployment of C-ITS? If so how?
- About Roles and Responsibilities :
  - 9. Which roles do you think your organisation might have?
    - User
    - Road operator/owner
    - Driver/traveller
    - C-ITS service provider Core system developer Communication provider Content provider
    - (C-ITS) infrastructure manufacturer
    - Mobile device manufacturer
    - Vehicle manufacturer
    - OEM

- Vehicle supplier
- Public key infrastructure/trusted third party
- Standardisation organisation Certification organisation Regulator
- Judiciaries
- Other

– Considering this list of Actors:

Role	Examples of actors
Policy	DoIT (inc ADR) NTC
Certification standards	DoIT (incl. ADR area) TCA
Road operator	Road Agencies, DPTI, RMS, TMR, NZTA VicRoads Body representing toll roads (TransUrban)
Vehicle OEM	FCAI, TIC
Equipment Manufacturer	Codha wireless Bosch
Service/content provider	Intellimatics Nokia
System management/integration/support	SCATS, Transmax, TCA, NICTA
User	AAA, NRSEG, TAC, Ministry of Transport

– 10. Considering the list of roles outlined earlier, which role do you see for these actors?

- Freight and fleet managers
- Drivers
- Motoring organisations
- Road agencies
- Austroads
- Tolling operators
- Rail operators
- Vehicle manufacturers
- Dealers
- Mobile device manufacturers
- Telecom Operators
- (C-ITS) infrastructure manufacturers
- Service providers
- Content/data providers
- International standardisation organisations
- National standardisation organisations
- Certification organisations (TCA)
- Regulator (Australian Communication and Media Authority, privacy commissioners)
- Department of Infrastructure and Transport
- Others

- 11. Do you think there are any types of actors missing?
- 12. What do you see as the role of government?

- III. Core System

The US Department of Transportation has developed a concept for a C-ITS core system that has three main functions:

1. Secure exchange of trusted data between users and applications without pre-existing relationship or entering into a permanent relationship.

2. Assurance of privacy between users and from third parties.

3. More efficient data collection from various sources and distribution to many users.

1) Certification

For obvious reason (compatibility, safety, security) the devices and the software involved in the system will need to meet specifications:

- 13. What certification process required? (Standards, quality testing, how open/restricted?)
  - For time-critical safety applications?
  - For other applications?
  - Should certification be part of the Core System?
- 14. Who is the best suited to manage the certification process? (State Authority? Car manufacturer?). Does it depend on the application?
  - For time-critical safety applications?
  - For other applications?
  - For the Core System?

2) Security management

Some characteristics of the system may need to be considered at different scales (the handling of misbehaving users, the definition of user groups) to take into account the local specificities.

- 15. How could we ensure a nationwide consistency of the system?

3) Data provision/ownership

Firstly, the data may be of a great importance for public agencies wishing to manage their transportation networks.

Secondly, the ownership of the produced data is a critical factor for the secondary market (e.g. development of complementary/additional applications by third parties).

Thirdly, it is at the same time a means for private agencies to preserve the investment they may have put into the collection of that data.

- 16. Do you see any conflicts that may arise from the ownership of the data?
- 17. Which data should be open? Which one should be private (and who should own them)?

Incentives

- 18. Do you think incentives will be needed for travellers to provide their data? If yes, which kind? (Financial? Added services?)

4) System performance management

- 19. The system should be able to identify malfunctioning devices that might indicate a risk to the Connected Vehicle environment. To what extent should the system be able to monitor the connected devices? (trade-off between safety/security and privacy)

5) Other

  - 20. What do you believe to be the critical operational policy areas from the viewpoint of your organisation? Can you provide details/examples why?

- V. Operational scenarios
  - 21. Please fill the blanks for three of the following operational scenarios

	Inputs	Enablers	Controls	Outputs
Contextual speed				
Vehicle probe data				
Signal phasing and timing information				
In-vehicle traveller information				
Railway level crossing				
Toll Roads				

  - 22. Are there other operational scenarios arising?

- VI. Conclusion
  - 23. Do you wish to add any other comments that you believe are relevant and have not been covered already by the questionnaire?
    - What are other problems or opportunities addressed by the system?
    - Are there any specific technologies of interest?
    - Other?

Appendix B Core Needs

This appendix lists the needs that are driving the definition of the core functions. It includes an overview of the needs and priorities, a description, and rationale for each need.

The description of the needs and most of the rationale are from the US Core System Concept of Operations (Research and Innovative Technology Administration 2011).

B.1 Overview of Core Needs and Priorities

Table B 1 provides a list of the core needs, the priority for the Australian and New Zealand context, and a reference to the priorities defined in the US *Core System: Concept of Operations*. The rationale for Australia and New Zealand is based on the limitations of the current situation as described in Section 4.1.2.

Generally, the rationale is the same as for the US *Core System: Concept of Operations*. The rationales are described below in Appendix A.3 of this appendix.

Table B 1: Core needs and rationale for AUS/NZ priorities

No.	Core need	Priority AUS/NZ	Rationale AUS/NZ	Priority US
1	Data protection	Essential	Same as US rationale	Essential
2	Core trust	Essential	Same as US rationale	Essential
3	System user trust	Essential	Same as US rationale	Essential
4	Core trust revocation	Essential	Same as US rationale	Essential
5	System user trust revocation	Essential	Same as US rationale	Essential
6	Authorisation management	Essential	Same as US rationale	Essential
7	Authorisation verification	Essential	Same as US rationale	Essential
8	Misbehaviour management	Essential	Same as US rationale	Essential
9	Time base	Essential	Same as US rationale	Essential
10	Data request	Desirable	Same as US rationale	Desirable
11	Data provision	Desirable	Same as US rationale	Desirable
12	Data forward	Desirable	Same as US rationale	Desirable
13	Network connectivity	Essential	Same as US rationale	Essential
14	Geographic broadcast	Desirable	Same as US rationale	Desirable
15	Core system service status	Desirable	Same as US rationale	Desirable
16	System integrity protection	Essential	Same as US rationale	Essential
17	System availability	Essential	Same as US rationale	Essential
18	System operational performance monitoring	Essential	Same as US rationale	Essential
19	Core system independence	Not applicable	Proposed AUS/NZ system is single national C-ITS platform	Essential
20	Core system interoperability	Not applicable	Proposed AUS/NZ system is single national C-ITS platform	Essential
21	Core system interdependence	Not applicable	Proposed AUS/NZ system is single national C-ITS platform	Essential
22	Core system data protection	Essential	Same rationale as data protection	Not available
23	Anonymity preservation	Essential	Essential to meet AUS/NZ privacy guidelines and regulations	Not available
24	Private network connectivity	Essential	Same as rationale for network connectivity	Not available

No.	Core need	Priority AUS/NZ	Rationale AUS/NZ	Priority US
25	Private network routing	Optional	Routing can be done by network and transport layer	Not available

B.2 Description of Core Needs

The Australian and New Zealand core needs are largely the same as those in the USA, since the purpose of the core is the same. The descriptions in the US Concept of Operations are adopted and are presented below:

1. **Data Protection:** The Core System needs to protect data it handles from unauthorised access. This is required to support applications that exchange sensitive information, such as personally identifying or financial information, which if intercepted could compromise the privacy or financial records of the user.
2. **Core Trust:** The Core System needs to establish trust with its System Users. Such trust relationships are necessary so that the Core System can be assured that System Users are who they say they are, and therefore trust the source and data it receives.
3. **System User Trust:** The Core System needs to facilitate trust between System Users. Such trust relationships are necessary so that System Users can be assured that other System Users are who they say they are, and therefore trust the source and data they receive from other System Users.
4. **Core Trust Revocation:** The Core System needs to revoke the trust relationship it has with its System Users when necessary. A trusted System User may operate in a fashion that indicates they should no longer be trusted, in which case the Core System must have a way of revoking that trust.
5. **System User Trust Revocation:** The Core System needs to facilitate the revocation of the trust relationships between System Users when necessary. A trusted System User may operate in a fashion that indicates they should no longer be trusted, in which case the Core System must have a way of facilitating revocation of trust between System Users.
6. **Authorisation Management:** The Core System needs to manage authorisation mechanisms to define roles, responsibilities and permissions for System Users. This enables the Core System to establish operational environments where different System Users may have different capabilities in terms of accessing Core services and interacting with one another. For instance, some Mobile elements may be authorised to request signal priority, or some Centres may be permitted to use the geographic broadcast service, while those without those permissions would not.
7. **Authorisation Verification:** The Core System needs to verify that System Users and Core Operations Personnel are authorised to perform an attempted operation. This enables the Core System to restrict operations to those users who are permitted to use those operations. For example, geo-broadcast may be restricted to transportation or public safety agencies, so other users may be prohibited from performing geo-broadcasts.
8. **Misbehaviour Management:** The Core System needs to identify System Users acting as bad actors. Bad actors are not necessarily malicious; they could be malfunctioning devices that may interfere with other System Users, Communication Layer Systems or the Core System. Identifying bad actors enables subsequent action to protect the integrity of all users sharing the transportation environment.
9. **Time Base:** The Core System and System Users need to operate on a common time base. Coordination of time between the internal systems that operate the Core System prevents internal synchronisation errors and enables time-sensitive interactions with System Users.

10. **Data Request:** The Core System needs to provide a mechanism for data consumers to request data that is produced by data providers. This is a single request for a subscription to a certain type of data, and subsequent modification of the request to change data types or subscription parameters. Parameters include data frequency, type and location of where the data was generated. This enables the distribution of anonymously-provided data to interested data consumers, without requiring them to enter into a relationship with data providers. Request formats need to provide data consumers with the ability to differentiate and receive only the types of data they requested. For example this includes data type, geographic range, frequency and sampling rate. This request method supports a wide variety of user needs, from planners requesting all traffic data all the time, to traveller information services requesting a subset of traffic data, to weather information services only interested in windshield wiper status for vehicles in a specific area.
11. **Data Provision:** The Core System needs to supply information to data providers enabling them to transmit data to interested data consumers. At a minimum, data characteristics need to include type, frequency and location where data was generated, so that users that have requested data (see need data request) can differentiate between available data. This need enables data providers to direct the data they create to data consumers, and serves as the provider-side corollary to the data request need. This supports a variety of applications, including those focussed on the centre provision of data to users. It also serves as the answer to the System User‘s question of – I have data, how do I provide it and to whom?
12. **Data Forward:** The Core System needs to provide a mechanism to distribute data that is produced by a System User acting as a data provider and requested by another System User. The Core System needs to provide this distribution mechanism, rather than relying on individual provider-consumer relationships, because multiple consumers may want access to the same data. By having the Core System distribute the data, System Users are relieved of the need to transmit the data multiple times. Also, some data may be critical to the proper functioning of mandatory applications, such as data supporting geo-location of users (position corrections), time base data and roadway geometry data, all of which likely comes from a single source and needs to be distributed to large numbers of System Users. Additionally, System Users may interact over resource-constrained communication links, so Core-provided data redistribution reduces the potential load on those links.
13. **Network Connectivity:** The Core System needs to connect to the Internet. This allows the Core to provide services to any System User capable of connecting to the Internet.
14. **Geographic Broadcast:** The Core System needs to provide the information necessary for System Users who wish to communicate with a group of System Users in a specific area to do so. This capability enables System Users to target those in a specific area for information they wish to distribute without having to send individual messages to each recipient. Examples of applications that might use this include Amber Alerts, traffic information, and air quality alerts.
15. **Core System Service Status:** The Core System needs to be able to monitor the status of Core System services and provide accurate status information to System Users. The Core System can then inform Core Operations Personnel when a service operates in abnormal or degraded fashion. Additionally, System Users may not be able to access a Core System service (because of their location for example) and would want to know where and when they could expect access to the Service.
16. **System Integrity Protection:** The Core System needs to protect its integrity. This includes defence against the loss of integrity from a deliberate attack, software bug, environmental or hardware failure. Protection of the Core System ensures that System Users have a high confidence in the security of the information they entrust to the Core System.
17. **System Availability:** The Core System needs to be available for System Users to access Core System Services. This includes both operational availability and the predictable return to normal operations after service degradation. Availability and a predictable return to normal operations ensures that System Users have a high confidence in the ability of the Core System to provide the services they require.
18. **System Operational Performance Monitoring:** The Core System needs to monitor its performance. This includes the status of interfaces, services, and metrics for the demand for services and the resolution of those demands. Monitoring the performance of Core System services and interfaces is necessary to understand when the system is operating properly, and to gauge when the system may be nearing capacity so that action may be taken to prevent the system from failing to provide services, e.g. maximum number of transactions/second, or internal communication bandwidth.

19. **Core System Independence:** The Core System needs to be independently deployed and operated, providing Core System services to all System Users within its operational scope. This ensures that one entity's Core System deployment is not contingent on or dependent on another for basic functionality.
20. **Core System Interoperability:** The Core System needs to provide services in such a way that if a mobile user moves into an area of another Core System, their interface to the Core System still operates. This helps manage user expectations and helps ensure that when a mobile user subscribes to a service or installs an application, the user experience is consistent across multiple Core Systems.
21. **Core System Interdependence:** The Core System needs to operate in coordination with other Core Systems. This ensures that Core services deliver information that is consistent with information delivered by other Core systems, which will help avoid inconsistencies and incompatibilities between Cores and between System Users interacting with multiple Cores.
22. **Core System Data Protection:** The Core System needs to protect data it maintains from unauthorised access. This ensures that information held by the Core, which may include sensitive information about System Users, is accessed only by authorised users.
23. **Anonymity Preservation:** The Core System needs to preserve the anonymity of anonymous System Users that use its services. This ensures that System Users communicating with the Core who wish to remain anonymous will not have their anonymity breached as a result of communicating with the Core.
24. **Private Network Connectivity:** The Core System needs to connect to a private network. This allows the Core to provide services to any System User that provides a private network connection to the Core, which contributes to meeting the deploy-ability goal. It also allows Cores to establish dedicated connections between them, which contributes to the Cores collectively meeting goals of scalability, maintainability and reliability.
25. **Private Network Routing:** The Core System needs to route communication between other Cores and System Users, when one or both of the parties involved in the communication is connected to the Core by a private network. This enables System Users connected by private network to interact with Centre-based applications, and also facilitates backup operations between Cores.

B.3 Australian and New Zealand Rationale for Core Needs

The priority for each of the core needs has been assessed from the Australian and New Zealand perspective. Generally, the rationale for the US priority is applicable to the Australian and New Zealand situation as well. Where the US rationale is applicable, the rationale descriptions from the US Concept of Operations are provided.

Needs are categorised into **essential**, **desirable** and **optional**.

Essential needs are provided by the core functions. Essential features are those which are minimally required to enable V2V and V2I safety, mobility and environmental applications. Desirable needs should be provided by the core functions to realise efficient operation of the C-ITS. Reasons why the needs are desirable are explained for each desirable feature. A feature may be considered desirable if it provides benefit, but is not minimally required in order to deploy safety, mobility and environmental applications. Optional needs are functions for which no coordination is required, so they can also be provided by other components of C-ITS:

1. Data protection

   Priority: Essential – Same as US

   Rationale: Without the ability to exchange data securely, privacy could be compromised, mobility applications that use financial data (e.g. tolling) would be more cumbersome to deploy, and any applications requiring the exchange of information that users would want to protect would be either easily compromised or never developed.

2. Core trust

   Priority: Essential – same as US

Rationale: Without the ability for the Core to trust System Users, it cannot trust the information they provide. If the Core cannot trust information from System Users, it cannot facilitate trust between System Users.

3. System User trust

   Priority: Essential – same as US

   Rationale: Without the ability to trust another user, many safety and mobility applications requiring interaction between System Users are not viable. System User trust can be established by any trusted Core System; once a System User's trustworthiness is established by one trusted Core it will be acknowledged by all System Users.

4. Core trust revocation

   Priority: Essential – same as US

   Rationale: Revocation is required to ensure trust; without revocation, many safety and mobility applications are not viable. The Core must revoke its trust relationship with a misbehaving System User to protect itself and the data it passes.

5. System Yser trust revocation

   Priority: Essential – same as US

   Rationale: Revocation is required to ensure trust; without revocation, many safety and mobility applications are not viable. Relationships between System Users must be revoked to ensure that misbehaving System Users do not compromise the safety or privacy of other System Users. This may not be done by every Core System, but must be done for every misbehaving System User.

6. Authorisation management

   Priority: Essential – same as US

   Rationale: Authorisation management is necessary to control access to system services and controls. Without authorisation management, the Core would be insecure, jeopardising the provision of any service.

7. Authorisation verification

   Priority: Essential – same as US

   Rationale: Authorisation verification is necessary to control access to system services and controls. Without authorisation verification, the Core would be insecure, jeopardising the provision of any service.

8. Misbehaviour management

   Priority: Essential – same as US

   Rationale: Without misbehaviour management, misbehaving actors could affect the operation of Core System services. Not including this service decreases the overall security and usability of a Core System service. Communication could still be enabled without Misbehaviour Management, but the level of trust between users would be compromised. This should not affect safety, but may affect mobility convenience applications, particularly those requiring financial transactions.

9. Time base

   Priority: Essential – same as US

   Rationale: Most applications require time coordination. While the Core System does not directly operate applications, it passes data that has time fields and that may support applications. Further, mechanisms used to ensure trust may use a time-based expiration mechanism. Without a consistent time base used by the Core System that is also available to System Users, success of time-sensitive applications will be limited and trust mechanisms constrained.

10. Data request

    Priority: Desirable – same as US

Rationale: Many mobility and environmental applications will require data to be exchanged between System Users. A Core that does not include Data Request or Data Provision would not serve the needs of System Users that need data from other System Users. If the Core System does not provide a data distribution mechanism, applications will need to provide the data exchange.

11. Data provision

    Priority: Desirable – same as US

    Rationale: Many mobility and environmental applications will require data to be exchanged between System Users. A Core that does not include Data Request or Data Provision would not serve the needs of System Users that need data from other System Users. If the Core System does not provide a data distribution mechanism, applications will need to provide the data exchange.

12. Data forward

    Priority: Desirable – same as US

    Rationale: This includes all of the Data Forward need except for the concepts parsing, sampling and data aggregation.

13. Network connectivity

    Priority: Essential – same as US

    Rationale: Network Connectivity is required for the Core System to provide services to any System User not able to provide a private connection to the Core System. It is thus an enabler for applications that pass data using the Core's services, and for applications that rely on the trust relationships between System Users that are facilitated by the Core's trust management services.

14. Geographic broadcast

    Priority: Desirable – same as US

    Rationale: Without geographic broadcast, individual messages will have to be sent from System User to System User, or System Users will have to manage their own multicast or broadcast operations. This will make the provision of data to groups of System Users more difficult and less efficient than if the Core System provides geographic broadcast.

15. Core system service status

    Priority: Desirable – same as US

    Rationale: Core System Service status helps set System User expectations. Without awareness of Core System service status, applications may attempt to access services that are not available, which could adversely affect communication resource use.

16. System integrity protection

    Priority: Essential – same as US

    Rationale: Without the ability to ensure the integrity of Core System services, those services could be hijacked or corrupted, compromising service delivery.

17. System availability

    Priority: Essential – same as US

    Rationale: If the Core System is not working, it cannot provide services.

18. System operational performance monitoring

    Priority: Essential – same as US

    Rationale: Without operational performance monitoring, it will be difficult to know when the system degrades or fails; managing maintenance and repair activities will be extremely difficult, and overall system reliability will suffer. This will lead to a reduced level of service.

19. Core system independence

    Priority: Not Applicable – proposed AUS/NZ system is single national C-ITS platform

20. Core system interoperability

    Priority: Not Applicable – proposed AUS/NZ system is single national C-ITS platform

21. Core system interdependence

    Priority: Not Applicable – proposed AUS/NZ system is single national C-ITS platform

22. Core system data protection

    Priority: Essential – US rationale not available

    Same rationale as data protection.

23. Anonymity preservation

    Priority: Essential – US rationale not available

    Rationale: Essential to meet AUS/NZ privacy guidelines and regulations.

24. Private network connectivity

    Priority: Essential – US rationale not available

    Rationale: Same as rationale for Network Connectivity.

25. Private network routing

    Priority: Optional – US rationale not available

    Rationale: Routing can be done by network and transport layer.

Appendix C C-ITS Applications and Use Cases

The European Telecommunication Standards Institute (ETSI) has a list of potential applications and use cases that are considered as deployable after a first complete set of C-ITS standards is available. The complete list of the potential use cases is presented in Table C 1 as examples of C-ITS applications that the core functions should be able to support.

Table C 1: ETSI use cases

Application	UC no.	Use case
Driving assistance – cooperative awareness	UC001	Emergency vehicle warning
	UC002	Slow vehicle indication
	UC003	Intersection collision warning
	UC004	Motorcycle approaching indication
Driving assistance – road hazard warning	UC005	Emergency electronic brake lights
	UC006	Wrong-way driving warning
	UC007	Stationary vehicle – accident
	UC008	Stationary vehicle – vehicle problem
	UC009	Traffic condition warning
	UC010	Signal violation warning
	UC011	Roadwork warning
	UC012	Collision risk warning
	UC013	Use of decentralised floating car data for hazardous location detection
	UC014	Use of decentralised floating car data for precipitations detection
	UC015	Use of decentralised floating car data for road adhesion detection
	UC016	Use of decentralised floating car data for visibility detection
	UC017	Use of decentralised floating car data for wind detection
Speed management	UC018	Regulatory/contextual speed limits notification
	UC019	Traffic light optimal speed advisory
Cooperative navigation	UC020	Traffic information and recommended itinerary
	UC021	Enhanced route guidance and navigation
	UC022	Limited access warning and detour notification
	UC023	In-vehicle signage
Location-based services	UC024	Point-of-interest notification
	UC025	Automatic access control and parking management
	UC026	ITS local electronic commerce
	UC027	Media downloading
Communities services	UC028	Insurance and financial services
	UC029	Fleet management
	UC030	Loading zone management
ITS Station life cycle management	UC031	Vehicle software/data provisioning and update
	UC032	Vehicle and roadside unit data calibration

Source: Adapted from ETSI TS 102 637.

Appendix D Document Structure Mapping to IEEE 1362-1998: 2007 for Concept of Operations

Table D 1 shows how the document structures compares to the standard document structure for a Concept of Operations as per the IEEE 1362-1998:2007 standard document. The main reason for diverting from the standard document format is that the standard document structure does not include sections on stakeholders, roles and responsibilities, which are an important element of the Concept of Operations for the core functions. For comparison, the structure of the US C-ITS core Concept of Operations is included as well.

Table D 1: Document structure mapping to IEEE 1362-1998:2007 for Concept of Operations

IEEE 1362-1998: 2007 Concept of Operations	Australian C-ITS core Concept of Operations	US C-ITS core Concept of Operations
1. Scope	1. Scope	1. Scope
1.1 Identification	1.1 Identification	1.1 Identification
1.2 Document Overview	1.2 Document Overview	1.2 Document Overview
1.3 System Overview	1.3 System Overview	1.3 System Overview
		1.4 Stakeholders
2. Referenced Documents	2. References	2. Documents
		2.1 Referenced Documents
		2.2 Resource Documents
3. Current System or Situation	3. Current Situation	3. Current System
3.1 Background, Objectives, and Scope	3.1 Background	3.1 Background, Objectives, and Scope
3.2 Operational Policies and Constraints	3.2 Policies	3.2 Operational Policies and Constraints
3.3 Description of the Current System or Situation	3.3 Description of the Current Situation	3.3 Description of the Current System
3.4 Modes of Operation for the Current System or Situation		3.4 Modes of operation for the Current System
3.5 User Classes and other Involved Personnel		
3.6 Support environment		
4. Justification for and Nature of Changes	4 Justification for and Nature of Changes	4. Justification for and Nature of Changes
4.1 Justification of Changes	4.1 Justification for Changes	4.1 Justification for Changes
4.2 Description of Desired Changes	4.2 Description of the Desired Changes	4.2 Description of Desired Changes
4.3 Priorities among Changes	4.3 Priorities Among Changes	4.3 Priorities among Changes
4.4 Changes Considered but not included	4.4 Changes Considered but not Included	4.4 Changes Considered but not Included
4.5 Constraints and Assumptions	4.5 Constraints and Assumptions	4.5 Constraints and Assumptions
5. Concepts for the Proposed System	5. Concepts for the Proposed System	5. Concepts for the Proposed System
5.1 Background, Objectives, and Scope	5.1 Background, Objectives and Scope	5.1 Background, Objectives and Scope
5.2 Operational Policies and Constraints	5.2 Operational Policies and Constraints	5.2 Operational Policies and Constraints
5.3 Description of the Proposed System	5.3 Description of the Proposed System	5.3 Description of the Proposed System
5.4 Modes of Operation	5.4 Modes of Operation	5.4 Modes of Operation
5.5 User Classes and other Involved Personnel	5.5 Organisational Structure	5.5 User Types and other Involved Personnel
5.6 Support Environment	5.6 Support Environment	5.6 Support Environment
6. Operational Scenarios	6. Operational Scenarios	6. Operational Scenarios
7. Summary of Impacts	7. Summary of Impacts	7. Summary of Impacts

IEEE 1362-1998: 2007 Concept of Operations	Australian C-ITS core Concept of Operations	US C-ITS core Concept of Operations
7.1 Operational Impacts	7.2 Operational Impacts	7.1 Operational Impacts
7.2 Organizational Impacts	7.3 Organisational Impacts	7.2 Organizational Impacts
7.3 Impacts during Development	7.3 Impacts during Development	7.3 Impacts during Development
		7.4 Measuring the Impacts
8. Analysis of the Proposed System	8. Analysis of the Proposed System	8. Analysis of the Proposed System
8.1 Summary of Improvements	8.1 Summary of Improvements	8.1 Summary of Improvements
8.2 Disadvantages and Limitations	8.2 Disadvantages and Limitations	8.2 Disadvantages and Limitations
8.3 Alternatives and Trade-Offs Considered	8.3 Alternatives and Trade-offs Considered	8.3 Alternatives and Trade-offs Considered
9. Notes		9. Notes
Appendices	Appendices	Appendices
Glossary	Glossary	Glossary

Glossary

Terms and Definitions

Actor	Party participating in a system.
Application, app	Software application to provide functionality to realize C-ITS.
Application programming interface (API)	Specifies how software components should interact with each other. In practice, most often an API is a library that includes specifications for routines, data structures, object classes, and variables.
Bounded secure managed domain (BSMD)	Secure peer-to-peer communication between entities (ITS-stations) that are themselves capable of being secured and remotely managed. The bounded nature is derived from the requirement for ITS-stations to be able to communicate amongst themselves, as well as with devices that are not secured (referred to as 'other ITS-stations'). Within C-ITS and ISO 21217 such ITS-stations are defined as operating within bounded secured managed domains (BSMD), or outside of the BSMD.
C-ITS	Group of ITS technologies that uses wireless communication to share information between vehicles, between vehicles and roadside infrastructure and between vehicles and centres. This will allow vehicle and transport applications to cooperatively work together to deliver outcomes that are beyond what is achievable with standalone ITS and vehicle applications.
C-ITS device	The combination of hardware, firmware and software used for C-ITS service provision, including all functions of the ITS-station (ISO 21217). C-ITS devices can be part of vehicles (either build in when first manufactured or retrofitted), ITS roadside equipment or mobile devices such as smart phones or mobile navigation devices.
Centre/central system	Management centres to support centralised control functions and supporting services managed through a central facility. Traditionally these are traffic management centres or commercial back office centres. Examples of centralised 'core functions' are generation of security certificates and misbehaviour management.
Communication	Wireless (and in some cases wireline) networks that facilitate data exchange, including roadside ITS-stations where appropriate.
Concept of Operations (ConOps)	Document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system; it is used to communicate the quantitative and qualitative system characteristics to all stakeholders.
Core functions	Combination of enabling technologies and services that will provide the foundation for the support of a distributed, diverse set of applications/application transactions which works in conjunction with support systems from certificate authorities. The system boundary for the core functions is not defined in terms of devices or agencies or vendors, but by the open, standardised interface specifications that govern the behaviour of all interactions between core function users.
End user	Citizen who exercises or benefits from the services of the transport system.
Equipped vehicles	Vehicles equipped with the communication and data collection and processing capacity (ITS-stations) to perform in the C-ITS context.
Global navigation satellite system (GNSS)	Comprises several networks of satellites that transmit radio signals containing time and distance data that can be picked up by a receiver, allowing the user to identify the location of its receiver anywhere around the globe.
Intelligent transport system (ITS)	Transport systems in which advanced information, communication, sensor and control technologies, including the Internet, are applied to increase safety, sustainability, efficiency, and comfort.
ITS application	Functionality that either completely provides what is required by an ITS service or works in conjunction with other ITS applications to provide one or more ITS services.
ITS service	Functionality provided to transport system users.
IT-station, ITS-s	Entity in a communication network (comprised of application, facilities, networking and access layer components) that is capable of executing ITS-S application processes

	(sometimes within a bounded, secured, managed domain), comprised of an ITS-S facilities layer, ITS-S networking and transport layer, ITS-S access layer, ITS-S management entity and ITS-S security entity, which adheres to a minimum set of security principles and procedures so as to establish a level of trust between itself and other similar ITS-stations with which it communicates.
Support systems	Facilities that assist in C-ITS service provision, including security credentials certificate and registration authorities, and thus allow devices and systems to establish trust relationships.

Abbreviations and Acronyms

2G	Second generation cellular phone technology e.g. GSM
3G	Third generation mobile phone technology e.g. UMTS
4G	Fourth generation mobile phone technology e.g. LTE
ADAS	Advanced driver assistance systems
API	Application programming interface
BSM	Basic safety message
BSMD	Bounded secure managed domain
CALM	Communications access for land mobiles
CAM	Cooperative awareness message
CAMP	Crash avoidance metrics partnership
CEN	European committee for standardization
C-ITS	Cooperative intelligent transport systems, cooperative ITS
ConOps	Concept of Operations
CRL	Certificate revocation list
CVIS	Cooperative vehicle infrastructure systems
DAB+	Digital audio broadcast
DENM	Decentralised environmental notification message
DoT	Department of transport
DSSS	Driving safety support system
ETSI	European telecommunications standards institute
FM	Frequency modulated
FRAME	European ITS framework architecture
GNSS	Global navigation satellite systems
GSM	Global system for mobile communication (2G mobile communications)
HMI	Human machine interface
IEEE	Institute of electrical and electronic engineers
IPv6	Internet protocol version 6
ISO	International organization for standardization
ITS	Intelligent transport systems
ITS-s	ITS-station
IVI	In-vehicle information
IVS	in-vehicle system
LAN	Local area network
MAP	Geometric intersection description
NTC	National transport commission

OSI	Open systems interconnection
PDM	Probe data management
PII	Personally identifiable information
PKI	Public key infrastructure
PVD	Probe vehicle data
PVM	Probe vehicle message
RDS-TMC	Radio data system – traffic message channel
RSA	Roadside alert message
RSE	Roadside equipment
SAE	Society of automotive engineers
SAM	Service announcement message
SCMS	Security credential management system
SPaT	Signal phase and timing message
SRM	Signal request message
SSM	Signal status message
TCA	Transport Certification Australia
TPEG	Transport protocol expert group
UNECE	United Nations economic commission for Europe
V2I	Vehicle to/from infrastructure
V2V	Vehicle to vehicle
WAVE	Wireless access in vehicular environments
WLAN	Wireless local area network
WTOTBT	World Trade Organisation's treaty on technical barriers to trade

Austroads

Level 9, 287 Elizabeth Street
Sydney NSW 2000 Australia

Phone: +61 2 9264 7088

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