AUDAX AT FIDELIS

Queensland
Government

Office of the
Director-General

Department of
Transport and Main Roads

Our ref: DG35835

19 NOV 2018

Dr Geoff Allan
Acting Chief Executive
National Transport Commission
Level 3 600 Bourke Street
MELBOURNE VIC 3000

Dear Dr Allan

Thank you for your letter of 27 September 2018 and the opportunity to make a submission to the National Transport Commission's (NTC) discussion paper on Regulating Government Access to Cooperative Intelligent Transport Systems (C-ITS) and Automated Vehicle (AV) Data.

I acknowledge that NTC is seeking whole-of government submissions to national AV policy reform projects. However, due to limited timeframes available for government approval, a Queensland Government response was not possible. Instead, the Department of Transport and Main Roads (TMR) offers the attached submission for your consideration. In the development of this submission, TMR, nevertheless, consulted with key Queensland Government agency stakeholders and input has been incorporated where relevant.

The enclosed submission has been drafted in response to NTC's discussion paper as well as the consultation workshop facilitated by NTC in Brisbane on 29 October 2018. It is understood that NTC is seeking jurisdictional views on whether further exploration of privacy issues associated with C-ITS and AV data are warranted. TMR is of the view that further work is required, and our submission offers suggestions for rescoping a more holistic review of information access, storage, use, disclosure and destruction.

The Queensland Government and TMR looks forward to continued partnership with NTC in the development and implementation of an end-to-end regulatory framework to facilitate the safe deployment of AVs in Australia.

If you have any questions or would like to discuss the TMR submission further, I encourage you to contact Mr Nick Mackay, Manager (Automated Vehicle Regulation), by telephone on (07) 3066 2840 or email at nicholas.l.mackay@tmr.qld.gov.au.

I trust this information is of assistance.

Yours sincerely

NScales

Neil Scales
Director-General
Department of Transport and Main Roads

Enc (1)

Department of Transport and Main Roads

Transport jurisdictions collection of Cooperative and Intelligent Transport System (C-ITS) and Connected and Automated Vehicle (CAV) data?

Prepared by	Miranda Blogg – Director
Telephone:	3066 8251
Branch/District	CAVI, Land Transport Safety
Division/Region	Customer Services, Safety & Regulation
Location	Floor 9, 61 Mary Street, Brisbane
Version date	7 November 2018
Status:	Final
DM ref. no.	

Queensland Government

Purpose

The purpose of this document is to provide a summary of transport jurisdictions collection of Cooperative Intelligent Transport Systems (C-ITS) – commonly referred to as connected vehicle data - and connected and automated vehicle (CAV) data.

The document includes the following sections:

- Today's collection of road operations data
- Day 1 or connected vehicle data collection
- Day 2 connected and automated vehicle data collection
- Day 3+ use-cases

1. Definitions and acronyms

Term	Meaning/Understanding
C-ITS	Cooperative Intelligent Transport Systems
CAV	Connected and automated vehicles
CCMS	Cooperative Credential Management System (security)
GDPR	European's General Data Protection Requirements
ITS	Intelligent Transport Systems

2. Today's collection of road operations data

Today, transport agencies operate intelligent transport systems (ITS) that include signalised intersections and motorway variable speed limits, variable message signs, ramp signals and lane control. Real-time traffic volume, speed, and occupancy are collected at these locations. A subset of these locations are also equipped with webcameras; and bluetooth devices that collect MAC addresses from passing drivers. This data is used in real time for traffic operations and aggregated and stored for transport planning, safety and capacity projects.

Industry is increasingly offering customers connected vehicle services that include vehicle maintenance, infotainment, and traveller information. Through the connected vehicle services, industry can collect the vehicle data and may also have access to personal information about the customer. Unlike industry, the ITS data captured by government transport agencies does not imply origin-destination. Data is collected at limited points across the transport network and does not constitute private information.

As illustrated in figure 1, transport agencies are connected to ITS infrastructure. Industry is becoming increasingly connected to the vehicle, but there is typically no connection between vehicles, between vehicles and infrastructure, or the transport jurisdictions' and industry back-office systems. To support current road operations business, transport agencies often purchase vehicle data from industry – which is historical, aggregated, and depersonalised.

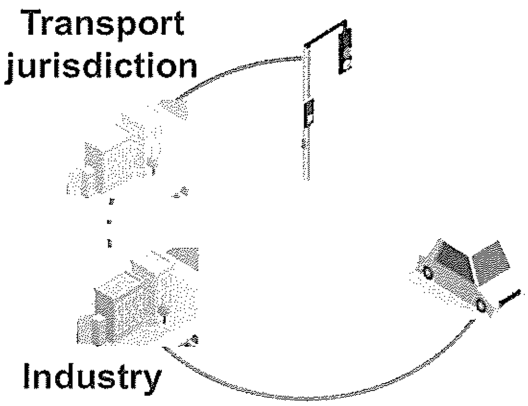


Figure 1: Today's government and industry services are not connected

3. What is a C-ITS?

A Cooperative Intelligent Transport System supports wireless communication of information between vehicles, roadside infrastructure, mobile devices and traffic management centres. This allows transport users to connect and work together cooperatively to deliver outcomes that are beyond what is achievable with standalone ITS or connected vehicle services.

There are hundreds of potential connected vehicle use-cases across multiple modes with a variety of societal benefits including safety, mobility, emissions and comfort. A list is available at https://local.iteris.com/arc-it/html/servicepackages/servicepackages-areaspsort.html. Public benefits from these technologies are large with even conservative national estimates in reduced congestion ($20Bp.a.) and road trauma ($27B p.a.) significant. The benefit-to-cost ratio expected by Europe, USA, and Queensland is in excess of $3 in benefit for every $1 spent

As agreed informally by industry and government through Austroads, C-ITS in Australia will align with European standards. Figure 2 illustrates this system, with C-ITS standards supporting the connection between vehicles, and vehicles and infrastructure. The standards are currently limited to short-range communication (referred to as ITS G5) – with a minimum communications range of 300 metres, up to a kilometre. Per Figure 1, the back-office systems from government to infrastructure and industry to vehicle do not change.

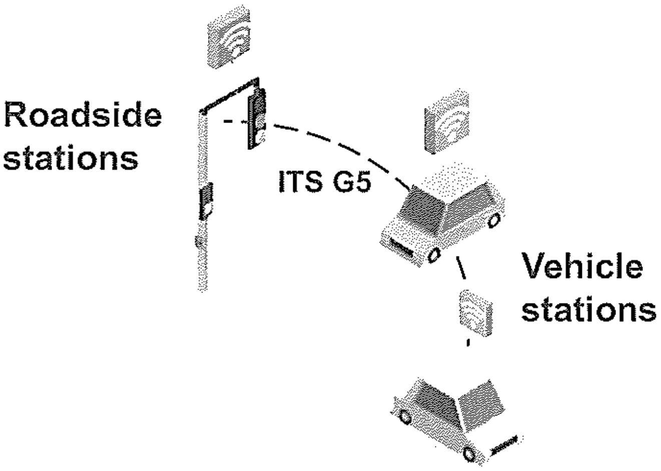


Figure 2: European C-ITS standards currently address short range communication

Day 1 C-ITS data collection

For Day 1 or near term C-ITS use cases, advice is provided to the driver through the following value chain:

- Observe the situation – C-ITS messages are generated and shared by the station. These stations' are located in vehicles or on the roadside.
- Assess the situation – the C-ITS messages are assessed by the vehicle stations.
- For vehicle to vehicle (V2V) use cases, the approaching cooperative vehicles use their own movement data and the downstream cooperative vehicle data to assess the hazard risk and, if relevant, will provide a warning to the driver.
- Vehicle to infrastructure (V2I) use data broadcast from roadside infrastructure. The cooperative vehicles use their own movement data to assess the hazard risk, and if relevant, will provide a warning to the driver.
- Deliver the advice – the vehicle has preconfigured advice based on the use case and condition. The advice is delivered to the driver via the human machine interface (HMI) as visual, audible, haptic and so on.
- Driver reads and reacts – the driver receives the advice and takes evasive or alternative action.

European standards currently define a number of C-ITS messages that ensure that the technology from different vendors speak the same language and hence can cooperate. The C-ITS messages include:

- **Continuous Awareness Message (CAM)** – generated by the vehicle indicating the vehicle's position, speed, etc. broadcast up to 10 times per second.
- **Decentralised Environmental Notification Message (DENM)** – generated from the vehicle or infrastructure to warn of a hazard such as hard-braking or roadworks.
- **Signal Request Message (SRM)** – generated by the vehicle to request a green light at a signalised intersection.
- **Signal Phase and Timing (SPaT)** – generated from the signalised intersection describing the intersections phase and timing information.
- **MAP** – a map shared from the signalised intersection describing the intersection geometry.
- **In Vehicle Information (IVI)** – regulatory information such as a posted speed sign.

The messages do not include personal information such as VIN, registration, name, phone number etc.

Vehicles need to be able to trust that the C-ITS messages that they receive are legitimate in order to make safety decisions. The vehicles need to be able to make this determination without ever having had contact with a vehicle before, and it needs to be done without identifying the other vehicle. The European standards require the implementation of a Cooperative Credential Management System (CCMS) to support trust and privacy, as follows:

- The CCMS acts as a trusted third party during V2V communications, a bit like the Justice of the Piece scheme.

- Each vehicle is handed out multiple random JP stamps (each with a different identity) to attest that they sent the message. They use this stamp on each communication that they send.
- The vehicles change the JP stamp that they use periodically.
- Vehicles that receive the stamped message can tell that whoever sent the message is part of the JP scheme (that the stamp was given to them by the CCMS), but they can't tell who sent it because they don't know which JP stamps were given out to whom.
- The CCMS knows who it has given stamps out to, that's obviously a privacy problem, so they split the CCMS up into 2 parts. One part hands out an authorisation to ask for JP stamps. The other part hands out the JP stamps. And the two must never share identifying information.

Day 1 vehicle data collection by transport agencies is summarised below:

Message	Collection	Privacy issue
Vehicle CAM	Collected at limited points that have a C-ITS roadside station such as signalised intersection and managed motorways	Issue - when the vehicle's origin and destination (O-D) can be inferred from CAM - e.g. a person's home and work location. CAM can be further linked to a person's identity. Management - As data is collected at a limited points and changes CCMS "stamps" frequently, the risk of implying an O-D would be low. Furthermore, increasing the density of roadside station to increase the likelihood of tracking O-D would be cost prohibitive. Given the two-part construct of the CCMS, the risk of linking CAM with personal information would be rare. The randomness of the "stamps", turning off transmission for small periods of time, using a "stamp" once, and the timings and periods that each "stamp" will be used is currently under decision by C-ITS standard committee's to further support the obfuscation of a vehicle's presence.
Vehicle SRM	Collected at signalised intersection	As above
Vehicle DENM	Collected at limited points that have a C-ITS roadside station such as signalised intersection and managed motorways	Issue – Europe has identified a privacy issue when the vehicle "self-incriminates" – in particular the use-case where the vehicle tells other vehicles it is running a red light. Management - As most Australian vehicles are built in Europe, which are subject to GDPR privacy requirements, use-cases that generate DENM that can "self-incriminate" are unlikely to be available in Australian vehicles.

Emerging Day 1 C-ITS data collection

In Europe, a hybrid C-ITS communications model is emerging that includes long range communications (3G/4G) and allows a central station to share C-ITS messages with other cooperative users. The central station can be owned/operated by any entity - government, industry, or both. European standards for a hybrid model and the scope of the central station will not be available until 2019.

As illustrated in Figure 3, a common central station model that is being explored through pilots, including Queensland, is one where the vehicle can register with a broker to access government C-ITS data. The broker is typically a third party or Telco. In this model, government has no transparency of the vehicle's information – IP address, station ID, or CAM.

Ideally, a vehicle should provide the government broker with their vehicle generated DENM. This information would assist traffic management centres to - locate the hazard, determine the need for emergency services, and inform upstream vehicles (beyond the range of vehicle-to-vehicle communication) of the hazard. This is similar to "e-call" that has been mandated in Europe.

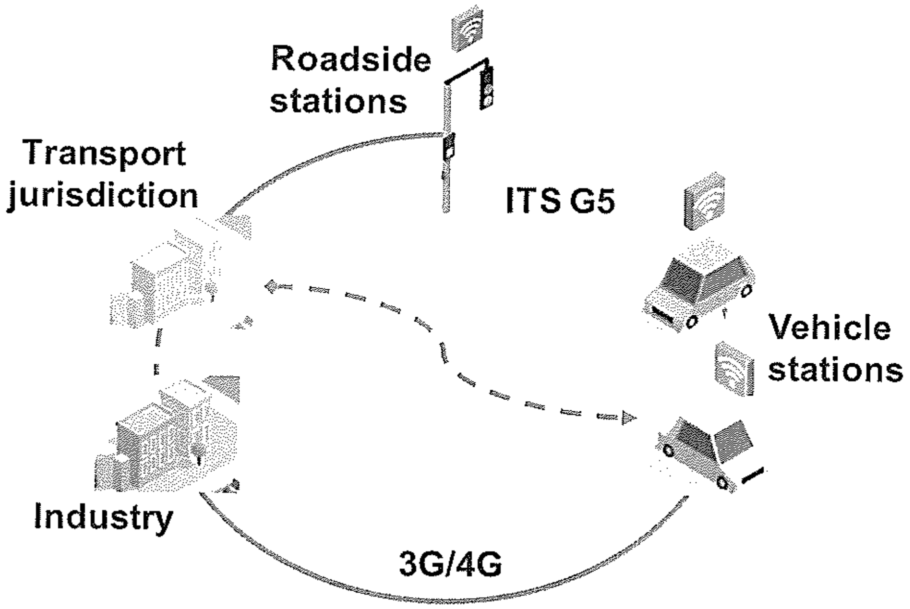


Figure 3: European C-ITS hybrid model includes short and long-range communications

Day 2 CAV data collection

There is an emerging consensus that a fully automated vehicle is not possible unless it is connected with other users and infrastructure. If connected data sharing is restricted, then a fully automated vehicle is unlikely to be realised beyond limited use cases or applications.

A number documents, such as SAE J3131, define an automated driving reference architecture for level 3 to level 5 automation (J3016), which include C-ITS (or Car 2X as illustrated in figure 4). The C-ITS applications' use automated vehicle's sensor data to share with other vehicles' and users. Similarly, other users shared their C-ITS data with the automated vehicle.

The GDPR working group note "It is likely, given the projected prevalence of (semi-) autonomous cars that the inclusion of this technology in vehicles will become mandatory at some point in time, comparable to the legal obligation on car manufacturers to include e-call functionality in all new vehicles."

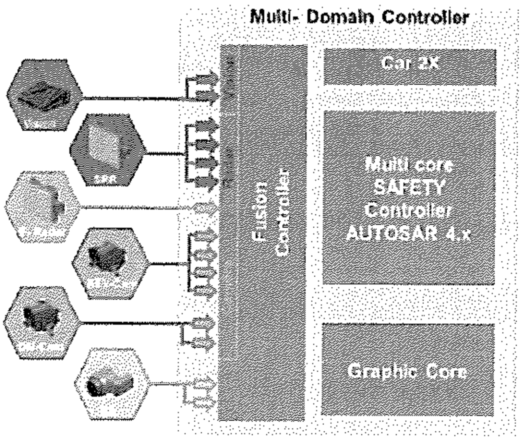
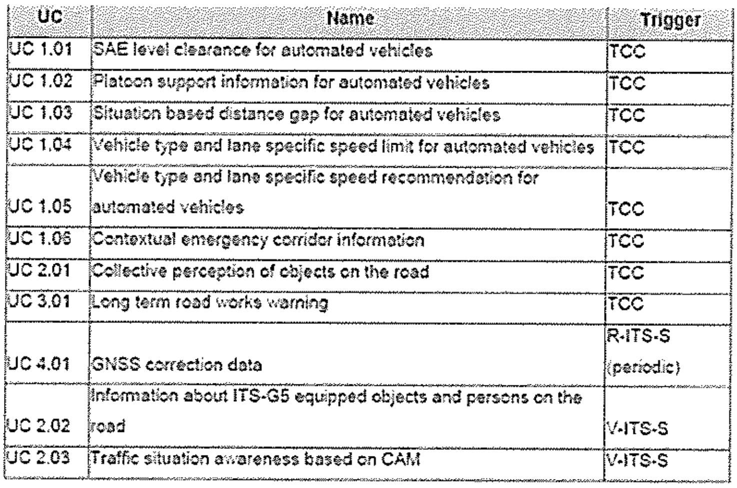


Figure 4: Adven view of the automated vehicle architecture

Emerging Day 2 use-cases that capture automated vehicles are currently under development and include, but are not limited to, the following:



UC	Name	Trigger
UC 1.01	SAE level clearance for automated vehicles	TCC
UC 1.02	Platoon support information for automated vehicles	TCC
UC 1.03	Situation based distance gap for automated vehicles	TCC
UC 1.04	Vehicle type and lane specific speed limit for automated vehicles	TCC
UC 1.05	Vehicle type and lane specific speed recommendation for automated vehicles	TCC
UC 1.06	Contextual emergency corridor information	TCC
UC 2.01	Collective perception of objects on the road	TCC
UC 3.01	Long term road works warning	TCC
UC 4.01	GNSS correction data	R-ITS-S (periodic)
UC 2.02	Information about ITS-G5 equipped objects and persons on the road	V-ITS-S
UC 2.03	Traffic situation awareness based on CAM	V-ITS-S

These new use-cases do not impact the communications model illustrated in figure 3.

Day 3+ data collection

Day 3+ use-cases are unknown and - while they may impact the privacy assumptions captured in this paper – are too early to consider.