Department of Transport and Main Roads

Ipswich Connected Vehicle Pilot

RSD9 Roadside Station Deployment Design

July 2022

Queensland Government

Copyright

Licence

CC BY licence summary statement

Translating and interpreting assistance

The Queensland Government is committed to providing accessible services to Queenslanders from all cultural and linguistic backgrounds. If you have difficulty understanding this publication and need a translator, please call the Translating and Interpreting Service (TIS National) on 13 14 50 and ask them to telephone the Queensland Department of Transport and Main Roads on 13 74 68.

Disclaimer

While every care has been taken in preparing this publication, the State of Queensland accepts no responsibility for decisions or actions taken as a result of any data, information, statement or advice, expressed or implied, contained within. To the best of our knowledge, the content was correct at the time of publishing.

Feedback

Please send your feedback regarding this document to: tmr.techdocs@tmr.qld.gov.au

Ipswich Connected Vehicle Pilot: Roadside Station Deployment Design

To ready government, industry, and road users, the Queensland Department of Transport and Main Roads deployed a - cooperative intelligent transport system (C-ITS) pilot in the City of Ipswich – referred to as the Ipswich Connected Vehicle Pilot (ICVP). The pilot was deployed for 12 months, aligned to the European C-ITS model, and comprised of 355 cooperative vehicles, 29 roadside stations and a central facility/station.

Roadside stations have an essential role in C-ITS in that they create a local interface for road operators to share information in real-time with passing vehicles. In the pilot, roadside stations were located at traffic lights, broadcasting signal status and timing and the intersection layout using ITS-G5 (5.9GHz). This information was used by passing participants' connected vehicles to generate red light and pedestrian crossing warnings.

The ability to deliver standards-based roadside station operation and to remotely maintain the roadside stations are key challenges for ongoing deployment of C-ITS technology. This paper examines the enhanced roadside station functionality delivered in the pilot, including the (Message Queue Telemetry Transport (MQTT) interface to the central facility, message handling (including security) and monitoring and maintenance.

The pilot implementation creates a blueprint for C-ITS deployment of roadside stations here in Australia and globally. The lessons learnt in developing and maintaining deployed roadside stations can provide consistency and efficiency for other C-ITS suppliers and operators.

Keywords:

Connected Vehicles (CV), Cooperative Intelligent Transport Systems (C-ITS), Roadside ITS Station (R-ITS-S), Central ITS Station (C-ITS-S), Vehicle ITS Station (V-ITS-S)

Contents

1 Introduction

In Australia, the Austroads' Future Vehicles 2031[1] report has predicted the future penetration of cooperative intelligent transport system (C-ITS) in new vehicles, which is estimated between 2% (slow penetration) and 50% (rapid penetration) by 2031. Further to this, the Australasian New Car Assessment Program recently aligned with Europe to include C-ITS in its 2025 five-star vehicle safety rating framework[2]. C-ITS technologies have a reliance on and interaction with infrastructure and assets owned and operated by road authorities. Whilst many of the developments are occurring globally, there is a need for Australian jurisdictions to integrate C-ITS with existing ITS applications. Australia has informally agreed to align with European C-ITS standards[3]. In Queensland, this will be achieved by modernising the Department of Transport and Main Roads' (the department's) systems, processes, and data to provide C-ITS compliant services.

From 2021 to 2022, the department conducted a C-ITS pilot to understand the deployment needs for C-ITS. In the pilot, Kapsch's roadside station product was installed at traffic lights, broadcasting signal status and timing and the intersection layout. This information was used by participant vehicles to generate advanced red light and pedestrian crossing warnings if a safety risk was identified.

This paper discusses the technical delivery of roadside stations to promote the Ipswich Connected Vehicle Pilot (ICVP) objective to encourage partnerships and build capability in private and public sectors. It is intended to promote consistency between government agencies considering the deployment of roadside stations and suppliers developing solutions by sharing learnings on functionality needed for a robust deployment. Specifically, the paper focuses on:

- How roadside stations can interact with a central ITS facility/station to meet the needs of an operational system using a combination of C-ITS standards and IoT standards (MQTT)[4].
- How the roadside station managed and assured high-quality operational performance to broadcast and receipt of C-ITS messages with compliance to standards and the departments' specifications.
- How the roadside stations were monitored and maintained in the pilot to ensure continued accurate reliable operation over time.

[1] Austroads Future Vehicles 2031 report (AP-R623-20)

[2] ANCAP (2021) Submission to Joint Select Committee on Road Safety 2021. Retrieved from: https://www.ancap.com.au/publications/ancap-submission-joint-select-committee-on-road-safety-2021.pdf

[3] Federal Chamber of Automotive Industries (2016) FCAI Submission to the Acma Consultation on C-Its. Retrieved from: https://www.fcai.com.au/news/publication/view/publication/83

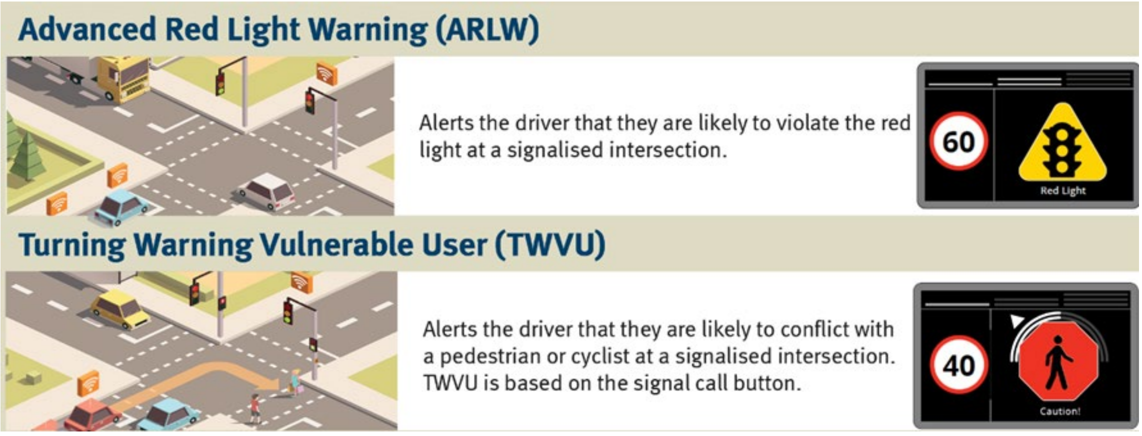
[4] ISO. (2016). Information technology – Message Queuing Telemetry Transport (MQTT) v3.1.1. ISO/IEC 20922:2016

1.1 *Pilot Background*

In response to the emerging C-ITS deployments around the world the department conducted an on-road Field Operational Test (FOT) in the City of Ipswich, Queensland using 355 vehicles, 29 signalised intersections and a central facility to test six “day-one” safety use cases. Day-one use cases are those defined by the C-ITS Platform[5] which are expected to be available near-term because of their societal benefits and maturity of technology.

In the pilot, 29 roadside stations were installed at 29 intersections for a 12 month duration. The roadside stations continuously broadcast signal state information called Signal Phasing and Timing Extended Message (SPATEM)[6] and intersection layout information called Map Extended Message (MAPEM)[7]. Vehicle stations compare the vehicle movement data to the received messages to assess the hazard risk, and if relevant, provides a warning to the driver. The SPATEM and MAPEM provided through the roadside stations enables the Advance Red Light Warning (ARLW) and Turning Warning Vulnerable Road User (TWVU) use cases illustrated in Figure 2.1(a).

Figure 2.1(a) – Ipswich connected vehicle pilot safety use cases that use roadside station data



Advanced Red Light Warning (ARLW)

Alerts the driver that they are likely to violate the red light at a signalised intersection.

Turning Warning Vulnerable User (TWVU)

Alerts the driver that they are likely to conflict with a pedestrian or cyclist at a signalised intersection. TWVU is based on the signal call button.

The architecture used to operate the intersection use cases is shown in Figure 2.1(b), where the left side illustrates the existing system, and the right side (dashed boxes) illustrates the pilot system. Both systems share the field processor (FP, which is running STREAMS® Connect software) – which includes new software and a firewall to separate the systems. Roadside and vehicle stations interact via ITS-G5 (DSRC) using IEEE 802.11p within the 5.9 GHz spectrum.

[5] European Commission (2017), C-ITS Platform Final Report Phase II. September 2017. Retrieved from https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf

[6] European Telecommunications Standards Institute. (2016). Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services. ETSI TS 103 301 V1.1.1

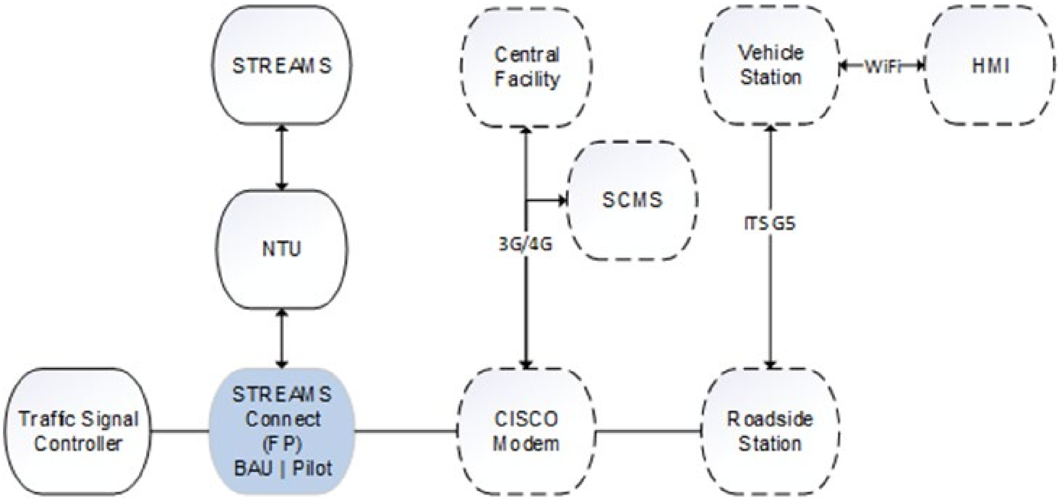
[7] European Telecommunications Standards Institute. (2014). Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. ETSI EN 302 637-2 V1.3.2

Short-range communication latency characteristics enable reliable fast changing, safety-critical messages for the ARLW, and TWVU use cases. Long range communication (3G/4G), support centralised services including the security credential management system (SCMS in C-ITS Public Key Infrastructure (PKI)) and the central facility (which includes the central station). Functionality was proven between the roadside station, central station, vehicle station and SCMS through collaborative development and testing.

In summary, the roadside station (R-ITS-S) connects to the following:

- Central Facility (C-ITS-F) via 3G/4G CISCO modem, over the pilot network – the central facility supports remote monitoring and maintenance of the roadside station, as well as the provision of MAPEM.
- Security Credential Management System (SCMS) via 3G/4G CISCO modem, over the pilot network - the roadside station requests certificates from the SCMS for signing SPATEM and MAPEM.
- Field Processor (FP) via Ethernet – the FP provides unsigned SPATEM to the roadside station from the traffic signal controller. This connection is firewalled to ensure controlled separation from the existing system.
- Vehicle station (V-ITS-S) via the ITS G5 – the roadside station sends signed SPATEM and MAPEM and receives signed Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM) from passing vehicle stations.

Figure 2.1(b) – Intersection Use Case Architecture



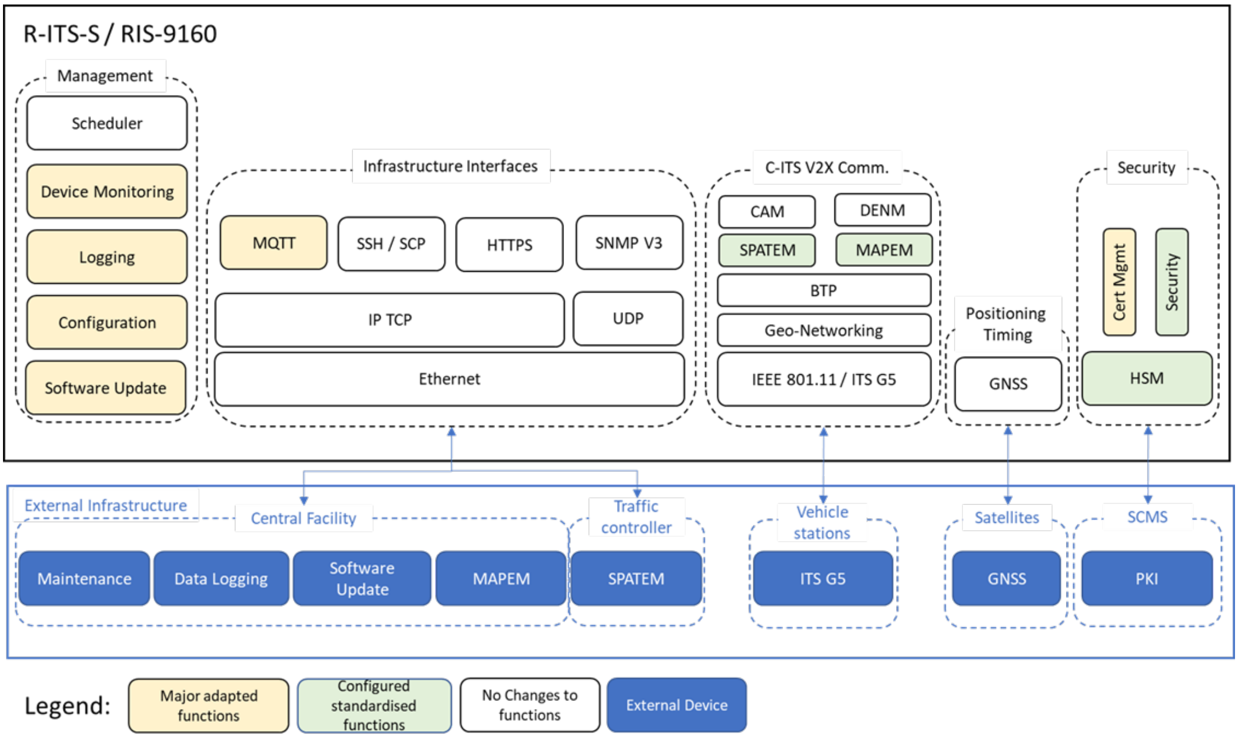
1.2 Roadside Station Design

The Kapsch roadside station (Model: RIS-9160) delivered for the pilot had extended functionality from the base product to meet the project requirements. The overview of the roadside station is shown in Figure 2.2. The major functional changes were MQTT, certificate management, station monitoring, logging, configuration, and software updates. Improvements to operational functionality were made to SPATEM processes, MAPEM processes and security. The roadside station architecture has the following major components:

- **Infrastructure Interfaces** handling the interaction with central facility, traffic controller via the field processor and common communication protocols. The roadside station connects to the central facility utilizing MQTT service via TCP/IP for C-ITS messages, logging, and configuration. Internet Protocol/User Datagram Protocol (IP/UDP) is used for SPATEM messages provided to roadside station by the FP connected to the Traffic Light Controller (TLC). Communication to the PKI / SCMS is via HTTPS.
- **C-ITS V2X Communication** handles the ETSI compliant layers which processes messages through the access layer ITS-G5 (IEEE 802.11p), transport layer Geo-Networking (GN) and Basic Transport Protocol (BTP) and facilities layer CAM7, DENM[8], SPATEM and MAPEM.
- **Security Services** provide the features for certificate management and signing/validation of ETSI compliant messages utilizing the internal Hardware Security Module where certificates are stored. Security services are also responsible for the management of device enrolment i.e. registration of the roadside station at the PKI and management of certificates including valid certificate availability and update of those in the timely manner. HTTPS is mostly used for the security services to interact with the PKI.
- **Positioning and timing** provide the location and time for the roadside station from GNSS satellites or manual configuration override. The roadside location may be configured by manual static parameter setting or derived on the dynamic geo-location calculation results of the GNSS receiver and its firmware. Time synchronization is a crucial function needed for ITS-G5 communication on radio and message exchange. In order to minimize any security threats, it is essential that messages include the most accurate time stamp when they are transmitted and the time will be validated by the receiver to avoid any man-in-the-middle type fraud attacks. In the pilot, there were instances where interference with LTE towers caused GNSS failure (and therefore roadside station failure). This was resolved by using a GNSS antenna with better off-band signal attenuation/suppression at all problem sites and future sites.
- **Management services** handles configuration of different device and utility parameters, device monitoring and supervision, automated software and firmware updates, logging functionality and provision of log data to central facility.

[8] European Telecommunications Standards Institute. (2014). Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3 Specifications of a Decentralized Environmental Notification Basic Service. ETSI EN 302 637-3 V1.2.2

Figure 2.2 – Roadside station system overview



2 MQTT Client

The roadside station required an MQTT client to establish a connection to the C-ITS-F broker for the receipt of MAPEM, configuration and upload of logs. The roadside station used the Amazon Web Services (AWS) Internet of Things (IoT) Software Development Kit (SDK)[9] to integrate with the C-ITS-F as it enabled the quickest access to the AWS MQTT broker. Compared to traditional TCP or TLS connection handling, MQTT (or any other publish-subscribe system) handles all the following natively which is highly beneficial to the pilot and C-ITS needs:

- Topic-based device addressing.
- TLS security.
- Authentication.
- Connection heartbeats.
- Quality of Service delivery guarantees.

[9] AWS IOT Device SDK Embedded C https://github.com/aws/aws-iot-device-sdk-embedded-C

2.1 Message Definition

For best message efficiency (and reusing the existing ASN.1 capabilities of C-ITS stations) all messages have been defined in ASN.1[10] with UPER message encoding. Several iterations were performed to optimize the definition and structure of data elements. Using ASN.1 has the additional advantage of being able to automatically create data structures and accessor methods for all involved programming languages to speed up the development process.

2.2 MQTT Connection Handling

For the client connection to work reliably within the roadside station and meet the requirements of the pilot, several modifications were made to the SDK:

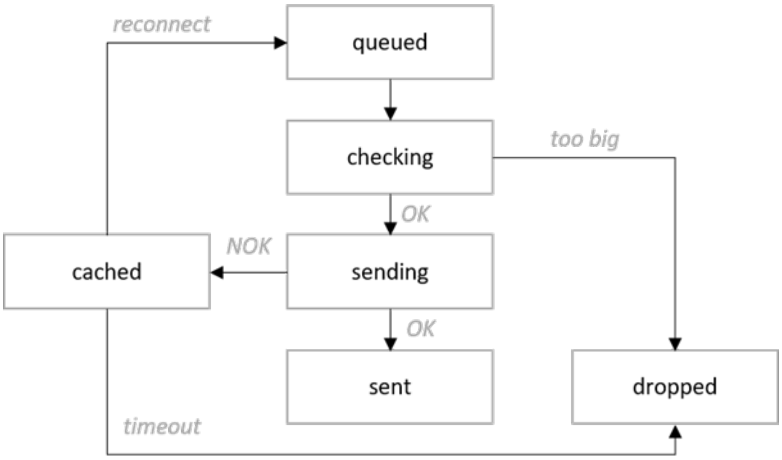
- The Kapsch base system build was updated to compile for the pilot with MQTT. Cross-compiling the roadside station firmware was not possible due to several problems with libraries being loaded from mismatched paths. This was resolved during the build process.
- The AWS IOT SDK does not allocate memory dynamically and uses fixed buffer sizes, Kapsch increased the receive and transmit buffer sizes from 4kBytes to 128kBytes and the number of concurrent topics from 5 to 50. This was needed to transfer the logging data with the Station Platform Message (SPM) and C-ITS Safety Evaluation Message (CSEM) format because messages transmitted to C-ITS-F were bigger than the default message size.
- Log to file instead of to STDOUT and provide logging strings for MQTT error codes. The AWS IOT SDK was logging to the console per default which is not helpful for troubleshooting in an operational environment. As such, the library was modified to log to a file which is helpful for post event analysis.
- Properly handle the *Session Present Flag* to maintain the MQTT connection. The AWS IOT SDK does not provide any advanced connection handling, so the SDKs API had to be wrapped in connection handling infrastructure. This ensures that the connection is handled gracefully and to re-establish connections and republish unacknowledged messages. The connection handler includes:
  - Automatic disconnect/reconnect when a message can’t be published, or the API reports a connection loss.
  - Automatic subscribe/unsubscribe during connect/disconnect.
  - Caching of messages on non-volatile memory in case the station is disconnected.
  - Cached messages are removed from the cache after a configurable timeout when the station is not connected.

[10] ASN.1 https://en.wikipedia.org/wiki/ASN.1

The automatic connection/disconnection is done in a thread that implements a state machine to properly handle the connection states (including subscribing/unsubscribing during connection changes). To decouple the thread, a message queue is used: messages are put into the queue from several parts of the system, the messages are then taken from the queue in the thread and either immediately sent via MQTT to the C-ITS-F when the connection is available or cached to non-volatile memory if unavailable (see Figure 3.2 - MQTT Message Caching). Cached messages are removed from the cache after a configurable timeout (default 4320 minutes: 3 days) when the station is not connected or reloaded into the queue when a message is successfully published on a new connection.

After deployment in the pilot, Kapsch has deployed other publish subscribe-based systems (with Protobuf[11] defined messages instead of ASN.1). This alternative approach works similarly as well.

Figure 3.2 – MQTT Message Caching



2.3 Topic Subscription

The publish-subscribe principle for the communication between field devices (roadside stations and vehicle stations) and the central facility makes subscription topics available to create proper addressing and grouping of messages and specific stations. Assuming a subscription topic is shared between several stations, all of them will receive the same information, or alternatively, all producers can publish to the same topic and the consumer can subscribe to a single topic without missing any information.

The following defined topics allowed communication between central facility and field devices to exchange relevant information:

- Published by roadside station subscribed by central facility:
  - Health and status information – SPM.
  - Collected messages (transmit/receive capture of ETSI messages from vehicles, central station, and the FP) – CSEM.

[11] Google Protocol Buffers https://developers.google.com/protocol-buffers

- Subscribed by roadside station published by central facility:
  - Station configuration message data – SCM.
  - MAPEM messages.

For field stations it is crucial to allow authenticity validation of received information through an IP based connection. To avoid relying on Transport Layer Security (TLS) only, a message signature system in the communication between central facility and roadside stations has been introduced. The existing ETSI signature concept including the use of PKI/SCMS certificates as applied for ITS-G5 messages has been reused. To make this work for long range communications, security was applied only on pure (facility) message content - omitting the geo-networking part. MAPEM content has been signed by the central station, allowing the roadside station to validate that the message hasn't been spoofed or altered. Only valid signed MAPEM messages are accepted into the facility layer service. Although the ETSI security definition provides everything needed to apply facility layer security, ICVP has been amongst the first pilots applying this variant of message security. From a roadside station supplier perspective, this approach is very effective as it supports re-use of functionality and providing end-to-end full chain of trust.

The performance of the MQTT connection and topic handling worked well for loading configuration and MAPEM whenever necessary i.e. on change only and for return of logged data by the roadside station. Roadside stations self-reported 46 instances of failure in validating MAPEM out of 10063 MAPEM received through the MQTT broker. While this did not impact operation since the MAPEM received rarely contained a change from the currently loaded MAPEM in ICVP, this may require further analysis of impact in future deployments. Across a year of roadside station reported data, there was 200 instances of MQTT outages on average per station. During these instances no log information was lost due to the 3 day caching timer being exceeded. Over the 12 month pilot period there were at least four instances where a roadside station had to be power cycled due to communication failures.

3 Message Management and Assurance

The primary role of the roadside station is to broadcast and receive C-ITS messages using ITS-G5. While this core functionality is well supported by ETSI standards, there were still requirements and operational decisions needed for the pilot to apply the standards. During the 12 months of the pilot, 99.94% of the expected SPATEM and MAPEM messages were sent from the 29 roadside stations. The times the C-ITS messages were not sent were due to:

- Message handling and checking when processing SPATEM, MAPEM and signing (as outlined in this section), or
- System/station hardware or software failures on the roadside station or associated equipment such as traffic signal controller, FP, router, etc. For example, the roadside station stopped sending messages seven times (three in pilot) in a 16 month period. The root cause was not identified, and Kapsch recommended the logging level to be raised across stations. The issue was cleared by resetting the affected stations.

The following sections describe the "by design" handling and quality assurance provided in the roadside station.

3.1 Process for SPATEM management

SPATEM are sent from the field processor (FP) via UDP, the message is validated using the steps listed in Table 1, if any of the steps fail the SPATEM is discarded.

Table 4.1 – SPATEM Handling

Process	Description
Station Status	Each station can be enabled or disabled from the C-ITS-F, i.e. when a station is disabled the sending of SPATEM is also disabled.
Message Integrity	The SPATEM is decoded from UPER. If the SPATEM ASN.1 schema decoding fails, then the SPATEM is discarded.
Message Error Handling	Discarded SPATEM events are logged in the monitoring system.
Signing	see section *Security Handling, Validation and Certificate Management*

3.2 Process for MAPEM management

MAPEM are published by the C-ITS-F to field station specific topics and then continuously broadcast by the roadside station on ITS-G5. Several mechanisms work in parallel to make sure that the correct MAPEM is sent out to the correct location: the steps in Table 4.2 are processed in order, if any step fails the MAPEM is discarded.

Table 4.2 – MAPEM Handling

Process	Description
Station Status	Each station can be enabled or disabled from the C-ITS-F, i.e. when a station is disabled the sending of MAPEMs is also disabled.
Message Integrity	The C-ITS-F signs the MAPEMs according to ETSI TS 103 097 V1.3.1,[12] with the distinction that the geo-networking payload is not signed but instead only the ITS message frame starting at the ItsPduHeader. Upon receipt at the station the signature is checked for relevance (has it been signed recently?), consistency (are the signature headers decodable and consistent?) and validity (is the signature valid and trusted?). If any of the criteria fails, the message is discarded. The MAPEM is then decoded from UPER, if the decoding fails the message is discarded as well.

[12] European Telecommunications Standards Institute. (2017). Intelligent Transport Systems (ITS); Security; Security header and certificate formats. ETSI TS 103 097 V1.3.1

Process	Description
Message Versioning	The configuration information sent by the C-ITS-F contains the current desired version of the MAPEM message to make sure that the station doesn't send outdated information. This configured version is compared against the msgIssueRevision in the MAPEM. Since the roadside station configuration and the MAPEM are not sent synchronously, a problem occurred where the station receives either the configuration with the new version first (and discards the currently used MAPEM) or first the MAPEM (which is discarded because it's not the desired version). To address this issue, MAPEMs with equal or greater versions are accepted. During an update of the version, *first* the MAPEM must be changed (and is still accepted because the version is now higher than the configured one) and *only then* the configuration is updated.
Message Error Handling	When an invalid MAPEM is received, the station is in an inconsistent state where it cannot send out the new MAPEM (because it is invalid) at the same time the old MAPEM is outdated. To prevent wrong MAPEM information from being sent out, the current scheduled MAPEM is also cancelled when an invalid MAPEM is received. This causes the station (and therefore intersection) to be in a failed operation state until a correct MAPEM is sent.
Message Location	To prevent misconfiguration, the station checks each received MAPEM against the current location. If the refPoint of the first intersection in the MAPEM is too far from the station's current location the MAPEM is discarded. The distance is configurable in the firmware and set during first startup to the default of 20,000 metres. This also prevents stations that have been transferred to a different location from sending out the MAPEM of the previous location.
Signing	see section Security Handling, Validation and Certificate Management.

3.3 Security Handling, Validation and Certificate Management

ICVP was the first pilot where Kapsch implemented the new ETSI Security standards according to ETSI TS 103 097 version 1.3.112 and TS 102 941 v1.3.1[13] (beside ETSI plug-tests used for interoperability and standard compliance checks). In C-ITS, two equally important aspects for security need to be considered:

1. The correct implementation of frame format including cryptographically relevant information like signer certificate, signature.
2. The interaction with the SCMS provider for retrieving certificate updates during a period of continuous operation.

[13] ETSI TS 102 941 https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/

Since security implementation requires a deep knowledge of applied protocols, cryptographic operations correct handling of signatures, many companies rely on 3rd party software for all cryptographic services needed for the correct handling of such frames, signatures and certificates. Both roadside station and vehicle station used the same provider for the cryptographic library in their stack implementation; due to non-existing online SCMS connectivity according to the latest ETSI standard the pilot started with certificate bundles from the SCMS provider manually installed on the stations. When the software-based PKI connection became available it allowed automated certificate retrieval and the certificate bundles got replaced with online SCMS operation with stations enrolled to the SCMS provider. The development process took longer than anticipated to achieve a stable operation, however once in place within each station (roadside, vehicle and central), the system integration was relatively seamless.

The following processes were implemented for security certificate enrolment and operation:

- Certificate validity period and permissions granted for particular device types have been agreed upon between the department and the PKI provider at the beginning of the project, e.g. roadside stations are only allowed to sign SPATEM, MAPEM, DENM and CAM with their certificates, this is reflected in the Specific Security Permissions (SSPs) of the Authorisation Tickets (ATs) used for signing outgoing messages.
- The device ID always needs to be unique, a device registered with the SCMS provider can only be registered with the same canonical name again when the old registration is deleted in advance.
- The security subsystem in the roadside station checks the server it is connecting to, by verifying that the server identity is known and valid.

The geo-networking version was updated to allow usage of the new C-ITS security standards. The C-ITS communication stack is responsible for handling the security for ITS-G5 messages including adding signatures to sent messages during creation of the geo-networking headers and verifying the received messages signature. The C-ITS communication stack usually only provides the stripped BTP payload to the upper layers. To log the raw message bytes (including the signature and geo-networking header) a special logging facility was added. The signing of messages sent and validation of incoming messages were monitored and logged when an error occurred.

The following security issues occurred during the pilot causing outages:

- Two stations had 2 3 day outages because of certificate signing errors.
- The validity of the Certificate Revocation List/ Certificate Trust List (CRL/CTL) provided by the SCMS expired on 9th September 2021. The expected behaviour of the stations was to reach out to the SCMS distribution point and retrieve a newly signed CRL/CTL. However, there was a delay in signing the CRL/CTL by the SCMS provider, which in combination with the roadside station's startup requiring a valid local version of these before checking if a new version is available meant that any roadside stations that were restarted during this time would fail to start. After re-issuing the CTL/CRL on 21st September 2021 from the SCMS, the devices had to be updated manually with a Kapsch provided script that downloads the new CTL/CRL before restarting the system. Devices that were not restarted did not require this manual intervention.
- The certificate signing failed on one station for approximately one week.

Generally, validation errors on CAMs received did not appear to be an indicator of system failure but rather a 'by design' limitation of the system such as messages received on the edge of the communications range. Stations outside of the system were rejected (this was verified with test vehicles on a different SCMS list).

4 Roadside Station Monitoring and Maintenance

Many pilots have focused on testing the core function of C-ITS, which from a roadside station perspective is to collect and share data with vehicles and central facilities. ICVP extended this to look at how roadside station operators (typically government) can monitor and maintain these devices over the life of the asset. For operation of intelligent transport systems, the operation and maintenance portion of a product or system creates some of the largest challenges. Solutions deployed at different times must be low maintenance and efficient to update or repair to achieve the operational life of the asset/system. For C-ITS roadside stations this is particularly true for two reasons:

- Roadside stations provide data that is used in safety systems within the vehicle, and
- Consistency and currency is required across all roadside stations regardless of installation date such that any vehicle station can receive the same data format with the same rules applied.

4.1 Device Monitoring and Logging

For a pilot project and the future operational deployment of roadside stations it is crucial to gather informative data to allow extensive data analysis even after the pilot. The implemented monitoring approach allows not only the gathering of relevant log information on field devices (both vehicle and roadside stations) but also processes for transferring the logged information to C-ITS-F for efficient monitoring of system performance and for long-term storage for historical data analysis.

To log the raw message bytes (including the signature and geo-networking header) a special logging facility was added. MAPEM were logged when received from the C-ITS-F and when sent in the C-ITS message stack (see Process for MAPEM management), SPATEM were logged when received via User Datagram Protocol (UDP) from the field processor and when sent in the C-ITS messages stack (see Process for SPATEM management), and CAM/DENM are logged when they are received via the C-ITS communication stack.

Allowing continuous 24/7 operation of Linux based devices requires a consideration of storage capacity usage. A device with 100% storage utilization might fail in operation or maintenance and could become inaccessible – so a clear target was to have continuous monitoring of storage utilization and taking appropriate countermeasures to prevent any file system from reaching full capacity.

The roadside station uses both a persistent file system for application, configuration and important log information (required to be persisted) and a temporary file system (tmpfs) to avoid heavy memory waring due to continuous write access.

In parallel, a separate process has been established to monitor file system utilization; when a certain threshold has been reached (e.g. 90%) the process starts to delete persisted log information starting from the oldest. The maintenance process is responsible for both the persistent and volatile file system preventing them reaching full capacity.

Using a month of roadside station reported data (March 2021), no processing limits, memory limits, storage capacity or high temperatures were observed.

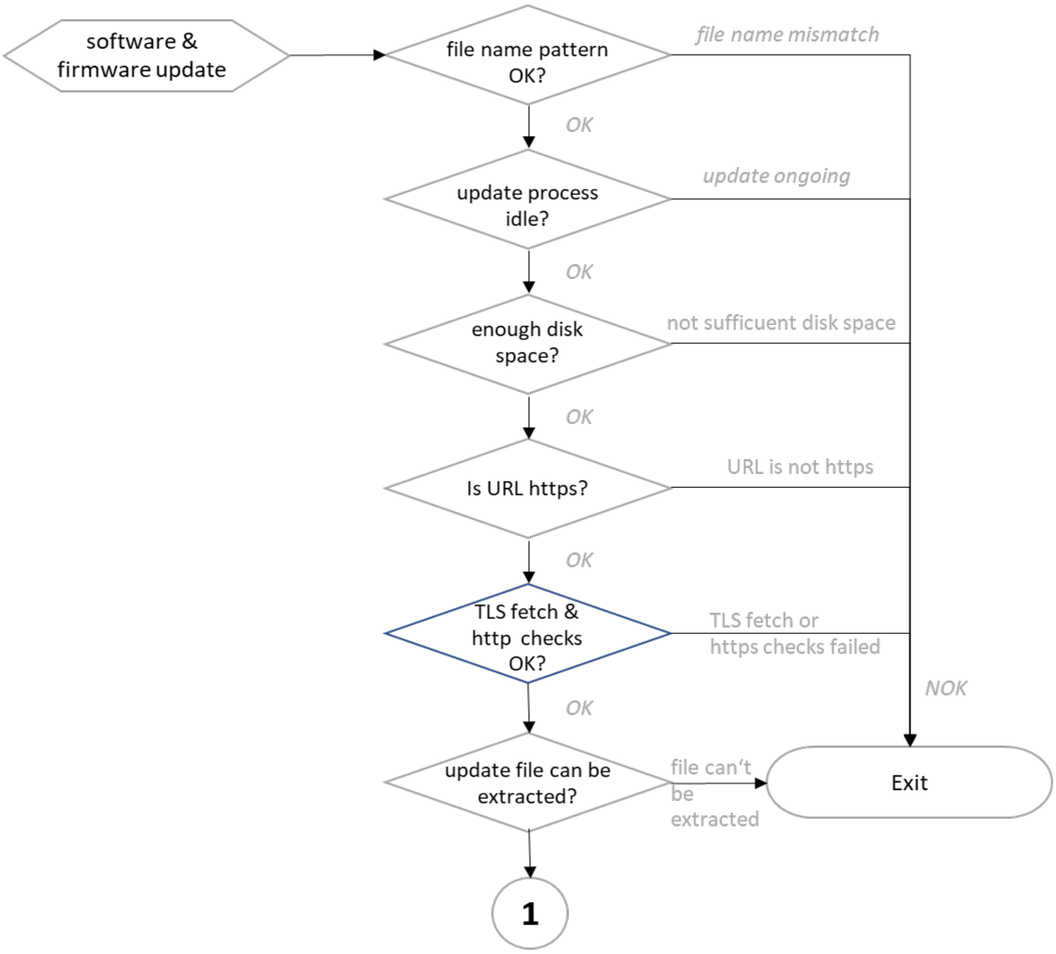
4.2 Maintenance (Software Updates and Configuration)

To maintain roadside compatibility to Standards, a software updates mechanism was essential. The central facility interface includes the ability to update the roadside station firmware remotely. Having a robust update mechanism that can be triggered remotely from the C-ITS-F is important in designing and implementing a maintainable system. Being able to test the update on one or more roadside stations and then roll out the update to more stations was found to be good practice in ensuring the stability of the overall system. To keep the system simple and efficient the following approach was developed:

- Each station has a persistent storage which contains a version string describing the currently installed software. The format of the version string is not further defined, it can be an arbitrary string.
- The C-ITS-F sends a configuration to the roadside station which contains:
  - The desired firmware version.
  - An URL to download this version.
- When the station detects a mismatch between its stored version information and the version information it downloads the new software from the URL and updates itself. As the last step after the update the new version information is written to persistent storage.

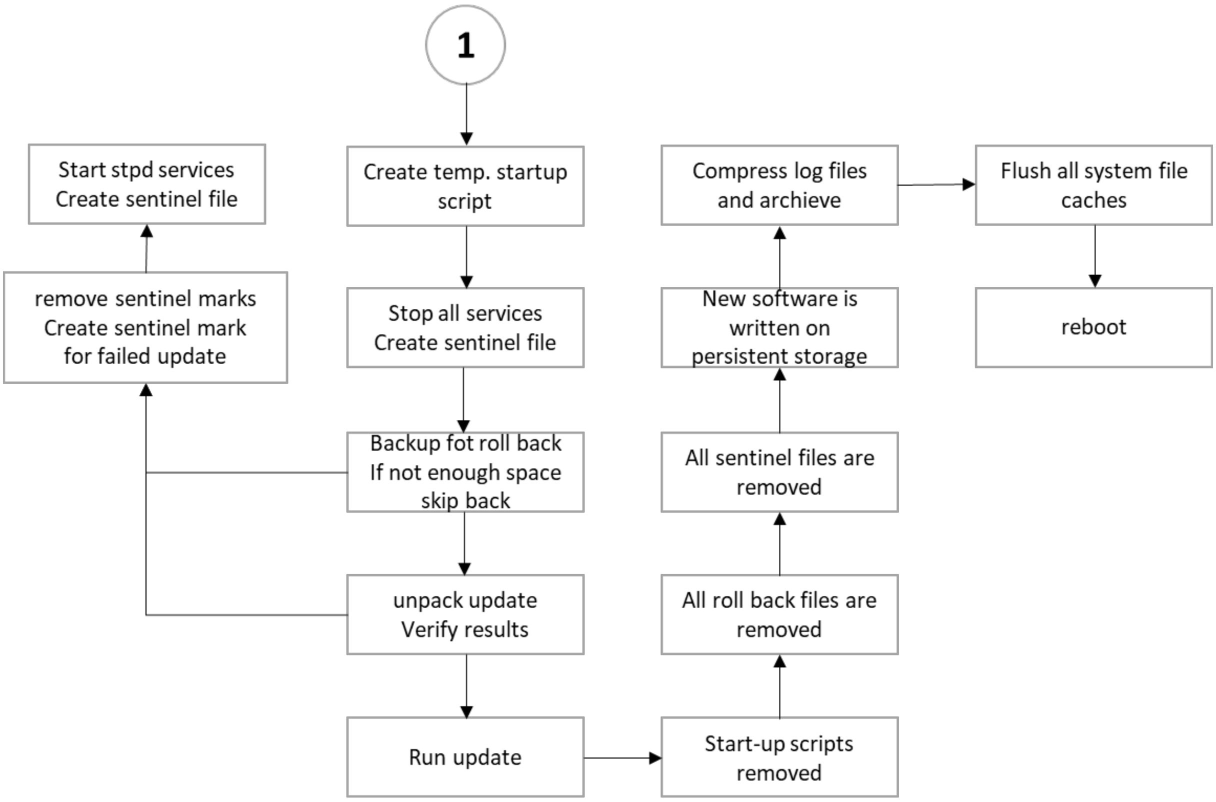
To ensure the stations operation the following checks are done before the installation of the update:

Figure 5.2(a) – Software or firmware update preparation and checks



On successful download of the software package, procedures for the software update are performed. If the software update is executed (Figure 5.2(b)) without errors, the processes to clean up the system are run to return to normal operation. In case any steps fail during update skip back and restore processes are executed. The error is communicated back to the software stack and reported to the C-ITS-F through monitoring logs.

Figure 5.2(b) – Software update execution and restart.


1
Create temp. startup script
Stop all services Create sentinel file
Backup fot roll back If not enough space skip back
unpack update Verify results
Run update
Start-up scripts removed
All roll back files are removed
All sentinel files are removed
New software is written on persistent storage
Compress log files and archieve
Flush all system file caches
reboot
remove sentinel marks Create sentinel mark for failed update
Start stpd services Create sentinel file

For OS updates the process is similar with the following notable differences:

- No backup is performed (with minimal interruption to operational behaviour of broadcasting SPATEM and MAPEM).
- The system reboots during the update, the start-up script then does the clean-up and removes itself.
- If a failed update is detected during the start-up, the update is started once more. If the start-up is from the second update already mark the update as finally failed.

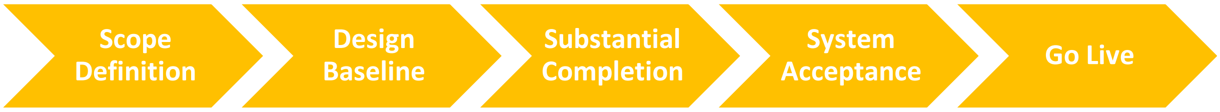
Since the update is running un-supervised on the roadside station making sure that all eventualities are covered was especially challenging. Also keeping the roadside station in a coherent state even when doing a manual intervention via the remote SSH interface was important to keep problems during updates to a minimum.

During the pilot, six separate software updates were performed across all 29 roadside stations resulting in 174 successful updates (no failures).

5 Roadside Station Development Process

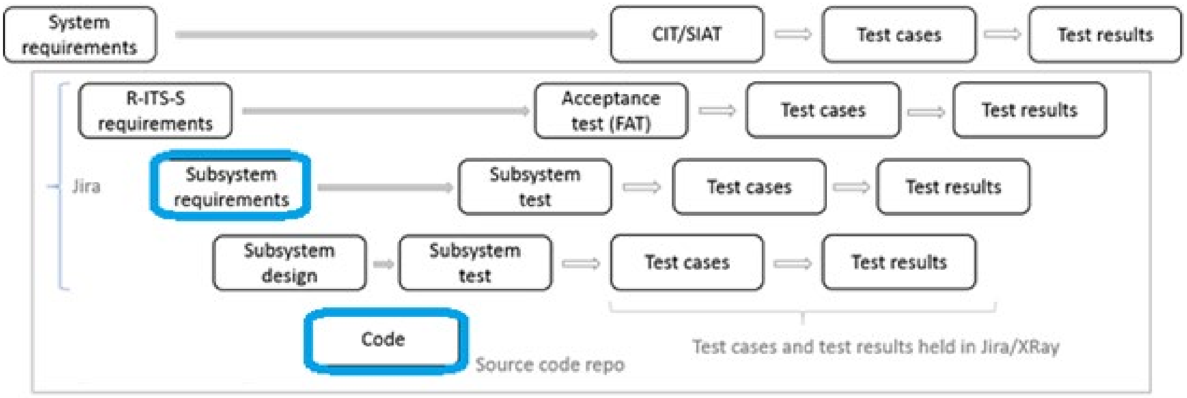
Due to the objectives of the pilot and the complexity of implementing new cooperative systems discussed earlier in this paper, the department engaged the roadside vendor, Kapsch TrafficCom, early in the process. The final requirements for the project were agreed upon through an iterative and pragmatic approach. This was a collaborative approach with other vendors such as Transmax, Cohda Wireless and the Queensland University of Technology (QUT) which led to a fully agreed requirements specification release. The collaborative approach was continued through all stages of the project (outlined in Figure 6) by embedding a Kapsch specialist engineer into the project, who had been trained with the product development team (in Vienna, Austria). The engineer was collocated with the Queensland project team and worked in close collaboration with the department. In case of anomalies or questions such as those outlined in this paper, the engineer served as a rapid and valuable connection from on-site to the product development specialists. It also meant the product development team in Vienna received pre-digested detailed information and first analysis results. While this was vital for a successful pilot where many parts of the system were new, it should not be required for an established ecosystem which requires efficient development, testing and deployment of new functions and devices.

Figure 6(a) – High level project process



All functionality and designs of the roadside station were developed and tested systematically as shown in Figure 6(b). The new implementation of the roadside station MQTT and maintenance interface with the central facility represented the most significant new functionality. The specification and design for the roadside station to central facility interface and schema was refined and improved. Kapsch implemented the interface on the roadside station to match the central facility implementation. The project partners integrated, tested and verified the common solution through a test plan which incrementally verified functionality from subsystem level to device level (FAT) to interface level (CIT) to end-to-end system level (SIAT).

Figure 6(b) – Requirement's traceability through integration, test, verification and acceptance



6 Conclusion

The Queensland Department of Transport and Main Roads successfully deployed a large-scale C-ITS pilot in the City of Ipswich. The system comprised of cooperative vehicles, roadside stations, a central facility and SCMS that comply with the European C-ITS standards. Kapsch delivered the roadside stations and integrated into the pilot’s C-ITS. The collaborative approach between suppliers' experts was viewed as beneficial to delivering a quality roadside station solution.

The use of the standards-based MQTT approach was a positive technical decision and one that aligns well with roadside station to central facility communication needs. The use of topics, ASN.1 schemas and C-ITS security, allowed for efficient functional delivery of C-ITS messages and has the potential for future use. While occasional disconnections occurred, the MQTT connection and topic functionality worked well, as needed for the pilot operation.

In order to reliably send and monitor the operation of the system, additional handling is required that is not detailed in the C-ITS standards. The implementation of the recently released security standards for the PKI interface and certificate management took longer than anticipated to achieve a stable roadside station operation. While the security implementation worked well, issues of multiple station failure occurred when there were issues with the interaction to the SCMS itself (e.g. receiving new certificates/ trust lists). There were many processes checked through the SPATEM, MAPEM and security handling, and while these created operational issues, the availability of SPATEM and MAPEM through the pilot was estimated at 99.94% of the expected messages.

Many pilots have focused on trialling the core functions of C-ITS, which from a roadside station perspective is to collect and share data with vehicles and central facilities. ICVP extended this to look at how roadside station operators (typically government) can monitor and maintain these devices over the life of the asset. Kapsch delivered a robust configuration and software update process which could be implemented by other jurisdictions. This provided capability to ensure all roadside stations were up to date and consistent with the latest optimisations and fixes. During the pilot, six updates across the 29 roadside stations were performed successfully.

Project implementation and pilot execution have created a blueprint for C-ITS deployment of roadside stations here in Australia and globally.

13 QGOV (13 74 68)
www.tmr.qld.gov.au | www.qld.gov.au