Project Specific Technical Specification

Transport and Main Roads
PSTS007 C-ITS Station Protocol Specification

October 2020

Queensland
Government

Document control sheet

Contact for enquiries and proposed changes

If you have any questions regarding this document or if you have a suggestion for improvements, please contact:

Contact officer Miranda Blogg

Title Director (CAVI)

Phone 07 3066 8251

Version history

Version no.	Owner	Date	Nature of amendment
1.0	Peter Chalmers	29/06/2018	Tender Issue
1.1	David Alderson	06/07/2019	Updates to match learnings from implementation
1.2	Peter Chalmers	28/10/2020	Updated MQTT topic names for the current implementation. Added the new EtsiMessageCollection message for default speeds.

Confidential

Copyright

Contents

1 Introduction 1

2 Definition of Terms 1

3 Reference Documents 2

4 C-ITS-F Protocol 3

4.1 Packet Structure and Descriptions 3

4.2 ASN.1 schema 3

4.3 Topics 5

4.4 Operational Behaviour 7

4.4.1 Connection to the Broker 8
4.4.2 Publish and Subscribe 9
4.4.3 Position Augmentation 9
4.4.4 Configuration, Tile and Static Speed IVIM Data Set Management 10
4.4.5 Applying Configuration Data 11
4.4.6 Logging Use Case Operation 11
4.4.7 MAPEM for R-ITS-S 12
4.4.8 Geomessaging 13
4.4.8.1 Retrieving Tiles Using the Recursive Tile Function 13
4.4.8.2 Static Speeds for V-ITS-S 15
4.4.8.3 BoQ, RHW, RWW, School Zone and Variable Speed Limits 16

5 SCMS Protocol 18

5.1 Packet Format 18

5.2 Security Certificates 18

5.3 Certificate Profile 19

5.4 Connection to the SCMS 19

5.5 Operational Behaviour 19

Appendix A AWS MQTT Implementation 20

Appendix B MQTT Messaging 22

1 Introduction

This document provides the standardised protocols for communication between stations in the C-ITS environment for Transport and Main Roads.

The protocols are defined based on the following interaction types:

1. C-ITS-F Protocol – interaction between C-ITS stations in the field and the Central ITS Facility
2. SCMS Protocol – interaction between the C-ITS stations and the Secure Credential Management System (SCMS) server for enabling secure transfer of data on other interactions

The protocols combine the international communication standards used in C-ITS and Internet-of-Things (IoT) to deliver the data transfer needs of the C-ITS environment. Detailed context to the use of the protocols in implementation can be found in the technical specifications.

Other C-ITS interfaces such as the ITS-G5 interaction between multiple field C-ITS stations are defined in C-ITS station specifications.

2 Definition of Terms

Table 2.1 – Acronyms

Acronym	Term
AA	Authentication authority of the SCMS
AT	Authentication ticket
AWS	Amazon Web Services
C-ITS-S	Central C-ITS station
EA	Enrolment authority of the SCMS
EC	Enrolment certificate
FOT	Field operational test
IoT	Internet of things
R-ITS-S	Roadside ITS station
SCMS	Security credential management system
SDK	Software development kit
TLS	Transport layer security
V-ITS-S	Vehicle ITS station

Table 2.2 – Definitions

Acronym/Term	Term Description
3G/4G	Cellular wireless network provided through a telecommunications company. 3G is the 3rd generation data network, 4G the fourth and LTE stands for Long Term Evolution.
AWS IoT platform	AWS implementation of MQTT as an IoT protocol https://aws.amazon.com/iot-platform/, AWS IoT platform specification https://aws.amazon.com/iot/sdk/ ,AWS IoT SDK specification.
C-ITS-F	Back-end C-ITS including C-ITS-S, monitoring system, data capture system and FOT logging system.
Geomessaging	Technology that provides the ability to send messages to clients that are specific to the client's current region. Pilot regions will be specified as closed polygonal lines.
HMI message presentation	Messages sent to the HMI device from the V-ITS-S HMI message manager to present to the driver. Presentations includes a pictogram with text and/or graphic components and an optional sound.
HMI Presentation Manager	Function of the V-ITS-S that arbitrates the information presentation requests to the HMI device.

Acronym/Term	Term Description
HMI message notification	Messages from the V-ITS-S platform (e.g. start-up, software update, error) and use case warnings sent to the HMI presentation manager.
Monitoring system	Sub-system of the C-ITS-F that monitors the operation of the C-ITS Pilot system.
Safety Evaluator	C-ITS Pilot actor responsible for delivery of the safety evaluation for the Field Operational Test (FOT).
Use case warning	A warning presented by the HMI when use case applications are triggered.

3 Reference Documents

Table 3.1 – Referenced documents – External

Document ID	Document Name / Description
ISO/IEC 20922 v3.1.1 (2016-06)	Information technology -- Message Queuing Telemetry Transport (MQTT):2016
ETSI TS 941 V1.2.1 (2018-05)	Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
ETSI TS 103 097 V1.3.1	Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats
IEEE 1609.2:2016	Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages
RTCM Standard 10403.3 (2016-10)	Differential GNSS (Global Navigation Satellite Systems) Services – Version 3

Table 3.2 – Referenced Documents – Internal

Document ID	Document Name / Description
PSTS006	Data Entity Catalogue
PSTS008	SCMS Station Certificate Profile

4 C-ITS-F Protocol

The Central ITS Facility (C-ITS-F) provides a Message Query Transport Telemetry (MQTT) publish and subscribe service for transferring data between C-ITS stations. MQTT v3.1.1 as defined in ISO/IEC 20922:2016 is the underlying protocol to support connections on this service. The Amazon Web Services (AWS) implementation of MQTT v3.1.1 is used and therefore the variations for the AWS MQTT service should be adopted by all stations (Appendix A).

Note there are other connections to the C-ITS-F such as remote software updates and remote device maintenance which are outside of the scope of the C-ITS-F Protocol defined in this section.

4.1 Packet Structure and Descriptions

The following tables describe all MQTT publish and subscribe messages exchanged between the C-ITS-F and other stations. MQTT connections are described in section 4.4.1. Responses to publish and subscribe messages are defined in the MQTT protocol.

Table 4.1 – C-ITS-F Packet Structure

MQTT (ISO-IEC 20922:2016)			
Fixed Header	Variable Header	MQTT payload	Custom payload as defined in Table 4.2

Table 4.2 – C-ITS-F Packet Descriptions

Packet Description	Payload	Relevant ASN
Station Configuration (see section 4.4.4)	UPER encoded *asn.1 schema*	*stationConfiguration.asn*
Station platform (see section 4.4.6)	UPER encoded *asn.1 schema*	*stationPlatformData.asn*
C-ITS message event (see section 4.4.6)	UPER encoded *asn.1 schema*	*citsMessageEvents.asn*
Geomessaging tile (see section 4.4.8.1)	UPER encoded *asn.1 schema*	*geoTile.asn*
Signed C-ITS Message (see sections 4.4.8.2, 4.4.8.3 and 4.4.7)	TS 103 097:2017 with TMR modifications. Includes signature and UPER encoded C-ITS message payload	N/A
Position Augmentation (see section 4.4.3)	RTCM Standard 10403.3:2016 data	N/A
Safety Evaluation (see section 4.4.6)	UPER encoded *asn.1 schema*	*safetyEvaluationData.asn*
ETSI Message Collection	UPER encoded *asn.1* schema	*EtsiMessageCollection.asn*

4.2 ASN.1 schema

The ASN.1 schemas used with the topics are described in Table 4.3. The ASNs and data element definitions are detailed in *Data Entity Catalogue PSTS006*.

Table 4.3 – ASN.1 schemas

Message Name	Short Name	Schema	Description
Station Configuration	SCM	stationConfiguration.asn	Used to deliver device specific configuration information to the R-ITS-S or V-ITS-S. This message will contain configuration information for multiple categories including system, participant, device and use case.
Station Platform	SPDM	stationPlatformData.asn	Heartbeat message from R-ITS-S and V-ITS-S. Used for session tracking, platform-level events and error logging.
C-ITS Message Event	CME	citsMessageEvent.asn	Used to capture information relevant to presentation of C-ITS use case warnings and speed limits on the HMI, including processing of C-ITS messages by use case applications.
Geo Tile Message	GTM	geoTile.asn	Implements the recursive tile function used to deliver geographic tiles that are used by a vehicle to select the set of C-ITS message appropriate to the vehicle's position.
Safety Evaluation	CSEM	safetyEvaluationData.asn	Captures C-ITS messages published and received by all stations. There are two separate messages that use the same schema. **Type 1:** Received and transmitted CAM only. **Type 2:** Received and transmitted DENM, IVIM, MAPEM and SPATEM only.

Message Name	Short Name	Schema	Description
ETSI Message Collection	*none*	EtsiMessageCollection.asn	This message contain default (static) speed IVIM as a collection per tile. There are about 25,000 default speed IVIM for the pilot area. Distribution as individual IVIM is too slow for operational purposes. IVIM are encoded and added to packets to reduce number of messages and hence the time to publish these messages to the V-ITS-S

4.3 Topics

Messages are distributed by the C-ITS-F using the topics described in Figure 4.1.

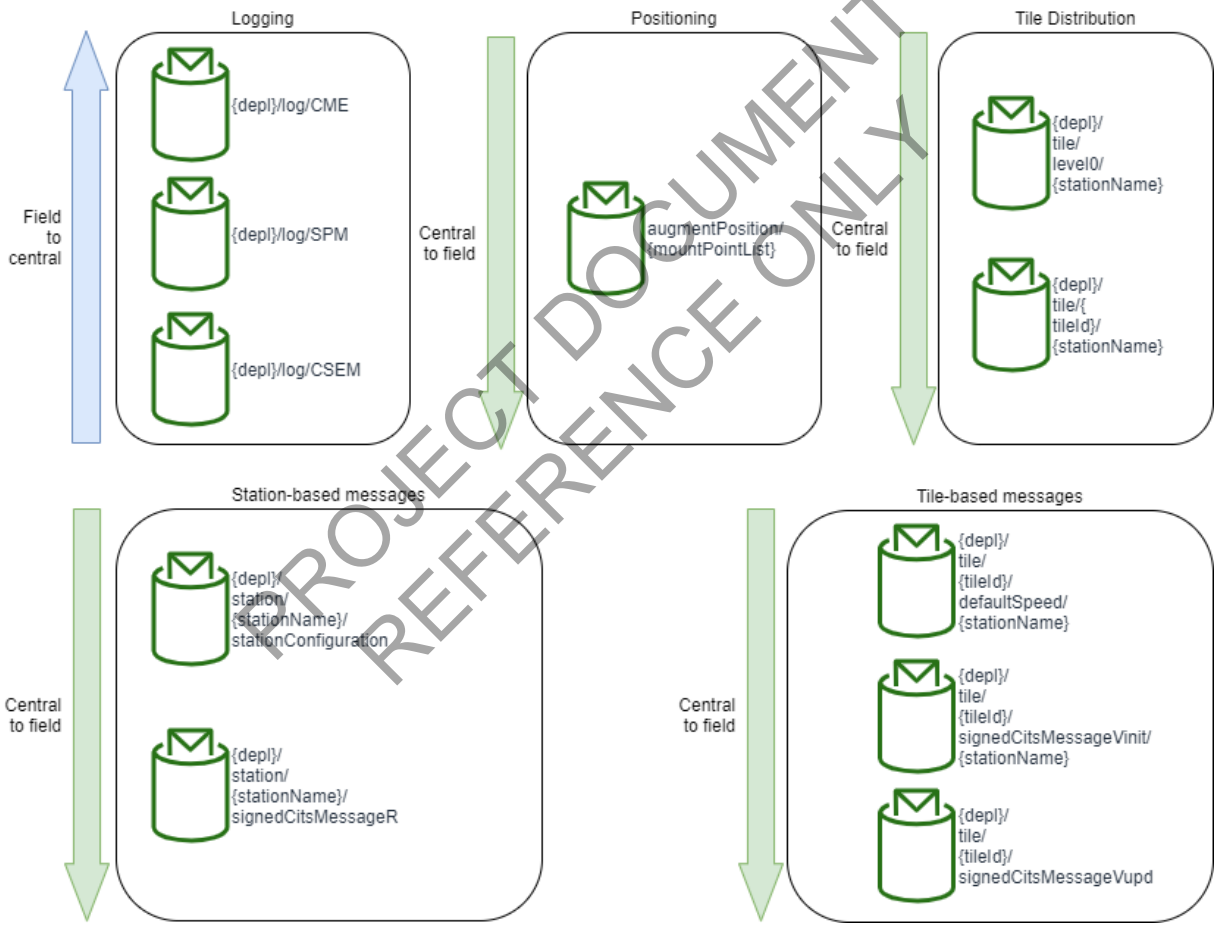


Figure 4.1 – MQTT topic structure

Stations publish and subscribe to the topics as defined in Table 4.4. Publication and subscription rights are managed and enforced by the broker.

Table 4.4 – Topic descriptions

Topic (case sensitive)	Publish/subscribe trigger	MQTT message payload
Position augmentation		
augmentPosition/ <mount point list> for example, augmentPosition/BEE24_CLEV4	At session start, change of tile (if required) or reconnection	RTCM GNSS data
Log data		
<depl>/ log/ stationPlatformData	Period: *logFrequency*	*stationPlatformData.asn*
<depl>/ log/ citsMessageEvent	Period: *logFrequency*	*citsMessageEvent.asn*
<depl>/ log/ safetyEvaluationData	Period: *csemLogWatchdogTimeout*	*safetyEvaluationData.asn*
Station configuration		
<depl>/ station/ <stationName>/ stationConfiguration	At session start or reconnection	*systemConfiguration.asn*
Geographic tiling		
<depl>/ tile/ level0/ <stationName>	Change in *tileDataSetVersion* in the *stationConfiguration.asn* message	*geoTile.asn*
<depl>/ tile/ <tileId>/ <stationName>	Change in *tileDataSetVersion* in the *stationConfiguration.asn* message	*geoTile.asn*
Static speed IVIM for V-ITS-S		
<depl>/ tile/ <tileId>/ defaultSpeed/ <stationName>	Change in *staticSpeedIvimDataSetVersion* in the *stationConfiguration.asn* message	EtsiMessageCollection.asn

Topic (case sensitive)	Publish/subscribe trigger	MQTT message payload
C-ITS BoQ, school zone and variable speed, RHW or RWW messages for V-ITS-S		
<depl>/ tile/ <tileId>/ signedCitsMessageVinit/ <stationName>	Session start or reconnection and *tileId* is calculated a new *tileId* is detected	TS 103 097:2017 structure
<depl>/ tile/ <tileId>/ signedCitsMessageVupd	Session start or reconnection and *tileId* is calculated a new *tileId* is detected	TS 103 097:2017 structure
MAPEM for R-ITS-S		
<depl>/ station/ <stationName>/ signedCitsMessageR	Session start or reconnection, pushed by C-ITS-S if intersection changes.	TS 103 097:2017 structure

Table 4.5 – Broker topics, security and permissions

Topic	Signed	C-ITS-F		V-ITS-S		R-ITS-S	
		Pub	Sub	Pub	Sub	Pub	Sub
<depl>/log/stationPlaformData			✓	✓		✓	
<depl>/log/citsMessageEvent			✓	✓			
<depl>/log/safetyEvaluationData			✓	✓		✓	
<depl>/tile/level0/<stationName>		✓			✓		
<depl>/tile/<tileId>/<stationName>		✓			✓		
<depl>/station/<stationName>/stationConfiguration		✓			✓		✓
<depl>/station/<stationName>/signedCitsMessageR	✓	✓					✓
<depl>/tile/<tileId>/signedCitsMessageVupd	✓	✓			✓		
<depl>/tile/<tileId>/signedCitsMessageVinit/<stationName>	✓	✓			✓		
<depl>/tile/<tileId>/defaultSpeed/<stationName>	✓	✓			✓		
<depl>/tile/<tileId>/augmentPosition		✓			✓		

4.4 Operational Behaviour

The messaging operational behaviour described in ISO/IEC 20922:2016 section 4 apply to the MQTT service. C-ITS application operational behaviour are described in the following sections.

4.4.1 Connection to the Broker

At session start and after loss of connection to the broker during a session a R-ITS-S and V-ITS-S will connect to the MQTT broker. The broker address will be specified in the configuration parameter set for the device and may change depending on the environment in use, for example, test or production. The connection request will use the parameters specified in Table 4.6.

Table 4.6 – MQTT connection parameters

Parameter	Value	Notes
clientId	*varies*	*stationName* for the station
cleanSession	true	AWS IoT does not permit persistent connections and will disconnect the client if a request is made with this parameter set to false
lastWillTopic	dev/<clientId>/will	From parameter set for the device
lastWillQos	1	
lastWillMessage	unexpected disconnect	Test for the will message
lastWillRetain	false	AWS IoT does not permit retained messages and will disconnect the client if a request is made with this parameter set to true.

The connection sequence is described in Figure 4.2.

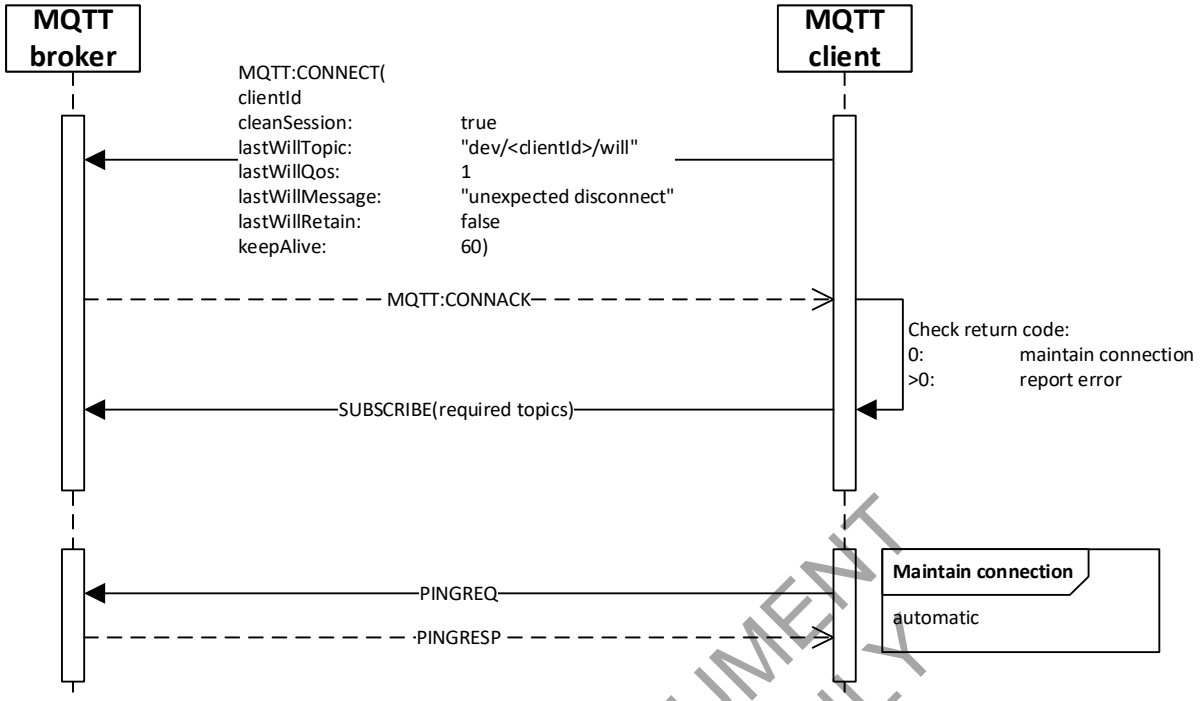


Figure 4.2 – MQTT connection sequence

4.4.2 Publish and Subscribe

All publication and subscription requests will be use quality of service of 1.

All publication requests will have *retainFlag* set to false. AWS IoT will disconnect any client requesting that messages be retained on the broker, that is, *retainFlag* set to true.

At session start and whenever the connection to the broker is lost during a session a R-ITS-S and V-ITS-S will subscribe to the following topics.

4.4.3 Position Augmentation

RTK positioning augmentation will use RTCM v3 standard transmitted using the Ntrip (Network Transport of RTCM via Internet Protocol). Geoscience Australia provides this at approximately 1Hz, and this data will be made available, as the data is received, via the MQTT topic *augmentPosition/<mount point list>* as shown in Figure 4.3. The RTCM GNSS data from the Ntrip message will be published as the payload of the message.

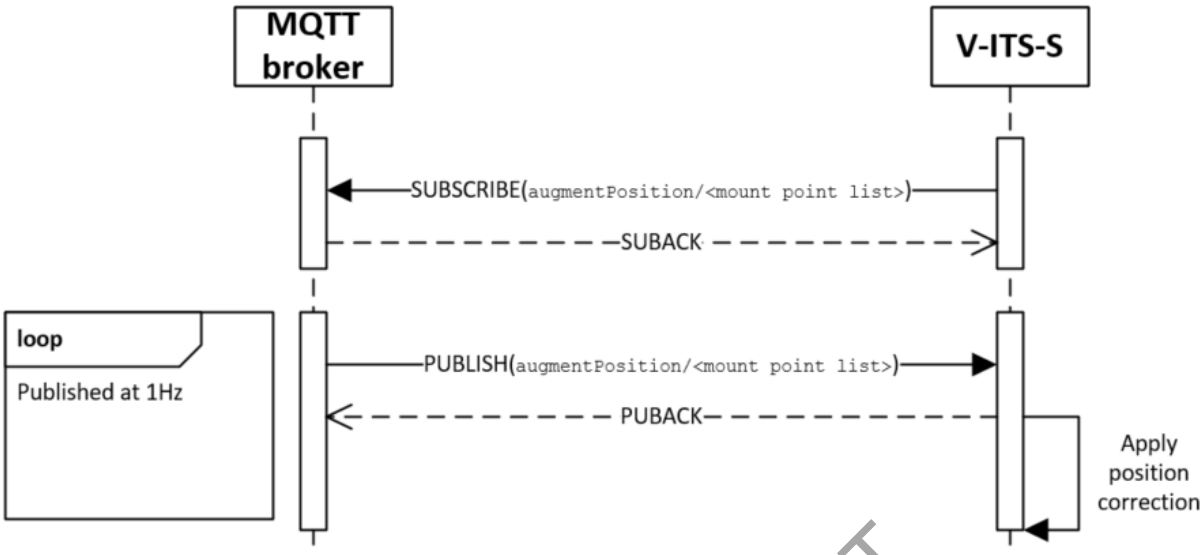


Figure 4.3 – Position augmentation

4.4.4 Configuration, Tile and Static Speed IVIM Data Set Management

Configuration, tile and static speed IVIM data set management used to minimise the transfer of slow-changing data for field C-ITS stations.

Configuration data is used by both R-ITS-S and V-ITS-S. Tile and static speed IVIM data is only applicable to the V-ITS-S.

Table 4.7 – Configuration, tile and static speed IVIM data management

Set	Set Version	Data	Processing
Configuration	*configDataSetVersion* changes whenever a configuration item in the set is updated	A unique identifier for this set version	
Tiles	*tileDataSetVersion* changes whenever a tile in the set is updated	A unique identifier for this set version	Recursive tile function (see section 4.4.8.1) is executed when the *tileDataSetVersion* in the message does not match the *tileDataSetVersion* stored by the station.

Set	Set Version	Data	Processing
Static speed	*staticSpeedIvimData SetVersion* changes whenever the static speed IVIM in any tile is updated	A unique identifier for this set version. Additionally, a list of *tileId* and the version number of the static speed IVIM set (*staticSpeedIvimSet Version*) for *tileId*.	Static speed IVIM downloads are triggered when *staticSpeedIvimDataSetVersion* in the message does not match the stored *staticSpeedIvimDataSetVersion* stored by the station. Only IVIM for *tileId* where *staticSpeedIvimSetVersion* has changed are downloaded.

4.4.5 Applying Configuration Data

The download of configuration data from the *<depl>/station/<stationName>/stationConfiguration* topic will be triggered by an update on the topic. Configuration in the *stationConfiguration.asn* message is applied by the station immediately as shown in Figure 4.4.

Figure 4.4 – Configuration data

4.4.6 Logging Use Case Operation

Logging data includes:

- *stationPlatformData.asn* message – forms the R-ITS-S and V-ITS-S heartbeat and contains platform-level hardware and software flags and event/error messages.
- *citsMessageEvent.asn* message – contains information relevant to presentation of C-ITS use case warnings and speed limits on the HMI, including processing of C-ITS messages by use case applications. This message is event driven.
- *safetyEvaluationData.asn* messages – captures C-ITS messages published and received by all stations. Each message type is logged separately by the device. The *stationPlatformData*, *citsMessageEvent* and *safetyEvaluationData* messages are sent as described in Figure 4.5.

- *stationPlatformData* and *citsMessageEvent* data is periodically uploaded to the C-ITS-F at the rate of *logFrequency*. *safetyEvaluationData* is uploaded on reaching one of the log size limits (*csemCamLogLimit, csemDenmLogLimit*, *csemIvimLogLimit*, *csemMapemLogLimit*, *csemSpatemLogLimit*) or periodically at *csemLogWatchdogTimeout*.

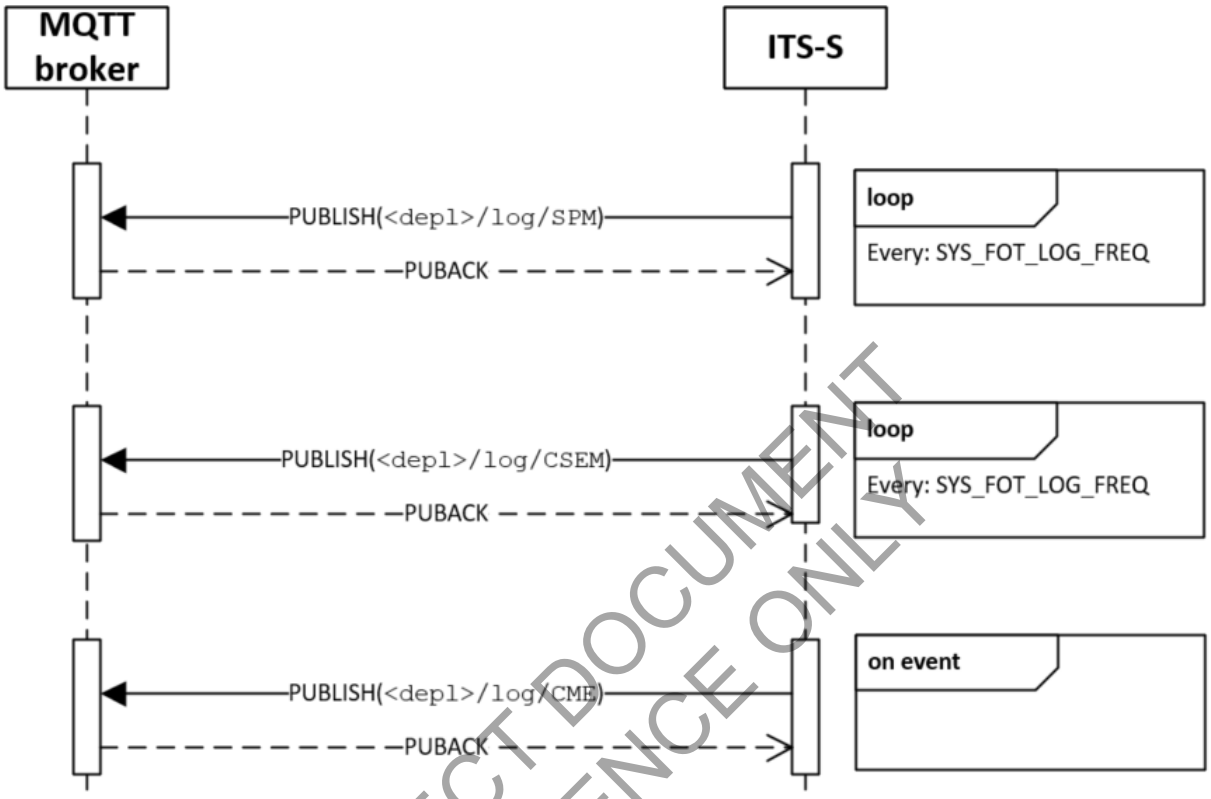


Figure 4.5 – Logging use case operation

4.4.7 MAPEM for R-ITS-S

MAPEM are made available to the R-ITS-S on the *<depl>/station/<stationName>/signedCitsMessageR* topic whenever the R-ITS-S subscribes and whenever the MAPEM version changes while a R-ITS-S is subscribed.

A R-ITS-S will load static speed as shown in Figure 4.6.

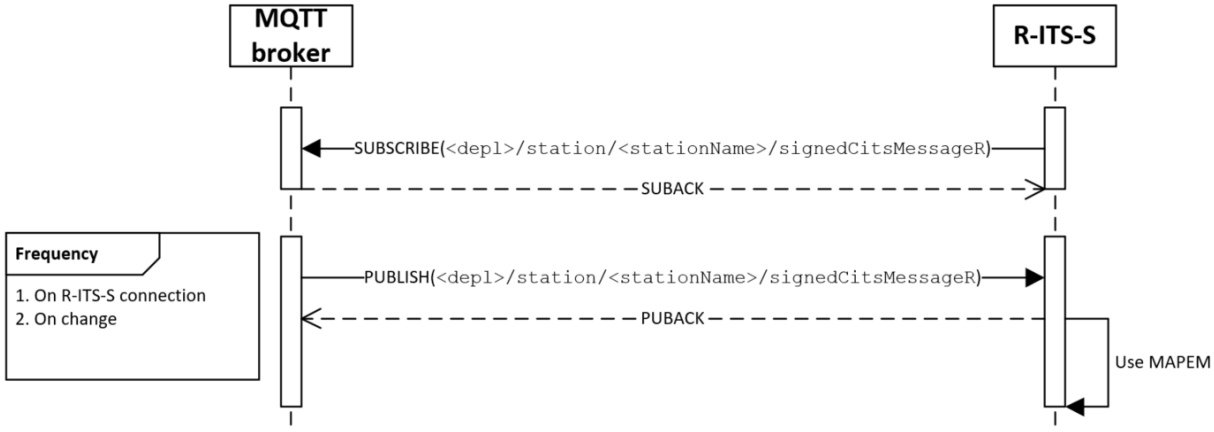


Figure 4.6 – MAPEM for R-ITS-S

4.4.8 Geomessaging

C-ITS messages that are disseminated from the C-ITS-F are grouped based on geographic boundaries using geomessaging. This allows stations to reduce the number of C-ITS messages it needs to deal with by restricting them to those relevant to its location. Geomessaging is used so that:

1. The V-ITS-S will not send its position to the C-ITS-F
2. The solution will work at all locations world-wide
3. The time taken to send a geographic tile's message set to a V-ITS-S meets the needs of the use case applications that are enabled.

The messages will include signed C-ITS messages such as DENM for RHW and RWW, IVIM for RWW and static, school zone and variable speeds that are provided only to the V-ITS-S.

Due to the differences in processing, C-ITS message delivery will be discussed separately and rely on the vehicle knowing the tile matching its current position. The sections noted in the following dot-points describe the process of geomessaging.

- The retrieval of tiles for matching tiles to vehicle position is discussed in section 4.4.8.1
- Static speed IVIM are numerous and change infrequently and are discussed in section 4.4.8.2
- BoQ, RHW, RWW, school zone and variable speed DENM and IVIM are discussed in section 4.4.8.3.

4.4.8.1 Retrieving Tiles Using the Recursive Tile Function

The MQTT topic <depl>/*tile/level0/<stationName>* is the start point for the recursive tile function. The following tile levels will be provided.

Tile set	**implementation**
Continents	Only Australia is specified
Country/state	All Australian states are specified
Region	One region will be provided corresponding to the boundary of the C-ITS area. Operation of use cases and logging is restricted outside the C-ITS area.
Sub-region	Tiles will be used to restrict the number of C-ITS messages that a device must process while travelling in the tile. The tiles shown in Figure 4.7 are an example and may be subject to change.

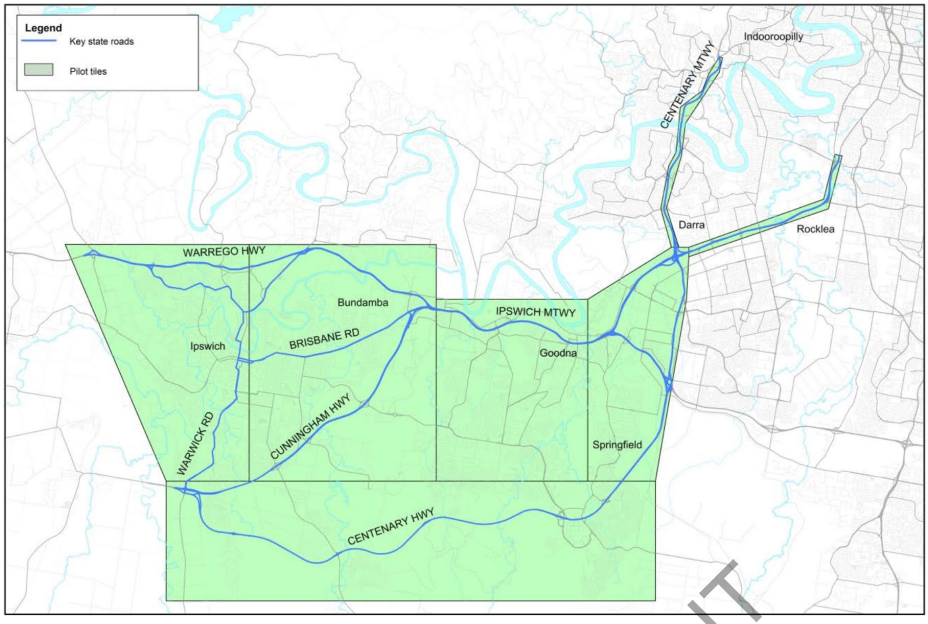


Figure 4.7 – Pilot tiles

The initiation of the recursive tile function is described in section 4.4.4. An example showing the subscription sequence for the C-ITS is shown in Figure 4.8.

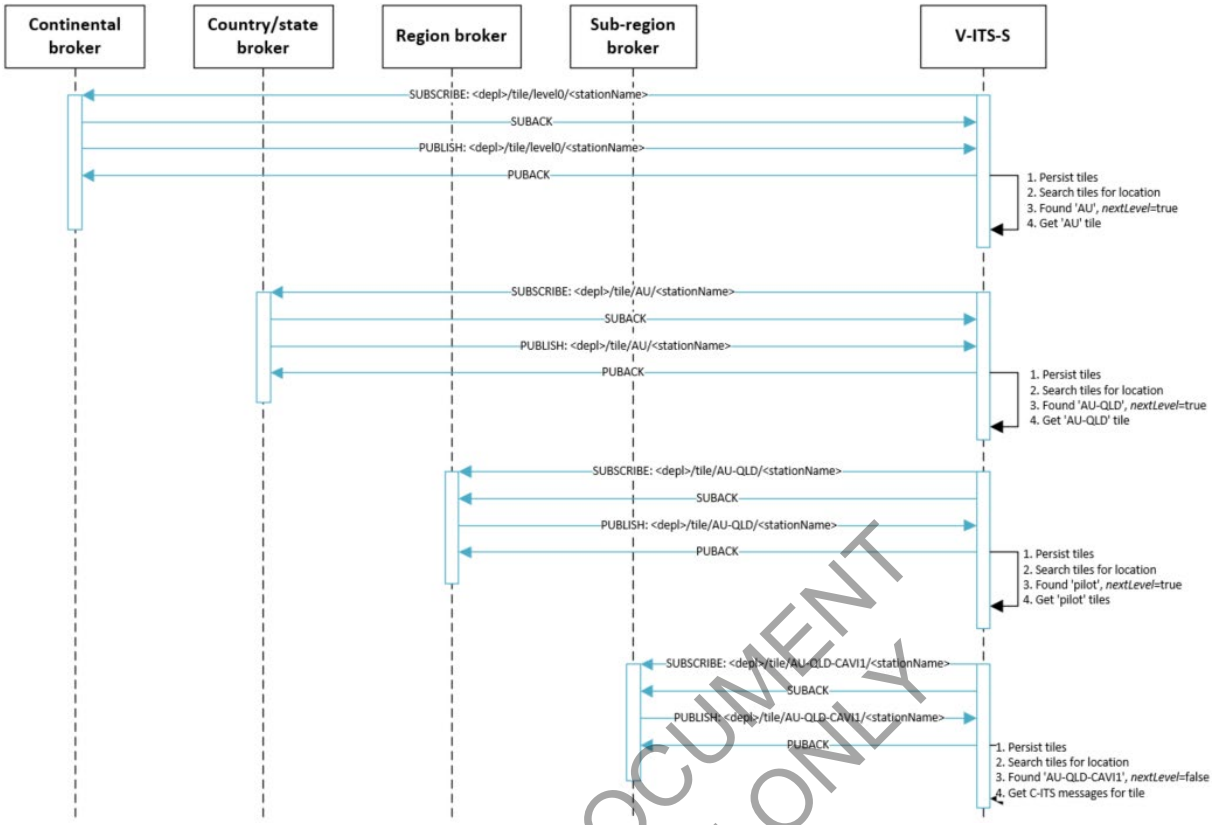


Figure 4.8 – Recursive tile function example

The *nextLevel* attribute of the *geoTile.asn* message is used to control recursion.

While *nextLevel* is true then the V-ITS-S will download sub-tiles of the current tile by using the referral topic for the tile relevant to the device. At each point the downloaded tiles are persisted so that they are retained when a station is switched off.

When *nextLevel* is false the level has a referral to a topic that provide the C-ITS messages. This triggers the processes describe in section 4.4.8.2 and 4.4.8.3.

4.4.8.2 Static Speeds for V-ITS-S

IVIM for static speeds will make up the bulk of the messages for a tile with one IVIM for each road segment in the spatial data set. The static speed IVIM are not expected to change frequently. The tile-data version control treatment described in section 4.4.4 is designed to reduce start-up time for the V-ITS and the number of times that static speed IVIM are transmitted to devices. Static speed IVIM will downloaded by the V-ITS-S and persisted over power loss events.

A V-ITS-S will load static speed as shown in Figure 4.9.

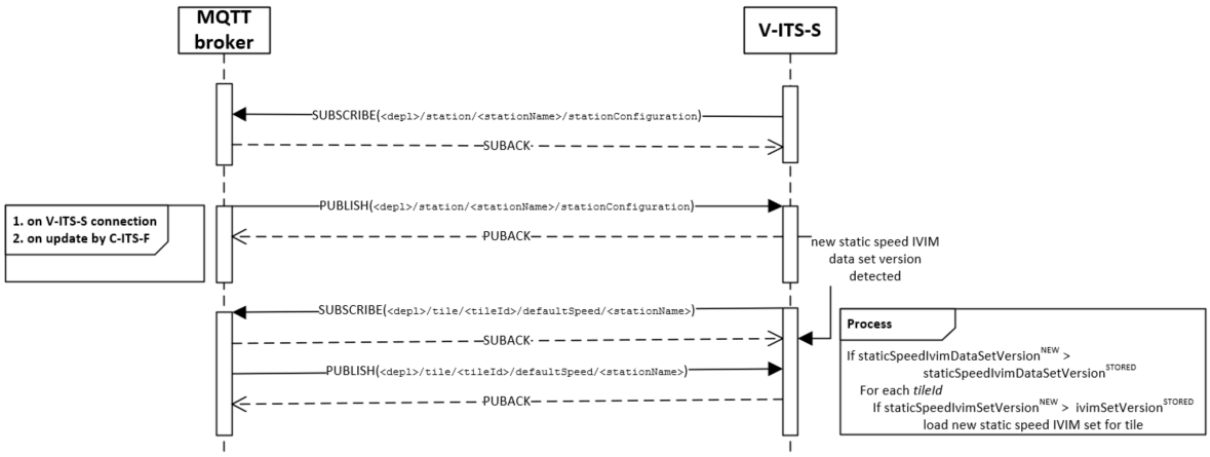


Figure 4.9 – Loading static speed IVIM

4.4.8.3 BoQ, RHW, RWW, School Zone and Variable Speed Limits

DENM and IVIM will be generated by the C-ITS-F because of BoQ, RHW, RWW, school zone and variable speed use case related operations. These messages are only used by the V-ITS-S.

When a V-ITS-S session is started and the device has determined the relevant *tileId* based on its position, the device will need to initialise itself with the current set and keep itself up to date with new C-ITS messages by subscribing to the topics *<depl>/tile/<tileId>/signedCitsMessageVinit/<stationName>* and *tile/<tileId>/signedCitsMessageVupd*.

The C-ITS-F will publish current C-ITS messages created prior to the subscription time only once to the *<depl>/tile/<tileId>/signedCitsMessageVinit/<stationName>* topic. When the vehicle leaves a tile the V-ITS-S will un-subscribe from the old tile. This subscription is described in Figure 4.10.

Figure 4.10 – Getting initial DENM and IVIM

Once the V-ITS-S session is established updates of DENM and IVIM messages will be published to all V-ITS-S subscribed to a tile through the MQTT topic *<depl>/tile/<tileId>/signedCitsMessageVupd*. When the vehicle leaves a tile the V-ITS-S will unsubscribe from the old tile. This subscription is described in Figure 4.11.

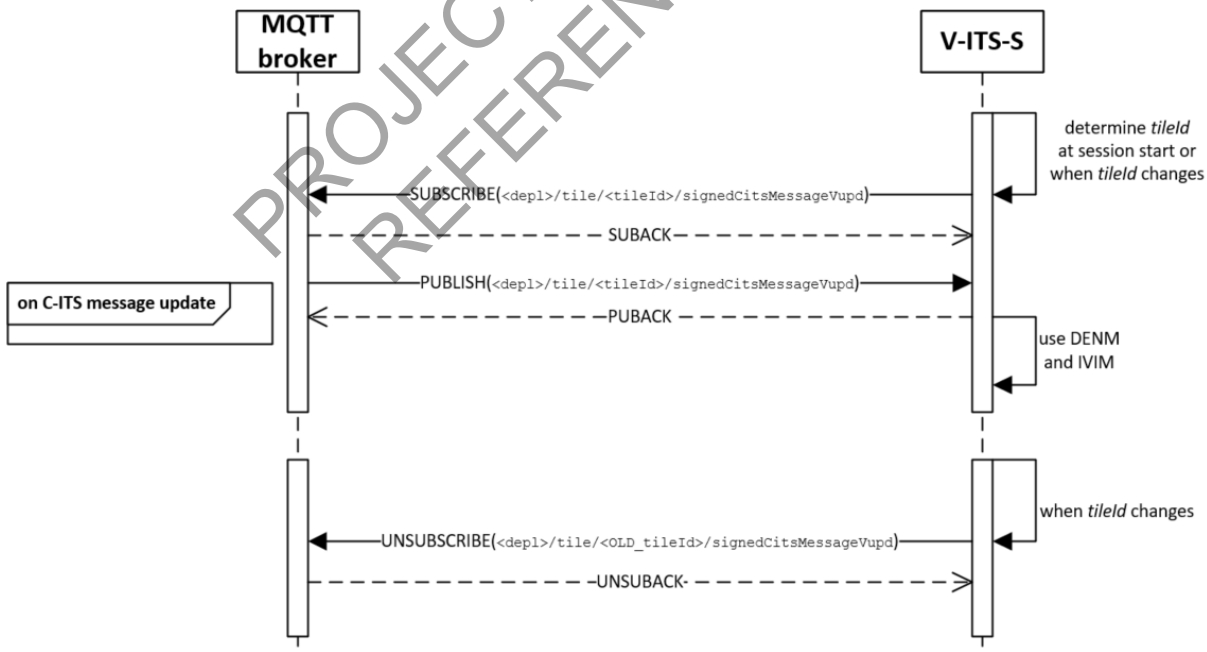


Figure 4.11 – C-ITS message updates for V-ITS-S

5 SCMS Protocol

The SCMS is used for the following purposes.

- Creation of a device's enrolment credential
- Creation and maintenance of a devices authorisation tickets
- Access to the root certification authority certificate
- Access to the certificate trust list
- Access to the certificate revocation list.

The C-ITS stations and their software/firmware development shall follow an applicable best practice security development guideline – such as the OWASP Developer Guide.

ITS-S design will incorporate the Australian Signals Directorate's Top 4 Strategies to Mitigate Cyber Security Incidents.

5.1 Packet Format

Over-The-Air message protocol shall use a REST API to fulfil requests via HTTPS.

All communication shall adhere to ETSI TS 102 94:2018 using a certificate format as defined in ETSI TS 103 097:2017.

5.2 Security Certificates

Communication data shall adhere to the clarifications and/or deviations from these standards described in this section.

R-ITS-S and V-ITS-S shall manage security certificates as follows.

a. Over-The-Air message protocol shall use a REST API to fulfil requests via HTTPS.

b. *EtsiTs102941Data* structure version shall not be set to integer 1 (ETSI TS 102 941:2018 "the version of EtsiTS102941Data structure shall be set to version v1 (integer value 1)"), and shall continue to use the current ETSI TS 103 097 (2017) ASN.1 specification where "EtsiTs103097Data ::= Ieee1609Dot2Data" with protocolVersion set to 3.

c. The version of *Ieee1609Dot2Data* structure shall be set to integer value 3 (ETSI TS 103 097:2017 contradicts ETSI TS 102 941:2018).

d. The version of *CertificateBase* structure shall be set to integer value 3 (ETSI TS 103 097:2017).

e. ITS-AIDs/PSIDs & SSPs must be set and adhered to according to the provided *SCMS Certificate Profile* document.

f. Component assuranceLevel of type SubjectAssurance, as defined in IEEE Std 1609.2:2016 shall be ABSENT in all cases.

g. GeographicRegion in ECs shall be "countryOnly" with the value 36 (ISO3166-1 Australia).

h. ITS-S must validate GeographicRegion in any certificates containing GeographicRegion.

i. The SCMS shall use only ECCp256 & SHA 256 for Root, EA, AA and ITS-S.

5.3 Certificate Profile

The certificate profile specified in PSTS008 Station Certificate Profile shall be adhered to.

5.4 Connection to the SCMS

Connections to the SCMS on IF2 will be made to the following endpoints that are specified in *stationConfiguration.asn*:

- scmsEaEndpoint
- scmsAaEndpoint.

These network endpoints are available from the Principal during software development and testing phases.

The connection will be made using an HTTPS opaque tunnel using a X.509v3 certificate on the SCMS.

5.5 Operational Behaviour

Processes required to obtain enrolment certificates, authorisation tickets, root certification authority certificate, certificate trust list and certificate revocation list are defined by ETSI TS 102 941:2018.

Messages will us the type `EtsiTs103097Data-SignedAndEncrypted`.

Appendix A AWS MQTT Implementation

Connections to the MQTT service should adopt the current variations described by AWS from https://docs.aws.amazon.com/iot/latest/developerguide/protocols.html.

As at 6th June 2018, the variations are:

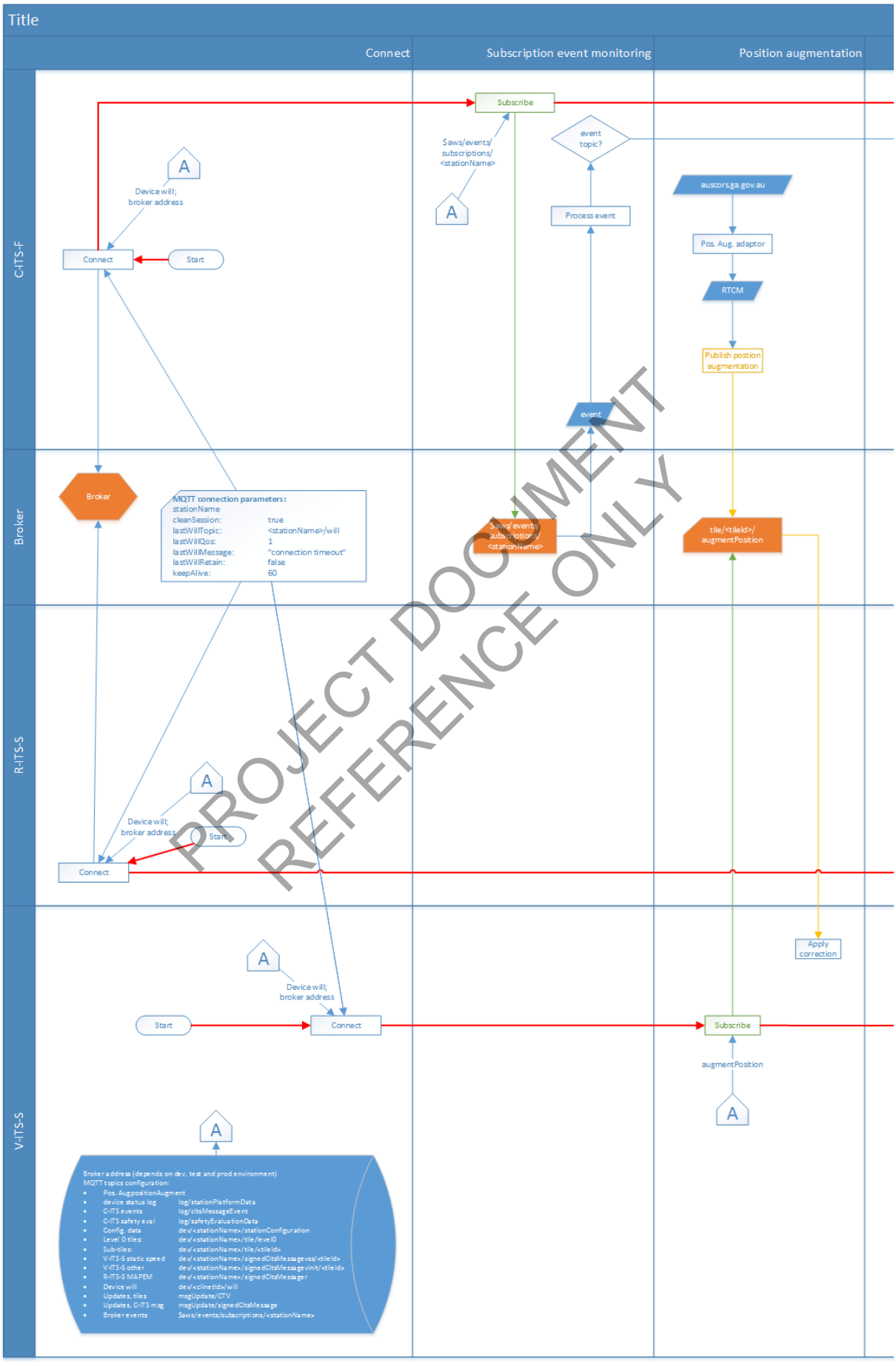
Although the AWS IoT message broker implementation is based on MQTT version 3.1.1, it deviates from the specification as follows:

- In AWS IoT, subscribing to a topic with Quality of Service (QoS) 0 means a message will be delivered zero or more times. A message might be delivered more than once. Messages delivered more than once might be sent with a different packet ID. In these cases, the DUP flag is not set.
- AWS IoT does not support publishing and subscribing with QoS 2. The AWS IoT message broker does not send a PUBACK or SUBACK when QoS 2 is requested.
- The QoS levels for publishing and subscribing to a topic have no relation to each other. One client can subscribe to a topic using QoS 1 while another client can publish to the same topic using QoS 0.
- When responding to a connection request, the message broker sends a CONNACK message. This message contains a flag to indicate if the connection is resuming a previous session. The value of this flag might be incorrect if two MQTT clients connect with the same client ID simultaneously.
- When a client subscribes to a topic, there might be a delay between the time the message broker sends a SUBACK and the time the client starts receiving new matching messages.
- The MQTT specification provides a provision for the publisher to request that the broker retain the last message sent to a topic and send it to all future topic subscribers. AWS IoT does not support retained messages. If a request is made to retain messages, the connection is disconnected.
- The message broker uses the client ID to identify each client. The client ID is passed in from the client to the message broker as part of the MQTT payload. Two clients with the same client ID are not allowed to be connected concurrently to the message broker. When a client connects to the message broker using a client ID that another client is using, a CONNACK message will be sent to both clients and the currently connected client will be disconnected.
- The message broker does not support persistent sessions (connections made with the cleanSession flag set to false. The AWS IoT message broker assumes all sessions are clean sessions and messages are not stored across sessions. If an MQTT client attempts to connect to the AWS IoT message broker with the cleanSession set to false, the client will be disconnected.
- On rare occasions, the message broker might resend the same logical PUBLISH message with a different packet ID.
- The message broker does not guarantee the order in which messages and ACK are received.

AWS IoT does not implement all features of the MQTT protocol.

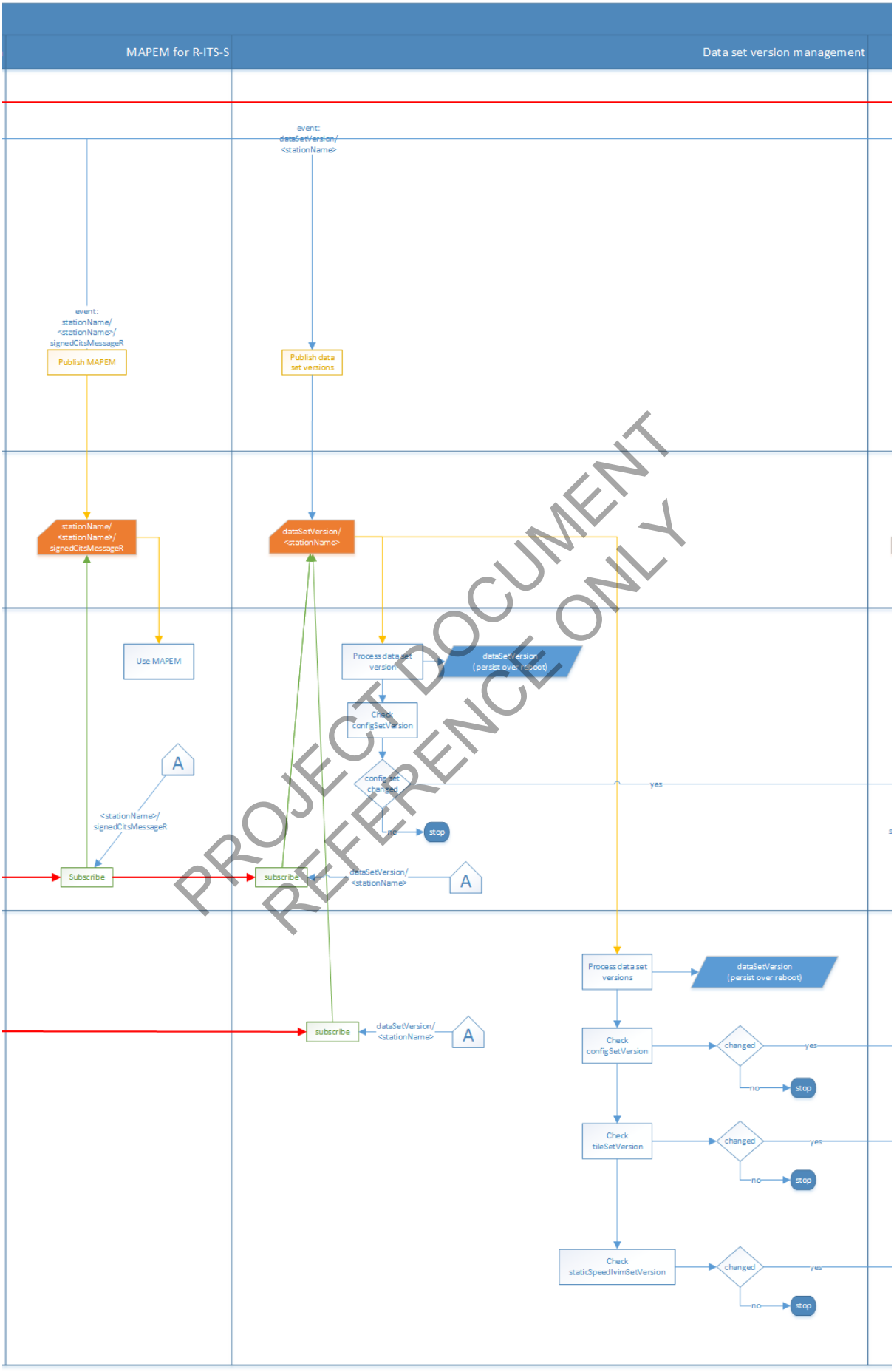
Feature	Description
Persistent Sessions	AWS IoT does not implement persistent sessions. Stations maintain a list of current MQTT topics so that topic subscriptions can be re-established after connection loss.
Retained Messages	The AWS IoT does not implement retained messages. The C-ITS-F will implement this functionality to provide timely data to stations after communications outages. This functionality is dependent on client subscriptions in line with persistent sessions above.
Service Limits	Stations should adhere to the current limitations of the AWS MQTT service from http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_iot

Appendix B MQTT Messaging



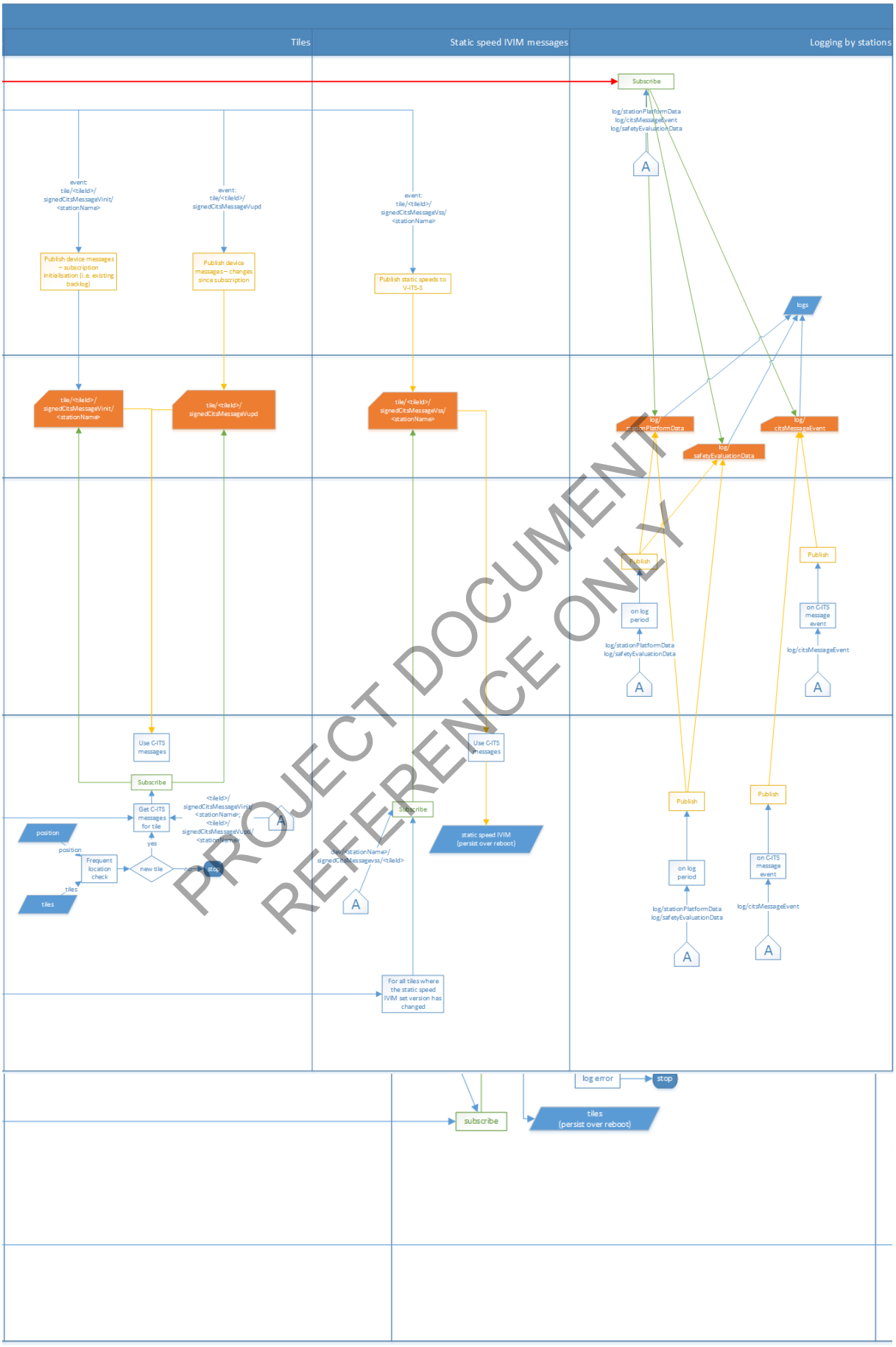
See Next Page

See Previous Page



See Next Page

See Previous Page



See Next Page