

PROJECT DOCUMENT
REFERENCE ONLY

Project Specific Technical Specification

**Transport and Main Roads
PSTS005 R-ITS-S Equipment**

AUGUST 2021

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 Nicholas Brook

Title Principal Engineer (CAVI)

Phone (07) 3066 8262

Version history

Version no.	Owner	Date	Nature of amendment
1.0	Terry Su	29/06/2018	Tender Issue
1.1	David Alderson	31/01/2019	Updates from inception meetings
1.2	David Alderson	06/07/2019	Updates to match learnings from implementation
2.0	Timothy Liu	10/11/2020	Update based on experience
2.1	Jian Qin	18/08/2021	Update Figure 5.1 remove Figure 5.2

Copyright



<http://creativecommons.org/licenses/by/3.0/au/>

© State of Queensland (Department of Transport and Main Roads) 2018

Contents

- 1 Introduction 1**
- 2 Definition of Terms 1**
- 3 Reference Documents 3**
- 4 Quality System Requirements 6**
 - 4.1 Testing and Commissioning 6
 - 4.1.1 Testing Methodology 6
 - 4.1.2 Testing Activities 6
- 5 System Requirements 8**
 - 5.1 C-ITS Architecture 8
 - 5.2 R-ITS-S Architecture 9
 - 5.3 ITS-G5 Communications (Interface IF4) 11
 - 5.3.1 Message Support 11
 - 5.4 Ethernet (Interface IF2, IF3 and IF5) 12
 - 5.4.1 Session and Communication Management 12
 - 5.4.1.1 Decoding and Encoding Messages 12
 - 5.4.2 Message Support 12
 - 5.5 GNSS 13
 - 5.5.1 R-ITS-S Positioning 13
 - 5.5.2 Timing and Synchronisation 13
- 6 Operational Requirements (Applications) 14**
 - 6.1 Data Logging 14
 - 6.1.1 Data Logging Security 14
 - 6.1.2 Log Data Retention 14
 - 6.1.3 Safety Evaluation Data Logging 15
 - 6.1.3.1 Data Definition 15
 - 6.1.4 Station Platform Data Logging 17
 - 6.1.4.1 Session Monitoring 17
 - 6.1.4.2 Platform Metrics 17
 - 6.1.4.3 Platform Error Logs 18
 - 6.1.4.4 Data Definition 18
 - 6.2 Control and Configuration 20
 - 6.3 R-ITS-S Software Update Client 20
 - 6.4 Remote Maintenance 21
- 7 Security 21**
 - 7.1 Network Security Certificates 21
 - 7.2 Station Lifecycle 22
 - 7.2.1 Manufacture 22
 - 7.2.2 Enrolment 22
 - 7.2.3 Authorisation 22
 - 7.2.4 Message Signing and Verification 22
 - 7.2.5 Pre-Installation Configuration 22
 - 7.3 Device Access Security 23
- 8 Technical Requirements 24**
 - 8.1 System Start-Up 24
 - 8.2 Storage 24

8.3	Maintenance Communications	24
8.4	Control/Diagnostic Software	24
8.5	Failure Modes	24
8.6	Radio Performance	24
9	Electrical Requirements	24
9.1	General	24
9.2	Powering R-ITS-S	25
9.3	Surge Protection	25
10	Mechanical and Physical Requirements	25
10.1	Environmental Conditions	25
10.2	R-ITS-S Enclosure	25
10.3	R-ITS-S Mounting Brackets	25
10.4	Location of R-ITS-S Equipment	26
10.5	Design Life	26
11	Installation	26
11.1	Initial Configuration	26
12	Key Configurable Parameters	27

PROJECT DOCUMENT
REFERENCE ONLY

1 Introduction

This Technical Specification defines the supply, functional, electrical, telecommunication, performance and physical requirements for the Roadside Intelligent Transport System Station (R-ITS-S).

The R-ITS-S was used in the Ipswich Connected Vehicle Pilot (ICVP) as an interface between a signalised intersection and vehicle stations for the purpose of locally broadcasting intersection information over ITS-G5. In the pilot 29 of these were installed and used.

The R-ITS-S consists of the hardware, firmware, software, applications, communication interfaces, antennae, cabling and any other items required to enable operation to the technical specifications defined.

This Technical Specification shall be read in conjunction with MRTS01 *Introduction to Technical Specifications*, MRTS50 *Specific Quality System Requirements* and other Technical Specifications as appropriate.

2 Definition of Terms

Table 2-1 – Acronyms

Acronym	Term
ACMA	Australian Communications and Media Authority
AS	Australian Standard
BTP	Basic Transfer Protocol
CAM	Cooperative awareness message (EU)
CAVI	Cooperative and Automated Vehicle Initiative
C-ITS	Cooperative intelligent transport systems
C-ITS-F	Central ITS facility
C-ITS-S	Central ITS station
CIT	Component Integration Test
CT	Commissioning Test
DC	Direct Current
DENM	Decentralised environmental notification message (EU)
EIRP	Equivalent Isotropically Radiated Power
ETSI	European Telecommunications Standards Institute
FAT	Factory Acceptance Test
FOT	Field operational test
FP	Field processor (for traffic signals) – uses STREAMS Connect software
GNSS	Global Navigation Satellite System
HDCP	High-Bandwidth Digital Content Protection
IEEE	Institute of Electrical and Electronic Engineers
IP	Ingress Protection
IPRT	Internet protocol remote telemetry (ITS network Telstra solution for TMR)
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
ITS	Intelligent transport systems
MAP	Cooperative ITS message, broadcasting geography/topology of intersection
MAPEM	MapData extended Message
MRTS	Main Roads' Technical Standards
NTRIP	Networked Transport of RTCM via Internet Protocol
NTU	Network terminal / termination unit
NZS	New Zealand Standard

Acronym	Term
PD	Power Devices
PoE	Power over Ethernet (IEEE802.3af)
PPP	Precise Point Positioning
PSE	Power Sourcing Equipment
PSTS	Project Specific Technical Specification
R-ITS-S	Roadside ITS station
RPEQ	Registered Professional Engineer of Queensland
RSU	Road side units
RTCM	Radio Technical Commission for Maritime Services
SCMS	Security credential management system
SIL	Safety Integrity Level
SIT	System Integration Test
SIAT	Site Integration Acceptance Test
SPATEM	Signal Phase and Timing Extended Message
TAI	International Atomic Time
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport layer security
TSC	Traffic Signal Controller
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
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.
C-ITS-F	Back-end C-ITS Facility including C-ITS-S (router and SCMS certificate addition), Maintenance tool, spatial service, integration and messaging engine, data capture system and logging service, and monitoring system.
C-ITS-F data logging service	A service provided by the C-ITS-F that is used to log data mainly for the FOT evaluation.
FOT	Field Operational Test – the period when the in-vehicle C-ITS systems are operational and logging data.
ITS-G5	Wireless Radio communications based on 802.11p and defined by ETSI EN 302 663:2013 Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz (5.9GHz) frequency band.

3 Reference Documents

The requirements of the referenced documents listed in Table 3-1 and Table 3-2 below apply to this specification.

Table 3-1 - Referenced documents – External

Document ID	Document Name / Description
ISO 14823 (2017-05)	Intelligent transport systems -- Graphic data dictionary
ISO 17419 (2018)	Intelligent transport systems — Cooperative systems — Globally unique identification
ISO/TS 19091 (2017)	Intelligent transport systems - Cooperative ITS - Using V2I and I2V communications for applications related to signalized intersections
ISO/TS 19321:2015 (2015-04)	Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures
ISO TS 3166-1 (2013)	Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes
ISO/IEC 20922:2016 (2016)	Information technology -- Message Queuing Telemetry Transport (MQTT) v3.1.1
SAE J2945/1 (2016)	On-Board System Requirements for V2V Safety Communications
SAE J2735 (2016)	Surface Vehicle Standard, Dedicated Short Range Communications (DSRC) Message Set Dictionary (SPAT,MAP)
ETSI EN 302 571 V2.1.1 (2017-02)	Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
ETSI EN 302 636-1	Vehicular Communications; GeoNetworking; Part 1: Requirements
ETSI EN 302 636-2	Vehicular Communications; GeoNetworking; Part 2: Scenarios
ETSI EN 302 636-3	Vehicular Communications; GeoNetworking; Part 3: Network Architecture
ETSI EN 302 663 V1.2.1 (2013-07)	ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band
ETSI EN 302 665 V1.1.1 (2010-09)	Intelligent Transport Systems (ITS); Communications Architecture
ETSI EN 302 890-2	Facilities Layer function; Part 2: Position and Time management (PoTi); Release 2
ETSI EN 302 931 V1.1.1 (2011-07)	Geographical Area Definition
ETSI TR 102 638 V1.1.1 (2009-06)	Vehicular Communications; Basic Set of Applications; Definitions
ETSI TS 101 539-1 V1.1.1 (2013-08)	Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification
ETSI TS 101 539-3 v1.1.1 (2013-11)	Intelligent Transport Systems (ITS); V2X Applications; Longitudinal Collision Warning (LCRW) application requirements specification
ETSI TS 102 894-1 V1.1.1	Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications
ETSI TS 102 894-2 V1.2.1 (2014-09)	Users and applications requirements; Part 2: Applications and facilities layer common data dictionary
ETSI TS102 941 V1.2.1(2018-05)	Intelligent Transport Systems (ITS) Security; Trust and Privacy Management
ETSI TS 103 301 V1.1.1 (2016-11)	Intelligent Transport Systems (ITS) – Vehicular Communications – Basic Set of Applications – Facilities layer protocols and communication requirements for I2V messages

Document ID	Document Name / Description
ETSI TR 103 415 V1.1.1 (2018-04)	Intelligent Transport Systems (ITS) ; Security; Pre-standardization study on pseudonym change management
ETSI EN 302 636-4-1 V1.3.1 (2017-08)	Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality
ETSI TS 102 636-4-2 V1.1.1 (2013-10)	Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5
ETSI TS 102 637-1 V1.1.1 (2010-09)	Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements
ETSI EN 302 636-5-1 2.1.1 (2017-05)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol
ETSI TS 102 687 V1.2.1 (2018-04)	Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part
ETSI TS 102 724 V1.1.1 (2012-10)	Harmonized Channel Specifications for Intelligent Transport Systems operating in the 5 GHz frequency band.
ETSI TS 102 731 V1.1.1 (2010-09)	Security; Security Services and Architecture
ETSI TS 102 792 V1.2.1 (2015-06)	Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range
ETSI TS 102 860 V1.1.1 (2011-05)	Classification and management of ITS application objects
ETSI TS 102 940 V1.3.1 (2018-04)	Security; ITS communications security Architecture and security management
ETSI TS 102 942 V1.1.1 (2012-06)	Security; Access Control
ETSI TS 102 943 V1.1.1 (2012-06)	Security; Confidentiality services
ETSI TS 102 965 V1.3.1 (2016-11)	Application Object Identifier (ITS - AID); Registration list.
ETSI TS 103 097 V1.3.1 (2017-10)	Intelligent Transport Systems (ITS); Security; Security header and certificate formats
ETSI TS 103 175 V1.1.1 (2015-06)	Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium
ETSI TS 103 248 V1.2.1 (2018-08)	GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP)
ETSI TS 103 600 V1.1.1 (2019-05)	Interoperability test specifications for security

Document ID	Document Name / Description
ETSI EN 302 637-3 V1.2.2 (2014-11)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service
ETSI EN 302 637-2 V1.3.2 (2014-11)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service
IEEE 1609.2:2017 (2A)	Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages
ISO/IEC 20922 v3.1.1 (2016)	Information technology -- Message Queuing Telemetry Transport (MQTT)
AS 1044 (1995)	Radio Disturbance characteristics
AS/NZS 17799 (2006)	Security techniques — Code of practice for information security management
AS/NZS 7799.2 (2003-02)	Information security management Specification for information security management systems
AS/NZS 3100 (2017)	General requirements for electrical equipment
AS 2578 (2009)	Traffic Signal Controllers
MRTS01 (2017)	Introduction to Technical Specifications
MRTS50 (2017)	Specific Quality System Requirements
MRTS97 (2017-07)	Mounting Structures for Roadside Equipment
IEEE 802.11 (2016)	Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
IEEE 802.15	Bluetooth Special Interest Group Bluetooth standard
RTCM Standard 10403.3 (2016-10)	Differential GNSS (Global Navigation Satellite Systems) Services – version 3:2016
ACMA Radio communications (Intelligent Transport Systems) Class Licence 2017	

Table 3-2 - Referenced documents – Internal

Document ID	Document Name / Description
PSTS006	Data Entity Catalogue
PSTS007	C-ITS Station Protocol Specification
PSTS008	SCMS Certificate Profile Specification
PSTS013	Advanced Red Light Warning
PSTS014	Turning Warning - Vulnerable Road user
TMRD18	Master Test Plan and Report from ICVP

4 Quality System Requirements

Quality system requirements shall be in accordance with this Technical Specification and the requirements of the Contract (including the requirements of MRTS01:2017 and MRTS50:2017).

4.1 Testing and Commissioning

TMRD18 Master Test Plan and Report describes the testing and commissioning requirements and their outcomes for ICVP, examining all project components, interdependencies and interoperability.

The R-ITS-S is one component within the broader C-ITS implementation and, as such, the rigorous device, integration and field testing were conducted prior to ICVP's C-ITS deployment.

4.1.1 Testing Methodology

There are three broad stages with which testing focus and activities align:

1. Development stages, as per the R-ITS-S planning, design and development activities,
2. Integration of system components, and
3. Installation and testing of the equipment at the Mt Cotton and Ipswich sites.

Integration testing consists of several test cycles in which the entire solution is tested.

The device vendor collaboratively developed testing documentation and assist with commissioning on-site. Specific objectives, entry/exit criteria for each phase of testing and test environment requirements and responsibilities are detailed in Master Test Plans.

4.1.2 Testing Activities

The R-ITS-S shall undertake the test types listed in Table 4-1.

Table 4-1 - R-ITS-S Tests

Test Type	Description
Development testing	Incremental testing by vendor throughout development process – may engage TMR for verification of requirement achieved
Factory Acceptance Test (FAT)	R-ITS-S functionality against requirements. Other interactions may be emulated, or demonstrable against a suitable test harness – the Principal to approve FAT document, and to witness the FAT as performed by the device vendor

Test Type	Description
Component Integration Test (CIT) – Bench	Per-unit integration with full system, including interfaces to C-ITS stations, operating on a bench with simulated data but actual functions – device vendor to co-author with others; Principal to approve
Component Integration Test – R-ITS-S and STREAMS® Connect – TSC (Bench)	Integration of STREAMS® Connect with R-ITS-S, on test bench with Traffic Signal Controller, to establish correct operations.
System Integration Test (SIT) – Bench	System satisfies C-ITS Specifications, operating end-to-end on a bench with integrated units, actual functions, and external data sources and outputs – device vendor to co-author with others; Principal to approve
Installation Acceptance Checklists	<p>Installers, device vendors and TMR asset owners will collaborate, test and implement a repeatable install procedure for equipment. Installation shall proceed based on successful passing of hold points to-date.</p> <p>An installation acceptance checklist shall be performed for each R-ITS-S. The installation acceptance checklist shall confirm that each R-ITS-S functions when installed on site based on basic in-situ tests.</p>
Commissioning Test	A Commissioning test of each installed R-ITS-S for correct integration will be performed after physical Installation Acceptance checks have passed, and prior to a R-ITS-S becoming part of the C-ITS environment – Principal to approve
Site Integration Acceptance Test (Mt Cotton)	Integration in off-road, real-world environment at Mt Cotton, and testing of all system functions, with a limited rollout of units – Principal to approve
Site Integration Acceptance Test (Ipswich)	Integration in on-road environment at Ipswich, and testing of all system functions, with a larger sample of units rolled out than at Mt Cotton – Principal to approve
Maintenance Tests	Ad hoc testing of fixes prior to being rolled out to operational stations – as needed, and ongoing

5 System Requirements

5.1 C-ITS Architecture

The R-ITS-S is a component of the broader C-ITS architecture as shown in Figure 5.1.

For ICVP, the R-ITS-S are installed at traffic signal intersections to relay intersection safety messages such as for the Advanced Red Light Warning (ARLW) and Turning Warning Vulnerable Road User (TWVR) use cases.

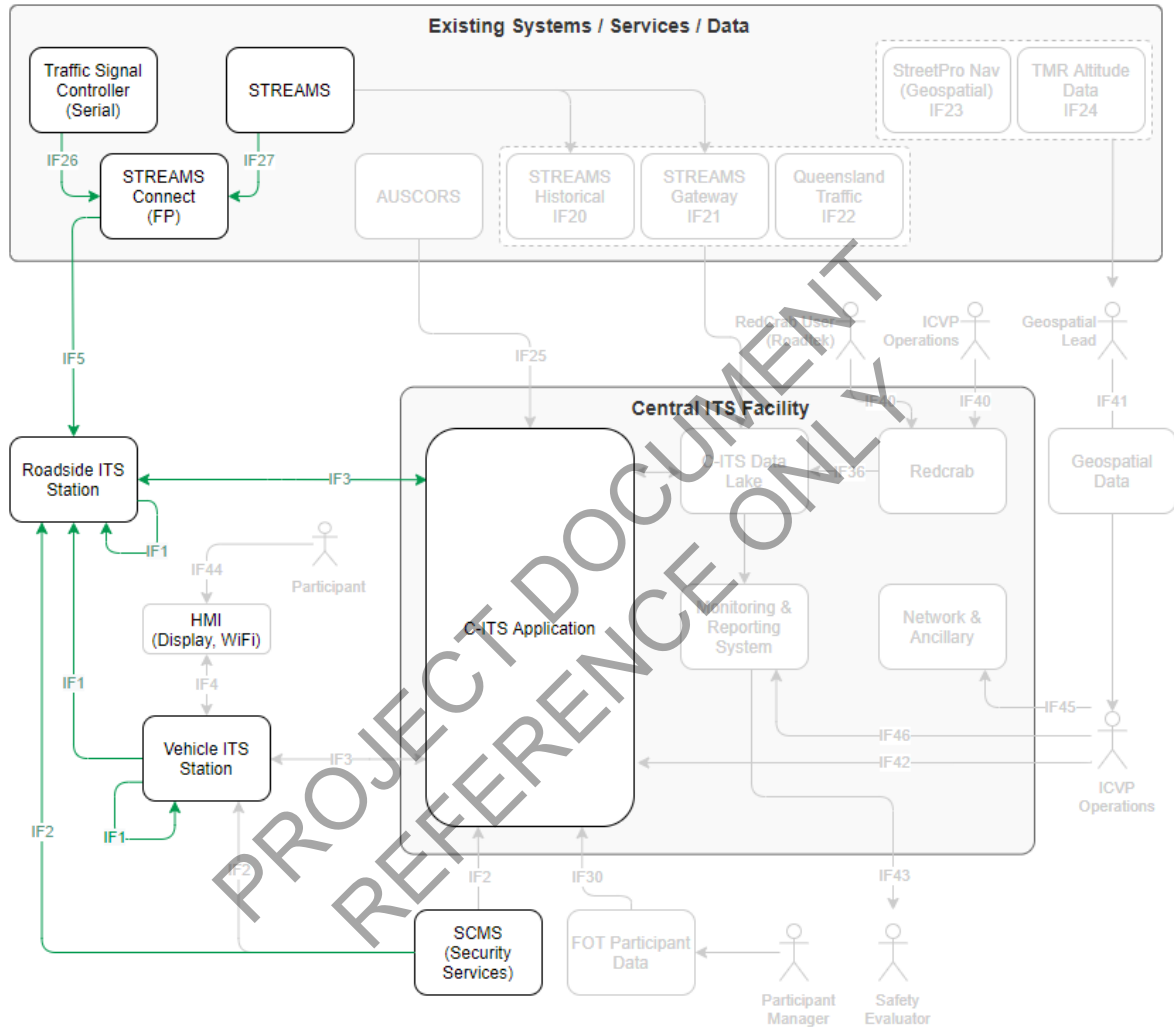


Figure 5.1 - C-ITS architecture

Table 5-1 presents the main interfaces of R-ITS-S in the C-ITS Pilot.

Table 5-1 - C-ITS Pilot system interfaces for R-ITS-S

Interface	Description	Interface Type
C-ITS communications		
IF1	V-ITS-S ↔ R-ITS-S ↔ V-ITS-S	ITS-G5 (DSRC)
IF2	SCMS → C/R/V-ITS-S	HTTPS (Internet)
IF3	C-ITS-F ↔ R/V-ITS-S	MQTT, HTTPS
IF5	FP → R-ITS-S	UDP (Ethernet)
Existing Systems / Services /Data		
IF26	TSC ↔ FP	Serial
IF27	STREAMS® → STREAMS® Connect	HTTPS (ITS network)

5.2 R-ITS-S Architecture

The R-ITS-S reference architecture has been adopted from ETSI EN 302 665 (v1.1.1 2010-09) and outlines the functionality contained within the R-ITS-S equipment. The architecture follows the principles of the Open Systems Interconnection (OSI) model for layered communication protocols. Figure 5.2 shows how the subsections of this specification apply to the R-ITS-S reference architecture.

The elements contained within the architecture as per ETSI EN 302 665:2010 are summarised below:

- "Access" representing R-ITS-S communication OSI layers 1 and 2 which includes interfaces as defined in Table 5-2.
- "Networking & Transport" representing OSI layers 3 and 4 with protocols as described in Table 5-2 .
- "Facilities" representing OSI layers 5, 6 and 7. This includes facilities required to support communications, operational requirements, applications, management and security functions on the R-ITS-S as described in Table 5-2.
- "Applications" representing the applications required by the R-ITS-S. Refer to Section 6 for further information on required applications
- "Management" representing management functions required by the R-ITS-S. Refer to Section 6.1.4.4 for further information on required management functions.
- "Security" provides security services to the OSI communication protocol stack, to the security entity and to the management entity. Refer to Section 7 for further information on required security requirements.

Requirement: The R-ITS-S shall implement all functions as defined in the reference architecture presented in Figure 5.2.

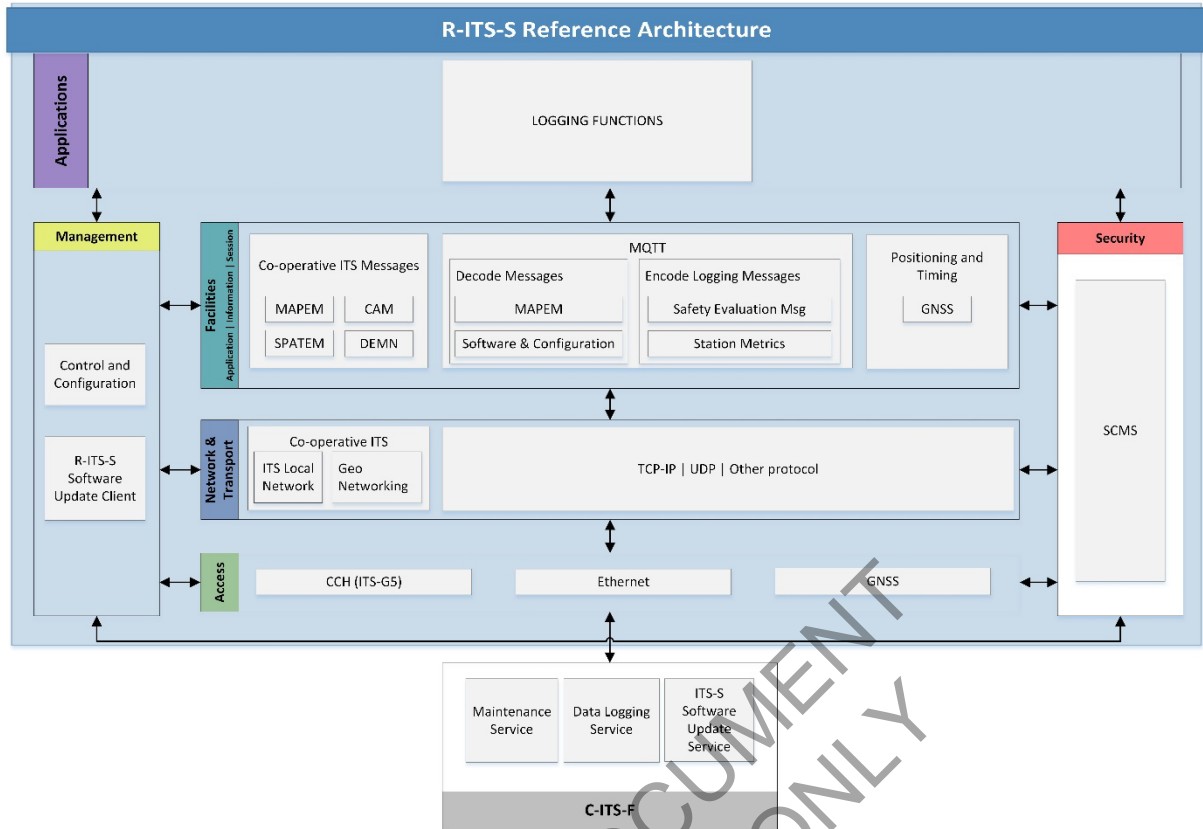


Figure 5.2 - R-ITS-S Reference Architecture (adapted from ETSI EN 302 665:2010)

The interfaces along with the communication methods, networking and transport requirements are listed below in Table 5-2.

Table 5-2 - Communication Methods

Interfaces	Access	Networking and Transport	Facilities Required
R-ITS-S to V-ITS-S (IF4)	ITS-G5	Geonetworking, BTP	Message Support (section 5.3.1)
R-ITS-S to SCMS (IF2)	Ethernet	TCP/IP, IPv4	Interface to the security layer
R-ITS-S to C-ITS-F (IF3)			Session and Communication Management (section 5.4.1), Message Support (section 5.4.2)
Field Processor to R-ITS-S (IF8)		UDP	Message Support
R-ITS-S to GNSS	Global Navigation Satellite System		Station position and timing

5.3 ITS-G5 Communications (Interface IF4)

The following section details the access, networking, transport and facilities requirements for ITS-G5.

Requirement: ITS-G5 communications shall be in accordance with the requirements of ETSI EN 302 663:2013, ETSI EN 302 571:2017 and the ACMA Radio communications (Intelligent Transport Systems) Class Licence 2017 and shall use the IEEE channel 180 or ITS-G5A control channel.

Requirement: The R-ITS-S transmit power shall be adjustable to a maximum Equivalent Isotropically Radiated Power (EIRP) of 23 dBm/MHz.

Requirement: Geonetworking and BTP shall be used for communications between V-ITS-S and R-ITS-S in accordance with ETSI EN 302 636-5-1:2017 and ETSI EN 302 636-4:2017.

Requirement: All messages between stations using ITS-G5 shall be signed in accordance with the security requirements of Section 7.

Requirement: ITS-G5 communications shall apply Decentralized Congestion Control (DCC) mechanisms in accordance with ETSI TS 102 687:2018.

Requirement: The R-ITS-S shall have system resources for operating with the following minimum performance:

- Transmit a minimum 20 signed ITS-G5 messages per second
- Processing of min. 220 received signed ITS-G5 messages per second

5.3.1 Message Support

Requirement: The R-ITS-S shall provide support for the following messages:

Table 5-3 - R-ITS-S supported message types

R-ITS-S Facility	Detail
Signal Phase and Timing Extended Message (SPATEM)	Receive SPATEM from FP via ethernet then broadcast the SPATEM via ITS-G5 to V-ITS-S at 100ms intervals and log each instance. In accordance with ETSI TS 103 301:2016
MAP Extended Message (MAPEM)	Receive MAPEM updates from C-ITS-F via cellular then broadcast stored latest MAPEM via ITS-G5 to V-ITS-S at 500ms intervals and log each instance. In accordance with ETSI TS 103 301:2016
Co-operative Awareness Messages (CAM)	Receive CAMs from V-ITS-S via ITS-G5 and log each instance. In accordance with ETSI EN 302 637-2:2014
Decentralized Environmental Notification Messages (DENM)	R-ITS-S does not receive or transmit DENM from any other station in ICVP. However, it should be able to in accordance with ETSI EN 302 637-3:2014.

Requirement: The R-ITS-S shall adopt the data element descriptions of the *Message Data Entity Catalogue PSTS006* which details each of the message types outlined in Table 5-3. If conflicting or competing definitions are identified between the *Message Data Entity Catalogue PSTS006* and the relevant Standard, the Contractor shall notify the Principal.

5.4 Ethernet (Interface IF2, IF3 and IF5)

Traffic signal information is processed by the FP and transformed into an UPER encoded SPATEM which is then sent to the R-ITS-S using UDP. The R-ITS-S timestamps, signs and broadcasts SPATEM received from the FP to surrounding V-ITS-S. The Ethernet port in the R-ITS-S is also used for energising the R-ITS-S via Power-over Ethernet (PoE or PoE+).

Requirement: Any communication from R-ITS-S to the FP IP address shall not be permitted.

Requirement: The R-ITS-S shall include an Ethernet (RJ45) port that supports PoE or PoE+.

Requirement: The R-ITS-S shall synchronise all messages including SPATEM and MAPEM with TAI time.

Requirement: Communication between the R-ITS-S and the SCMS shall be in accordance with *C-ITS Station Protocol Specification PSTS007* and *Station Certificate Profile Specification PSTS008*.

Requirement: TCP/IP, IPv4 shall be used for communications between the C-ITS-F and the R-ITS-S equipment.

5.4.1 Session and Communication Management

Requirement: Message Queuing Telemetry Transport (MQTT) publish / subscribe protocol shall be utilised to establish the client / broker connection for communications between the R-ITS-S and the C-ITS-F. This shall be undertaken in accordance with the requirements of *C-ITS Station Protocol Specification PSTS007* and ISO/IEC 20922:2016.

5.4.1.1 Decoding and Encoding Messages

Messages received via MQTT are decoded for use by R-ITS-S functions. These include MAPEM, software updates and configuration data. Messages to be sent by the R-ITS-S to the C-ITS-F via MQTT are encoded and grouped. These include the logging functions as detailed in Section 6.

Requirement: The R-ITS-S shall provide the required facilities to decode and encode MQTT messages for use by application, management and security functions of the R-ITS-S in accordance with the *C-ITS Station Protocol Specification PSTS007*.

5.4.2 Message Support

Requirement: The R-ITS-S shall support for the following messages as summarised in Table 5-4.

Table 5-4 - R-ITS-S supported message types

Message Name	Payload	Relevant ASN	Details
Station Configuration (SCM)	UPER encoded <i>asn.1 schema</i>	<i>stationConfiguration.asn</i>	Used to deliver station specific configuration information to the R-ITS-S.
Station Platform (SPM)	UPER encoded <i>asn.1 schema</i>	<i>stationPlatformData.asn</i>	Heartbeat message from R-ITS-S. Used for session tracking, platform-level events and error logging.
Safety Evaluation (CSEM)	UPER encoded <i>asn.1 schema</i>	<i>safetyEvaluationData.asn</i>	Captures C-ITS messages published and received by all stations including: Received and transmitted DENM, SPATEM, MAPEM and CAM as per section 6.1.
Signed C-ITS Message	TS 103 097 v1.3.1 with TMR modifications. Includes signature and UPER encoded C-ITS message payload	N/A	MAPEM

5.5 GNSS

5.5.1 R-ITS-S Positioning

Requirement: The R-ITS-S shall store a manually configurable reference position.

Requirement: The R-ITS-S shall maintain a GNSS location for placement verification.

5.5.2 Timing and Synchronisation

Requirement: R-ITS-S shall be synchronised to Coordinated Universal Time (UTC) using GNSS and shall be accurate to within 10ms.

Requirement: R-ITS-S shall maintain a system clock based on timing information from the local GNSS receiver that manages leap second corrections.

Requirement: R-ITS-S shall log an error if the deviation between GNSS time and FP time has exceeded *spatSourceTimeDiffThreshold* (default 300ms).

6 Operational Requirements (Applications)

6.1 Data Logging

Requirement: Data logging shall commence as soon as R-ITS-S has powered-up and initialised and continue as long as the R-ITS-S is turned on.

Requirement: The R-ITS-S shall log C-ITS Safety Evaluation Messages as described in *C-ITS Station Protocol Specification PSTS007*, and *Data Entity Catalogue PSTS006*.

Requirement: The R-ITS-S shall be capable of individually enabling/disabling the logging of the following data:

1. SPATEM data using *spatemDirection* (received messages from FP communications and ITS-G5 transmitted messages)
2. MAPEM data using *mapemDirection* (received messages from C-ITS-F communications and ITS-G5 transmitted messages)
3. CAM data using *camDirection* (ITS-G5 received messages)
4. DENM data using *denmDirection* (ITS-G5 received messages)

Requirement: The R-ITS-S shall log C-ITS Station Platform Messages as described in *C-ITS Station Protocol Specification PSTS007*, and *Data Entity Catalogue PSTS006*.

Requirement: *Safety Evaluation Data* shall be sent by the R-ITS-S to the C-ITS-F when the respective message count limit is reached (*csemCamLogLimit*, *csemDenmLogLimit*, *csemMapemLogLimit* or *csemSpatemLogLimit*) or at the rate specified by the parameter *csemLogWatchdogTimeout* if the respective count is not reached. Parameters are as specified in *Station Configuration Message*.

Requirement: *Station Platform Data* shall be sent by the R-ITS-S to the C-ITS-F at the rate specified by the parameter *logFrequency* as specified in *Station Configuration Message*.

Requirement: R-ITS-S data logging shall not interfere with the sending and receipt of C-ITS messages via ITS-G5 and Ethernet.

6.1.1 Data Logging Security

Requirement: Data log messages shall not be signed (as described in section 7), however, messages shall be encrypted using TLS as described in as described in the *C-ITS Station Protocol Specification PSTS007*.

6.1.2 Log Data Retention

Requirement: The R-ITS-S shall retain a store of logged data that has not been uploaded to the C-ITS-F logging service for the period specified by the *logMessageRetentionWindow* data element in the *Safety Evaluation* data. The stored data shall persist over power cycles. When communication is restored, the R-ITS-S shall send data logs to the C-ITS-F logging service. Logged data shall be retained for *Safety Evaluation Data* and *Station Platform Data*.

Requirement: Data logs sent to the C-ITS-F logging service and confirmed shall not be re-uploaded to the C-ITS-F. Any data logs uploaded to the C-ITS-F may be removed from the station (consideration should be given for local diagnostics and testing functions). Data logs are considered to have been confirmed if they are included in the count of messages.

6.1.3 Safety Evaluation Data Logging

Safety Evaluation data logging is an application that executes the capture, encoding and transmission functions for C-ITS messages published and received by all individual stations.

Requirement: The R-ITS-S shall capture the receipt and transmission of all C-ITS *Safety Evaluation* Messages per the logging frequencies described in Table 6-1.

Table 6-1 - C-ITS message logging frequency







Type	Direction	Logging frequency
CAM	Received	At receipt rate
DENM	Received	At receipt rate
MAPEM	Transmitted	At broadcast rate
	Received	At receipt rate
SPATEM	Transmitted	At broadcast rate
	Received	At receipt rate

To allow the management of logging bandwidth the collection of message content shall be controlled per C-ITS message type. The control parameters are *camDirection*, *denmDirection*, *mapemDirection* and *spatemDirection*.

Requirement: When data logging is enabled the R-ITS-S shall collect both a count of *messageType* (e.g. *denm*) received and transmitted per station and the UPER encoded messages. When data logging is disabled then only a count of message type received and transmitted per station per log period is collected. Data logging shall be controlled for both receipt and transmission. Messages that fail to be signed or verified successfully shall be logged as *secfail*. Messages that fail to be encoded or decoded successfully shall be logged as *unknown*.

6.1.3.1 Data Definition

Figure 6.1 describes the overview of the C-ITS Safety Evaluation Message (CSEM). Details are specified in *C-ITS Station Protocol Specification* document *PSTS007*, and *Data Entity Catalogue* *PSTS006*. The message structure identifies the following data components:

1.  CAVI CSEM PDU container
2.  Message set
3.  Data frame
4.  Sequence of data frame
5.  Data element
6.  Not used

Requirement: The Safety Evaluation data shall be encoded in accordance with *safetyEvaluation.asn* protocol.

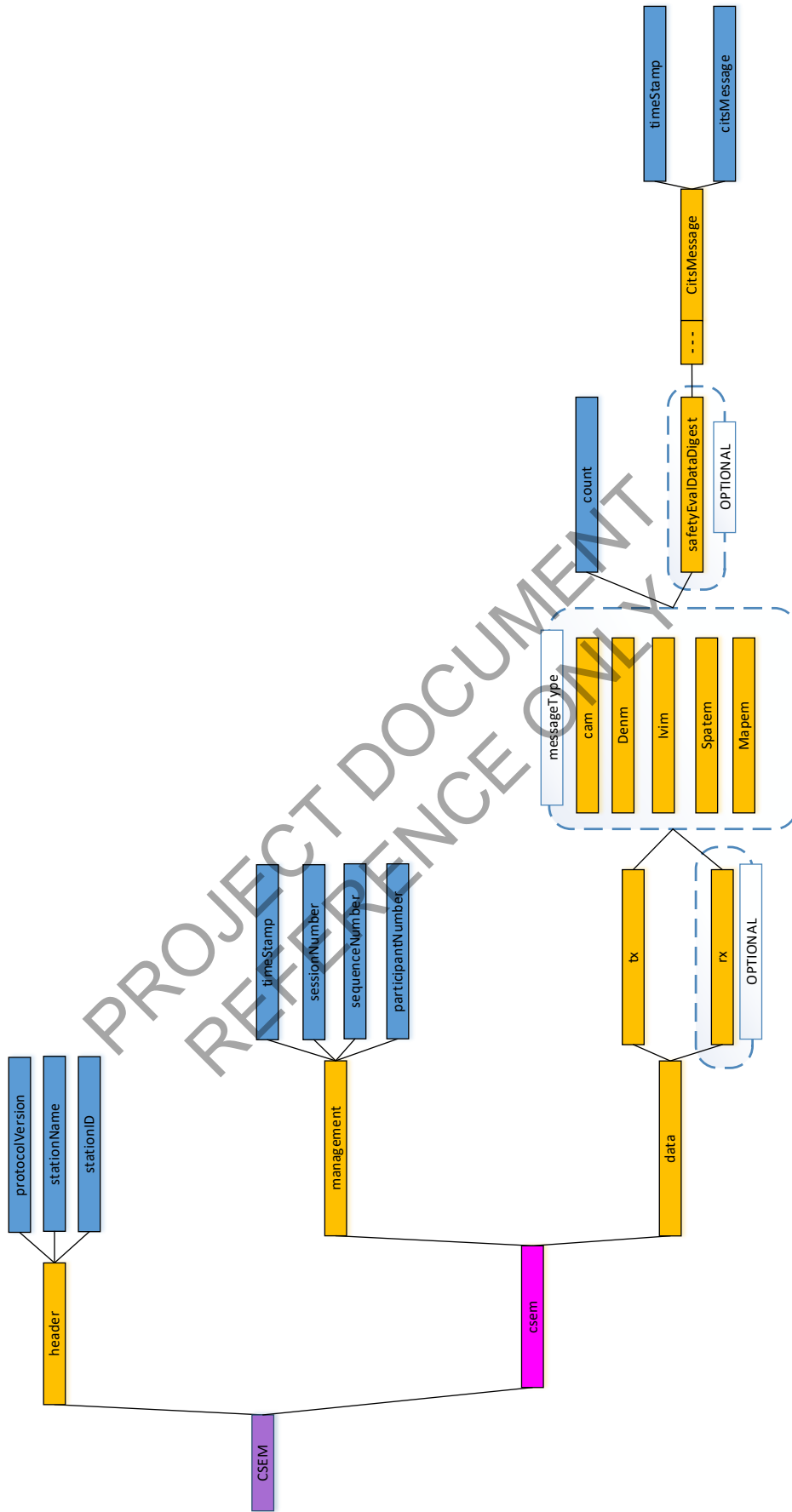


Figure 6.1 – CSEM Structure

6.1.4 Station Platform Data Logging

Station Platform data is used by the C-ITS-F manager to monitor the operation of the system.

Requirement: Platform-level data shall include:

- Session monitoring - used to identify a R-ITS-S session and to detect session exceptions
- Platform metrics - monitors station performance
- Platform exception/ error logs - captures the station failures.

6.1.4.1 Session Monitoring

Session monitoring is the measurement of a MQTT session. The attributes of this data frame include measuring the station availability and communications outages.

Requirement: The Platform data shall log MQTT session information (section 5.4.1) and associated roadside metrics.

6.1.4.2 Platform Metrics

Platform metrics are used to monitor station performance and to diagnose and rectify system exceptions so that the collection of data for the safety evaluation remains optimal.

Requirement: The Platform data shall log station metrics in accordance with the metrics defined in Table 6-2.

Table 6-2 – Platform metrics

Metric	Value	Threshold	Notes
numberProcessingUnits	Count		
cpuOneMinuteLoadAverage	Decimal	# cores * 3	Uses the 1-minute average value collected at message generation time
cpuTemperature	Decimal	-	Uses the value collected at message generation time (CPPU temp or board temp)
storageInUse	%	<i>storageThreshold</i>	For all disks or partitions including memory resident storage
gnssHdopErrorCount	Count	<i>dopThreshold</i>	
gnssPdopErrorCount	Count	<i>dopThreshold</i>	
gnssVdopErrorCount	Count	<i>dopThreshold</i>	
gnssSatelliteErrorCount	Count	<i>minNumberOfSatellitesThreshold</i>	
networkInterfaceError	Count	Unavailable	sum of RX and TX interface errors per interface. Always ordered in incrementing interface number. Do not include local loopback
freePhysicalMemory	%	-	Uses the values collected at message generation time

Metric	Value	Threshold	Notes
systemUptime	Minutes	-	Uses the value collected at message generation time
messageSignatureErrorCount	Count	Any	Uses the values collected at message generation time
gnssNoSyncTime	Count	Any	Count maintained and reported at each report interval
fpRitssTimeSyncErrorCount	Count	300ms	the deviation between GNSS time and FP time has exceeded 300ms
citsMessageDecodeErrorCount	Count	Any	Count maintained and reported at each report interval

6.1.4.3 Platform Error Logs






Platform error logs capture the failures identified through this specification (e.g. platform metrics warnings) and Contractor defined errors. This allows fast response time to the diagnosis and rectification of system errors so that data collection for the safety evaluation remains optimal.

Requirement: The error log shall support errors logged by any level of the system (i.e. hardware, platform access, transport and network, facilities, application).

Requirement: The R-ITS-S limits the size of these logs (within a 4 stage severity level system) so that network bandwidth and data rates are managed.

6.1.4.4 Data Definition

Figure 6.2 describes the overview of the *C-ITS Station Platform Message* (CSPM). Details are specified in *C-ITS Station Protocol Specification* document PSTS007, and *Data Entity Catalogue* PSTS006. The message structure identifies the following data components:

1.  CSPM PDU container
2.  Message set
3.  Data frame
4.  Sequence of data frame
5.  Data element

Requirement: The *Station Platform* data shall be encoded in accordance with *stationPlatformData.asn* protocol.

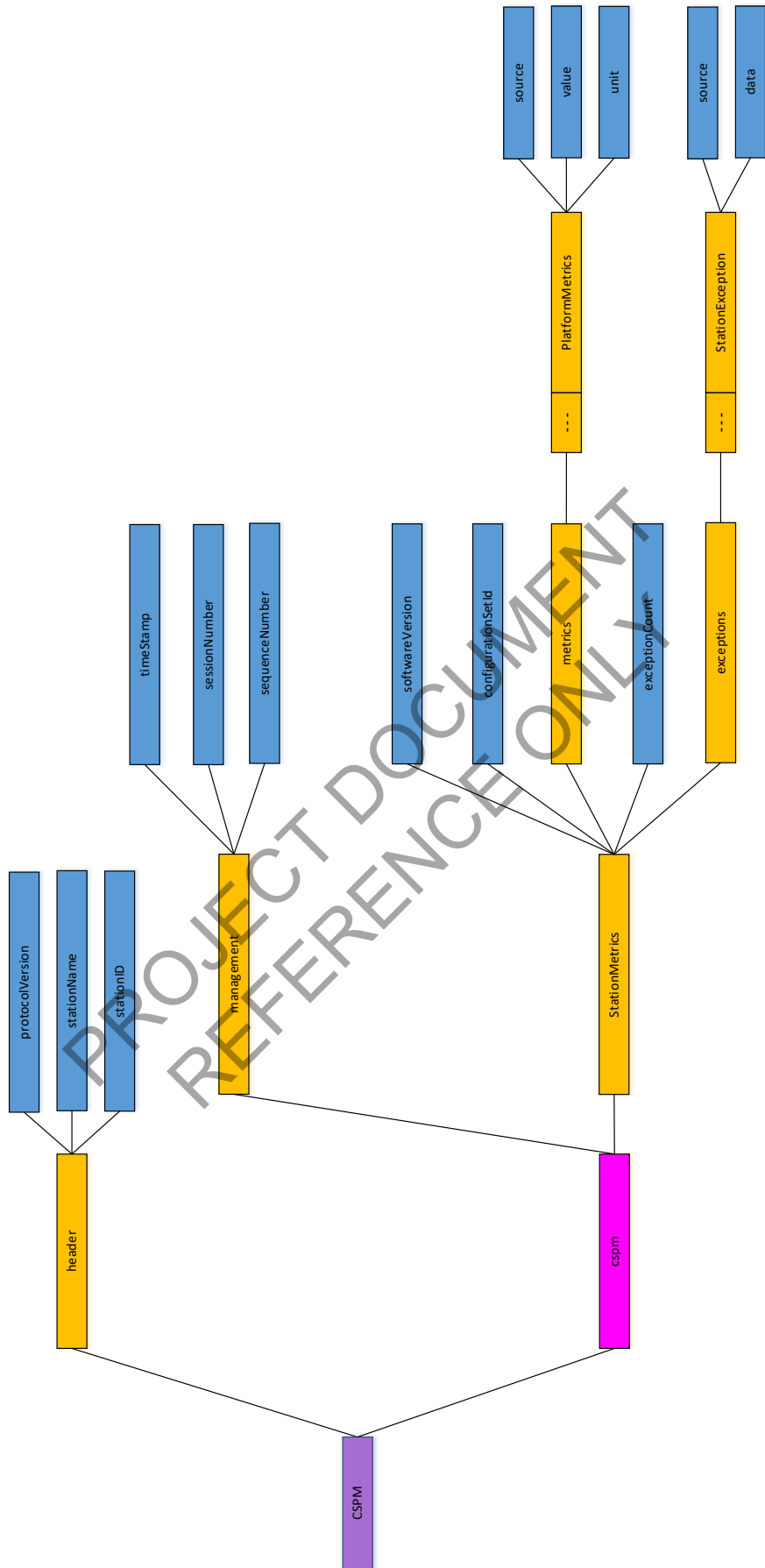


Figure 6.2 - SPM Data Structure Management

The management entity of the R-ITS-S is shown in the reference architecture as shown in Figure 5.2 and is defined in Section 7 of ETSI EN 302 665:2010.

Requirement: The functionality of the R-ITS-S management entity shall be implemented as defined in the reference architecture as shown in Figure 5.1.

6.2 Control and Configuration

R-ITS-S configuration is retrieved from the C-ITS-F as specified in the *C-ITS Station Protocol Specification PSTS007*, and *Data Entity Catalogue PSTS006*.

The *Station Configuration Message*, *stationConfiguration.asn*, forms the protocol specification that describes the configuration message. Key configurable parameters are outlined below. Section 12 contains further information on key configurable parameters and should be referenced for further information.

- Control of the ITS-G5 message forwarding application running on the R-ITS-S.
- C-ITS platform configuration
- Heartbeat message transmission rate. See parameter *logFrequency* in section 12.

Requirement: The R-ITS-S shall implement changes contained in control and configuration requests when received and ensure that the platform and application begin using the control and configuration parameters. System or application components may need to be restarted after the receipt of a control and configuration request.

Requirement: The full set of configuration items for R-ITS-S will be sent in one message as described in the *C-ITS Station Protocol Specification PSTS007* and *Data Entity Catalogue PSTS006*. Each set of configuration parameters (*stationParametersVersion* and *systemParametersVersion*) for a station will be given a unique identifier. The R-ITS-S shall store this unique identifier so that it can be included in platform-level messages sent to the C-ITS-F.

Requirement: The R-ITS-S shall subscribe to a configuration topic unique to the station and maintain the subscription. A new configuration set will be published to the station when it makes a subscription. A new configuration may be published by the C-ITS-F at any time whilst that the station is subscribed which the R-ITS-S should implement without requirement for a restart.

6.3 R-ITS-S Software Update Client

The C-ITS will implement one or more industry-standard package management systems to support the update of the following software categories on R-ITS-S:

- Security updates – to meet TMR information security requirements. These updates are related to the correction of security vulnerabilities
- Platform packages.

Requirement: The package management system shall be proposed by the R-ITS-S vendor and approved by the Principal to support software updates.

Requirement: Packages shall be prepared by R-ITS-S vendors. Packages shall be applied and become active without user intervention. If a package requires the system configuration to be modified to become active then the configuration change shall be included in the package.

Requirement: The R-ITS-S shall connect to the package management system using the update-system's native process.

Requirement: The R-ITS-S shall recover with a previous software version if there is a removal of power during the download or installation of software updates.

Requirement: The delivery of software packages shall use Ethernet with consideration of batching to multiple R-ITS-S.

6.4 Remote Maintenance

Limited information will be logged in the maintenance portal. This level of information will unlikely allow low-level diagnosis of issues. Vendor specific diagnostic tools will be used by accessing the stations remotely using a secure connection (e.g. SSH).

Requirement: R-ITS-S shall have a facility to allow remote maintenance access. This includes access to information in regard to the station operation, status, communication channels or other relevant system information required for diagnostics.

Requirement: The R-ITS-S remote maintenance facility shall provide information back to the C-ITS-F in accordance with configuration parameter *spmExceptionLoggingLevel* as defined in Section 12.

Requirement: Additional remote maintenance activities shall be undertaken using vendor specific tools via secure remote connection (eg. SSH protocol) and through the access controlled C-ITS-F service.

7 Security

The security entity of the R-ITS-S is as shown in the reference architecture in Figure 5.2 and is defined in Section 8 of ETSI EN 302 665:2010. Additional security requirements are defined in *C-ITS Station Protocol Specification PSTS007*.

Only R-ITS-S installed by the C-ITS can participate in the trial. Each station must be verified before being allowed to interact with other ITS stations.

V2I interactions will be managed using processes specified by the *SCMS Certificate Profile Specification PSTS008*. The C-ITS-F will verify that the R-ITS-S is a C-ITS trusted station. For this purposes stations must be enrolled before they can participate in V2I interactions.

Requirement: The R-ITS-S shall facilitate field station enrolment in accordance with *SCMS Certificate Policy PSTS008* and *C-ITS Station Protocol Specification PSTS007*.

Requirement: The R-ITS-S shall be capable of enabling or disabling the SCMS security such as signing of messages (*securityEnable* in *Station Configuration Message*)

Requirement: All station interface messaging to SCMS components shall adhere to ETSI TS 102 941:2018 v1.2.1 using a certificate format as defined in ETSI TS 103 097 v1.3.1. Connection to the SCMS shall comply with the *C-ITS Station Protocol Specification PSTS007*.

7.1 Network Security Certificates

Requirement: A SCMS shall be utilised by all C-ITS stations and details are provided in the *C-ITS Station Protocol PSTS007* and *SCMS Certificate Profile Specification PSTS008*.

Requirement: The roadside station must encrypt all MQTT traffic using the provided X.509 certificates to establish TLS.

7.2 Station Lifecycle

ETSI TS 102 941 v1.2.1 defines a station lifecycle, however, does not specify the timeframes that this lifecycle will occur over. The following set of requirements specify these timeframes.

7.2.1 Manufacture

Requirement: SCMS network addresses shall be incorporated into the R-ITS-S as provided to the R-ITS-S vendor by the Principal.

Requirement: Public Key Certificates for the Root Certification Authority (Root CA certificate), the Enrolment Authority (EA CA certificate) and the Authentication Authority (AA CA certificate), shall be incorporated into the R-ITS-S as provided to the R-ITS-S vendor by the Principal.

Requirement: The globally unique, canonical identifiers for ITS-S shall be incorporated into the R-ITS-S as provided to the R-ITS-S vendor by the Principal.

Requirement: Permissions within the *SCMS Certificate Profile PSTS008* shall be adhered to.

7.2.2 Enrolment

Requirement: Enrolment shall take place prior to the station being deployed to the field. Enrolment certificates shall be set to expire in 5 years.

7.2.3 Authorisation

Refer to *Station Certificate Profile PSTS008* for station authorisation requirements.

7.2.4 Message Signing and Verification

Requirement: All ETSI defined messages shall be signed at transmit source and verified on receipt. This shall occur in accordance with the ETSI certificate format ETSI TS 103 097 v1.3.1. Messages that are unsigned or contain an invalid certificate (including an expired certificate) shall be ignored by the station.

7.2.5 Pre-Installation Configuration

Requirement: Prior to installation the R-ITS-S shall be configured with required SCMS tickets and the initial connection endpoint. This will be verified through a pre-commissioning test.

8 Technical Requirements

8.1 System Start-Up

Requirement: In order to facilitate fast and accurate timing and synchronisation a battery backed real time clock shall be provided in addition to the requirements of Section 5.5.2.

Requirement: The R-ITS-S shall subscribe to the following MQTT topics at the start of each session and whenever a reconnection is made.

- a. <stationName>/signedCitsMessageR
- b. <stationName>/stationConfiguration.

8.2 Storage

Requirement: The R-ITS-S shall have non-volatile memory to store all information required to meet the operational and technical requirements.

8.3 Maintenance Communications

Requirement: Additional to the ability to perform remote maintenance as defined in Section 6.4, the R-ITS-S shall be capable of local maintenance and configuration activities by SSH.

8.4 Control/Diagnostic Software

Requirement: The R-ITS-S vendor shall provide the Principal with control and diagnostic software required for the R-ITS-S and associated equipment.

Requirement: All software shall be licensed on behalf of, and in the name of, the Principal.

8.5 Failure Modes

Requirement: The R-ITS-S vendor and Principal shall agree on what constitutes critical failures and minor failures.

Requirement: In the event of critical failures, the R-ITS-S equipment shall:

- Return failures as part of the error log in the *Station Platform Data*. If the failure is an operational and/or telecommunications failure, the R-ITS-S shall continue all background data logging functions for upload back to the C-ITS-F when the interface communication link is re-established.
- Monitor the failure and automatically recover if possible.
- If failure requires a restart, automatically shut down in a safe manner maintaining any stored data.

8.6 Radio Performance

Requirement: The R-ITS-S equipment shall provide ITS-G5 communications of a high probability of transmission success over 300 meters line of sight and under typical intersection conditions. ITS-G5 communication performance shall be tested and subject to the approval of the Principal.

9 Electrical Requirements

9.1 General

Requirement: All electrical equipment shall comply with the requirements of AS3100:2017.

9.2 Powering R-ITS-S

Requirement: The R-ITS-S shall be powered by PoE or PoE+ in accordance with IEEE 802.3af or IEEE 802.at.

9.3 Surge Protection

Requirement: Each R-ITS-S shall be protected from surge damage of mains power supply and/or induced by lightning strikes and shall comply with the requirements of AS/NZS 1768:2007.

10 Mechanical and Physical Requirements

10.1 Environmental Conditions

Requirement: The equipment shall be capable of continuous, normal operation in the conditions described below:

- installed directly in sunlight
- ambient air temperature range between -5°C and 50°C
- maximum wind conditions likely to occur at the installation Site in accordance with AS4055:2012 wind category classifications
- Queensland coastal environment with salt deposit densities in the range of 2.0 to 3.0 g/m^2
- varied light intensity due to shadows
- a relative humidity of up to 95% non-condensing over the temperature range of 4.4°C to 43.3°C
- conditions, both permanent and temporary, that may be unique to the specified location, for example instances of thick smoke and electromagnetic interference, and
- vibrations reasonably expected in the installed location

Equipment operation shall cause no adverse effect on the surrounding environment in which it is installed. Likewise, Equipment shall not be affected by adverse environmental conditions expected at the intended installation location.

10.2 R-ITS-S Enclosure

Requirement: The R-ITS-S housing shall comply with the following general requirements:

- each R-ITS-S shall be enclosed in a weatherproof housing rated for at least IP66
- the housing shall be corrosion resistant in construction
- coatings and fittings shall tolerate exposure to salt atmosphere and motor vehicle fumes
- the R-ITS-S housing design shall maintain the ambient environment inside the housing to within the rated operating conditions of the equipment, in all weather conditions and ambient temperatures likely to be experienced in the installed location
- the layout of the equipment shall maximise the cooling capabilities
- exterior surface colour shall not distract drivers' attention
- Maximum physical dimensions of 300mm x 220mm x 90mm (not including antenna)
- Maximum weight of R-ITS-S of 4 kg (not including mounting bracket).

10.3 R-ITS-S Mounting Brackets

The mounting structure is to be provided by the Principal. The mounting bracket for attaching the R-ITS-S to the mounting structure will be provided by the Contractor.

Requirement: The R-ITS-S mounting bracket shall be able to be fastened securely on a 70~170mm diameter circular or square stainless steel pole.

Requirement: The mounting bracket must be manufactured from a durable resilient material and be stiffened where necessary to resist distortion due to wind and extreme temperatures and prevent the R-ITS-S coming loose and/or detaching.

Requirement: Similar to other Roadside ITS Equipment, the mounting brackets for R-ITS-S shall comply with *MRTS97 Mounting Structures for Roadside Equipment*.

Requirement: The following information shall be submitted to verify that the mounting bracket meets the requirements of *MRTS97 Mounting Structures for Roadside Equipment*.

- RPEQ Engineering drawings and calculations of the mounting bracket and any associated equipment
- if a GNSS antenna is mounted separately to the R-ITS-S, then all requirements relevant to the R-ITS-S equipment shall apply to the GNSS antenna and associated mounting bracket/s
- all information regarding the installation position, the structure to be mounted on (for example traffic signal pedestal post or mast arm) and any other relevant information to ensure best practice installation of the stations.
- installation procedure for the mounting brackets and supply of any specialised equipment if required for installation
- any other details as requested by Bridge and Structures division of Transport and Main Roads within 5 business days of the request.

10.4 Location of R-ITS-S Equipment

The installers will ensure the correct operation of R-ITS-S equipment given the following typical limitations of the mounting arrangement:

- a minimum mounting height of 4 meters height from the road surface level. Where possible the R-ITS-S equipment may be mounted between 6-8 meters from the road surface level.
- R-ITS-S may be mounted on traffic signal posts, mast arms or joint-use poles.
- R-ITS-S locations have been chosen to minimise occlusion from vegetation (when fully grown) and other objects such as buildings, signs and structures.
- where practical, the R-ITS-S will be mounted in a way that allows the antenna to be vertical

10.5 Design Life

Requirement: The design life of the R-ITS-S shall be a minimum of 10 years.

11 Installation

11.1 Initial Configuration

Requirement: The R-ITS-S shall be provided with all initial configuration set up, including but not limited to; key parameters, applications, management, certificates and security functions of the R-ITS-S. Typical initial configuration activities include but are not limited to:

- Configuration of key configurable parameters relating to applications, management function, data logging, control, configuration and security functions
- Setting of Unique station ID
- SMCS Bootstrapping
- MQTT service configuration including client, endpoints and global topic.

Requirement: The R-ITS-S shall be configured with an Amazon Web Services (AWS) Internet of Things (IoT) certificate.

12 Key Configurable Parameters

Requirement: The following parameters shall be configurable within the R-ITS-S.

Table 12-1 - Software operation and maintenance parameters

Data Element Identifier	Use (M/O)	Format	Default Value	Description/purpose	Message Tree Reference
citsSoftwareEnabled	M	BOOLEAN	TRUE	Turn off ITS-G5 communications and logging back to C-ITS-F	scm- station
spmExceptionLoggingLevel	M	ENUM: critical(0), error(1), information(2), debug(3)	error(1)	Determines the verbosity of logging returned	scm- station
camDirection	M	BIT STRING {transmit(0),receive(1)}(SIZE(2))	11	BIT STRING 0: Transmit 0 – do not collect CAM content; 1 = collect CAM content; BIT STRING 1: Receive 0 – do not collect CAM content; 1 = collect CAM content <i>Note: R-ITS-S will not typically transmit CAM</i>	scm- station
denmDirection	M	BIT STRING {transmit(0),receive(1)}(SIZE(2))	11	BIT STRING 0: Transmit 0 – do not collect DENM content; 1 = collect DENM content BIT STRING 1: Receive 0 – do not collect DENM content; 1 = collect DENM content <i>Note: R-ITS-S will not typically transmit DENM</i>	scm- station
mapemDirection	M	BIT STRING {transmit(0),receive(1)}(SIZE(2))	11	BIT STRING 0: Transmit 0 – do not collect MAPEM content; 1 = collect MAPEM content BIT STRING 1: Receive	scm- station

Data Element Identifier	Use (M/O)	Format	Default Value	Description/purpose	Message Tree Reference
				0 – do not collect MAPEM content; 1 = collect MAPEM content	
spatemDirection	M	BIT STRING {transmit(0),receive(1)}(SIZE(2))	11	BIT STRING 0: Transmit 0 – do not collect SPATEM content; 1 = collect SPATEM content; BIT STRING 1: Receive 0 – do not collect SPATEM content; 1 = collect SPATEM content	scm- station
storageThreshold	M	INTEGER (50..95)	85	tation storage threshold above which an exception is reported	scm- station
dopThreshold	M	INTEGER (1..10)	4	Dilution of Precision (DOP) above which an exception is reported	scm- station
minNumberOfSatellitesThreshold	M	INTEGER (2..5)	4	As indicated in the NMEA GSA string. Required to achieve acceptable positioning accuracy	scm- station
spatSourceTimeDiff Threshold	M	INTEGER (50..500)	300	Used to compare FP time to R-ITS-S time	scm- station
mapemVersionNumber	M	INTEGER (0..127)	0	if this isn't equal to the stored MAPEM then the R-ITS-S needs to download the new version	scm- station
csemCamLogLimit	M	INTEGER (1..600)	150	count of CAMs logged after which a CSEM is generated and logged	scm- station
csemDenmLogLimit	M	INTEGER (1..600)	150	count of DENMs logged after which a CSEM is generated and logged	scm- station
csemMapemLogLimit	M	INTEGER (1..600)	150	count of MAPEMs logged after which a CSEM is generated and logged	scm- station
csemSpatemLogLimit	M	INTEGER (1..600)	150	count of SPATEMs logged after which a CSEM is generated and logged	scm- station

Data Element Identifier	Use (M/O)	Format	Default Value	Description/purpose	Message Tree Reference
ritssSoftwareUpdate	M	HttpEndpoint	-	the location of a new software package	scm- station
ritssSoftwareCurrentVersion	M	IA5String(SIZE(1..32))	-	the version of the software required on the R-ITS-S (trigger to download if not matching)	scm- station
logFrequency	M	INTEGER(5..300)	60	Period for R-ITS-S and V-ITS-S to send time-aggregated messages (platform, behavioural, messages) to the C-ITS-F. Used to balance total message throughput and message size Unit: seconds	scm- system
csemLogWatchdogTimeout	M	INTEGER(1..1440)	10	if a CSEM has not been sent for this time a CSEM is sent with the current messages and counts	scm- system
logMessageRetentionWindow	M	INTEGER(1..1440)	1440	Period that the stations retain log data not uploaded to the C-ITS-F logging service. Used to allow log data to be uploaded after a 3G/4G communications outage.	scm- system
securityEnable	M	BOOLEAN	TRUE	Used to enable/disable C-ITS message signing.	scm- system
scmsEA	M	HttpEndpoint	-	location of the enrolment authority	scm- system
scmsAA	M	HttpEndpoint	-	location of the authorisation authority	scm- system

PROJECT DOCUMENT
REFERENCE ONLY