Department of Transport and Main Roads

Technical Specification

MRTS214 Provision of Wireless Traffic Sensors (WTS)

March 2025

Queensland Government

Copyright

Licence

CC BY licence summary statement

In essence, you are free to copy, communicate and adapt this work, as long as you attribute the work to the State of Queensland (Department of Transport and Main Roads). To view a copy of this licence, visit: https://creativecommons.org/licenses/by/4.0/

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

Contents

1 Introduction

This Technical Specification defines the design, supply, installation, testing and commissioning, performance, documentation, training, maintenance and handover requirements for Wireless Traffic Sensors (WTS) consisting of MAC-address detector with antenna and a MAC-address processor either in a single enclosure or as separate components.

Data from the WTS is used by Transport and Main Roads for a few applications including:

- real-time Travel time information for incident detection
- average speed and real-time Travel time information for traffic analysis, planning and network optimisation
- Origin-Destination routes for network planning and optimisation.

The WTS shall typically collect MAC-addresses in the following modes:

- Classic Bluetooth
- Bluetooth Low energy (BLE)
- Low address part (LAP), or
- Wi-Fi.

There are WTS devices that only support classic Bluetooth detection and identified as Wireless Traffic Sensor-Single Receiver (WTS-SR) in this Technical Specification.

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.

This Technical Specification forms part of the Transport and Main Roads Specifications Manual.

2 Definition of terms

The terms defined in MRTS201 *General Equipment Requirements* apply to this Technical Specification. Additional terminology relevant to this Technical Specification is defined in Table 2 below.

Table 2 – Definitions of terms

Term	Definition
ACMA	Australian Communication and Media Authority
BLE	Bluetooth Low Energy
EAP	Extensible Authentication Protocol
FAT	Factory acceptance test
GNSS	Global Network Satellite System
ITS	Intelligent Transport Systems
LAP	Low address part
MAC address	Media Access Control address, which is a unique identifier assigned to a network communication device for communications at the data link layer of a network segment
PoE	Power over Ethernet

Term	Definition
QADF	Principal's Telecommunication Network
QADF	Queensland Asset Data Format
QTDF	Queensland Traffic Data Format
RADIUS	Remote Authentication Dial-In User Service
RCM	Regulatory Compliance Mark
SNMP	Simple Network Management Protocol
TACACS	Terminal Access Controller Access-Control System
UI	Universal Identifier
VRU	Vulnerable Road Users (Pedestrians & cyclists)
WTS	Wireless Traffic Sensor
WTS-FP	WTS - Field Processor
WTS-MR	Wireless Traffic Sensor – Multiple Receiver
WTS-SR	Wireless Traffic Sensor – Single Receiver

3 Reference documents

The requirements of the referenced documents listed in Table 3 of MRTS201 *General Equipment Requirements* and Table 3 below apply to this Technical Specification. Where there are inconsistencies between this Technical Specification and the referenced documents, the requirements specified in this Technical Specification shall take precedence.

Table 3 – Referenced documents

Reference	Title
AS/CA S009	*Installation requirements for Customer Cabling (Wiring Rules)*
AS/NZS 61000.6.1	*Generic standards—Immunity for residential, commercial and light industrial environments*
AS/NZS 61000.6.3	*Generic standards—Emission standard for residential, commercial and light-industrial environments*
AS/NZS 3000	*Wiring rules*
MRTS61	*Gantries and Support Structures for Road Signs, Tolling Systems and ITS Devices*
MRTS71	*Reinforcing Steel*
MRTS201	*General Equipment Requirements*
MRTS207	*Traffic Monitoring Foundation Equipment*
MRTS226	*Telecommunications Field Cabinets*
MRTS245	*ITS Telecommunications Network (ITS TN)*
MRTS255	*Traffic Signal Controllers*
MRTS263	*Standalone Solar (PV) Power Systems*
SD1781	*ITS IPRT network - Typical Traffic Controller with Tophat Telstra Modem and Associated Communications Cabling*
SD1782	*ITS IPRT network - Typical Traffic Controller with Telstra Modem and Associated Next G Antenna*

Reference	Title
SD1783	*ITS IPRT network - Typical Traffic Controller with Tophat Telstra Modem and Associated Next G Antenna*
SD1905	*ITS - Traffic Monitoring Cabinet*

4 Quality system requirements

The quality system requirements defined in MRTS201 *General Equipment Requirements* apply to this Technical Specification. Additional quality system requirements relevant to this Technical Specification are defined in Table 4.1 below.

4.1 Hold Points, Witness Points and Milestones

General requirements for Hold Points, Witness Points and Milestones are specified in Clause 5.2 of MRTS01 *Introduction to Technical Specifications*.

The Hold Points, Witness Points and Milestones applicable to this Technical Specification are summarised in Table 4.1. There are no Milestones defined.

Table 4.1 – Hold Points, Witness Points and Milestones

Clause	Hold Point	Witness Point	Milestone
4.2	1. Detailed design documentation to be provided 2. RCM compliance		
7.3	3. Detailed design documentation of mounting structure and footings location and reduced levels (RLs)		
12.2		1. Factory Acceptance Tests – (FAT)	
12.3		2. Installation Acceptance Test (IAT)	
12.4		3. Commissioning Test (CT)	

4.2 Sample WTSs

Detailed designs of the WTS layout, fabrication and assembly drawings, calculations, specifications and certifications of the WTS components (signed by the Contractor's RPEQ) shall be submitted to the Principal via the Administrator for verification of compliance to this Technical Specification. These components include the WTS processor, detector and antennae, power supply (including surge protection and back-up batteries), communication ports, cable termination, enclosure and mounting accessories. **Hold Point 1**

All radio communications shall comply with the relevant regulatory requirements of ACMA as well as the immunity and emissions requirements in AS/NZS 61000.6.1 and AS/NZS 61000.6.3 respectively. RCM compliance confirming the WTS radiofrequency performance requirements shall be submitted before delivery to site. **Hold Point 2**

As specified in MRTS201 *General Equipment Requirements*, a sample WTS shall be provided for the FAT. The sample WTS shall be complete with all components intended to be used in the WTS to be provided under the Contract.

4.3 Warranty

The contractor installing the WTS shall warrant all work performed and all materials supplied for the installation against defects for a minimum of 3 years in accordance with the warranty requirements of MRTS201 *General Equipment Requirements*.

Minimum 3 year warranty provision is required for WTS as they fall under a category of products with high quantity although not necessarily high cost or safety critical – see MRTS201 *General Equipment Requirements* for details.

5 Functional requirements

5.1 WTS components

The WTS shall as a minimum consist of:

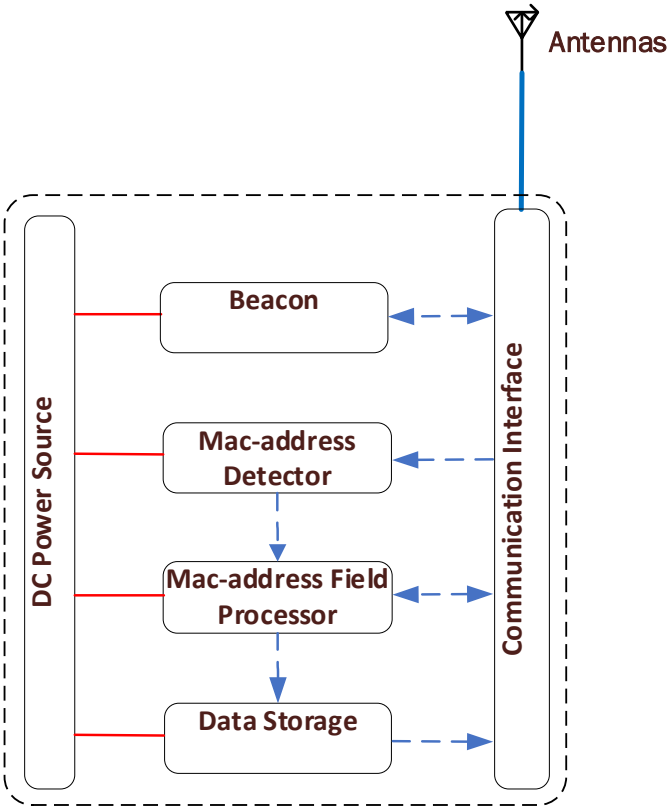
- MAC-address Detector (with receive antenna)
- WTS Field Processor (WTS-FP) capable of connecting to the department's ITS network as well as any IP based network using IPv4. IPv6 support is desirable.
- Beacon (Transmit antenna) (Beacon is optional for WTS-SR)
- Data storage device
- Power supply, and
- Network and communications interface (see Clauses 5.1.1 and 5.1.5)

The WTS components shall be physically connected in a compact arrangement such that they can be collocated in the same enclosure. In addition, to minimise the use of separate antennas, the WTS RF interface shall support all frequency bands used by the device and shown in Table 5.1.5. This can be done using a single multiband antenna.

Each of these components is further described below.

The WTS-FP is different to the typical FP used by the department for connection to STREAMS.

Figure 5.1 – WTS components



The antenna used on the WTS shall be independently assessed and approved by the Principal.

5.1.1 MAC address detector and Beacon

The MAC address detection of the WTS-MR shall be capable of capturing MAC addresses from the target vehicular and pedestrian environments using different modes including, classic Bluetooth, BLE, LAP and Wi-Fi. The WTS-SR shall support Bluetooth detection as a minimum.

The WTS shall have provision to be used as a beacon to transmit ITS messages to the relevant vehicular and pedestrian environments.

After receiving ITS messages from the back-end, the WTS-MR beacon shall continue to broadcast the ITS messages to the vehicular/pedestrian environment and only cease broadcasting when a negating message is sent from the back-end, or a pre-defined broadcast duration is reached, whichever occurs first.

> The range of transmission of the WTS device is generally about 150 m. However, the maximum range depends on the signal strength, environmental conditions or interference from other signals.
>
> AddInsight® is currently the back-end application intended to broadcast ITS messages.
>
> Beacon is an option feature for WTS-SR.

5.1.2 WTS Field Processor

The WTS FP shall receive MAC address data, and transmit the data in a format compatible with the current version of AddInsight ® as well as the UI format described in Appendix A. The FP shall have provisions to support custom data formats prescribed by the Principal.

BT data format described in Appendix B is acceptable for WTS-SR.

5.1.3 WTS Data storage

The WTS shall have provision for data storage to enable the retrieval of historical data. Refer to Clause 6.3 for details.

5.1.4 WTS Power supply

The WTS power requirements shall be as described in Clause 9.

5.1.5 WTS interfaces and connectors

To enable communication with the vehicular and pedestrian environment as well as the Principal's Telecommunications Network (PTN), the WTS shall as a minimum provide interfaces as shown in Table 5 1.5.

Table 5.1.5 – WTS interfaces

Interface	Technology	Minimum Standard	Typical RF Frequency
GNSS	**GNSS**	local GNSS	L1 (1575.42 MHz), L2(1227.6 MHz), L3(1176.45 MHz)
MAC address interface	**Classic BT**	WPAN (IEEE802.15)	2.400 to 2.485 GHz
	BLE	WPAN (IEEE802.15)	2.400 to 2.485 GHz
	LAP	WPAN (IEEE802.15)	2.400 to 2.485 GHz
	Wi-Fi	WLAN (IEEE802.11)	2.4 or 5.8 GHz
PTN interface	**Ethernet**	Ethernet (IEEE802.3)	
	4G / 5G	4G	520 MHz, 900 MHz, 1.8 GHz, 2.1 GHz
Power console	**AC / DC**		
	USB / RS232	USB2.0 / TIA-232-F	

Preferred connectors for the RF interfaces (antenna ports) include SMA and SMA-RP. For wired connection to the PTN, RJ45 connectors are preferred. For local access the WTS shall provide a USB port or RS232 access. All connectors shall be secured such that they are firmly in place and resistant to extreme shock and vibration

The WTS should be able to integrate to the department's system as described in Clause 6.

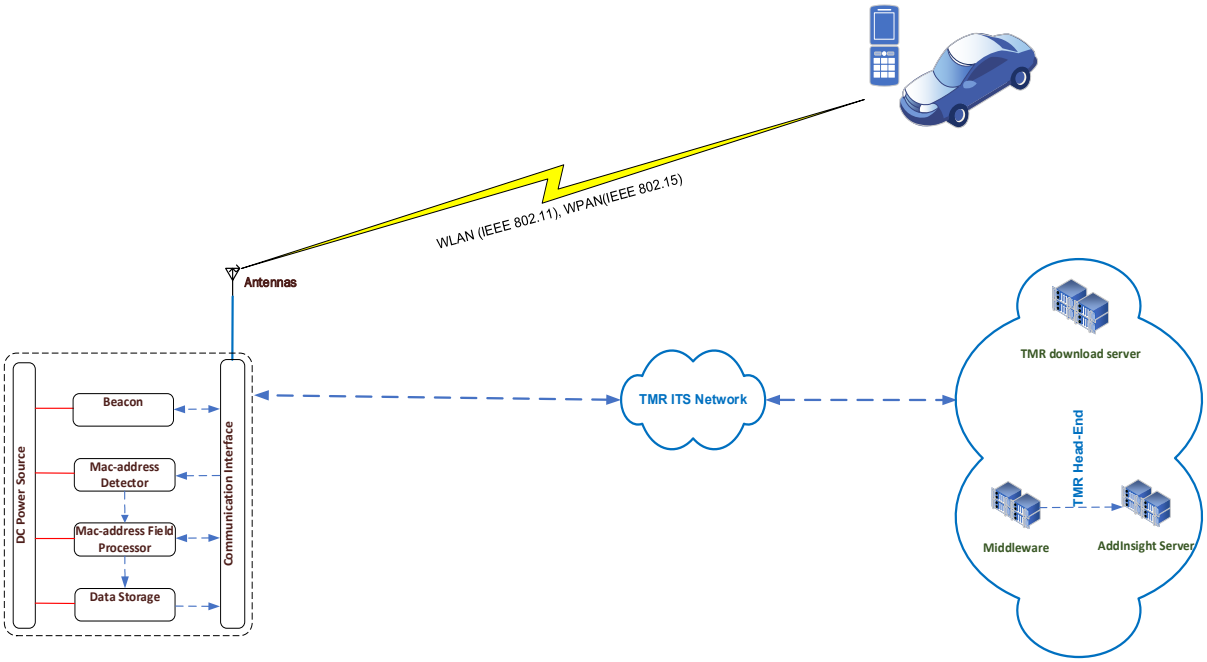
5.2 Timing and Synchronisation

The WTS shall implement the NTP protocol and be synchronised to an NTP server prescribed by the Principal. NTP is required for the log file to be downloaded as described in Clause 6.2.

6 Operational Requirements

6.1 System Architecture

Figure 6.1 – WTS system architecture



The WTS will detect MAC addresses from the vehicular environment for traffic analysis as well as transmit relevant information to the vehicles or VRU's in its vicinity where required. The detected data will be used for analysis by AddInsight as well as other departmental systems located at the Transport and Main Roads back-end as shown in Figure 6.1.

The WTS shall be capable of communicating via the department's ITS network either wirelessly using 4G / 5G or via ethernet. All communications with the departmental ITS network shall be in accordance with MRTS245 *ITS Telecommunications Network (ITS TN)*. Where the WTS uses an in-built modem, it shall comply with the requirements of the department's local telecommunications provider.

The WTS shall also be capable of interfacing directly with a message-oriented middleware selected by the Principal or directly with AddInsight ®.

> At the time of this Technical Specification, the department uses kafka® to interface between the field devices and other application servers including AddInsight ®.

The WTS shall make provision for the download of data stored in the WTS storage. The department's download service will extract data from the WTS on a daily basis.

6.2 Data Capture, Streaming and Logging

Data capture shall commence as soon as the WTS has powered-up and initialised and continue as long as the WTS is turned on. The WTS shall be synchronised with the department’s NTP server within 30 seconds after turned on and the WTS shall be capable of remote NTP query access via back-end systems for audit purposes. Data capture shall not commence until after NTP synchronisation.

The WTS shall be capable of individually enabling / disabling the capture of the following data:

1. Classic BT
2. BLE
3. LAP and
4. Wi-Fi.

The WTS shall stream MAC-addresses in real-time as described in the UI format (see Appendix A). The WTS shall also stream data compatible with the current AddInsight ® version at the time of purchase. The WTS shall log data to disk in QTDF format. The WTS shall be capable of individually enabling / disabling the UI, AddInsight ® and QTDF formats. BT data format described in Appendix B is acceptable for WTS-SR.

The logged MAC address records shall be retrieved from the WTS by the back-end system via FTP in batches. The batch size shall be a configurable parameter based on the time of the MAC-address capture, ranging from hourly to daily batch sizes.

> Currently the department's download service downloads data daily. A more frequent rate may be required in the future.

WTS MAC address data logging must not interfere with the sending and receipt of log messages and configuration messages to and from the back-end system.

6.3 Data Retention

The WTS shall locally retain a store of logged data of up to 2 million collected MAC address records on a circular buffer, while also streaming data to the back-end system via the Principals telecommunications Network. The retained data shall be in accordance with the QTDF format and shall persist over power cycles. This feature will also act as a back-up in the event of loss of communications with the Principal's back-end system.

> Once the department downloads and deletes the log file via FTP, generally that data is no longer required on the device. Therefore, the circular buffer is only required to ensure that the WTS has the capability to store accumulated data up to a maximum of 2 million MAC addresses with oldest being deleted when full.

6.4 Management

The WTS vendor shall provide a management facility for local and remote control and configuration of the WTS and shall support access via web interface, Command Line Interface (CLI), and centralised management platform access that could be hosted within the Principal's network environment.

The management facility shall implement multiple levels of user access.

The management facility will support centralised configuration management, archival of device configurations, administration and monitoring of the field deployed Processors.

The management facility shall provide 2 options for registering the location of the WTS device, namely, entered manually or automatically based on GNSS connectivity.

The department currently registers the location of the WTS manually for data consistency and to guard against GNSS inaccuracies due to drifting. Automatic location of WTS using in-built GNSS may be required in the future as accuracy improves.

Firmware updates might be done via the field processor directly via the communications interface.

The WTS management facility shall have sufficient capacity to support the configuration and monitoring of up to 2,000 field deployed WTS units. The WTS shall support remote monitoring capability, such as voltage and temperature.

The monitored data will be accessed locally via a Command Line Interface (CLI). Remote monitoring capability shall be provided via SNMPv2 (or better), and optionally Modbus protocols in a secure manner. Also, critical events notifications (e.g. significant power deviations) shall trigger alerts using SNMP trap protocols.

6.4.1 Alarms

The WTS shall support a Dying Gasp function for remote power failure detection (via SNMP traps or equivalent). Other event notifications to be alerted using SNMP trap protocols shall include:

- Significant voltage or power deviations
- High temperature.

6.4.2 WTS FP monitoring

The WTS management facility shall support WTS FP monitoring including:

- Session monitoring – used to identify a FP session (Uptime, Downtime) and to detect session exceptions
- Platform performance metrics (e.g. CPU, memory)
- Platform exception logs.

6.4.3 WTS watchdog

The WTS shall have internal hardware watchdog to recover from system errors that may result in lockup.

6.4.4 Power management

The WTS shall provide a means for entering a low power sleep mode during a pre-configured time schedule such as low traffic periods. The WTS shall also provide a means for entering a low power sleep mode during a pre-set event such as a drop in supply voltage below a configurable setpoint as would be required in solar / battery applications.

Once normal voltage resumes the WTS shall wake-up and resume normal operation.

6.5 Security

The following security requirements apply to the WTS. The WTS Field Processor shall:

- Support user authentication for both local and remote access using standard industry recognised secure authentication protocols such as EAP, TACACS, RADIUS,LDAP and so on).

- Support granular user access levels for different device support functions (e.g. configuration, monitoring, etc.).
- Shall be able to record user login and logout session. The logging function will be supported locally and through the WTS management facility (e.g. via Syslog function).
- Centrally log any configuration changes performed on the WTS FP for auditing and/or forensic purposes (e.g. via Syslog function).
- Support network access Filtering capability.
- The following features will be supported:
  - Certificate or shared key device authentication (Phase 1)
  - Local, RADIUS, LDAP based user authentication (Phase 2)
  - Advanced Encryption Standard (AES) 256-bit encryption, and
  - The use of Public Key Infrastructure (PKI) X.509 based certificates.
- Support a virtual account for FTP so that that account can't be used for other areas of system access.

7 Mechanical and physical requirements

The mechanical and physical requirements defined in MRTS201 *General Equipment Requirements* and MRTS61 *Gantries and Support Structures for Road Signs, Tolling Systems and ITS Devices* apply to work provided under this Technical Specification. Additional mechanical and physical requirements for equipment provided under this Technical Specification are described below.

7.1 Design life

The WTS shall comply with the product lifecycle requirements specified in MRTS201 *General Equipment Requirements*. In addition, unless otherwise specified, the WTS design life shall be a minimum of 10 years.

7.2 Environmental conditions

The WTS and associated mounting structures and electronics, shall comply with the environmental requirements of MRTS201 *General Equipment Requirements*. Additional environmental requirements are as follows.

The WTS FP shall:

- Be capable of continuous, normal operation where the ambient air temperature is between -10°C and 55°C.
- Be capable of continuous, normal operation where the enclosure air temperature is between -10°C and 75°C.
- Be capable of continuous, normal operation where the humidity is between 0 to 95% non-condensing.
- Support environmental monitoring capability (e.g. for remote temperature monitoring). The monitored data will be accessed locally via a Command Line Interface (CLI) and remotely using SNMP or Modbus protocols. Also, critical events notifications (e.g. high temperature) will be able to be alerted via SNMP traps protocols.

7.3 Mounting structure

The location and type of mounting structure to be provided to mount each WTS shall be shown on the design documentation. The mounting structure shall comply with the requirements of MRTS201 *General Equipment Requirements*, MRTS61 *Gantries and Support Structures for Road Signs, Tolling Systems and ITS Devices* and MRTS71 *Reinforcing Steel*.

The final design documentation shall include details of the final footing design, location and heights of the structure. Contractor shall not commence fabrication of the footing and support structure until final design documentation has been accepted by the Administrator. **Hold Point 3**

7.4 Field cabinets

All WTS equipment and associated devices shall be installed in a suitable roadside enclosure, being:

- a traffic signal cabinet extension (Tophat), or
- a ground mounted field cabinet complying with requirements of MRTS226 *Telecommunications Field Cabinets*, or
- a ground mounted Traffic Monitoring cabinet complying with requirements of MRTS207 *Traffic Monitoring Foundation Equipment*, or
- an enclosure complying with the requirements of MRTS201 *General Equipment Requirements* installed on a mounting structure.

8 Technical requirements

8.1 System Start-Up

In order to facilitate fast and accurate timing and synchronisation the WTS shall have a battery backed real time clock.

The WTS shall be capable of interfacing with a message-oriented middleware selected by the Principal as well as AddInsight ®. The contractor shall contact the Principal to determine the current mechanism for interfacing to the field devices.

> At the time of this Technical Specification, the department uses kafka® to interface between the field devices and other application servers including AddInsight ®.

8.2 Storage

In addition to the storage requirements defined in Clause 6.3, the WTS shall have non-volatile memory to store all information required to meet the operational and technical requirements. These include additional storage for firmware updates and system logs.

8.3 Maintenance Communications

The WTS shall have provision for both local and remote maintenance and configuration.

8.4 Control/Diagnostic Software

The Contractor shall provide the Principal with control and diagnostic software required for the WTS and associated equipment.

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

8.5 Failure Modes

The Contractor and Principal shall agree what constitutes critical failures and minor failures.

In the event of critical failures, the WTS equipment shall:

- Return failures as part of the error log. If the failure is an operational and/or telecommunications failure, the WTS shall continue all background data logging functions for upload back to the PTN 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 and automatically send failure logs once the system is restored.

8.6 Radio Performance

The WTS equipment shall provide wireless communication to the vehicular environment with a high probability of transmission success over 150 m line of sight and under typical traffic conditions. Wireless communication performance including antenna selection shall be subjected to testing and approval by the Principal.

In addition to collecting MAC addresses for traffic analysis, The WTS shall also be used as a beacon to transmit information to vehicles or VRU's in its vicinity. In this case, the WTS being used as a transmitting device shall meet the relevant ACMA requirements.

Beacon is an optional requirement for the classic Bluetooth traffic sensor.

9 Electrical Requirements

9.1 General

The electrical requirements defined in MRTS201 *General Equipment Requirements* apply to work provided under this Technical Specification. Additional requirements are as described below.

Electrical wiring shall be in accordance with the requirements of AS/NZS 3000 and AS/CA S009.

The power consumption of the WTS including associated components shall not exceed 9W. This includes any attached devices that may draw power from the device (e.g. Flash memory card, USB etc.). The WTS operating voltage will be 12V DC with an operating voltage range in the interval +9V and +24V DC. The WTS shall be powered by an external power adapter suitable for the operational environment specified in Clause 7.2.

The WTS shall support reverse polarity protection.

Options for energising the WTS shall include Mains power and stand-alone power. In addition, where required, the WTS shall support Power over Ethernet, PoE or PoE+ (IEEE 802.3af).

9.2 Mains-powered WTS installations

The WTS shall have provision for connection to mains power using an external adaptor or PoE.

WTS energised from mains power may not require secondary battery back-up. However, in order to facilitate fast and accurate timing and synchronisation upon start up, the WTS shall have a battery backed real time clock. The clock shall be able to be synchronised with the Principal's network time server. Error of the real time clock shall be no more than one second over a period of one week.

9.3 Solar powered WTS installations

The requirement of the MRTS263 *Standalone Solar (PV) Power Systems* shall apply to the Technical Specification. The WTS shall have provision for connection the stand-alone power supplies such as solar power.

A battery backup system shall be provided with each solar powered WTS. The battery back-up shall have the capacity to maintain normal WTS operation for a period of 168 continuous hours, including any communication services.

Batteries used in the backup shall be in accordance with MRTS263 *Standalone Solar (PV) Power Systems*. The WTS management system shall have provision for monitoring the solar power system including voltage levels.

10 Telecommunications requirements

The telecommunications requirements defined in MRTS201 *General Equipment Requirements* apply to work provided under this Technical Specification. In addition, all telecommunication equipment shall comply with the relevant regulatory requirements and standards of Australian Communications and Media Authority (ACMA).

11 Installation requirements

The installation requirements defined in MRTS201 *General Equipment Requirements* apply to this Technical Specification.

WTS are generally installed in:

- Traffic signal controller cabinet extension (Tophat) complying with the requirements of MRTS255 *Traffic Signal Controllers,* or
- A ground mounted or pole-mounted ITS field cabinet complying with the requirements of MRTS226 *Telecommunications Field Cabinets*.

Where the WTS is installed in the traffic signal controller extension, it shall be in accordance with the arrangement described in SD1781, and SD1783.

> SD1781 and SD1783 show how a modem is connected in a Tophat. The intent is to use the same configuration but replacing the Modem with the WTS device.

WTS installed on ground mounted or pole-mounted ITS cabinet shall follow typical installation practices for ITS devices and the arrangement described in SD1905. The location of the WTS antenna shall be such that its detection range is in accordance with the requirements of the project design.

12 Testing and commissioning

12.1 General

The testing and commissioning requirements defined in MRTS201 *General Equipment Requirements* apply to work provided under this Technical Specification. The minimum additional testing and commissioning requirements for equipment provided under this Technical Specification are described below.

12.2 Factory acceptance tests (FAT)

The FAT shall include all the performance parameters in this Technical Specification that can be tested under laboratory/factory conditions.

The Contractor shall demonstrate that the equipment meets the AddInsight interface requirements to the satisfaction of the Principal.

The data quality and compliance with the UI format shall be verified by the Principal. **Witness Point 1**

12.3 Installation acceptance tests (IAT)

Once the WTS is installed on Site, the Contractor shall demonstrate and certify that the WTS has been installed to allow correct operation, exhibiting similar results in the intended operating environment as the results in the FAT. **Witness Point 2**

12.4 Commissioning tests (CT)

The commissioning requirements defined in MRTS201 *General Equipment Requirements* apply to work provided under this Technical Specification.

The commissioning report sheet in MRTS214 Appendix C shall be completed as part of the test and included in the operations manuals. **Witness Point 3**

13 Documentation

The documentation requirements defined in MRTS201 *General Equipment Requirements* apply to work provided under this Technical Specification.

14 Training

The training requirements defined in MRTS201 *General Equipment Requirements* apply to work provided under this Technical Specification.

15 Maintenance

The maintenance requirements defined in MRTS201 *General Equipment Requirements* apply to work provided under this Technical Specification.

16 Handover

The handover requirements defined in MRTS201 *General Equipment Requirements* apply to work provided under this Technical Specification. Further requirements are as described below.

The contractor shall provide asset data for the installed WTS in the format prescribed by the QADF document. The contractor shall liaise with the Principal regarding the inclusion of the WTS asset into the Road Operations Asset Management Systems (ROAMS) database.

17 Type Approval

The contractor may apply for type approval of the WTS in accordance with the department's type approval process. Appendix D contains a type approval checklist, which the contractor shall complete and submit with the type approval application.

Appendix A: UI data structure

Table A1 – UI Data Structure

Position	Bytes	Type	Description
1	1	UI	Header ID (T)
2	1	Packet	Packet ID = Encoded Value - 0x22H (Range = [0x20, 0x7D])
3-8	6	Tx Date	Date of transmission - ASCII Encoded Date (YYMMDD)
9-14	6	Tx Time	Time of transmission - ASCII Encoded Time (HHMMSS)
15-20	6	Event Date	Date of event data - ASCII Encoded Date (YYMMDD)
21-16	6	Event Time	Time of event data - ASCII Encoded Time (HHMMSS)
27	1	Type	Alphanumeric datatype of unique identifier address: 0 (0x30):Bluetooth Classic 1 (0x31):Bluetooth Low Energy 2 (0x32):Lower Address Part for Bluetooth Classic 3 (0x33):Lower Address Part for Bluetooth Low Energy 4 (0x34):Wi-Fi
28	variable (max 12 bytes)	Device ID	Device identifier with up-to 12 bytes allocated as follows: • Exactly 3 bytes reserved for departmental-generated manufacturer code • Up to 9 bytes determined by the manufacturer. It is preferred that the last 6 digits of the IMEI (excluding the check digit) be used, where possible.
N/A	1	Sep	Pipe (0x7C) separation
N/A	variable	Unique Identifier	Datatype of wireless MAC address, each separated by 1 byte (Sep)
N/A	1	EOT	End of transmission character is ETX (0x03)

Table A2 – UI Data example

Type	Hex encoded	Decoded
UI	54	T
Packet	22	"
Tx Date	31	24/06/2015
	35	
	30	
	26	
	32	
	34	
Tx Time	31	16:29:20
	36	
	32	

Type	Hex encoded	Decoded
	39	
	32	
	30	
Event Date	31	24/06/2015
	35	
	30	
	36	
	32	
	34	
Event Time	31	16:29:20
	36	
	32	
	39	
	32	
	30	
Type	30	0
Device ID	51	ABC94367
	52	
	53	
	39	
	34	
	33	
	36	
	37	
Sep	7C	|
Unique Identifier 1	37	74DE2BA5DDF2
	34	
	44	
	45	
	32	
	42	
	41	
	35	

Type	Hex encoded	Decoded
	44	
	44	
	46	
	32	
Sep	7C	|
Unique Identifier 2	31	123456789ABC
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	41	
	42	
	43	
Sep	7C	|
Sep	7C	|
Unique Identifier N	43	CBA987654321
	42	
	41	
	39	
	38	
	37	
	36	
	35	
	34	
	33	
	32	
	31	
EOT	03	ETX

Appendix B: BT data structure

Table B1 – BT data structure

Position	Bytes	Type	Description
1	1	UI	Header ID (T)
2	1	Packet	Packet ID = Encoded Value - 0x20H
3-8	6	Tx Date	Date of transmission - ASCII Encoded Date (YYMMDD)
9-14	6	Tx Time	Time of transmission - ASCII Encoded Time (HHMMSS)
15-23	9	Device ID	Device identifier in ASCII format and left padded with Space (0x20)
24-29	6	Event Date	Date of event data - ASCII Encoded Date (YYMMDD)
30-35	6	Event Time	Time of event data - ASCII Encoded Time (HHMMSS)
36-37	2	MAC Count	Number of MAC addresses in the packet encoded in the Binary Coded Decimal (BCD) format
N/A	Variable	Unique Identifier	List of 12 byte MAC addresses without separation
N/A	1	EOT	End of transmission character is ETX (0x03)

Table B2 – BT Data example

Type	Hex encoded	Decoded
BT	54	T
Packet	22	[Space 0x20]
Tx Date	31	24/06/2015
	35	
	30	
	26	
	32	
	34	
Tx Time	31	16:29:20
	36	
	32	
	39	
	32	
	30	

Type	Hex encoded	Decoded
Device ID	20	ABC94367
	51	
	52	
	53	
	39	
	34	
	33	
	36	
	37	
Event Date	31	24/06/2015
	35	
	30	
	36	
	32	
	34	
Event Time	31	16:29:20
	36	
	32	
	39	
	32	
	30	
MAC Count	30	2
	32	
MAC 1	37	74DE2BA5DDF2
	34	
	44	
	45	
	32	
	42	
	41	
	35	
	44	
	44	
	46	
	32	

Type	Hex encoded	Decoded
MAC 2	31	123456789ABC
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	41	
	42	
	43	
EOT	03	ETX