WAKA KOTAHI
NZ TRANSPORT
AGENCY

VARIABLE MESSAGE SIGNS AND LANE AND CARRIAGEWAY SIGNS SYSTEM INTERFACE STANDARD

Intelligent Transport Systems (ITS) Core Requirements Standard

20 SEPTEMBER 2024
VERSION 0.11

New Zealand Government

Copyright information

Disclaimer

NZTA has endeavoured to ensure material in this document is technically accurate and reflects legal requirements. However, the document does not override governing legislation.

NZTA does not accept liability for any consequences arising from the use of this document. If the user of this document is unsure whether the material is correct, they should refer directly to the relevant legislation and contact NZTA.

More information

If you have further queries, contact the Intelligent Transport Systems Standards and Specifications (ITS S&S) team via email: itsspec@nzta.govt.nz

More information about ITS is available on the NZTA website at https://www.nzta.govt.nz/its

This document is available on the NZTA website at https://www.nzta.govt.nz/itsspecs

Template version

1.8, 03/11/2021

Contents

List of figures

List of tables

1 OVERVIEW AND OUTCOMES

This section defines the core requirements to support operational outcomes for ITS with respect to the transport network.

1.1 Purpose

This core requirements standard defines expected practices in control interfaces with all electronic messaging and signalling equipment that is connected to NZTA networked systems to deliver information to users on the national road network. The intent is a balanced standard that sets common expectations of compliance to ease integration of cohesive future systems while preserving flexibility for innovation. To achieve the desired levels of cohesion and interoperability across future ITS device networks, and to ease integration of future additions, it is necessary to identify a set of widely accepted standards and define a required level of compliance. Additional detail of certain behaviours is also proposed to further maintain a common understanding of system behaviours between all stakeholders.

This core requirements standard formally adopts the ISO 20684 series of standards as normative, to be the common standard for operational communication with and between the control systems of variable message sign (VMS) and lane and carriageway sign (LCS) field devices when operational on the NZTA Intelligent Transportation Systems Network (ITSN). This is supplemented by additional user needs specific to NZTA systems, and application notes on expected behaviours for certain functions.

The target application of this core requirements standard is SM031 and SM032 – State highway construction and maintenance contract proforma manuals.

1.2 Overview

This core requirements standard represents the formal adoption of concepts expressed in the ISO 20684 series, both where explicitly referenced as well as for general intent, and should be read in conjunction with that document and its supporting literature.

As display technologies improve and reliance on them for control of the transport system increases, the potential consequences for distraction or misdirection from inappropriate message display increases. There is also a potential for these devices to become used as roading signals with legal standing. For these reasons, NZTA is obliged to secure complete control of all VMS devices and unfettered visibility of status, including records of all commands received and executed.

Additionally, this core requirements standard introduces cybersecurity requirements as a fundamental element of interface implementation.

For the purposes of this core requirements standard, interactions with a VMS or LCS are categorised into three logical groups:

i. Control of the VMS or LCS
ii. Configuration of the VMS or LCS
iii. Monitoring of the VMS or LCS.

These align with operational features detailed in *NTCIP 1203 version v03 National Transportation Communications for ITS Protocol – Object definitions for dynamic message signs (DMS)* (NTCIP 1203 v03) section 2.5 Features. The distinction is repeated here as the three categories each differ in their requirements and potentially lend themselves to different interface protocols. Each logical category is detailed in this core requirements standard according to the NZTA system design principles.

1.2.1 NZTA ITS class

012 System interfaces
Class definitions

1.3 Scope

This standard is to apply to all communication between VMS and LCS field devices and any system interfacing with such devices when connected to the client network systems. In this context, remote includes devices physically co-located but connected only through network systems, but excludes communication between controllers and the displays themselves or other peripheral devices, as illustrated in Figure 1. Note that this excludes mobile VMS and LCS and independently controlled devices and does not cover the communications protocols. Note also that devices not connected to the ITSN or its successors are also excluded. Further, compliance with this core requirements standard is compulsory for devices or systems which interface with the client systems, but in other cases is advisory only.

Details of system integration and implementation are treated separately. However, for certain functional requirements this core requirements standard specifies the expected behaviour from the perspective of the user. Where intent diverges from ISO 20684 standards, this core requirements standard details the expected device behaviours. Effort has been made to reference content in that document rather than reproducing it; however, selected content is reproduced for the sake of clarity. Where contradictions arise, this core requirements standard shall take precedence for application on New Zealand roads, in accordance with the NZTA document framework.

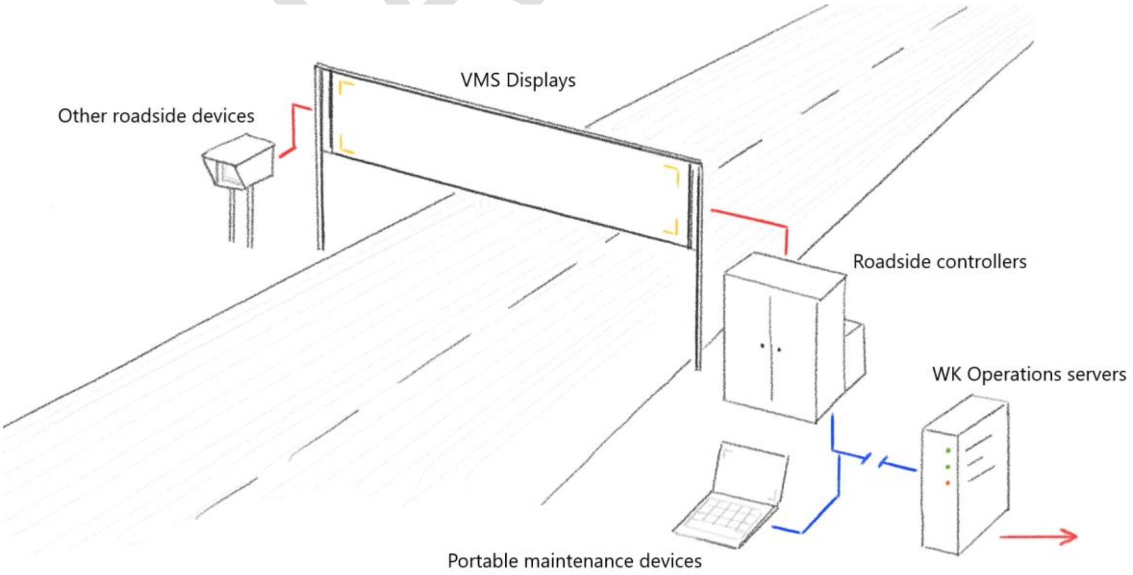


Figure 1. Diagram of applicability of this core requirements standard to network architecture. Only connections shown in blue are covered by this core requirements standard.

1.4 Outcomes

This section defines the operational outcomes for ITS with respect to the transport network.

Three critical outcomes are identified:

i. a clearly defined set of commands and data attributes against which functional compliance can be measured
ii. a defined set of responses or states expected from a display device subject to command execution or a change of state due to external stimulus
iii. a clear path to alignment with operational expectations or requirements, or another functionality defined to meet user needs, including anticipated future user needs.

2 DESIGN FOR OPERATION

2.1 Devices to demonstrate compliance with ISO 20684 standards

All VMS and LCS devices on the client road network shall demonstrate compliance with the ISO 20684 series of documents as defined in those standards unless a departure has been granted by Waka Kotahi. Refer to section 5 Conformance of ISO 20684-1:2021 *Intelligent transport systems – Roadside modules SNMP data interface – Part 1: Overview* (ISO 20684-1) for details on the conformance matrix approach to specification of and conformance to requirements, which differs from the Protocol Requirements List used by NTCIP 1203 v03.

Noting the dependencies of the ISO 20684 series on other standards such as IETF RFC 3584 *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework* (RFC 3584) and NTCIP 1203 v03, those referenced documents should be considered compulsory only insofar as the context in which they are referenced by ISO 20684 standards. For example, user needs concerning failure modes and pixel testing are defined by ISO/TS 20684-10:2021 *Intelligent transport systems – Roadside modules SNMP data interface – Part 10: Variable message signs* (ISO/TS 20684-10), but the Requirements Traceability Matrix defines the associated functional and non-functional requirements by referencing specific sections of NTCIP 1203 v03. Other elements of NTCIP 1203 v03 not referenced in this way should not be considered mandatory.

Differences between NTCIP 1203 v03 and the ISO 20684 series are summarised in ISO/TS 20684-10 annex C: Relationship to NTCIP 1203.

2.1.1 Supplemental user needs

An extensive set of user needs are defined in the User needs section of each ISO 20684 series standard, with their attendant conformance requirements detailed in the Conformance section of each standard. Certain additional features are required by NZTA, which reflect behavioural requirements stemming mostly from matters of integration. This core requirements standard supplements ISO 20684 series user needs with a further set specific to NZTA systems, detailed in the following subsections.

2.2 Control and monitoring interface user needs

2.2.1 Control interface

This section details supplemental user needs related to normal operational use of the device.

2.2.1.1 Default fonts

A set of fonts will be defined by NZTA, and all messages shall be displayed in these supplied fonts. Refer to Appendix A: Default fonts for these fonts. The provided fonts should be the only fonts loaded on the device and in the specified slot order and with the specified selection keys (nominally using the supplied data objects `fontNumber` and `fontName` in accordance with NTCIP 1203 v03 section 5.4.2 Font Table Parameter), or else using the MULTI font selection keys in the form `Fxx`. Where it is not possible to remove or replace any default fonts loaded in non-volatile, non-changeable memory, selection keys detailed in annex A or in any overriding device specification shall select the Waka Kotahi issued fonts, unless a departure is granted by NZTA.

Default fonts will be specified using UTF-8 encoding as mandated by ISO/TS 20684-10 and will include vowels with macrons for the correct rendering of te reo Māori.

2.2.1.2 Standard graphics

A standardised list of graphics will be defined by the Client for each installation, which are to be stored on the device in a specified order and with known reference keys. Graphics shall be defined by their functional purpose and linked to the relevant symbols as per the current *Traffic control devices manual* (TCD manual). This approach leaves flexibility in rasterisation to best utilise the capabilities of the display and preserves the TCD manual as the single source of truth for physical and digital signage on New Zealand roads. Details of the prescribed graphics are given in Appendix B: Default graphics library.

A method shall be provided by which the Client may update the stored graphics as per section 4.1 Configuration interface. A conversion or editing tool is not required unless the file format is proprietary, but a Consultant must detail the necessary resolution, colour data, file format and any other attributes to enable Client to populate the graphics library to best match the capabilities of the sign.

2.2.1.3 User-based message control

Priority paradigms established through ISO 20684-10 section 8.3.2.6 Display a message on the sign display are message-based and limited to a list of value assignments. A priority paradigm based on command source is preferred, which is achievable without modification of the existing Activation and Runtime Priority datagrams if the following concepts are combined. These together will create a user-based access control paradigm.

2.2.1.3.1 Activation and Runtime Priority assignment lists

Client must retain control over message priority lists encoded on roadside devices, including the ability to remotely make changes to these lists on deployed signs. All users will be assigned a set of priority bands, which they are permitted to use when commanding the activation of a message. These user-based priority assignments tables will be issued and maintained by Client with the acceptable range of values. This also applies to automated command sources: a management station should not command messages with priority outside its assigned band.

2.2.1.3.2 Per-user command restrictions

Simple Network Management Protocol (SNMP) v3 introduces the capability to restrict use of management information base (MIB) objects on a per-user basis. Where this is to be applied, the set of object identifiers that a given user or user group will be restricted to shall be defined byClient. Refer to section 5.5 Protocol security layer for details on the adoption of these protocols.

2.2.1.3.3 Informative: Safety-critical functions

The highest priority band assigned in the issued lists are strictly reserved for emergency situations. Safety-critical function events such as over-height warnings are typically triggered and managed by a programmable logic controller (PLC) at the roadside, so these local peripheral devices shall be assigned the highest priority. Management stations not assigned this priority should not issue commands at these priority bands except to activate remote safety-critical functions. An example of a remotely activated safety-critical function is wrong-way driver alarms or civil defence emergency notifications, which may override multiple signs to alert drivers to imminent hazards. It should be noted that this is achievable within the defined message priority paradigms, and no further override functions are necessary or permitted.

2.2.1.3.4 Informative: Setter ID

Implementation of priority and arbitration strategies will necessitate capturing the identity of the originating management station. This is facilitated through security protocols covered in section 5.5.1.1 All SNMP communications to employ SNMPv3 security features, and management stations must at all times operate using only the identifier allocated to it. See also section 2.2.2 Monitoring interface for obligation to record the origin of commands.

2.2.1.3.5 Command validity

The primary SNMP communication channel should not be used for functions beyond those defined by datagrams in the ISO 20684 standards or any supplementary MIB issued by Client. Extraneous datagrams should not be actioned or responded to except to notify a management station of the refusal. Note that this requirement applies only when the device is in service and controlled through the ITSN, and maintenance actions are covered in section 4 Design for maintenance.

2.2.1.4 Idle state and blanking a sign face

If not actively displaying a message, a sign display face should be dark and its controller in a state to accept further commands. Devices should enter this state directly when powered on, and this should be the default state of a sign with no immediate message for display.

Deliberate blanking is a special case requiring an explicit note on procedure. Blanking should put a sign back into pool ready for use, and never block further messages. Blanking has in the past been forced by creating an entry in the message table of type blank with high activation and runtime priorities. This is considered bad practice, effectively taking a device out of service until the condition is manually rectified. The standard method for causing a sign to cease displaying a message is to cause its queue of messages for immediate display to be empty such that it enters an idle state. Where the practice of activating a blank message cannot be eliminated, it must always be assigned the lowest possible runtime priority.

2.2.2 Monitoring interface

This section covers supplemental user needs related to ensuring reliable visibility of field device states, and the logging of all actions for transparency and diagnostics.

2.2.2.1 Normal status reporting

Typical operational reports are provided for by SNMP functionality detailed in the ISO 20684 series. Specific logging and reporting needs of Waka Kotahi are detailed in the following subsections.

2.2.2.1.1 Polling

Nominal monitoring of status is to be achieved through polling of field devices at regular intervals. Any combination of the available datagrams provided in the ISO 20684 series may be read as part of this process. Polling is generally intended to capture the status of the device and the currently displayed message, but may include any combination of datagrams defined in the ISO 20684 series.

2.2.2.1.2 Event-driven alerts and notifications

It is desirable for VMS and LCS devices to be capable of generating notifications driven by time-sensitive events. Functionality is defined in ISO/TS 20684-4:2022 *Intelligent transport systems – Roadside modules SNMP data interface – Part 4: Notifications* (ISO/TS 20684-4). Events that are desirable to actively report include:

i. intrusion detection or security violations
ii. temperatures reported by any sensor available to the device that threaten the device or surrounding areas
iii. degraded power supply, or a switch to a battery backup or uninterruptable power supply (UPS) source
iv. damage to or failure of subcomponents, where this can be detected, especially where the condition threatens road safety.

2.2.2.2 All devices to always be in a known state

A VMS or LCS operating in a live environment should be always in a known state. Entering a maintenance, update, self-cleaning or test state or otherwise removing itself from service is acceptable only if the change is intentional and the responsible management stations are aware of the unavailability.

2.2.2.3 Heartbeat

A device should discontinue displaying a message when contact with management stations is lost. The period or number of polling periods without contact before presuming contact lost should be a configurable value on the device. Once the device determines contact has been lost, it should blank its display and return to an idle state (see also section 2.2.1.4 Idle state and blanking a sign face).

3 DESIGN FOR SAFETY

This section defines the core requirements to ensure the ITS can be operated and serviced safely.

This section details needs related to potential to cause harm if an incorrect or distracting message were displayed. It is anticipated that VMS and LCS devices will increasingly be deployed displaying roading signals that carry legal weight and have direct consequences for road safety. It is therefore imperative that command of these devices is tightly controlled and secured against neglectful or malicious actions.

3.1 User needs

3.1.1 Design for safety processes

Any supplier of a VMS or LCS system commissioned for display of road signals with legal standing shall be able to demonstrate their processes in design for safety with regard to preventing unsafe conditions.

3.1.2 Safety-critical functions

Devices with safety-critical applications, such as over-height warnings and wrong-way driver signalling systems, or any other emergency notification, must always prioritise messages serving such time- and/or safety-critical functions. This applies whether these are initiated by a local peripheral or by a remote management station, and should be reflected both in handling prioritisation and operator interfaces.
While this may require assigning highest priority to safety-critical messages, the device must return itself to normal operation once the emergency condition has been lifted. Specific events and management station prioritisation order is reflected in priority assignments detailed in Appendix E: Message priority assignment table.

3.1.3 Continued operation in degraded states

Where a sign performs a safety-critical function, continued operation is desirable under adverse conditions that would otherwise cause the sign to go out of service. This may involve increased tolerances for condition limits and/or continued operation in a degraded state or at reduced capacity. The condition should still be notified to the Client (Waka Kotahi operations team) in the normal way. Where this applies, the device specification will note this and detail the new values or any additional measures needed.

4 DESIGN FOR MAINTENANCE

4.1 Configuration interface user needs

This section supplements the ISO 20684 series by defining user needs related to configuration interfaces.

4.1.1 Principle of remote maintenance

To facilitate the anticipated future scale of deployment of VMS and LCS devices on New Zealand roads, functions for administration, configuration, diagnostics and software maintenance are to be served remotely. Once a device is operational, the channel for these functions is to be the ITSN.

4.1.2 Proprietary administration software dependencies not acceptable

The long lifespans of VMS and LCS devices pose a high risk of deprecated platforms limiting functionality and future compatibility. Reliance on specific software platforms such as proprietary applications or features of these platforms is not acceptable unless a departure has been granted.

All VMS and LCS devices on the road network shall be configurable without dependence on proprietary software beyond the device itself. Configuration must be accessible using typically common devices and software, either self-contained such as a device-hosted web portal or through an open and well-defined application programming interface (API) approved by the Client. Reliance on proprietary hardware or software external to the device itself is not acceptable unless a departure has been granted.

4.1.3 Administration API

If an API is furnished for administration of devices beyond what functionality is offered by the ISO 20684 series, it shall be made compatible with a library of functions to be issued by the Client. Such an API is not currently a requirement but is considered desirable for future integration. A library of functions is not yet issued but will be made available in the ITS document library.

4.1.4 Supplier reporting systems permitted but limited

Suppliers may have their devices report telemetry and usage statistics for the exclusive purpose of supporting continuing development and quality of service analysis. However, any such traffic including telemetry-only reporting will only be routed through the Client nominated networks where a departure from this standard has been granted. It will be a requirement of a departure that any such reporting shall never conflict with the operational interfaces of the device, nor be capable of command or configuration of the device, and never cause the device to enter unknown or uncontrolled states.

4.1.5 Device-specific configurations

Certain configuration requirements specific to a device or device type – such as temperature alarms, thresholds for serviceability, or other non-generic limitations – may be detailed and issued as part of the acquisitions process. Where this is the case, the acquisitions process documents shall list the relevant conformance table entries to be considered mandatory. Note that this is in addition to any conformance table entries modified by Appendix C: Conformance matrix supplement.

4.2 Logging and reporting requirements

4.2.1 Logs to be kept

Devices shall generate, store, and expose logs. The paragraphs of this section outline the needs and purpose for the collection of data categories, and classes of data required to be recorded and exposed are detailed in Appendix D: Logging data.

4.2.2 Consultant to provide complete definitions of all logging codes

Beyond the requirements of section 4.2.1, any additional logs or fault codes that a device may generate shall be defined in full to Waka Kotahi by consultant at time of acquisition or application for the purposes of maintenance and forensics.

4.2.3 Enhanced logging requirements

Supplemental to logging requirements given in the section titled Internal logging requirement in the latest version of ITS delivery specification: Variable message signs – fixed, any changes to device status, display, or any configuration variable must be recorded, whether resulting from an external command or internal logic. Note that this requirement goes beyond recording changes to status or fault conditions.

4.2.3.1 Recording of all commands

Further, any authenticated command received by a VMS or LCS device – whether actioned or not – should be logged, including an identifier of the issuing entity. This requirement relates to capturing attempts to control the sign. Refer to section 5 Design for security for more information.

4.2.3.2 Retrieval of logs

All logs must be both recorded locally and retrievable remotely by a central management system in accordance with ISO/TS 20684-5:2022 *Intelligent transport systems – Roadside modules SNMP data interface – Part 5: Logs* (ISO/TS 20684-5).

4.2.4 Message persistence for debugging

It is desirable for diagnostic and debugging purposes that a history of messages displayed by a device be retained and visible to operators and maintainers, whether through the on-device storage of messages or another reporting channel. It would be sufficient where logging functions capture enough detail to recreate the message and its configuration, or for a message stack to preserve messages in a rolling fashion after they have been deactivated. At present, this function is optional.

5 DESIGN FOR SECURITY

This section defines the core requirements to ensure the ITS can be secured and maintain integrity.

A layered approach to hardening devices and the network against attack is adopted in this section. General guidance for securing communications systems is offered in the *New Zealand information security manual* (NZISM). Specific requirements for the deployment of these security features are defined here.

5.1.1 Threats and countermeasures

The key threat identified is of unauthorised access to the ITSN. Unauthorised control over a single sign is a safety risk, and access to multiple signs increases the risk exponentially. Message stream modification is considered a threat but involves a more sophisticated attack. Disclosure of command messages are a concern in their potential to inform attempts to gain unauthorised access. Denial of Service is also a threat, particularly critical for LCS, which must maintain high availability. Malformed requests may also cause unintended behaviour.

Suitable countermeasures depend on the available techniques and complexity of implementation, but as a general guide, usernames transmitted in cleartext are inadequate. A VMS or LCS device should accept commands only when verified at the device using an accepted hashed message authentication code (HMAC) or else through an otherwise end-to-end encrypted channel. In this way, a device not capable of HMAC methods might be made compliant by securing communication at the transport layer. Note that this does not mandate the use of transport encryption, although its use is recommended wherever possible.

5.2 General security principles

5.2.1 Default credentials to be changed

Any default credential shall be changed on receipt by Client to meet complexity requirements as defined by Waka Kotahi Security.

5.2.2 Device configuration hardening

Devices should be hardened to relevant Center for Internet Security (CIS) benchmark standards, and in compliance with AS ISO/IEC 27002:2015 *Information technology – Security techniques – Code of practice for information security controls* (AS 27002), unless a departure has been granted by Waka Kotahi to accept an equivalent standard.

5.3 Physical security layer

Requirements for the physical security layer are defined in ITS delivery specification: Variable message signs – fixed.

5.4 Network security layer

Although significant portions of the communications network consist of fibre-optic connections owned and maintained by Waka Kotahi, it is inevitable that exposure should occur where services and providers require access to these facilities, and where it is necessary to interface with other networks. It is also inefficient to preclude the use of national and commercial wide area network (WAN) facilities. For these reasons, a closed network should not be expected.

However, network layer controls in the form of jump hosts and gateways, virtual private networks and tunnelling should be deployed where possible. Specific deployment requirements are not exhaustively covered here due to the variety of capabilities involved but shall align with practices described in the most recently released version of the NZISM, to the satisfaction of Waka Kotahi.

5.4.1 Security conditions and obligations

5.4.1.1 Configuration traffic on the network to be logged

Normal operating traffic notwithstanding, all configuration activity including connection attempts shall be logged and the logs forwarded to a central repository for the purposes of performance assessment, anomaly detection, and forensics. Refer to section 4.2 Logging and reporting requirements for more detail.

5.4.1.2 Local control to be through local network switch

Where commissioning and maintenance activity performed on site requires issuing device commands, this should be done using the normal network interface by connecting a management workstation to the local networking switch. The intent is to preserve normal operating, logging, and security procedures for all actions wherever possible. Actions performed by any party directly on the sign control systems should be as a last resort and must always be logged.

At the completion of commissioning or maintenance activity, any roadside access to the ITSN other than for the device itself shall be disabled.

5.4.1.3 Unused WAN ports to be secured

As a general precaution, networking ports of field devices should be closed to all traffic when not used in operations or maintenance.

5.4.1.4 Unused wireless capabilities to be disabled

Unless explicitly called for in device specifications, wireless transport layers shall be disabled on all fixed roadside VMS and LCS devices unless a departure has been granted by Waka Kotahi.

5.4.1.5 Additional network connections not permitted

Devices may not be connected to communication networks other than the ITSN unless a departure has been granted by Waka Kotahi.

5.5 Protocol security layer

The ISO 20684 series and NTCIP 1203 v03 section 2.6 Security explicitly decline to address network security, directing system integrators to implement security features at the communications protocol level. This section addresses expected general standards of authentication and cryptographic methods, and defines certain protocol-specific conditions.

5.5.1 Security conditions and obligations

5.5.1.1 All SNMP communications to employ SNMPv3 security features

Version 3 of the SNMP standard offers a suite of security features. Use of these features shall be mandatory for SNMP communication with all roadside devices.

The architecture of the SNMP framework was designed with mutually independent definitions of management information and the protocols. This foresightful structure allows the adoption of security enhancements offered by SNMPv3 with minimal requirement to redefine management information. Migration between versions is described in RFC 3584.

The recommended profile is Authentication and Privacy (`authPriv`), whereby both the authorisation elements and the packet payloads are encrypted. Although there are no privacy conditions on the content of these packets, their content can inform attacks. Encryption of authentication elements (`AuthNoPriv`) should be considered the minimum acceptable standard, but the objective should always be the highest security configuration achievable.

5.5.1.2 SFTP to replace FTP

Where File Transfer Protocol (FTP) was used previously, it shall now be a requirement to deploy Secure File Transfer Protocol (SFTP) with strong ciphers at or above Transport Layer Security (TLS) 1.2 standard or later. Certificate management is to be administered by Waka Kotahi Security.

5.5.1.3 Web portals to be served over Hypertext Transfer Protocol Secure (HTTPS) with TLS 1.2+

Robust modern security protocols for service of device-hosted configuration portals shall be mandated by Waka Kotahi Security. Waka Kotahi Security will issue the most current and case-specific requirements.

6 APPENDIX A – DEFAULT FONTS

6.1 Fonts for use with VMS and LCS devices

The default font must comply with the font standard in ITS core requirements standard: Electronic message signage fonts. This should be stored in the primary font slot [fo1], should default to centre-justified and shall overwrite any existing defaults or fonts.
Note: All non-standard fonts must be removed from the sign before testing and commissioning.

More than one font set may be prescribed depending on the application. An example of the arrangement is given in Table 1.

Index	Function	Description
[fo1]	Default and primary font	General use font, sized to match display face dimensions and best match TCD requirements
[fo2]	Secondary font	Special use font, sized to match display face dimensions and best match TCD requirements
[fo3]	Variable signal font, light on dark	For overlay on graphics to form variable signals
[fo4]	Variable signal font, dark on light	For overlay on graphics to form variable signals
	…	

Table 1. Example font assignment table

7 APPENDIX B – DEFAULT GRAPHICS LIBRARY

7.1 Default graphics library for use with VMS and LCS devices

The single source of truth for sign and signal graphics on New Zealand roads is the *Traffic control devices manual* (TCD manual) or, until replaced, the *Manual of traffic signs and markings (MOTSAM) – Part 1: traffic signs*. The rendering of signs and signals defined in those manuals by their appearance and dimensions depends on the capabilities of individual devices. Therefore, entries in the standard graphics library are prescribed only by their assigned slot number (`dmsGraphicNumber`) and their functional purpose, which can be related to entries in the TCD manual. Table 2 gives an example standard graphics assignment table. Appropriate adjustments such as light/dark inversion may also be detailed. In this way, a reliable selection can be made by operators of the correct forms of each sign or signal, and flexibility is preserved for various device attributes and future changes in the TCD manual.

Once identified, graphics definitions from the TCD manual are to be converted to raster images to best meet the capabilities of the individual display device, accounting for variations in attributes such as physical dimensions, resolution, and colour capabilities. Provided the storage capacity given in device specifications and the capability to store and display graphics in accordance with other parts of this core requirements standard is met, it is sufficient for device suppliers to provide the file attributes (and optionally, tools) necessary for appropriate graphics files to be generated by Waka Kotahi for loading onto the device. Required storage capacity should be inferred from the latest version of these specifications or any device specifications issued during acquisition processes but shall be not less than 255 slots at the resolution relevant to the device.

7.1.1 File-naming convention

Once generated, filenames for graphics shall follow a labelling convention giving `dmsGraphicNumber`, function, colour palette, and resolution. For example, if a light-on-dark variable speed limit graphic is to be assigned to slot G50 on a VMS, the file should be labelled

```
<height> <width> G50_speed_limit_dark
```

Graphics files are then to be loaded onto signs, assigned with the correct `dmsGraphicNumber` for its purpose. Then at time of use, a graphic would be called in the usual way with a MULTI tag reference as part of a message definition, along with any other message elements such as beacon graphics (wig-wag) or text. Where text numerals are overlaid on graphics – for example, to form changeable speed signs – the font, size and position of numerals should be configured for display to best match the font standard in ITS core requirements standard: Electronic message signage fonts.

Index	Function	Description	TCD Rule
Gxx	Speed limit frame, light on dark	Standard speed limit background frame on a dark background	R1-2-1
Gxx	Speed limit frame, 2/3 width	For use in sequencing of pulse effect	R1-2-1-pulse-2
Gxx	Speed limit frame, 1/3 width	For use in sequencing of pulse effect	R1-2-1-pulse-1
…			

Table 2. Example standard graphics assignment table (see Appendix F for LCS standard configuration)

8 APPENDIX C – CONFORMANCE SCHEDULE SUPPLEMENT

8.1 Conformance schedule supplement

To be developed for future use - The conformance schedule in Table 3 will lay out additional compliance requirements for VMS and LCS communication and shall be additional to or override specific entries in the conformance matrices found throughout the ISO 20684 series of standards. Only additions or exceptions to ISO 20684 conformance matrices will be listed here – for example, to override the status of a specific requirement from mandatory to optional. Otherwise, the conformance matrices found in the Conformance section of ISO 20684 series documents apply as printed.

Section or reference	Description	Conformance to read
Nil	No current conformance schedule supplements.	–

Table 3. Conformance schedule supplement

9 APPENDIX D – LOGGING DATA

9.1 Data elements of interest

Core logging requirements are listed as data disciplines in Table 4, accompanied by an indication of the conformance requirement of each discipline. Note that this represents a subset of the data disciplines given in NTCIP 1203 v03 section 3.5.3.1.2 Provide General DMS Error Status Information, and relevant and applicable datagrams can be derived from that document.

Discipline	NTCIP Functional Requirement ID	Description	Conformance
System errors	3.5.3.1.3.5	Errors in controller software	Optional (O)
Subsystem errors	3.5.3.1.4	Errors in peripherals and subsystems	Mandatory (M)
Power supply errors	3.5.3.1.4.1	Power system errors	M
	3.5.3.1.3.1	Monitor power errors	M
Networking events	TBC	Network errors	M
Environmental information	3.5.3.1.3.4	Light sensor errors	M
	3.5.3.1.3.7	Temperature threshold exceptions	M
	3.5.3.1.3.8	Humidity threshold exceptions, if humidity sensors present	M
	3.5.3.1.7	Ambient temperature monitoring	O
Climate control	3.5.3.1.4.6	Climate-control systems error, if system present	O
Display errors	3.5.3.1.4.3	Pixel errors	M
		Beacon errors	O
Physical security events	3.5.3.1.3.10	Door status	M
Message errors	3.5.3.1.4.5	`dmsActivateMsgError`, `dmsValidateMessageError`	O
Message history	TBC	See section 4.2.4 Message persistence for debugging	O

Table 4. Data elements of interest for logging of events

10 APPENDIX E – MESSAGE PRIORITY ASSIGNMENT TABLE

10.1 Message priority assignment table

Table 5 outlines the approach and nominal bands but is subject to change. Note that this approach requires no modification of device software or protocols – these are operational procedures, and for control software.

Priority range	Class – Purpose	Subclasses – User band		Notes
Highest priority				
225 to 255	Reserved	255	Reserved	A band of priorities are kept at the highest level for future use, and to permit override actions.
		225–254	To be assigned	
194 to 224	Safety critical	214–224	Local control	Safety-critical actions, typically generated by local devices or peripherals, but may also be ordered by remotely co-ordinated actions such as wrong-way driver alarms.
		194–214	To be assigned	
163 to 193	Traffic control	163–193	To be assigned	Mandatory signals, such as speed or lane control.
132 to 162	Civil defence (reserved)	132–162	To be assigned	Future use of signs to support civil defence such as recent flooding events.
101 to 131	Incident message	101–131	To be assigned	Incident management, non-emergency, typically executed by TOC Operator manually or as part of a pre-defined plan.
70 to 100	Driver caution or advisory	70–100	To be assigned	Non-urgent safety information. Messages notifying drivers of factors influencing road safety on the corridor ahead, such as conditions, road quality, or events.
39 to 69	Driver information message	44–69	To be assigned	Travel time messages, future road closures, works notifications, etc.
		39–44	Travel information manager (TIM)	
8 up to 38	Campaign message	8–38	To be assigned	Waka Kotahi safety awareness campaigns.
0 to 7	Idle	5–7	To be assigned	Sign must always return to blank and idle state when message queue is finished, or message times out. Low-priority test messages may also use this band.
		1–5	Test messages	
		0	0 Reserved	
Lowest priority				

Table 5. Nominal message priority assignments by purpose and user category

11 APPENDIX F – LCS STANDARD CONFIGURATION

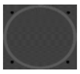
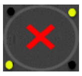
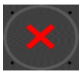
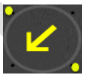
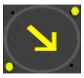
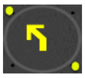
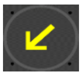
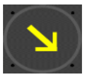
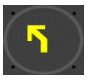
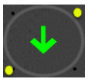
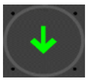
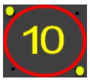
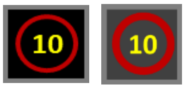
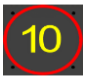
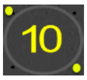
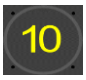
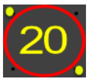
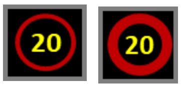
The default font must comply with the font standard in ITS core requirements standard: Electronic message signage fonts. This should be stored in the primary font slot [fo1], should default to centre-justified and shall overwrite any existing defaults or fonts.

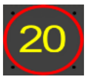
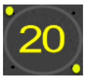
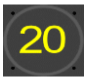
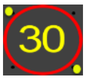
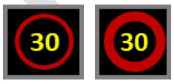
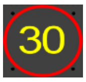
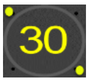
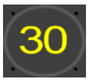
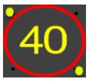
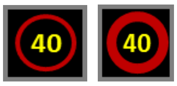
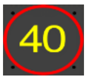
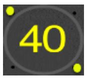
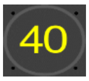
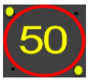
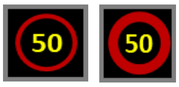
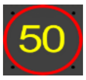
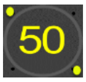
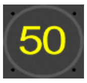
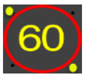
Note: All non-standard fonts must be removed from the sign before testing and commissioning.

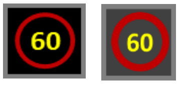
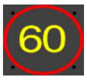
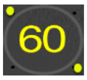
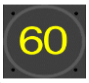
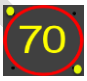
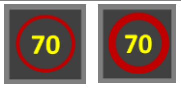
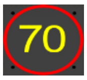
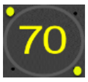
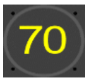
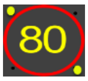
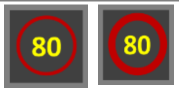
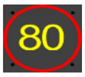
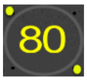
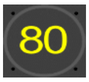
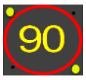
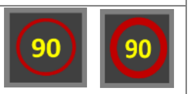
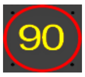
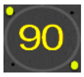
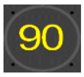
Aspect	NTCIP Graphics Name	Generic File Name
red_X	G190X	<height>_<width>_G190_red_X.bmp
red_X_wig	G189XWIG	<height>_<width>_G189_red_X_wig.bmp
red_X_wag	G188XWAG	<height>_<width>_G188_red_X_wag.bmp
red_roundel_full	G187RFUL	<height>_<width>_G187_red_roundel_full.bmp
red_roundel_1-3	G186R1-3	<height>_<width>_G186_red_roundel_1-3.bmp
red_roundel_wig	G185RWIG	<height>_<width>_G185_red_roundel_wig.bmp
red_roundel_wag	G184RWAG	<height>_<width>_G184_red_roundel_wag.bmp
divert_arrow_left	G183L	<height>_<width>_G183_divert_arrow_left.bmp
divert_arrow_left_wig	G182LWIG	<height>_<width>_G182_divert_arrow_left_wig.bmp
divert_arrow_left_wag	G181LWAG	<height>_<width>_G181_divert_arrow_left_wag.bmp
divert_arrow_right	G180R	<height>_<width>_G180_divert_arrow_right.bmp
divert_arrow_right_wig	G179RWIG	<height>_<width>_G179_divert_arrow_right_wig.bmp
divert_arrow_right_wag	G178RWAG	<height>_<width>_G178_divert_arrow_right_wag.bmp
exit_left	G177E	<height>_<width>_G177_exit_left.bmp
exit_left_wig	G176EWIG	<height>_<width>_G176_exit_left_wig.bmp
exit_left_wag	G175EWAG	<height>_<width>_G175_exit_left_wag.bmp
ahead_arrow	G174A	<height>_<width>_G174_ahead_arrow.bmp
ahead_arrow_wig	G173AWIG	<height>_<width>_G173_ahead_arrow_wig.bmp
ahead_arrow_wag	G172AWAG	<height>_<width>_G172_ahead_arrow_wag.bmp
blank_beacons_wig	G171BLKWIG	<height>_<width>_G171_blank_beacons_wig.bmp
blank_beacons_wag	G170BLKWAG	<height>_<width>_G170_blank_beacons_wag.bmp
	…	

Table 6. LCS Aspects and Graphic File Names

11.1 Message priorities for use with LCS devices

DYNAC Internal Priority	Message	Expected Message MULTI String	ACTIVATION Priority	RUNTIME Priority	Illustration
0	Blank		TBC	190	
2	Close Beacons	[pt10o0][g189][np][g188]	TBC	189	
3	Close	[g190]	TBC	188	
4	Divert Left Beacons	[pt10o0][g182][np][g181]	TBC	187	
4	Divert Right Beacons	[pt10o0][g179][np][g178]	TBC	187	
4	Lane Exit Left Beacons	[pt10o0][g176][np][g175]	TBC	187	
5	Divert Left	[g183]	TBC	186	
5	Divert Right	[g180]	TBC	186	
5	Lane Exit Left	[g177]	TBC	186	
8	Green Arrow Beacons	[pt10o0][g173][np][g172]	TBC	185	
9	Green Arrow	[g174]	TBC	184	
10	Speed Limit 10 Annulus Beacons	[pt10o0][g185]10[np][g184]10	TBC	183	
10	Speed Limit 10 Rondel Flash	[pt10o0][g187]10[np][g186]10	TBC	183	
11	Speed Limit 10 Annulus	[g187]10	TBC	182	
12	Speed Limit 10 Beacons	[pt10o0][g171]10[np][g170]10	TBC	181	
13	Speed Limit 10	10	TBC	180	
14	Speed Limit 20 Annulus Beacons	[pt10o0][g185]20[np][g184]20	TBC	179	
14	Speed Limit 20 Rondel Flash	[pt10o0][g187]20[np][g186]20	TBC	179	

DYNAC Internal Priority	Message	Expected Message MULTI String	ACTIVATION Priority	RUNTIME Priority	Illustration
15	Speed Limit 20 Annulus	[g187]20	TBC	178	
16	Speed Limit 20 Beacons	[pt10o0][g171]20[np][g170]20	TBC	177	
17	Speed Limit 20	20	TBC	176	
18	Speed Limit 30 Annulus Beacons	[pt10o0][g185]30[np][g184]30	TBC	175	
18	Speed Limit 30 Rondel Flash	[pt10o0][g187]30[np][g186]30	TBC	175	
19	Speed Limit 30 Annulus	[g187]30	TBC	174	
20	Speed Limit 30 Beacons	[pt10o0][g171]30[np][g170]30	TBC	173	
21	Speed Limit 30	30	TBC	172	
22	Speed Limit 40 Annulus Beacons	[pt10o0][g185]40[np][g184]40	TBC	171	
22	Speed Limit 40 Rondel Flash	[pt10o0][g187]40[np][g186]40	TBC	171	
23	Speed Limit 40 Annulus	[g187]40	TBC	170	
24	Speed Limit 40 Beacons	[pt10o0][g171]40[np][g170]40	TBC	169	
25	Speed Limit 40	40	TBC	168	
26	Speed Limit 50 Annulus Beacons	[pt10o0][g185]50[np][g184]50	TBC	167	
26	Speed Limit 50 Rondel Flash	[pt10o0][g187]50[np][g186]50	TBC	167	
27	Speed Limit 50 Annulus	[g187]50	TBC	166	
28	Speed Limit 50 Beacons	[pt10o0][g171]50[np][g170]50	TBC	165	
29	Speed Limit 50	50	TBC	164	
30	Speed Limit 60 Annulus Beacons	[pt10o0][g185]60[np][g184]60	TBC	163	

DYNAC Internal Priority	Message	Expected Message MULTI String	ACTIVATION Priority	RUNTIME Priority	Illustration
30	Speed Limit 60 Rondel Flash	[pt10o0][g187]60[np][g186]60	TBC	163	
31	Speed Limit 60 Annulus	[g187]60	TBC	162	
32	Speed Limit 60 Beacons	[pt10o0][g171]60[np][g170]60	TBC	161	
33	Speed Limit 60	60	TBC	160	
34	Speed Limit 70 Annulus Beacons	[pt10o0][g185]70[np][g184]70	TBC	159	
34	Speed Limit 70 Rondel Flash	[pt10o0][g187]70[np][g186]70	TBC	159	
35	Speed Limit 70 Annulus	[g187]70	TBC	158	
36	Speed Limit 70 Beacons	[pt10o0][g171]70[np][g170]70	TBC	157	
37	Speed Limit 70	70	TBC	156	
38	Speed Limit 80 Annulus Beacons	[pt10o0][g185]80[np][g184]80	TBC	155	
38	Speed Limit 80 Rondel Flash	[pt10o0][g187]80[np][g186]80	TBC	155	
39	Speed Limit 80 Annulus	[g187]80	TBC	154	
40	Speed Limit 80 Beacons	[pt10o0][g171]80[np][g170]80	TBC	153	
41	Speed Limit 80	80	TBC	152	
42	Speed Limit 90 Annulus Beacons	[pt10o0][g185]90[np][g184]90	TBC	151	
42	Speed Limit 90 Rondel Flash	[pt10o0][g187]90[np][g186]90	TBC	151	
43	Speed Limit 90 Annulus	[g187]90	TBC	150	
44	Speed Limit 90 Beacons	[pt10o0][g171]90[np][g170]90	TBC	149	
45	Speed Limit 90	90	TBC	148	

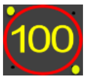
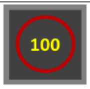
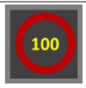
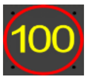
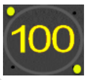
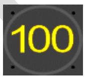
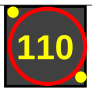
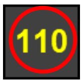
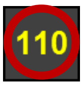
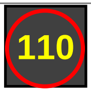
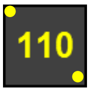
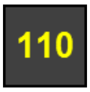
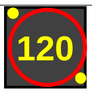
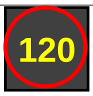
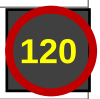
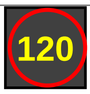
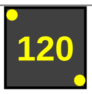
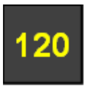
DYNAC Internal Priority	Message	Expected Message MULTI String	ACTIVATION Priority	RUNTIME Priority	Illustration
46	Speed Limit 100 Annulus Beacons	[pt10o0][g185]100[np][g184]100	TBC	147	
46	Speed Limit 100 Rondel Flash	[pt10o0][g187]10[np][g186]100	TBC	147	 
47	Speed Limit 100 Annulus	[g187]100	TBC	146	
48	Speed Limit 100 Beacons	[pt10o0][g171]100[np][g170]100	TBC	145	
49	Speed Limit 100	100	TBC	144	
50	Speed Limit 110 Annulus Beacons	[pt10o0][g185]110[np][g184]110	TBC	143	
50	Speed Limit 110 Rondel Flash	[pt10o0][g187]11[np][g186]110	TBC	143	 
51	Speed Limit 110 Annulus	[g187]110	TBC	142	
52	Speed Limit 110 Beacons	[pt10o0][g185]110[np][g184]110	TBC	141	
53	Speed Limit 110	110	TBC	140	
54	Speed Limit 120 Annulus Beacons	[pt10o0][g185]120[np][g184]120	TBC	139	
54	Speed Limit 120 Rondel Flash	[pt10o0][g187]12[np][g186]120	TBC	139	 
55	Speed Limit 120 Annulus	[g187]120	TBC	138	
56	Speed Limit 120 Beacons	[pt10o0][g185]120[np][g184]120	TBC	137	
57	Speed Limit 120	120	TBC	136	
…					

Table 7. LCS Message Priorities

12 TERMINOLOGY USED IN THIS DOCUMENT

Term	Definition
DRAFT	The document is being written and cannot be used outside of NZTA.
PENDING	The document has been finalised and is pending approval and ratification by NZTA. It can be used for procurement at this status.
RATIFIED	The document is an official NZTA document. NZTA projects and other road controlling authorities connected to NZTA back-end systems must include this document in the contracts. The obligation to follow the requirements in this document would come from the inclusion of the S&S document in the contract.
RETIRED	The document is obsolete, and/or superseded.
NZTA	This is noted as being equivalent to the New Zealand Transport Agency.
API	Application programming interface
AS	Australian standard
CIS	Center for Internet Security
DES	Data Encryption Standard
Field device	Generic term for any collection of roadside units for the display of messages, including a single display and its controllers, and any additional connected peripherals
FTP	File Transfer Protocol
HMAC	Hashed message authentication code
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO/TS	International Organization for Standardization technical specification
ITS	Intelligent transport systems
ITSN	ITS Network, the communications network established and controlled by NZTA
LCS	Lane and carriageway sign, a subset of VMS but explicit distinction is made in this document
Manager	Generic term for any person or system interacting with a field device through interfaces specified in this document. These may or may not be located remote from the sign.
MD5	Message Digest Algorithm 5
MIB	Management information base
MOTSAM	*Manual of traffic signs and road marking*
MULTI	Markup language for transportation information
NTCIP	National Transportation Communications for ITS Protocol
NZISM	*New Zealand information security manual*

Term	Definition
PLC	Programmable logic controller
RFC	Request for Comments document (published by IETF)
RGB	Red-green-blue (colour model based on additive colour primaries)
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell (Protocol)
TCD	Traffic control devices
TIM	Travel information manager
TLS	Transport Layer Security
TOC	Transport operations centre
UTF-8	Unicode Transformation Format – 8-bit
UPS	Uninterruptable power supply
VMS	Variable message sign, including its control systems
WAN	Wide area network

13 REFERENCES

This section lists all external and Waka Kotahi references included in this document.

13.1 Industry standards

Standard number/name
AS ISO/IEC 27002:2015 Information technology – Security techniques – Code of practice for information security controls
IETF RFC 3584 Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
ISO 20684 series – ITS roadside modules SNMP data interface
ISO 20684-1:2021 Intelligent transport systems – Roadside modules SNMP data interface – Part 1: Overview
ISO/TS 20684-4:2022 Intelligent transport systems – Roadside modules SNMP data interface – Part 4: Notifications
ISO/TS 20684-5:2022 Intelligent transport systems – Roadside modules SNMP data interface – Part 5: Logs
ISO/TS 20684-10:2021 Intelligent transport systems – Roadside modules SNMP data interface – Part 10: Variable message signs
NTCIP 1203 v03 National Transportation Communications for ITS Protocol – Object definitions for dynamic message signs (DMS)
New Zealand information security manual (NZISM) v3.5

13.2 Waka Kotahi standards, specifications and resources

13.2.1 Standards and specifications

See the Waka Kotahi website for the latest versions of the ITS S&S documents listed below.

Document name
ITS core requirements standard: Electronic message signage fonts
ITS delivery specification: Variable message signs – Fixed

13.2.2 Resources

Document name/code
Traffic control devices manual (TCD manual)
Manual of traffic signs and markings (MOTSAM) – Part 1: traffic signs

13.3 ITS standard drawings

See the Waka Kotahi website for the latest versions of the ITS standard drawings listed below.

Drawing number
Nil

14 CONTENT TO BE REDIRECTED

This section records any circumstances where content from this document will be reclassified and moved into future documents. This table is then updated with a reference to the new location.

Section reference	Section name	Future document	Class

15 DOCUMENT CONTROL

15.1 Document information

Document number	ITS-STND-VLSI-202409
Previous document number/s (if applicable)	
Document status	FINAL DRAFT
[IF RETIRED] New document details	
Online ISBN	
Document availability	The controlled version of this document can be accessed from https://www.nzta.govt.nz/roads-and-rail/intelligent-transport-systems/standards-and-specifications/its-current-interim-and-legacy-standards-and-specifications

15.2 Document owner

Role	ITS S&S Steering Committee
Organisation	NZTA

15.3 Document approvers

This table shows a record of the approvers for this document.

Approval date	Approver	Role	Organisation
DD/MM/YYYY			

16 FULL VERSION HISTORY

This table shows the full history of changes made to this document, both minor and major, in chronological order, since the document was first authored.

Minor versions are numbered 0.1, 0.2 etc until such point as the document is approved and published, then it becomes 1.0 (major version). Subsequent edited versions become 1.1, 1.2 etc, or if it's a major update 2.0, and so on.

Version	Date	Author	Role and organisation	Reason
0.1	27/10/2022	Simon Allen	Author, Beca Ltd	For initial comments
0.2	23/02/2023	Simon Allen	Author, Beca Ltd	Panel comments actioned
0.3	03/03/2023	Russell Pinchen and Anandita Pujara	Waka Kotahi	Added details to appendix A to E and updated document name
0.4	12/04/2023	Simon Allen	Author, Beca Ltd	Updated as per industry feedback
0.5	14/04/2023	Matthew Bauer	Editor, Clear Edit NZ	Copyedit
0.6	19/04/2023	Simon Allen	Author, Beca Ltd	Review copyedited draft
0.7	21/04/2023	Matthew Bauer	Editor, Clear Edit NZ	Proofread final draft
0.8	10/05/2023	Anandita Pujara	Document Manager, Waka Kotahi	Updated as per Technical Standards Committee's feedback
0.9	6/07/2023	Anandita Pujara	Document Manager, Waka Kotahi	Updated to clarify the contractual roles as per ratification group's feedback
0.10	18/01/2023	Anandita Pujara	Document Manager, Waka Kotahi	Updated as per further comments from RG
0.11	20/09/2024	Brenda Fitzgerald	Senior Business Analyst, NZTA	Updated Appendix A, B,C,D,E,F