WAKA KOTAHI
NZ TRANSPORT AGENCY

VARIABLE MESSAGE SIGNS AND LANE AND CARRIAGEWAY SIGNS SYSTEM INTERFACE STANDARD

ITS Core Requirements Standard

3 MARCH 2023
0.3

New Zealand Government

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

Waka Kotahi 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 Waka Kotahi.

More information
If you have further queries, contact the ITS S&S team via email: itsspec@nzta.govt.nz

More information about intelligent transport systems (ITS) is available on the Waka Kotahi website at https://www.nzta.govt.nz/its

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

Template version
1.8, 03/11/2021

Contents

List of figures

List of tables

1 DOCUMENT CONTROL

1.1 Document information

Document number	ITS-01-012-YYYYMM-STD-VLSI
Previous document number/s (if applicable)	
Document status DRAFT | PENDING | RATIFIED | RETIRED	DRAFT
[IF RETIRED] New document details	
Online ISBN number	
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

1.2 Document owner

Role Head of Technology Engineering

Organisation Waka Kotahi

1.3 Document approvers

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

Approval date	Approver	Role	Organisation
DD/MM/YYYY			

1.4 Version history – major changes

Document version control is the process of tracking and managing different versions (or drafts) of a document to easily identify the current iteration of a file.

This table shows a record of all major (published) versions of this document (for Waka Kotahi use only). To record minor versions (author updates, amendments etc), go to section 15 Full version history.

Version	Date	Author	Role and organisation	Reason
0.1	DD/MM/YYYY			
0.2	DD/MM/YYYY			
0.3	DD/MM/YYYY			

Table 1. Example of a sequentially numbered table caption

2 TERMINOLOGY USED IN THIS DOCUMENT

Term	Definition
DRAFT	The document is being written and cannot be used outside of Waka Kotahi.
PENDING	The document has been finalised and is pending approval and ratification by Waka Kotahi. It can be used for procurement at this status.
RATIFIED	The document is an official Waka Kotahi document. Road controlling authorities are obliged to follow a document with this status.
RETIRED	The document is obsolete, and/or superseded.
API	Application Programming Interface
C2F	Refers to communication from a Centre node to a Field node
C2X	Refers to communication from a Centre node to any node
DES	Data Encryption Standard
F2C	Refers to communication from a Field node to a Centre node
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
ITS	Intelligent transport systems
ITSN	ITS Network, the communications network established and controlled by Waka Kotahi
LCS	Lane and Carriageway Signs, 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
MULTI	Markup language for transportation information
RFC	Request For Comments document – published by the Internet Engineering Task Force
SHA	Secure Hash Algorithm
SSH	Secure Shell
UTF-8	Universal coded character set Transformation Format – 8-bit
VMS	Variable Message Sign, including its control systems.
WK	Waka Kotahi
WAN	Wide area network

3 OVERVIEW AND OUTCOMES

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

3.1 Purpose

This document defines expected practices in control interfaces with all electronic messaging and signalling equipment that are connected to Waka Kotahi networked systems to deliver information to users on the national road network. The intent is a balanced standard which 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 document 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 Signs (VMS) and Lane and Carriageway Signs (LCS) field devices when operational on the ITSN. This is supplemented by additional user needs specific to Waka Kotahi systems, and application notes on expected behaviours for certain functions.

3.2 Overview

This document 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, Waka Kotahi 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 document introduces cybersecurity requirements as a fundamental element of interface implementation.

For the purposes of this document, interactions with a VMS or LCS are categorised into three logical groups;

a) Control of the VMS or LCS
b) Configuration of the VMS or LCS
c) Monitoring of the VMS or LCS

These align with operational features detailed in National Transportation Communications for ITS Protocol NTCIP 1203 v03 Section 2.5. 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 document according to the Waka Kotahi system design principles.

3.2.1 Waka Kotahi ITS class

012 System interfaces
Class definitions

3.3 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 Waka Kotahi 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. 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 Waka Kotahi Intelligent Transtportation Systems Network (ITSN) or its successors are also excluded. Further, compliance with this document is compulsory for devices or systems which interface with Waka Kotahi systems, but in other cases is for advisory only.

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

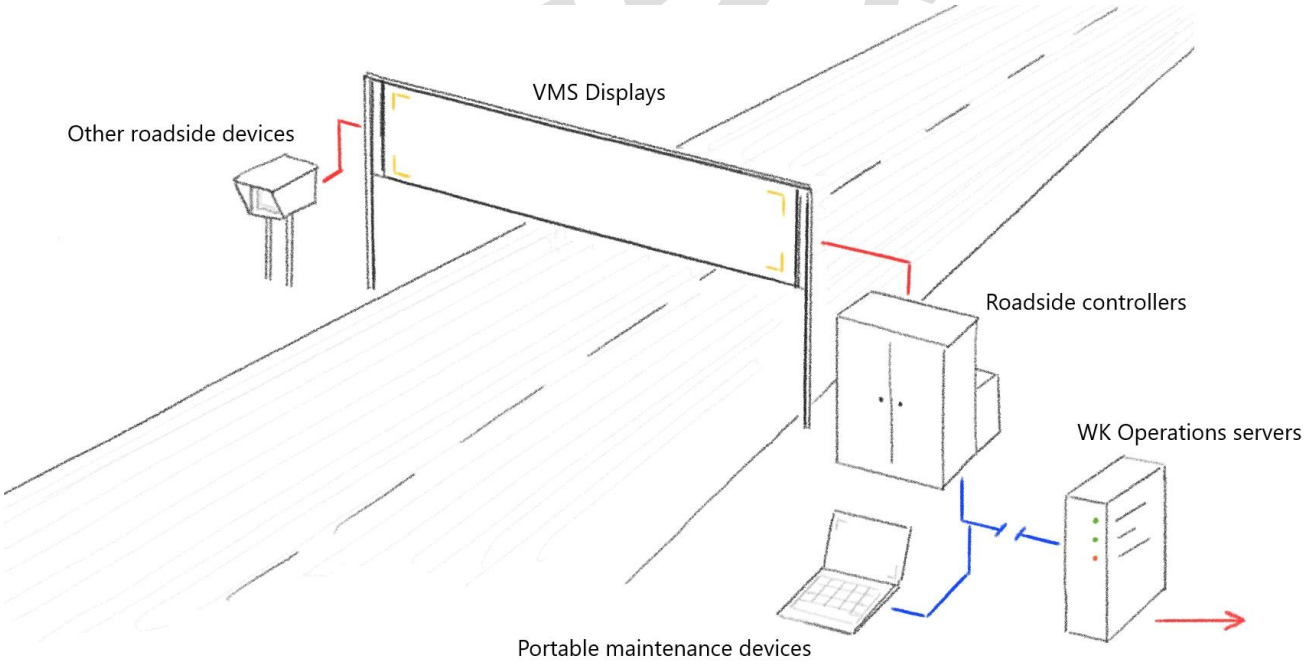

Figure 1. Applicability of this document to network architecture. Only connections shown in blue are covered by this document.

3.4 Outcomes

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

Three critical outcomes are identified.

I. Clearly defined set of commands and data attributes against which functional compliance can be measured.
II. 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.

3.4.1 For road controlling authorities and transport operations centres

This document details a standard communications interface for control, configuration and maintenance of fixed roadside VMS and LCS devices in operation on New Zealand roads. Adopting and supplementing an existing communication standard minimises technical debt and devices can be sourced from wider range of international suppliers, while setting requirements particular to the needs of Waka Kotahi. This document avoids issuing non-functional requirements, allowing vendors flexibility in how the defined needs are met. Where several functions are capable of satisfying a given user need, but where mixed implementation may cause problems, this document specifies the preferred method.

This document does not detail the test procedures to demonstrate compliance, which are issued in test plans published separately in ITS Systems Integration Test Plan ITS-03-001-202104-TEST-VMS-FIXED.

3.4.2 For users of the transport network

This document promotes reliably displaying accurate and timely information to road users for efficiency and safety through consistent central control of all fixed roadside displays. Securing communication and providing a pipeline to verify displays or detect and respond to faults will reduce disruption from distracting or incorrect displays. This standard will also enable the use of macrons and other diacritical marks for correctly rendering words of Te Reo Māori through UTF-8 encoding.

3.4.3 For vendors and system integrators

This standard defines a framework to structure communication with VMS and LCS systems installed on the New Zealand road network. It offers vendors a collection of user needs to be met in tenders and proposals to supply or interact with fixed VMS and LCS systems, and seeks to simplify compliance with acceptance processes. It defines expectations for a set of user needs and their associated behaviours to permit efficiency and consistency in testing, but the test plans themselves are published separately in the ITS Systems Integration Test Plan. This document seeks to balance the rigidity necessary for pre-defined compliance with an allowance for innovation and future technology growth.

4 DESIGN FOR OPERATION

4.1 Devices to demonstrate compliance with ISO 20684 standards

All VMS and LCS devices on the Waka Kotahi 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 ISO 20684-1 Section 5 for details on the Compliance 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 and NTCIP 1203v3, 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 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 not referenced in this way should not be considered mandatory.

Differences between NTCIP 1203 and ISO 20684 are summarised in ISO 20684-10 Annex C.

Supplemental user needs

An extensive set of user needs are defined in Section 7 of each ISO 20684 series standard, with their attendant conformance requirements detailed in Section 5 Conformance of the various parts. Certain additional features are required by Waka Kotahi, which reflect behavioural requirements stemming mostly from matters of integration. This document supplements ISO 20684 series user needs with a further set specific to Waka Kotahi systems, detailed in the following subsections.

4.2 Control and Monitoring Interface User Needs

4.2.1 Control Interface

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

4.2.1.1 Default Fonts

A set of fonts will be defined by Waka Kotahi in the Electronic message signage fonts standard (ITS-01-001-YYYYMM-STD-FONT). All messages should be displayed in these suppliedfonts. 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 5.4.2 Font Table Parameters). Where it is not possible to replace any default fonts loaded in non-volatile, non-changeable memory, selection keys Default fonts are to be specified using UTF-8 encoding as mandated by ISO 20684-10 and will include vowels with macrons for the correct rendering of Reo Māori.

4.2.1.2 Standard graphics

A standardised list of graphics will be defined by Waka Kotahi for each installation, which are to be stored on the device in a specified order and with known reference keys. Required storage capacity should be inferred

from the latest version of these specifications. Graphics shall be defined by their physical attributes, leaving rasterization to best utilise the capabilities of the display. Visual attributes of graphics as displayed by a device shall comply with the relevant sign specifications given in Appendix B Default Graphics Required storage capacity should be inferred from the latest version of these specifications.
A method shall be provided by which Waka Kotahi may update the stored graphics. Refer to section 6.2 Configuration Interface. At minimum, a vendor must detail the necessary resolution, colour data, file format and any other attributes to enable Waka Kotahi to populate the graphics library to which best match the capabilities of the sign.

4.2.1.3 User-based message control

Priority paradigms established in ISO 20684 Section 8.3.2.6 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.

4.2.1.3.1 Activation and Runtime Priority assignment lists

Waka Kotahi 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 Waka Kotahi 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.

4.2.1.3.2 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 (OID) which a given user or user group will be restricted to shall be defined by Waka Kotahi. Refer to Section 7.5 Protocol Security Layer for details on the adoption of these protocols.

4.2.1.3.2 Witheld pending edit

4.2.1.3.3 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 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.

4.2.1.3.4 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 7.5.1.1 Protocol security layer, and management stations must at all times operate using only the identifier allocated to it.See also section 4.2.2 Monitoring interface for obligation to record the origin of commands..

4.2.1.3.5 Command validity

The primary SNMP communication channel should not be used for functions beyond those defined by datagrams in ISO 20684 or any supplementary MIB issued by Waka Kotahi. 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 6 Maintenance.

4.2.1.4 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 could formally be forced under NTCIP 1203v01 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.

4.2.2 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.

4.2.2.1 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 paragraphs..

4.2.2.1.1 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 tocapture the status of the device and the currently displayed message, but may include any combination of datagrams defined in the ISO 20684 series.

4.2.2.1.2 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 20684 Part 4: Notifications. Events which are desirable to actively report include;

I. Intrusion detection or security violations
II. Temperatures reported by any sensor available to the device which threaten the device or surrounding areas
III. Degraded power supply, or a switch to a battery backup or UPS source.
IV. Damage to or failure of subcomponents, where this can be detected, especially where the condition threatens road safety.

4.2.2.2 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.

4.2.2.3 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 4.2.1.4).

5 DESIGN FOR SAFETY

This section defines the core requirements to ensure the intelligent transport system 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 will be deployed displaying roading signals such as speed limits which 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.

5.1 User Needs

5.1.1 Design for Safety processes

Any vendor 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.

5.1.2 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. Specific events and prioritisation order is reflected in priority assignments given in Annex
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.

5.1.3 Continued operation in degraded states

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

6 DESIGN FOR MAINTAINANCE

6.1 Withheld.

Withheld. Remove this section on completion of edits.

6.2 Configuration Interface User Needs

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

6.2.1 Principle of remote maintenance

To facilitate the anticipated future scale of deployment of VMS and LCS devices on NZ 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.

6.2.2 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 API approved by Waka Kotahi. Reliance on proprietary hardware or software external to the device itself is not acceptable unless a departure has been granted.

6.2.3 Administration API

If an API is furnished for administration of devices beyond what functionality is offered by ISO 20684, it shall be made compatible with a library of functions to be issued by Waka Kotahi. 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.

6.2.4 Vendor reporting systems permitted but limited

Vendors 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 NZTA 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.

6.2.5 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.

6.3 Logging and reporting requirements

6.3.1 Logs

Devices shall generate, store and expose logs in accordance with ISO 20684 Part 5 Logs. The classes of data required to be recorded and exposed are detailed in Appendix D. 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.

6.3.2 Vendors to provide complete definitions of all logging codes

Beyond the requirements of Section 6.3.1, any additional logs or fault codes which a device may generate shall be defined in full to Waka Kotahi by vendors at time of acquisition or application for the purposes of maintenance and forensics.

6.3.3 Enhanced logging requirements

Supplemental to logging requirements given in section 4.12 of ITS-02-001-202110-SPEC-VMS-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.

6.3.3.1 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 7 Design for security for more information.

6.3.3.2 Reporting of all configuration changes

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

6.3.4 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.

7 DESIGN FOR SECURITY

This section defines the core requirements to ensure the intelligent transport system 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 NZ Information Security Manual (NZISM). Specific requirements for the deployment of these security features are defined here.

7.1.1 Threats and countermeasures

The key threat identified is of unauthorised access to the ITSN. Unauthorised control over a single sign is a safety risk but risk increase with access to multiple signs is exponential. Message stream modification is considered a threat but involves a more sophisticated attack. Disclosure of command messages are only a concern in their potential to inform attempts to gain unauthorised access, but this requires its treatment to the same level. Denial of Service is also a threat, with LCS particularly critical to have 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.

7.2 General Security principles

7.2.1 Default credentials to be changed

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

7.2.2 Device configuration hardening

Devices should be hardened to relevant CIS Benchmark standards, and in compliance with AS ISO/IEC 27002 Code of practice for information security controls (AS 27002), unless a departure has been granted by Waka Kotahi to accept an equivalent standard.

7.3 Physical security layer

Requirements for the physical security layer are defined in ITS-02-001-202110-SPEC-VMS-FIXED.

7.4 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 WAN facilities. For these reasons, a closed network should not be expected.
However, network layer controls in the form of jump hosts and gateways, VPN 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 NZISM, to the satisfaction of Waka Kotahi.

7.4.1 Security conditions and obligations

7.4.1.1 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 6.3 Logging for more detail.

7.4.1.2 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.

7.4.1.3 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.

7.4.1.4 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.

7.4.1.5 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.

7.5 Protocol security layer

The ISO 20684 series and NTCIP 1203 v03 Section 2.6 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.

7.5.1 Security conditions and obligations

7.5.1.1 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.

7.5.1.2 SFTP to replace FTP

Where File Transfer Protocol (FTP) was used previously, it shall now be a requirement to deploy (Secure FTP) SFTP with strong ciphers at or above TLS1.2 standard or later. Certificate management is to be administered by Waka Kotahi Security.

7.5.1.3 Web portals to be served over 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.

8 APPENDIX A – DEFAULT FONTS

8.1 Fonts for use with VMS and LCS devices

These will be supplied by NZTA with instructions on where to store them through the Font standard. Basically, the default font for each sign type will go in slot 0 as standard, specialty fonts such as for journey times in slot 1.

All fonts will be approved by NZTA before installation. All non-approved fonts must be removed.

9 APPENDIX B – DEFAULT GRAPHICS

9.1 Default Graphics Library for use with VMS and LCS devices

Waka Kotahi will publish a set of graphics specifications specifically for use with VMS and LCS devices, will specify the positions of each graphic in the sign's graphics library, as well the priority settings for the use of each graphic. Until such a list is released, appropriate graphics specifications should be drawn from the Traffic control devices manual (TCD Manual) or until replaced, the Manual of traffic signs and markings (MOTSAM) Part 1. As those specifications are intended for non-variable signs and signals, appropriate adjustments such as light/dark inversion may be required and will be detailed in device specifications.

Provision of the necessary information (display pixel attributes) or tools for Waka Kotahi to create and modify graphics files is also a requirement. Provided storage capacity given in device specifications and the capability to store and display graphics in accordance with other parts of this document is met, it is sufficient to provide these attributes or tools such that appropriate graphics files can be generated by Waka Kotahi.

10 APPENDIX C – CONFORMANCE MATRIX SUPPLEMENT

10.1 Conformance matrix supplement

This compliance matrix lays out compliance requirements for VLSI. Only exceptions to ISO20684-10 will be listed here, for example to override the status of a requirement from mandatory to optional. Otherwise, the compliance matrix in Annex B of ISO20684 applies as mandatory.

Specific Waka Kotahi requirements that have extended this standard beyond ISO20684, for example additional security requirements, will be listed here only.

Section 4 - Design for operations				
VLSI section	Reference to compliance	attributes	notes	Status
4.1	ISO 20684-10 Annex B	all	See note about exceptions above.	Mandatory
Section 5 – Design for safety				
Section 6 – Design for Maintenance				
Section 7 – Design for security				

11 APPENDIX D – LOGGING DATA (TO BE DEFINED)

11.1 Data elements of interest

Discipline	Objects	Conformance
Environmental information		M
Fan Monitoring		O
Power supply		M
System		O
Errors		M
Physical Security		M
Networking events		M
Watchdog triggers		O

12 APPENDIX E – MESSAGE PRIORITY ASSIGNMENT TABLE

12.1 Message priority assessment table

Highest priority	Class	Notes
TBC	Reserved	A band of priorities are kept at the highest level free for future use, and if control of a sign is lost then it will allow to manually override and recover it
TBC	Safety Critical	Safety critical should always have the highest priority. Through the VMS design standard, the primary purpose of the sign when it is in design stage, eg for over height signalling. Any other uses are secondary and must not override this.
TBC	Civil defence (Reserved)	Future use of signs to support Civil defence such as recent flooding events.
TBC	Incident message	Dynac day to day incident management, typically executed by Toc operator manually or as part of a pre-defined plan.
TBC	Drive information message	This would be things like general travel time messages or future road closures etc.
TBC	Campaign message	The regular “don’t drink and drive” type messages
TBC	Blank and idle	Sign must always be returned to blank and idle state when user is finished, or message times out.
Lowest priority		

13 REFERENCES

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

13.1 Industry standards

Standard number / name	Source	Licence type and conditions
Health and Safety at Work Act 2015	NZ Legislation website	Publicly available
NTCIP 1203v3 - Object Definitions for DMS	NTCIP Org website	Publicly available
ISO/TS 20684 series - ITS Roadside modules SNMP data interface	Standards NZ website	Available for purchase
NZISM v3.5 - Information Security Manual	GCSB website	Publicly available
IETF RFC 3584	IETF website	Publicly available
AS ISO/IEC 27001:2015 Information technology - Security techniques – Information security management systems – Requirements	Standards NZ website	Available for purchase
AS ISO/IEC 27002:2015 Information technology - Security techniques - Code of practice for information security controls	Standards NZ website	Available for purchase

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 design standards, delivery specifications and core requirements listed below.

Document name
ITS Delivery Specification: Variable message signs – Fixed (ITS-02-001-202211-SPEC-VMS-FIXED)
ITS Design Standard: Variable message signs – Fixed (ITS-01-001-202105-STD-VMS-FIXED)
ITS Design Standard: Optical fibre (ITS-01-008-202006-STD-CABLE-FIBRE)
ITS Systems Integration Test Plan (ITS-03-001-202104-TEST-VMS-FIXED)

13.2.2 Resources

Document name / code	Waka Kotahi website link
Traffic control devices manual (TCD manual)	nzta.govt.nz/resources/traffic-control-devices-manual/
Manual of traffic signs and markings (MOTSAM)	nzta.govt.nz/resources/motsam/part-1/

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 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