Roads

Master Specification

RD-ITS-D1 Design of Intelligent Transport Systems (ITS)

Document Information	
KNet Number:	13449010
Document Version:	3
Document Date:	August 2020

DEPARTMENT FOR
INFRASTRUCTURE
AND TRANSPORT

Government of South Australia
Department for Infrastructure
and Transport

Document Amendment Record

Version	Change Description	Date
1	Initial issue	02/07/19
2	Formatting for publishing	19/09/19
3	Numerous technical changes throughout.	August 2020

Document Management

This document is the Property of the Department for Infrastructure and Transport and contains information that is confidential to the Department. It must not be copied or reproduced in any way without the written consent of the Department. This is a controlled document and it will be updated and reissued as approved changes are made.

Contents

RD-ITS-D1 Design of Intelligent Transport Systems (ITS)

1 General

1.1 This Design Standard specifies the minimum functional, architectural and technical requirements for the design of the Intelligent Transport Systems (ITS), including communications Network and associated equipment.

1.2 This Design Standard does not include design and functional specification for the Tunnel Supervisory Control and Data Acquisition (SCADA) System.

1.3 The ITS design requirements for a specific Contract will be found in the Contract Documents for Road Design. The designer shall perform its obligations to design Intelligent Transport Systems (ITS) in accordance with the Contract Documents.

Definitions

1.4 The following definitions apply to terms used in this Part:

Table RD-ITS-D1 1-1 Definitions

Term	Definition
Equipment	All electronic and electrical components, devices, hardware, associated systems and associated infrastructure (structures, conduits, pits and the like) that together form the ITS, spanning telecommunications network, communications, and control systems. The term “Equipment” in the context of this specification applies to all equipment (whether expressly identified or not) required to provide a fully functional system in compliance with the requirements of this specification, whether the Equipment is located within the Project Boundary, on approach roads or any area immediately outside of the Project Boundary, within the remote TMC, local Computer Equipment Room (CER) or any other secondary Computer Equipment Room location.
Statenet	South Australian government secure network managed by DPC (Department of Premier and Cabinet), supporting all Government agencies for connectivity to the internet, email and communications internally between agencies.
STREAMS	The proprietary traffic management control system comprising software and hardware (developed by Transmax Pty Ltd) and licensed by the Principal for the management of traffic signalling, incident response, motorway management and other traffic services from a single system across the State of South Australia.
TMC	Traffic Management Centre (Norwood unless stated otherwise) (or elsewhere given similar telecommunications connectivity and operations systems).
TrafficNet	Secure, isolated Network of ITS (Intelligent Transport Systems) equipment owned and managed by the Department’s Traffic Management Centre for the management of South Australia’s major roadways. (This forms part of the state’s critical infrastructure.)

2 Design Standards

2.1 Unless specified otherwise, all design and / or documentation shall comply with the most recent revisions (including published amendments) of the following design standards and / or specifications:

a)	AS/NZS 1170.1	Structural design Actions - Permanent, imposed and other actions.
b)	AS/NZS 1664	Aluminium structures.
c)	AS/NZS 1768	Lightning protection.

d)	AS 1670	Fire detection, warning, control and intercom systems - System design, installation and commissioning.
e)	AS 2144	Traffic Signal Lanterns.
f)	AS 2578	Traffic signal controllers.
g)	AS/NZS 3000	Electrical installations (known as the Australian/New Zealand Wiring Rules).
h)	AS/NZS 3008	Electrical installations - Selection of cables - Cables for alternating voltages up to and including 0.6/1 kV - Typical Australian installation conditions.
i)	AS 3011	Electrical installations - Secondary batteries installed in buildings.
j)	AS/NZS 3085.1	Telecommunications installations - Administration of communications cabling systems - Basic requirements.
k)	AS/NZS 3100	Approval and test – General requirements for electrical Equipment.
l)	AS 3990	Mechanical Equipment – Steelwork.
m)	AS 4055	Wind loads for housing.
n)	AS 4070	Recommended practices for protection of low-voltage electrical installations and Equipment in MEN systems from transient over-voltages.
o)	AS 4852	Variable Message Sign.
p)	AS 5156	Electronic Speed Limit Sign.
q)	AS 60038	Standard Voltages.
r)	AS 60529	Degrees of protection provided by enclosures (IP Code).
s)	AS 61508	Functional Safety for Electrical/Electronic/Programmable Electronic Safety-related Systems.
t)	AS 62040	Uninterruptible power systems (UPS).
u)	AS/CA S008	Requirements for customer cabling products.
v)	AS/CA S009	Installation requirements for customer cabling.
w)	AS ISO/IEC 27001:2015:	Information technology - Security techniques - Information security management systems – Requirements.
x)	AP-R341/09	Austroads Guide for Freeway Design Parameters for Fully Managed Operations.
y)	AP-R344/09	Austroads Best Practice for Variable Speed Limits: Best Practice Recommendations.
z)	IEEE 802.3	Ethernet.
aa)	IEEE 802.3u	Fast Ethernet.
bb)	IEEE 802.3z	Gig Ethernet.
cc)	IEEE 802.3ae/an	10 Gigabit Ethernet over fibre/copper twisted pair.
dd)	IEC 60268-16	Sound system equipment - Part 16: Objective rating of speech intelligibility by speech transmission index.
ee)	National Managed Motorways Working Group Vision and Action Plan and Prioritisation Report.	
ff)	OCIO/S6.3	Network Technology Standards (SA Government – Office of CIO).
gg)	VICROADS	Managed Freeway – Freeway Ramp Signals Handbook 2013.

hh) RPS3 Radiation Protection Standard for Maximum Exposure Levels to Radiofrequency Fields - 3 kHz to 300 GHz (2002), Australian Radiation Protection and Nuclear Safety Agency (ARPANSA)

2.2 The Contractor's design shall comply with all relevant parts of Department standards and specifications. Department Technical Standards and Guidelines (Road & Marine) are available from https://www.dpti.sa.gov.au/standards/roads-all.

2.3 Where this Part specifies a higher standard than that required by the above Australian Standards, the requirements of this Part will take precedence.

2.4 For a list of Department approved product, refer to: https://www.dpti.sa.gov.au/__data/assets/pdf_file/0012/330105/DPTI_Approved_Products_Contract_Works.pdf.

3 Definitions

Term	Definition
ACIF	Australian Communications Industry Forum
ACMA	Australian Communications and Media Authority
AS	Australian Standards
AWS	Advanced Warning Sign
BTMC	Backup Traffic Management Centre
CCTV	Closed Circuit Television
CER	Computer Equipment Room
CHAZOP	Control Hazard and Operability
CMS	Changeable Message Sign
D&C	Design & Construct (Contract)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EIA	Electronic Industries Alliance
FAT	Factory Acceptance Test
FES	Field Equipment Sub-Network
FP	Field Processor (proprietary STREAMS communications hardware)
HTTPS	Hyper Text Transfer Protocol Secure
HVAC	Heating / Ventilation / Air Conditioning
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
I/O	Inputs and Outputs (System)
IP	Internet Protocol
ISO	International Organization for Standardization
ITS	Intelligent Transport (or Traffic) System(s)
LAN	Local Area Network
LED	Light Emitting Diode
LUMS	Lane Use Management Sign
MABN	Metropolitan Area Broadband Network
MTBF	Mean Time Between Failure
NTP	Network Time Protocol
NVR	Network Video Recorder
OEM	Original Equipment Manufacturer
O&M	Operations and Maintenance
OHVD	Over-Height Vehicle Detection (System)
OS	Outstation (may also be referred to as a Field Cabinet)
OSPF	Open Shortest Path First
OST	Operation Scenario Test
PABX	Private Automatic Branch Exchange (digital telephony)
PLC	Programmable Logic Controller / Programmable Logic Control (hardware)

Term	Definition
POA	Point of Access (of a Field Equipment Sub-Network into a Field Network)
PPP	Point-to-Point Protocol
PSSB	Police Security Services Branch
PTZ	Pan Tilt Zoom (camera)
QoS	Quality of Service
RIO	Remote Input / Output Module (hardware)
RIP	Routing Information Protocol
SABRENet	South Australian Broadband Research and Education Network
SAT	Site Acceptance Test
SCADA	Supervisory Control And Data Acquisition (System)
SCATS®	Sydney Coordinated Adaptive Traffic System, property of RMS NSW.
SIAT	Site Integration Acceptance Test
SIL	Safety Integrity Levels
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TIRTL	The Infra-Red Traffic Logger
TMC	Traffic Management Centre (Norwood unless stated otherwise)
TSC	Traffic Signal Controller (SCATS®)
UPS	Uninterruptable Power Supply
VIDS	Video Incident Detection System
VLAN	Virtual Local Area Network (soft configured virtual network within LAN)
VMS	Variable Message Signs (LED)
VoIP	Voice over Internet Protocol (digital telephony)
VSLS	Variable Speed Limit Sign
WAN	Wide Area Network

4 ITS Design Development

4.1 In addition to any other requirement in the Contractor’s Design Program, the Contractor shall provide (as an integrated part of its broader civil works design program) a fully detailed ITS Systems Design package capturing all milestones and hold points as listed in Part PC-EDM1 “Engineering and Design Management Framework”.

4.2 The Department’s “Approved Products” list will provide guidance to the Contractor regarding equipment that is acceptable to the Department. If the Contractor chooses to propose alternative ITS equipment or infrastructure that is not on the Approved Products list, the Contractor shall demonstrate that the alternative equipment or infrastructure meets the specified requirements. Acceptance of proposed alternatives shall be at the discretion of the Principal. Provision of the proposed list of ITS equipment or infrastructure shall constitute a **Hold Point**.

4.3 ITS equipment shall be numbered in accordance with the Department’s ITS Asset Identification Process (and be provided by the Principal upon request). Final numbering shall be approved by the Department’s Traffic Management Centre, and Road and Marine Asset Management, and the approval shall constitute a **Hold Point**.

5 ITS System Functional Requirements

General

5.1 The Project ITS System design shall fulfil the operational functional requirements as defined in the Contract Documents.

5.2 The ITS field equipment and systems provided shall form a wholly integrated part of those similar systems installed elsewhere within South Australia generally, ensuring commonality in operational management capability, a homogenous driver experience and continuity in ITS service level provision.

Telecommunications Network Requirements

5.3 This section is to be read in conjunction with RD-ITS-C3 “Telecommunications Cabling” and RD-ITS-S5 “Imaging Equipment”.

5.4 The ITS communications network shall integrate with, and extend, the Principal’s existing ITS communications network (informally known as “TrafficNet”). TrafficNet is an isolated network with no external connectivity to other networks. TrafficNet shall align with Statenet condition of connection. It extends from its northern-most extent at Gawler to Seaford, and east as far as Carey Gully on the SE Freeway. TrafficNet uses the Metropolitan Area Broadband Network (MABN) to provide back-haul services via a dual redundant 10Gbps fibre backbone network interconnecting all major computer room / network concentration points, with the current exception (as of Jan 2019) of the Adelaide Crafers Highway / South Eastern Freeway / Heysen Tunnels. This part of TrafficNet uses 2x legacy licensed microwave links to provide redundant connections to the rest of TrafficNet.

5.5 Connectivity between the field and the core will be firewalled and align with 3 tiered redundant connection “Core MABN, Distribution and Field Network” design.

5.6 The ITS Communications Network shall transmit all data between ITS Equipment in the field and the Traffic Management Centre.

5.7 The network shall be capable of carrying all projected (worst-case) data generated or consumed by ITS equipment on the project (including CCTV, Incident Detection, SCADA, and other data streams that may be required) with at last 50% headroom for future expansion.

5.8 All network equipment supplied by the Contractor shall be covered by a maintenance and support agreement providing both hardware (support / repair / replacement) and software (tech support / maintenance / upgrades) for a minimum of 4 years - 5x8 Next Business day service, taken out in the name of the Principal. Support Contract details shall be provided to the TMC TrafficNet Team leader prior to handover. Provision of support Contract details shall constitute a **Hold Point**.

5.9 No network equipment shall be supplied that has a published / notified End-of-Sale or End-of-Support date at the time of supply.

5.10 The telecommunications network provided by the Contractor shall utilise the Metropolitan Adelaide Broadband Network (MABN) for back haul communications purposes between the site located CER and the TMC. The Contractor shall assume all responsibility for the extension of the MABN to the CER via diverse paths working under the close oversight of the Principal’s representative at all times.

5.11 Remote access to devices connected to TrafficNet shall only be by a secure VPN connection using 2 factor authentication, in accordance with TrafficNet policy document TP014 and TOP022. Request for VPN access shall be in writing to Manager, Traffic Management Centre.

5.12 The operation of ITS Equipment shall not be compromised by bandwidth or latency limitations of the ITS Communications Network under full utilisation conditions, including projected future data traffic. CCTV coverage shall be presented at the TMC in real time and full colour.

5.13 The Principal’s traffic management and control system is referred to as “STREAMS”. The STREAMS system consists of a suite of distributed software applications operating on a server located at the TMC and on Field Processors located in the field. Unless otherwise specified, all ITS equipment that integrates with or is controlled by STREAMS shall connect to the ITS Communications Network via a STREAMS compatible Field Processor.

Power Supply, Transient Protection and Earthing Requirements

5.14 All communications network infrastructure shall feature UPS support (4 hrs), transient protection and appropriately designed earthing arrangements. Refer also Clause 8 “ITS Infrastructure” – “Power”

Design Life

5.15 The design for the Intelligent Transport Systems and ITS equipment shall meet or exceed the following minimum design life at the date of Completion:

Table RD-ITS-D1 5-1 Element Design Life

Element	Design Life (Years)
Network Fibre	30 years
Cables (Fibre and Copper)	25 years
Enclosures and cabinets	25 years
Electronics	10 years
Display Elements	10 years
Uninterruptible power supplies (UPS)	10 years
UPS batteries	5 years
Other electronic power supplies	10 years
Vehicle Detector loops	10 years
Field Processors	10 years
ITS telecommunications network devices	7 years
CCTV cameras	10 years
Video Incident Detection devices	7 years
All other Equipment	10 years

5.16 Appropriate consideration shall be made by the Contractor to the specified equipment life and the nature and location of the project, such as the potential for heavy saline presence.

Vandalism

5.17 The ITS field equipment and wide area telecommunications network shall be designed and located so as to protect such equipment and infrastructure from unauthorised access and vandalism as far as is reasonably practicable.

Traveller Information Systems (TIS)

5.18 The Contractor shall provide traveller information systems including Variable Message Signs (VMS) in accordance with AP-R341/09"Austroads Guide for Freeway Design Parameters for Fully Managed Operations".

Maintenance Access

5.19 Maintenance access shall be designed and provided as specified in RD-ITS-C1 "Installation and Integration of ITS Equipment".

5.20 ITS field cabinets, CCTV and LUMS/VSLS/CMS/VMS equipment shall be located generally at grade.

5.21 Other maintenance access options, including shoulder access for pits in the shoulder, or existing and new pedestrian and / or cycling pathways, may be considered on a case by case basis, and are subject to approval by the Principal.

5.22 The designer shall produce a maintenance strategy report (can be included in the ITS design report), detailing maintenance access and requirements for all devices. Provision of the maintenance strategy report shall constitute a **Hold Point**.

Safety Integrity Level (SIL) – Application of AS 61508 to ITS Systems Design Development

5.23 The Contractor shall determine the required Safety Integrity Level (SIL) in consultation with the Principal's representatives and the Independent Verifier (refer PC-EDM3 "Independent Design

Certification") for any life safety critical functionality identified by its design process. The SIL Study process shall be undertaken at the 30% design stage.

5.24 The Contractor shall address the interdependencies of all computer systems with the safety management of the overall operation of the road.

5.25 The Department's Traffic Management systems and communications networks (including the STREAMS motorway management system) shall not be relied upon for the provision of any life safety critical functionality and as such the safety life cycle and SIL determination shall be limited to the Contractor's solution provided in response to the requirements included in this Part.

5.26 Determination of any life safety critical functionality and the allocation of attendant SIL level shall constitute a **Hold Point**.

5.27 Should the Contractor's SIL Study identify any life safety critical functionality that demands a low Probability of Failure Upon Demand as defined by AS61508, the Contractor shall address all such requirements within its subsequent detailed design development, undertaking a further closing SIL review at the 70% design stage, addressing all such requirements within its 70% ITS Design Report.

5.28 As a minimum the following requirements shall be provided in the Nominal 70% and Final Design:

a) an overview hazard and risk assessment, including an outline Control Hazard and Operability (CHAZOP) study, shall be undertaken and documented with the submission of the design packages. The overview assessment shall include an analysis of the risks, identify the key assets and consider the impact upon the road user, system performance, system reliability, the TMC operators' ability to manage the road network, and the need to maintain the public reputation of the Department;

b) software integrity requirements for the equipment deployed by the works to meet the system operational performance criteria;

c) safety requirements;

d) safety management and planning of the solution provided by the Contractor; and

e) safety documentation.

5.29 The overview hazard and risk assessment and outline CHAZOP shall include a workshop with the Contractor, the Principal and the relevant Emergency Services personnel and will review:

a) the analysis of risks;

b) identification of the systems and architecture; and

c) safety related functions to be provided by the design and the expected performance of the overall design once implemented.

5.30 The assessment shall include consideration of the manufacturer's claims for the mean time before failure and the suitability of the solution to the intended purpose.

5.31 The hazard and risk assessment and outline CHAZOP shall exclude the detailed review beyond that of a due diligence of suitability to task and fit for purpose of the stability and security of the software code for each network or end device.

5.32 A final hazard and risk assessment analysis and its report shall be submitted to the Principal before the finalisation of the Contractor's ITS design. The provision of the hazard and risk assessment analysis report shall constitute a **Hold Point**.

Department Traffic Management Centre Computer Systems

5.33 The Contractor's ITS solution shall be fully integrated with, and be interoperable by, the Principal's existing Traffic Management Centre (TMC) and Backup Traffic Management Centre (BTMC) computer systems in managing the road network utilising the expanded STREAMS MMS application.

5.34 The Contractor shall coordinate and integrate the design of their ITS solution with the Principal's TMC in accordance with the requirements of Clause 9 "ITS Communications Network" and Clause

10 “Network Architecture” with specific reference to STREAMS compatibility and telecommunications network requirements.

6 STREAMS

6.1 The Principal uses a wide area traffic and motorway management system, known as STREAMS, to provide operational control of the ITS devices and subsystems installed across its road network. The STREAMS platform comprises a range of hardware and software products required to support the STREAMS application, as well as the IP based telecommunications networks that provide communications between the various platform components (located in TMC, CER and at roadside).

STREAMS Integration with ITS Plant and Equipment

6.2 The Contractor shall engage Transmax to undertake the following Works to integrate ITS Plant and Equipment into STREAMS at the Contractor’s cost:

a) configuration and integration of all ITS devices into STREAMS;

b) testing and commissioning, namely FAT, SAT, SIAT, OST (Operational Scenario Testing);

c) permissible Frame Configuration for LUMS;

d) schematic creation; and

e) any new software development in STREAMS, if the equipment selected requires changes to the STREAMS software.

6.3 The Contractor shall undertake any modifications to the Department’s STREAMS platform to accommodate any further devices not previously carrying STREAMS homologation. In such a case the Contractor shall engage Transmax to:

a) undertake any such modifications and further development to the STREAMS platform as may be required to accommodate their selected (alternative) devices; and

b) carry out all testing and commissioning of all ITS devices to ensure that each device is fully integrated into STREAMS, providing documented evidence of such to the Principal.

6.4 A list of currently supported devices and their protocols will be provided by the Principal upon request. Devices not currently supported in STREAMS which the Contractor may wish to use shall be fully integrated into the STREAMS platform by the Contractor at the Contractor’s cost, including any Transmax associated costs, prior to the device Factory Acceptance Testing process.

6.5 Inclusion in the design of devices intended to be operated by STREAMS but not currently integrated into STREAMS requires the approval of the Principal.

6.6 Proposals to include devices not currently integrated into STREAMS shall constitute a **Hold Point**.

6.7 The Contractor shall submit the scope and the program of Transmax STREAMS integration Works to the Department’s TMC for review prior to the 70% ITS design review stage. The Department TMC’s approval and endorsement of the Works proposal shall constitute a **Hold Point**.

7 ITS Equipment

General

7.1 Unless specified otherwise, the Contractor shall provide all ITS equipment required by their ITS design. All equipment supplied shall comply with RD-ITS-S1 “General Requirements for the Supply of ITS Equipment” and any other relevant parts as may be identified by the Principal.

7.2 All ITS equipment shall use a ‘Plug n Play’ modular design that permits equipment failures to be easily repaired via module replacement in the field without the need of full closure of carriageway or affecting the operation of other devices wherever possible, including (but not limited to) all electronic signs, cameras, signals, and Field Processors.

7.3 The Contractor shall submit details to the Principal of all proposed ITS Equipment prior to its procurement of such for approval purposes, including:

a) manufacturer, model number and equipment technical details, including rated ambient operating temperature capability;

b) compatibility with Department TMC computer systems;

c) compatibility with STREAMS (where relevant);

d) details of maintenance requirements;

e) details of design life;

f) estimated average power consumption (watts) and electrical load (amps);

g) IP Rating; and

h) fixing / fastening / bracketry arrangements.

7.4 Submission of proposed ITS equipment technical data package for the Principal's approval prior to procurement shall constitute a **Hold Point**.

Connection to STREAMS

7.5 Unless specified otherwise, the Contractor shall design, supply, install, test and commission all ITS Equipment for integration with the STREAMS system in accordance with Section 6 "STREAMS".

7.6 The Contractor shall provide a STREAMS compatibility statement for each device type, which is current at the time of commissioning.

Removal of Existing ITS Equipment

7.7 The Contractor shall decommission and remove to secure store all redundant ITS equipment, including support structures, footings and associated cabling.

7.8 The Contractor shall make good any areas affected by decommissioning and removal of any equipment. This includes repairs to remaining structures (e.g. removing surplus brackets, patching holes, repairing finishes, making safe) and making good of surrounding environment (e.g. footpaths, landscaping and so forth).

7.9 Any existing equipment that is temporarily removed pending later reinstallation shall be carefully removed and securely stored by the Contractor, pending re-erection.

7.10 The Contractor shall only decommission equipment once the Principal has declared such equipment redundant and no longer required for operational traffic management.

7.11 Decommissioning of any equipment shall not affect operation of the remaining network equipment.

7.12 The Contractor shall gain approval for any decommissioning works via the Principal's change management processes prior to the commencement of any such works.

7.13 The Contractor shall ensure that any decommissioned equipment is offered to the Principal prior to disposal, and if specified by the Principal, delivered to a Department/Contractor Depot in the condition that it was prior to removal.

ITS Device Drivers and Firmware

7.14 The Contractor shall submit all software, including (but not limited to) embedded software and device drivers to the Principal for approval. Where a proprietary solution is proposed, the Contractor shall justify the selection whilst meeting any attendant STREAMS developmental costs incurred by such selection.

7.15 The submission of the proposed embedded software shall constitute a **Hold Point**.

7.16 All upfront and ongoing software licensing for all or any third party products shall be supplied by the Contractor for a minimum of three (3) years. Any specially developed software (and / or firmware), including configuration data, shall be supplied to the Principal in native format.

7.17 Provision of the licensing schedule for proprietary software shall constitute a **Hold Point**.

Closed Circuit Television (CCTV)

7.18 Closed Circuit Television (CCTV) systems provided as part of this Contract shall comply with RD-ITS-S5 “Imaging Equipment”.

Incident Detection

7.19 The Contractor shall design and implement a video based incident detection system utilising the FLIR (ex Traficon) IP based VID system.

7.20 The Contractor shall ensure that if required, the video incident detection system is integrated and configured in accordance with any life safety critical functionality as may be identified by the Contractor in complying with Clause 5.23-5.32 “ITS System Functional Requirement” - “Safety Integrity Level (SIL)”.

Video Incident Detection System (VIDS)

7.21 The Video Incident Detection System shall comply with the requirements specified in RD-ITS-S5 “Imaging Equipment”.

7.22 A Video Incident Detection System shall be designed and installed to ensure full coverage (100%) of the areas as specified in the Contract Documents.

7.23 The detection of fallen objects along the motorway is only required where such functionality is possible using the camera spacing determined by satisfying all other requirements of this clause.

7.24 The Principal uses the FLIR Incident Detection Management System, which is currently operating on the South Road Superway and in and around the Heysen Tunnels and is to be installed to the nearby T2T Project. All video incident detection equipment shall be fully supported by FLIR T-Port and Flux and connected to a new VIDS server, which shall be installed (rack mounted) within the local CER.

7.25 All imaging equipment provided by the Contractor for video incident detection shall be fully supported by FLIR VIP detector boards (fully digital video stream).

7.26 All video feeds from the Video Incident Detection System shall be available on the network as multicast video streams that can be viewed using the Principal’s IndigoVision Control Centre.

7.27 The TMC relies on the VIDS to generate field responses within the STREAMS platform in the event of an incident. As such a Field Processor located in the CER needs to be connected to the FLIR VIDS server, such that real time alarms and video images are transferred to the TMC automatically upon annunciation by the VIDS.

7.28 At a minimum, the VIDS shall generate the following alarms at the TMC for the incidents identified below:

a) stopped vehicles / slow moving vehicles;

b) fallen objects (not for full coverage of motorway);

c) pedestrians (motorway on / off ramps – pedestrian detection not being required within the lowered motorway / cutting section of the works); and

d) reverse direction vehicles.

7.29 The VIDS shall be commissioned by the manufacturer, i.e. FLIR Systems, or their nominated local agent / technical representative.

7.30 The VIDS and all associated mounts, brackets and fixings shall be appropriately designed and constructed to ensure that any inadvertent camera movement is within FLIR specification extents, as excessive camera movement will cause the system to malfunction. Any such issues noted following commissioning and opening to traffic shall be rectified by the Contractor at its own expense as a part of its defects liability responsibilities.

7.31 The VIDS shall be designed and installed to minimise false alarms as far as is reasonably practicable. The Contractor shall specify the upper limit of false alarms expected from the system in any given 24 hour period and provide any post-opening system tuning support as maybe required to ensure that the system performs in accordance with this specification. The Principal anticipates no more than 5% false positive alarms from the final commissioned system.

In-Pavement (Inductive Loop) Detectors

7.32 In-pavement detectors will be used for a number of purposes including (but not limited to) incident detection and congestion monitoring.

7.33 Loop detectors shall be provided at regular intervals on the main carriageway in both directions as specified in AP-R341/09 “Austroads Guide for Freeway Design Parameters for Fully Managed Operations” and VicRoads’ “Managed Freeway – Freeway Ramp Signals Handbook 2013”.

7.34 As a minimum this shall include the following:

a) locations of potential incidents and bottlenecks;

b) downstream of merge points and areas of heavy weaving;

c) to detect queuing on off-ramps and end of the motorway prior to the queue extending back onto the main carriageway;

d) at a maximum spacing of 500 m on the main carriageway;

e) on all entrances to the motorway;

f) at least in one location between entrances and exits of the motorway; and

g) along all parallel lowered arterial roads.

7.35 All loop detection systems shall be installed by the Contractor as specified in RD-ITS-S7 “Supply and Installation of Vehicle Detector Systems”.

7.36 Vehicle detector loops on the road shall be installed in the following configuration:

a) 2 m loops; and

b) pairs of loops 6 m head-to-head distance apart.

7.37 Preformed loops shall be used on the road, including entry and exit points.

7.38 Conduits for the in-pavement loops shall be installed in accordance with Drawing 4500 sheet 4.

Alternative Detection Technologies

7.39 The Principal may consider innovative solutions (such as a radar based incident detection technology) which provide the same functionality as listed above for VIDS.

7.40 Battery powered pavement embedded systems shall not be utilised.

7.41 Where the Contractor opts to offer such alternative technology, the Contractor shall sponsor a comparative trial, generating a thoroughly researched trial report for the Principal’s consideration whilst assuming sole responsibility for meeting all / any (Transmax) STREAMS integration and test costs and any subsequent system performance issues.

Signs

7.42 The designer shall provide fully engineered mounting design drawings for each sign, specifying sign face aiming and alignment including orientation to road and horizontal tilt. Aiming and alignment shall be compliant with AS 4852.1.

Advance Warning Signs (AWS)

7.43 AWS shall be provided on all service road access ramps to the main carriageway, at all approach locations prior to the point of no return for entering the main carriageway. VMS of a size determined in the detailed design, with some form of conspicuity display, and intended to be legible at a distance designed for the posted speed, shall be provided to serve the following traveller information functions:

a) motorway closure / incident ahead;

b) ramp metering in effect (where ramp metering is provided); and

c) travel time information (by default).

7.44 AWS shall be connected to a STREAMS Field Processor.

7.45 The Contractor shall provide individual drawings and descriptions detailing the method of safe maintenance access for all AWS which minimises the effect on traffic. Submission of alignment drawings and method of adjustment descriptions shall constitute a **Hold Point**.

Traveller Information Systems (TIS)

7.46 The Contractor shall provide traveller information systems including Variable Message Signs (VMS) and Changeable Message Signs (CMS) in accordance with AP-R341/09 “Austroads Guide for Freeway Design Parameters for Fully Managed Operations” as a minimum.

Variable Message Signs (VMS)

7.47 VMS shall be capable of displaying pictograms, text or a combination of both in full colour simultaneously. Where composite signs (e.g. VMS with a text section and a pictogram section) are to be used, the sign shall be configured as one sign within the STREAMS platform.

7.48 VMS shall be supplied as specified in RD-ITS-S4 “Supply of Electronic Signs”.

7.49 The Contractor shall provide individual drawings and descriptions detailing the method of safe maintenance access for all VMS which minimises the effect on traffic. Submission of alignment drawings shall constitute a **Hold Point**.

Changeable Message Signs (CMS)

7.50 CMS displays shall be provided in accordance with the Contract Documents provided by the Principal as a minimum.

7.51 CMS shall be supplied as specified in RD-ITS-S4 “Supply of Electronic Signs”.

7.52 CMS utilising multiple changeable facets shall be configured via a single STREAMS Field Processor. Each facet shall have its own port on the Field Processor. Each sign actuator shall be individually electrically supplied from the field cabinet.

Variable Speed Limit Signs (VSLS) and Lane Use Management Signs (LUMS)

7.53 Variable Speed Limit Signs (VSLS) and Lane Use Management Signs (LUMS) shall be supplied as specified in RD-ITS-S4 “Supply of Electronic Signs”.

7.54 VSLS and LUMS shall be designed and installed along the full length of the main carriageway for both directions of travel to facilitate traffic and incident management by the Principal’s remote TMC STREAMS operator in accordance with AP-R344/09. Spacing of LUMS along the main carriageway shall be no greater than 500 m.

7.55 Locations shall include, but not be limited to, the following requirements:

a) VSLS shall be provided on the at-grade surface roads and upstream of the merge with the main carriageway in accordance with Austroads requirements;

b) LUMS shall also be provided along the main carriageway and lowered arterial roads and prior to any underpasses in accordance with Austroads requirements; and

c) the VSLS size type and mounting arrangement (either pole mounted or gantry) shall be determined by the Contractor's detailed design and subject to the Principal's approval.

7.56 Where interlocking of signs is required for a speed zone, this shall be provided by a common sign group controller with reference made to any specific SIL requirements. The group controller shall ensure that only permissible frame sets are sent to the sign group.

7.57 The mounting design for VSLS and LUMS shall include suitable mounting arrangements which can provide for aiming and aligning. Preference will be given to LUMS designs that enable the LUMS to be hot swappable (i.e. without isolating power or communications) with quick release mechanisms for cabling and mechanical anchors, to assist with rapid changeover of the sign.

7.58 VSLS shall be oriented to be compliant with AS 5156.

7.59 The Contractor shall provide individual drawings detailing the alignment for all VSLS and LUMS groups. Submission of alignment drawings shall constitute a **Hold Point**.

7.60 The Contractor shall provide individual drawings and descriptions detailing the method of safe maintenance access for all LUMS groups which minimises the effect on traffic. Submission of alignment drawings and descriptions will constitute a **Hold Point**.

Traffic Signals

7.61 The Contractor shall provide compliant traffic signal design in accordance with RD-EL-D2 "Traffic Signal Design".

Vehicle Count and Classification Devices (TIRTLs)

7.62 The Contractor shall provide vehicle classification devices and associated infrastructure capable of Austroads 12-bin classification on all traffic lanes at the locations as agreed with the Principal.

7.63 The Contractor shall provide Non-invasive Vehicle Count and Classification Devices with no damage to road.

7.64 The Vehicle Count and Classification Devices shall be capable of capturing traffic data including date and time, speed, direction, lane, presence, headway, gap, axle count, vehicle class, truck class, mass class, lateral road position, and axle data.

7.65 The Vehicle Count and Classification Devices shall not be the only technology or equipment used for incident detection purposes.

7.66 Vehicle classification shall use axle detections providing Austroads94, heavy vehicle (HV) mass classes (4.5T+, 8T+, 12T+) and custom truck classes.

7.67 The classification devices shall be The Infra-Red Traffic Logger (TIRTL) devices manufactured by CEOS Industrial Pty Ltd, installed in accordance with their TIRTL Motorway Installation Manual. The TIRTL shall be integrated into the STREAMS platform such that vehicle data pertaining to speed, volume, occupancy and vehicle classification is available at the TMC.

7.68 The Vehicle Count and Classification Devices shall meet the following functional requirements at a minimum:

a) Web interface with real-time traffic, unit monitoring, log retrieval and site configuration.

b) Automated data download, formatting and reporting.

c) Integrated into STREAMS.

d) Trigger output for external IP camera (wherever required).

e) HV matching between local and remote sites.

f) LV matching between adjacent freeway data stations for use in back-office systems including travel time, heat maps for SVO data, lane change analysis, vehicle trajectory and origin – destination tracking and any future system for automatic incident detection (AID).

g) Back-office GIS system providing vehicle statistics, including speed, count, class and other vehicle attributes for all sites.

h) Time synchronisation using NTP with internal GPS secondary timing.

i) Internal 3G modem with antenna for remote access.

j) Internal 10/100BASE-T Ethernet port.

7.69 The Vehicle Count and Classification Devices shall meet the following performance and rating:

a) Vehicle count error: < 1.0% for 4 to 6 lanes and 120,000 AADT.

b) Vehicle classification error (AustRoads94): < 1.0%.

c) Vehicle speed measurement error: < 0.5% (1 to 250kph).

d) Independent accreditation for speed measurement (NATA ISO/IEC 17025 certification).

e) Occupancy error (calculated from presence): < 1.0 to 2.0%.

f) Vehicle lane error < 0.1%.

g) Vehicle time stamp error < 20 ms.

h) HV mass classification (LV, HV4.5T+, 8T+, 12T+) capture rate > 97.0%, error rate < 1.0%.

i) Tailgating distance measurement error: < 2.0 m.

j) Internal storage capacity > 40 million vehicles.

k) Operating temperature range: -40 to +85ºC.

l) Product life > 25 years, MTBF > 10 years.

m) Power consumption less than 10W for all elements.

n) Environmental rating: IP67 for external devices.

o) A false positive rate of no more than once per year is required, and how this is to be achieved shall be described in the Detailed Design Report.

p) The vehicle classification controller shall ensure that a detection event is triggered into the control system within 0.5s.

Bluetooth Capture Stations

7.70 The Contractor shall provide, install test, and commission any Bluetooth Capture Stations within all field cabinets or as nominated and agreed with the Principal.

7.71 Bluetooth capture stations shall comprise an industrial DIN-mount Programmable Communications platform capable of Bluetooth (Classic and Low Energy) and WI-Fi MAC address capture from passing vehicles, which shall be connected into a port at the nearest network (TrafficNet) access point (Layer 2 switch).

7.72 The installation shall include an external antenna configured to provide coverage only of the targeted road corridor and be capable of excluding other nearby roads to minimise the data collection of non-targeted corridors.

7.73 Bluetooth Capture Stations shall be located along the primary road alignment with a spacing of no greater than 1000 metres and at every interchange, signalised intersection and pedestrian crossing along the project corridor. For rural roads with speed greater than 100km/h, Bluetooth Capture Stations can be further spaced at about 5km.

7.74 For roads with grade separation, Bluetooth Capture Stations shall be located and configured to target traffic separately on the surface roads and the motorway corridor.

7.75 Bluetooth Capture Stations shall be compatible with the Department's AddInsight – Traffic Intelligence System, including beacon / broadcast functionality. Bluetooth Capture Station hardware shall be compatible with both "Classic" Bluetooth (v2.1), Bluetooth Low Energy (v4.x) and Wi-Fi (2.4 GHz and 5 Ghz) technology.

Ramp Metering

7.76 If required by the Contract Documents, the Contractor shall provide a full design and install conduits and pits for future ramp metering installation.

7.77 Ramp metering shall be designed in accordance with RD-GM-D4 “Traffic Analysis and Modelling”.

7.78 The ramp metering sites shall be designed to suit Transmax’s Ramp Metering Signal Controller, and utilise STREAMS (via a Field Processor) for control and monitoring of each ramp metering site.

7.79 The design of ramp metering shall be provided with:

a) 2 aspect ramp signal lights on either side of the on-ramp;

b) loop detection including stop bar and queue loop detection;

c) AWS on approaches;

d) advance amber warning signals on either side of the on-ramp on approach to the ramp signals; and

e) any other fixed signage required.

Wire Rope Safety Barrier Monitoring System

7.80 If specified in the Contract Documents, where wire rope safety barrier is installed, the Contractor shall provide, install, test, and commission a wire rope safety barrier monitoring system, providing the following components:

a) strain gauge sensors on individual wire rope;

b) controller; including SMS capability for transmission of maintenance and impact alarms, and for ad hoc interrogation of system status;

c) interface via common industry protocols, including Modbus TCP/IP, to a local Field Processor for STREAMS communication; and

d) any particular infrastructure required to support the installation.

7.81 The system shall adequately measure ambient temperature and automatically correct OEM recommended tension level as well as +/- allowable tolerance according to the measured temperature for the whole stretch of the monitored sections.

7.82 The System design shall include a web-based or GUI software to allow Department maintenance personnel to access the WRSB system directly to receive a live feed of tension data in real-time to assist in scheduled re-tensioning.

ITS Cabinets

7.83 Unless otherwise specified, ITS Cabinets shall be provided according to RD-ITS-S3 “ITS Enclosures”. All cabinets, apart from small “single purpose” cabinets (e.g. pole mounted CCTV control cabinets), shall at a minimum have front, rear and side doors. Openings larger than 800 mm width shall be fitted with dual doors.

7.84 A standard design, including the layout of equipment within the cabinet, shall be used for all cabinets. Equipment layout shall follow a logical design, allow for the segregation of power (including UPS facilities) and communications, and allow for adequate ventilation and / or air movement between and around equipment. Individual design drawings shall be provided for each cabinet. Where large batteries are fitted (e.g. for a UPS), batteries shall be located and accessible to allow safe removal and replacement. Consideration shall be given to the mitigation of direct solar load in cabinet design. Heat load calculations per cabinet shall be provided.

7.85 If the ITS device cannot be seen from the ITS cabinet that controls the said device, the Contractor shall implement a method to enable the Principal’s maintenance technicians to see the status and function of the device in question whilst undertaking maintenance activities within the cabinet. Any such method shall be approved by the Principal prior to implementation.

7.86 Unless otherwise approved by the Principal, ITS cabinets shall not be located in the centre median.

7.87 A minimum 1 m clearance shall be maintained in spite of any retaining around ITS cabinets.

7.88 ITS cabinet doors shall include door alarms that connect to the Field Processor which will be remotely monitored by the Department TMC Operator via STREAMS. Opening of ITS cabinet doors shall result in an alarm being generated at the TMC via STREAMS which identifies the cabinet location and the door status (i.e. open / closed).

7.89 Where any other equipment cabinets such as power distribution or CCTV cabinets are located adjacent to or near (within 15 m) the ITS cabinet (e.g. in the same maintenance location), the door alarm circuit shall be extended from the ITS cabinet out to the adjacent cabinets monitoring all cabinet doors within any particular location. In this case, the alarm generated in STREAMS shall at a minimum identify the equipment location and door status, but not necessarily which cabinet door is open.

7.90 With reference to Clause 7.88, additional door monitoring via STREAMS is not required for traffic signal controller cabinet doors as they are monitored via SCATS®. Where a UPS cabinet is required for a Traffic Signal site and is co-located with the traffic signal controller, the SCATS® door alarm functionality shall be extended to the UPS cabinet door.

7.91 All cabinets shall be co-located in the design to maximise the number of doors which are monitored.

7.92 ITS cabinets (excluding single use cabinets such as CCTV) shall include the following minimum requirements:

a) 20A nominal load extra power capacity from ITS cabinets where ITS cabinets are more than 500 m from an ITS or lighting electrical service point;

b) 10A nominal load extra power capacity from ITS cabinets where ITS cabinets are less than 500 m from an ITS or lighting electrical service point;

c) space for installation of extra connection network access points within the cabinet with a nominal future requirement of 10 connections;

d) one spare 100 mm white conduit and one spare 100 mm orange power conduit within the ITS network and from the ITS cabinet;

e) 2 RU gap between each rack mounted device;

f) a minimum of 300 mm gap at the bottom of each cabinet to allow for cable management;

g) a minimum of 4 RU spare in each cabinet;

h) gland plates at the base of the cabinet to be divided into 3 sections running front to rear. 1 gland plate to be used for power, centre gland plate to be left as spare for access, and 1 gland plate to be used for comms. Gland plates to provide a complete seal to prevent entry of vermin / insects;

i) all cable entry to be through glands to provide a complete seal to prevent entry of vermin / insects; and

j) include a 50 mm deep pocket on the door for document storage. The pocket shall accommodate and allow for easy retrieval of an A3 and A4 documents. The pocket shall be installed such that it does not interfere with the equipment or cable within the cabinet.

k) at commissioning, each cabinet shall contain laminated detailed A3 drawing(s) of the local road area serviced by the cabinet, including;

   i) locations of every field device controlled by the cabinet, annotated with the Principal's asset identification;

   ii) details of power supply to the cabinet, and from the cabinet to each device;

   iii) details of communications to the cabinet, including spare fibre cores;

   iv) details of pits and conduits; and

   v) cabinet internal layout, including power and communications reticulation.

7.93 “Single use” cabinets (e.g. pole mounted CCTV only cabinets; small single device only ITS cabinets) shall have a spare power capacity of 10 amps and not be more than 60% populated by volume.

Field Processors

7.94 The Contractor shall provide all STREAMS Field Processors required by its design in accordance with RD-ITS-S6 “Field Processors” and the manufacturer’s specifications. The Contractor’s design shall be developed on the basis that each Field Processor (FP) has a local console port available for diagnostics, in addition to the serial ports provided for field device communications.

7.95 The FP serial ports shall be configured such that Port No. 1 of each FP is for TIA/EIA232 communications and subsequent ports will be utilised for TIA/EIA422 communications. Where more than one ITS device requires RS232 communications to the FP, protocol converters may be used within the Contractor’s design to allow for a change of communications protocol to RS422. Port No 1 of the FP is typically reserved for in-pavement loop detector units.

7.96 The Contractor shall design the FP installation in accordance with the manufacturer / supplier’s specifications and recommendations.

7.97 Departure from the above, Field Processor port configuration is subject to the Principal’s approval and shall constitute a **Hold Point**.

8 ITS Infrastructure

General

8.1 The Contractor shall provide all Equipment required by their ITS design. All Equipment supplied shall comply with RD-ITS-S1 “General Requirements for the Supply of ITS Equipment” and other relevant parts.

8.2 All ITS infrastructure design for equipment systems and devices shall:

a) use Department approved products and equipment to minimise the possibility of interfacing and operational problems;

b) use standard non-proprietary “open” interfaces to facilitate ease of maintenance and the future expansion / extension of the system by others;

c) provide redundancy;

d) be suitable for future expansion;

e) consider the design life of all electronic and telecommunications components;

f) have conformal coated electronics when equipment is located in non-conditioned environments such as field cabinets;

g) be able to use NTP setup on the ITS Network where involved with time stamping of events;

h) use a “Plug n Play” modular design that permits equipment failures to be easily repaired by module replacement without the need of full closure of carriageway or affecting the operation of other devices wherever possible, including but not limited to all electronic signs, cameras, signals and Field Processors;

i) use of mature technologies, and commercially available equipment; and

j) ensure that each device has its own individual power circuit.

Protective Treatment for Roadside Equipment

8.3 Protective treatments for roadside equipment shall be in accordance with RD-ITS-C1 “Installation and Integration of ITS Equipment” to provide effective solutions to meet ITS equipment needs, ensure safe maintenance access and ensure safety of the public.

8.4 At a minimum all roadside equipment including field cabinets shall be appropriately positioned and located outside of a crash risk zone, or protected by the installation of road side safety barriers. The road side barrier shall extend to protect the working area around the equipment.

Power

8.5 The Contractor shall determine the location of all power supply points in conjunction with SAPN and the Principal. Where applicable, the supply point location shall be designed in conjunction with the SAPN service relocation designs.

8.6 The design of power supply shall be undertaken on the basis that all usage shall be metered with the exception of the following devices:

a) Department traffic signals;

b) Department road lighting; and

c) Council street lighting.

8.7 Unless otherwise specified:

a) mains power shall be provided for all equipment installed according to the requirements specified in RD-ITS-C2 “Mains Power for Traffic Management Equipment”;

b) electrical switchboards shall be provided in accordance with RD-ITS-S2 “Electrical Switchboards”;

c) all equipment shall support an input voltage of 230VAC as specified in AS 60038;

d) each ITS device shall be supplied by a separate power cable individually protected by its own circuit breaker;

e) where field devices are located more than 50 metres from a cabinet supplying them with power each field device shall be capable of being easily isolated at its location, e.g. via a local circuit breaker or fuse which is accessible from ground level; and

f) equipment power supply and communications shall emanate from a common field cabinet.

8.8 Power supply to all equipment shall incorporate protection against electrical transients and overvoltage in accordance with AS 1768 and AS 4070.

8.9 Power and signal earthing / grounding to all equipment sites which incorporate electrical equipment shall be designed to minimise any incidence of equipment damage or unreliability due to electrical surges, transients and stray currents.

8.10 Use of a multiple earthed neutral supply configuration shall be made, configured in accordance with the requirements of AS3000.

8.11 All electronic power supplies shall be din-rail mountable and individually feed each device. Plug-pack type power supplies shall not be used. Where devices have an integral power cable which plugs directly into a general purpose outlet (GPO) or an IEC socket, the plug and socket design shall incorporate a method of locking or holding the plug into place, to prevent it moving or loosening over time.

8.12 Where devices incorporate the facility for redundant power supplies to be connected (e.g. Ethernet switches, media converter racks and so forth), redundant supplies shall be provided and connected.

8.13 Power for ITS equipment in ITS cabinets should be supplied and controlled via a network-managed power distribution system, to allow remote power control and monitoring of connected equipment. Each piece of equipment should have its own controlled outlet feeding its power supply. Where multiple power supplies are provided for a single piece of equipment (e.g. redundant or Power-over-Ethernet supplies for network switches), each power supply should be on a dedicated output.

8.14 Managed power distribution units shall provide for both individual and grouped control of power outlets, and be capable of “sequenced” power up of individual or grouped outlets.

8.15 Managed power distribution units shall be capable of monitoring using SNMP v3, compliant with Clause 11.12 - 11.23.

8.16 Devices that support Power over Ethernet (PoE) (e.g. CCTV cameras) may be used. PoE devices shall be compatible with 802.3af (PoE up to 15W), 802.3at (PoE+ up to 30W) or 802.3bt (Type 3 up to 55W or Type 4 up to 100W). Where PoE devices are used, the Ethernet cabling chosen shall be capable of handling the maximum voltage and current specified in the relevant standard.

8.17 For 802.3af/802.3at compliant PoE devices, preference shall be given to the use of compatible PoE switches rather than mid-span PoE injectors. For higher powered 802.3bt devices, midspan injectors are likely to be needed until 802.3bt compliant switches become available. Regardless of the power source, all PoE sources shall be capable of being remotely controlled via a network interface to allow for remote isolation and / or power cycling of PoE-powered devices.

Power Distribution Board Cabinet

8.18 A standard design, including the layout of equipment within the cabinet, shall be used for all power distribution cabinets. Equipment layout shall follow a logical design, and allow for adequate segregation, ventilation and / or air movement between and around equipment, supported by heat load calculations per cabinet. Individual design drawings (physical layout and single line power schematics) shall be provided for each cabinet.

8.19 The switchboard must be contained within a dedicated, sealed enclosure that prevents contact with any live LV surface. The switchboard enclosure must comply with the requirements of RD-ITS-S3 “ITS Enclosures”.

8.20 Unless otherwise approved by the Principal, power distribution cabinets shall not be located in the centre median.

8.21 Cabinets shall be designed with:

a) a load capacity of 140% of the design calculated maximum demand;

b) a 40% spare capacity of poles;

c) a minimum of 300 mm gap at the bottom of each cabinet to allow for cable management;

d) finger ducts for internal cable management, designed to be maximum 50% full on completion of cable installation; and

e) a 50 mm deep pocket included on the door for document storage. At commissioning, each cabinet shall contain a laminated detailed A3 drawing(s) of the local road area serviced by the cabinet, including;

i) locations of every field device powered by the cabinet, annotated with the Principal’s asset identification;

ii) details of power supply to the cabinet, and from the cabinet to each device; and

iii) cabinet internal layout, including power reticulation.

Backup Power

8.22 In accordance with RD-ITS-D2 “ITS Design for TrafficNet Infrastructure Buildings”, essential equipment located within the CER shall be provided with 4 hour UPS support with this supplemented via the provision of a diesel driven standby generating set complete with on-board day tank and acoustic enclosure sized to ensure 24 hours of operation at full load.

UPS Systems

8.23 The Contractor shall supply and install all UPS units as required by the Project, generally spanning all field equipment and the CER.

8.24 The UPS shall be integrated with STREAMS via a Modbus TCP/IP interface.

8.25 The following devices and subsystems shall be provided with an appropriately rated UPS such that they continue to function on full load for a minimum of 4 hours during a power outage:

a) all traffic signals containing a network access point;

b) all field cabinets, unless specified otherwise by the Principal;

c) all ITS equipment;

d) all communications devices which provide communications to ITS equipment which is backed up by either UPS or internal battery; and

e) all racks and essential equipment within the CER.

8.26 The Contractor shall ensure an appropriately sized UPS is nominated with the consideration of the start-up loads and run modes of the multiple devices connected.

8.27 In reference to Clause 8.25, ITS equipment may have internal backup power supplies in lieu of a UPS, e.g. VMS and CMS, providing that the device operates correctly for 4 hours.

8.28 The UPS design shall ensure that all devices are still controllable at all times from the TMC via STREAMS during a power outage.

8.29 UPS shall be designed to allow maintenance and battery replacement to be undertaken without any power interruption to the load. Batteries shall be hot swap replaceable.

8.30 UPSs for ITS or Traffic Signal infrastructure shall provide a facility for monitoring via SNMP V3 and optionally via a secure web interface (https) and shall be connected to the ITS communications network for this purpose.

ITS Equipment Connections

8.31 Unless otherwise specified, ITS Equipment shall be connected to a STREAMS Field Processor and shall use industry standard serial interfaces (EIA/TIA232, EIA/TIA422 or TIA/EIA 485). More than one item of ITS equipment may be connected to a single Field Processor. Each Field Processor shall have at least two spare (unused) ports, to allow for subsequent expansion. Where multiple Field Processors are located within the same cabinet, provision shall be made for at least two spare (unused) ports between the Field Processors.

8.32 Multidrop communications (where a single communications cable drives more than one device) shall not be used between Field Processors and ITS equipment.

8.33 For CMSs which have more than one CMS element in a sign face, each of the CMS elements within such a sign shall be controlled via a separate port from a common Field Processor.

8.34 All TIA/EIA232, TIA/EIA422 or TIA/EIA485 connections between the Field Processor serial port and the device serial port shall comply with the specifications detailed in, and be designed according to the recommendations in the relevant TIA/EIA standards documents and Telecommunications Systems Bulletins (TSB).

8.35 The Principal specifies the colour coding of serial twisted pair cores as:

a) White / Blue – (FP) command positive.

b) Blue – (FP) command negative.

c) Orange – (FP) return Positive.

d) White / Orange – (FP) return negative .

8.36 Standards based 802.3 Ethernet technology shall be used for Ethernet connections. The minimum data rate for Ethernet connections shall be no less than 100 Mbps cabling.

8.37 All IP equipment shall connect directly to a network access point.

8.38 Where media converters are used (e.g. to extend an Ethernet connection to a single device over optical fibre), managed media converters shall be given preference. If unmanaged devices, they shall support Link Fault Pass Through.

8.39 Where ITS Equipment is located remotely from a Field Processor or control / communications device, communications links shall provide full galvanic isolation between the Field Processor and the remote equipment. The selection of the technology for the electrically isolated communication links shall be in accordance with the following order of precedence:

a) fibre optic cable, regardless of distance;

b) copper wire with appropriate surge suppression, optical isolation and grounding design at the location of both devices (notwithstanding the use of surge suppression and optical isolation devices, the field equipment shall be powered from the Outstation (Field Cabinet) which controls it) – such links shall be designed in accordance with the recommendations contained in the relevant TIA/EIA standards document; and

c) wireless (3G/4G/5G, radio or microwave, only with the approval of the Principal).

8.40 The Contractor shall use the technology with the highest order of precedence which is practicable. Technology other than fibre optic shall only be used with the Principal's prior approval. Directional wireless links over private property shall not be accepted.

8.41 Co-location of any comms related equipment (e.g. microwave asset) with hinged type CCTV camera pole should be assessed and endorsed by the Principal as a **Hold Point**.

8.42 The Contractor shall provide proof that any proposed wireless link design will operate correctly and reliably with Department TMC computer systems over the expected wireless path, prior to approval. The Contractor shall provide documented and independently verified proof that any wireless proposal meets all ACMA requirements, and specifically for radiated power.

8.43 Where the Contractor proposes to use a technology other than optical fibre or twisted pair copper, the submission of the communication link design constitutes a **Hold Point**.

8.44 Spare power and communications cables installed on-site shall be tested, terminated, labelled and documented in as-built drawings.

Computer Equipment Room (CER)

8.45 Unless otherwise specified in the Contract, the Contractor shall design and install a computer equipment room (CER) in the location agreed by the Principal.

8.46 The CER shall be designed and constructed in accordance with RD-ITS-D2 "TrafficNet Infrastructure Building ITS Design" and with the requirements of the Building Code of Australia. A certificate of occupancy shall be included with the handover documentation.

9 ITS Communication Network

General

9.1 The ITS communications network design shall be compatible with, and connect to, the Principal's existing ITS infrastructure. All data streams, including digital video and audio streams, shall be transmitted with correct levels of services between the field and the CER.

9.2 The ITS communications network shall include, but not be limited to, the following elements:

a) the installation of new conduit / pit systems for ITS communications network fibre-optic cable along the full length of the project, including for ITS devices on approach roads;

b) where the network adjoins or is in reasonable proximity to an existing ITS network, integration of new conduit / pit systems with the existing ITS network;

c) ITS cabinets, which shall be used to house network and associated communications and power supply equipment; and

d) integration with the existing MABN network systems including, but not limited to:

i) 2 x 10 GB MABN ring core connectivity, including redundant core switches at the CER, redundant CER routers and distribution switches, redundant firewalls and redundant field connection switches;

ii) network monitoring and management;

iii) Network Time Protocol (NTP);

iv) Dynamic Name System (DNS);

v) ITS data traffic;

vi) the installation of optical fibre runs on both sides of the Project for use with redundant expanded-ring topology; and

vii) the deployment of an optical fibre expanded self-healing ring network topology utilising both fibre trenches located at each side of the main carriageway alignment to carry the primary backbone between the CER and the field equipment.

9.3 The Contractor shall design the ITS communications network to allow for additional ITS equipment and geographical extension and shall include, at minimum, 60 fibre cores or 100% of the total used number of fibre cores as spares (whichever is the greater) between the layer 3 switch located at the ends of the Project. The fibre cable used for the network backbone shall contain not less than 144 fibre cores. This capability shall be demonstrated in the design and fully documented.

9.4 Spare fibre cores shall be terminated and tested to the same specification as utilised fibre cores, so that they are immediately useable. Unterminated / untested fibre cores left in splice trays or enclosures will not be considered as fulfilling the requirement for the provision of spare fibre cores.

9.5 The Telecommunications network shall be provided as specified in Clause 9 and 10 of this Part and RD-ITS-C3 “Telecommunications Cabling”.

Functional Requirements

9.6 The ITS communications network shall provide connectivity between the TMC and the ITS field equipment via the CER and the MABN.

9.7 The ITS communications network shall provide a high level of availability with a Mean Time Between Failure (MTBF) that exceeds required lifetimes. The Contractor shall fully document the designed network availability in their ITS design.

9.8 Provision of the Contractor’s MTBF calculations shall constitute a **Hold Point**.

9.9 The equipment selected shall have a published product life cycle (e.g. On Sale, End of Sale Notice, End of Sale, and End of Support) and be on sale / current equipment at the time of the installation and commissioning. No equipment shall be supplied that has a published End of Sale / End of Support notice at the time of supply.

9.10 ITS equipment selected shall be supported by the vendor for the entire specified design life.

9.11 The operation of ITS equipment shall not be compromised by bandwidth or latency limitations of the ITS communications network under full utilisation conditions, including all projected traffic volumes across the entire network from field to TMC/BTMC. The network bandwidth shall be designed to accommodate data from all CCTV cameras operating at not less than 25 frames per second (interlaced) or 50 fps (non- interlaced) at full HD (1080p or 1920x1080 progressive scan) resolution without impact on the performance of other networked devices.

9.12 Sufficient bandwidth shall be provided to accommodate at least a 100% increase in the number of connected CCTV cameras, with latency and jitter remaining sufficiently low to ensure imperceptible degradation of performance (including that of other network-connected equipment).

9.13 All networking equipment shall support the Internet Protocol (IP) suite of protocols including, but not limited to, IPsec, IPv4, IPv6, ICMP, SNMP v3 and IGMP (multicast) version 2 and 3. Layer 3 network switches and routers shall support PIM Sparse Mode multicast routing and bootstrap router (BSR) protocol. All equipment shall adhere to IEEE, IETF and ISO standards and meet all requirements without the use of proprietary technologies.

9.14 Layer 3 Switches and Routers shall support and be licensed for at least the following dynamic routing protocols:

a) Enhanced Interior Gateway Protocol (EIGRP - full implementation – not “stub only”) for IPv4 and IPv6

b) Open Shortest Path First (OSPF) for IPv4 and IPv6

c) Intermediate System to Intermediate System (IS-IS)

In addition, network edge devices intended to connect to foreign networks shall support Border Gateway Protocol (BGP).

9.15 All networking equipment shall include programmable Application Specific Integrated Circuits (ASICs) compatible with Cisco's Dynamic Network Architecture (DNA) Software-Defined Networking fabric, and support network automation using open standards including (but not limited to) Network Configuration Protocol (NetConf) and Representational State Transfer Configuration Protocol (RESTConf) Application Programming Interfaces (API's).

9.16 The Contractor shall provide hot-swappable equipment as well as redundant power supplies for network equipment.

9.17 All network equipment shall be covered by a manufacturer support agreement (e.g. Cisco SMARTNET agreement or equivalent) for a minimum of 4 years or the duration of the Defects Liability Period, whichever is longer. The support agreement shall be established in the name of the Commissioner (TMC TrafficNet Operations), not in the name of the Contractor or equipment vendor / supplier. The following service levels shall apply:

a) Network equipment defined by the principal as operations-critical: 24hrs per day, 7 days per week, 4 hour response time (24x7x4).

b) Other network equipment: 8 hours per day, 5 days per week, next business day response (8x5xNBD).

9.18 The Contractor shall provide full details of the support Contract to the Principal prior to hand-over. Provision of support Contract details shall constitute a **Hold Point**.

9.19 All network servers provided under this Contract shall provide "Lights-out" management capability via an integrated management card with a dedicated network interface that is separately configured from the main server network interfaces. The management card shall remain operational when the server is powered off, as long as there is power available at the server's power supplies.

9.20 The lights-out management card shall provide full control and monitoring of the server hardware, including a "virtual console" that allows remote access to the server as if connected via a local monitor. The Contractor shall be responsible for ensuring that licenses are purchased and installed to enable the full functionality of the lights-out management card (i.e. no features shall be disabled due to license levels).

10 Network Architecture

General

10.1 All connections from the CER to the field and between field cabinets (including to devices that are not co-located with their associated field cabinet) shall be made using Single Mode Optical Fibre. Wireless links shall not be used, except in cases where a fibre connection is not reasonably practicable. (The distance or the need to trench / bore outside a project boundary is not to be used as a determinant of what is "reasonably practicable".) Departure from this paragraph requires approval from the Principal. Such approval shall constitute a **Hold Point**.

10.2 The ITS Communications Network shall comprise the following:

a) ITS Backbone fibre-optic cable along each side of the Project's main alignment for its full length;

b) network access points providing multi-port Ethernet connectivity to allow connection of ITS Field Equipment;

c) network access points shall be incorporated in a layer 2 expanded ring topology;

d) ITS cabinets, which shall be used to house network access points and associated equipment communications cable equipment; and

e) backhaul link between the CER and the TMC (Contractor to extend MABN to CER via diverse connectivity).

10.3 TrafficNet (MABN) backhaul links installed by the project shall provide high availability and redundancy using multiple geographically diverse links to the nearest existing MABN-connected site or sites. The location of interconnections to the existing MABN network shall be as agreed with the Principal.

10.4 The field network shall provide full redundancy and high-availability to each field cabinet using Rapid Spanning Tree protocol (Redundant Ethernet Protocol – REP – may be used if supported). Individual spanning-tree instances per Virtual Local Area Network (VLAN) shall be supported. The primary (backbone) network rings shall be constructed as expanded rings with geographic diversity for the redundant path. “Collapsed rings” shall not be used with the exception of spurs from the mainline network to field cabinets.

10.5 The field network shall be designed to separate traffic using VLANs based on role / purpose / function (e.g. separate VLANs for network switch management, CCTV, Incident Detection devices, STREAMS, ramp metering, SCATS®, Bluetooth).

10.6 No more than 7 field cabinets (or Ethernet switches) shall be incorporated into an individual network ring. If more than 7 cabinets are required, multiple network rings shall be used.

10.7 Network rings should ideally be “interleaved” (e.g. odd numbered cabinets on one ring and even numbered cabinets on the alternate) to avoid loss of control and / or visibility of an entire section of road with the loss of an entire ring.

10.8 The network within the CER shall be based on a full structured-cabling design allowing for cross-connection of equipment without the need to run patch leads from rack to rack (whether fibre or copper). All cabling shall comply with and be tested according to the requirements specified in RD-ITS-C3 “Telecommunications Cabling”.

ITS Backbone

10.9 The ITS Backbone shall consist of a fibre-optic cable and associated network equipment, and shall extend along both sides of the road corridor for the extent of the Project. The ITS Backbone shall be configured as a self-healing expanded ring in the layer 2 network.

10.10 Spare conduit requirement shall be designed in accordance with RD-EL-D3 “A Guide to Conduit Design for Road Lighting, Traffic Signals and ITS”.

10.11 Where trenches are required for purposes other than ITS backbone cabling (e.g. to ITS equipment located off the backbone or for Road Lighting which does not use the backbone trench), 1x spare communications conduit, minimum diameter 100 mm shall be installed in the trench and connected to the ITS backbone conduit system, unless otherwise specified. The conduit shall terminate in a pit no smaller than P4 at the end of the trench.

Connection to ITS Equipment

10.12 ITS Field Equipment other than CCTV cameras shall connect into a Network Access Point via a STREAMS compatible Field Processor. Digital CCTV cameras shall connect directly to a Network Access Point. Other IP Equipment shall connect directly to a Network Access Point and communicate via the same switch as the Field Processor.

10.13 Industry standard patch leads shall be used to connect all equipment and electrically isolated communication links shall be used.

Network Access Points

10.14 The Network Access Points allow for the connection of ITS Field Equipment at a localised area into the ITS Communications network.

10.15 At least one network switch shall be provided in every ITS field cabinet. The network switches shall have sufficient ports for each device in the field cabinet, plus 2 uplink ports, plus at least 3 spare ports once all device are connected (for future expansion / additions and technician maintenance access).

10.16 For remote cabinets associated with network connected devices not co-located with an ITS cabinet (e.g. pole-mounted CCTV cabinets or VMS cabinets), a managed network switch shall be provided to allow for local technician access as well as device connection. The same requirements for port count specified in Clause 11.15 also apply here.

10.17 All network switches and media converters shall be managed devices. No unmanaged network devices shall be used.

10.18 The level of provision of Network Access Points shall be covered within the Contractor’s 30% design submission.

ITS Communications Network – Conceptual Diagram

10.19 An example of ITS Communications Network reference design is shown in the concept diagram in Appendix 1: ITS Network Reference Design. While the concept diagram shows only four layer 2 field rings, the proposed architecture shall comprise sufficient rings to ensure reliability and redundancy.

10.20 The submission of the proposed ITS communications network shall constitute a **Hold Point**.

Network Connections

10.21 The ITS Telecommunication Network shall provide full-duplex connectivity between the TMC and an Ethernet port at the Network Access Point. The ITS Communications Network shall be of modular design to facilitate future network expansion at minimal cost. The network shall allow the connection of Network Equipment from multiple vendors.

10.22 All network-connected equipment shall support both DHCP and static IPv4 and IPv6 addresses.

10.23 “Uplink” (backbone) ports between field switches, and from field networks to the CER, shall be configured as 802.1q Trunk ports. All VLANs shall be tagged – the trunk “native” VLAN shall not be used.

10.24 Field network rings shall terminate on a Layer 3 Switch Stack in the Computer Equipment Room. This Layer 3 switch will provide inter-VLAN routing for the field network and be the default gateway for the field networks. It shall support dynamic routing protocols compatible with those already in use on TrafficNet (Refer to Clause 9.14).

10.25 Field network rings shall utilise 802.1w Rapid Spanning Tree Protocol (RSTP) to prevent switching loops. Per-VLAN RTSP (PV-RSTP) or Multiple Spanning Tree Protocol (MSTP) extensions may be used. The protocol shall be configured for the minimum possible convergence time.

10.26 Each member of the switch stack shall be capable of switching the full, worst-case network load in the case of the other stack member failing or being taken offline (e.g. for maintenance).

10.27 A stateful firewall shall isolate the field network from the CER network. Firewall redundancy shall be provided through clustering (preferred) or an active / passive failover pair.

10.28 The firewalls shall support dynamic routing protocols compatible with those already in use on TrafficNet, including (but not limited to) EIGRP for IPv4 and IPv6, OSPF for IPv4 and IPv6, and IS-IS.

10.29 The firewalls shall be configured to allow all outgoing connections from TrafficNet to the field networks, and to block all connections from the field network into TrafficNet except those required for normal equipment operation.

10.30 The CER network shall be designed around the 3-layer network model:

a) the Access Layer: provides Layer 2 connections to devices (e.g. servers, workstations, security cameras, UPSs, Generators, etc.), with traffic being functionally separated using VLANs;

b) the Distribution Layer: provides Layer 3 connectivity and intra-site routing between VLANs; a switch stack is preferred in this application. Redundant connections to access switches shall be provided using port aggregation (Ether Channel / Port Channel) controlled using Link Aggregation Control Protocol (LACP). Each member of the distribution switch stack shall be capable of switching and routing the full expected worst-case network load should the other member fail or be taken offline; and

c) the Core Layer: provides Layer 3 connectivity to the rest of TrafficNet (via the MABN and inter-site routing (including route summarisation).

10.31 See Appendix 1: ITS Network Reference Design for a reference network design template (to be modified and / or extended by the designers as required).

10.32 Interconnection to the MABN shall be provided by Layer 3 switches running dynamic routing protocols compatible with those already used on the MABN. Connection to the MABN backhaul networks shall be at 10 Gigabits per second (10Gbps) using Single Mode Optical Fibre transceivers.

10.33 MABN switches shall be individual switches, not stacked.

10.34 Inter-site routing shall be provided by two routers separate to the MABN switches. Each router shall be capable of routing in real time the full expected worst-case network load if the other fails or is taken offline.

11 Level of Service

General

11.1 CCTV video and control data shall use Internet Protocol (IP) and be transmitted over the same communications channel as all other data. QoS mechanisms shall be used to give priority as required for the data packets.

11.2 The Contractor shall perform network calculations and select network equipment models and licensing in accordance with the above requirements. The network load calculations shall be performed for each field network ring, the CER network, and the expected worst-case inter-site traffic. The network load calculations shall be incorporated in the relevant project Design Report and submitted to the Principal for review and comment, along with the proposed network equipment list.

11.3 “End to End” network latency for the ITS network supplied by the Contractor shall not exceed 10 mS with the network loaded to its full, expected worst-case load (can be tested using a “Ping” test to end devices from a workstation or laptop connected to an access layer switch in the CER). Overall latency from an end device to the Department’s Traffic Management Centre or Backup Traffic Management Centre shall not exceed 30 mS (to be tested from a workstation at each of the aforementioned locations).

11.4 Firewalls shall be capable of processing the full expected network load (plus at least 50% headroom for future growth / expansion) in real time. Where a firewall cluster is used, each member of the cluster shall be capable of handling the full bandwidth (plus the specified headroom) if other cluster members fail (e.g. if the calculated worst-case network bandwidth crossing the firewall cluster is 800 Mbps), all cluster members shall be capable of passing / processing the full 800 Mbps bandwidth.

11.5 The bandwidth of each connection to the firewall (from the field L3 switch and the distribution switch) shall be sized to carry the full, worst-case network load in the case that it is the only active port (e.g. if the overall field network bandwidth exceeds 1 Gbps, this will necessitate 10 Gbps links between the firewall and the L3 switches)..

Dynamic Routing

11.6 Dynamic routing protocols shall be used on Layer 3 links to manage routing within the project and to the backhaul network. The dynamic routing protocols shall integrate with or extend those already used on TrafficNet. Neither RIP (Routing Information Protocol) nor RIPng (RIP next generation) shall be used. The protocol used shall support, and be configured for, sub-second failover / convergence in the case of a network link failure.

11.7 Layer 3 network links shall be configured to detect a failure of Bidirectional Forwarding Detection (BFD). This shall be integrated with the dynamic routing protocol to facilitate the fastest possible routing protocol reconvergence after a network link failure.

11.8 IP addresses will be allocated to maximise the opportunity for route summarisation. Route summarisation should be used as far as is practicable to minimise routing table size.

11.9 Route redistribution should be avoided unless absolutely necessary. Wherever possible, routes should be advertised natively rather than as redistributed routes.

11.10 All Layer 3 network devices (routers, multi-layer switches, and firewalls) shall support multicast routing using Protocol-Independent Multicast (PIM) Sparse Mode, and shall be able to dynamically learn of (and advertise) multicast Rendezvous Points using the PIM Bootstrap Router (BSR) protocol.

Communication Standards

11.11 Unless approved otherwise, Network Equipment shall use non-proprietary communication protocols.

Network Management

11.12 All network-connected devices shall support monitoring via Simple Network Management Protocol (SNMP) version 3. If a proposed device is not available with SNMP v3 support and the manufacturer declines to add such support, approval shall be sought from the Principal to use SNMP version 2c. Such approval shall constitute a **Hold Point**. Under no circumstances will approval be given for the use of SNMP version 1 or version 2 prior to version 2c.

11.13 SNMP devices shall be configured for SNMP v3 Authentication and Privacy (auth / priv) using non-default passwords (and usernames if possible) and encryption keys. Configured passwords / usernames / encryption keys shall be provided to the Principal to facilitate them being added to the Principal's network monitoring software.

11.14 Devices shall be configured to use the strongest available authentication and encryption hashes. For example, for authentication, SHA1 shall be preferred over MD5. For encryption, AES-256 is preferred over (from next-most to least preferred) AES-192, AES-128 and DES-56.

11.15 Network-connected devices should support remote logging using the “Syslog” protocol. Details of the Principal's syslog server(s) shall be provided by the Principal's Authorised Representative along with the IP address assignments in Clause 11.12 above.

11.16 Layer 2 network links shall provide a means of detecting and raising alarms for unidirectional network links (Unidirectional Link Detection (UDLD)). This is essential on optical fibre links and optional on copper Ethernet links.

11.17 All device passwords (and, if possible, usernames) shall be changed from their default values. Strong passwords shall be used. A database with configured device passwords shall be supplied by the Contractor to the Principal along with (but not incorporated as part of) the As-built documentation to allow management access by the Principal's nominated representatives or Contractors.

11.18 All network switches / routers / firewalls shall be configured for Radius Authentication / Authorisation and Accounting using the Principal's TrafficNet Radius servers. Relevant configuration details shall be provided by the Principal's Authorised Representative along with the IP address assignments in Clause 11.12 above.

11.19 All network-connected devices that use real-time clocks shall synchronise their clocks with the Principal's network time server(s) using Network Time Protocol. The IP address(es) of relevant time servers shall be provided by the Principal's Authorised Representative along with the IP address assignments in Clause 11.12 above.

11.20 All network-connected devices that require name resolution shall use the Principal's TrafficNet Domain Name Service (DNS) servers. The IP addresses of the DNS servers shall be provided by the Principal's Authorised Representative along with the IP address assignments in Clause 11.12 above.

11.21 All network switches / routers / firewalls shall be configured for Radius Authentication / Authorisation and Accounting using the Principal's TrafficNet Radius servers. Relevant configuration details shall be provided by the Principal's Authorised Representative along with the IP address assignments in Clause 11.12 above.

11.22 All multi-layer switches and routers shall be configured with a loopback interface that will be assigned a host address (/32) by the Principal. This loopback interface is to be used for the purposes of PIM routing, as the router identifier for the dynamic routing protocol and as the source interface for NTP, DNS and radius authentication requests and will be the primary management address used for access to the device. It is to be advertised as an internal route by the dynamic routing protocol.

11.23 Layer 2 Switches (both field and CER access switches) shall be configured with a Switched Virtual Interface (SVI) port on a VLAN other than VLAN 1 for management access.

Special Requirements

11.24 The ITS Communications Network will transmit different data streams with differing priorities. The network shall be able to control the data traffic in accordance with these differing priorities.

11.25 The PLC and ITS communications network shall provide a high level of availability of a minimum 99.995%. The Contractor shall prove that the Equipment to be supplied meets the highest industry standards for reliability and performance.

11.26 Unless approved by the Principal, the Contractor shall specify hot-swappable Equipment and redundant power supplies.

11.27 IP addresses and VLAN numbers shall be provided on request to the Contractor by the Principal's Authorised Representative. With the request, the Contractor shall provide to the Principal's Authorised Representative a spreadsheet containing a list of all devices requiring IP addresses, in a format agreed on with the Principal. The Principal's Authorised Representative shall respond to said request within 15 working days of being notified of the request.

11.28 All network information provided to the Contractor by the Principal is to be treated as sensitive information and will be provided as Commercial-In-Confidence. It is not to be included in the As-Built documentation.

11.29 The Contractor shall be responsible for configuration of all network equipment. The Principal will review all network-connected equipment configurations and will either approve as-is or suggest / request any required changes to ensure compatibility and compliance with existing network practices and procedures, prior to the commencement of Factory Acceptance Testing. At least 5 clear working days' notice is required for scheduling network configuration review. 1 to 3 working days may be required for the review, depending on the number of devices involved. Approval of network equipment configuration shall constitute a **Hold Point**.

Wireless Installation

11.30 This Clause applies where wireless technology is to be used, subject to meeting the requirements of Clause 10.12 "Connection to ITS Equipment".

11.31 Antennas shall be positioned so that ongoing Line of Sight to the opposite communication partner is guaranteed at all times. Directional wireless links over private property shall not be accepted. Installation of Antennas shall not impact traffic and / or pedestrians.

11.32 Antennas shall be placed on structures that protect the Equipment from unauthorised access and vandalism. In addition, easy and safe access for maintenance staff shall be allowed for and documented in the Maintenance Access Strategy Report (refer Part CH70 "Handover"). Antennas shall be connected to the related Equipment via industry standard connectors.

11.33 Antenna gains shall be within the legal limits as specified in the relevant legislation. For Class-Licensed Equipment in the 900 MHz, 2.4 GHz, 5.4 GHz, and 5.8 GHz bands, the relevant legislation is the Radio communications (Low Interference Potential Devices) Class Licence 2000.

11.34 The maximum wind loading of antenna Equipment shall be appropriate for the specific wind speed and terrain categories of the proposed Equipment location, as specified with AS 4055. Wireless antennas shall be fitted with suitable surge protection to protect connected network and ITS Equipment in the event of surges or lightning strikes.

11.35 The site shall be designed to minimise the risk of occupational or public exposure to radiation, in accordance with the principles outlined in the Radiation Protection Standard – Maximum Exposure

Levels to Radiofrequency Fields – 3kHz to 300Ghz (Radiation Protection Series 3, hereafter referred to as RPS3), published by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA). Compliance shall be verified and compliance records shall be provided in accordance with section 4 of RPS3.

Indicators

11.36 At a minimum, the network Equipment shall display (e.g. by LED) the following: Link Integrity, Disabled, Activity, Full-Duplex indicators for each port and System power.

Physical Interfaces

11.37 Physical interfaces provided at the POA shall utilise industry-standard connections. Physical interconnections shall be captive (in the following order of preference):

a) automatic “click” type (such as RJ-45);

b) manual “click” type; and

c) screw-type.

11.38 Where practicable, the interconnection with the highest order of precedence shall be used. Enclosures that incorporate conduits for entry of telecommunication cables shall comply with the requirements of the AS/CA S009.

Security

11.39 TrafficNet is gazetted as State Government critical ICT infrastructure and as such, falls within the scope of the OCIO’s Information Security Management Framework (ISMF).

11.40 The Network Equipment shall comply with the Principal’s Information Security Management Policies requirements for authentication, authorisation, accountability and data integrity. (TP007 and TP016 to be provided by the Principal during the design.)

11.41 Security requirements of the network equipment and data transfer shall also comply with the following:

a) any data that is to travel over third party links is to be encrypted (whole payload encryption not just header) with an IPSec tunnel between the sites (for the purposes of this requirement, a third party link is defined as one where the Principal does not have control over all active devices in the end-to-end data transmission path;

b) all equipment attached to the network that is managed remotely shall support secure protocols such as SSH (v2 or later) and / or HTTPS with the ability to disable any insecure protocols that it might support;

c) all equipment that is part of the network operation is to support remote management;

d) all equipment is to support the ability to take offline or disable any portion or segment of the equipment that is not required to be in use at any time (e.g. the ability to remotely disable and enable ports on switches, routers, firewalls);

e) access to any equipment will be via an authorised username / password exchange or other approved authentication mechanism, and at no time is this exchange to be carried “in the clear” or via “clear text” forms of exchange;

f) any equipment that requires authorisation to access should support the ability to remotely verify the appropriate credentials (e.g. via a RADIUS (server authentication mechanism));

g) any network communications are required to be 802.3 Ethernet and the protocols IP based;

h) all cabinets, racks and other housings in which equipment is to be stored shall have intrusion detection systems present that alarm when physical access is obtained (these systems shall be compatible with the Department’s TMC STREAMS system , refer Clause 7 “ITS Equipment” - “ITS Cabinets”);

i) all equipment and computer rooms are to be kept under 24x7 video surveillance with 100% coverage at all times, without the need to pan / tilt the CCTV systems in order to obtain this 100% coverage (refer Clause 8 “ITS Infrastructure” - “Computer Equipment Room”); and

j) any location on the network where equipment is installed that will allow for network access to occur is to be able to be monitored via CCTV from the TMC.

11.42 Physical access to Network Equipment shall be restricted to authorised users by fitting appropriate physical security mechanisms.

11.43 The Contractor shall undertake a security audit to ensure that these requirements are met at the completion of installation and prior to connection to the Department’s network and provide results of the audit to the Principal. Provision of the security audit report shall constitute a **Hold Point**.

12 Site Layout

12.1 Further to the requirements of RD-ITS-C1 “Installation and Integration of ITS Equipment”, the design of the site layout shall facilitate the achievement of the following objectives:

a) provide safe access to the site, and protection while on site, for personnel undertaking maintenance;

b) minimise the requirement for traffic restrictions (e.g. speed and lane restrictions);

c) minimise the requirement for specialist access equipment;

d) enable maintenance and inspection to be undertaken efficiently and safely;

e) minimise unauthorised access and damage from vandalism; and

f) minimise the probability of damage or injury to maintenance staff from out of control vehicles.

12.2 The Design Documents shall include plans showing the physical layout at each site where Equipment will be installed. Where appropriate, the Design Documents shall show:

a) general layout;

b) reduced levels and inclines;

c) equipment position;

d) coordinates or offsets;

e) speed zones;

f) conduit and pit locations;

g) mounting structure positions and foundation details;

h) any protective barriers; and

i) details of site access (Refer to Clause 6 “Vehicular Site Maintenance Access” and Clause 7 “Non-Vehicular Access” of RD-ITS-C1 “Installation and Integration of ITS Equipment”).

12.3 Verge treatments for barriers and conduits shall be in accordance with RD-ITS-C1 “Installation and Integration of ITS Equipment” to provide effective solutions to meet ITS equipment needs and ensure safe maintenance access.

12.4 At a minimum, all ITS equipment including field cabinets shall be appropriately positioned and located outside of a crash risk zone, or protected by the installation of road side safety barriers. The road side barrier shall extend to protect the working area around the equipment and allow for safe vehicular access.

12.5 For the purposes of integrating the design and construction process, the Principal requires that all installed field devices are mapped with GPS co-ordinates, and that these co-ordinates shall be supplied to the Principal in a format specified by the Principal as a part of the As-Built documentation.

13 Design of Support Structures

General

13.1 Unless the Principal has specified details of the Equipment support structures, the Contractor is responsible for the design of suitable support structures in accordance with the requirements of this Clause.

13.2 The mounting structures shall be easily and safely accessible for inspection and maintenance purposes. The access system shall prohibit access by unauthorised personnel.

13.3 The access system and platform shall provide for secure mounting points for effective rescue of incapacitated personnel from the platform.

13.4 Unless specified otherwise, the support structures shall generally be of the same form and be aesthetically compatible with any other similar structures on the adjoining road network.

13.5 The design of the support structures and footings shall be undertaken by a chartered Professional Engineer with qualifications admitting to Corporate Membership of the Institution of Engineers who is suitably experienced in the design of such structures. The design shall be verified in accordance with AS 9001: Clause 7.3.5 “Design and Development Verification”.

Design Requirements

13.6 Unless specified otherwise, all design and documentation shall be undertaken in accordance with the following documents:

a) Department Design Standard – Structural, available from: https://www.dpti.sa.gov.au/contractor_documents/masterspecifications/Structures;

b) Department Structural Drafting guidelines for Consultants, available from https://www.dpti.sa.gov.au/documents/major_structures_documents;

c) AS 1100 – Technical drawing;

d) AS/NZS 1170.2 – Structural design actions - Wind actions;

e) AS 1657 – Fixed platforms, walkways, stairways and ladders - Design, construction and installation;

f) AS 2312 – Guide to the protection of structural steel against atmospheric corrosion by the use of protective coatings; and

g) AS/NZS 5100 – Bridge design.

13.7 Structures shall be designed for the design life specified in ST-SD-S1 Design of Structures.

Design Documentation

13.8 Prior to the commencement of fabrication or any work on site, the Contractor shall supply a copy of the calculations and an electronic copy of drawings in .pdf, .dwg and .dwf format with a file name in accordance with the protocol supplied by the Principal.

13.9 Provision of the above calculations and drawings shall constitute a **Hold Point**.

14 Design Deliverables

14.1 The Contractor shall develop and submit an ITS Design Report detailing all aspects of the ITS Design including, but not limited to:

a) traffic operations;

b) Safety Integrity Level (SIL) requirements;

c) ITS communications network;

d) ITS network layout drawings;

e) incident detection and management;

f) location and details of all ITS equipment;

g) technical details / specifications of all proposed equipment;

h) details of hardware and software;

i) provision of future ITS network expansion;

j) details of integration with the Department's TMC and Department communications networks;

k) performance monitoring and evaluation tools;

l) risk management;

m) security;

n) maintenance requirements (including but not limited to access methods, preventive maintenance schedules, site or equipment specific safe working procedures, etc.);

o) details of conduit systems provided (including, but not limited to, conduits, pits and road crossings) for power and communications; and

p) comprehensive, detailed description of the network and associated design calculations.

15 Testing and Commissioning, Handover

15.1 The design shall incorporate all elements necessary to meet the requirements of testing and commissioning and handover as detailed in RD-ITS-C1 "Installation and Integration of ITS Equipment".

16 Training

16.1 The designer shall incorporate all element necessary to meet the requirement of training as specified in RD-ITS-S1 "General Requirements for the Supply of ITS Equipment" and RD-ITS-C1 "Installation and Integration of ITS Equipment".

17 Warranty and Spares

17.1 The design shall incorporate all element necessary to meet the requirement of warranty and spare parts as specified in RD-ITS-S1 "General Requirements for the Supply of ITS Equipment".

18 Records

18.1 The Contractor shall provide following records to the Principal:

Drawings

18.2 The design drawings in accordance with Department Design Presentation Standards, in particular "DP001 – General requirements", "DP002 - Title and Index", and DP018 "Intelligent Transport Systems (ITS)"

18.3 Update of any existing infrastructure drawings.

18.4 All As-built documentation and O&M Manuals shall be provided to the Principal within 8 weeks of Completion.

Reports

18.5 ITS Communications Network Design Report, which includes comprehensive detailed descriptions of the network and all associated design calculations covering and including, but not limited to:

a) traffic operations using ITS (including any nominated SIL implications);

b) incident detection and management;

c) details and suppliers technical data for all Equipment;

d) details of hardware and software;

e) communications network including provision of future network expansion;

f) cable and termination schedules including link budgets for each transmitter and receiver type;

g) details of integration with TMC, STREAMS, and the Principal's communications networks;

h) performance monitoring and evaluation tools;

i) maintenance requirements (including but not limited to access methods, preventive maintenance schedules, site or equipment specific safe working procedures, and so forth);

j) details of conduit systems provided (including, but not limited to, conduits, pits and road crossings) for power and communications;

k) detailed description of the IP network and associated design calculations;

l) any specific calculations to demonstrate the Equipment and associated system meets the performance requirements specified and as required by the Contractor’s design;

m) demonstration of cross checks with other discipline designs including, but not limited to, road layout and geometry, road cross section, road surface finish level, roadside furnishing and barriers, roadside signage and lines, safety design, power reticulation design, and SCADA system design; and

n) closeout and documentation of discipline specific and safety related comments from the Principal and the Independent Verifier.

18.6 The Design Report may preferably be separated into multiple documents so as to cover specific aspects succinctly, such as the Communications Network.

Other

a) Safety Integrity Level Report;

b) Bill of Materials and Data Sheets for all major Equipment;

c) Operations and Maintenance Manuals;

d) Completion of Training Manuals;

e) Preventive maintenance and fault diagnosis reports; and

f) 1,000 hours initial operating fault log.

19 Hold Points

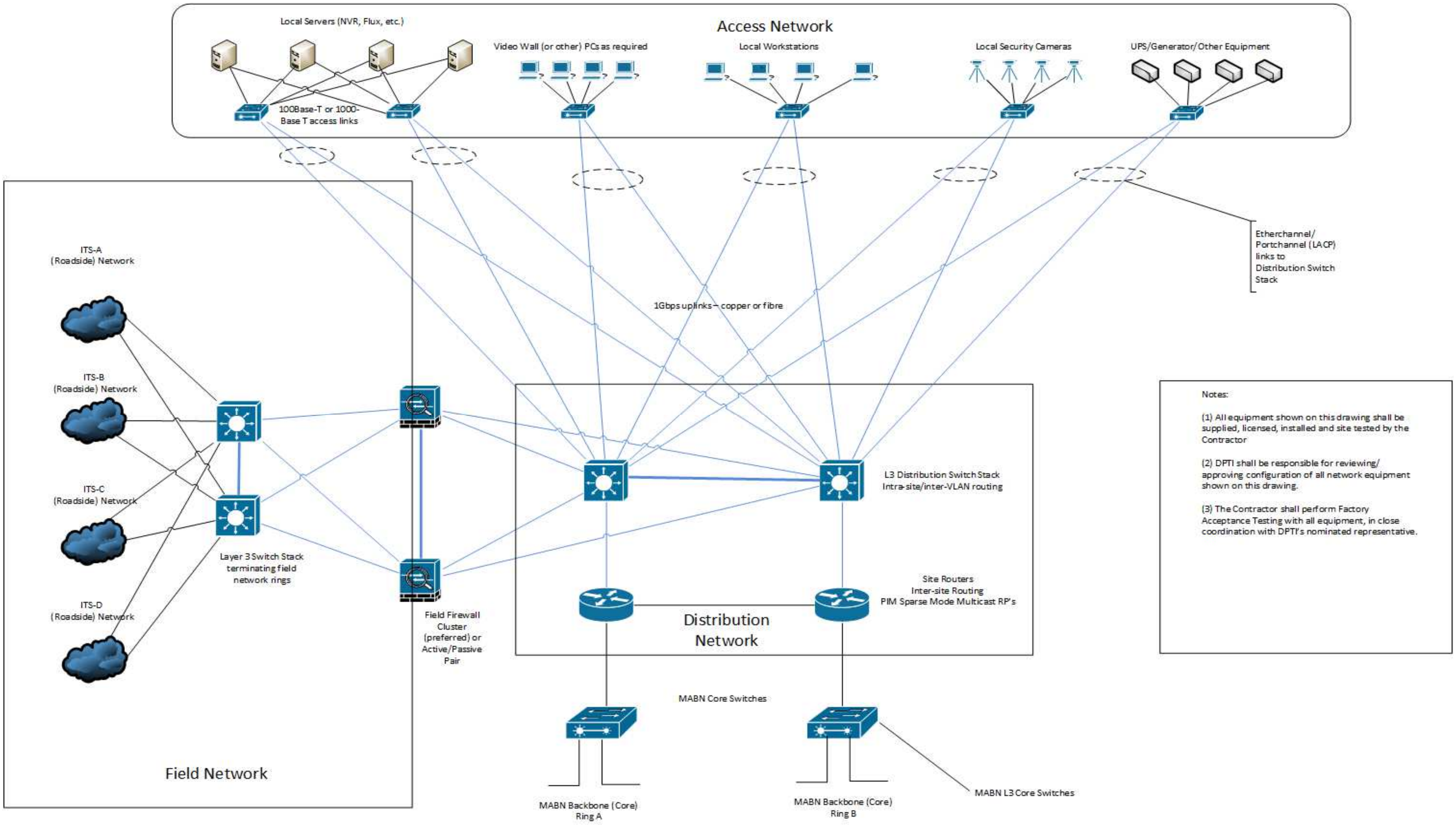
19.1 The following is a summary of Hold Points referenced in this Part:

Table RD-ITS-D1 19-1 Hold Points

Document Ref.	Hold Point	Response Time
4.2	Provision of the proposed list of ITS Equipment and infrastructure for approval	10 Working Days
4.3	The Principal’s approval for ITS asset numbering	10 Working Days
5.8	Provision of maintenance and support agreement document for Network Equipment	15 Working Days
5.22	Provision of Maintenance Strategy Report	10 Working Days
5.26	Determination of the SILS	10 Working Days

Document Ref.	Hold Point	Response Time
5.32	Safety and Hazard Risk Assessment Analysis Report	20 Working Days
6.6	Inclusion of devices not currently integrated into STREAMS	20 Working Days
6.7	The approval and endorsement of the STREAMS integration Works proposal	15 Working Days
7.4	Provision of the proposed ITS Equipment technical data package	10 Working Days
7.15	Proposed Software Design	10 Working Days
7.17	Provision of the licensing schedule for proprietary software	10 Working Days
7.45	Provision of the drawing detailing the alignment of AWS signs	10 Working Days
7.49	Provision of the drawing detailing the alignment for VMS signs	10 Working Days
7.59	Provision of the drawings detailing the alignment for all VSLS and LUMS groups	10 Working Days
7.60	Provision of drawings / descriptions detailing the method of safe maintenance access for all LUMS groups which minimises the effect on traffic.	10 Working Days
7.97	Field Processor Port Configuration	10 Working Days
8.41	The Principal’s approval to co-locate other comms assets on hinged CCTV Camera Pole	10 Working Days
8.43	ITS Equipment Connections	10 Working Days
9.8	Provision of the Contractor’s MTBF calculations	10 Working Days
9.16	Provision of full details of the support Contract prior to hand-over.	10 Working Days
10.1	The Principal’s approval on the departure from fibre connection	10 Working Days
10.20	Proposed ITS Communications Network	10 Working Days
11.12	The Principal’s approval to use SNMP version 2c	5 Working Days
11.29	The Principal’s approval of network equipment configuration	10 Working Days
11.42	Security Audit Report	10 Working Days
13.9	Design calculations, drawings and other Design Documents (only where design of the support forms part of this contract)	10 Working Days

20 Appendix 1: ITS Network Reference Design


Access Network
Local Servers (NVR, Flux, etc.)
100Base-T or 1000-Base T access links
Video Wall (or other) PCs as required
Local Workstations
Local Security Cameras
UPS/Generator/Other Equipment
Etherchannel/ Portchannel (LACP) links to Distribution Switch Stack
1Gbps uplinks – copper or fibre
ITS-A (Roadside) Network
ITS-B (Roadside) Network
ITS-C (Roadside) Network
ITS-D (Roadside) Network
Layer 3 Switch Stack terminating field network rings
Field Firewall Cluster (preferred) or Active/Passive Pair
Field Network
L3 Distribution Switch Stack Intra-site/inter-VLAN routing
Site Routers Inter-site Routing PIM Sparse Mode Multicast RP's
Distribution Network
MABN Core Switches
MABN Backbone (Core) Ring A
MABN Backbone (Core) Ring B
MABN L3 Core Switches

Notes:

(1) All equipment shown on this drawing shall be supplied, licensed, installed and site tested by the Contractor

(2) DPTI shall be responsible for reviewing/ approving configuration of all network equipment shown on this drawing.

(3) The Contractor shall perform Factory Acceptance Testing with all equipment, in close coordination with DPTI's nominated representative.