PART R63

TELECOMMUNICATIONS NETWORK

CONTENTS

1. GENERAL

.1 This Part specifies the requirements for the Principal's Telecommunications Network (PTN) as infrastructure for an Intelligent Transport System (ITS). This refers to the architectural, functional, operational, and technical requirements for the network and related Equipment as well as procedural requirements in regards to installation, commissioning, training and maintenance. This Part shall be read in conjunction with Part R60 General Requirements for the Supply of ITS Equipment and if installation forms part of this Contract, Part R61 Installation of ITS Equipment.

.2 The PTN shall transmit all data, video and voice between field devices and network node cabinets at the road-side and provide also a suitable communications path to the Principal's Traffic Management (or Control) Centre (TMC). The scope of the communications provided by the network specification may include:

Field Network fibre backbone communications which connect the Field Equipment Sub-Networks (FES) along the facility;

Backhaul communications which provide connectivity between the Field Network and the TMC or in some instances to a designated access point to the existing ITS network infrastructure;

Field switches (Field Network nodes) which provide multi-port Ethernet connectivity to the FES;

Ethernet communications to each FES.

.3 Documents referenced in this Part are listed below:

AS1044	Radio disturbance characteristics
AS1170.1	Structural design Actions - Permanent, imposed and other actions
AS1664	Aluminium structures
AS1768	Lightning protection
AS2578	Traffic signal controllers - Physical and electrical compatibility
AS3000	Electrical installation-building structure and premises (wiring rules)
AS3085.1	Telecommunications installations - Administration of communications cabling systems - Basic requirements
AS3990	Mechanical Equipment - Steelwork
AS4055-2006	Wind loads for housing
AS4070	Recommended practices for protection of low-voltage electrical installations and Equipment in MEN systems from transient over-voltages
AS60529	Degrees of protection provided by enclosures (IP Code)
AS61508	Functional Safety for Electrical/Electronic/Programmable Electronic Safety-related Systems
AS/ACIF S008:2006	Requirements for customer cabling products
AS/ACIF S009:2006	Installation requirements for customer cabling
AS 3100	Approval and test – General requirements for electrical Equipment
AS 7799.2	Information security management - Specification for information security management systems
AS 17799	Information technology – Code of practice for information security management

.4 Equipment supplied under this Contract shall comply with applicable Australian Standards, or where no appropriate Australian Standard exists, the Equipment shall comply with the appropriate British Standard.

.5 The telecommunications Equipment shall comply with relevant Australian Communications Authority technical standards and requirements. Equipment requiring connection to telephone lines shall be Austel approved and be labelled with the appropriate approval number. All radio communications shall comply with the requirements of the Australian Department of Communications.

.6 The following abbreviations are used in this Part:

CCTV	Closed Circuit Television
EIA	Electronic Industries Alliance
FAT	Factory Acceptance Test
FES	Field Equipment Sub-Network
FP	Field Processor
LAN	Local Area Network
LED	Light Emitting Diode
ITS	Intelligent Transport Systems
STREAMS	Traffic Management system developed by Transmax Pty Ltd
TMC	Traffic Management Centre
VLAN	Virtual LAN
VMS	Variable Message Signs
OSPF	Open Shortest Path First
POA	Point of Access (of a Field Equipment Sub-Network into a Field Network)
PPP	Point-to-Point Protocol
QoS	Quality of Service
RIP	Routing Information Protocol
SAT	Site Acceptance Test
SIAT	Site Integration Acceptance Test
SNMP	Simple Network Management Protocol
TMC	Traffic Management Centre (also Traffic Control Centre)

2. QUALITY REQUIREMENTS

.1 The Contractor shall prepare and implement a Quality Plan that includes the following documentation: Acceptance test plans, which provides full details of tests necessary;

Training plan;

Routine maintenance recommendations; and

Spare part requirements.

.2 If not submitted beforehand, the documentation required by this Clause shall be submitted at least 28 days prior to the commencement of site work or placing an order for Equipment.

.3 Provision of the documentation listed in this Clause shall constitute a **HOLD POINT**.

3. ARCHITECTURAL REQUIREMENTS

Network Architecture

.1 The network shall connect to and integrate with the Principal's Intelligent Transport Systems (ITS) Network and provide connectivity between the TMC and field Equipment network sites along the proposed Facility.

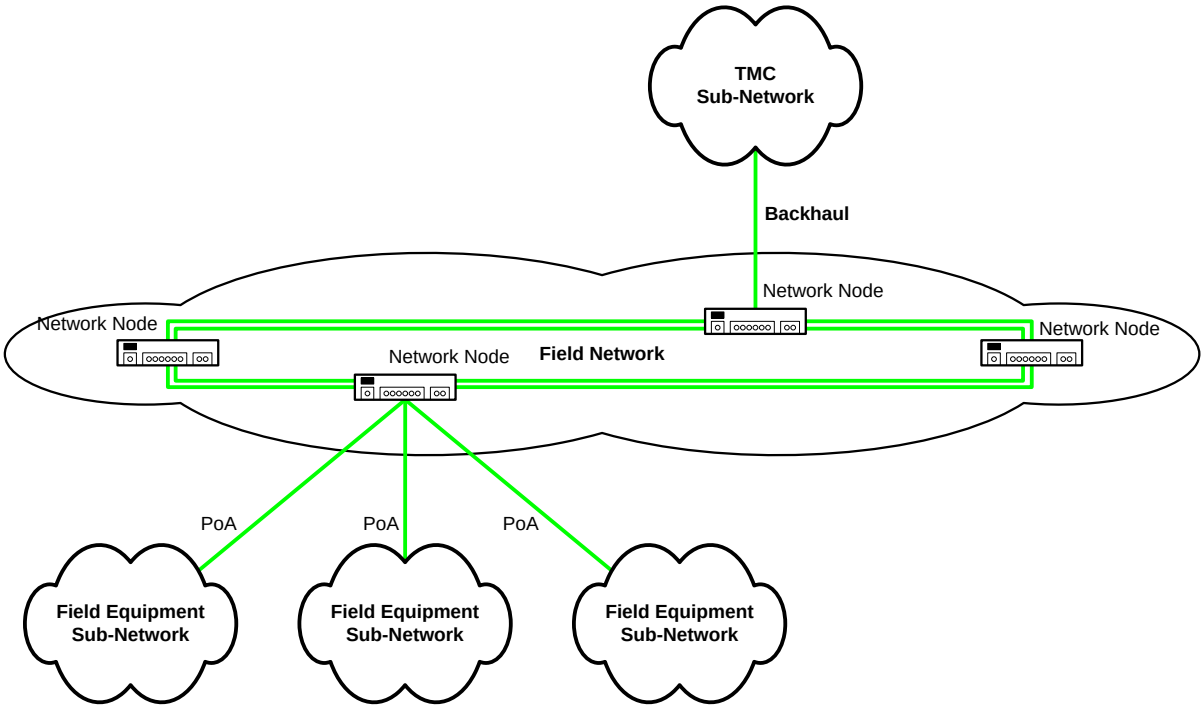

Figure 1 - ITS Network Architecture

.2 The standard ITS network is based on a hierarchical network design as specified Figure 1.

Field Network

.3 The Field Network should consist of a full duplex, bi-directional backbone ring with a number of Network Nodes to connect the Field Equipment Sub-Networks (FES) with the TMC.

.4 The network should connect via a Layer 3 (IP routable) switch to the ITS backbone which in turn connects to a router or switch with Layer 3 functionality at the TMC. An IP address range for the Field Network shall be allocated by the authorised manager of the ITS Network, as appointed by the Principal. IP Allocation on this range shall conform to the relevant ITS Network IP Allocation Policy as specified in the Project-Specific Requirements.

Backbone Architecture

.5 The backbone shall extend along the full length of the facility as a Field Network. The Field Network will be accessible at a number of ITS Points of Access (POAs) along the facility, as required, to connect field Equipment in localised areas.

.6 A full duplex, asymmetric, redundant fibre ring should be installed along the full length of the facility. The ring shall add a level of redundancy against failure of the fibre Equipment. However, it will not provide physical separation if the fibre cores are housed in one conduit (referred to as a collapsed ring architecture). Alternatively, a wireless backbone can be deployed along the facility, utilising either a ring or a mesh topology to achieve the same level of redundancy as the aforementioned fibre ring.

.7 To overcome the limited redundancy of the collapsed ring architecture, it is advised to place one network node at each end of the proposed backbone. These nodes will then individually connect back to the TMC (by the means of fibre, xDSL, GWIP, or the like), thereby creating a real redundant ring with the backbone along the road (refer to Figure 2 for a fibre solution). If the fibre core is severed at any point, the surrounding switches on the ring shall automatically route around the break-point through the additional communications paths.

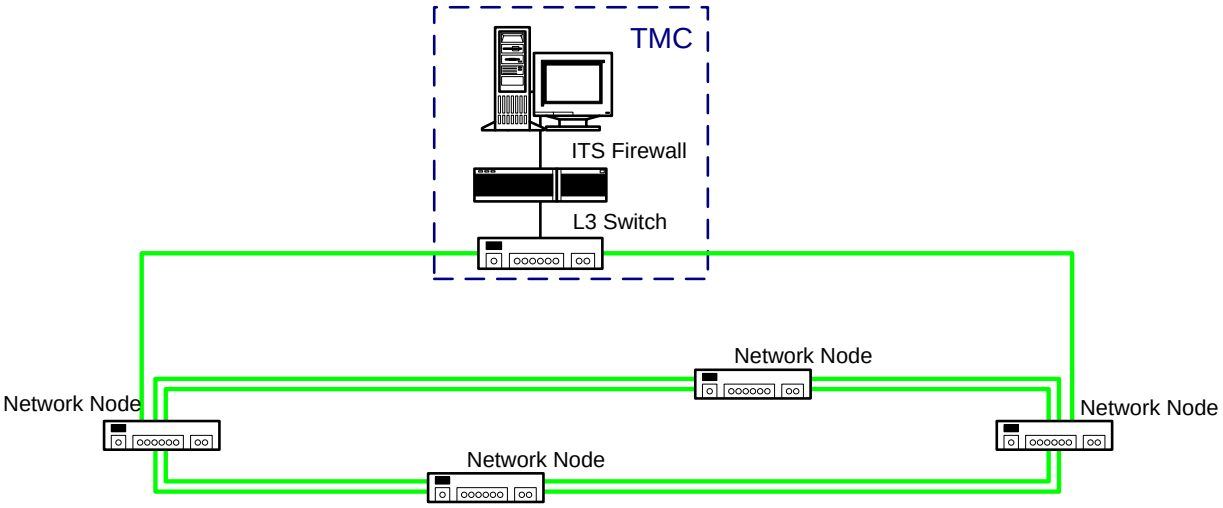

Figure 2: Redundant Fibre Ring Concept

.8 Alternatively, a wireless backbone can be deployed to provide a redundant communications path for the fibre backbone or vice versa. An adequate technology is strongly dependent on project specific requirements and will be defined in more detail in the project specific design documentation, as defined in the contract.

.9 Equipment should use dynamic routing protocols such as RIP or OSPF to achieve the desired functionality. All Equipment used on the backbone should be configured as Layer 3 devices and be compatible for route distribution. Dynamic routing updates should use industry standard routing authentication. Configuration information shall be given to the Principal.

.10 The backbone architecture shall be modular in design with demonstrated capability to facilitate future network expansion and minimise future associated costs.

.11 Communications protocols shall support Equipment from multiple vendors.

ITS Network Points of Access (POAs)

.12 An ITS Network Point of Access (POA) is the connection point of a FES into the Field Network. Electrically isolated communications links such as fibre or wireless are preferred.

Field Equipment Sub-Network (FES)

.13 A FES typically connects Field Equipment in a localised area either via an FP or directly to the Network Node in the case of IP video. At least one field processor is normally installed at each ITS Network POA if any field device (excluding cameras) connects through the POA.

.14 If more than one network device is to be connected at a certain location an Ethernet switch shall be provided. At least two (2) spare (unused) ports per site should be provided in this case. Industry standard patch leads shall be used to connect all Equipment. Electrically isolated communications links such as fibre or wireless are preferred. The FES should be connected to the Field Network by a standard RJ-45 10Base-T or 100Base-TX Ethernet connection.

TMC Sub-Network

.15 The ITS Control system's (e.g. STREAMS) application server and work stations are located on an Ethernet LAN within the TMC. Connectivity between the Field Network and this LAN is provided via a Layer 3 switch and a firewall at the TMC. Switch and Firewall are outside of the scope of this standard.

STREAMS Architecture Overview

.16 STREAMS is a platform used for management and control of road traffic on motorways and arterial roads. The STREAMS system typically consists of a suite of distributed software applications operating on a STREAMS Application Server located in a TMC and on STREAMS Field Processors located in the field. STREAMS Workstations provide a user interface to the applications.

.17 Unless otherwise specified, all field devices shall connect to STREAMS through a FP. STREAMS ensures that data telecommunications between the STREAMS server and the FPs are secure.

4. FUNCTIONAL REQUIREMENTS

Connectivity

.1 The Field Network shall provide total connectivity between the Equipment and the TMC.

System and Device Interfaces

.2 The Equipment shall be connected to Field Processors. Industry-standard hardware interfaces for Ethernet and serial protocols shall be used. ITS devices and/or systems shall connect to the Field Equipment Sub-Network using either:
an Ethernet LAN connection with a data rate of 10/100 Mbps UTP connection; or
via a Field Processor using serial communication.

Network connections

.3 The communications system shall provide full-duplex connectivity between the TMC (or the defined point of access to an existing ITS network infrastructure) and an Ethernet port at the FES. The network shall be of a modular design to facilitate future network expansion and minimise future associated costs. The network shall be suitable for connecting devices from multiple vendors.

.4 It shall be possible for Equipment with network interfaces connected to a POA to dynamically receive an IP address and have a routing path (in both directions) to the Layer 3 switch located at the TMC. The supply and configuration of the layer 3 switch (router) and firewall located at the TMC may be performed by others as specified in the Contract.

.5 Virtual local area networks (VLAN) tagging support shall be available to logically combine (and network isolate) parts of the system providing the same function, if required.

.6 Dynamic routing protocols such as RIP or OSPF should be used to support redundant backbone connections. Dynamic routing updates shall use industry-standard routing authentication.

.7 Direct links between ITS devices and Ethernet switches should support Ethernet LAN connections at 10/100Mbps.

Serial Connections

.8 Serial links between ITS devices and/or systems and FPs should support EIA RS232 and RS422/RS485 interfaces.

.9 More than one ITS device and/or system may be connected to a single FP. Where an ITS device and/or system is located remote to an FP an alternative communication link shall be provided. Electrically isolated communication links such as fibre or wireless are preferred; however a copper solution may be implemented, if suitable.

.10 Media converters, if necessary to transmit serial data over longer distances, shall comply with the requirements for network Equipment as specified in this standard.

Level of Service

.11 The Field Network shall provide the specified acceptable level of service (e.g. bandwidth, latency, etc.) to support all Equipment connected by it, and provide sufficient capacity for future growth in connected devices.

Redundancy

.12 Certain traffic management applications are considered “mission critical” ie failure or disruption will result in a major disruption(s) to traffic management operations. Depending on their requirements the Field Network and connecting Equipment should have a high level of availability to deliver a continuous service. Full redundancy is achieved by ensuring there is no single point of failure in the communications path between the field processor or networked device in the FES and the TMC.

.13 If the primary communications channel is deployed as bus or collapsed ring (i.e. more than one segment of a fibre ring share the same physical conduit), a secondary communications channel should be provided to provide full backup of the primary network (refer to .4). This secondary communications channel shall provide full-duplex communications and utilise a separate physical route to that of the primary communication channel. Where physical separation of fibre segments or a (redundant) wireless network are provided a secondary communications channel is not necessary.

Dynamic Routing

.14 Data shall be routed via the primary communications channel as the first preference. However, in the case of failure or congestions of segments of the primary channel traffic needs to be routed around these failures. Traffic is to be re-routed to the primary ring after of restoration of the affected segment within the time specified by the Principal.

Security

.15 Connected Equipment cannot afford to be compromised, as information transmitted over the network (e.g. camera images) can be of a sensitive nature. The chosen transmission media of the network shall have a high level of security to protect the connected Equipment and the transferred data.

.16 To ensure a high level of security, the network Equipment shall comply with the ITS Network security requirements for authentication, data integrity and visibility as specified in relevant South Australian Government security standards. The Contractor shall undertake a security audit to ensure that these requirements are met and will be carried out as specified in the Contract.

.17 All network Equipment shall support secured communication and password protection for access to the configuration. Physical access to network Equipment shall be restricted to authorised user by putting appropriate physical security mechanisms in place.

.18 Communications between network Equipment is only granted after successful authentication. The required level of authentication is defined in the Contract Specific Requirements. Appropriate mechanisms to meet those requirements have to be proven in the design.

.19 ITS network data on the backhaul shall be separated from other traffic sharing this medium. This can be implemented on a physical circuit basis using separate fibre cores or integrated in a virtual circuit technology over optical fibre or other technologies (i.e. using dedicated logical links such as VPN, MPLS or VLAN).

Communication Standards

.20 The Field Network is a long term infrastructure investment. To protect this investment Equipment constituting the network should use non-proprietary standard communication protocols.

.21 Equipment and protocols deployed in the network shall use non-proprietary, open standards to ensure future support and expansion. If the Contractor proposes to use proprietary solutions, the Contractor has to provide evidence in the design that advantages of this solution outweigh the limitations of proprietary systems.

Scalability

.22 The Field Network shall be designed to allow for future geographical extension; this capability shall be demonstrated in the design.

Manageability

.23 The Field Network will be managed remotely. The Equipment used to implement the network shall have the capability to be managed remotely.

Special Requirements

.24 The Field Network will transmit different data streams with individual priorities. The network shall be able to control the traffic flow in accordance with these requirements.

CCTV

.25 CCTV video images and control data (compressed or otherwise) transmitted on an Ethernet LAN connection shall use the Internet Protocol (IP) and be transmitted over the same communications channel. The CCTV camera control system data and the video images shall be transmitted over the PTN but may be isolated from other telecommunications traffic/applications where shown in the design documentation. Where data from the vehicle detectors and/or system data share the same communications channels as CCTV data, QoS mechanisms shall be utilised to give priority to the vehicle detector and/or system data.

Vehicle Tolling Data

.26 The PTN shall be suitable to allow data concerned with the Principal's vehicle tolling operations to be transmitted using the PTN, if required. Where CCTV data shares the same communications channel as vehicle tolling data, Quality of Service (QoS) techniques shall be utilised to give priority to the vehicle tolling data.

5. OPERATIONAL REQUIREMENTS

Availability

.1 Unless otherwise specified:
Equipment and systems shall have an operational availability as specified by the Principal.

The MTBF shall comply with the requirements stated by the Principal.

After a power outage, the Equipment is expected return to a fully operational state without manual intervention (i.e. manually switching on, starting applications or loading configurations).

Failure Modes

.2 In the case of failure, the network Equipment shall react in a deterministic way thereby minimising the chance for loss of communication and/or data. The Equipment shall:
where specified, enter or display a default mode during power and/or communications failure;

automatically shut down in a safe manner upon power and/or communications failure; and/or

automatically restart in a safe manner upon restoration of power supply and/or communications.

.3 In addition, the Equipment shall:
be assessed for functional safety in accordance with AS 61508; and

comply with the assessed functional safety requirements as specified in AS 61508.

Security

.4 All Equipment shall be developed in accordance with, and with due regard to AS 17799 and AS 7799.2.

6. TECHNICAL REQUIREMENTS

Level of Service

.1 The network shall provide an adequate level of service (e.g. bandwidth, latency, etc.) to support all Equipment connected to it, and to provide sufficient capacity for future growth.

Quality of Service

.2 Unless otherwise specified, the latency and jitter in data communications across the Field Network shall be on average not higher than 20 msec for wired and 40 msec for wireless networks. However, the combined latency between the field Equipment and the layer 3 switch in the TMC shall not exceed 40 msec (100 msec respectively) in a fully loaded network. Unless specified otherwise, the latency of individual pieces of network Equipment shall not exceed 5 msec.

Bandwidth

.3 The PTN shall provide an adequate level of service (e.g. bandwidth, latency etc.) to support all Equipment connected to it, and provide sufficient capacity for future growth in connected devices. The network shall provide sufficient capacity to transmit the data specified in the contract plus an additional 50% traffic.

.4 However, a fibre-based primary Field Network backbone shall utilise Gigabit Ethernet (1000Mbs) and the FES Fast Ethernet (100Mbs), as a minimum. Network traffic calculations are to be included in the design. Depending on the network operations (e.g. data or video) different numbers may be defined in the Project-Specific Requirements.

.5 Where redundant communications channel utilise a medium other than fibre, these channel may provide a reduced bandwidth, as long as they are sufficient to carry the traffic from the primary channel in the case of failure. Notwithstanding the above requirements, the network design and Equipment shall ensure economic use of capacity (i.e. QoS techniques rather than more bandwidth).

Traffic Calculation

.6 Traffic calculations should be included in the Contractor's design document, considering the average bandwidth requirements of field Equipment and the field Equipment locations. It should contain a list of field and network Equipment and its required bandwidth:

Type of field Equipment; e.g. FP with VMS:	an average of xxx kbit/s each
Type of field Equipment; e.g. PTZ camera:	an average of xxx Mbit/s each

Note: If it is not required that all CCTV sites deliver data simultaneously the necessary upload bandwidth will be reduced.

.7 The total expected traffic for up- and download in the PTN shall be contained in the calculations:

Upload (from the field):	xxx Mbit/s
Download (to the field):	xxx Mbit/s

Manageability

.8 Equipment installed as part of the network shall support remote management from the TMC. Remote management of network Equipment is supported through:
Simple network management protocol (SNMP).
Web-based secure interface to enable configuration and management.

.9 The deployed Equipment shall be capable of being managed centrally by the use of a network management software system. This software shall have functions for performance monitoring, diagnostics and the management of the network configuration, security, quality of service and resources down to the device interface level. Name and Version of the used or planned Network Management System Application is to be provided by the Principal upon request by the Contractor.

.10 If multiple Field Networks are included in the network design, all network management protocols shall be integrated.

.11 The software shall be able to operate from any STREAMS workstation (running Microsoft XP Professional) on the TMC's LAN.

Ethernet switches

Backbone Communications

.12 Switches, deployed as part of the backbone, shall comply with the following:
high speed LAN switching and routing – Ethernet / TCP / IP based;
interface speeds up to 1Gbps;
ability to support multiple media types (e.g. fibre single mode and multi mode) via hot swappable modules;
number of data ports sufficient to meet contractual requirements;
full-duplex operation on all ports;
auto-negotiation for automatically selecting half-and full-duplex operation;
congestion control features including IEEE 802.3x-based flow control;
maintenance hot-swappable;
software upgradeable;
user-selectable address learning mode;
web-based network management;
redundant switching fabric;
redundant power supply;
VLAN tagging support;
at least 1024 MAC addresses configurable;
QoS to support prioritisation of data streams; and
configuration of QoS priorities via network management software.

Field Equipment Sub-Network

.13 Switches, deployed as part of the FES, shall comply with the following:
high speed LAN switching – Ethernet / TCP / IP based;

interface speeds up to 100 Mbps;
ability to support multiple media types (e.g. fibre single mode and multi mode) via hot swappable modules;
number of data ports sufficient to meet contractual requirements;
full-duplex operation on all ports;
auto-negotiation for automatically selecting half-and full-duplex operation;
congestion control features including IEEE 802.3x-based flow control;
software upgradeable;
user-selectable address learning mode;
web-based network management; and
VLAN tagging support.

Standards

.14 Network Equipment deployed as part of the ITS network needs to comply with the relevant standards (protocols and transmission technologies).

Network Installation

.15 Faultless installation and operation of the backbone is crucial for the network communications. The minimum optical performance requirements for Single Model Optical Fibre (SMOF) and applicable standards for wireless installations are described in this section.

Fibre Installation

.16 All telecommunication cables shall comply with Part R70 Telecommunications Cabling.

Wireless Installation

.17 This sub-clause applies only where wireless technology is to be used.

.18 Where practicable, antennas should be positioned so that Line of Sight to the opposite communication partner is guaranteed. Installation of Antennas shall not impact traffic and/or pedestrians. Antennas should be placed on structures that protect the Equipment from unauthorised access and vandalism. However, easy and safe access for maintenance staff shall be allowed for. Antennas shall be connected to related Equipment via industry standard connectors.

.19 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.

.20 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 AS4055-1992. Wireless antennas shall be fitted with suitable surge protection to protect connected network and ITS Equipment in the event of a lightning strike. Surge protection is in accordance with ITS-01.

Indicators

.21 The network Equipment shall comply with the following:
status LEDs: Link Integrity, Disabled, Activity, and Full-Duplex indicators for each port; and
system status LEDs: System, RPS, Module Enabled and bandwidth utilisation indicator.

Connectors and Cabling

.22 Cabling shall comply with Part R70 Telecommunications Cabling. The network Equipment connectors shall comply with the following:
for 10Mbps ports: RJ-45 connectors; two pair Category 3, 4 or 5 UTP cabling; DB15 connector on AUI port;
for 100BaseTX ports: RJ-45 connectors; two-pair Category 5 UTP cabling;
for 100BaseFX and Gigabit Ethernet: SC connector, fibre optic cabling; and
for management console port: RJ-45 connector.

.23 Cables intended for connection of network Equipment to a telecommunications network shall comply with the requirements of the AS/ACIF S008:2006.

Physical Interfaces

.24 Physical interfaces provided at the POA shall utilise industry-standard connections. Physical interconnections shall be captive, (in the following order of precedence):
automatic “click” type (such as RJ-45);
manual “click” type; and
screw-type.

.25 Enclosures that incorporate conduits for entry of telecommunication cables shall comply with the requirements of the AS/ACIF S009.

Power

.26 The network Equipment should support input voltages between 100 and 240 VAC and shall be supplied with redundant power modules.

.27 If the Equipment is specified for other voltages, a converter has to be provided accordingly. Network Equipment specified for DC voltages shall have overload current and reverse polarity protection.

Network Node Cabinets

.28 Network node cabinets shall be used to house termination of the fibre optic cables and provide a telecommunications concentration point for connection between the Field Network and FES. The Network Nodes shall also allow for a full-duplex, bi-directional ring connecting the PTN and TMC.

.29 The requirements for cabinets are specified in Part R65 ITS Enclosures (for network node cabinets). Unless specified otherwise, cabinets shall be located at points of data concentration and in a way that connections to mains power and leased telecommunication services can be easily made.

.30 Provision of the final locations shall constitute a **HOLD POINT**.

.31 Network node cabinets shall comply with the following:
outer dimensions shall not exceed 1600mm (H), 2100mm (W) and 700mm (D);
the concrete mounting plinth shall be a single pour that contains a rag bolt assembly customised to suit the cabinet; and
the plinth shall extend at least 1200mm past the outer dimensions of the cabinet as part of the same pour as that housing the rag bolt assembly.

.32 Prior to installation, the Contractor shall allow inspection of the Equipment and provide FAT records and final design approval.

.33 Provision of the documentation shall constitute a **HOLD POINT**.

7. HOLD POINTS

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

CLAUSE REF.	HOLD POINT	RESPONSE TIME
2	Quality Plan	7 days
6.30	Locations of Network Node Cabinets	2 days
6.30	Provision of FAT Records	2 days