Government of South Australia
Department for Infrastructure and Transport

Communications Network Principles and Practices for Public Transport

Engineering Standard

Asset Management/Rail Commissioner

CE5-DOC-003525

DOCUMENT AMENDMENT RECORD

REV	CHANGE DESCRIPTION	DATE	COMMENTS
1	Release	08/02/18	
2	Review/updates	06/04/22	
3	Update for SAPTA and all transport modes, format change and document number change. MOCs KDA2563342 and TC052.	14/08/23	This Standard supersedes PTS-AR-10-CN-SPE-00200400
Document Review Schedule:		3 yearly	

TABLE OF CONTENTS

1. **Introduction** 4
2. **Purpose** 4
3. **Scope** 4
4. **Related Documents** 4
5. **References** 5
6. **Overview and requirements** 5
7. **Signalling Network** 6
8. **Communication Network Design** 6
   - 8.1. **CORE Communication Network Layer** 7
   - 8.2. **Interoperability Network Layer Design** 7
   - 8.3. **Hardware consideration** 7
9. **IP Address Scheme** 8
10. **Clock Synchronisation** 8
11. **AMPRN Cabling and Link Diversity** 8
    - 11.1. **Physical Diversity** 8
    - 11.2. **Route Diversity** 8
    - 11.3. **Cable / Path Diversity** 9
12. **Cabling Instructions** 9
    - 12.1. **New (Greenfield) Sites** 9
    - 12.2. **Existing (Brownfield) Sites** 9
    - 12.3. **Transmission** 9
    - 12.4. **Transmission Protocols** 9
13. **Engineering Waiver** 9
14. **Security** 10
    - 14.1. **Physical Security** 10

1. Introduction

The South Australian Public Transport Authority (SAPTA) is a Directorate within the Department for Infrastructure and Transport (DIT) responsible for the delivery of public transport services.

SAPTA on behalf of the department manages the Adelaide Metropolitan Public Transport Network (AMPRN). As part of the execution of responsibilities of this role, it must have a governance structure which includes the adoption of standards, policies, and procedures.

This document is intended to be read and applied by designers familiar with the principles and terminology generally employed by communication design engineers when performing tasks based on, or broadly complying with, communication design practices.

2. Purpose

The purpose of this document is to specify the principles for designing The Department's transport communications networks, associated architecture, and Infrastructure.

3. Scope

This Communications Network Principles and Practices for Public Transport document describes the fundamental principles to be adopted when designing the communication architecture and infrastructure for applications within the AMPRN and public transport digital communication environments and applies to both Safety Critical and non-Safety Critical systems.

These Principles must be applied to all new communication networks and systems within the AMPRN and public transport communication environments. Where significant alterations to existing networks are required, these Principles must be followed unless agreed otherwise in writing in accordance with the Engineering Waiver process by the respective Engineering discipline, with the aim to standardise the network architecture, improve network reliability and reduce the probability of total system failure and interruption to business operations.

4. Related Documents

DOCUMENT NAME	DOCUMENT NUMBER
ISMF – Information Security Management Framework	ID DFC / F4.1 Ver 3.3
Signalling Principles and Practices for the AMPRN	PTS-AR-10-SG-STD-00000068
Practices and Requirements for Tramline Signalling on the Adelaide Tram Network	SG2-DOC-002021
Protective Security Policy Framework	PC030
Communication, signalling and processing systems – Safety-related communication in transmission system	EN 50159
Public Transport Infrastructure Security Systems	PI5-DOC-003517
VSS/CCTV Scope of works procedure	PI5-DOC-003526
Railway Signalling Cables	SG4-DOC-000455
Pit and conduit standard for signalling and communication cables	PTS-MS-10-STD-00000094
Australian Government Physical Security Management Guidelines	Version 1.2 (Amended June 2016)
Digital Addressable Lighting Interface	IEC 62386
Signalling & Communications Project – Communications Subsystem Description	CE1-DOC-001254
Signalling & Communications Project – Communications Subsystem Application rules	CE1-DOC-001255
Management of Change – AMPRN Asset Baseline	PR-AM-GE-674

5. References

- *Rail Safety National Law Act (South Australia) 2012*
- *Adelaide Metropolitan Passenger Rail Network Rules and Procedures*
- *AS/NZ 3000*
- *EN 50129 – Communication, signalling and processing systems – Safety-related electronic systems for signalling*
- *EN 50126 – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part1: Basic requirements and generic process*
- *AS.4292.4 – Railway safety management – signalling and telecommunications systems and equipment*
- *AS/ACIF S008 Requirements for customer cabling products*
- *AS/ACIF S009 Installation requirements for customer cabling*
- *CISCO – Intelligent WAN Deployment Guide (April 2017)*
- *AS HB292-2006 A Practitioners Guide to Business Continuity Management*

6. Overview and requirements

The Department communication requirements used can be categorised onto two areas:

- Safety Critical (e.g., Signalling), or
- Non – Safety Critical (e.g., signalling Telemetry, Passenger Information, CCTV, Lighting, SCADA etc.).

All safety critical (Signalling) communications must adhere to *EN50159* which requires physical separation from non-Safety critical communications.

The Safety Critical systems (Signalling and Train Control systems) will operate on and be referred to as the “Signalling Network” and all non-Safety Critical systems will operate on and be referred to as the “Communication Network”.

Passenger Information & ICT is responsible for the control, support, and maintenance of the Communications Network.

Signals and Control System Engineering is responsible for the control, support, and maintenance of the Signalling Network.

Both categories may or will use the same or similar technologies and possibly perform business critical functions.

The separation of Safety Critical and Non-Safety Critical communications is to ensure there is no interference to Safety Critical systems from Non-Safety Critical systems and vice versa.

New systems installed into the communications network will be reviewed regarding the fault tolerance requirements and the risk they pose to other applications. This must be considered on a case-by-case basis to avoid single points of failure, where required, with the purpose to prevent disruption to mission critical services and applications resulting from transmission or equipment failures.

The fault tolerant architecture must be designed so no single point of failure can cause loss to the entire communications network. The design should consider redundant, diverse communication links, routes, hardware, and may deploy alternate technologies to achieve flexible, reliable, and highly available solutions.

Safety Critical and non-Safety Critical transmission cables may share a common conduit or trench installed in accordance with the Department’s “Pit and Conduit Standard for Signalling and Communication Cables”, *PTS-MS-10-STD-00000094* and *AS/NZS 3000* “Wiring Rules”.

Network equipment must implement SNMP (Simple Network Management Protocol) which will be presented to The Department provided SNMP server(s) which will make available proactive alarm reporting and access to historical performance statistics.

7. Signalling Network

Refer to the document “Signalling Principles and Practices for the Adelaide Metropolitan Passenger Rail Network”, number *PTS-AR-10-SG-STD-00000068* or the document “Practices and Requirements for Tramline Signalling on the Adelaide Tram Network”, number *SG2-DOC-002021*. Also refer to the signalling process.

8. Communication Network Design

The Communication Network comprises of two parts:

- CORE Network Layer
- Interoperability Network layer

Figure 1 below displays the CORE network layer which provides the centralised network or “backbone” which the non-Safety critical services and applications connect through. The non-Safety critical services are represented in the Interoperability Network Layer and are connected to the CORE network as required by The Department, by physical links with or without VPNs.

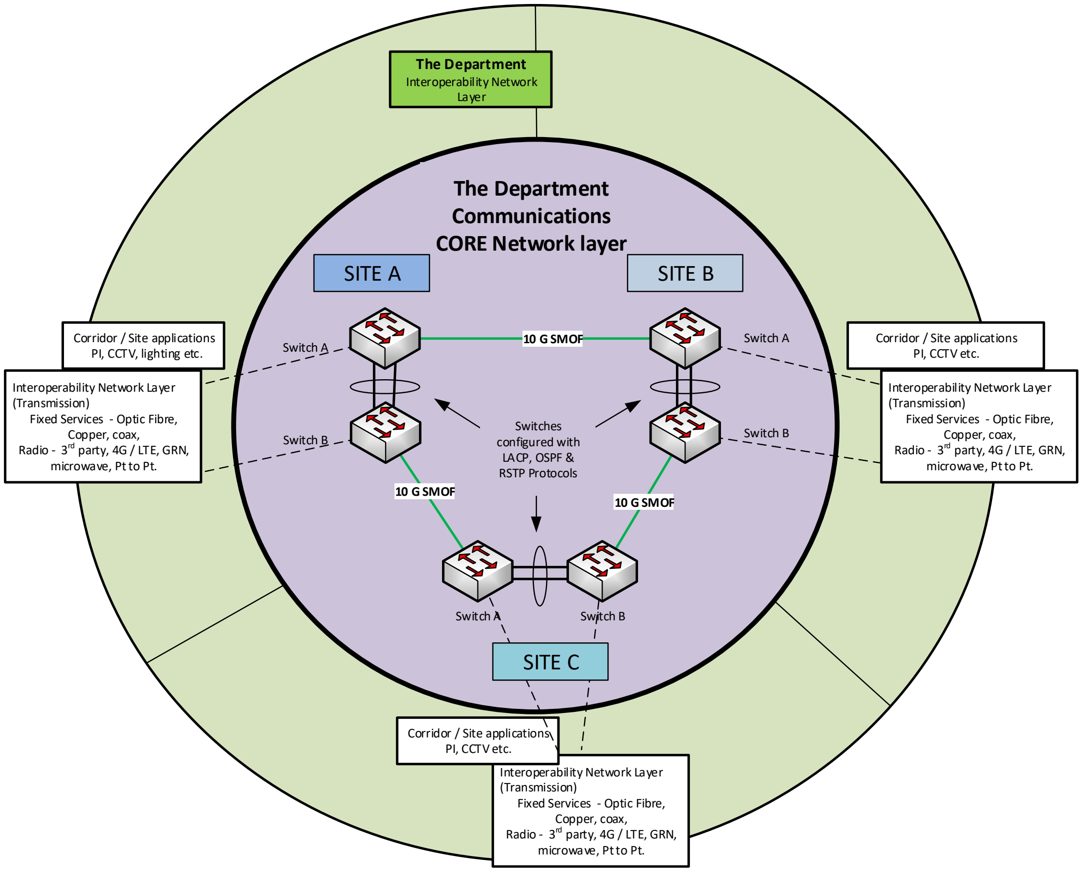
The Department
Interoperability Network Layer
The Department
Communications
CORE Network layer
SITE A
SITE B
SITE C
Switch A
Switch B
Switch A
Switch B
Switch A
Switch B
10 G SMOF
10 G SMOF
10 G SMOF
Switches configured with LACP, OSPF & RSTP Protocols
Corridor / Site applications
PI, CCTV, lighting etc.
Corridor / Site applications
PI, CCTV etc.
Corridor / Site applications
PI, CCTV etc.
Interoperability Network Layer
(Transmission)
Fixed Services - Optic Fibre, Copper, coax,
Radio - 3rd party, 4G / LTE, GRN, microwave, Pt to Pt.
Interoperability Network Layer
(Transmission)
Fixed Services - Optic Fibre, Copper, coax,
Radio - 3rd party, 4G / LTE, GRN, microwave, Pt to Pt.
Interoperability Network Layer
(Transmission)
Fixed Services - Optic Fibre, Copper, coax,
Radio - 3rd party, 4G / LTE, GRN, microwave, Pt to Pt.

Figure 1. Communications Network diagram, displaying the department’s Core Network and the outer Interoperability network Layer connecting operational services.

8.1. CORE Communication Network Layer

The CORE Communications Network must be designed as a Fixed Mesh (Node-to-Node) network which will tolerate single failure conditions to single transmission links and single network device failures and enable self-healing to allow data to pass in either direction. Remote locations or sites (e.g., Railway Stations, Bus inter-change locations, Operation Control Centre, and Support / Maintenance depots) will connect to the Core network via the Interoperability Network layer.

The Department's communications architecture must include the characteristics specified in the *EN 50159* Category 2 (open) network:

- ICT Standard network connecting different systems (broadly categorised as safety critical and non-Safety critical) within a controlled and limited environment.
- Network control and management systems are capable of routing messages via any path between applications.

The CORE network consists of three nodes which are physically separated and designed to support or incorporate the following:

- Standards based topology (e.g., use open source and non-propriety protocols, systems, and interfaces),
- Supports high (bursting) data bandwidth demands,
- A fixed Mesh (Node-to-Node) Topology with self-healing functionality for reliability and availability (configured using RSTP (802.1w) and LACP (802.3ad) protocols for network diversity and resilience),
- Network Path Diversity (Node / Link Diversity, Router / Switches redundancy),
- Scalable and modular design,
- Satisfy Operational requirements while in a degraded mode,
- Network and Application visibility with performance and fault monitoring,
- IPsec V2 tunnelling for privacy and integration protection, (Reference RFC5406 – "Guidelines for specifying the use of IPsec V2", for IPsec security considerations),
- Zone based firewalls/routers with strict access controls.

8.2. Interoperability Network Layer Design

The Interoperability Network layer will provide the network integration and distributed services across Communications / Business services. The Interoperability Network layer will be flexible and dynamic where new infrastructure and services are installed, reconfigured, or removed, with the ability for users, systems, and services to be integrated to work together and share information and functionality, as required.

The following are examples of services or applications:

- CCTV — Operates on a secure dedicated distributed data platform where the information and data are accessed and connected to the Security Control Hub, Police Security Services Branch, Operational Security, Operations Control Centre, and Maintenance Staff via The Department's Communication CORE Network,
- Passenger Information system (PI) — Each PI site operates independently with real time updates from the railway signalling system, with batch mode update data (PI update information) being automatically pushed out over night from a centralised location to all PI sites,
- Lighting (DALI) — This network is used to remotely manage and control the lighting services located at Railway stations, Tram stops or other infrastructure.

8.3. Hardware consideration

The following should be considered when new systems / infrastructure is being installed or upgraded:

- Redundant Routers, Switches and Servers
- Redundant Hot Swap Power supplies

- Redundant Hot Swap CPU assemblies
- Servers / Storage arrays to have RAID 1 or RAID 5 configurations with Hot Swap HDDs
- Suitable UPS (and generator) to support at least 5 hours up time without mains power, with remote management (Alarms and Control)
- Back-ups – Systems and Data
- Environmental Conditions

9. IP Address Scheme

The IP Address scheme will conform to the master IP Network plan. The master IP Address plan will be obtained from The Department and the development of IP address schemes must be developed in consultation with the responsible The Department IP Address administrator in the respective Engineering discipline.

10. Clock Synchronisation

All relevant system clocks in The Department communications network will be synchronised to the department's nominated time source.

11. AMPRN Cabling and Link Diversity

The department has installed an extensive optic fibre network along the electrified metropolitan rail corridors and is planning to install additional optic fibre when the remaining rail corridors are electrified.

The Department's electrified rail corridors provide secure and physically separated optic fibres in the rail corridor. The installed fibres are located in:

- Buried in conduit along the rail corridor, and
- Included in the overhead Optical Ground Wire (OPGW - IEEE 1138).

All new services and redundant links must use the existing The Department's infrastructure, where practical. If constraints exist, new infrastructure links must be considered in the following order:

1. The Department infrastructure (MABN) - optic fibre,
2. SabreNet optic fibre,
3. The department's infrastructure (Copper, Wireless links etc.),
4. Third Party networks (e.g., OPTUS NBN, Telstra GWIP services etc., 5G/4G / LTE tails with appropriate levels of service).

The aim of link diversity is to prevent disruption to operational services because of link or transmission failure. The level of link diversity must be considered for all new services and reviewed to determine the link fault diversity requirements on a user or case-by-case basis.

For example: Measured Failure (risk) verses link diversity cost for the level of diversity required (Risk Mitigation).

There are multiple options for link diversity available with associated complexity, cost, and risk. Listed below in order of preference are the diversity options,

11.1. Physical Diversity

The optic fibres and/or copper pairs for each path of the duplicated link are in separate cable routes or trunks and restricted to the rail corridor.

11.2. Route Diversity

Where physical diversity is not available or feasible in the rail corridor, alternate communication links and services should be considered. The links and services in order of preference may comprise of the following:

- Optical fibre,

- Copper Services, or
- Radio / Wireless (point to point services).

11.3. Cable / Path Diversity

The redundant services for each link or service, where possible, will use different cable ducts, routes, and cables.

12. Cabling Instructions

12.1. New (Greenfield) Sites

The communication cabling installed for all new (Greenfield) sites connected to The Department communication network must be:

- Single Mode Optic Fibre (SMOF) –1Gbs (or better) with a minimum 48 cores for the backbone fibre, and
- Ethernet Cat 6a (*AS 3080*) – (1 Gbs) for local LAN requirements

12.2. Existing (Brownfield) Sites

During any changes to existing sites, existing transmission cabling will be utilised to reduce expenses, provided such cabling can be reasonably expected to perform at the required speeds and reliability. Single Mode Optic Fibre cabling is the preferred option and must be undertaken when it is necessary for cabling to be replaced or upgraded.

Existing sites may consist of various cabling arrangements and listed below is the existing cabling preference order:

1. Single Mode Optic Fibre (minimum data speed 1Gb/s).
2. Multimode Optic Fibre (minimum data speed 100Mb/s; preferred data speed 1Gb/s). Multimode optical fibre can be used for enterprise and data centre applications up to the 500–600 metre range. Multimode optical fibre must conform to the OM3 standard as a minimum. Beyond this, single-mode optical fibre must be used.
3. UTP Cat5+ (minimum data speed 100Mb/s; preferred data speed 1Gb/s).
4. COAX (existing) as thin Ethernet (minimum data transmission speed 100Mb/s).

12.3. Transmission

The preferred option for all new installations is Single Mode Optic Fibre Cables.
If constraints exist, new transmission links must be considered in the following order:

1. Single Mode Optic Fibre (SMOF) – Minimum 1Gb/s,
2. Copper (xDSL – (SHDSL, VDSL2, ADSL) – Minimum 5 Mb/s),
3. Radio / Wireless Point to Point (Licensed / unlicensed),
4. Third Party (NBN, 5G/4G, Minimum 5 Mb/s sustained upload speeds).

12.4. Transmission Protocols

The following transmission protocols are widely used in the design of the AMPRN Communications network:

- TDM – SDH & PDH
- Stat MUX 802.2
- MPLS (Multiprotocol Label switching)
- VLANs / IPSEC
- Ethernet over Radio

13. Engineering Waiver

When the preferred option is not feasible due to physical or financial constraints, an alternate design (or solution) must be submitted in writing in accordance with the Engineering Waiver process with the respective Engineering discipline.

14. Security

The objective of security is to manage the security risk, to ensure confidentiality, reliability, availability, and integrity of the network, data, and infrastructure:

- Security threats and risks,
- Business requirements / objectives,
- Access controls and User management,
- Legal Statutory and Contractual requirements.

All care should be taken not to make available or disclose confidential information including network security and customer personal detail data to unauthorised parties.

All Agencies (Suppliers and contractors) are required to comply with the South Australian Government "South Australian Cyber Security Framework (SACSF)" which is a Cabinet approved, whole of government policy framework which draws on international best practice for risk based cyber security management.

14.1. Physical Security

The objective of physical security is to prevent unauthorised physical access, damage, and interference to The Department's communication information, operations, and infrastructure.

The Australian Government Physical Security Management Guidelines provides guidance to achieve a consistent approach to determining physical security controls for information and communications technology (ICT) equipment, systems and facilities holding Australian Government information.

For additional information on protection of information and ICT assets against environmental or man-made threats refer to:

- Australian Government Protective Security Policy Framework website https://www.protectivesecurity.gov.au/
- Australian Standard "*AS/NZS ISO/IEC 27002 Information Technology–Security techniques–Code of practice for information security Controls, Section – Physical and environmental security".*

The following should be considered as part of the physical controls and access for equipment rooms and huts:

- Electronic access control system (SiPass system currently used in The Department's transport infrastructure),
  - providing distributed management and control,
  - Controlled and monitored swipe card access,
  - Secure and restricted access,
  - Door Monitoring,
  - Intruder and equipment tamper alarms.
- Logging of all user access (audit trail),
- Camera monitoring for equipment rooms,
- Restricted (mechanical) and controlled keys for all equipment rooms and field cabinets (for example, door locks and field padlocks).