TS 06220:1.0

T MU TE 41004 ST

Standard

Packet Switched Networks – Wireless Local Area Networks

Issue date: 15 December 2023

Effective date: 15 December 2023

Disclaimer

This document has been prepared by Transport for NSW (TfNSW) specifically for its own use and is also available for use by NSW public transport agencies for transport assets.

Any third parties considering use of this document should obtain their own independent professional advice about the appropriateness of using this document and the accuracy of its contents. TfNSW disclaims all responsibility and liability arising whether directly or indirectly out of or in connection with the contents or use of this document.

TfNSW makes no warranty or representation in relation to the accuracy, currency or adequacy of this document or that the document is fit for purpose.

The inclusion of any third party material in this document, does not represent an endorsement by TfNSW of any third party product or service.

For queries regarding this document, please email Transport for NSW Asset Management Branch at standards@transport.nsw.gov.au or visit www.transport.nsw.gov.au

Document information

Owner: Director Telecom Engineering
Asset Management
Safety, Environment and Regulation

Mode: Multimodal

Discipline: Technology

Document history

Revision	Effective date	Summary of changes
1.0	25 August 2016	First issue as T MU TE 41004 ST.
1.0	15 December 2023	First issue as TS 06220. Version numbering recommenced in line with new designation. Changes from the previous version include extending application to all modes of transport, amendment of minor changes to technology implementation, removal of withdrawn international requirements and inclusion of latest requirements.

Preface

This standard is a first issue as TS 06220 and supersedes T MU TE 41004 ST *Packet Switched Networks – Wireless Local Area Networks*, version 1.0.

This document provides the requirements for WLANs, commonly known as wi-fi, used for the operational technology on TfNSW assets.

The requirements in the previous version (T MU TE 41004 ST version 1.0) were specific to WLAN systems used for heavy rail within the metropolitan rail area and to rapid transit. This document amends those requirements to suit light rail, metro, roads and maritime. It also amends minor changes to current technology implementation.

Table of contents

1 Scope

This standard specifies the functional requirements for WLAN system interfaces and minimum non-functional requirements for WLAN systems.

2 Application

This document applies to WLAN systems used in all transport modes.

This document is intended to be used by all parties involved in the design, installation, operation and maintenance of WLAN systems.

Operational technology comprises electronic or programmable electronic systems that satisfy at least one of the following conditions:

1. is necessary for customers to safely and securely use transport services
2. is necessary for one or more of the operating modes of transport services. For example, operating modes can include normal, interim, degraded, emergency and maintenance
3. monitors or controls systems that satisfy conditions 1 or 2.

3 Referenced documents

The following documents are cited in the text. For dated references, only the cited edition applies. For undated references, the latest edition of the referenced document applies.

International standards

EN 50125-3 *Railway applications – Environmental conditions for equipment – Part 3: Equipment for signalling and telecommunications*

IEC 60050-192 *International electrotechnical vocabulary – Part 192: Dependability*

IEEE 802.11 *Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*

IEEE 802.1X *IEEE Standard for Local and Metropolitan Area Networks – Port Based Network Access Control*

ISO/IEC 7498-1 *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model – Part 1*

PD IEC TR 62380 *Reliability data handbook. Universal model for reliability prediction of electronics components, PCBs and equipment*

Australian standards

AS/NZS 62368.1 *Audio/video, information and communication technology equipment – Part 1: Safety requirements*.

AS/NZS IEC 60825.1 *Safety of laser products – Part 1: Equipment classification and requirements*

AS/NZS IEC 60825.2 *Safety of laser products – Part 2: Safety of optical fibre communication systems (OFCSs)*

Transport for NSW standards

TS 00031.1 *OT10 Threat-Based Cyber Security Controls – Part 1: Controls and Implementation Requirements*

TS 03948 (T MU MD 81001 ST) *Common Requirements for Programmable Electronic Equipment*

TS 04003 (T MU RS 17002 ST) *Prohibited and Restricted Materials*

TS 04982 (T MU MD 20002 ST) *Risk Criteria for Use by Organisations Providing Engineering Services*

TS 04990 (T MU SY 10010 ST) *Cybersecurity for IACS – Overview*

TS 04991 (T MU SY 10012 ST) *Cybersecurity for IACS – Baseline Technical Cybersecurity System Requirements and Countermeasures*

TS 04993 (T MU SY 10013 PR) *Cybersecurity for IACS – Cyber Risk Management Procedure*

TS 06178 (T MU MD 00005 GU) *Type Approval of Products*

TS 06218 *Packet Switched Networks – Wired Networks*

TS 06219 (T MU TE 41003 ST) *Radiocommunication in LIPD Class Licensed Bands*

TS 06221 *Telecommunication Equipment – Network Management*

TS 06222 (T MU TE 81003 ST) *Test Processes and Documentation for Programmable Electronic Systems and Software*

Legislation

Industrial Chemicals (General) Rules 2019 (Cth)

Radiocommunications (Low Interference Potential Devices) Class Licence 2015 (Cth)

Other referenced documents

European Union, 2011, *Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment*

RFC 792 *Internet Control Message Protocol*

RFC 1122 *Requirements for Internet Hosts – Communication Layers*

RFC 1157 *A Simple Network Management Protocol (SNMP)*

RFC 1242 *Benchmarking Terminology for Network Interconnection Devices*

RFC 2865 *Remote Authentication Dial In User Service (RADIUS)*

RFC 2866 *RADIUS Accounting*

RFC 3412 *Message Processing and Dispatching for Simple Network Management Protocol (SNMP)*

RFC 3413 *Simple Network Management Protocol (SNMP) Applications*

RFC 3414 *User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)*

RFC 3415 *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

RFC 3416 *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

RFC 3417 *Transport Mappings for the Simple Network Management Protocol (SNMP)*

RFC 3418 *Management Information Base for the Simple Network Management Protocol (SNMP)*

RFC 4186 *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)*

RFC 4187 *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*

RFC 4443 *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*

RFC 5216 *The EAP-TLS Authentication Protocol*

RFC 5281 *Extensible Authentication Protocol Tunneled Transport Layer Security, Authenticated Protocol Version 0 (EAP-TTLSv0)*

RFC 5424 *The Syslog Protocol*

RFC 5448 *Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')*

RFC 6241 *Network Configuration Protocol (NETCONF)*

State of New South Wales, *NSW Cyber Security Policy*

Telcordia Technologies, 2016, SR-332 *Reliability Prediction Procedure for Electronic Equipment, Issue 4*

United States Department of Defense, 1991, MIL-HDBK-217F *Notice 2 Reliability Prediction of Electronic Equipment*

Wi-Fi Alliance, 2012, *Hotspot 2.0 (Release 3) Technical Specification*

4 Terms, definitions and abbreviations

The following terms, definitions and abbreviations apply in this document.

allow list a list of entities or users that are allowed to access a specific service, privilege or mobility

ANT antenna subsystem

AP access point subsystem

CBC-MAC cipher-block chaining with message authentication code

CFR constant failure rate; that period, if any, in the life of a non-repaired item during which the failure rate is proximately constant (Source: IEC 60050-191:1990)

chargen character generator protocol

configuration datastore as defined in RFC 6241

CPU central processing unit

CTR counter mode

DTE data terminal equipment; a computer system with one or more internet protocol addresses assigned to its network interfaces for the purpose of resource sharing amongst systems connected to the communication network

EOS end of sale; the date when the original equipment manufacturer withdraws a product from sale, both directly and through its authorised points of sale; for example, distributors and resellers

FOFS first offered for sale; the date when the original equipment manufacturer first offers a product for sale in the Australian market

FRU field replaceable unit

LAN local area network; communications network designed to connect computers and other intelligent devices in a limited geographic area (typically less than 10 km)

LIPD low interference potential device

metropolitan rail area area bounded by Newcastle (in the north), Richmond (in the northwest), Bowenfels (in the west), Macarthur (in the southwest) and Bomaderry (in the south), and all connection lines and sidings within these areas, but excluding private sidings

MTTF mean time to failure

NTP network time protocol

OEM original equipment manufacturer

RADIUS remote authentication dial-in user service

running configuration datastore as defined in RFC 6241

SNMP simple network management protocol

SNTP simple network time protocol

SSH secure shell

startup configuration datastore as defined in RFC 6241

TACACS+ terminal access controller access-control system plus

TfNSW Transport for NSW

WLAN wireless local area network

5 Functional requirements for WLAN system interfaces

The functional requirements specified in this document principally relate to the physical, data link and network layers of the open systems interconnection (OSI) model specified in ISO/IEC 7498-1 and the link and internet layers of the internet protocol suite (commonly referred to as the TCP/IP model).

System interfaces include the following:

- WLAN to wired LAN
- wireless DTE to WLAN
- WLAN to WLAN
- WLAN systems to physical environment
- WLAN systems to network management systems.

Figure 1 is a diagrammatic representation of the system interfaces. Figure 1 is informational and is not intended to convey any architectural information. The solid lines represent systems and system interfaces. The dashed lines within the solid lines represent subsystems and subsystem interfaces.

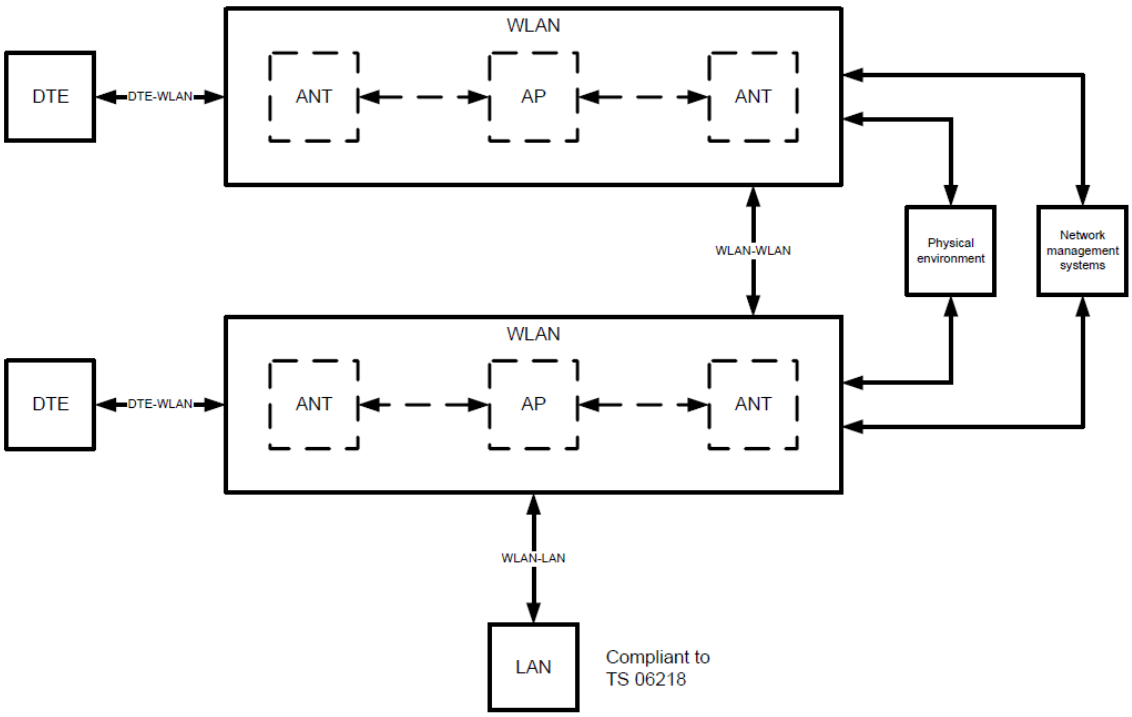

Figure 1 – System interfaces (informational)

5.1 Interfaces between WLAN and LAN systems

Figure 2 shows the interfaces between the WLAN and LAN systems.

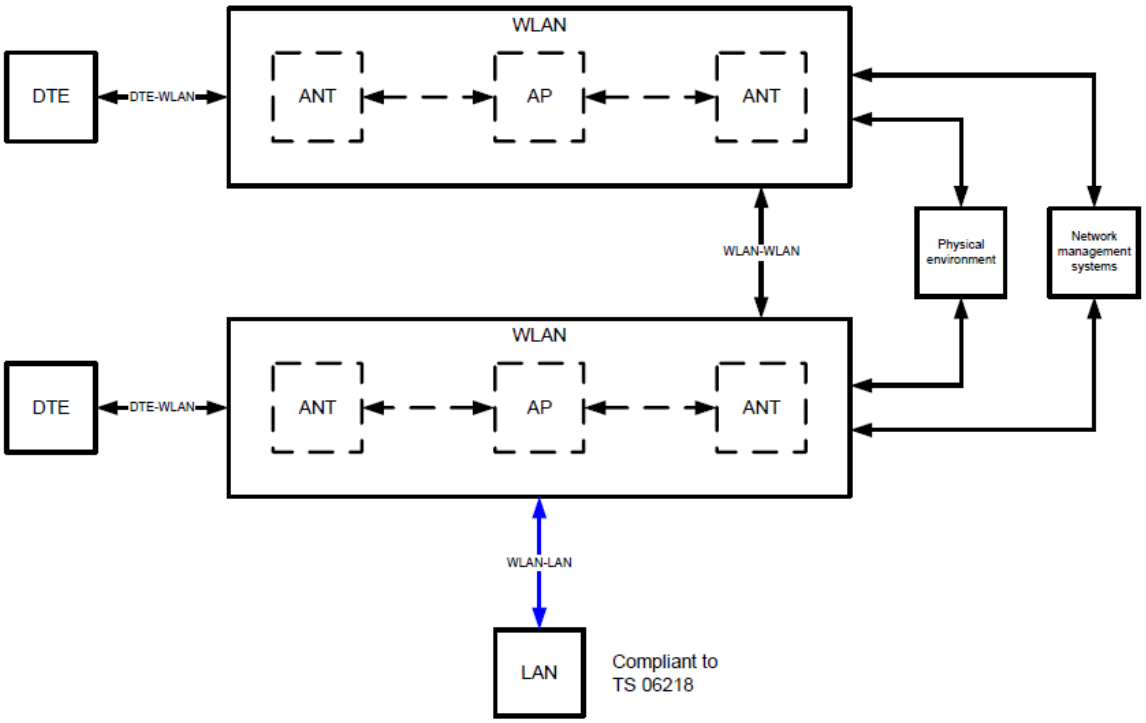

Figure 2 – WLAN to LAN system interfaces (informational)

WLAN systems shall comply with the requirements specified in TS 06218 as data communication equipment (DCE) for the following attributes:

- bridging and management, except the requirements for link layer discovery protocol (LLDP)
- 100 Mb/s ethernet interfaces
- 1 Gb/s ethernet interfaces
- modular transceiver packages, except the requirements for XFP (small form factor pluggable transceiver) and QSFP+ (4X pluggable transceiver)
- port-based network access control
- quality of service.

WLAN systems shall comply with the power over ethernet requirements provided in TS 06218 as DTE.

5.2 Interfaces between DTE and WLAN

Figure 3 shows interfaces between the wireless DTE and WLAN.

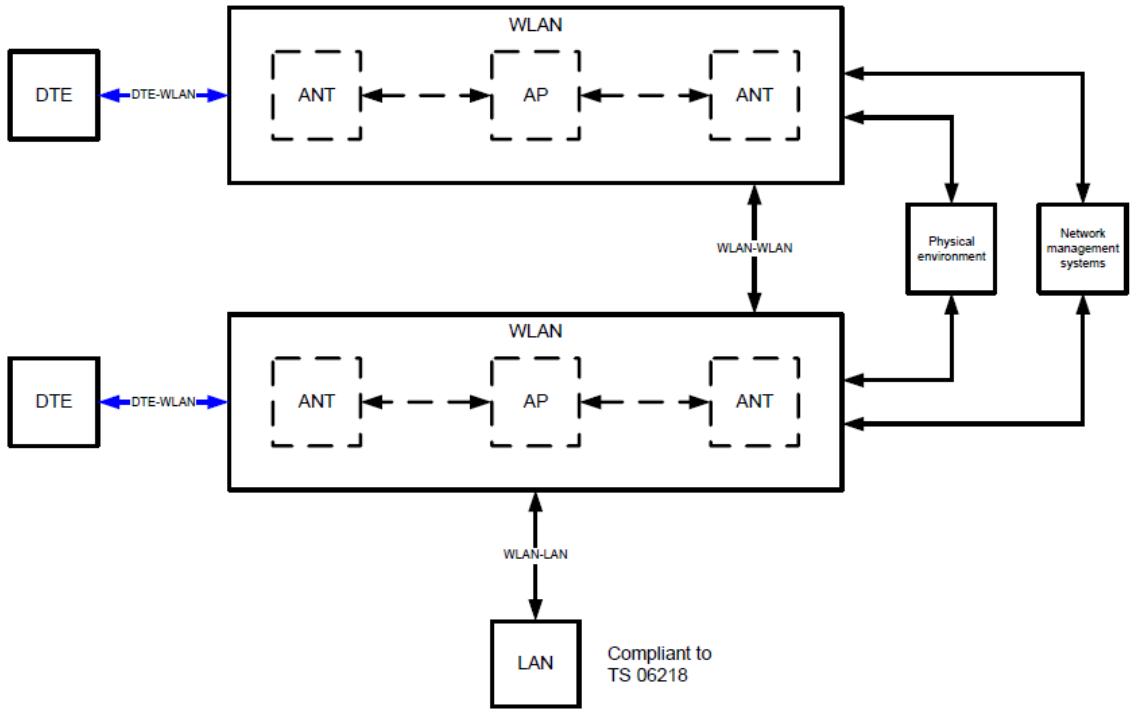

Figure 3 – DTE to WLAN system interfaces (informational)

5.2.1 Media access control and physical layer

Systems shall comply with the medium access control and physical layer specifications specified in IEEE 802.11, with the exception of physical layer specifications that use infrared or frequency-hopping spread spectrum.

Systems shall be configured to use the physical layer specifications specified in IEEE 802.11. For backwards compatibility, systems may be additionally configured to use the extended rate physical specifications (commonly known as IEEE 802.11).

Systems shall be configured to use CCMP which is CTR with CBC-MAC protocol as specified in IEEE 802.11.

Systems shall use one of the following extensible authentication protocol (EAP) methods:

- RFC 5216
- RFC 5281
- RFC 4186
- RFC 4187
- RFC 5448.

Systems shall be additionally configured to comply with IEEE 802.11 and the *Wi-Fi Alliance Hotspot 2.0 (Release 3) Technical Specification,* if public access to the system is to be provided (for example, to customer laptops, tablets, or smartphones).

5.2.2 Radiocommunications

Systems shall operate in class licensed bands as specified by items 55 to 57 and 59 to 63AB inclusive of Schedule 1 of the *Radiocommunications (Low Interference Potential Devices) Class Licence 2015*.

Systems shall comply with TS 06219.

5.3 Interfaces between WLAN systems

Figure 4 shows the interface between one WLAN system and another WLAN.

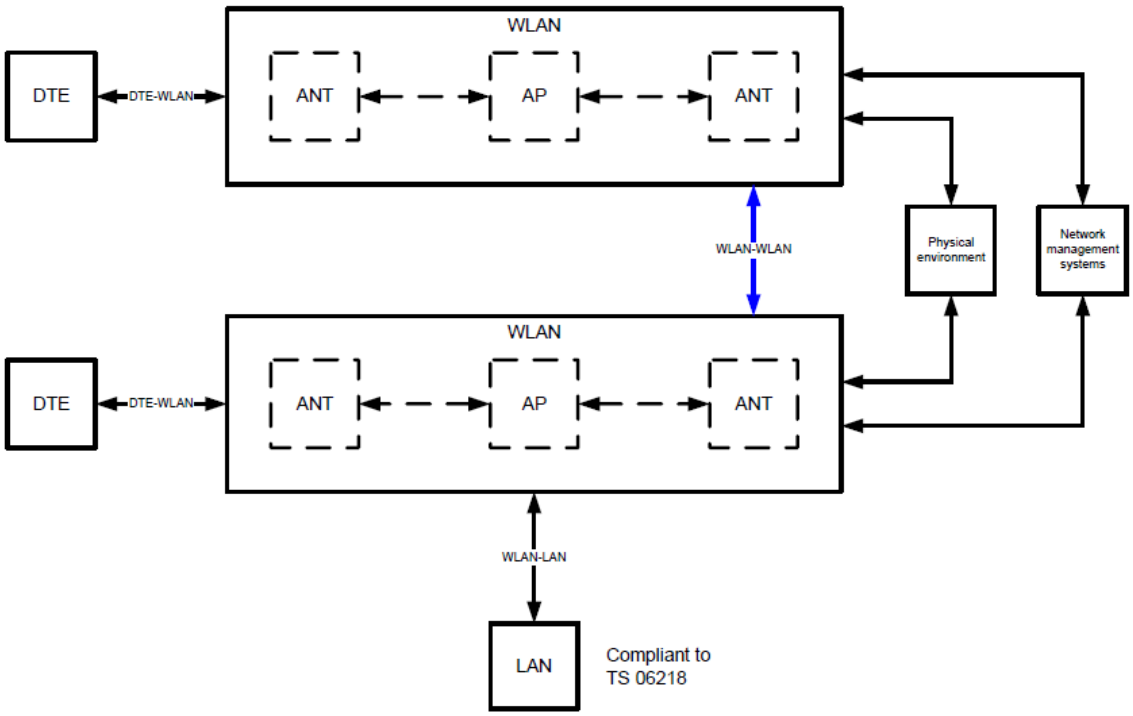

Figure 4 – WLAN to WLAN system interfaces (informational)

Systems shall comply with the requirements stated in Section 5.2 of this document.

Systems shall be configured to use mesh networking as specified in IEEE 802.11.

5.4 Interfaces to the physical environment

Figure 5 depicts the WLAN interfaces with the physical environment. The physical environment includes power supply, earth connections, equipment cords, environmental conditions and electromagnetic emissions and immunity.

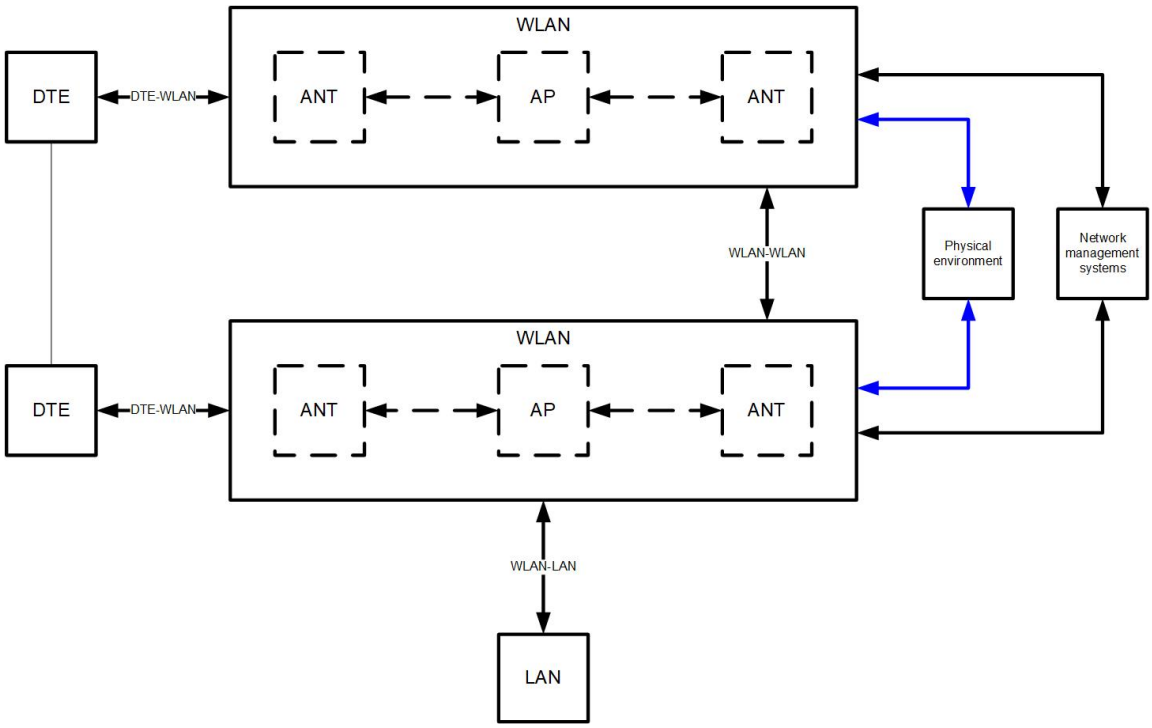

Figure 5 – Interfaces to the physical environment (informational)

WLAN systems shall comply with the requirements specified in TS 03948 for the following physical environment attributes:

- power supply interfaces
- earth connections
- equipment cords
- environmental conditions
- electromagnetic emissions and immunity.

5.5 Interfaces to network management systems

Figure 6 shows the WLAN interface with network management systems. Network management systems comprise fault and performance management, configuration management and security management.

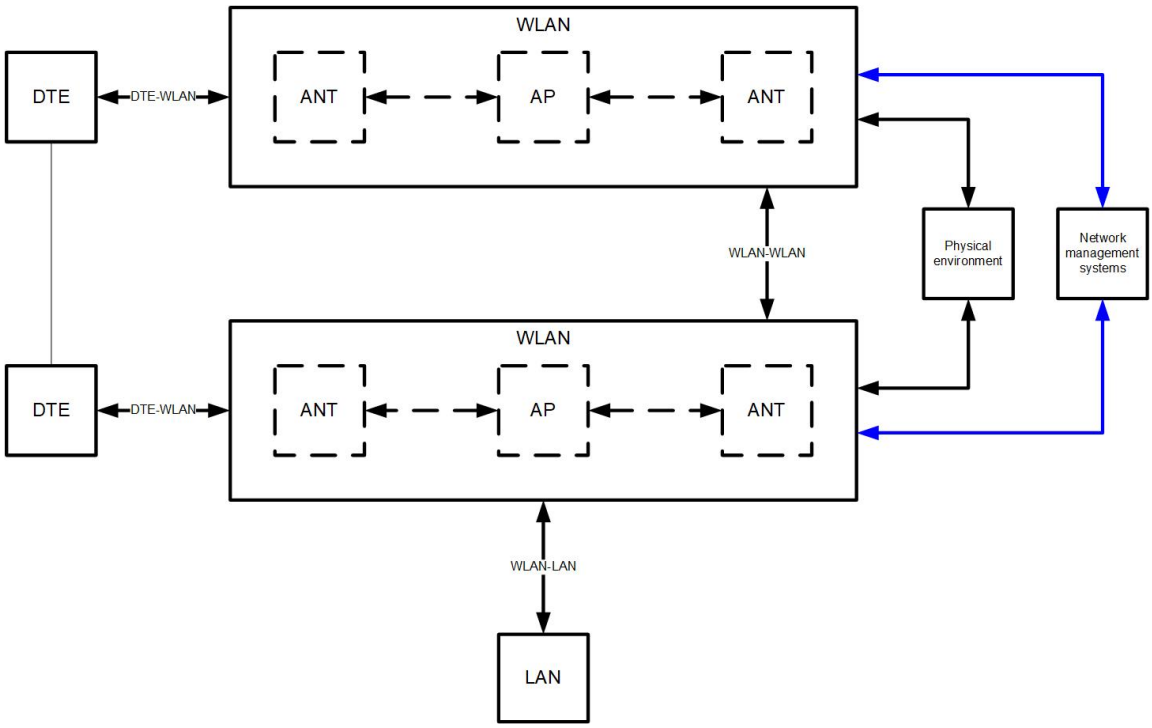

Figure 6 – Interfaces to network management systems (informational)

WLAN systems shall comply with TS 06221.

6 Non-functional requirements

Non-functional requirements specified in this document include minimum standards for a range of quality attributes for WLAN systems. These requirements provide a baseline for the assessment of the system's performance. WLAN system designers may wish to implement higher standards than those provided in this document as appropriate to specific business needs.

6.1 Availability

The requirements for availability in this section refer to both the operational and steady state availability of all factors that contribute to the system down time within the operational conditions that include both the physical environment and network management systems.

Operational availability qualifies a value determined under given operational conditions. Steady state availability qualifies a value determined for conditions of an item when characteristic parameters of the item remain constant. Refer to IEC 60050-192 for information on availability.

The minimum availability requirement for the WLAN system excluding the DTE to WLAN and WLAN to WLAN radiocommunications interfaces shall be 99.99%. The demonstrated availability value shall be rounded down to two decimal places.

Where the radio frequency interference and channel utilisation are stable and quantifiable throughout system life, the minimum availability of the DTE to WLAN and WLAN to WLAN

radiocommunications interfaces shall be 95%. The demonstrated availability value shall be rounded down to zero decimal places.

Where the radio frequency interference and channel utilisation are neither stable nor quantifiable throughout system life, such as in public access applications, it is not possible to specify a minimum availability of the DTE to WLAN and WLAN to WLAN radiocommunications interfaces.

Availability shall be demonstrated by the reliability block diagram (RBD) method as part of a reliability, availability, and maintainability (RAM) program.

6.2 Interoperability

Systems shall comply with open standards for interoperability, unless otherwise stated in this document.

Interoperability with nominated type approved or existing operators' systems shall be verified by testing the systems in accordance with TS 06222 as part of the verification plan. This is in addition to other verification methods such as certification that may form part of the verification plan.

Where modular transceiver packages are used, WLAN shall interoperate with any compliant modular transceiver package from any third party.

If a third-party modular transceiver package is used, then the following applies:

- the WLAN equipment shall not disable or degrade its performance
- the WLAN supplier shall not alter the support or warranty conditions for the WLAN.

6.3 Maintainability

Preventative maintenance programs shall be identified and developed for all components that are modelled by an increasing failure rate such as fans, filters, transceivers, and connectors.

Maintenance programs shall be implemented to detect imminent or conditional failures such as CPU and memory exhaustion, interface overload and errors, high temperature, power supply current and voltage abnormalities, and radio frequency coverage.

Maintenance programs shall be implemented for all assets to ensure that the hardware, firmware, software, and physical and logical configuration are as designed throughout system life.

Where installed in a redundant configuration, insertion or removal of cards and modules shall not affect the system operation; that is, the system is hot swappable. Hot swapping shall be performed without issuing any system commands.

Message logs severity levels shall be as specified in RFC 5424.

All message logs with a severity level between 0 and 4 inclusive shall be logged to syslog.

All message logs with a severity level between 0 and 2 inclusive shall be regarded as failures requiring immediate corrective action.

All message logs with a severity level of 3 or 4 shall be regarded as conditional failures requiring corrective maintenance action within a defined period as specified in the technical maintenance plan.

6.4 Manageability

WLAN shall support the following logical configuration management capabilities:

- support separate running and startup configuration datastores
- retrieve all of a configuration datastore
- load all of a configuration to a target configuration datastore
- create or replace a configuration datastore with the contents of another configuration datastore
- delete a configuration datastore
- retrieve running configuration.

Refer to RFC 6241 for information on configuration datastores.

When queried, the WLAN access point shall return configured values for the following logical configuration attributes:

- hostname (sysName)
- location (sysLocation)
- contact (sysContact).

When queried, the WLAN access point shall return values from published product documentation for the following physical configuration attributes:

- hardware revision
- firmware revision
- software revision
- serial number of chassis and FRUs
- manufacturer name of chassis and FRUs
- model name of chassis and FRUs.

6.5 Performance

Performance requirements with confidence levels and confidence intervals of the system shall be specified to include at least throughput, latency, frame loss rate, and received signal strength (RSS) within a defined coverage area.

Refer to RFC 1242 for the definition and parameters for throughput, latency and frame loss benchmarks.

The confidence level shall be 95% or greater.

The confidence interval (margin of error) shall be 0.1 or less.

The performance shall be analysed using a radio frequency simulation tool.

The performance shall be verified by testing the system in accordance with TS 06222. The population, for sampling purposes, shall consist of discrete points at every linear or square metre within the defined coverage area. A minimum of 100 random samples from the population shall be used to verify the design.

> Note: With a confidence level of 95% and confidence interval of 0.1, the sample size approaches 97. This is rounded up to 100.

Where a confidence level is greater than 95% or where the confidence interval of less than 0.1 is used, the increased sample size shall be statistically calculated.

Where the radio frequency interference and channel utilisation are neither stable nor quantifiable throughout system life, such as in public access applications, the test results shall state that they are only valid at the time the test was performed and coverage is not guaranteed in future since radio frequency interference and channel utilisation are neither stable nor quantifiable.

A traffic policy shall be implemented to ensure network quality of service guarantees is achieved. The traffic policy shall assign priority levels and information rates to all traffic flows.

6.6 Reliability

Failure models inclusive of the failure distribution and the required parameters for all FRUs that comprise WLAN shall be specified. For example, a common failure model is the CFR with exponential distribution and MTTF.

The MTTF of all CFR FRUs shall exceed 150,000 hours.

Failure model parameters shall comply with the yearly average temperature for reliability, availability, maintainability, and safety calculations as specified in EN 50125-3.

> Note: EN 50125-3 applies as specified in this document, regardless of whether the equipment applies to railways or another transport mode.

Acceptable methods for predicting the failure model for electronic equipment, as stated in any of the following standards, shall be followed:

- PD IEC TR 62380
- Telcordia SR-332 Issue 4
- MIL-HDBK-217F Notice 2.

Where multiple MTTF estimates are available, the lowest estimate shall be used.

Failure models shall be justified by stating the data source, methodology, environment, assumptions, and parameters.

6.7 Safety

WLAN shall comply with the safety of information technology requirements as specified in AS/NZS 62368.1.

If modular transceiver packages are used, WLAN shall comply with the safety of laser products requirements as specified in AS/NZS IEC 60825.1 and AS/NZS IEC 60825.2.

6.8 Security

6.8.1 General

Defences against digital information and cyber security vulnerabilities such as interruption, interception, modification, intrusion, and deception for WLAN systems, subsystems and their interfaces shall be implemented in accordance with TS 04990, TS 04991 and TS 04993; and in the case the asset has been identified as a crown jewel under the *NSW Cyber Security Policy*, then also in accordance with TS 00031.1.

These defences shall mitigate internal or external and intentional or unintentional security vulnerabilities.

6.8.2 Management plane security

Full compliance to the management-plane security defences provided in Table 1 may not be necessary for WLAN that is dedicated to a single application and where it is demonstrated that it is not feasible to implement a network management system as specified in TS 06221. Table 1 provides the management-plane security defences, and identifies those defences that are mandatory and optional for WLAN for single application without a network management system.

All other WLAN shall comply fully with each of the management-plane security defences that are listed in Table 1.

Table 1 – Management-plane security defences

Management-plane security defence	Compliance requirement for WLAN for single application without network management system
in-band management ports shall be on dedicated management VLAN (not VLAN 1)	optional
prune management VLAN from 802.1Q trunks where not required	optional
enable password security (hashing) for local passwords	mandatory
disable local password recovery using the console, that is, the WLAN system shall be factory reset to reset local password	mandatory
disable all unused services, such as discard, daytime, chargen and protocols, such as SNMPv1 (in accordance with RFC 1157), SNMPv2 (in accordance with RFC 3416 and RFC 3417)	mandatory
enable an idle timeout of 5 minutes on console and remote terminal sessions	mandatory
enable the generation of a trap or message notification when memory utilisation exceeds 80%	mandatory (to local message log)
enable the generation of a trap or message notification when CPU utilisation exceeds 80%	mandatory (to local message log)
enable authentication in protocols where the support exists; for example, NTPv3, SNMPv3 (in accordance with RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417 and RFC 3418)	optional
enable encryption in protocols where the support exists; for example, SNMPv3 (in accordance with RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417 and RFC 3418)	optional
implement access control allow list to permit access to the WLAN system management-plane services, such as SSHv2, HTTPS, from authorised network management clients	mandatory
implement access control allow list to permit access to the WLAN system management-plane services, such as SNMPv3 (in accordance with RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417 and RFC 3418), syslog, DNS, NTPv3, SNTP, TACACS+, RADIUS (in accordance with RFC 2865) from authorised network management servers	optional

Management-plane security defence	Compliance requirement for WLAN for single application without network management system
implement access control allow list to permit access to the WLAN system using internet control message protocol (ICMP) types 0, 8, and 11 from authorised network management servers and clients in accordance with RFC 792, RFC 1122 and RFC 4443. All other access to the WLAN system using ICMP types 0, 8, and 11 is denied	optional
restrict access to management services to configured interfaces	mandatory
disable insecure management protocols, such as trivial file transfer protocol (TFTP), telnet, SNMPv1 (in accordance with RFC 1157), SNMPv2 (in accordance with RFC 3416 and RFC 3417), FTP, HTTP	mandatory
enable a retry limit for protocols that support authentication	mandatory
disable any auxiliary or unused management ports	mandatory
enable a warning on login to the management-plane as shown in Figure 7 to notify unauthorised users that they are not permitted to use the system	mandatory
manufacturer default passwords for all preconfigured accounts (admin, root, user, support, config) shall not be used	mandatory
manufacturer default service set identifier (SSID) shall not be used	mandatory
manufacturer default keys or passphrases shall not be used	mandatory
configure the primary method of authentication, authorisation and accounting to TACACS+ or RADIUS (in accordance with RFC 2865 and RFC 2866)	optional
configure the secondary method of authentication, in the event of the failure of the primary method, to local passwords	mandatory (as primary method)
configure logging of messages with a severity level between 0 and 4 inclusive, as specified in RFC 5424 to syslog servers	mandatory (to local message log)
disable logging of messages to local console and remote terminal	mandatory
enable logging of configuration change, authentication and authorisation events	mandatory (to local message log)

Figure 7 shows the warning to be used on login to the management plane.

```
***** This service is for authorised clients only *****
************************************************************
* WARNING: It is a criminal offence to:                    *
* i. Obtain access to data without authority               *
* ii Damage, delete, alter or insert data without authority  *
************************************************************
```

Figure 7 – Example of warning on login to management plane

6.8.3 Control plane security

As a minimum, the following control-plane security defences shall be implemented on WLAN:

- implement access control allow list to permit access to the control-plane. All other access to the control-plane shall be denied
- enable authentication in protocols where the support exists.

6.8.4 Data plane security

As a minimum, the following data plane security defences shall be implemented on WLAN:

- VLAN 1 from 802.1Q trunks shall be pruned where not required.
- IEEE 802.1X port-based network access control shall be enabled for all access to the network (both wired and wireless interfaces).
- Traffic flow statistics shall be enabled.
- Access control allow list shall be implemented to permit access to data plane, specified by internet layer, such as IP, ICMP or transport layer, such as TCP, UDP rules.

All other access to data plane shall be denied.

6.9 Supportability

In addition to the supportability requirements of this section, equipment comprising WLAN used on railway applications may require type approval. Refer to TS 06178 for further information.

The supportability life cycle parameters for WLAN components are provided in Table 2.

Table 2 – Parameters for the supportability life cycle model for WLAN

WLAN subsystem equipment	I (years)	S (years)	U (years)
Access point subsystem	3	2	3
Antenna subsystem	3	2	3

The parameters used in Table 2 (as shown in Figure 8 and Figure 9) are as follows:

- ‘I’ is able to install and use product
- ‘S’ is propose to use product
- ‘U’ is able to use existing product.

The support requirements to be met by suppliers for the supply of WLAN components are as follows:

- An advance notice shall be issued by the OEM more than 6 months (180 days) prior to the EOS. The EOS is the date when the OEM withdraws a product from sale, both directly and through its authorised points of sale.
- Equipment comprising the WLAN shall only be proposed for use or submitted for type approval (if applicable) if the following supportability requirements are met:
    - the OEM guarantees that EOS is at least 'I' years from the date of proposed commissioning
    - the equipment has been FOFS for less than 'S' years from the date of proposed commissioning. The FOFS date is the date when the OEM first offers a product for sale in the Australian market.
- While the product is available for sale, full software and hardware repair and replacement services shall be available.
- Software support services for operating system software shall be commercially available for at least 'U' years following EOS.
- Hardware repair and replacement services shall be commercially available for at least 'U' years following EOS.

The use of existing installed products may continue whilst software support and hardware repair and replacement services are available after EOS.

Discontinued use of existing installed products when software support or hardware repair and replacement services are unavailable after EOS. Where discontinuation is not reasonably practicable, associated risks including increasing hardware failures, software functionality defects and security vulnerabilities shall be managed in accordance with TS 04982.

Figure 8 is a diagrammatic representation of the supportability life cycle based on time until EOS and Figure 9 is a representation of the supportability life cycle based on time from FOFS.

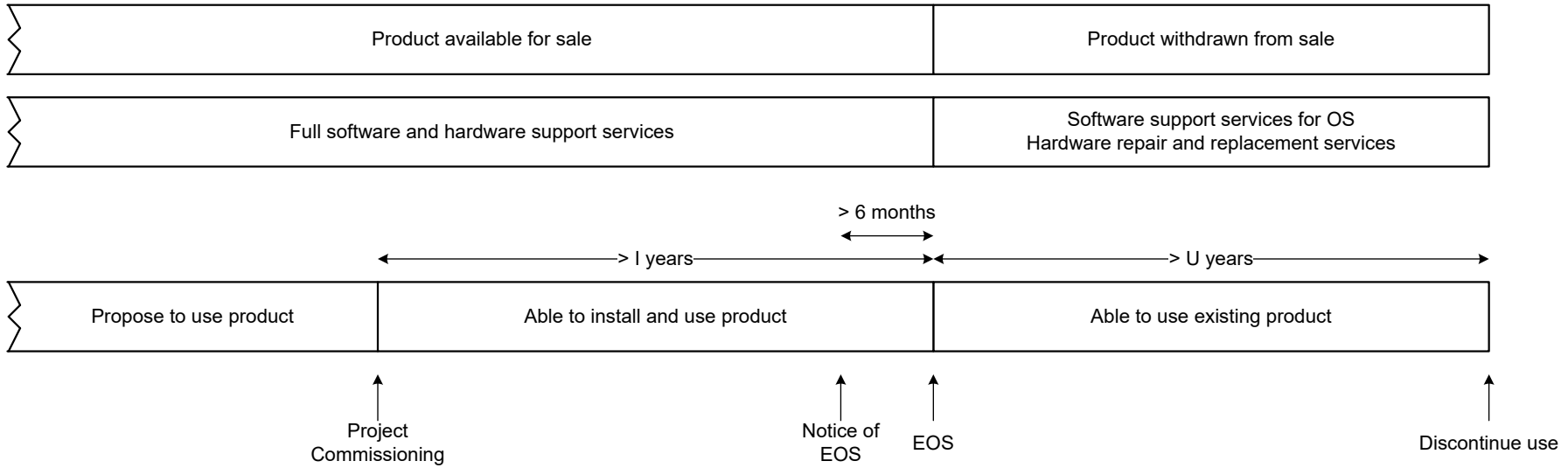

Figure 8 – Supportability life cycle based on time until EOS

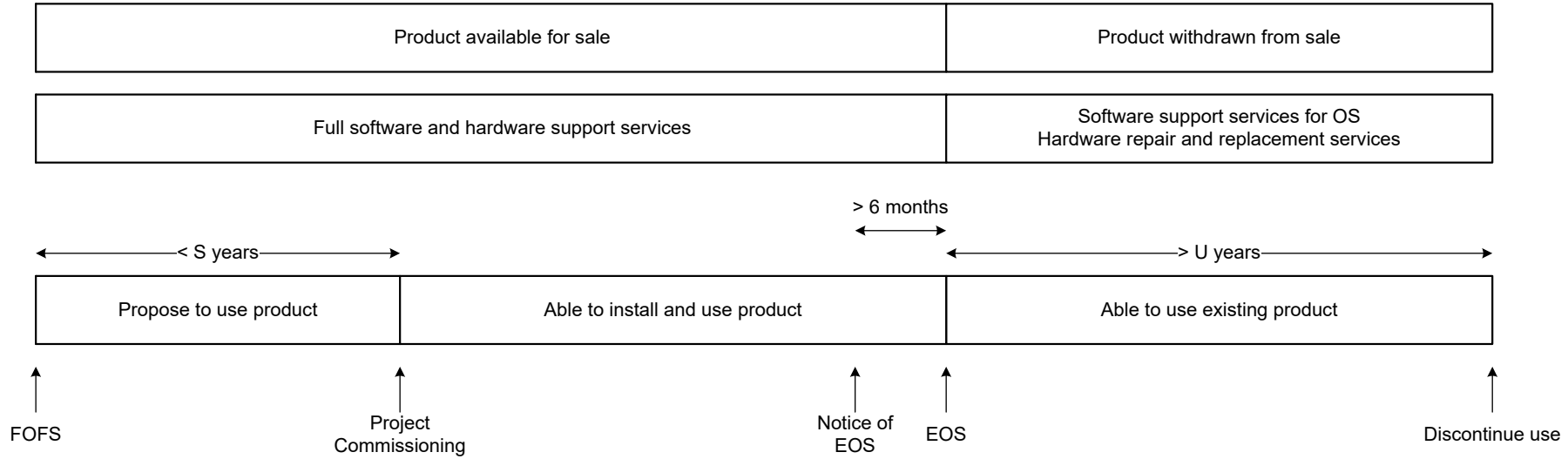

Figure 9 – Supportability life cycle based on time from FOFS

6.10 Sustainability

Materials and substances used at any stage of the asset life cycle throughout the entire supply chain shall comply with the prohibited and restricted materials as specified in *Industrial Chemicals (General) Rules 2019.*

Additional requirements for prohibited and restricted materials for conveyances are specified in TS 04003.

WLAN shall comply with *Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.*