

Video Surveillance System Architecture

Issue date: 19 December 2023

Effective date: 19 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	19/12/2023	First issue.

Preface

This standard specifies the minimum performance and interface requirements for the video surveillance systems that are used in the TfNSW transport network.

This standard has been developed by the AMB in consultation with various TfNSW divisions and industry representatives.

This standard is a first issue.

Table of contents

1	Scope	6
2	Application	6
3	Reference documents	6
4	Terms, definitions and abbreviations.....	9
5	General requirements	10
5.1	Video surveillance system	11
5.2	Video management and control.....	12
5.3	Camera	12
5.4	Recording.....	12
5.5	Interface to external systems.....	13
5.6	Viewer	13
5.7	Transmission	13
5.8	Alarms, events, and video analytics	14
6	Functional requirements for audio and video interfaces	14
6.1	Control and delivery of video	14
6.2	Video communication	15
6.3	Audio communication	15
7	Functional requirements for physical interfaces	16
7.1	Common requirements	16
7.2	Interface to physical environment.....	16
8	Functional requirements for network interfaces.....	16
8.1	Interface to data communication network.....	16
8.2	Interface to network management	17
8.3	Time synchronisation	17
9	Non-functional requirements	17
9.1	Availability	17
9.2	Interoperability	18
9.3	Scalability.....	18
9.4	Maintainability	18
9.5	Manageability.....	18
9.6	Performance	19
9.7	Reliability.....	19
9.8	Safety.....	20
9.9	Security	20
9.10	Supportability	21
9.11	Sustainability.....	22

1 Scope

This document specifies the minimum requirements applicable to video surveillance systems (VSSs) used across the TfNSW operational technology network to ensure interoperability and consistency in the design.

This standard specifies the minimum technical and interface requirements for VSSs installed for safety, security and operational monitoring purposes.

This standard does not contain the camera coverage requirements for the VSSs. Those requirements can be found in TS 04989. Additional fleet specific requirements can be found in TS 03994 and TS 04089. For motorways and tunnels, refer to TS 06319, TS 06320 and TS 06225.03.

2 Application

This document applies to VSSs that are used for customer safety and security, infrastructure safety and security, and operational needs in conveyances, infrastructure, and premises on the TfNSW transport network.

This standard applies to new systems and configuration changes to existing systems.

For configuration changes only relevant requirements apply.

Conveyances include any rolling stock, vehicle, or vessel that is classified as public transport.

Infrastructure and premises include any stations, interchanges, wharves, bus stops, state owned roads, motorways, tunnels, bridges and other ancillary facilities.

This standard should be read in conjunction with TS 04989.

3 Reference 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 50125-1 *Railway applications – Environmental conditions for equipment – Part 1: Rolling stock and on-board equipment*

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

IEC 60050-191 *International Electrotechnical Vocabulary – Part 191: Dependability and quality of service*

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

ISO/IEC 14496-2 *Information technology – Coding of audio-visual objects – Part 2: Visual*

ISO/IEC 14496-3 *Information technology – Coding of audio-visual objects – Part 3: Audio*

ISO/IEC 14496-10 *Information technology – Coding of audio-visual objects – Part 10: Advanced Video Coding*

ISO/IEC 23008-2 *Information technology — High efficiency coding and media delivery in heterogeneous environments – Part 2: High efficiency video coding*

ITU-T Recommendation G.711 *Pulse code modulation (PCM) of voice frequencies*

ITU-T Recommendation G.726 40, 32, 24, 16 kbit/s *Adaptive differential pulse code modulation (ADPCM)*

RFC 3261 *Session Initiation Protocol (SIP)*

RFC 3550 *Real-time Transport Protocol (RTP)*

RFC 6241 *Network Configuration Protocol (NETCONF)*

RFC 7826 *Real-Time Streaming Protocol (RTSP)*

Australian standards

AS/CA S008 *Requirements for Customer Cabling Products*

AS/CA S009 *Installation Requirements for Customer Cabling (Wiring Rules)*

AS 60529 *Degrees of protection provided by enclosures (IP Code)*

AS 62262 *Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)*

AS/NZS ISO/IEC 27001 *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*

AS/NZS ISO/IEC 27002 *Information security, cybersecurity and privacy protection – Information security controls*

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

AS/NZS 62676.1.2 *Video surveillance systems for use in security applications – Part 1.2: System requirements – Performance requirements for video transmission*

Transport for NSW standards

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

TS 03947 (T MU MD 21001 ST) *Equipment Rooms and Cubicles for Programmable Electronic Systems*

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

TS 03954 (T HR SS 80002 ST) *Low Voltage Electrical Installations*

TS 03985 (T HR RS 01701 ST) *Mounting and Installation of Electrical Equipment*

TS 03994 (T HR RS 13002 ST) *Surveillance Systems for Heavy Rail Vehicles*

TS 04089 (T LR RS 13002 ST) *Surveillance Systems for Light Rail Vehicles*

TS 04942 (T MU SS 90002 ST) *Shelter at Railway Stations and Interchanges*

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

TS 04989 (T MU SY 10001 ST) *Public Transport Closed Circuit Television Functional Requirements Standard*

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 06208 (T MU TE 61007 ST) *Time Synchronisation of Industrial Automation and Control Systems*

TS 06210 (T MU TE 01001 ST) *Campus Backbone Telecommunication Routes and Cabling*

TS 06212 (T MU TE 01005 ST) *Optical Fibre Cable*

TS 06218 (T MU TE 41001 ST) *Packet Switched Networks – Wired Networks*

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

TS 06220 (T MU TE 41004 ST) *Packet Switched Networks – Wireless Local Area Networks*

TS 06221 (T MU TE 81002 ST) *Telecommunication Equipment – Network Management*

TS 06225.03 (IC-DC-TS912) *Motorway Systems – Traffic Management and Control System*

TS 06225.05 (IC-DC-TS914) *Motorway systems – electrical power supply and distribution system*

TS 06305 (T MU SY 10014 GU) *Application Guide to NSW Cyber Security Policy for Operational Technology*

TS 06319 (RMS 17.167) *Smart motorway design guide – Traffic monitoring and surveillance*

TS 06320 (RMS 17.168) *Smart motorway design guide – Tunnel traffic management*

Legislation

Industrial Chemicals (General) Rules 2019 (Cth)

Privacy and Personal Information Protection Act 1998 (NSW)

Surveillance Devices Act 2007 (NSW)

Other referenced documents

MIL-HDBK-217F Notice 2 *Reliability Prediction of Electronic Equipment*

Open Network Video Interface Forum, *ONVIF Profile S, T and G*

State of New South Wales *NSW Cyber Security Policy*

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

4 Terms, definitions and abbreviations

The following terms, definitions and abbreviations apply in this document. For dated references, only the cited edition applies. For undated references, the latest edition of the referenced document applies.

AAC advanced audio coding

AMB Asset Management Branch

API application programming interface

DVMS digital video management system

EOS end of sale

FOFS first offered for sale

HD high definition

IK code coding system to indicate the degree of protection provided by an enclosure against harmful external mechanical impacts

IP internet protocol

IP code ingress protection code; a coding system to indicate the degrees of protection provided by an enclosure against access to hazardous parts, ingress of solid foreign objects, ingress of water and to give additional information in connection with such protection

LIPD low interference potential device

MPEG4 Moving Picture Expert Group Phase 4

NTP network time protocol

Onvif Open Network Video Interface Forum

PTZ pan tilt zoom

SDK software development kit

TCP transmission control protocol

TfNSW Transport for NSW

TfNSW transport network the transport system (transport services and transport infrastructure) owned and operated by TfNSW, its operating agencies or private entities upon which TfNSW has power to exercise its functions as conferred by the *Transport Administration Act 1988* or any other Act.

TMC Transport Management Centre

UDP user datagram protocol

VSS video surveillance system

5 General requirements

A video surveillance system (VSS) usually consists of devices for image capturing, control, management, storage, retrieval, and associated transmission interconnections. This standard defines the technical and interface requirements for the VSS as a whole. Figure 1 shows the VSS system components, solid lines represent the components which are in scope and dashed lines represent the external systems which are not in the scope of this standard. The diagram is informational and is not intended to convey the solution architecture.

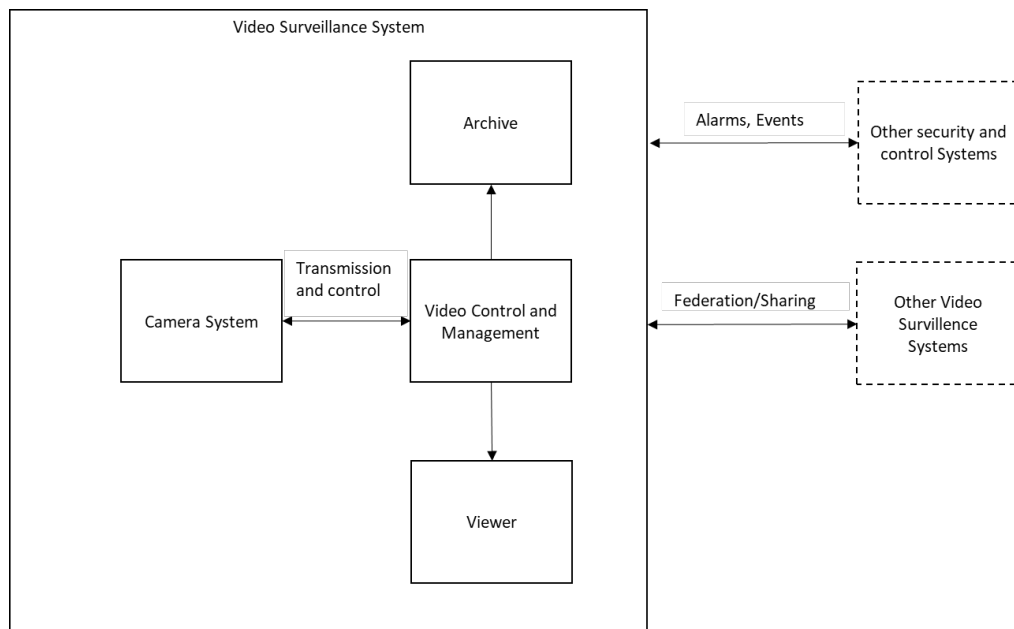


Figure 1 – Video surveillance system components

5.1 Video surveillance system

The VSS shall be a fully IP based system.

The VSS shall be ONVIF compliant as defined in profile G, S, and T specifications.

The VSS shall comply with the following ONVIF features:

- NTP
- MPEG4
- H.264
- H.265
- G726
- G711
- AAC
- PTZ.

VSS core components shall be designed to eliminate the risk of system failure due to single points of failure.

Note: Core components include components for video control, management and associated archive.

VSS core components except archive shall be located centrally for management and control. Video archive shall be centrally located for redundancy and management unless there are valid operational reasons to distribute them.

VSS core components shall automatically switch over to a redundant site during a failure.

The VSS shall be able to share video streams with other TfNSW VSSs to achieve operational objectives. Licencing provisions should be considered to reduce costs of sharing video streams.

Note: At present all TfNSW VSSs require integration with TMC DVMS such that it is able to share its video streams and recordings with the TMC DVMS. By supporting seamless integration at the video management layer, video streams, events, alarms, and related metadata will be able to be transferred across various TfNSW operators without significant extra cost.

The VSS shall support federation with other standalone VSSs and leverage features such as camera events, alarms, and metadata.

The VSS shall be designed and managed to prevent unauthorised access, see section 9.9.

VSS shall log all user activities for auditing purposes.

VSS shall be capable of detecting video tampering and validating authenticity by a video authentication mechanism such as watermarking.

5.2 Video management and control

The VSS shall support PTZ camera protocols from multiple manufacturers.

The VSS shall be capable of programming preset positions, guard tours, and auto tracking on PTZ cameras.

The VSS shall provide priority-based control for PTZ cameras according to the user configuration.

The VSS shall allow text to be overlayed on the video data image. The inserted text shall be configurable to meet operational requirements.

The VSS shall support privacy masking.

5.3 Camera

Cameras shall have a minimum resolution of HD 1080p for high level of detail.

Cameras shall support wide dynamic range to overcome high contrast lighting conditions.

Cameras may incorporate built-in edge storage when needed for operational purposes, such as addressing constraints related to bandwidth.

When edge storage is required, storage shall be appropriately designed to cater for operational needs.

When video data is stored in edge storage it shall be protected in accordance with the TfNSW cybersecurity requirements.

Each camera's bit rate, frame rate, and resolution shall be able to be set independently from other cameras in the system and altering these settings shall not affect the recording and display settings of other cameras.

Cameras shall record minimum metadata relevant to the camera ID, date and time. Time shall be NSW government time as per TS 06208.

5.4 Recording

The VSS shall support continuous, at alarm, and at motion recording.

For public transport applications, video image data shall be recorded in accordance with the requirements of TS 04989.

For motorways and tunnels, video image data shall be recorded for minimum of 31 days in accordance with the requirements of TS 06225.03.

The VSS shall allow an operator to mark a recording as permanent so that it cannot be overwritten.

Retrieval of the image recordings shall be possible without physically accessing the storage devices.

When video data is stored in cloud storage it shall be an existing private TfNSW approved cloud.

5.5 Interface to external systems

The VSS shall support integration with external control and security systems for receiving alarms and events.

The VSS shall provide a fully documented API/SDK to allow for monitoring and control of cameras by the external control system.

5.6 Viewer

Remote viewing of live video data images shall be possible for authorised people.

The VSS shall support display of video images to a video wall display and operator workstation displays.

The VSS shall be able to use multiple camera keyboards to operate the entire set of cameras throughout the system, including cameras from various manufacturers and their PTZ functionalities.

The VSS shall support activating certain camera displays on operator screens based on certain alarms and events.

5.7 Transmission

IP based transmission shall be used for the transmission of the video image data from the cameras to the VSS core.

5.7.1 Wireless interconnections

Mobile carriage services and satellite backhaul may be permitted when wired or dedicated wireless interconnections are impractical. Suitability of the mobile carriage service or satellite backhaul shall be determined based on the bandwidth requirements of individual cameras. Cameras which are connected to the VSS via mobile carriage services or satellite backhaul shall have communication secured in accordance with TfNSW cyber security requirements.

Wireless transmission systems based on LIPD class licenced bands as detailed in TS 06219 should not be used.

5.7.2 Cabling

Twisted pair cable or optical fibre cable shall be used.

Coaxial cabling shall not be used in new or substantially upgraded VSSs.

Cabling shall comply with AS/CA S008 requirements for customer cabling products, and AS/CA S009 installation requirements for customer cabling (wiring rules).

Campus backbone cabling shall comply with TS 06210 and TS 06212.

5.8 Alarms, events, and video analytics

The VSS shall support defining events for triggering alarms.

Where it is needed for operational reasons, the VSS shall support video analytics such as motion detection, object detection, intrusion detection, face recognition, and number plate recognition. For motorway/tunnels, video analytics shall comply with TS 06225.03.

When video analytics is supported, it shall be possible to integrate multiple video analytics products without any modifications to the existing VSS hardware.

Video analytics shall not impact the VSS performance.

Alarms and event logs shall be stored with the relevant metadata for forensic analysis and auditing. They shall be stored for an appropriate number of days as determined by the operational risk assessment. The number of days shall not be less than 90.

6 Functional requirements for audio and video interfaces

In the VSS, devices shall use standardised industry protocol for the collection, storage, distribution, and display of video image data. Devices with proprietary and non-standardised protocols might not be interoperable with each other.

6.1 Control and delivery of video

Communications protocols are necessary to control and deliver video communication over IP networks.

Protocols are specified for interoperability of control and delivery of video communication.

The following protocols shall be supported and used:

- RFC 3261
- RFC 3550
- RFC 7826.

6.2 Video communication

Video codecs encode and decode a digital data stream of video in a specific format.

Video codecs are specified for interoperability of video communication and surveillance.

One or more of the following video codecs shall be supported for video communication and surveillance:

- MPEG4 that complies with ISO/IEC 14496-2
- H.264 that complies with ISO/IEC 14496-10
- H.265 that complies with ISO/IEC 23008-2.

Other video codecs may be used, provided sharing of video with other TfNSW VSS platforms is not required as this is likely to introduce transcoding overhead, loss of metadata, and licensing costs.

The VSS shall be capable of video transmission via Unicast TCP/UDP and Multicast UDP from the camera.

For network topologies that restrict the VSS from sending multicast UDP streams, the server shall act as a gateway and redirect audio/video streams to active viewing clients on the network using multicast UDP.

The VSS shall support frame rates and resolutions in accordance with TS 04989 for public transport applications.

The VSS shall support frame rates and resolutions in accordance with TS 06225.03 for motorway and tunnel applications.

For applications not specified in TS 04989 or TS 06225.03, the VSS shall support a resolution of at least 1080p.

For applications not specified in TS 04989 or TS 06225.03, the VSS shall support a frame rate of at least 12 frames per second.

6.3 Audio communication

Audio codecs encode and decode a digital data stream of audio in a specific format.

Audio codecs are specified for interoperability of voice communication.

One or more of the following audio codecs shall be supported by the VSS:

- G.711 that complies with ITU-T Recommendation G.711
- G.726 that complies with ITU-T Recommendation G.726
- AAC that complies with ISO/IEC 14496-3.

Other audio codecs may be used provided that audio can be encoded and decoded with non-proprietary licence free codecs.

Audio recording shall not be enabled in cameras without valid operational requirements.

Note: Audio recording is needed to comply with various state and federal law requirements including *Surveillance Devices Act 2007*.

7 Functional requirements for physical interfaces

The functional requirements specified in Section 7.1 and Section 7.2 relate to system–system interfaces.

7.1 Common requirements

Equipment comprising the system shall comply with TS 03948.

In addition, within conveyances the VSS shall comply with TS 03994 and TS 04089.

7.2 Interface to physical environment

VSS components shall be suitable for use in the environmental conditions they are expected to operate.

In infrastructure and premises, camera housings shall comply with one of the following minimum 'IP code' ratings as defined in AS 60529:

- IP54 for indoor and sheltered areas
- IP66 for outdoor areas.

In conveyances, camera housings shall comply with TS 03994 and TS 04089.

Cameras shall comply with a minimum IK code rating of IK08 as defined in AS 62262.

8 Functional requirements for network interfaces

8.1 Interface to data communication network

The VSS shall operate over a data communication network.

Equipment that comprises the system shall interface to the wired or wireless data communication network as data terminal equipment in accordance with the following standards:

- TS 06218
- TS 06220.

The data communication network shall be designed to meet the network capacity required for the anticipated VSS operation.

8.2 Interface to network management

The VSS shall comply with the requirements of TS 06221.

8.3 Time synchronisation

Programmable electronic equipment comprising the system shall comply with TS 06208.

9 Non-functional requirements

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

9.1 Availability

The system is only considered available when the following functions are available:

- real time monitoring
- recording.

For the purpose of determining the availability requirements, the VSS shall be divided into two sub-systems as below:

- Core components within the VSS that are necessary for the functionality of the VSS where availability is expressed as A_c .
- All other individual components where availability is expressed as A_a .

Note: Core components include video management system and associated archive.

Core components used in safety critical functions such as fire life safety shall achieve an availability $A_c = 99.97\%$.

Core components used in all other applications shall achieve an availability $A_c = 99.93\%$.

For individual components, availability shall be determined based on a risk assessment carried out according to TS 04982.

For motorways/tunnels, the availability target and associated process is defined in TS 06225.01 and TS 06225.02.

Refer to TS 03947 and TS 03954 for backup power supply requirements. For motorways and tunnels, backup power supply requirements are specified in TS 06225.05.

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

9.2 Interoperability

The VSS shall be based on a true open architecture that allows for the use of non-proprietary workstation and server hardware, non-proprietary network infrastructure, and non-proprietary storage.

9.3 Scalability

The VSS shall offer a complete and scalable video surveillance solution that allows cameras to be added on a unit-by-unit basis.

9.4 Maintainability

The design and location of the cameras shall take into account the human factors for those maintaining and cleaning the units.

If the VSS is intended to be used in high-risk locations, then the unit shall implement continuous self-tests to detect and notify functional, imminent, and conditional failures of subsystems within the unit necessary for the emergency function.

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

Maintenance programs shall be implemented to detect imminent or conditional failures such as central processing unit (CPU) and memory exhaustion, interface overload and errors, high temperature, power supply current and voltage abnormalities.

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

Where installed in a redundant configuration, cards and modules shall be able to be inserted or removed without affecting the system operation; that is, the system shall be hot swappable. Hot swapping shall be performed without issuing any system commands.

9.5 Manageability

The VSS shall support the following logical configuration surveillance capabilities:

- 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.

The VSS shall support updating its camera drivers independent from the VSS installation. New drivers shall be released at least once a year to extend support for new devices and features.

9.6 Performance

Performance of live video streaming and PTZ control are subject to accumulated delay called latency and delay variance called packet jitter. Delay and delay variance metrics are inclusive of transmission, switch fabric, queuing, propagation, coding, decoding and display delays.

The VSS shall have a maximum 2-way latency of 150 ms for a live view and control in accordance with AS/NZS 62676.1.2.

The VSS shall have a maximum of 20 ms packet jitter between the end devices in accordance with AS/NZS 62676.1.2.

9.7 Reliability

Failure models inclusive of the failure distribution and required parameters for all field replaceable units (FRU) that comprise a system shall be specified. For example, a common failure model is the constant failure rate (CFR) with exponential distribution and mean time to failure (MTTF). The CFR is the period in the life of a non-repaired item during which, the failure rate is approximately constant as defined in IEC 60050-191.

The MTTF of all CFR field replaceable units shall exceed 150,000 hours.

In infrastructure and premises, failure model parameters shall comply with the yearly average temperature for reliability, availability, maintainability, and safety (RAMS) calculations as defined in EN 50125-3.

In conveyances, failure model parameters shall comply with the yearly average temperature for RAMS calculations as defined in EN 50125-1.

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

- IEC 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.

9.8 Safety

The VSS shall comply with the safety of information technology requirements as defined in AS/NZS 62368.1.

9.9 Security

Security requirements include physical security, digital information security, and cybersecurity.

9.9.1 Cybersecurity

TfNSW has produced cybersecurity requirements for operational technology considering the *NSW Cyber Security Policy*.

The standards that any VSS shall comply with include, but are not limited to the following:

- TS 04990
- TS 04993
- TS 04991
- TS 00031.1.

Additional guidance can be found in the following standard:

- TS 06305.

9.9.2 Digital information security

The VSS shall comply to AS/NZS ISO/IEC 27001 and AS/NZS ISO/IEC 27002 for information security.

Personal information stored in the VSS shall comply with applicable legal frameworks and legislations such as *Privacy and Personal Information Protection Act 1998* (NSW).

9.9.3 Physical security

Cameras shall be capable of detection and notification of tampering and removal.

All network and access equipment shall be installed within equipment rooms and cubicles that comply with TS 03947.

Cameras shall be installed with a minimum vertical clearance of 2400 mm from any ground and floor surface to reduce the likelihood of vandalism, unless unavoidable.

Installations on platforms of railway stations shall also comply with the canopy structure envelope and clearance set back from the platform edge as defined in TS 04942.

In conveyances, all equipment shall be installed in compliance with TS 03985.

9.10 Supportability

In addition to the supportability requirements of this section, some VSS components may require type approval. Refer to TS 06178 for further information.

The supportability life cycle parameters for VSS subsystem equipment are provided in Table 1.

Table 1 – Supportability life cycle parameters

Equipment	I (years)	S (years)	U (years)
Cameras	7	7	3
Servers	5	5	3
Modems	3	2	3

The parameters used in Table 1 (as shown in Figure 2 and Figure 3) are as follows:

- 'I' is able to install and use product before EOS
- 'S' is propose to use product after FOFS
- 'U' is able to use existing product after EOS.

An advance notice shall be issued by the original equipment manufacturer (OEM) more than six months (180 days) prior to the end of sale (EOS). The EOS is the date when the original equipment manufacturer withdraws a product from sale, both directly and through its authorised points of sale.

Equipment comprising the VSS shall only be proposed for use or submitted for type approval (if applicable) if the following two supportability requirements, relating to Table 1, are met:

- the OEM guarantees that EOS is at least 'I' years from the date of proposed commissioning
- the equipment has been first offered for sale (FOFS) for less than 'S' years from the date of proposed commissioning.

Note: The FOFS date is the date when the OEM first offers a product for sale in the Australian market.

While 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 while software support and hardware repair and replacement services are available after EOS.

The use of existing installed products or components should be discontinued 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 2 shows the supportability life cycle based on time until EOS and Figure 3 shows the supportability life cycle based on time from FOFS.

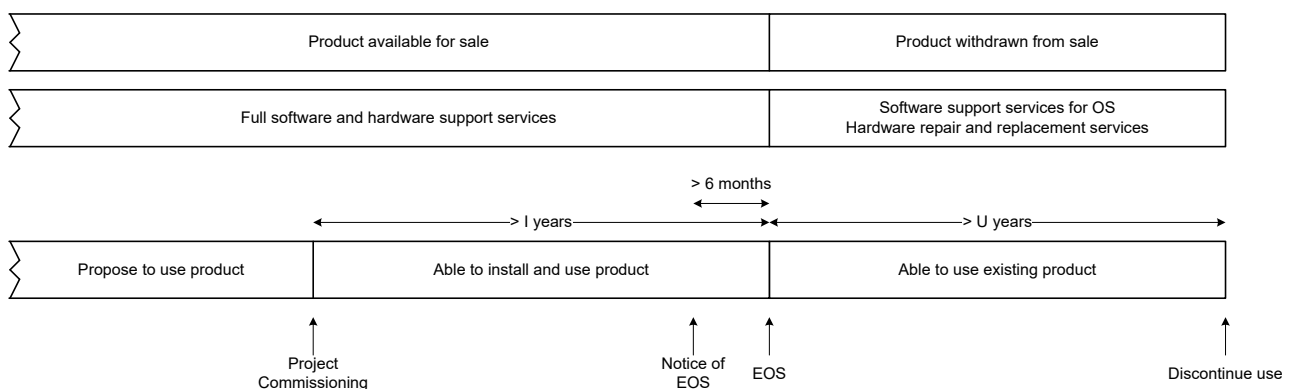


Figure 2 – Supportability life cycle based on time until EOS

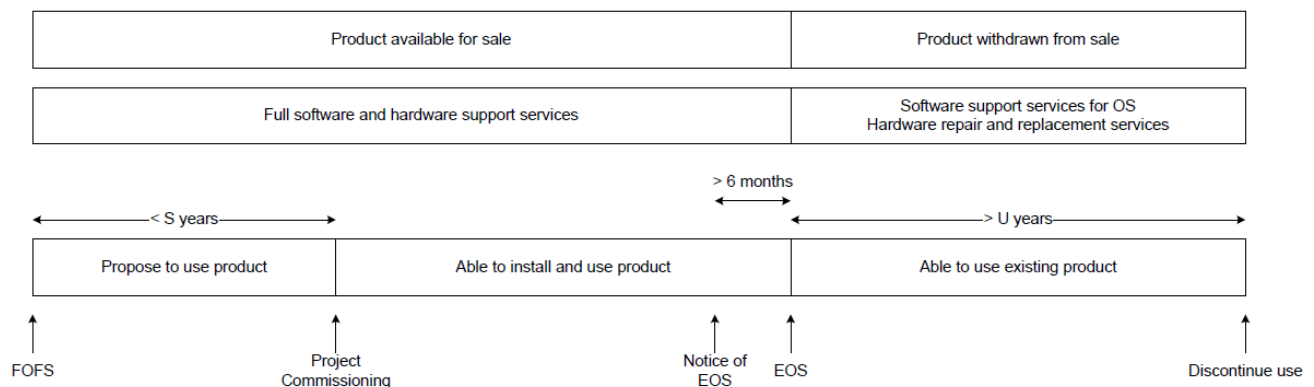


Figure 3 – Supportability life cycle based on time from FOFS

9.11 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*.