

Category 1 Standard

S1147 Surveillance & Security Systems



**Please read the Written Notices
attached to this standard**

Issue No.: A1

Issue date: May 2014

Review date: May 2019

MAYOR OF LONDON

AVA Documents
Document Sharing Hub



Contents

1	Purpose	3
2	Scope	3
3	Requirements	3
3.1	General	3
3.1.1	General	3
3.1.2	Asset Documentation	4
3.1.3	Asset Records	5
3.1.4	Asset Labelling	5
3.1.5	System Compliance	5
3.2	Surveillance and Security – Site Specific Risk Assessment (SSRA) Outline	6
3.3	System Requirements	9
3.3.1	System Development	9
3.3.2	Installation	11
3.3.3	System Integration & Interfaces	12
3.3.4	System Acceptance	13
3.4	Power Supplies	14
3.5	Environment	14
3.6	Processes	15
3.6.1	CCTV Data Downloads	15
3.6.2	Configuration Management & Change Control	15
3.6.3	Analogue to Digital Migration Strategy	16
3.7	Software	17
3.8	Network Security (Electronic)	18
3.9	CCTV	19
3.10	Surveillance & Security (Transmission) Networks	27
3.11	Intruder Detection System (IDS)	29
3.12	Access Control Systems (ACS)	32
3.13	Applications	35
3.13.1	Stations	35
3.13.2	LU Rolling Stock	36
3.13.3	Depots and Sidings	38
3.13.4	Substations	39
3.13.5	Specified Locations (including Escape/Vent Shafts)	40
3.13.6	Special (Surveillance / Alarm) Applications	40
3.14	System Dependability	41
3.15	System Operation & Maintenance	42
3.16	System Decommissioning	42
4	Responsibilities	43
4.1	Head of Telecommunications	43
5	Supporting information	44
5.1	Background	44
5.2	Safety considerations	44
5.3	Environmental considerations	44
5.4	Customer considerations	44
5.5	Attachment 1 – Surveillance & Security Risk Assessment (SSRA)	45
5.5.3	LU Station (Default) Security Grades	52
5.6	Attachment 2 – Surveillance & Security Metadata	56
6	References	63
6.1	References	63
6.2	Abbreviations	67
6.3	Definitions	69
6.4	Person accountable for the document	70
6.5	Document history	70
7	Current Written Notices attached to this standard	70

1 Purpose

The purpose of this standard is to define the minimum operational, system and technical requirements for Surveillance and Security systems deployed across London Underground (LU)

2 Scope

- 2.1 This standard covers Surveillance CCTV, Access control and Intruder detection systems designed and installed for the following applications;
- a. Stations
 - b. Depots and sidings
 - c. LU Rolling Stock
 - d. Substations
 - e. Specified Locations
 - f. Specified infrastructure
 - g. Ventilation and escape shafts
- 2.2 This standard covers the integration and interoperability requirements for these systems when they are configured as networks; to enable local or remote access and control via local area network (LAN) or wide area network (WAN) connectivity.
- 2.3 This standard applies to LU staff, projects and business units including their contractors involved in the design, delivery and maintenance of surveillance and security systems.
- 2.4 This standard covers remote viewing of CCTV services provided to (but not limited to) Service control centres, British Transport Police, Group station control, and Command and Control centres.
- 2.5 OPO (One Person Operation) CCTV used for station Platform to Train Interface (PTI) surveillance and train despatch are not covered this is covered in 1-150.
- 2.6 This standard supersedes SCS-ST- 0015, SCS-ST-0011, SCS-ST-0012, 1-334 and G-334

3 Requirements

3.1 General

Note 1 This standard focuses on CCTV, IDS (Intruder detection systems) and ACS (Access control systems) and how these deliver surveillance and security functions via integrated digital networks (where needed) across the LU network as defined in this standard's scope.

3.1.1 General

- 3.1.1.1 The design and operation of Surveillance and Security sub-systems e.g. CCTV must be compatible with relevant statutory requirements and published guidance particularly in relation to the Data Protection Act 1998 and Human Rights Act 1998.
- 3.1.1.2 For CCTV, clearly visible notices must be installed to inform staff, customers and contractors that they are being monitored and recorded for their safety and security.
- 3.1.1.3 LU contractors engaged in duties requiring security clearance shall conform to requirements set out by LU Network security including compliance with 5-461.

- 3.1.1.4 Surveillance and security systems procurement and design strategies shall use the minimum number of assets consistent with minimising system whole-life costs by;
- a. use of COTS and avoiding bespoke/ captive products
 - b. adopting low energy / low component count designs
 - c. using generic / re-useable specifications
 - d. reducing design variants across surveillance and security sub-systems
 - e. ensuring obsolescence risks during asset lifecycle are minimal
 - f. using a risk-based approach in setting operational and system requirements
- 3.1.1.5 For a given system solution, the design / build contractor shall make it known to LU at Pre-contract stage if there are IPR / licensing issues that are likely to impact whole-life costs and LU liability.
- 3.1.1.6 An escrow agreement or equivalent shall be made to protect LU's interest where it is unable to secure for given product or system; the IPR ownership or unrestricted usage license to operate that product or system.
- 3.1.1.7 Migration strategies for replacement of analogue systems by digital systems shall be phased to ensure compatibility between legacy and new systems. See also section 3.6.3.
- 3.1.1.8 Personnel engaged in the system specification, design, installation, commissioning/ testing and maintenance of surveillance and security systems shall be certified competent as possessing the required knowledge and skills to perform their duties.
- 3.1.1.9 Competence management and certification systems shall conform to Head of Engineering (CPD) requirements.

3.1.2 Asset Documentation

- 3.1.2.1 The following shall be subject to LU approval and provided as a minimum for all new Surveillance and Security systems within the scope of this standard;
- i) System user/ operation manuals
 - ii) System commissioning and testing manuals
 - iii) 1st / 2nd /3rd line maintenance manuals as directed/ required by LU
 - iv) as-built drawings, wiring /system schematics, spares inventory
 - v) configuration management manual that includes all system changes
 - vi) system and detailed design documentation
 - vii) system safety documentation e.g. fault trees/ HAZID/HAZOP (as applicable)
 - viii) Compliance evidence in accordance with 3.1.5
- 3.1.2.2 System user and maintainer representatives shall be consulted as part of the approval process regarding requirements for clause 3.1.2.1 i) and 3.1.2.1 ii) / iii) respectively
- 3.1.2.3 The LU maintenance authority/ contractor shall keep an accessible and retrievable library of relevant documentation and archives to include the following as a minimum:
- 5) all asset /compliance documentation listed in 3.1.2.1
 - ii) reliability growth data where applicable, fault histories etc.
 - iii) design changes / concessions applicable to assets
- 3.1.2.4 All asset documentation shall be released to LU in electronic format under version control. Hard copies shall be provided for approved (signed & dated) versions. Information and documentation integrity and retrieval shall be compatible with BS 10008.

3.1.3 Asset Records

- 3.1.3.1 All asset records / information shall be kept up-to-date throughout the asset lifecycle and managed to a standard compatible with BS EN ISO 9001 and BS ISO 15489-1.
- 3.1.3.2 The LU maintenance authority/ contractor shall maintain (under change control) master controlled copies of all documentation / drawings defined in section 3.1.2.
- 3.1.3.3 Asset records shall conform with LU engineering asset information standard S1041
- 3.1.3.4 Drawings (formats/ conventions/ notations) shall comply with R0588

3.1.4 Asset Labelling

- 3.1.4.1 All surveillance and security system assets shall be permanently labelled / numbered to conform to LU asset numbering conventions.
- 3.1.4.2 Label design (size, colour/ contrast) shall ensure displayed characters, text or numeric are clearly legible under normal ambient lighting levels.
- 3.1.4.3 Labels shall be resistant to the adverse effects of the LU environment such that text /numeric identification information shall remain legible for the life of the asset.
- 3.1.4.4 Asset records, labelling and information management systems shall be subject to periodic inspections and audits to ensure compliance with this standard.

3.1.5 System Compliance

- 3.1.5.1 For new or altered surveillance and security systems as part of design validation; a statement of compliance shall be provided against this standard including relevant referenced requirements i.e. BSEN's etc in respect of ACS/CCTV / IDS/ Networks.
- 3.1.5.2 Compliance against referenced Industry standards / ACOP's shall be to the latest published version unless specifically advised otherwise by LU
- 3.1.5.3 The management and delivery of safety and technical assurance shall comply with LU standard 1-538.
- 3.1.5.4 A controlled plan of commissioning, testing and acceptance shall be provided to give assurance regarding technical compliance of system and performance requirements.
- 3.1.5.5 Compliance for operational requirements shall be verified against system and functional performance checklists supported by reference information.
- 3.1.5.6 The system and functional performance checklists shall be based on the verification of the URS and SRS.
- 3.1.5.7 For CCTV day and night reference images shall be captured. Reference images shall be stored electronically with high quality printed copies made available to the operator for comparison purposes.
- 3.1.5.8 Source images should be compared with the relevant stored reference image by the operator at appropriate intervals and FRC (fault report centre) notified of any defects.
- 3.1.5.9 For PTZ cameras reference images should be stored relating to each preset position.
- 3.1.5.10 Compliance against relevant legislative requirements including DPA 1998 shall be periodically checked by users/ maintainers in respect of signage, public privacy, data-security, integrity, retention and retrieval capability against this standard. Data in this respect includes video, audio and metadata.

3.2 Surveillance and Security – Site Specific Risk Assessment (SSRA) Outline

Note2. A) The SSRA is adapted from principles defined in the standards; BSEN 50132-1, BSEN 50132-7/ IEC 62676-4; and HOSDB publication 28/09.

b) The basic premise that underpins the SSRA process is that operational and security risks are not uniform across the LU network. Therefore a risk-based approach to system design could provide opportunities to improve operational efficiency and reduce whole-life costs.

c) For the purpose of this standard three relevant terms are defined:

i) Operational requirement- this is considered from a user-centred perspective and is defined as “any performance requirement (surveillance or security) that directly affects the user’s ability to operate the system or gain information from the system to make operational decisions”.

ii) Security – “the state of being free from danger or threat”

iii) Risk – this is defined as “an undesirable outcome caused by a base-event that by itself or in combination with specific triggers (a human activity, system state or condition) could result in system degradation or failure leading to a human or financial loss”.

3.2.1 All new surveillance and security system designs shall be preceded by a Site Specific Risk Assessment (SSRA) except in circumstances qualified by 3.2.5

3.2.2 The purpose of the SSRA shall be to confirm site-specific operational and system requirements at an early stage of system development taking into account the impact of the system environment and local risk factors.

3.2.3 The SSRA shall identify and assess the risks to the delivery of Surveillance and Security system functions at a given site / station to the extent that these impact the security of;

- a) Customers / Staff / other authorised personnel
- b) Premises / Assets / Infrastructure

3.2.4 This shall be achieved via a site survey that reviews local risk factors and assesses their impact on key surveillance/ security operational and system requirements. The output of the survey shall be a report that provides input to the design process.

Note. 3

The risks stated in 3.2.3 are managed via the following sub-systems;

1. CCTV – this provides visual surveillance and when supported by Video Analytics (VA) software, is also used as an intelligent object / intruder detection system. CCTV is often integrated with modern Access control systems to provide visibility of zones assigned to access control and intruder detection systems.

2. Intruder Detection System (IDS) – this can be a standalone system or be integrated with CCTV / ACS. IDS is based on a variety of object / target detection methods including typically proximity (e.g. infrared) sensors/ trip beams, electrical contacts and others as listed in 3.11.5

3. Access Control Systems (ACS) – the primary function of this system is regulate and secure access to LU Buildings or specific designated areas / rooms to authorised individuals only. Modern ACS is integrated with CCTV in the majority of applications. Integration with IDS in conjunction with CCTV is seen in applications where site perimeters and building entrances/ exits are required to be secured.

3.2.5 For low risk applications i.e. site security grade = 2 or where an existing SSRA can be adapted for reuse; the project manager and telecoms sponsor (or their nominees) may jointly agree that a new or full SSRA is not needed.

- 3.2.6 All LU sites shall be assigned a security grade to ensure system performance for a given site is commensurate with assessed local system and operational risks. The default grades (risk classifications) are given in table A below. Station classifications are given in section 5.5.3 (attachment 1)

Table A – Site Security Grades (Default)

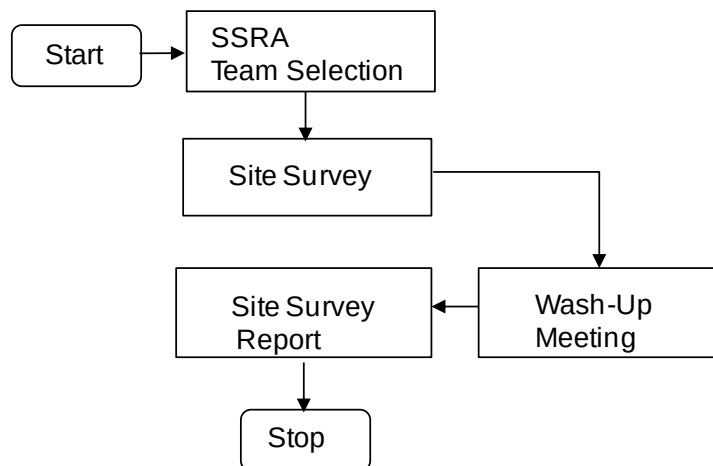
Security Grade	Station /Site classification	Classification comments
1	Non-station site – very low risk	security grading not normally applicable to LU railway locations requiring surveillance
2	Low risk surface stations or other low risk locations	Minimum level of system protection /access security. Failure of surveillance and security systems at this site may lead to local (containable) risks that will require managing but that are unlikely to have impact on the rest of the LU network.
3	Moderate risk surface, sub-surface & tube stations. Depots, substations and other sites	Moderate – high level of system protection/ access security-Failure of surveillance and security systems at this site could expose LU to moderate levels of risks during emergencies and significant service delays during degraded operation
4	High risk sites including major inter-changes/ large stations and line/ network control centres	Maximum level of system protection/ access security-Failure of surveillance and security systems at this site could expose LU to high levels of risks during emergencies and prolonged service delays during degraded operation

Note.4 The site security grade concept is based on BS EN 50132-1. The default security grades given in Table A are not related to LU Network security classifications, but are based on impact of system integrity /failures on LU services and security risks identified in 3.2.3/ 3.2.4.

- 3.2.7 The SSRA team can review any default security grading for a site suggested in this standard and change it to ensure alignment of system /functional requirements with the local risks.
- 3.2.8 The SSRA process shall comprise of a site survey and survey report. An accredited project engineer with assistance from an appropriate sponsor representative shall;
- select the SSRA team
 - coordinate the SSRA
 - record all issues, concerns raised during the survey / wash-up session
 - produce survey report with the SSRA team recommendations
- 3.2.9 The SSRA team shall be provided copies of relevant site-specific documentation /drawings (ideally ahead of the survey) prior to survey commencement.
- 3.2.10 For a given site; key functional / system requirements shall be considered in accordance with the assigned site security grade and the SSRA.
- 3.2.11 Risk-based system requirements and functionality based on BS EN 50132-1 are covered in tables A3/ A4 of attachment 1. These are not necessarily equally applicable to all LU railway environments hence the level of compliance shall be determined by the SSRA team and the design contractor.
- 3.2.12 The SSRA participants shall identify and assess on a zone-by-zone basis any risks they believe will impair key operational, system and security requirements delivered via ACS, IDS and / or CCTV.
- 3.2.13 Mitigations should be sought for moderate and high risk concerns and these shall satisfy LU cost-benefit and ALARP criterions as applicable. Wherever possible risk estimation shall be based on site-specific data sets.

- 3.2.14 The project engineer shall organise and preside over a 'wash-up' meeting following the SSRA survey to review issues / concerns raised by SSRA team and agree appropriate mitigations for moderate /high risk items if these cannot be resolved by design. The outputs from this session shall be used by the project engineer to produce the survey report that shall include SSRA recommendations for the design contractor.
- 3.2.15 The design contractor shall factor comments / recommendations from the SSRA team into the concept design and issue the document accordingly under change control.
- 3.2.16 The SSRA report is a key design input document and shall be approved and kept on file as a permanent system record subject to change control.
- 3.2.17 The SSRA team shall comprise of members from the following stakeholders;
- a) Site security managers / operational staff managing site/station
 - b) Project manager representative (Project engineer)
 - c) Telecoms discipline engineer
 - d) Network security/ BTP representative
 - e) Appropriate sponsor representative
- 3.2.18 SSRA process implementation shall be compatible with the outline given in this section (illustrated below). A suggested template is provided in attachment 1.

SSRA Process– Outline



3.3 System Requirements

3.3.1 System Development

- 3.3.1.1 The constituent parts (CCTV, ACS, IDS) needed for a given surveillance and security system and the required design specifications shall be based on a formal design brief (URS, PRS) adjusted where applicable by an approved SSRA.
- 3.3.1.2 Non-telecoms system elements of surveillance & security systems e.g. security fencing, barriers, turnstiles, lighting etc shall comply with relevant LU/BS/EN standards as referenced in section 6.
- 3.3.1.3 All surveillance and security hardware and software upgrades shall not cause compatibility or integration conflicts with existing systems or interfaces. For upgraded systems it shall be possible to revert to the last known working system version / configuration.
- 3.3.1.4 Surveillance and security system hardware and software support shall be agreed with the supplier (s) with a view to ensure optimum performance is maintained and any obsolescence risks are managed throughout the asset lifecycle.
- 3.3.1.5 Surveillance and security systems shall be designed to have a scalable architecture that is modular for ease of maintenance and upgradeable to allow future expansion including hardware and or software upgrades throughout the system life cycle.
- 3.3.1.6 IP networks and devices used for the delivery of surveillance and security systems functions shall be compatible with Ipv6
- 3.3.1.7 Retention of recorded CCTV video shall comply with LU's current policy of 14 days minimum except in trains or other mobile applications where storage limitations or other risk factors that may reduce this duration. See also 3.13.2.16
- 3.3.1.8 Surveillance and security systems shall incorporate built-in test routines and self-monitoring to continuously check system integrity and system/ user-defined settings. Unacceptable deviations detected during monitoring shall be reported as individually identifiable alarms accompanied by audible/ visual indications as defined by LU.
- 3.3.1.9 All alarms/ events, video and audio streams shall be time stamped to an accuracy within +/- 1 sec of UTC and stored permanently in a fully retrievable log in non-volatile memory. Event log retention shall not be less than 1 year unless varied by the SSRA.
- 3.3.1.10 Time-stamps shall automatically update for changes between any daylight saving offsets and UTC.
- 3.3.1.11 It shall be possible to conduct fault diagnostics, reconfiguration and software updates on Surveillance and security systems both locally/ remotely via a secure IP-data link.
- 3.3.1.12 Access to Surveillance & security systems and particularly any network connection points /interfaces installed in equipment rooms or external cubicles shall be restricted to authorised personnel only.
- 3.3.1.13 Where practicable Surveillance and security systems shall be controlled by an IS²MS (Integrated Surveillance and Security Management System).

Note. 5 IS²MS type systems are currently deployed on the LU network; e.g. station management system (SMS) installed on certain SSR/BCV stations and (MICA) management integration & control system installed on certain JNP stations.

- 3.3.1.14 IS²MS design shall be client-server based and may require to be dual-redundant depending on operational /safety risks that are required to be managed.

- 3.3.1.15 IS²MS software failures shall not be detrimental to standby, recording, emergency alarm management or event logging systems.
- 3.3.1.16 IS²MS monitored events, system alarms and operator actions shall be time stamped and stored permanently in a retrievable log in accordance to 3.3.1.9
- 3.3.1.17 The supplier shall ensure availability of technical support (from relevant OEMs) for SDK-based device /GUI integration (e.g. interface data / code/ run-time etc.)
- 3.3.1.18 IS²MS shall be based on a modular architecture and shall deliver the following functions;
- a) System and Alarm management
 - b) Surveillance and Security functions
 - c) Video management
 - d) Data storage / retrieval
 - e) Network management
 - f) System configuration management
 - g) IS²MS secure access and privileges management
- 3.3.1.19 IS²MS shall be networked and shall be protected against;
- a) unauthorised access
 - b) malware
 - c) intentional/ unintentional misuse
- 3.3.1.20 Access to the IS²MS shall be via time-limited sessions and shall require user authentication and authorisation. Password information and entry process shall be secured by default e.g. by using salted hashes and character masking respectively.
- 3.3.1.21 IS²MS users/ administrators shall be assigned the minimum privileges /functionality necessary to complete given tasks
- 3.3.1.22 Users shall be able to log out without shutting down the IS²MS workstation or any application software
- 3.3.1.23 Access and network security requirements for surveillance & security systems and the IS²MS shall comply with section 3.8 of this standard.
- 3.3.1.24 IS²MS shall support 3 modes of operation;
- a) Manual – operator has logged in to the IS²MS from a fixed position (control room). The balance of tasks/ interventions carried out by the operator and the IS²MS shall be in accordance with an HF assessment and the IS²MS specification
 - b) Automatic – in this mode IS²MS manages the site in the absence of an operator. Alarm events, customer queries are automatically handled/ managed in accordance with the IS²MS specification.
 - c) Semi-automatic – operator has logged in via a registered mobile device i.e. is on site but not in the control room. The balance of tasks/ interventions carried out by the mobile operator and the IS²MS shall be in accordance with an HF assessment and the IS²MS specification. In this mode the IS²MS shall default to auto operation if the operator ignores or is unable to respond to specific IS²MS alarms.
- 3.3.1.25 A full IS²MS cold boot /reboot shall be achieved within 5 minutes
- 3.3.1.26 The surveillance and security system supplier shall provide at LU's request all relevant certification / declarations of conformity needed to demonstrate product compliance against all applicable EN (harmonised) standards and EC directives

3.3.2 Installation

- 3.3.2.1 Surveillance and Security systems shall be installed and commissioned to a high quality of workmanship and conform to manufacturer's installation instructions and Industry good practice including;
- a) BS EN 50174 (parts 1 – 3) Cabling
 - b) BS EN 62491 – Labelling of cables / cable cores
 - c) BS EN 61935 / BS EN 50346 – Cable Testing
 - d) TIA/EIA-568 series – Structured Cabling
 - e) IEC 60793-2 – Fibre Optic cables
 - f) BS 6701 – Cable Installation /Maintenance
 - g) BS 7671 – IET Wiring Regulations
 - h) BS 7430 – COP Protective Earthing for Electrical Installations
 - i) BSEN 50132 series –Surveillance CCTV in security applications
 - j) BS EN 50131 series – Access control in security applications
 - k) BS 50133 series – Intrusion and Hold-up systems
 - l) IEEE 802.3 Wired Ethernet LAN
 - m) IEEE 802.11 Wireless Ethernet LAN
- 3.3.2.2 Surveillance and security equipment shall be protected against electrostatic discharge and electrical surge voltages/currents that can occur in the operating environment.
- 3.3.2.3 Surveillance and security equipment shall be earthed in compliance with 1-106 and relevant standards listed in 3.3.2.1 covering protective and functional earthing.
- 3.3.2.4 Surveillance and security equipment shall be installed/ maintained to ensure mechanical damage is not caused to any gaskets/ seals that will compromise IP ratings.
- 3.3.2.5 Cables shall be installed so that its armour / insulation (as applicable) is not damaged and that its bend radius is within manufacturers guidelines.
- 3.3.2.6 Cables shall be installed and tested to relevant Industry standards listed in 3.3.2.1
- 3.3.2.7 Cable joints shall be avoided wherever possible, where this is not possible joints shall be located so it is protected from mechanical damage and it can be inspected.
- 3.3.2.8 Cable selection and layouts shall take into account of voltage drop and signal losses. Signal loss calculations shall take into account future repairs.
- 3.3.2.9 Where cables are installed in runs or trunking adjacent to cables of other services, all adverse effects from and to that cable / service shall be considered.
- 3.3.2.10 Where ever possible equipment installation shall not adversely impact maintainability
- 3.3.2.11 Where practicable external surveillance and security equipment in public areas shall be installed at minimum heights from finished floor surface as required in S1371. For non-station areas, minimum height based on a local risk assessment shall be achieved.
- 3.3.2.12 System elements installed on station platforms or elsewhere close to the track shall comply with 1-356 and 1-156.

3.3.2.13 Camera Installation shall comply with the following requirements;

- a) Cameras shall be installed to ensure field of view(s) are clear of obstructions
- b) Camera enclosures shall;
 - i. Minimise internal reflections and be protected from direct sunlight
 - ii. In external environments shall be protected against condensation via thermostatic controlled internal heater
 - iii. Be mechanically secured against environment induced movement e.g. vibration / wind or accidental knocks
- c) Mounting brackets/poles shall be protected against corrosion in external environments
- d) All Cameras shall be correctly back-focused in low ambient light conditions or via an ND filter prior to installation on site
- e) Box cameras shall (where practicable) be mounted on tilt and over columns for ease of maintenance

3.3.2.14 Wherever possible installation of surveillance and security systems shall minimise the need for new infrastructure, existing poles/ brackets/ housings etc. shall be reused.

3.3.2.15 Rack assemblies used shall conform to IEC 60297 (rack unit standard).

3.3.2.16 System elements requiring mechanical protection shall where possible be installed so that it outside the reach envelope of a 95th percentile male.

3.3.2.17 Installed system elements exposed to external LU environments and where there is risk of vandalism, then these elements shall meet IP 65 (ingress protection) and IK10 (mechanical impact rating).

3.3.3 System Integration & Interfaces

3.3.3.1 Digital IP-CCTV products shall be compatible with ONVIF™ specifications to provide basic integration between products and VMS / IS²MS. Further enhanced integration of device features as required shall be achieved via SDK(s) provided by product suppliers /OEM's.

3.3.3.2 System elements involving HMI/ HCI interfaces shall comply with S1217 and S1218.

3.3.3.3 The project engineer in conjunction with the LU design contractor who approves new or modified surveillance and security systems, shall ensure;

- a) relevant HSE managers and Heads of Profession of peer disciplines are consulted in respect of any interface and integration requirements.
- b) The same consultation as in a) is repeated for end to end testing across multi-disciplined interfaces (where applicable)

3.3.3.4 Telecoms service functions delivered by multiple contracts shall be integrated to ensure end-to-end delivery of these functions.

3.3.3.5 Interfacing with OPO CCTV systems for shared coverage of station platforms shall comply with relevant requirements stated in 1-150 (See also section 3.13.1).

3.3.3.6 Lifts CCTV / alarm Interface requirements shall comply with S1093 & S1095

3.3.3.7 Passenger Help Point interface requirements shall comply with 1-142

3.3.3.8 Passenger help points (PHP) equipped with emergency alarms shall be assigned at least one non-dedicated CCTV camera view at full frame rate recording when triggered.



3.3.4 System Acceptance

- 3.3.4.1 Surveillance and security systems shall be accepted against current LU Engineering/ Project Management and Assurance processes.
- 3.3.4.2 The installed and commissioned system shall be inspected and tested by the LU contractor with a minimum of 360 hours fault free in-service trial operation having expired before being submitted by the contractor to LU for inspection and acceptance.
- 3.3.4.3 All acceptance documents including test plans / scripts shall be approved and signed off by accredited persons recognised by relevant LU Heads of Profession.
- 3.3.4.4 Final acceptance shall be based on verification against User & System Requirement Specifications (URS/SRS).
- 3.3.4.5 URS and SRS based acceptance shall be underpinned by verified (witnessed and signed-off) sub-system and system integration tests.
- 3.3.4.6 a) System acceptance is an incremental verification process that includes;
- i. Factory acceptance test (FAT)
 - ii. Site acceptance test (SAT)
 - iii. Sub-system tests
 - iv. Interface testing
 - v. System integration and interoperability testing
 - vi. System functional testing
- b) The above tests shall be witnessed by accredited LU project and discipline engineers and relevant site /station operational / security representatives.
- 3.3.4.7 The FAT provides LU representatives the first opportunity to see and test (albeit in the contractors controlled environment) the performance of the designed sub-systems /system. The level of system performance and testing that the contractor is able to demonstrate may have to be limited / truncated for practical reasons. Where this is the case LU project & discipline engineers shall assess the risks for the next stage; SAT.
- 3.3.4.8 All tests shall be traceable to documents referenced in the design compliance including URS /SRS / FRS and detailed designs etc.
- 3.3.4.9 Successful completion of system user / maintainer training shall be considered part of system acceptance unless advised otherwise by LU.
- 3.3.4.10 Where applicable the training provider shall agree with LU, the course content and competence levels to be achieved by users / maintainers /engineering managers etc.
- 3.3.4.11 Unless agreed otherwise a minimum 1 year defect liability period shall apply to all Surveillance and Security systems accepted into operational use. The supplier shall be responsible to repairing any equipment or system failures found during this period.

3.4 Power Supplies

- 3.4.1 Surveillance and security systems in the scope of this standard operated on sub-surface and tube stations and other sites with similar risks shall remain operational during periods of primary mains power failure.
- 3.4.2 Backup/ Standby power supply arrangements shall comply with 1-069 and 1-123.
- 3.4.3 Within the tolerances of S1105, surveillance and security systems shall remain fault free on the incidence of: supply transients, harmonics, over and under voltage faults.
- 3.4.4 Supply interruptions and subsequent restoration shall not cause any adverse effects.
- 3.4.5 Surveillance and security system power supply resilience shall be commensurate with the security grading for the site being protected.
- 3.4.6 The level of power supply resilience at sites that require it shall be determined by a risk assessment that takes into account;
 - i. supply bias – LU/ DNO (where applicable)
 - ii. reliability of the standby/ backup supply
 - iii. site evacuation requirements (where applicable)
 - iv. requirements for controlled system shutdown
 - v. system load requirements (Ampere-hours)

3.5 Environment

- 3.5.1 The supplier shall ensure that surveillance and security systems shall comprise of materials that do not cause a health hazard to staff or LU customers at any time. Fire safety compliance shall be against 1-085.
- 3.5.2 Where applicable the design and installation of surveillance and security systems shall comply with LU standard 1-355.
- 3.5.3 Surveillance and security systems and system interfaces, including CCTV monitors provided, shall be immunised against electro-magnetic interference, surges/ transients in accordance with BS EN 50121-4, BS EN 61643-11 and BS EN 62305-1.
- 3.5.4 System performance requirements shall be met for the full range of installation / operating environments likely to be encountered by surveillance and security systems. This shall include all parameter ranges and tolerances defined in BS EN 50125-3.
- 3.5.5 Central equipment rooms / Cubicles used to house and protect surveillance & security equipment shall be designed and maintained such that environmental parameters e.g. ambient temperature, humidity, mechanical impact/ vibrations and dust / moisture ingress etc. do not adversely affect system operation or equipment operating life.
- 3.5.6 Surveillance and security systems within the scope of this standard shall not be adversely affected by problematic environmental conditions inherent on the LU infrastructure.
- 3.5.7 Camera image performance shall be usable throughout the range of existent lighting levels including bright sunlight on surface sites and emergency lighting levels in sub-surface/ tube stations and other enclosed locations.
- 3.5.8 Surveillance and security systems shall comply with the LU standard: S1222 (EMC). The equipment shall also conform to BS EN 61000 series. These standards are documents written to comply with directive EMC 2004/108/EC.
- 3.5.9 Intruder alarms installed in open environments adjacent to residential properties shall take into account the statutory (noise regulation) requirements under EPA 1990. IDS design / installation shall comply with relevant Industry standards and codes of practice.

3.6 Processes

3.6.1 CCTV Data Downloads

3.6.1.1 Whilst local CCTV recording is still prevalent; an LU wide and consistent video downloading process shall be agreed by all relevant stakeholders in particular;

- a. Site users / operators
- b. BTP/ LU Network security
- c. CCTV system maintainer

3.6.1.2 A general video download process shall be designed to cover all VRS/ VRF's used across LU. Variations to cover particular system types shall be treated by exception. Where specific LU guidance is available on CCTV downloads, this shall be followed where practicable.

3.6.1.3 The downloading process shall take into account;

- a) Whether the download is local or from a remote position
- b) Security and access arrangements to the VRS
- c) Average download time and video file size
- d) Requirements / limitations to view downloaded video
- e) Training requirements to conduct download
- f) Equipment requirements to conduct download
- g) Cost to the maintenance organisation for each download
- h) Authentication, traceability and evidential weight of video recording

3.6.1.4 Guidance in respect 3.6.1.3 can be found in HOSDB publication 21/06 and BS 8495

3.6.2 Configuration Management & Change Control

3.6.2.1 Configuration management plans and change control processes shall comply with LU HSE change control / concession standards and be compatible with BS ISO 10007.

3.6.2.2 Changes impacting CCTV device /system configuration, views or performance shall comply with LU's change control procedure set out in Engineering Bulletin ENG006.

3.6.2.3 Changes to surveillance and security systems that contravene LU standards, system specifications or manufacturer's recommendations shall not be carried out without an approved concession from the Head of Telecommunications.

3.6.2.4 All system changes; hardware and software shall be approved and documented and kept as a record for the asset operational life.

3.6.2.5 All repairable/replaceable items shall have unique asset numbers and fault histories

3.6.2.6 It shall be possible to identify where and when a given repaired item was last used.

3.6.2.7 Hardware and software changes shall be tracked and compatibility checked through-out the system/asset lifecycle to ensure updates are aligned and interoperable.

3.6.2.8 The maintenance configuration management process shall minimise the risk of hardware/ software compatibility conflicts.

3.6.2.9 Physical repairs carried out during maintenance shall be recorded and traceable to the individual personnel that conducted the repair together with time of repair

3.6.2.10 Version control procedures shall be used to ensure the latest compatible (conflict free) system components (hardware /software) are being used and maintained.

3.6.3 Analogue to Digital Migration Strategy

Note. 6 Digital (IP-based) systems provide a number of key advantages over legacy analogue systems. These include in no particular order;

1. Higher immunity to signal noise
2. Reduced whole-life costs
3. More efficient resource utilisation (wired / wireless network connectivity)
4. Greater flexibility in system integration
5. Unlimited secure data storage
6. Remote access (for operators and maintainers)
7. Improved image quality
8. Flexible distribution of images/ alarms
9. Higher system availability / resilience to failures (dependant on system architecture)

IP (Internet Protocol) based edge devices / front end systems integrated with Ethernet /Ethernet compatible transmission systems is the de facto method of transporting communication traffic.

- 3.6.3.1 For maximum value from existing / recently installed analogue systems, migration to digital systems shall align with LU asset renewal programmes/ strategies.
- 3.6.3.2 The migration strategy shall be compatible with this standard
- 3.6.3.3 The migration strategy target shall be digital IP (Internet Protocol) based systems integrated with Ethernet / Ethernet compatible transmission systems.
- 3.6.3.4 Migration shall be phased such that system elements with the least residual life or those that cause the highest operational / service disruption (LCH) are replaced first.
- 3.6.3.5 Incremental migration shall not cause any compatibility conflicts between old and new system elements or adverse effects to the overall system objectives.
- 3.6.3.6 Where feasible, reuse of legacy elements shall be considered to ensure optimal return from installed legacy systems.
- 3.6.3.7 Migration strategy shall factor in the option of using Connect transmission services for providing networked functions as directed by LU.
- 3.6.3.8 Maintenance procedures / strategies shall be revised accordingly for partially migrated systems.

3.7 Software

- 3.7.1 This section shall be read in conjunction with sections 3.3.1, 3.6.2 and 3.8
- 3.7.2 Software requirements for individual sub-systems and particular applications are given in the respective sections;
- a) CCTV – section 3.9
 - b) IDS – section 3.11
 - c) ACS – section 3.12
- 3.7.3 Software used in surveillance & security systems shall wherever possible be COTS and be provided with an unrestricted usage license.
- 3.7.4 Embedded and application software (including security software) shall be routinely upgraded as soon as updates become available.
- 3.7.5 For software upgrades, where the un-installation of the existing (working) version is unavoidable, it shall be possible to revert to the previous version.
- 3.7.6 Software with SIL 0 or higher integrity shall be compatible with the BS EN 50128.
- 3.7.7 Software malfunctions or failures shall not prevent the use of any manual fallback system.
- 3.7.8 Regression testing shall be conducted following all software changes to reveal any adverse effects to the system.
- 3.7.9 Software changes that could impact system security shall be followed by a vulnerability assessment and if necessary full penetration tests shall be conducted to confirm that the integrity of the security system has not been reduced.
- 3.7.10 All software changes/ upgrades and testing shall be via formal planning /approvals and conducted by competent and authorised personnel.
- 3.7.11 The design, development and quality management of software used in the operation of surveillance and security systems shall be compatible with BS ISO/IEC 90003 and the guidance on software dependability stated in BS EN 62628.
- 3.7.12 Software dependability shall be consistent with target sub-system MTBF / availability requirements stated in section 3.14.
- 3.7.13 Software testing shall be compatible with the BS ISO/IEC 29119.
- 3.7.14 Software tests shall not compromise the security of the system.
- 3.7.15 Software test documentation shall be compatible with BS ISO/IEC/IEEE 29119-3.
- 3.7.16 The supplier shall provide an SDK (software development kit) for API development, GUI/ equipment interface development and integration of sub-systems/ cameras.
- 3.7.17 To aid understanding of system operation and for fault diagnostics and testing, the software supplier / developer shall produce a sufficiently detailed system architecture model that shows the interactions / coupling between the individual software modules.
- 3.7.18 A modular and structured approach with clear and defined functions for each module shall be used in the design and development of all system / sub-system software.
- 3.7.19 Clean backup copies of current system /application software shall be maintained to ensure system restoration in the case of catastrophic failures / software corruption.

3.8 Network Security (Electronic)

Note. 7 Digital (IP) networks provide system users and maintainers the capability of remotely monitoring/ managing integrated surveillance and security systems. This gives rise to security risks e.g. unauthorised access, interception/ modification of data, malware etc. This section looks at some of the basic precautions that could be taken to avoid these risks.

- 3.8.1 This section shall be read in conjunction with sections 3.3.1 and 3.7. The overall security objectives of surveillance and security systems shall be compatible with LU/TfL security standard 5-461.
- 3.8.2 Network access arrangements for surveillance and security systems shall require user authentication and authorisation and be compatible with Engineering Bulletin ENG002
- 3.8.3 User/ administrator accounts shall be assigned the minimum privileges necessary to complete given tasks. Password information and entry process shall be secured by default. For example by using salted hashes and character masking respectively.
- 3.8.4 The network design shall be (as far as it is practicable) a closed network with defined end-points, see BS EN 50159 for guidance in this respect. Data encryption shall be considered for un-trusted parts of the network.
- 3.8.5 Network design and security strategies shall be compatible with BS ISO/IEC 27002 with guidance from an LU appointed authority on electronic network security.
- 3.8.6 Software / hardware malfunctions /failures that could degrade network security shall be prevented by design or detected as an alarm sent to a central monitoring station.
- 3.8.7 Actual security breaches e.g. unauthorised access/ network attack shall be detected and contained until the network /system is free from the detected threats / risks.
- 3.8.8 Remote access over un-trusted networks shall be via a secure arrangement e.g. VPN
- 3.8.9 For a given surveillance and security system that is to be networked for remote CCTV viewing /system monitoring or local wireless access; the LU design contractor shall produce a risk assessment that reveals the vulnerabilities of the system.
- 3.8.10 The vulnerability risk assessment methodology shall be compatible with that provided in BS ISO/IEC 27005.
- 3.8.11 The vulnerability risk assessment shall;
- Identify all elements of the system that could be used to gain unauthorised access
 - Define the conditions needed to gain access to each identified element
 - Define how system security/ integrity will be maintained during a security breach
 - Propose appropriate risk control strategies and mitigations.
- 3.8.12 If the network has an external data link then this shall be protected by appropriate security controls (e.g. firewall) to secure the network against unauthorised connections malware etc. Security control configurations such as firewall filtering and blocking policies shall be reviewed and updated as needed to minimise the risk to the network.
- 3.8.13 Risk of unauthorised network access shall be minimised by turning off script execution, unused system functions and protocols by default.
- 3.8.14 Unused physical and logical ports shall be disabled. Switches and routers shall be configured to restrict usable MAC / IP addresses.
- 3.8.15 It shall be possible to objectively test security arrangements for the whole or a part of the network as required to meet LU specified Pass/fail criteria.

3.9 CCTV

3.9.1 Cameras and Lenses

- 3.9.1.1 All CCTV cameras shall be to a colour specification unless directed otherwise by LU.
- 3.9.1.2 The number and types of cameras (SD / HD) needed for a given site shall be determined in accordance with the SSRA taking into account:
- number and size of areas that need monitoring
 - user operational requirements (ref. HOSDB publication 28/09)
 - local environmental and other risk factors
 - image resolution/ size
 - project budget (for CCTV)
- 3.9.1.3 Minimum camera sensitivity for all cameras shall be < 0.5 lux (colour) for usable video equivalent to 50 IRE at f1.2, AGC OFF, based on scene reflectance of 89% and minimum ambient lighting according to 1-066.
- 3.9.1.4 The CCTV system (including lens) resolution shall be measured end-to end using BS EN 50132-7 / IEC 62676-4 test methodology such that;
- For analogue systems the minimum resolution shall be 4CIF/ 400 TV lines
 - For digital systems the minimum resolution shall be 600 TVL for HD 720p and 750 TVL for Full HD 1080p cameras.
- 3.9.1.5 The CCTV camera specification shall conform to and support a range of minimum performance requirements and features. A sample of these shown in table B below.

Camera Characteristic	Specification Requirements [Table B]
Imager types	Low noise progressive scan- colour CCD or CMOS sensors Delivering PAL/ HD compatible aspect ratio (4:3 / 16:9). Min. Effective pixels $\approx$ 440,000 (752 (H) x 582 (V) (PAL). HD sensors 720p (720 x 1280) or 1080p (1080 x1920). Non-standard high resolution Megapixel sensors e.g. for Panorama / 360° view
Imager format	$\geq \frac{1}{4}$ inch for dome cameras and $\geq \frac{1}{3}$ inch for all other camera types
Frame Refresh	Adjustable for each camera. Full frame rate: 25fps (Interlaced camera); 50fps(Progressive) Time lapse rate: 4 fps (default); Triggered rate: 12 fps
Resolution	CIF – Full HD (adjustable for each video stream)
Dynamic range	> 60dB
SNR	> 50dB (AGC OFF)
Shutter Speed	1/1s to 1/10000s minimum range
Video Codec	Shall support H.264, M-PEG 4 (AVC), M-JPEG
Streaming capability	Minimum two (independent) streams – any combination of (M-JPEG/ MPEG-4/ H.264), I-stream only capability
Features to be supported	Backlight compensation (BLC); Dynamic noise reduction; image enhancement; tone correction; white balance (ATW), adjustable colour, contrast, brightness, sharpness, AGC, privacy masking, camera angle adjustment, Video codec (settings) adjustment.
Lens type	Varifocal auto-iris lens (DC/ Video) shall be used for most SD applications. For HD applications P-iris or similar technology shall be considered. Fixed / zoom lenses shall be used where appropriate to achieve system performance.
Lens mount	Box camera; C and CS compatible; Dome: Integrated
Lens design	Standard or Aspherical construction using high quality glass optics. The latter for wide-angle views. Lens design shall minimise internal reflections, optical distortion and chromatic aberration.
Lens resolution	lens resolution performance shall be consistent with camera imager pixel resolution and the overall (end to end) system resolution requirement
Interoperability	ONVIF™ profile S (Streaming)

- 3.9.1.6 Image conspicuity shall be measured as a percentage ratio of a standard test target relative to the viewing screen height e.g. as defined in BS EN 50132-7/IEC 62676-4.

- 3.9.1.7 For ease of installation and maintenance the video and power to LU camera systems shall be carried by a common cable where ever possible.
- a) For analogue systems a co-axial (typically RG-59) cable is used, the power is AC line-fed via a CCU in conjunction with ITU-R BT.1700 (PAL) CBVS signal. Separate power cable may be used where camera distance will cause an unacceptable volt drop in a Line-feed.
 - b) For IP-based systems, a IEEE 802.3af / 802.3at compatible Power over Ethernet (PoE) minimum Cat 5e (UTP) cable shall be used to connect to an Ethernet switch. For noisy environments the use FTP/ STP variants should be considered.
 - c) For camera installations utilising fibre optic LAN's, media converters and PoE injectors shall be used as required.
- 3.9.1.8 Both analogue and Ethernet links shall be designed /installed to accommodate their respective signal bandwidths / operating distance. Thus analogue links shall for be for 5MHz (PAL) CVBS and IP links shall be over 10/100BASE-TX Cat.5e/ Cat.6 connection.
- 3.9.1.9 Extenders/ signal converters used to increase the camera (installation) range shall take into account factors such as overall system reliability, additional power /cabling requirements and effects of noise and signal attenuation/distortion on picture performance.

Note.8 Legacy CCTV systems usually comprise of CCU AC line-fed analogue colour cameras connected to a CCTV matrix / switcher. These may be partially upgraded to provide IP connectivity using multi-channel PAL to H.264 encoder(s). Legacy cabling may be retained if encoder design permits it otherwise a balun can be used to enable co-axial to Category 5e conversion.

- 3.9.1.10 Hybrid systems using digital (H.264) encoders shall provide minimum 4CIF image resolution
- 3.9.1.11 CCTV views delivered by hybrid systems shall not be used for safety-related functions (e.g. monitoring of the PTI) if the end to end latency delay exceeds 250ms.
- 3.9.1.12 LU multiple camera installations shall be synchronised from a central timing source;
- a) Analogue cameras- shall be line-locked over the common video/ power line-feed. Alternately an internal crystal sync (for encoders) or external sync may be used.
 - b) IP cameras and other network elements e.g. routers, switches, servers etc shall be synchronized using an NTP (Network Time Protocol) server. The reference time for this server shall be derived from a GPS receiver or equivalent precision source.
- 3.9.1.13 Where ever possible cameras shall be selected so that on-site local adjustments and configuration changes are minimised. Where needed adjustments /changes shall be non-intrusive and simple to perform via an integral remotely accessible data link.
- 3.9.1.14 Cameras shall be capable of automatically tracking, maintaining and holding white balance under varying colour temperatures.
- 3.9.1.15 Cameras shall automatically and simultaneously adjust shutter speed, iris setting and gain to optimise imager exposure and image quality for static /dynamic images.
- 3.9.1.16 For specialist applications (e.g. 360 degrees/ panoramic viewing) where very high resolution is recommended; higher order Megapixel cameras (> 2 Megapixel), HD-SDI cameras based on SMPTE-SDI (uncompressed video) standards may be considered.
- 3.9.1.17 The use of Hemispheric/ fisheye lens cameras shall be subject to an SSRA and the minimum performance requirements set out in this standard. Where approved, image correction / dewarping software shall be used to remove image distortion.
- 3.9.1.18 Performance of dewarped images shall be tested in accordance to IEC 62676-1-1 section 6.5 using the ISO 12233 resolution chart.

- 3.9.1.19 Auto-iris lens shall close upon power failure to prevent damage to the imaging sensor
- 3.9.1.20 IP cameras shall as a minimum;
- a) incorporate a built-in web-browser
 - b) support unicast and multicast video transmission
 - c) support the network protocols: HTTP, HTTPS, SSL, TCP, UDP, ICMP, RTSP, RTP, RTCP, TELNET, IGMPv2/v3, SMTP, FTP, DHCP client, ARP, DNS, DDNS, DNS, NTP, SNMP (MIB-2), UpnP, iSCSI, IEEE 802.1x
- 3.9.1.21 IP Cameras assigned to viewing areas where image conspicuity requirement is higher than detection; should have alarm input/output, video analytics and I-stream only capability
- 3.9.1.22 IP cameras that are accessible and capable of supporting remote downloads can be fitted with SDHC cards.
- 3.9.1.23 IP cameras shall support both dynamic and static IP addresses.
- 3.9.1.24 IP camera systems shall have minimum intra frame refresh rate ≥ 1 s. This frequency may need to be increased where there are noticeable motion / compression artefacts or where IP video is used in safety-related (OPO CCTV) applications. The optimum IP camera settings shall be determined locally.
- 3.9.1.25 LU CCTV cameras shall support programmable privacy masking to mask off one or more areas of a scene where a camera's FOV overlaps LU and private space.
- 3.9.1.26 Camera video outputs shall not be encrypted
- 3.9.1.27 PTZ cameras, mechanical or non-mechanical shall not be provided for surveillance in stations and trains except when fixed cameras cannot be used and when explicitly directed by an LU SSRA.
- 3.9.1.28 Where PTZ cameras are used they shall conform with the following additional requirements;
- a) PTZ maintenance/configuration changes shall comply with 3.9.1.13
 - b) PTZ cameras shall be able to connect into an IP CCTV network
 - c) PTZ camera-mechanical assembly shall support multiple control protocols e.g. Pelco-D, Pelco-P, Biphase, Bilinx, RS422/485
 - d) PTZ pan speed shall be 100 degrees/sec minimum
 - e) PTZ tilt speed shall be 40 degrees/sec minimum
 - f) Pan and tilt range shall be consistent with local operational requirements
- 3.9.1.29 IP PTZ's shall conform with 3.9.1.20 to 3.9.1.24
- 3.9.1.30 IP PTZ camera design shall be compatible with ONVIF™ PTZ service specification
- 3.9.1.31 All PTZ cameras shall have a home or default position that the camera will return to after operated away from this position either automatically or manually.

3.9.1.32 Where Video Analytics is incorporated into the CCTV system the analytics algorithms shall support the following features as required by operational requirements;

- a) Motion detection
- b) Virtual trip wire
- c) Double trip wire
- d) Congestion detection
- e) Counter flow detection (Wrong way movement)
- f) Theft detection (Museum Mode)
- g) Abandoned object / left package detection
- h) ROI (Region of Interest) editor
- i) Alarm sensitivity configuration (e.g. motion sensitivity/ object size/ persistence)
- j) Alarm activation on ACS / IDS or other LU defined triggers

Note. 9 Video analytics may be performed on the edge device (CCTV camera) or by centralised equipment. Each option has advantages and disadvantages.

3.9.1.33 The method and equipment used to perform the Video analytics shall be determined by consideration of operational requirements, system costs and reliability.

3.9.2 Video Switching and Multiplexing

3.9.2.1 Dedicated video switchers /matrices shall be avoided where a DVR/ NVR can perform the virtual switching function.

3.9.2.2 Camera inputs shall be monitored for video loss at the switcher / DVR for analogue cameras or for IP cameras at the hybrid DVR /NVR or other relevant LAN device.

3.9.2.3 Loss of video detection on any camera input or other system failure shall cause an alarm to be sent to a local or remote control room as directed by LU.

3.9.2.4 All alarm events detected by the video switching system shall be time-stamped and logged into a non-volatile memory store/device

3.9.2.5 The video switching system /device shall be non-blocking i.e. it can switch any camera input to any of the designated video output.

3.9.2.6 The video switching system / DVR / Hybrid DVR /NVR or other relevant LAN device shall support alarm inputs from serial data links or relay contacts.

3.9.2.7 Analogue video switchers shall be designed to receive PAL video signal (1V pk-pk) and IP video switchers shall be compatible with IEEE 802.3 and RFC 894.

3.9.2.8 Switchers shall not cause picture roll/flutter and switched views shall settle within 0.5s.

3.9.2.9 Analogue switched output performance shall be compatible with BS EN 50132-5-3

Note 10. Scene descriptors, camera ID and timestamps visible on CCTV views are collectively termed *Metadata* and can be programmed into a camera/ switcher via a character generator. Further guidance on metadata is provided in attachment 2 of this standard.

3.9.2.10 Metadata including the timestamp shall be inserted at the camera or video switching system and shall;

- a) conform to LU coding schemes /formats
- b) be clearly visible and legible and be located outside the viewing screen safe area