BBH4464

Draft Version 1.0

TRANSNET
freight rail

RAIL NETWORK
TECHNICAL SPECIFICATION
CCTV Network and Intrusion Detection Systems

Authors:	Engineering Team	
Reviewed	Infrastructure Manager Rail Network	P Dzhivhuho
Reviewed	Technical Manager Security	L Moramang
Approved	Technology Management ICTM	Nkululeko Gobhozi
Approved	Rail Network Telecommunications	Samuel Nyamah
Approved	Technology Management Electrical	Sguda Sibande

Date: 23 April 2021

Circulation Restricted To:

Transnet Freight Rail

Transnet and Relevant Third Parties

1 BACKGROUND 1

2 SCOPE 1

3 COMPLIANCE 1

4 OPERATING CONDITIONS 2

5 STANDARDS 2

6 OPERATIONAL REQUIREMENTS 2

6.1 SERVICE LEVEL AGREEMENT 2

7 TECHNICAL REQUIREMENTS 4

7.1 CCTV CAMERA SOLUTIONS 4
7.2 NETWORK VIDEO RECORDER REQUIREMENTS 6
7.3 NETWORK VIDEO MANAGEMENT SOFTWARE 7
7.4 CAMERA MOUNTING POLE 10
7.5 LOCAL AND REMOTE MONITORING WORKSTATION: CONTROL AND OBSERVATION CENTRE 10
7.6 CAMPUS NETWORK REQUIREMENTS 11
7.7 LINK AND BACKHAUL REQUIREMENTS – BACKBONE NETWORK SUPPORT 19
7.8 NETWORK CABLE AND INSTALLATION REQUIREMENTS 20
7.9 ENCLOSURE REQUIREMENTS 22
7.10 INTRUSION DETECTION SYSTEMS 23
7.11 FAILSAFE TELECOMMUNICATION CONNECTIVITY 27
7.12 INFORMATION AND COMMUNICATION TECHNOLOGY 27
7.13 POWER REQUIREMENTS 30
7.14 BACKUP POWER SYSTEM AND BATTERIES 32
7.15 ACCESS CONTROL 34

8 GUIDELINES AND PROCEDURES 36

8.1 ADDITIONAL INSTALLATION REQUIREMENTS 38

9 EVALUATION AND PERFORMANCE TESTING 38

APPENDIX A: CCTV CAMERA PERFORMANCE REQUIREMENTS 39

I. Document Authorisation

FUNCTION	NAME	TITLE & DIVISION	SIGNATURE	DATE
Reviewed By:				

II. Distribution

Once updated, a copy of the latest revision will be published on the document management system, “Project Wise”.

III. Document Change History

ISSUE NO.	DATE ISSUED	ISSUED BY	HISTORY DESCRIPTION

IV. Changes since Last Revision

CLAUSES	DESCRIPTION
1.10	

V. List of Abbreviations and Acronyms

Abbreviation	Description
AC	Alternating Current
AD	Active Directory
AES	Advanced Encryption Standards
AH	Ampere Hour
bit	Binary Digit
BS	British Department of Trade and Industry Specification
CAT5e	Category 5 Enhanced

CCTV	Closed-circuit Television
CoC	Certificate of Compliance
DC	Direct Current
EMI	Electro-Magnetic Interference
EN	CENELEC
ETSI	European Telecommunications Standards Institute
FQDN	Fully Qualified Domain Name
GPa	Giga Pascal
GPS	Global Position System
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
Hz	Hertz
ICASA	Independent Communications Authority of South Africa
ID	Identification
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronic Engineers
IP	Ingress Protection
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
km	kilometer
KVA	Kilo-Volt Amperes
LC	Lucent Connector
m	Meters
Mbps	Megabits per second
ML	Machine Learning
mm	Millimetre
MPa	Mega Pascal
MPPT	Maximum Power Point Tracking
MTBF	Mean Time Between Failure
nm	nanometer
NVR	Network Video Recorder
NVR	Network Video Recorder
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PoE	Power Over Ethernet
PTZ	Pan-Tilt-Zoom
SABS	South African Bureau of Standards
SANS	South African National Standards

SC	Standard Connector
SFP+	Enhanced Small Form-factor Pluggable
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Shielded Twisted Pair
TACACS+	Terminal Access Controller Access Control System protocol
TFR	Transnet Freight Rail
TIA/EIA	Telecommunications Industries Association/Electronic Industries Association
UPS	Uninterruptable Power Source
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
V	Volts
W	Watts
WAN	Wide Area Network

VI. Relevant Documentation Applicable

DOCUMENT NO.	DESCRIPTION	LOCATION
CENELEC	European Committee for Electro technical Standardization	External
ETSI	European Telecommunications Standards Institute	
ICASA	Independent Communications Authority of South Africa	External
IEC	International Electro technical Commission	External
ISO 9000	Quality Management Systems.	External
BS 3939	British Department of Trade and Industry Specification:	External
SABS	South African Bureau of Standards	External
SANS	South African National Standard	External
BBB3235	Installation of earthing and lightning protection of electronic measurement equipment housing	Internal
CSE-1154-001-CAT E48 Ver 2	Standard of Physical Characteristic of the Railway Environment in South Africa	Internal

1 Background

Transnet Freight Rail experiences theft on a daily basis. Theft and vandalism of TFR assets are prohibiting the company to reach its milestones and goals. Additional security measures such as CCTV networks and intrusion detection systems as part of a security system. These technologies coupled with security operational processes/services will reduce or mitigate vandalism incidents.

2 Scope

The purpose of this document is to specify the requirements needed to implement a CCTV network and intrusion detection system within Transnet Freight Rail and integrate it with the current security system. This document focuses on the components needed by Transnet to implement such a system.

The quantities and the number of accessories will be provided in the Schedule of Requirements, or Bill of Quantities, or Design Document, this will be specific to an area/site and will be outlined in the Scope of Works.

The main areas/sites of installation will be in and outside substations, relay rooms and telecommunication buildings, however it is not limited to these areas/sites, any area/site that needs to be safeguarded can form part of the scope of this specification.

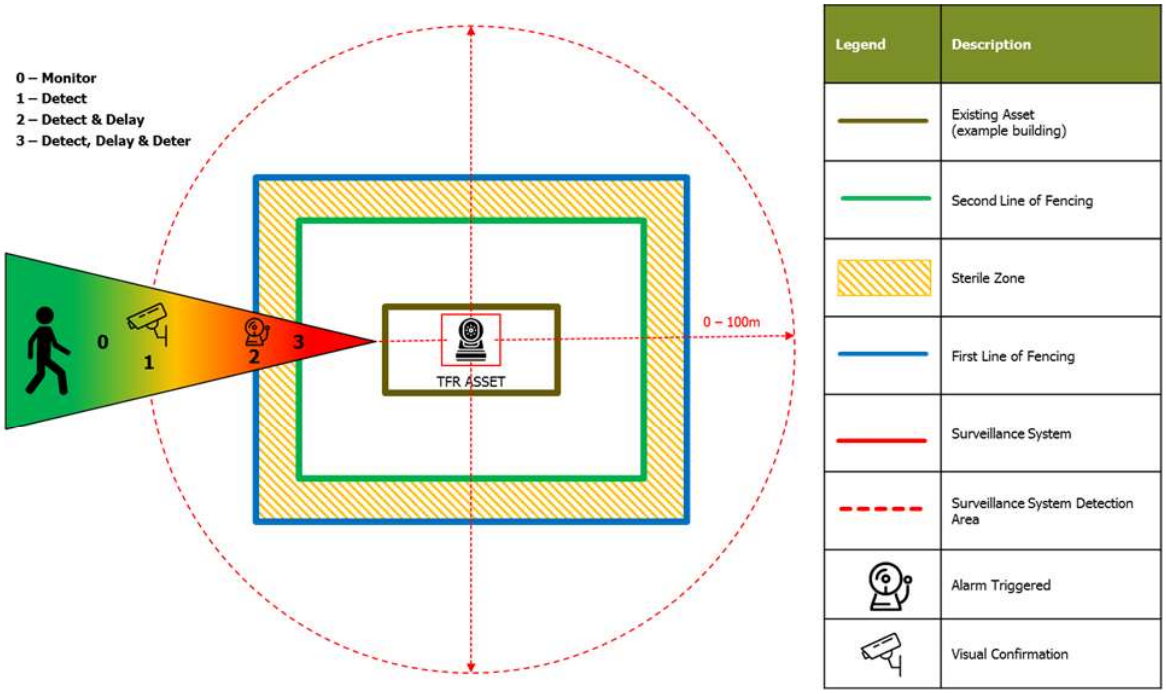

Figure 1: Context Diagram of system

3 Compliance

a) Tenders shall comply with all the specifications and requirements as indicated in this document. Any deviation from the specification shall be indicated in the tenderer's submission

document. Transnet Freight Rail shall have the prerogative to accept or reject any deviation which may lead to a disqualification of a noncompliant bidder.

b) Transnet Freight Rail reserves the right to inspect all equipment, components and subsystems before finalisation and approval of the contract.

4 Operating Conditions

All equipment supplied shall be designed to operate without degradation in accordance with the most conservative figures outlined in the Physical Characteristic of the Railway Environment in South Africa standard (CSE-1154-001-CAT E48 Version 2)

5 Standards

a) Except where otherwise stated in this specification, all equipment, installation shall conform to the latest recommendations of the ITU-T, ETSI, SANS, ISO, IEEE, SABS, CENELEC and IEC Standards, relevant to all technologies that will be proposed as a solution.
b) All standards and requirements in this document shall be adhered to and any deviations shall first be discussed with the Transnet Freight Rail and a formal agreement which is signed by both parties shall be drawn up to state Transnet Freight Rail's acceptance of deviance
c) Tenderers shall certify with proof that they are familiar with these deliverables and shall state all instances where their equipment offered is unable to comply. If tenderers do not comply with this requirement, their tenders shall no longer be considered and their bid shall be cancelled.

6 Operational Requirements

6.1 Service level agreement

Transnet Freight Rail requires a service level agreement (SLA) with the contractor for the duration of the contract. This agreement shall focus on the maintenance, guarantee and warranty policies related to the components that make up the CCTV network and intrusion detection systems. The conditions of the Service Level Agreement shall be dictated by Transnet Freight Rail prior to awarding of the contract and shall be a separate document outlining service-related expectations from the contractor.

6.1.1 Maintenance

Transnet Freight Rail requires maintenance to be added as a service by the contractor where and if required by Transnet Freight Rail. If the maintenance of certain components of the CCTV and intrusion detection system is required by Transnet Freight Rail, then the maintenance shall be done on a schedule proposed by the contractor and approved by Transnet Freight Rail. The maintenance shall include physical component maintenance and software maintenance if Transnet Freight Rail deems the hardware used by the contractor necessary of routine maintenance. When maintenance is done by the contractor, the contractor shall provide a document which clearly distinguishes the difference between a replace and a repair as per their maintenance procedures. This document will be used by Transnet Freight Rail to verify routine maintenance procedures conducted by the

contractor, if these routine maintenance procedures are required by Transnet Freight Rail. The downtown will be defined on the maintenance document.

6.1.2 Warranty and Guarantee

Transnet Freight Rail requires that each individual piece of equipment (included it subsets and dependent components) contains a warranty period of at least 3 years.

6.1.3 Training

Transnet Freight Rail may require training at the specific areas/sites where the CCTV systems or Intrusion detection systems are installed. When training is needed, Transnet Freight Rail shall determine how many individuals per site require training, prior to the contract being awarded. Transnet Freight Rail shall also determine what type of training the individuals need. For each of the different training requirements listed below, a standard operating procedure (SOP) document shall be supplied by the contractor.

6.1.3.1 Maintenance training

Transnet Freight Rail requires basic maintenance training to designated personnel for the new equipment being installed. The supplier shall provide training.

6.1.3.2 Fault finding training

Transnet Freight Rail requires basic fault finding training (first line support and train the trainer training for internal TFR training) to be given to designated personnel. This training shall focus on fixing basic faults that occur with the different components forming the CCTV network and intrusion detection system. A designated diagnostic manual shall be provided for all equipment which outlines error codes or probable errors to enable a maintenance worker to perform maintenance, once the agreed upon terms of maintenance has been settled within the definitions of the contract.

6.1.4 Planning

Transnet Freight Rail requires both a business continuity plan and a disaster recovery plan issued by the contractor for the system installed.

6.1.4.1 Business continuity plan

A procedure shall be put in place that shall allow Transnet Freight Rail business to continue if one of the components of the CCTV system or intrusion detection system fails. That is to say whenever a piece of equipment is used for access control or remote control purposes, that can affect the operations of Transnet Freight Rail and its personnel, a failsafe procedure shall be built into the equipment to ensure that faulty equipment does not hinder access to a site, service or any operational function of the company. This procedure shall contain different cases and shall be approved by Transnet Freight Rail.

6.1.4.2 Disaster recovery plan

A procedure shall be put in place that allows Transnet Freight Rail business to restore the CCTV network or intrusion detection system in the case of equipment and infrastructure being destroyed or

damaged. This procedure shall focus on how quickly the system can be restored. This procedure shall contain different cases and shall be approved by the Transnet Freight Rail. This procedure shall follow only after the SLA has lapsed.

7 Technical Requirements

7.1 CCTV Camera Solutions

This section discusses the multiple variations of CCTV cameras. The general camera requirements that shall be applicable to all the cameras are listed below:

a) The cameras will be at least full High Definition (HD) JPEG2000 lossless digital IP type, or at least H.264 lossy digital IP type, as specified in the BOQ. The cameras shall be selected for suitability for internal and external Surveillance.
b) Indoor cameras shall be standard vandal resistant ceiling/wall mount fixed dome and fitted with built in variable focal, dc-auto iris lenses to ensure optimal optical efficiency. Where no false ceiling is available, cameras will be mounted against wall.
c) Outdoor cameras shall be mounted in purpose made weatherproof housings to protect camera from dust, rain and strong winds.
d) All camera signal, data and power cable will be wired to the equipment enclosure closest to its position. The video data signal cable (Cat6 UTP) will be terminated to the Security LAN Network (SLN) via a 24 way TCP/IP data switch inside the 19” equipment rack cabinet.
e) All cameras will be Power-Over-Ethernet compliant.
f) A suitable communication path shall be provided to ensure reliable transmission of control signals from the control equipment to any camera assembly.
g) All signal, control and power cables shall be installed inside bosal conduit, trunking and cables racks/baskets. The bidder shall agree with the engineer all routes. All equipment and cables shall be protected against lightning damage.
h) All camera lenses shall be Mega Pixel 1/3” or 1/2” (Or latest) or 9-22mm or higher (scientific grade) DC Iris type. All lenses shall be of Day/Night optics type, even if the lens is build-in. The correct angles of view will be set up for each individual camera. All lenses shall be of glass type lens and not plastic.
i) The bidder is required to supply and install a modern high-definition IP-Based Video Surveillance system of the best quality.
j) All cameras mounted within and on the facility buildings will be linked to and powered by a star-topology distributed network of POE switches with fibre uplinks to the Central Control Room. An Observation Control Room with mirrored recording is essential for a completely fail-safe solution.
k) The IP-based Surveillance cameras offered are required to function in conjunction with the Network Video Management Software (NVMS) to provide a complete solution that delivers full situation awareness and indisputable detail, leading to faster response times, reduced investigation times, compliance validation and superior overall protection.
l) To achieve this level of detail all camera types supplied and installed should not provide less than 170 pixels/metre of digital clarity. All cameras must be able to adequately cope with variable lighting conditions and in scenes where simultaneous low and high light exist concurrently. This will ensure facial identification in all scenes where cameras are to be installed.

m) Certification and training for authorized integrators shall be available from the manufacturer or his local representative.
n) The manufacturer's warranty, extended warranty and replacement policies shall be included for each specified component. All major components are to carry a 36-month warranty.
o) The solution offered shall be well proven in the field and have been installed and operating in similar configurations for at least three years. References shall be provided for a minimum of three operational sites.
p) Due to the security nature of this requirements and the critically of this application only proven products shall be considered.
q) Products could be approved only after investigation by all applicable parties.
r) All externally mounted cameras supplied by the contractor are to be protected against power surges with suitable inline 100 BaseT single POE protection devices which shall meet or exceed the following design and performance specifications:-
   - Cable CAT6, Clamping Voltage <70 V, Max Discharge Current 4.5kA (coarse protection), Max Discharge Current 300A (fine protection), Pairs Protected 1-2, 3-6, 4-5, 7-8, Standards Compliance Fast Ethernet 802.3u; IEC 11801; IEEE 802.3, Insertion Loss in dB <0.10@20Mhz, <0.10@62.5Mhz, <0.30@100Mhz, Next (As per IEC 11801) >43@20Mhz, >32.4@62.5Mhz, >33.6@100Mhz, Return Loss (IEC 11801) >27.8@20Mhz, >31.4@62.5Mhz, >22.8@100Mhz, Data Rate >200 Mbps, Bandwidth (3dB) per pair >350 Mhz.

7.1.1 General Specifications for H.264 High Definition Day/Night IP Cameras (Dome and Box)

a) The Camera shall support 100BASE-TX and PoE 802.3af network interfaces for streaming video and control data over standards compliant networks.
b) The Camera shall operate in the SYSTEM Control Centre environment with support for automatic detection of cameras, encoders and NVRs in the same broadcast domain.
c) The Camera shall be ONVIF (AND/OR PSIA IF APPLICABLE) compliant.
d) The Camera shall have multi-streaming support including different frame rate, bit rate, resolution, and quality and compression format from an individual camera.
e) The Camera shall have a built-in web server to make video and configuration available in a standard browser environment. The built-in web server shall support multiple users with different permission levels and unique usernames and passwords.
f) The Camera shall support user configuration of network parameters including: Static IP address; Subnet Mask; Gateway; and Control Port for control communications.
g) The Camera shall support user configuration of camera parameters including: Camera Name; Location and Logical ID.
h) The Camera shall support user configuration of image acquisition parameters including: Exposure Control; Flicker Control; Iris Control; Day/Night Control; White Balance Control; Colour Saturation and Sharpening.
i) The Camera shall support a mode that automatically removes the IR filter and enters a monochrome mode when the available light drops below a set threshold.
j) The Camera shall support user configuration of an unlimited number of independent motion detection zones within the camera field of view.
k) The Camera shall support user configuration of up to 3 Privacy zones within the camera field of view.

l) The Camera shall support remote zoom and focus control of the lens and performing automatic focus.
m) The Camera shall support user configuration of compression format, compression quality, maximum bit rate, key frame interval, and image rate per individual camera.
n) The Camera shall have input/output terminals for connecting alarm inputs and alarm outputs.
o) The Camera shall have an audio input for connecting external microphones.
p) The Camera shall have a video output for connecting external monitors.
q) The Camera shall support UDP transport.
r) The Camera shall be remotely upgradeable over an IP network for feature enhancements and investment protection.
s) The Camera shall have a 3-axis pan-tilt-twist gimbal system for positioning the lens and image sensor.
t) The Camera shall have tamper resistant screws.
u) The Camera shall have a ceiling mount bracket.
v) The OUTDOOR IP DOME Camera Series shall be functional in outdoor environments.
w) The OUTDOOR IP DOME Camera Series shall have a built in heater.
x) The Camera shall meet or exceed the detail design and performance specifications (Appendix A).

7.2 Network Video Recorder Requirements

a) Each Multi-Megapixel Network Video Recorder (NVR) is to be provided in a space saving 2U 19” rack-mount chassis and is to be designed to achieve the highest performance for high definition video recording and playback.
b) The NVR must be scalable to operate seamlessly in an environment with multiple NVRs, as a single solution.
c) Each NVR must be preloaded with Multi-Megapixel Network Video Management Software and configured for maximum performance and reliability.
d) The NVR is to record up to 32 MB/s of image data from 10 up to 96 camera channels or more running at 30 images per second. It is to be of enterprise-class reliability with a RAID-5 hot swappable hard drive (6 SATA) configuration, and the option for redundant power supplies.
e) Both the hard drives and the power supplies are to be hot-swappable for online repairs.
f) Each NVR is to have 4 gigabit Ethernet ports and an effective 10TB of on-board recording Capacity or more. The NVRs in the Central Control Room must incorporate an expansion card for connection to an external 15TB (effective) storage expansion unit or more, also configured in Raid-5.
g) The Network Video Recorder (NVR) Storage Expansion units are required in the Central Control Room to expand the recording capacity of the NVR servers in this location. Each expansion unit is to be provided in a space-saving 3U rack-mount chassis and is to have enterprise class reliability with a RAID-5 hard drive configuration and redundant power supplies. Both the hard drives and power supplies are to be hot-swappable for online repairs. The storage expansion units are to have 15TB effective recording capacity and are to connect directly to a RAID card in NVR server using a SAS cable.

7.3 Network Video Management Software

7.3.1 The video management software provided is to be a licenced Enterprise Edition and is to run seamlessly on the NVRs provided. It is to function in conjunction with the cameras installed to provide a complete solution that delivers full situation awareness and indisputable detail, leading to faster response times, reduced investigation times, compliance validation and superior overall protection.

7.3.2 The NVMS is to have the capability to manage both audio and video from a broad range of multi-megapixel IP cameras. In addition, the system must have the capability to accommodate conventional and PTZ analogue cameras and both audio and video from a broad range of 3rd party IP cameras, and encoders from leading manufacturers.

7.3.3 The NVMS is to be powerful, yet intuitive, with an easy to use interface that allows operators to efficiently evaluate and respond to events with minimal training.

7.3.4 As it is a requirement to integrate the NVMS into both Access Control and Intercom Control systems the NVMS is to be an open-source platform with access to the Control Centre SDK source code and technical support from the software developer.

7.3.5 The NVMS shall have all video and integration licenses provided as a once-off fee with unlimited client connections to all NVRs at no charge. Recurring annual license fees are not acceptable.

7.3.6 The NVMS shall be pre-loaded on turn-key servers running the latest version of Microsoft Windows with configurable storage.

7.3.7 The NVMS shall be an enterprise level software solution that shall be scalable from one client, server, and camera to hundreds of clients, servers, and cameras.

7.3.8 The NVMS shall include the Server Software Applications (Control Centre Server, Control Centre Admin Tool), Client Software Applications (Control Centre Client, Control Centre Web, Client Control Centre Player, and Control Centre Camera Installation Tool).

7.3.9 The NVMS shall permit server and client software applications to be installed and run on both the same computer or on separate computers.

7.3.10 The NVMS shall support High Definition Stream Management (HDSM) architecture which includes, Support for industry standard JPEG2000, MJPEG, MPEG-4, and H.264 compression formats.

7.3.11 Support for reducing the required client bandwidth and processing power by only transmitting what is necessary to view the video stream at full quality (e.g. if a user is viewing a 5MP camera in a 1MP window then a 1MP representation of the 5MP image shall be transmitted).

7.3.12 The NVMS shall support recording and monitoring video and audio streams from sources with bandwidth up to 90 Mbit/sec, frame rate up to 60 fps, and video resolution up to 16MP (4872x3248).

7.3.13 The NVMS shall require no proprietary recording hardware, no hardware multiplexer or time-division technology for video and audio recording or monitoring.

7.3.14 The NVMS shall not limit the storage capacity and shall allow for upgrades of recording capacity.

7.3.15 The NVMS shall digitally sign recorded video and audio using 256-bit encryption or higher so video can be authenticated for evidentiary purposes.

7.3.16 The NVMS shall securely transmit all command and control data via TCP/IP using cryptographic keys based on SSL to prevent eavesdropping or tampering.

7.3.17 The NVMS shall be capable of being upgraded from one version to another without having to uninstall the previous version.

7.3.18 The NVMS shall automatically detect if video or audio source firmware is out of date with respect to the current installed software and upgrade it.

7.3.19 The NVMS shall run as a service configured to automatically start when the server or workstation is powered on and automatically recover from failure or attempted tampering.
7.3.20 The NVMS shall allow system administration, and live and recorded video and audio monitoring all from a single client application that can be located anywhere on the network.
7.3.21 The NVMS shall provide a search functionality to discover Control Centre Server instances running on computers connected on a different network segment than the Control Centre Client by using IP addresses or hostnames.
7.3.22 The NVMS shall provide the ability to connect a video or audio source to multiple NVRs to achieve redundant recording.
7.3.23 The NVMS shall provide the ability to create a failover connection for a video or audio source. If the NVR that the video or audio source is connected to goes offline then the failover NVR will take over the connection.
7.3.24 The NVMS shall provide administration of all system connections from a single window.
7.3.25 The NVMS shall support receiving Simple Network Management Protocol (SNMP) messages from servers and alert the user.
7.3.26 The NVMS shall provide the capability to rename all video and audio sources and NVRs.
7.3.27 The NVMS shall record video and audio streams based on a recording schedule that can be defined individually for each video source. The schedule shall be created with the parameters (Recording Mode, Continuous, Motion, Digital Inputs, Alarms, License Plates, Time and Date Settings, Daily, Weekly, and Monthly).
7.3.28 The NVMS shall provide the ability to manually trigger recording.
7.3.29 The NVMS shall provide a pre-event and post-event recording option.
7.3.30 The NVMS shall provide a reference frame recording option in the absence of events.
7.3.31 The NVMS shall perform motion detection on each individual video source with adjustable sensitivity, threshold and detection zones.
7.3.32 The NVMS shall provide the ability to reduce the image rate of recorded video over time as a means of increasing record time. The image rate shall be able to be reduced to one half or one quarter of the original image rate. This setting can be configured separately for each video source.
7.3.33 The NVMS shall provide the ability to set a maximum recorded video retention time for each video source.
7.3.34 The NVMS shall authenticate users before granting access to the system. Access rights for each user shall be able to be defined individually for each user, and shall and include, Viewing live images, viewing recorded images, Connect and disconnect cameras, Setup cameras, Setup servers, and Access to individual video and audio sources.
7.3.35 The NVMS shall provide the ability to import Windows users and use Windows credentials to authenticate users.
7.3.36 The NVMS shall provide the ability to create alarms.
7.3.37 The NVMS shall provide the ability to schedule backups of recorded video with associated events to a local folder or mapped network drive.
7.3.38 The NVMS shall provide the ability to email users and system administrators when an event or system health error occurs.
7.3.39 The NVMS shall have the capability to execute User Notification Actions (Display on-screen message, Play a sound), Monitoring Actions (Start live streaming video), Device Actions (Reboot camera, Trigger digital output), PTZ Actions (Go to pre-set, Run a pattern, Set auxiliary, Clear auxiliary), Alarm actions (Trigger an alarm, Acknowledge an alarm) in response to any of the events listed above.
7.3.40 The NVMS shall provide a maintenance log and audit trail of all system errors and events.

7.3.41 The NVMS shall provide the ability to define a region of an image where license plate detection is performed. Detected license plates shall be stored along with the video data.

7.3.42 The NVMS shall provide the ability to create a Watch-list that will be used to create events when any license plate on the watch-list is detected in the images being analysed.

7.3.43 The NVMS shall provide the ability to enable and configure PTZ control on the RS-485 interface of a video source.

7.3.44 The NVMS shall support a wide range of PTZ camera protocols.

7.3.45 The NVMS shall provide the ability to change the network settings for a video and audio source.

7.3.46 The NVMS shall provide the ability to change image quality and image rate parameters for a video source without affecting the settings on the other video sources.

7.3.47 The NVMS shall provide the ability to enable a secondary stream for live viewing.

7.3.48 The NVMS shall provide the ability to change the exposure, iris, IR filter, backlight compensation, gain, priority, sharpening, saturation, focus, and white balance settings for a video source.

7.3.49 The NVMS shall provide the ability to change the image dimensions for a video source.

7.3.50 The NVMS shall provide the ability to add Privacy zones to a video source to block unwanted areas in the image field of view.

7.3.51 The NVMS shall provide the ability to save and restore the window layout.

7.3.52 The NVMS shall provide the ability to control the system using a PC keyboard or joystick.

7.3.53 The NVMS shall provide the ability to import and export client settings such as maps, views, and web pages.

7.3.54 The NVMS shall support live or recorded video monitoring of 1 to 36 video streams simultaneously on a single monitor with an unlimited array of user-defined layouts.

7.3.55 The NVMS shall support the ability to display the following list of image overlays (Camera Name, Camera Location, Timestamp, Record Indicator, PTZ Controls, Motion Activity and License Plate).

7.3.56 The NVMS shall support an unlimited number of monitors for monitoring video and audio streams.

7.3.57 The NVMS shall support monitoring live and recorded video and audio streams simultaneously on the same monitor.

7.3.58 The NVMS shall support viewing the same live or recorded video stream at different zoom levels.

7.3.59 The NVMS shall support the ability to cycle through views (guard tour) based on a specified interval.

7.3.60 The NVMS shall support the ability to drag and drop a video source from a tree of video sources into a window for live or recorded video and audio monitoring.

7.3.61 The NVMS shall support the ability to create a map that represents the physical location of cameras and other devices throughout the Surveillance system. Maps shall be created from images stored in JPEG, BMP, PNG, or GIF image formats. Maps shall have the ability to contain links so as to create a hierarchy of interlinked maps.

7.3.62 The NVMS shall highlight a camera on a map when an alarm linked to the camera is triggered.

7.3.63 The NVMS shall support digital zooming and panning on live and recorded video streams.

7.3.64 The NVMS shall support forward and reverse playback of recorded video and audio at variable speeds.

7.3.65 The NVMS shall support navigation of recorded video and audio via calendar, timeline, or events.
7.3.66 The NVMS shall support the ability to export recorded audio in WAV format.
7.3.67 The NVMS shall support the ability to snapshot a live or recorded image and export it from the system.
7.3.68 The NVMS shall support the ability to export a live stream of images in the various formats (JPEG, PNG, TIFF)
7.3.69 The NVMS shall support the ability to export video from multiple camera streams in Native format.
7.3.70 The NVMS shall support reviewing video and audio that was exported in the Native format.
7.3.71 The NVMS shall support authenticating video that was exported in the Native format to validate that it was not tampered with.
7.3.72 The NVMS shall support converting video that was exported in the Native format to an industry standard format.
7.3.73 The NVMS shall support reviewing video and audio stored in a backup.
7.3.74 The NVMS shall super users who will be able to create users, allocate user levels, edit user details, and delete users off the system

7.4 Camera Mounting Pole

7.4.1 The masts for PTZ and static outdoor cameras shall be 9m hollow spun concrete and shall be planted in 32Mpa concrete basis of 1.2 x 1.2 x 1.2m.
7.4.2 A 1,5m x 15mm steel rod with molecularly bonded copper cladding shall be mounted to the apex of the mast. This shall serve as the air termination of a lightning conduction system which will further consist of a 50mm2 stranded bare copper down conductor running inside the mast to four 1,5m copper clad earth rods driven into the ground at the extremities of the excavation for the base of the mast before the concrete is cast.
7.4.3 The tops of the earth rods will be interconnected with the continuous 50mm² down conductor.

7.4.4 All connections in this down conduction path shall be hard soldered or fusion welded ('Cadweld').
7.4.5 The specifications of the pole must make provision for lightning protection.

7.5 Local and remote monitoring workstation: control and observation centre

This section should be used when local monitoring is required.

7.5.1 Supply a professional high performance Local and Remote Monitoring Workstations (RMWS) specifically designed to achieve the highest performance for a client control station within a multi-megapixel High Definition Surveillance System.
7.5.2 Each workstation, supplied in a desktop form factor, must have the capacity to support up to four high resolution (full-HD) monitors displaying a total 144 channels of concurrent video. The RMWSs are to be pre-loaded with Control Centre Client Software and supplied with a keyboard and mouse.
7.5.3 The RMW must meet or exceed the technical Specifications (Control Centre Edition Enterprise, Viewing Streams Up to 144 concurrent / workstation, Viewing Rate Up to 10MB/s,

latest Microsoft Windows OS, Network Interface , Display hardware, Video Outputs 4, 4 Display Port, or 4 DVI, Optical Drive 1 DVD-RW, Form Factor Desktop , and Power Consumption.

7.5.4 The HD Video Surveillance Monitor offered must meet or exceed the technical specifications (Diagonal Screen Size 40", Type 120Hz LED BLU, Resolution 1920 x 1080p, Aspect Ratio 16:9, Pixel Pitch 0.461(H) x 0.153(V), Brightness 450 cd/m², Contrast Ratio 6000:1**,** Response Time 6ms, Input Display Port / DVI to suite RMWS, and Mounting Wall-Mount VESA 400 x 400mm

7.6 Campus Network Requirements

The purpose of this section is to define the requirements needed by Transnet Freight Rail to create a network for IP end devices. This network will be called a campus area network and the IP end devices will be the CCTV cameras or intrusion detection sensors. This campus network will be used in areas that are large, such as Transnet Freight Rail yards, fuel depots and terminals where a simple CCTV and NVR solution will not suffice.

To form a campus area network IP devices (CCTV cameras or intrusion detection sensors) connect to various mini switches/media converters, from where the mini switch/mini converter can use a wireless path or landline path (fibre optic cable) to connect to a core switch. From the core switch the series of IP end devices can be connected to Transnet Freight Rail's backbone network. The backbone network link is described in section 7.6.

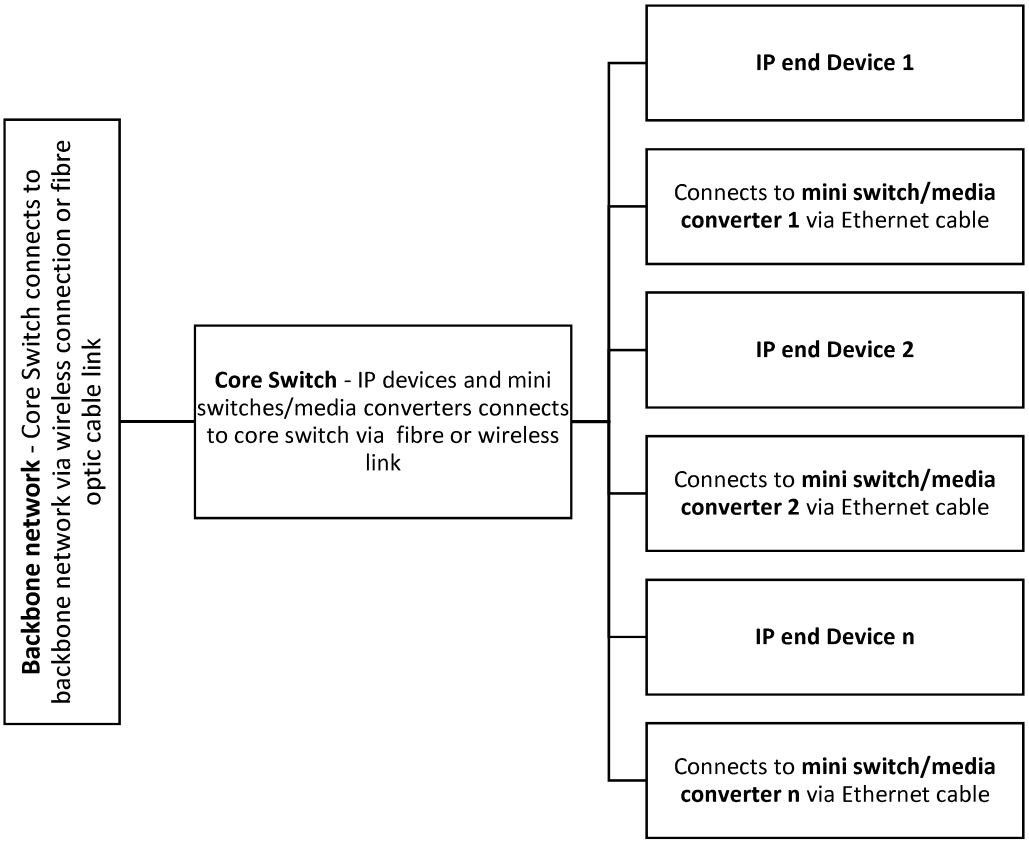

Figure 2 Campus Network Configuration

The components of the CAN are broken down into enclosures, switches, media converters, wireless communication requirements and power requirements. Two main subsystems shall exist, being the networking requirements and the power requirements. The quantities and the number of accessories shall be provided in the Schedule of Requirements, or Bill of Quantities, and Design Document which are part of the tender documents.

7.6.1 Fibre Switch

This section discusses the distribution fibre switch (This fibre switch may also be used as distribution switch where and if required by Transnet Freight Rail). This switch shall serve as the main hub for the relevant CCTV cameras/intrusion detection sensors to connect to at a specific site.

a) The fibre switch shall be installed and configured to work on a Transnet's campus network.
b) The fibre switch shall be able to fit within a 19" network rack (, appropriate connectors and adaptors shall be supplied and installed to make the switch fit by the contractor.
c) This fibre switch should be installed at each site where all the CCTV or intrusion detection information will be sent, this is to store information at servers installed. This fibre switch will act as hub/core for all rings which will be created.

Dual voltage power supply capabilities are required on the switch, in other words, the ability to be powered by either a DC power source or AC power source (230 VAC, 50 Hz), depending on the needs of Transnet Freight Rail for a specific situation. If a dual power supply is not applicable to a certain switch, appropriate adapters/converters shall be supplied by the contractor. These adapters/converters shall implement a dual voltage capability, thus being able to supply the switch via DC power or AC (230 VAC, 50Hz) power. This should contribute to n + 1 back up supply.

7.6.1.1 General Requirements

The following list shall be applicable to all the types of fibre switch as well as media modules mentioned in section 7.3.2 mentioned below.

a) Shall have OSI layer 2 and layer 3 capability.
b) Fully SNMP manageable with remote configuration.
c) Advanced QoS routing support
d) OSPF routing support.
e) IPv4 and IPv6 routing.
f) Support for TACACS+.
g) 48 Volts DC power supply integrated in chassis.
h) 802.1Q-based VLANs enable segmentation of networks
i) Secure remote management of the switch via Secure Shell (SSH) and SSL encryption.
j) Shall include operating system and licenses.
k) Local configuration via Ethernet, USB or RS232.
l) The weight shall not exceed 9 kg, with a tolerance of 0.5kg.
m) The SFP+ port shall be compatible with SFP+ and 1000Base-LX SFP transceivers.
n) Up to 25.5 W available on the copper ports for PoE. Must comply with IEEE 802.3at
o) All CCTV cameras in section 7.1 shall be able to be connected to the switch, the switch shall provide enough power through PoE and bandwidth to operate the cameras optimally.

7.6.1.2 Type A

a) 48 x 1000 Base LX ports with SFP interface card
b) 4 x 10GBase –LR with SFP ports interface card
c) Modular chassis with expansion slots
d) Industrial Ethernet standard
e) 48 – 10/100/1000 UTP Ethernet interface card
f) 4 x Port 10 Gigabit Ethernet copper interface card
g) 48 volts DC power supply integrated in chassis.
h) Rack mountable

7.6.2 Media modules Requirements

This section discusses the multiple variations of the media modules. Media modules will be used to connect IP end devices via Ethernet cable. In this case the IP end devices will be the CCTV cameras or intrusion detection sensors. Thus, a media module is a switch that allows an IP end device using a UTP Ethernet connection to connect to an IP network or the Transnet Telecoms network.

a) All the types of media modules listed in section 7.6.2 shall be able to communicate with each other (transmission and reception of data) when connected on the same campus network. This communication shall be done over a fibre optic cable link between two different media module. Media modules shall also be able to communicate with each other over a wireless link, as specified in section 7.6.8.
b) All the types of media modules listed in section 7.6.2 shall be able to communicate (transmission and reception of data) with all the types of switches listed in section 7.6.1, when connected on the same campus network. This communication shall be able to be done over a fibre optic cable link between different media module modules and different cores switches. Media modules shall also be able to communicate with core switches over a wireless link, as will be explained below in section 7.6.6.
c) The media modules shall be installed and configured to work on a Transnet Freight Rail's campus network.
d) The media modules switch selection shall be able to fit within a 19" network rack, appropriate connectors and adaptors shall be supplied and installed by the contractor to make the switch fit.
e) This media modules should be installed in a ring topology at each region being secured and this ring should be connected to a fibre switch mention in 7.3.1.
f) N + 1 electrical supply should be installed for power back up. Can either be a DC or AC.

Dual voltage power supply capabilities are required on the switch, in other words, the ability to be powered by either a DC power source or AC power source (230 VAC, 50 Hz), depending on the needs of Transnet Freight Rail for a specific situation. If a dual power supply is not applicable to a certain switch, appropriate adapters/converters shall be supplied. These adapters/converters shall implement a dual voltage capability, thus being able to supply the switch via DC power or AC (230 V, 50Hz) power.

7.6.2.1 General Requirements

All media modules variations will be the interface between the optical fibre cable and the STP cable and must meet the following requirements:

a) It should have automated route protection, such as if the optical fibre breaks in one direction, traffic will be re-routed automatically using the opposite direction.
b) The module should support O-ring for redundancy (recovery time <20 ms or better).
c) The module must be console and telnet manageable.
d) The module must support SNMP network management (also SNMP trap event)
e) The module should have RS232 serial console port for local area management purposes.
f) These modules should be industrial specified modules and should thus be able to operate in harsh environments and meet the following standards:
    I. IEC 60068-2-27 - Shock protection
    II. IEC 60068-2-32 - Free fall protection
    III. IEC 60068-2-6 - Vibration protection
    IV. IEC 60950 - Safety
    V. IEC 60529 - Dust and water protection

7.6.2.2 Type A

a) 12 x 10/100/1000 Base-T PoE+ ports.
b) 2 x 1000Base-LX SFP ports.
c) Minimum IP30 housing design
d) Maximum 850 grams
e) Rail mounting enabled.

7.6.2.3 Type B

a) 8 x 10/100/1000 Base-T PoE+ ports.
b) 2 x 1000Base-LX SFP ports.
c) Minimum IP30 housing design
d) Maximum 850 grams
e) Rail mounting enabled.

7.6.2.4 Type C

a) 4 x 10/100/1000 Base-T PoE+ ports.
b) 2 x 1000Base-LX SFP ports.
c) Minimum IP30 housing design
d) Maximum 850 grams
e) Rail mounting enabled.

7.6.3 Fibre Cable Properties, Accessories and Installation Requirements

This section describes the scenario when fibre optic cable is used to connect the CCTV cameras or other IP end devices to the core switches.

The fibre cable will be supplied by Transnet Freight Rail. Only installation of the fibre optic cable is required. The installation of the fibre optic cable shall comply with Transnet Freight Rail's telecommunication standards. All installation connectors, adaptors and accessories related to fibre optic installations shall be supplied by the contractor. All supplied adaptors, connectors and accessories shall integrate and correspond with current Transnet Freight Rail network configurations. The fibre accessories shall comply with Transnet's latest Specification for Optical Fibre Accessories

SPC-00583. All fibre optic installation accessories and configurations shall be approved by the quality assurance department of Transnet Telecommunications.

7.6.3.1 Cable Fittings and Installations

a) All fibre cabling connectors, tensioners, mounting equipment, termination equipment shall be supplied and installed by the contractor.

7.6.3.2 Fibre Patch Leads

Fibre patch leads shall to be supplied and installed by the contractor. The types of connectors and length of the patch lead will vary per requirement. All the patch lead requirements shall be approved by Transnet's telecommunications team.

a) Ruggedized patch leads are required, in the following standard lengths i.e. 1, 2, 7, 10, 15 m.
b) The patch leads shall be suitable for single mode applications.
c) It shall be duplex patch leads.

7.6.3.3 Redundancy with Fibre Campus Networks

Transnet Freight Rail requires redundancy to be implemented on its fibre ring loops where they are part of the network campus, this shall be in the form of a self-healing ring topology. All media converters and core switches listed in section 7.6.2 and section 7.6.1 respectively, shall be able to connect in this ring topology structure where required by Transnet Freight Rail. The following scenarios shall be possible:

(A node refers to either a core switch or a media converter.)

a) If a fibre link between two media converters in a ring fails, the communication between all the nodes in the fibre ring shall still be possible.
b) If a fibre link between one media converter and one core switch in a ring fails, the communication between all the nodes in the fibre ring shall still be possible.
c) If a fibre link between two core switches in a ring fails, the communication between all the nodes in the fibre ring shall still be possible.

7.6.4 SFP Requirements

The following section describes the SFP module requirements. These SFP modules shall be supplied, installed and configured by the contractor.

7.6.4.1 Type A

a) The module shall be hot pluggable.
b) The module shall be compatible with the switches in section 7.6.2 and 7.6.1.
c) 1000Base-LX accomplishing a maximum distance of 10 km, with a tolerance of 500m.
d) Dual LC ports shall be available.
e) It shall be a single mode fibre SFP.
f) Wavelength shall be 1310 nm.

7.6.4.2 Type B

a) The module shall be hot pluggable.
b) The module shall be compatible with the switches in section 7.6.1.
c) 10GBase-LR SFP+ accomplishing a maximum distance of 10 km, with a tolerance of 500m.
d) Dual LC ports shall be available.
e) It shall be a single mode fibre SFP.
f) Wavelength shall be 1310 nm.

7.6.4.3 Type C

a) The module shall be hot pluggable.
b) The module shall be compatible with the switches in section 7.6.1.
c) 10GBase-ER SFP+ accomplishing a maximum distance of 40 km with a tolerance of 1km.
d) Dual LC ports shall be available.
e) It shall be a single mode fibre SFP.
f) Wavelength shall be 1510 nm.

7.6.5 Patch Panel Requirements

The following section discusses the requirements of the fibre patch panels.

The connecter type of the fibre patch panel may vary between SC and LC depending on the need of Transnet Freight Rail.

7.6.5.1 General requirements

The following are general requirements that shall be applicable to all fibre patch panels.

a) It shall fit in a standard 19” network cabinet.
b) It shall not take up more than 1U rack space.
c) It is for single mode purposes.
d) It shall be suitable for simplex fibre.
e) Relevant pigtailed splice cassette shall be supplied and installed.
f) Relevant splice protector holders shall be included.
g) All relevant adapters/connectors for fibre installation shall be supplied and installed by the contractor.

7.6.5.2 Type A

a) Number of ports shall be 24.

7.6.5.3 Type B

a) Number of ports shall be 12.

7.6.5.4 Type C

a) Number of ports shall be 6.

7.6.6 Link Requirements

Needs may change according to the specific site of installation, refer to contract requirements.
The following section will describe the type of links that Transnet can use to link the media converter switches (devices) to the core switches and the core switches to the backbone network. These links can either be fixed landline or wireless.

7.6.7 Fibre link

The following section describes the requirements when a fibre link is used.

a) Transnet Freight Rail shall supply the fibre optic cable where needed.
b) The fibre cable shall be installed by the contractor.
c) All termination equipment shall be supplied and installed by the contractor.
d) All fibre accessories shall be supplied and installed by the contractor.
e) Any mounting equipment and connectors for the fibre shall be supplied and installed by the contractor.
f) After fibre installation quality assurance tests shall be conducted on the fibre installed complying with Transnet Freight Rail telecommunications standards. These results shall be provided to the Transnet telecommunication team.
g) If the overhead traction equipment masts are used to mount fibre it shall comply with standards set out by Transnet Freight Rail for this type of mounting. Fittings and connectors for this type of mounting shall be approved by Transnet Freight Rail. The latest version of the specification PRC-00112, -*Written Safe Work Procedure for Erection of Self-Supporting Optical Fibre on AC OHTE,* shall be adhered to.
h) Fibre optic cable inspections shall be done before installation of the fibre optic cable by the contactor. These results shall be communicated to the Transnet telecommunications department. The standard procedure *Pre-Test Quality of Optic Fibre Cable on Drums*, PRC-00107 shall be adhered to.
i) Fibre optic cable inspections shall be done after the installation of the fibre optic cable by the contactor. These finding shall be communicated to the Transnet telecommunications department. The standard procedure *Post-Installation Tests of Optic Fibre Cable*, PRC-00106 shall be adhered to.

7.6.7.1 Wooden Poles

Transnet Freight Rail may require wooden poles to be supplied and planted. These wooden poles will serve as overhead telecommunication routes for the fibre optic cable or UTP/STP cable.

a) Standard 9 and/or 11 metre wooden poles are required.
b) All Transnet Freight Rail wooden pole requirements are specified in the Transnet Freight Rail specification document SPC-01242 (Specification for Wooden Telephone Poles). The wooden poles shall comply with the latest revision of this specification document.
c) All testing and quality assurance documentation as required by specification document SPC-01242 shall be supplied.
d) The wooden poles erection requirements are specified in Transnet Freight Rail specification document SPC-01279 (Specification for the Erection of Wooden Telephone Poles for the Support of Optical Fibre Cables). The wooden poles erection method shall comply with the latest revision of this spec document.
e) All connectors and mounting equipment for mounting the fibre optic or UTP/STP cables on wooden poles, shall be supplied and installed by the contractor.

7.6.7.2 Concrete Poles

Transnet may require concrete poles to be supplied and planted. These concrete poles will serve as overhead telecommunication routes for the fibre optic cable or UTP cable. The poles shall be planted as per specification (Transnet Freight Rail shall provide the specification).

a) All connectors and mounting equipment for the fibre optic or UTP/STP cables shall be supplied and installed by the contractor.

7.6.8 Wireless Connectivity

The following section describes the needs and requirements when wireless connectivity is used to provide connection for the network campus elements. This section focuses on two different types of wireless solutions. The first being point to point and the second being point to multipoint wireless links.

Dual voltage power supply capabilities are required for the access points/links, in other words, the ability to be powered by either a DC power source or AC power source (230 VAC, 50 Hz), depending on the needs of Transnet for a specific situation. If a dual power supply is not applicable to a certain access point/link, appropriate adapters/converters shall be supplied, these adapters/converters shall implement a dual voltage capability, thus being able to supply the switch via DC power or AC (230 V, 50Hz) power.

7.6.8.1 Wireless Links

This section focuses on a wireless point to point and point to multipoint link systems. This system will predominately be used to wirelessly connect switches. IP end devices will be connected to the switches.

7.6.8.1.1 General Requirements

a) It shall be a wireless IP-based network.
b) Point to point and point to multipoint performance of the wireless communication shall be at least 100 Mbps .The data being transmitted and received shall be encrypted, shall Transnet Freight Rail shall confirm on encryption requirements.
c) The solution shall operate in a licensed band and comply with all rules and regulations as defined by ICASA.
d) All wireless components used in outdoor applications which are directly exposed to the outdoor weather shall be rated with an ingress protection rating of IP66.
e) All antenna and link module mounting hardware shall be supplied and installed by the contractor.
f) The wireless links shall be able to connect and communicate between two points.
g) The switches specified in section 7.6.2 and 7.6.1 with Ethernet capability shall be compatible with the wireless link system.
h) Shall include operating system and licences.
i) The links shall be installed and configured to work on a Transnet Freights Rail's campus network

7.6.8.1.2 Wireless Multipoint Radio Unit

a) Shall have a 10/100Base-T and Ethernet interface port. The multipoint radio unit shall at least have one Gigabit Ethernet 1000Base-T port to connect to the selected switch.
b) IPv4 management enabled and interface capabilities.
c) The device shall be connected to a suitable antenna.
d) The multipoint radio unit (excluding antenna) shall fit in a 19-inch network cabinet.
e) The antenna for a multipoint radio unit shall have a maximum dimension of not more than 350 width x 350 depth x 650 height mm, with a tolerance of 50mm in each dimension.
j) The multipoint radio unit shall connect and communicate to the switches specified in section 7.6.2 and 7.6.1. with an Ethernet connection.

7.6.8.1.3 Directional Radio Unit

This section describes the directional radio unit that shall be used to form the point to point links.

a) Shall have a 10/100Base-T or RS-232 interface port. The directional radio unit shall at least have one Gigabit Ethernet 1000Base-T port to connect to the selected switch.
b) IPv4 management enabled and interface capabilities.
c) Point to multipoint communication shall be possible with the multipoint access link (in section 7.6.8.1.2).
d) Point to point links shall be able to both transmit and receive data
e) The directional radio unit shall be able to connect and communicate to the switches specified in section 7.6.2 and 7.6.1. with an Ethernet connection.

7.3.8.1.4 All antenna dimensions are subject to contractual agreement of site-specific requirements. All antenna shall be able to offer functional capabilities listed above.

7.7 Link and Backhaul Requirements – Backbone Network Support

The following section describes the type of links that can be used to link the CCTV NVR system, network campus and the intrusion detection network to the nerve centre. The nerve centre is in a Transnet building where Transnet Security will monitor the alarms and CCTV footage. Remote control monitoring is explained in detail in section 7.8.

It shall be either a wireless link or a landline medium such as a fibre network.

7.7.1 Wireless link – CCTV Cameras and Intrusion Detection

The following section describes the needs and requirements when a wireless link is used to provide connection for the CCTV cameras, campus network and intrusion detection systems. This wireless link will be a high bandwidth backbone link that will transmit the data to the nerve centre or to the closest Transnet telecoms hub.

a) It shall be a wireless IP-based network.
b) The data being transmitted and received shall be encrypted. Encryption shall be specified to the contractor prior to commencement of installations by Transnet Freight Rail
c) The solution shall operate in a licensed band and comply with all rules and regulations as defined by ICASA.
d) Point to point performance of the wireless communication shall be at least 100 Mbps.

e) All wireless components used outdoors which are directly exposed to outdoor weather shall be rated with an ingress protection rating of at least IP66
f) All antenna and access point mounting hardware shall be supplied and installed by the contractor.
g) The communication modules shall be capable of operating in environmental temperatures between -10ºC to 65ºC no airflow.
h) The link to link communication shall be able to maintain 100 Mbps over a distance of 40 km.
i) The system shall be powered via the power system as specified in section 7.13.
j) The contractor shall supply and install all cabling and mounting equipment for the wireless links.
k) If the antenna is not a standalone system all additional network equipment shall be fitted into the network cabinet in section 7.9.
l) All power supplies for the system shall be supplied and installed by the contractor.
m) The wireless antenna and mount shall have a maximum dimension not more than 600 width h x 600 depth x 600 height mm with a 20mm tolerance.

7.7.2 Wireless Communication – Intrusion Detection

The following section describes the requirements when a wireless communication system is used to provide connection for alarms of certain intrusion detection sensors to the nerve centre. This can be a standalone system, for example it can be a mobile modem.

a) The modules shall have nationwide South African coverage to ensure network connectivity at specified sites.
b) The communication modules shall be capable of operating in environmental temperatures of up to 65 °C with no airflow.
c) The data being transmitted and received shall be encrypted. Encryption requirements shall be specified to the contractor prior to site installation by Transnet Freight Rail.
d) The solution shall operate in a licensed band and comply with all rules and regulations as defined by ICASA.
e) All wireless components used outdoors which are directly exposed to outdoor weather shall be rated with an ingress protection rating of IP65.
f) The module shall have a maximum dimension not more than 300 width h x 300 depth x 300 height mm with a tolerance of 20mm.
g) The communication protocol for wireless communication shall provide coverage across at least 85% of the population and at least 85% of the national railways and roads across the Republic of South Africa.

7.8 Network Cable and Installation Requirements

The following section specifies the requirements of the UTP/STP cabling that is to be installed as part of the respective CCTV networks. The UTP/STP cabling shall be supplied and installed by the contractor. The decision on whether to use STP or UTP cable shall be determined by the site requirements.

All relevant connectors and mounting equipment shall be supplied and installed by the contractor. All outdoor UTP/STP cables shall be waterproof and be capable of withstanding all outdoor weather

conditions such as rain and etc. they shall comply with an Ingress Protection rating of 66 (IP66). Appropriate outdoor RJ45 connectors shall be supplied and installed by the contractor

7.8.1 CAT5e Ethernet Cable

a) This cable shall be installed from the NVR to an end device, such as an IP camera.
b) The cable may also be used for certain types of intrusion detection systems
c) The cable may also be used for the wireless link system
d) When installed outdoors it shall be inside a protection pipe which TFR will confirm and agree with the contractor upon the award of the contract
e) The following shall be complied to when working with this cable:
   The cable shall be ruggedized such that it is designed or improved to be hard-wearing or shock-resistant.
   I. If the CAT5e is installed outdoors, the exterior shall be waterproof and UV protected which TFR will confirm and agree with the contractor upon the award of the contract.
   II. If the CAT5e is installed indoors, the exterior shall still be ruggedized such that it is designed or improved to be hard-wearing or shock-resistant.
f) The cable shall comply with the IEC 24702 Industrial Ethernet standard
g) Below are some of the properties of installation that shall be considered.
   I. Careful consideration needs to be taken with respect to insertion loss and bending radius of the cable.
   II. With respect to installation methodologies and quality assurance the EN 50174 – 1 and EN 50174 – 2 shall be complied with.
   III. With respect to required earthing for information technology equipment in buildings the EN 50310 shall be complied with.
   IV. The testing of building infrastructure shall comply with EN 50346
   V. Installation shall comply with EN 50174 – 3

7.8.2 Cable Fittings and Installations

All fittings and installation components shall be approved by the Transnet Telecommunications QA department

a) The contractor shall supply and install suitable cable mountings, fitting equipment, connectors and tensioners.
b) Fittings and mounting connectors shall be able to support UTP/STP cables on poles and buildings such that all environment parameters such as wind are taken in account.
c) Fittings and mounting connectors shall be able to support UTP/STP cables within buildings.
d) The UTP/STP cable in use shall adhere to the accompanying bend radius specification.
e) UTP/STP cable shall be protected against its own stress and weight, such that they are securely mounted and not free hanging
f) Cables shall be labelled clearly, such that it shows the designation of the device it is connected to in a form of a label.
g) COC certificates shall accompany installation of the UTP/STP cables from a licensed institution and evidence thereof shall be presented by the contractor.
h) Adequate cable trays, wire ways and conduits shall be supplied and installed where applicable.
i) If drilling is required, it shall first be discussed with the Transnet Telecommunications division and appropriate Transnet procedures shall then be followed where required.
j) The relevant parts of ISO/IEC 11801 Standards shall be followed for installations.

k) The installation shall comply with ICASA regulation where applicable
l) All data cables shall be compliant with ISO 11801, TIA/EIA 568A and EN 50173 where relevant.

7.9 Enclosure Requirements

7.9.1 Indoor

The following section specifies the requirements of the indoor cabinet, into which network components shall be installed, such as the NVR system, switches and all relevant battery/power sources.

7.9.1.1 General Requirements

The following are general requirements that shall be applicable to all indoor enclosures.

a) The cabinet shall have a solid particle protection of at least 5 and an IP rating of IP52.
b) All the different types of NVR systems as specified in section 7.2 shall fit in the indoor cabinet.
c) All the different types of switches as specified in section 7.6 shall fit in the cabinet.
d) Any required connectors and adaptors for the NVR system shall be supplied and installed by the contractor.
e) All wall mounting connectors shall be supplied and installed by the contractor. Mounting connectors will be specified by Transnet Freight Rail prior to site installation for a specific site.
f) Sufficient cooling (active or passive) shall be supplied in the cabinet, suitable of cooling different electronic components. The cooling system can be determined by the contractor.
g) The cabinet shall have fitted mains power sockets.
h) All the types of UPS and battery configuration requirements shall be able to fit inside the cabinet as specified above. If the cabinet does not have enough space for the external batteries of an UPS, it shall be discussed with the Transnet telecommunications team prior to site installation.
i) Cabinets shall be earthed as per Transnet Freight Rail standard which can be found in applicable documents section.
j) Cabinets and components shall be labelled in order to clearly distinguish what equipment they hold are what functional designation they occupy.
k) Cabinets shall be securely fitted and have lock with key.

7.9.1.1.1 Type A Cabinet

A standard 19” with 12U rack space network cabinet with opening and closing front and back doors.

7.9.1.1.2 Type B

A standard 19” with 16U rack space network cabinet with opening and closing front and back doors.

7.9.2 Outdoor Cabinet and Concrete Poles

The following section specifies the requirements of the outdoor cabinet, into which network components shall be installed.

7.9.2.1 General Requirements

The following are general requirements that shall be applicable to all outdoor enclosures.

a) The complete installation of the outdoor cabinet shall comply with the Ingress Protection rating of IP 65.
b) Shall allow Top Hat DIN type rack to accommodate variety of components, otherwise it shall allow a G section DIN type rail if Heavy equipment is to be used (e.g. PLC)
c) All the different types of communication modules a specified in section 7.6.2 shall be able to fit in the outdoor cabinet, the maximum dimension of the media converter which shall be not more than 440 width x 300 depth x 88.9 height mm shall be able to fit in the cabinet.
d) Appropriate and adequate electrical surge protection and earthing are required for the outdoor cabinets. This protection shall comply with the latest version of the Transnet Specification for Outdoor LV Installations for Telecommunication Networks. This protection shall be supplied and installed by the contractor.
e) Cabinets shall be earthed as per Transnet Freight Rail standard.
f) Sufficient cooling (active or passive) shall be supplied in the cabinet. The cooling solution shall not compromise the ingress protection rating of 65 of the cabinet.
g) Heat generation calculations shall be done according to the communications components inside the enclosure (maximum environmental temperatures shall also be taken into consideration); the cooling solution shall be derived from these calculations.
h) The cabinet shall be able to mount on concrete poles and also overhead electrical traction equipment masts of Transnet Freight Rail. Mounting equipment shall be supplied and installed by the contractor. Transnet Freight Rail mounting standards can be found under applicable documents section.
i) Standard 9 and/or 11 meter concrete poles shall be supplied and installed where required by Transnet Freight Rail. The concrete pole shall be able to support the full weight of the outdoor cabinet and a full complement of components and also solar panels (section 7.13.2) (with mounting equipment) where required by Transnet. All poles shall be in accordance to SANS 470:2012 Concrete poles for telephone, power and lighting purposes.
j) The mounting equipment shall be able to support the weight of the cabinet and all the equipment within the cabinet.
k) The cabinet shall be able to support all of its contents.
l) All types of fibre patch panels from section 7.6.5 shall be able to fit in the enclosure.
m) Appropriate cable glands shall be fitted to ensure an IP rating of 65. This shall be done where any cable enter the cabinet which could compromise the ingress protection rating of the cabinet

7.9.2.1.1 Type A

a) The maximum tolerance dimensions of the outdoor cabinet: 600mm width x 400mm depth x 750 mm height. (Standard 19” components shall be able to fit).

7.9.2.1.2 Type B

a) The maximum dimensions of the outdoor cabinet: 600mm width x 400mm depth x 400 mm height. (Standard 19” components shall be able to fit).

7.10 Intrusion Detection Systems

This section specifies the various types of intrusion detection systems that are required.

7.10.1 Types of Intrusion Detection Systems

a) Virtual fences.
b) Passive Movement Detection alarm.
c) Door alarms.
d) Radar system.
e) Tamper detection.
f) Fence sensors

7.10.1.1 Virtual Fences

There are two types of virtual fences that can be created. The first is using software, integrated within advanced camera surveillance systems. This is camera-specific and our only requirement is that no alarms are generated for any activity outside of the virtual fences configured on the camera. These types of software will undergo the same amount of scrutiny and shall fulfil specifications as outlined in section 7.8 regarding Remote Control and Monitoring.

The fixed cameras in section 7.1 shall be able to be set up with virtual fence intrusion detection. A single camera should be able to be configured with at least 3 virtual fenced areas, each area shall be capable of detecting movement and triggering alarms. For example if a single camera is installed on the outside wall of a substation facing the fence, it shall be able to be configured with a virtual fence zone outside the fence, a zone on the fence and a zone inside the yard.

The other type of virtual fences uses a laser or infrared beams to detection motion between two fixed points, creating a literal virtual fence instead of a physical fence. For these types of fences, the requirements will be the same as for alarm beams.

7.10.1.2 Passive Movement Detection Alarms

a) For Passive Movement Detection alarm placed inside buildings or structures, the sensors shall be able to monitor an area with a tolerance of at least 10m x 10m and have a detection angle of at least 110 degrees.
b) Passive Movement Detection alarm shall utilise infrared or appropriate electromagnetic spectrum to ensure sensors do not generate false alarms from spiders, mice etc.
c) Passive Movement Detection alarm shall be wall-mounted and positioned in such a way as to be discreet in its detection capabilities.
d) Passive Movement Detection alarm shall be coupled to an appropriate electric system and back-up power or batteries to ensure continuous protection, as specified in section 7.13.
e) For Passive Movement Detection alarm outside the building/s, sensors shall be able to operate in all South African weather as specified in the Transnet Freight Rail environment specification under applicable documents.
f) For Passive Movement Detection alarm mounted outside, configuration and direction of beams shall be formally agreed upon by a Transnet Freight Rail to ensure its detection capabilities are able and sanctioned for the relevant security risk.
g) For Passive Movement Detection alarm mounted outside, the casing shall be of a design that shall not attract unwanted attention from potential intruders. Transnet Freight Rail shall formally agree to the appearance and robustness of sensors prior to installation.

7.10.1.3 Door Alarm Requirements

a) Door alarm sensors shall be capable to be placed on metal doors.
b) Door alarm sensors shall not be susceptible to any electromagnetic interference.
c) Door alarm sensors shall be appropriately positioned and securely fixed to the doors to ensure they will be sensitive to the door being opened or an attempted intrusion.
d) Door alarm sensors shall always be installed indoors.
e) Door alarm sensors shall comply with IP 67.
f) Door alarm sensors shall be supplied by an electric system and back-up power or batteries to ensure continuous protection, as specified in section 7.13.

7.10.1.4 Fence Sensors (Vibration Sensors)

This section specifies vibration sensors to be mounted on fences surrounding the site which may be existing or installed fences. This type of sensor shall detect vibration on fences that is related to theft, vandalism and intrusion. The sensor shall transmit an alarm to notify the relevant security and Transnet personnel of a probable intrusion.

a) The module shall have a maximum tolerance dimension not more than 100 width x 60 depth x 100 height mm.
b) The components of the fence sensor shall be enclosed in an IP66 housing.
c) Maximum weight of the module shall not exceed 500 grams.
d) All wireless communications shall be ICASA approved.
e) All mounting equipment shall be supplied and installed.
f) The sensor enclosure shall be ruggedized such that it is designed or improved to be hard-wearing or shock-resistant and withstand tampering.
g) The sensor shall be battery powered. The battery shall be able to supply power for 1 year without recharging or replacement.
h) The sensor shall have a false alarm rate less than 10%. Each sensor's sensitivity settings shall be set that false triggered alarm events are less than 10% of total alarm events. Contractor shall provide guideline on how to distinguish false from actual alarm events.
i) The system shall be able to be mounted on fences as describe in technical specification. (Rail Network Technical Specification Fencing & Sterile Zones)
j) The sensor modules shall be capable of operating in environmental temperatures as specified in section 6.2 of the accompanying TFR environmental standard (Physical Characteristic of The Railway Environment In South Africa)

7.10.1.5 Higher Order Frequency Systems

a) Any type of system that utilises a system operating on a frequency outside the radio or infrared band shall ensure its operating frequencies comply with the necessary South African government regulations and comply with such standards.
b) Higher-Order Frequency sensors shall be able to function at a range of at least from 3m to 1000m to detect possible intruders.
c) Higher-Order Frequency sensors shall be able to distinguish targets (i.e. humans only and no other objects) to an accuracy of at least 95% confidence and shall be able to distinguish multiple targets, from a minimum of 1 target and upwards.
d) Higher-Order Frequency sensors shall be appropriately mounted to attain range as specified above. Sensors shall be positioned such that they are able to detect targets at least 180 degrees and have rotational capabilities or have a complete 360-degree detection radius.

e) Higher-Order Frequency sensors shall have communication capabilities to communicate target movements and alarm notifications to the Transnet Nerve Centre either directly or via the NVR / Campus network configuration.
f) Higher-Order Frequency sensors shall be able to continuously monitor and distinguish when a target is moving towards a high-value location or object prioritised for security.
g) Higher-Order Frequency sensors shall be rigged and shall be able to operate in all South African weather conditions including rain and wind etc. and shall comply to IP66
h) The sensitivity of Higher-Order Frequency sensors shall be adjustable and configured with approval by a relevant Transnet employee or representative to ensure proper security functionality.
i) Higher-Order Frequency sensors shall be coupled to an appropriate electric system and back-up power or batteries to ensure continuous protection, as outlined in section 8.
j) If the electromagnetic spectrum emitted by the Higher-Order Frequency sensors has the potential to be dangerous for humans, then it shall be stipulated as such and a formal agreement of the safe working conditions, for maintenance and normal operation within the sensor's vicinity, shall be drawn up by the supplier and the Transnet Safety department.
k) Higher-Order Frequency sensors shall be able to continuously provide protection and only need maintenance once a year or longer.
l) Higher-Order Frequency sensors shall be able to integrate with the PTZ-type CCTV camera system from section 7.1. When the higher order frequency sensor detects movement or intrusion, it shall be able to redirect the PTZ camera's field of view to a specific point of intrusion/movement.

7.10.1.6 Other Intrusion Detection Sensors

Any type of sensor that has not been outlined above or is contained in section 7.7.1 outlining the intruder detection via optic fibre, falls into this category. This includes tamper detection sensors and capabilities which shall pre-emptively detect and identify possible targets before they can attempt vandalism or theft.

a) Intrusion detection sensors may include vibration, motion, pressure or any combination of these to detect intrusion or tampering. These sensors shall provide continuous data to either an on-site device with storage capabilities that are connected to the Transnet network or the sensor itself shall be connected to the network to provide feedback to the Transnet Nerve Centre.
b) Intrusion detection sensors may be mounted to a wall to detect break-in or underneath a floor, depending on the metric that the sensor measures. In any case, the sensor shall not be exposed but hidden from the detection from a target's point of view. Tamper detection for buildings shall be placed inside buildings. Pressure plates shall be hidden beyond sight underneath a surface. A Transnet employee or representative shall confirm whether the state of proposed installation fits this specification.
c) Intrusion detection sensors may be wireless or wired. Wireless communication with a central hub or relay shall be immune to interference and interruption and not contend with other types of technology using the same communication media. For example, if the sensor communicates via a radio signal to a central hub in a nearby building, it shall not disrupt the radio communication of remote control switches in the perimeter.
d) Intrusion detection sensors shall be coupled to an appropriate electric system and back-up power or batteries to ensure vital protection. For sensors placed outside a building or structure and provides wireless communication, sensors shall be coupled with a standalone battery to ensure optimal functioning at all times.

e) Intrusion detection or tamper sensors placed outside a structure shall be rigged and able to operate in all South African weather conditions including rain and wind etc. and shall, therefore, be IP66 rated.
f) Intrusion detection and tamper sensors shall be dependable and able to continuously provide data with a capacity to only undergo maintenance once a year or less.

7.11 Failsafe Telecommunication Connectivity

A redundancy is required.

a) All wireless communications shall be ICASA approved.
b) The device shall have a minimum of 2 Meg link capacity to transmit the video footage back to the nerve centre. The video footage shall be able to be streamed back to the nerve centre with a video resolution of at least 720pixels.
c) All mounting equipment shall be supplied and installed by the contractor.
d) The device shall be capable of operating in environmental temperatures as specified in Transnet Freight Rail environment specification under applicable document section.
e) The device shall support Ethernet connectivity.
f) The device shall be able to be mounted in the indoor cabinet as mentioned in section 7.9.1. All connectors and mounting equipment shall be supplied and installed by the contractor.
g) The device shall be able to be powered via a normal 230 VAC power source, and the power supply shall be included in the installation.
h) The duration of the network contract will be site specific and shall be approved and agreed to by Transnet Freight Rail. Transnet ICT and Transnet Freight Rail shall be consulted on the contractual agreements.
i) A ring topology should be used, this shall assist with redundancy.

7.12 Information and Communication Technology

7.12.1 Remote Control Monitoring

All surveillance equipment (including cameras, sensors, radar etc.) shall be connected to the TFR WAN and provide an active control and alarm communication to the main Transnet Security Nerve Centre. An active security system shall detect intrusions as accurately as possible and notify the relevant Transnet security authorities. All monitoring and control features of the associated surveillance systems shall be managed by appropriate Transnet security officers (henceforth referred to as the ‘operator’) at the Nerve Centre.

All surveillance equipment and systems shall adhere to the following specifications:

a) Alarm notifications and events generated by surveillance equipment in the event of a possible security risk shall be monitored at the Nerve Centre.
b) The status of batteries or powering systems of each site shall be displayed to ensure all surveillance systems are up and running and continuous protection is available.
c) The operator shall have the system rights to arm and disarm an intrusion system and the status of each sub-system shall be displayed on the GUI of the software detection system remotely.

d) The GUI shall be developed such that it is compatible with Microsoft Windows (this includes Windows 7 and newer versions) and is compatible with both 32 bit and 64 bit processors.
e) The GUI shall implement Active Directory (AD) authentication protocols to access the platform and monitor/adjust the data and devices.
f) The user interface shall enable employees employed in the relevant control centres to remotely operate access control systems based on the business need as specified by Transnet.
g) Either upon request by the operator from the control software or via an alarm event, a live media feed shall be streamed to the Nerve Centre. Such a media feed shall include video, audio, thermal imaging or any appropriate media that the surveillance equipment can produce and record.
h) Previously recorded media from the NVR, CCTV system or campus area network shall be accessible to an operator with the proper permissions, to review media. Surveillance equipment shall record media for a minimum of 24 hours locally and be stored on associated servers on the network for a minimum period of one month.
i) All equipment installed shall be identified and stored in the system database by their unique ID and Global Position System (GPS) coordinates.
j) The operator shall be able to send a system generated SMS to the armed response team. The SMS shall contain GPS coordinates of the triggered equipment.
k) The operator shall be able to access the event log of any piece of surveillance equipment for a period of 3 months. The sensitivity settings of filtering of false events as defined by the smart features of specific surveillance equipment shall be remotely adjustable by the operator.
l) All software features including Machine Learning (ML), Artificial Intelligence (AI) or other 'smart' video analytic features shall be viewable and accessible to an operator at the Nerve Centre.
m) All surveillance equipment shall be fully integrated with the Nerve Centre. Associated Application Programming Interfaces (API) or equipment protocols or commands shall be provided for full integration with the Nerve Centre.
n) In the case of any supplier wanting to protect the intellectual property of their unique software features and not fully integrate but provide third party access, a formal agreement between the supplier and Transnet SOC Ltd shall be drawn up to negotiate the terms of partnership. Remote access to any surveillance system by the supplier is prohibited unless expressly and formally granted by Transnet.
o) All administrator rights of and software access to the surveillance equipment will be supplied to the operator with appropriate security clearance and the supplier will not retain the right to edit or update any software or settings of the surveillance equipment without the explicit consent of Transnet.
p) Remote control of the physical capabilities of the surveillance equipment, such as optical or digital zoom and rotation, will be executed by the operator.
q) Remote control of the digital imaging or processing of media, such as the adjusting of wide dynamic range and object and face recognition, will be executed by the operator.
r) All attributes and characteristics of the surveillance equipment and systems will be logged and stored at the Nerve Centre.
s) Where the surveillance equipment is able, the operator shall retain the right and control to stream audio to the surveillance equipment, to warn a potential security threat, or remotely trigger an alarm siren.

t) The contractor shall be responsible for maintenance and updates of the software and/or API.
u) Confidentiality agreements shall be signed by the contractor to keep the data safe and secured. Only authorised personnel may view and download it.
v) Data transmitted to the platform shall employ the relevant Advanced Encryption Standards (AES) in all encryption and decryption techniques to prohibit signal hacking, eavesdropping and the loss of data integrity.
w) The security protocols shall be implemented such that it complies with SANS 15816:2006. All data shall be encrypted and treated as confidential.
x) The supplier shall give permission for some of their systems to run on Transnet Servers.

7.12.2 User Interface Licences, Training and Handover

An operational licence, user assistance and training for the software in section 7.8 should be provided to Transnet Freight Rail personnel. Transnet will determine how many people requires the license and training.

7.12.3 Remote Monitoring and Servers

This section will describe the requirements for the servers and storage for the remote control monitoring as mentioned in section 7.8.

a) The requirements for the servers and data storage for the remote monitoring and control shall be discussed with Transnet ICT.
b) Transnet ICT may provide the servers and storage where possible, the contractor will then have to integrate their solution with the allocated system.
c) If Transnet ICT cannot provide the servers and storage then the contractor shall offer a server/storage system. Transnet will have the right to decline or accept the offer.
d) The server system shall be able to offer the requirements as set out in section 7.8.

7.12.4 Transnet Freight Rail Intranet Domain

a) The system application shall be configured to connect to the Transnet Freight Rail Intranet domain.
b) The administrator of the system shall log on using his SAP number ID and domain password.
c) The system application shall call Windows Active Directory and pass on the SAP ID and password.
d) The system application shall use the Fully Qualified Domain Name **(**FQDN) to connect to the Active Directory with the SAP ID and password as parameters where after the Active Directory shall confirm if the logon parameters are correct.
e) The system application has to be tested on the Transnet Freight Rail Intranet because each Active Directory has its own FQDN.

7.13 Power Requirements

The following section discusses the requirement of the variations of 230 VAC power supply options.

7.13.1 Indoor Power Requirements

The following section describes the power requirements needed to supply power to the indoor network campus system, CCTV cameras, electric fence energizers and intrusion detection system while using Transnet power outlets or distribution boards on site.

a) Standard 230 VAC, 50 Hz power connections will be used.
b) Power cable with adequate thickness for the given scenario needs to be supplied and installed for networking requirements.
c) Power cable sizing calculations shall be done and provided, showing that the selection of cable is adequate.
d) All mounting equipment and connectors shall be supplied and installed.

7.13.2 Outdoor Power Requirements

7.13.2.1 Outdoor AC Power

The following section describes the power requirements needed to supply power to the outdoor network campus, CCTV system, electric fence energizers and intrusion detection system while using Transnet power outlets, distribution boards or kiosk substations on site.

a) Standard 230 VAC, 50 Hz power connections will be used.
b) Power cable with adequate thickness for the given scenario needs to be supplied and installed for networking requirements.
c) Power cable sizing calculations shall be done and provided, showing that the selection of cable is adequate.
d) All mounting equipment and connectors shall be supplied and installed.
e) The power cable shall be suitable for outdoor use.

7.13.2.2 Solar Panels

This section specified the solar power requirements for a network campus or network campus networks. The solar panels, solar equipment and network campus requirements will be mounted on concrete pole structures as per SANS 470:2012 specification. The solar power system shall be electrically protected according to the latest version of Transnet's Specification for Outdoor LV Installations for Telecommunication Networks as defined in BBB 3235 and SANS 10198. This means of power will be used where and if required by Transnet.

Transnet may also request that the solar panel system be used to power the security equipment and sensors installed in a certain building such as a substation, relay room or telecommunications building. Where this solar power system is used and installed is purely Transnet's discretion.

7.13.2.3 Panels

7.13.2.3.1 Type A

a) 330 W polycrystalline panels.

b) Shall have an ingress protocol rating of at least 65.
c) One solar panel shall have a maximum dimension not more than 2000 length x 1000 width x 45 height mm with a 10% tolerance on each dimension of length, width, and height.

7.13.2.3.2 Type B

a) 150 W polycrystalline panels.
b) Shall have an ingress protocol rating of at least 65.
c) One solar panel should have a maximum dimension no more than 1600 length x 800 width x 45 height mm with a 10% tolerance on each dimension of length, width, and height.

7.13.2.4 Battery

A battery intended to serve as an energy storage system for a UPS complying with this standard shall comply with the IEC 62040-1 requirements for location, ventilation, marking and protection of a battery.

7.13.2.4.1 Type A

a) 200 AH gel deep cycle battery with nominal12 V output.
b) A combination of 2 x 100 AH 12 V gel batteries may be used in parallel.
c) The battery setup shall be capable of fitting in the Type A outdoor 19” cabinet as specified in section 7.9.2 with all the other systems also installed.
d) The battery shall be capable of operating in an outdoor cabinet with no airflow.

7.13.2.4.2 Type B

a) 100 AH gel deep cycle battery with nominal 12 V output.
b) The battery setup shall be capable of fitting in the Type A outdoor 19” cabinet as specified in section 7.9.2 with all the other systems also installed.
c) The battery shall be capable of operating in an outdoor cabinet with no airflow.

7.13.2.4.3 Type C

a) 50 AH gel deep cycle battery with nominal 12 V output.
b) The battery setup shall be capable of fitting in the Type A outdoor 19” cabinet as specified in section 7.9.2 with all the other systems also installed.
c) The battery shall be capable of operating in an outdoor cabinet with no airflow.

7.13.2.5 Inverter

7.13.2.5.1 Type A

a) A pure sine wave inverter capable of supplying continuous power of 300 W.
b) The inverter shall have an efficiency of at least 85%.
c) The output voltage shall be nominally 230 VAC, 50 Hz.
d) The inverter shall be passively cooled. However, where necessary Transnet may request actively cooled inverters to mitigate damage to the different components due to environmental conditions.
e) The inverter shall be capable of operating in an outdoor cabinet with no airflow.

7.13.2.5.2 Type B

a) A pure sine wave inverter capable of supplying continuous power of 200 W.
b) The inverter shall have an efficiency of at least 85%.
c) The output voltage shall be nominally 230 VAC, 50 Hz.
d) The inverter shall be capable of operating in an outdoor cabinet with no airflow.

7.13.2.5.3 Type C

a) A pure sine wave inverter capable of supplying continuous power of 100 W.
b) The inverter shall have an efficiency of at least 85%.
c) The output voltage shall be nominally 230 VAC, 50 Hz.
d) The inverter shall be capable of operating in an outdoor cabinet with no airflow.

7.13.2.6 Charge controller

a) A Maximum Power Point Tracking (MPPT) charge controller shall be used for battery charging.
b) The controller shall be able to integrate with the selection of solar panels and the batteries.
c) The controller shall be capable of operating in an outdoor cabinet with no airflow.
d) The charge controller shall be adequate for the operational requirements of Transnet as detailed.

7.13.2.7 Integration and Accessories

a) All the solar panel components shall be integrated with each other.
b) All solar panel equipment (except the solar panel) shall be able to fit in the Type A and Type B outdoor network cabinets as described in section 7.9.2., together with network cabinet requirements such as a media converter switch (section 7.6.2) and fibre patch panels (section 7.6.5). The components within the cabinet shall operate in this outdoor network cabinet without any performance loss.
c) Necessary mounting equipment and connectors shall be supplied to perform installation of the solar panel system.
d) The solar power system shall be installed and tested by the contractor. In addition, test reports shall be submitted by the contractor to validate that the system operation complies with the technical requirements defined in this specification.
e) The system shall be earthed and electrically protected according to the latest version of Transnet's Specification for Outdoor LV Installations for Telecommunication Networks. This is outlined in BBB 3235.
f) Systems shall be earthed as per SANS 10198.
g) All cabling and connectors necessary to integrate and install final system shall be supplied and installed by the contractor.

7.14 Backup Power System and Batteries

The purpose of this paragraph is to define the requirements to install a power system to be used to supply power and backup power to the CCTV/ NVR system, campus network system, intrusion detection system and the wireless links. This system shall be in the form of a UPS with batteries.

7.14.1 System Operation Description

The UPS shall provide high quality AC power for electronic equipment loads and shall offer the following features in line with SANS 62040:

I. R.M.S. voltage variation ± 10 % of rated voltage (230 Vac)
II. Frequency variation ± 2 % of rated frequency (50 Hz)
III. Total Harmonic Distortion (THD) of voltage ≤ 8 %
IV. Power blackout protection.
V. Output overvoltage protection

7.14.2 Operating Procedure

7.14.2.1 Normal Mode

The backup power system shall be configured such that in the normal mode the critical load is continuously supplied by the UPS. The rectifier shall convert the AC source into DC power while the battery charger maintains the battery in a fully charged operational condition. The inverter shall convert the DC power into clean and related AC power, which is supplied to the critical load through a static switch.

7.14.2.2 Overload

In the event of an inverter overload, manual stop or failure, the static switch shall automatically transfer the critical load to bypass without interruption. The transfer time shall be not more than 500 microseconds.

7.14.2.3 Emergency Conditions

If the AC main supply fails or reduces to a value outside the limits of the input voltage to the UPS, the critical load shall be supplied without any switching, by the inverter drawing its power from the Battery supply. There shall be no interruption to the critical load upon failure, reduction or restoration of the AC main supply.

7.14.2.4 Monitoring

The UPS shall have the capability to be monitored from a remote location through wireless data transmission to a GUI. The GUI shall comply with the requirements as outlined in 7.12. Even during a complete Shutdown of the UPS the information relating to the operating parameters shall not be lost. Indications measurements and alarms, together with power indications and battery status shall be available on both the GUI and the physical unit.

7.14.3 Mechanical Requirements

a) The UPS shall be housed in a freestanding modular enclosure with removable panels and a protection rating of IP20 as standard. The enclosure shall be designed for industrial room applications in accordance with operational conditions listed in section 7.9 where required by Transnet, the UPS and battery pack shall be fitted into the enclosure as stated in section 7.9, all connectors and adaptors shall be supplied and installed by the contractor.
b) Where needed, active cooling shall be provided to ensure that all components are operated within specification with air entry in the base and exit at the top.

7.14.4 UPS and Battery Requirements

The following section discusses the requirement of the variations of uninterruptible power supplies that are required. The load that will be placed on the UPS and battery system will be site specific, but may include the CCTV system, communication system and intrusion detection system for that specific site.

7.14.4.1 General Requirements

The following are general requirements that shall be applicable to all indoor UPS systems.

a) Internal battery bank that shall support full load of UPS for 8 hours minimum if the particular site does not have a backup generator. If a backup generator is present, the battery bank shall supply 15 minutes of backup power.
b) If the internal battery bank of the UPS cannot supply the 8-hour requirement, additional batteries shall be supplied and installed by the contractor. This shall first be discussed with the Transnet electrical department and installed upon approval by the relevant department heads.
c) The UPS and battery system (internal or external) shall be able to fit in a standard 19” network cabinet. This system shall be able to fit in the enclosure as discussed in 7.9.
d) UPS interfacing with either one of the following: RJ-45 10/100 Base-T, USB or RS-232.
e) Power interface of 230 VAC, 50 Hz

7.14.4.1.1 Type A

a) 1 KVA online uninterruptible power supply

7.14.4.1.2 Type B

a) 2 KVA online uninterruptible power supply

7.14.4.1.3 Type C

a) 3 KVA online uninterruptible power supply

7.15 Access Control

7.15.1.1 General Requirements

Remote locking is an essential requirement to secure and facilitate the protection of Transnet Freight Rail’s assets, thus each lock shall be developed such that it enables remote triggering through a digital key. The contractor shall provide and install locks that adhere to the following general requirements for access control systems.

a) Upon the unlocking of an asset, employee validation shall be done through the request of employee credentials and the validation thereof through a secure and linked database. Validation shall be done through engagement with a control centre or through any other secure digital medium.
b) A successful validation shall unlock the relevant asset and log the details of the individual who accessed the asset, the time, the date and credentials of the individual who authorized the unlocking event.

c) The system shall ensure that an invalid digital key cannot grant access to a controlled area.
d) The developed system shall store these details in the database of the system which can be accessed only by the administrator or relevant personnel in the control centre or Transnet ICT employees as per section 7.12. The system shall generate automated reports periodically being either daily, weekly, monthly, yearly or upon request based on the timeframe requirements.
e) The system shall be usable with low physical and cognitive effort by a widespread population and shall cater to individuals who are physically incapacitated.
f) The system shall be developed such that unique digital keys are implemented in order to accurately distinguish individual characteristics. The implemented system shall also be robust such that weather or any adverse environmental conditions do not affect the operation of the locking system.. This addresses the operation of Bluetooth or any other digital medium for asset unlocking.
g) Only the lock status shall be visible on the lock. No other monitoring signals or indicators such as signal strength, battery life, etc. shall be visible on the lock.
h) All machined parts of a lock shall have a smooth finish and shall be free from ragged edges and tool marks. Where welds are exposed on the outside of the relay rooms, substations and other site locks, they shall be flush with the parent metal to give an acceptable finish.
i) When not made of a metal that is inherently corrosion resistant, the door and its locks and bolt work shall be so protected as to resist the corrosive influence to which they are subjected in normal service.
j) The dimensions of the locking device will be limited to the infrastructure assets doors or gates.
k) The locking system shall be resistant to signal jamming and magnetic tampering.
l) Fixed wiring for access control systems shall comply with the provisions of SANS 10142-1.

7.15.1.2 Technical Requirements

To lock a digital keyless lock means to use a device or mechanism for securing the railway infrastructure doors or gate in a closed position. In contrast, an unlocking event can be defined as the contrast of operating a device or mechanism to access a specific railway asset. The locking solution for access control shall comply with following requirements.

a) The system should be able to collect the characteristics easily from the subjects and the characteristics should be sufficiently distinct and repeatable to achieve successful recognition of the subject as per SANS 24745:2013.
b) The system shall be spoof resistant, which indicates the difficulty to which it is able to replicate the individual digital key characteristics, being either biometric, password or control centre based to circumvent the locking system.
c) The weight of the lock shall not exceed 25 kg.
d) The system shall be able to frequently update the stored profile for each individual and build an employee profile to ensure that false or unauthorized access is mitigated.
e) The operational time limits for the digital key validation shall comply with the time requirements set as per SANS 2220.
f) The lock shall be designed such that the locking status can be viewed remotely by a monitoring centre.
g) The Mean Time Between Failures (MTBF) of the digital key readers assessed in accordance with IEC 60050-191 and IEC 60300 under normal operating conditions shall be at least 8 000 h.

h) The false rejection rate during any 50 000 presentations of the digital key shall not exceed 0.5%.
i) The access control system shall operate through a wireless, keyless system.
j) The digital key shall be configured such that data exchanged during an electronic commerce transaction remains unchanged and cannot be interfered with by any third party. This is to prevent eavesdropping or unauthorized asset access,
k) The lock used for access control shall be securely mounted such that it does not detach or fall off from the railway asset door or gate during operation.
l) Relevant notifications should be sent from the lock to a mobile and computer application to indicate the lock status.
m) One lock shall have a service life of at least 5 years under normal operating conditions of two locking and unlocking events per day. Technical reports from an accredited SANS facility shall be provided as evidence for product service life.
n) The power unit of an access control system shall comply with the requirements of SANS 2220-1-7.
o) The barrier materials used to manufacture the lock shall meet the following mechanical properties:
    I. Hardness, Brinell: 230
    II. Shear modulus: minimum of 70 GPa
    III. Tensile strength: minimum of 350 MPa
    IV. Yield strength: minimum of 400 MPa

8 Guidelines and Procedures

All other specifications listed throughout in this document shall also be adhered to.

Depending on the site of installation, additional Transnet specifications might need to be adhered to when performing installation, configuration and testing.
The following list provides the guidelines and procedures that may need to be followed and adhered to depending on the specific site. (The latest versions of these specifications/ procedures needs to be used).

All equipment and installations shall adhere to the latest SANS standards. Some of the required SANS standards are listed in this document. It shall be noted that the applicable SANS standards are not only limited to the listed ones in this section, it is merely a guideline.

Transnet will determine at which sites the Transnet procedures in this list shall be adhered to.

- SPC-00029: Trenching, Laying and Hauling in of Communication Cables (Section: “Hauling Cable in Pipe and Chamber Systems”)
- SPC-00588: Installation and Laying of Main and Sub Cable Conduit for the Protection of Underground Telecommunication Cables.
- SPC-00589: Civil Engineering Works associated with Underground Telecom Plant
- E7/1: Works on, over, under or adjacent to railway lines and near high voltage equipment. (BBD8210)
- E.4E: Compliance with the Occupational Health and Safety Act (Act 85 of 1993)
- BBF3690 – Electrical Safety Instructions
- BBB3235 – Installation of earthing and lightning protection of electronic measurement equipment housings

- EN 50173:
    - Defines the structure and configuration of the backbone cabling subsystems of generic cabling systems within the types of premises.
    - EN 50173 – 1: Information technology
        - Generic cabling systems Part 1: General requirements
    - EN 50173-2: Information technology
        - Generic cabling systems Part 2: Office premises
    - EN 50173-3: Information technology
        - Generic cabling systems Part 3: Industrial premises
- EN 50174:
    - Defines installation requirements of the backbone cabling subsystems of generic cabling systems within the types premises
    - EN 50174-1: Information technology
        - Cabling installation Part 1: Installation specification and quality assurance
    - EN 50174-2 Information technology
        - Cabling installation Part 2: Installation planning and practices inside buildings:
    - EN 50174-3: Information technology
        - Cabling installation Part 3: Installation planning and practices outside buildings
- EN 50310:
    - Application of Equipotential Bonding and Earthing in Buildings with Information Technology Equipment.
- EN 50346:
    - Information technology - Generic cabling systems - Testing of installed cabling
- Compliance to ISO/IEC 11801
- Compliance to TIA 568
- Compliance to all regulations as set out by ICASA.

- SANS 10142-1: The wiring of premises Part 1: Low-Voltage installations
- SANS 10198: The selection, handling and installation of electric power cables of rating not exceeding 33 kV
- SANS 24745:2013 Information technology — Security techniques
- SANS 2220: Electrical security systems
- SANS 470:2012 Concrete poles for telephone, power and lighting purposes
- SANS 60529: Degrees of protection provided by enclosures (IP Codes).
- SANS 62040: Uninterruptible power systems (UPS).
- SANS 10313: Protection against lightning- Physical damage to structures and life Hazard.
- SANS 10108: The classification of hazardous locations and the selection of equipment for use in such locations
- SANS 10140-2: Identification colour marking Part 2: Identification of hazards and equipment in work situations
- SANS 1574-3: Electric flexible cables with solid extruded dielectric insulation Part 3: PVC insulated cables for industrial use.
- SANS 1507-3:2015 Electric cables with extruded solid dielectric insulation for fixed installations (300/500 V to 1 900/3 300 V) Part 3: PVC Distribution cables
- IEC 60050-191, International electrotechnical vocabulary – Chapter 191: Dependability and quality of service.
- IEC 60300 (all relevant parts), Dependability management.

- IEC 62040-1, Uninterruptible power systems (UPS) –Part 1-1: General and safety requirements for UPS used in operator access areas

8.1 Additional Installation Requirements

Additional installation requirements:

a) A Transnet Freight Rail telecoms and electrical technician shall at all-time be present during the installation of the system.
b) Transnet, technology Management, ICT, Electrical and Telecoms engineers form the Central Office of Transnet Freight Rail shall approve the designs, network architecture and installations proposed by the contractor.
c) Transnet Safety Specialists shall approve the designs and installations proposed by the contractor.
d) The contractor shall ensure that the installations do not violate any Railway Safety Regulator (RSR) regulations or rules.
e) The contractor shall supply compliance certificates for all installations and it shall be delivered for approval by the Transnet Freight Rail Quality Assurance department.
f) All wireless communications shall comply with ICASA regulations.
g) All installations and operations shall comply with the Occupational Health and Safety Act (Act 85 of 1993) guidelines and regulations.

9 Evaluation and Performance Testing

Acceptance tests on site shall be conducted. The system shall be tested on site; these tests shall be satisfactory to Transnet's requirements.

a) Final word of verification of correctly installed equipment and correctly selected equipment described in this document will be given by the TFR Quality Assurance team.
b) The TFR engineering department will receive all performance and operation results and conduct the acceptance tests.

Appendix A: CCTV camera performance requirements

1 HD SRVL CAMERA 3.0MP, H.264, DAY-NIGHT, IN DOOR IP DOME

a) This camera shall meet or exceed the following design and performance specifications.
General:

- Image Sensor: 1/2.0” progressive scan CMOS
- Active Pixels: 3.0MP = 2048 (H) x 1536 (V)
- Imaging Area: 6.6 mm (H) x 4.9 mm (V),
- Minimum Illumination: In colour and in monochrome mode 0.2 lux (F1.4) 0.02 lux F1.4
- Dynamic Range: 61 dB
- Lens: Best lens for a 3.0 MP camera, auto irise, remote focus and zoom
- Angle of View: 35° - 88°
- Image Compression: H.264 (MPEG-4 Part 10/AVC), Motion JPEG, JPEG2000
- Image Rate: 12 @ full resolution; 39 @ 1280 x 720
- Resolution Scaling: Down to 640 x 480
- Motion Detection Selectable sensitivity and threshold
- Electronic Shutter: Automatic, Manual (2 to 1/30,000 sec)
- Iris Control: Automatic, Manual
- Day/Night Control: Automatic, Manual
- Flicker Control: 50 Hz, 60 Hz
- White Balance: Automatic, Manual
- Privacy Zones: Up to 4 zones
- Audio Input Line input, A/V mini-jack (3.5 mm)
- Audio Compr. Method: G.711 PCM 8kHz
- Video Output NTSC/PAL, A/V mini-jack (3.5 mm)
- I/O Terminals: Alarm In, Alarm Out; terminal strip
- Backlight compensation: Automatic

Electrical:

- Power Source: PoE: IEEE 802.3af Class 3 compliant 24 VAC, 12 VDC
- Power Consumption: 5 W maximum
- Power Connector: 2 pin terminal block

Network:

- Network: 100BASE-TX
- Cabling: CAT6
- Connector: RJ-45
- API: ONVIF (AND/OR PSIA IF APPLICABLE) compliant (www.ONVIF.org)
- Security: Password protection, HTTPS encryption, digest authentication, WS authentication, user access log.
- Protocols: IPv4, HTTP, HTTPS, SOAP, DNS, NTP, RTSP, RTCP, RTP, TCP, UDP, IGMP, ICMP, DHCP, Zeroconf, ARP
- Streaming Protocols: RTP/UDP, RTP/UDP multicast, RTP/RTSP/TCP, RTP/RTSP/HTTP/TCP, RTP/RTSP/HTTPS/TCP, HTTP

Physical and environmental:

- Dome Bubble: Polycarbonate, clear
- Body: Plastic
- Housing: Recessed mount, tamper resistant
- Finish: Plastic, RAL 9003
- Adjustment Range: 360° pan, 180° tilt, 360° azimuth
- Operating Temp: -10°C to +50°C (14°F to 122°F)
- Storage Temp: -10°C to +70°C (14°F to 158°F)
- Humidity: 20 - 80%, relative humidity (non-condensing)

Certification and regulations:

- FCC, Class B

- CE, Class B
- UL/cUL Listed

2) HD SRVL CAMERA: 3.0 MP, H.264, D-NIGHT, IP, OUTDOOR BULLET

a) This camera shall meet or exceed the following design and performance specifications.

- Image Sensor: 1/2.0" progressive scan CMOS
- Active Pixels: 3.0MP = 2048 (H) x 1536 (V)
- Imaging Area: 6.6 mm (H) x 4.9 mm (V)
- Minimum Illumination: In colour and in monochrome mode 0.2 lux (F1.4) 0.02 lux F1.4
- Dynamic Range: 61 dB
- Lens: Build-in 3.0 MPF1.4, auto irises, remote focus and zoom
- Angle of View: 35° - 88°
- Image Compression: H.264 (MPEG-4 Part 10/AVC), Motion JPEG2000
- Image Rate: 12 @ full resolution; 39 @ 1280 x 720 or smaller
- Resolution Scaling: Down to 640 x 480
- IR illumination 150mm maximum distance at 0 lux
- Motion Detection: Selectable sensitivity and threshold
- Electronic Shutter: Automatic, Manual (2 to 1/30,000 sec)
- Iris Control: Automatic, Manual
- Day/Night Control: Automatic, Manual
- Flicker Control: 50 Hz, 60 Hz
- White Balance: Automatic, Manual
- Privacy Zones: Up to 3 zones
- Audio Input Line input, A/V mini-jack (3.5 mm)
- Audio Compr. Method: G.711 PCM 8kHz
- Video Output NTSC/PAL, A/V mini-jack (3.5 mm)
- Serial comms: RS-485; Terminal strip
- Backlight compensation: Automatic
- I/O Terminals: Alarm In, Alarm Out; terminal strip

Electrical:

- Power Source: PoE: IEEE 802.3af Class 3 compliant 24 VAC, 12 VDC
- Power Consumption: 9 W maximum
- Power Connector: 2 pin terminal block

Network:

- Network: 100BASE-TX
- Cabling: CAT6
- Connector: RJ-45
- API: ONVIF (AND/OR PSIA IF APPLICABLE) compliant (www.ONVIF.org)
- Security: Password protection, HTTPS encryption, digest authentication, WS authentication, user access log.
- Protocols: IPv4, HTTP, HTTPS, SOAP, DNS, NTP, RTSP, RTCP, RTP, TCP, UDP, IGMP, ICMP, DHCP, Zeroconf, ARP
- Streaming Protocols: RTP/UDP, RTP/UDP multicast, RTP/RTSP/TCP, RTP/RTSP/HTTP/TCP, RTP/RTSP/HTTPS/TCP, HTTP

Physical and environmental:

- Dome Bubble: Polycarbonate, clear
- Body: Aluminum
- Housing: Outdoor = Surface mount, vandal resistant Pendant = Treaded screw interface for Pendant hardware
- Finish: Powder coat, cool gray 2
- Adjustment Range: 360° pan, 180° tilt, 360° azimuth
- Operating Temp: -30°C to +50°C (-22°F to 122°F)
- Storage Temp: -10°C to +70°C (14°F to 158°F)
- Humidity: 20 - 80%, relative humidity (non-condensing)

Certification and regulations:

- FCC, Class B

- CE, Class B
- UL/cUL Listed
- Meets IP66 standards

3) HD PTZ CAMERA

3.1 The High Definition PTZ camera must have a built in IR illumination range to ensure that the cameras provides exceptional images in a wide range of applications and environments.

3.2 The PTZ camera housing must be IP65 rated to withstand a wide range of weather and outdoor surveillance applications.

3.3 The PTZ camera must have Pan-Tilt-Zoom capabilities for operators to easily detect and follow a moving object with high level precision and control.

3.4 The PTZ camera shall have the self-learning video analytics at the home position.

3.5 The PTZ camera shall have suitable accessories for mounting on existing structures, corner mount, and poles.

3.6 This camera shall meet or exceed the following design and performance specifications.

General:

- Image Sensor: WDR 1/2.8" progressive scan CMOS
- Resolution: 1280 (H) x 720 (V) = 1.0MP
  1920 (H) x 1080 (V)
- Imaging area: 4.8 mm (H) x 2.7 mm (V); 0.189" (H) x 0.106" (V)
- IR Illumination: 250 m maximum distance at 0 lux
- Minimum illumination: 0 lux in IR mode; 0.1 lux (F/1.6) in colour mode (no IR); 0.03 lux (F/1.6) in monochrome mode (no IR)
- Aspect Ratio: down to (16:9) 384x216 or (5:4) 320x256
- Dynamic Range: 120+ Db
- Lens: 4.3 to 129 mm, F/1.6 – F/4.7, autofocus 2.0MP
- Angle view: 2.3° - 63.7°2.0MP
- Optical Zoom: 30x 2.0MP
- Video Compression: H264 (MPEG-4 Part 10/AVC), Motion JPEG, HDSM SmartCodec
  technology
- Image Rate: Up to 60 fps

- Motion Detection Selectable sensitivity and threshold
- Electronic Shutter: Automatic, Manual (1/1 to 1/10,000 sec)
- Iris Control: Automatic, Manual
- Day/Night Control: Automatic, Manual
- Streaming: Multi-stream H.264 and Motion JPEG
- Flicker Control: 50 Hz, 60 Hz
- White Balance: Automatic, Manual
- Backlight Compensation: Manual
- Privacy zones: Up to 64 zones, 3D privacy mask supported
- Presets: 500 named presets
- Tours: 10 named guard tours
- Audio Compression Method: G.711 PCM 8 kHz
- Electronic Image Stabilization:On/Of
- Digital Defog: Adjustable/Of

Electrical:

- Power Source: 24 VDC ± 10%; 24 VAC rms ± 10%, 50 or 60Hz
- Power Consumption: 75 W max with 24 VDC aux power, 71W max with 95W PoE,
- POE: 105 VA with 24 V AC RMS aux power
  95W PoE: POE-INJ2-95W
  60W PoE: POE-INJ2-60W
- Power Connector: Red and Black wires
- RTC Backup Battery: 3V manganese lithium

Network:

- Network: 100Base-TX
- Cabling: CAT6
- Connector: RJ-45
- API: ONVIF Profile S Compliant
- Device Management protocol: SNMP v2c, SNMP v3

- Security: Password protection, HTTPS encryption, digest Authentication, WS authentication, user access log, 802.1x port based authentication
- Protocols: IPv6, IPv4, HTTP, HTTPS, SOAP, DNS, NTP, RTSP, RTCP, RTP, TCP,UDP, IGMP, ICMP, DHCP, Zeroconf, ARP, LLDP

Environmental:

- Operating Temp: -40 °C to +60 °C (-40 °F to 140 °F) with external power or 95 W PoE-10 °C to +50 °C (14 °F to 122 °F) with 60W PoE Wiper is functional at 1 °C to +60 °C (34 °F to 140 °F)
- Storage Temp: -10°C to +70°C (14°F to 158°F)
- Humidity: 0 - 95% non-condensing

Mechanical:

- Housing: Pendant Mount
- Body: Aluminium
- Tilt: -20° to 90°, Auto-Flip, 300°/second max
- Pan: 360°, endless, 300°/second
- Front window: Optical glass

Video analytics:

- Objects in area: The event is triggered when the selected object type moves into the region of interest
- Object loitering: The event is triggered when the selected object type stays within the region of interest for an extended amount of time.
- Objects crossing beam: The event is triggered when the specified number of objects have crossed the directional beam that is configured over the camera's field of view. The beam can be unidirectional or bidirectional.
- Objects appears: The event is triggered by each object that enters the region of interest. This event can be used to count objects
- Object not present in area: The event is triggered when no objects are present in the

region of interest.

- Objects enters area: The event is triggered when the specified number of objects have entered the region of interest.
- Object leave area: The event is triggered when the specified number of objects have left the region of interest.
- Object stops in area: The event is triggered when an object in a region of interest stops moving for the specified threshold time.
- Direction violated: The event is triggered when an object moves in the prohibited direction of travel.
- Temper detection: The event is triggered when the scene unexpectedly changes.

Certification and regulations:

- Certifications/Directives: UL, cUL, CE, ROHS, WEEE, RCMCE, Class A
- Safety: UL 62368-1, CSA 62368-1, IEC/EN 62368--1
- Electromagnetic immunity: EN 55024, EN 61000-6-1
- Environmental: IK10 Impact Rating, IEC 60529 IP66 Rating, UL/CSA/IEC 60950-

END OF SPECIFICATION