Transnet National Ports Authority

PA & Security System Technical Specification

Engineering Design Services: Control & Instrumentation

1127672-B01-SP-0002

Prepared By:	Tebogo Mahlalela Engineer	2021-05-05 Date
Reviewed & Approved By:	Lonwabo Mgushelo Engineer	2021-05-07 Date
Approved By:	Thokozani Mhlongo Engineering Manager	10 May 2021 Date
Accepted By:	Siyabonga Gadu Project Manager	13 May 2021 Date
Accepted by:	Sicelo Tiyo Security Manager	13/5/2021 Date
Accepted by:	Sandisiwe Mtintsilana BUR	2021/05/14 Date

01	March 2021	Revised to Include Intruder Detection System and PSIM
00	December 2019	Issued for Client Acceptance
Rev No.	Date	Revision Details

Contents

1 Acronyms and Abbreviations

The acronyms and abbreviations applicable to this report are summarised in the following table:

Abbreviation	Description
BMS	Building Management System
FoV	Field of View
FOIDS	Fibre Optic Cable Intruder Detection System
NIC	Network Interface Card
OEM	Original Equipment Manufacture
OLE	Object Linking and Embedding
OLT	Operations/Operational Leadership Team
OTDR	Optical Time-Domain Reflectometer
PA	Public Announcement/Address
P&ID	Process/Piping and Instrumentation Diagram
PAS	Public Announcement/Address System
PC	Personal Computer
PDU	Power Distribution Unit
PIDS	Perimeter Intruder Detection System
PE	Port Elizabeth
PoE	Power over Ethernet
POI	Point of Interest
PON	Port of Ngqura
PSIM	Physical Security Information Management
PTZ	Pan, Tilt and Zoom
PVC	Polyvinyl Chloride
RWS	Remote Work Station
S&A	Systems and Automation

Abbreviation	Description
SAT	Site Acceptance Test
SI	International System of Units
SPL	Sound Pressure Level
STP	Shielded Twisted Pair
SWA	Steel Wire Armoured
TCP/IP	Transmission Control Protocol/ Internet Protocol
TGC	Transnet Group Capital
TIA	Telecommunications Industry Association
TNPA	Transnet National Port Authority
TPT	Transnet Port Terminals
UPS	Uninterruptible Power Supply
URS	User Requirements Specification
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VOIP	Voice Over Internet Protocol
WAN	Wide Area Network
24/7	24 Hours a Day, 7 Days a Week

2 Introduction and Background

2.1 Project Description

The liquid product berth in PE is approaching its end of life, as a result TNPA is building a new tank farm facility at the Port of Ngqura with facilities such as a new liquid product berth, a new general cargo berth and other infrastructure. As part of scope, a Security system and a Public Address System are required to aid in the safety of personnel and to provide protection of infrastructure in the port.

#1 The project scope as detailed in the scope of work is for the provision PSIM, Access control & Intruder Detection System, CCTV and a Public Address System in the following areas;

a. Entrance Plaza
   - CCTV – Buildings, lanes, and external general areas
   - ACS – Lanes, buildings.
   - PA – Buildings and external general areas

b. Substation
   - CCTV – Building, gate and perimeter
   - ACS – Building entrance doors

c. Berth B100
   - CCTV – Buildings, perimeter and gate and fire protection monitoring
   - ACS – Gate and Buildings
   - PA – Buildings and external general areas

d. Perimeter Fence
   - CCTV – cameras along perimeter fence
   - PIDS – Intruder Detection System along the fence

e. Access Roads
   - CCTV – cameras along the road

f. Emendi Building (system)
   - Physical Security Information Management

2.2 Purpose

The purpose of this technical specification is to set out the minimum technical requirements for functional quality, standardisation and system standards for the detailed design (where required), supply, installation, construction, testing and commissioning of equipment and associated infrastructure for the systems in the subsection above.

2.3 Document Terminology

This document makes use of the words shall, should, may and will, with regard to requirements and specifications. To avoid any confusion among these terms, their legal and binding meaning, is indicated here. The reader is advised to be familiar with their contextual usage and meaning.

#2 In this document the word:

a. Shall is used to indicate a mandatory requirement.

b. Should is used as a preference.

c. May is used as a permissive (i.e. neither mandatory nor necessarily recommended).

d. Will is used as a declaration on behalf of something/ someone else.

#3 The word should shall be treated as a requirement by the contractor, although it may be negotiated, amended, approved or declined by the employer based on appropriate justification.

3 Statutory Requirements

#4 In addition to the specifications detailed on this document, the design shall comply with the following relevant South African Acts, Standards and Regulations and shall apply in the order of precedence as listed below:

a. Occupational Health and Safety Act 85 of 1993
b. South African National Standards and Codes of Practice
c. IEC Standards and Recommendations
d. International Standards and Codes – ISO, DIN, BS, ASME, ASCE, ANSI, ASTM, EU
e. All local, provincial or S.A. Government laws in force at the time.

4 Guidelines, Standards and Specifications

#5 All equipment and material to be supplied for the project must be designed, assembled and inspected in accordance with the publications shown in tables below. Each publication shall be the latest revision and addendum in effect on the date the specification is issued for construction unless noted otherwise.

#6 Where conflicts occurs the more stringent requirement of the code, standards and project specifications must be met.

#7 The *Contractor* shall adhere to the following further requirements:

a. All installations shall be inspected and witnessed in accordance with this specification, the manufacturer's instructions and recommendations and the approved quality control plans for each activity.
b. All calibration and test equipment shall hold valid, traceable calibration certificates, which shall be held on Site and shall form part of the quality control dossiers.
c. All equipment, instruments and accessories shall, where appropriate, be calibrated and tested at the manufacturer’s premises or by a duly authorised representative of the manufacturer.
d. All test and calibration certificates shall be included in the on Site quality control dossiers and the as-constructed data packs.

4.1 Transnet Standards and Specifications

The Transnet standards and specifications listed below, shall take precedence in terms of compliance.

	Document Title	Document No.
[1]	CAD Drawing Standards	ENG-STD-0001
[2]	Equipment Tag Numbering Standards	SYS-P-0001
[3]	Contractor Documentation Submittal Requirements	DOC-STD-0001
[4]	Group Security Management – Transnet Physical Security Systems Standard	TPSSS20/05/2016

	Document Title	Document No.
[5]	Transnet Group - Integrated Electronic Security and Related Systems Specification: PIDS Part 6.1 Rev-02	-
[6]	Transnet Group - Integrated Electronic Security and Related Systems Specification: HD IP Video Surveillance System Part 6.3 Rev-02	-
[7]	Transnet Group - Integrated Electronic Security and Related Systems Specification: Part 6.2. Access Control System	-
[8]	Transnet Group - Integrated Electronic Security and Related Systems Specification: Part 6.17. Auxiliary And Related System	-
[9]	Transnet Group - Integrated Electronic Security and Related Systems Specification: Part 5.2. General Specification	-
[10]	Transnet Group - Integrated Electronic Security and Related Systems Specification: Part 6.21. Security System installation Standards	-
[11]	Transnet Group – Integrated Electronic Security And Related Systems Specification: Part-6.16. Access Control Hardware System	-
[12]	Transnet Group – Integrated Electronic Security And Related Systems Specification: Part-6.22. Physical Security Information Management (PSIM)	-
[13]	Specification For The Supply And Installation Of Medium Voltage And Low Voltage Electrical Cables	TPD: 003-CABLESPEC
[14]	Specification For Earthing And The Protection Of Buildings And Structures Against Lightning	TPD: 004-EARTHINGSPEC
[15]	Specification For Electrical Installations To Buildings Other Than Dwellings Houses	TPD-001-EL&PSPEC
[16]	Transnet ICT Equipment Standardization Specification – 2016-06-07_v2.01(1)(002)	-
[17]	Transnet ICT Physical and Environmental Security Standard 1.1	-
[18]	Transnet Pipelines NMPP Functional Design Specification – Situation Management	2684358-S-A100-AY-SP-005

#8 It is the responsibility of the *Contractor* to ensure that he/she obtains all of the *Employer*'s standards (latest amendments apply). The *Employer* shall not be held liable for any losses incurred by the *Contractor* which may arise as a result of non-compliance of the Works by the *Contractor* to the standards.

4.2 National and International Standards

These national and international standards must be adhered to, except where it conflicts with Transnet standards.

#9 Where South African National Standards (SANS) do not cover a specific item, the *Contractor* shall ensure that the item is supplied and installed in compliance with all other relevant/mandatory national and/or international standards, as applicable. Where South African National Standards (SANS) fully cover the item(s) in question, further reference to associated international standards is not required.

#10 The *Contractor* may request approval by the *Employer* for the adoption of a standard not listed in the tables below. Acceptance of such standards will however be at the sole discretion of the *Employer*.

Document Title		Document No.
[19]	(International Code for the Security of Ships And of Port Facilities) ISPS Code – Parts A and B	SOLAS/CONF.5/34
[20]	Degrees of protection provided by enclosures (IP code)	SANS IEC 60529
[21]	Optical fibres	SANS IEC 60793
[22]	Optical fibre cables	SANS IEC 60794
[23]	Splices for optical fibres and cables	SANS 61073-1
[24]	Electrical security installations Part 5-1-2: CCTV installations - CCTV surveillance systems for use in security applications - System design requirements	SANS 10222-5-1-2
[25]	National Electrical Safety Code	IEEE SA C2
[26]	National Fire Protection Association National Fire Codes	NFPA Standards
[27]	EIA/TIA-568 Commercial Building Telecommunications wiring standard	EIA/TIA-568
[28]	EIA/TIA-569 Commercial Building for Telecommunications pathways and Spaces	EIA/TIA-569
[29]	EIA/TIA-606 Administrative Standards for the Telecommunications infrastructure of Commercial Building	EIA/TIA-606
[30]	EIA/TIA-568A premises cabling standard	EIA/TIA-568A
[31]	The application of the National Building Regulations	SANS10400
[32]	Power over Ethernet standard	IEEE 802.3at
[33]	Standard for Ethernet	IEEE/ISO/IEC 802.3
[34]	Design, Installation, Commissioning and Maintenance fire detection and alarm systems	BS EN 5839 Part 1
[35]	Design of Voice Alarm Control and Indicating equipment	BS EN 54 Part 16

5 References

The following documents and drawings serve as reference for this design premise.

5.1 Documents

	Document Title	Document No.
[36]	Employer's Works Information for Public Address and Security Systems	1127672-B01-WI-0002
[37]	Employer Works Information for ICT Systems	1127672-B01-WI-0001
[38]	Camera Masts Security System Technical Specification	1127672-B01-SP-0001

5.2 Drawings

	Drawing Title	Document No.
[39]	Landside Entrance Facility Security Layout	1124367-1-004-K-LA-0001-01
[40]	Landside Phase 2 Substation Security Layout	1124367-1-004-K-LA-0005-01
[41]	Landside Phase 2 Main road Security Layout 1 of 5	1124367-1-005-K-LA-0002-01
[42]	Landside Phase 2 Main road Security Layout 2 of 5	1124367-1-005-K-LA-0002-02
[43]	Landside Phase 2 Main road Security Layout 3 of 5	1124367-1-005-K-LA-0002-03
[44]	Landside Phase 2 Main road Security Layout 4 of 5	1124367-1-005-K-LA-0002-04
[45]	Landside Phase 2 Main road Security Layout 5 of 5	1124367-1-005-K-LA-0002-05
[46]	Landside Phase 2 Perimeter Fence Security Layout 1 of 4	1124367-1-005-K-LA-0003-01
[47]	Landside Phase 2 Perimeter Fence Security Layout 2 of 4	1124367-1-005-K-LA-0003-02
[48]	Landside Phase 2 Perimeter Fence Security Layout 3 of 4	1124367-1-005-K-LA-0003-03
[49]	Landside Phase 2 Perimeter Fence Security Layout 4 of 4	1124367-1-005-K-LA-0003-04
[50]	Berth B100 CCTV and PA System Layout	1126901-1-B01-K-LA-0001-01
[51]	Berth B100 Control and Electrical Buildings CCTV,PAS & ACS Layout	1126901-1-B01-K-LA-0001-02
[52]	Berth B100 Pump-house CCTV and ACS Layout	1126901-1-B01-K-LA-0001-03
[53]	Berth B100 Guard-house ACS,CCTV and PAS Layout	1126901-1-B01-K-LA-0001-04
[54]	9m CCTV Type Mast Typical Details	1124367-1-005-K-LA-0006-01
[55]	3m CCTV Type Mast Typical Details	1126901-1-B01-E-LA-0016-02
[56]	Landside Phase 2 Network Architecture 1	1124367-1-004-K-LA-0006-01
[57]	Landside Phase 2 Network Architecture 2	1124367-1-004-K-LA-0006-02
[58]	Landside Phase 2 Network Architecture 3	1124367-1-004-K-LA-0006-03
[59]	Landside Phase 2 Network Architecture 4	1124367-1-004-K-LA-0006-04
[60]	Berth B100 Network Architecture	1126901-1-004-K-LA-0006-05

6 GENERAL

6.1 Site Conditions

#11 The following environmental conditions shall apply:

Altitude:	Sea level up to 2500m above
Temperature range:	-5°C to +45°C
Relative humidity:	up to 95% RH
Atmospheric conditions:	Salt laden. Electrolytic corrosion conditions prevail in all areas.
Lightning conditions:	Severe, equipment must withstand and be immune to a maximum lightning ground flash density of 11 flashes per km² per annum
Wind Speed:	120kph

6.2 General Requirements

#12 The scope of the Work to be undertaken by the shall be as highlighted in the Works Information and other documents in section 5. The scope for the contractor also includes, but is not limited to, the following:

#13 Evaluate existing designs and make changes where necessary as requested by the *Employer*.

#14 Further design, supply, installation and commissioning of all infrastructure and equipment required as covered in this document, design drawings, bills of quantities/ activity schedules, specifications and other documents as referenced in this specification.

#15 Maintaining coordination with other services to ensure the correct and proper integration of the scoped systems with other associated systems.

#16 Supply of commissioning and operational spares, required for normal wear and tear during plant operation for the period of one year after commissioning.

#17 Provide operating and maintenance manuals, training and back-up support.

#18 The configuration and integration of all the respective equipment shall include the development, in conjunction with the *Employer*, of the final requirements and functionality for monitoring, control, logic and integration of the entire systems. Additional payments will not be made for costs resulting from any omissions, additions or time required for programming, integration and subsequent re-iterations, as described in the contract.

#19 Earthing philosophy shall comply with TNPA electrical standards and specifications.

#20 The contractor shall verify that there are adequate measures in place to protect against lightning strikes and power surges. If not they shall inform TNPA for corrective action.

#21 Cables, boxes, cabinets and equipment shall be marked and labelled as per TNPA specifications.

#22 The SI system of units and measures shall be used to express all numerical quantities.

#23 Use of any component or device, not expressly specified herein, that is required to implement the work, shall be subject to Transnet engineer's approval of required submittals.

6.3 Maintenance and Warranty

#24 All equipment used shall come with a certified warranty with a minimum 2 years, with an option to extend (with a letter from the manufacturer which shall be issued to Transnet with the end user being TNPA, stating warranty/extended-warranty periods and guarantees on those periods, independent of the *Contractor*).

#25 The system implementing Contractor must be accredited and certified by the manufacturer as an EXPERT (or equivalent) integrator, whether as a direct or indirect contractor.

#26 System warranty shall take effect from date of first use, after site acceptance testing.

#27 Contractor shall supply commissioning and operational spares required for a period of one year after commissioning, and special tools required for maintenance purposes, as detailed in Section 8.

6.4 Designs, Calculations by the *Contractor*

#28 All documents, for which prior approvals are required, shall be timeously submitted to the *Employer* for review and approval, prior to placement of orders, fabrication or manufacture.

#29 The *Contractor* shall, as necessary, appoint specialist *Subcontractors* and OEMs to undertake the designs, calculations and drawings, which shall be prepared and checked by suitably qualified and experienced professional engineers, registered with the Engineering Council of South Africa (ECSA) or an equivalent institution recognised by ECSA.

#30 The design engineers shall be appointed by the *Contractor,* subject to approval by the *Employer*. Designs, calculations and drawings shall not be prepared and checked by the same person and shall be reviewed by the *Employer* before the commencement of fabrication.

#31 The *Employer* may, at his sole discretion, request additional design calculations, drawings and associated information, as deemed necessary for verification of the correctness and compliance of the designs. The cost of providing such additional information shall be deemed to be included in the tendered rates, i.e. further payments for such information will not be made.

#32 The *Contractor* shall submit all required calculations in a neat and legible manner. Where calculations are performed using specialised software programs, the *Contractor* shall also furnish copies of the final native software files, without any exclusions. The calculations shall be provided in a professional, neat format, to include, but not be limited to, the following, in the order as stated below:

- Summary of assumptions and conclusions.
- Table of contents.
- List of all associated drawings.
- List of compliancy standards.
- List of all text and references used.
- Calculations.

6.5 Documents and Drawings by the *Contractor*

#33 The *Contractor* shall be solely responsible for the submission of any drawings that are to be provided by his appointed specialist *Subcontractors* and/or OEM's. Drawings shall be accompanied by instruction manuals properly bound for maintenance purposes. The drawings and manuals shall conform to specifications and standards in Section 4 and 5.

#34 The scope of information to be provided by the *Contractor* shall include, but is not limited to:

- Type and routine tests documentation (includes test procedures, punch-list, test-sheets, drawings, and equipment list and certificates)
- FAT and SAT tests documentation (includes test procedures, punch-list, test-sheets, drawings and equipment list and certificates).
- Data sheets and associated detailed specifications of equipment.
- Operations and maintenance manuals.
- Where applicable, detailed designs and calculations. The native software files for any detailed design calculations undertaken in software programmes shall also be provided to the *Employer* for verification purposes. Accepted software programmes for detailed designs and calculation purposes shall include, but are not limited to, AutoCAD.
- As-built drawings in hard and soft copies ('dwg' and 'PDF' formats.)
- Any other as-built documentation as required by the *Employer*.
- Other information required for the completion of engineering design reviews.
- Critical and routine spare part lists.
- Equipment guarantees/warrantees.
- Cable schedules.
- Applicable systems software and licenses, including all final programming of equipment on CD-ROMs.
- Testing and measuring equipment calibration certificates.
- Method statements for systems integration, civil works and mechanical works.
- Electrical Load schedules
- Bills of Material
- Certificate of Compliance where applicable
- Patching Schedule and/or Schedule of IP addresses, switch ports used, PoE on and off, etc.
- Equipment lists
- Equipment data sheets
- Specification of software.
- Documents and Drawings Register
- Configuration documents
- Bills of Material
- Certificate of Compliance where applicable

#35 All project engineering drawings shall include, but not be limited to, the following:

- Single line diagrams
- Detailed schematic diagrams
- Detailed Network diagrams
- General Arrangement diagrams (GA) (panels, junction boxes, turnstiles, boom-gates and poles)
- Site/building layouts drawings where applicable

#36 Unless specifically directed otherwise, Transnet standard format and symbols shall be used.

6.6 Safety

#37 Reference is made to the environmental and safety requirements as detailed in the Works Information, project safety specifications and the particular requirements as described below.

#38 The *Contractor* shall take all necessary safety precautions to prevent static electricity discharge, sparking and any other unsafe condition, which could pose a safety risk to personnel, property and/or equipment.

#39 The location and extent of potentially explosive atmospheres are to be identified and indicated on hazardous area classification drawings. All electrical equipment and instruments for use in hazardous classified areas shall be supplied with a hazardous area certificate issued by a certifying authority approved by SABS/SANS/IEC. Certificates shall be indexed and filed in a certification register.

6.7 South African Electrical Compliance

#40 Any equipment designed and fabricated/manufactured overseas shall have an electrical certificate of compliance to South African Regulations before it is delivered (and operated) in South Africa. The compliance certificate(s) shall fully cover high voltage, medium voltage and low voltage equipment. These certificates shall be issued by an accredited South African professional engineer.

6.8 *Employer* QA Representative

#41 The *Contractor*'s QA requirements shall be as set out in the Works Information.

#42 The *Employer* may choose to appoint a QA/QC representative to monitor and report on some or all aspects of the production and fabrication processes. Full cooperation shall be extended to the appointed QA/QC representative. Associated costs for such services will be borne by the *Employer*.

6.9 Contractor's Subcontractor Declaration

#43 Where Works are to be performed by a *Subcontractor*, the *Contractor* shall provide notices and obtain the *Employer*'s approval prior to the appointment of the *Subcontractor.* This shall include all *Subcontractors* providing design, fabrication, assembly, installation and related services.

7 System Requirements

#44 The PA and Security Systems drawings presented in Section 5.2 serve as a provisional guideline to the contractor, the layout and device numbers shall be verified and validated in the final contractor designs which are subject to Transnet engineers approval.

#45 The Access Control system to be installed shall be compatible with the Babylon XMP system currently installed in Neptune (North) Entrance Plaza.

#46 The CCTV system to be installed shall be compatible with the current CCTV system currently used at the Port which is monitored with the NiceVision Enterprise System.

#47 All Access control (controllers) and CCTV (cameras) end devices shall be connected to Cisco access switches (which will be installed by the ICT Network Contractor) which are housed in the indoor ICT panels and field junction boxes.

#48 Equipment fixing shall comply with the Transnet Group - Integrated Electronic Security and Related Systems Specification: General Specification. Where the specification requirements clashes with other related standards used on the Project, the Contractor shall notify the Project Manager of such developments.

#49 Contractor to advice the *Client* whether the systems provided make use of a Subscription Software license or a Perpetual Software License, including software lifecycle and applicable future costs.

7.1 Access Control System

7.1.1 General

#50 The Access Control System hardware and software shall be compatible with the Port's existing Access Control System.

#51 The Access Control System shall be integrated to existing port Access Control System for control, monitoring and management of access.

#52 All Access Control System installation shall comply with the Group Security Management – Transnet Physical Security Systems Standard and the Transnet Group - Integrated Electronic Security and Related Systems Specification: Access Control System. Where the specification conflicts with the requirements of this document then this document shall take precedence.

#53 The Access Control System shall accept cards already used by TNPA at the port or that have been approved by Transnet.

#54 Software for the Access Control System shall have a time and attendance feature that gives it the capability to interface to the Transnet SAP system for future when required.

#55 The Berth B100 and new East Entrance Plaza shall be equipped with the following Access Control System:

a. Hardware: Babylon system compatible hardware peripherals (controllers and readers)

b. Software: Babylon XMP system

#56 All outdoor Access Control devices shall be IP65, IK10 rated and tamper proof.

#57 All outdoor Access Control end-devices shall be mounted on a stainless steel flush-mount tamper proof IP65 bracket with rain-cover/ sun-shield. Where flush mount installation is not possible, a surface mounted stainless steel bracket shall be used subject to Client's approval.

#58 All indoor Access Control end-devices shall be mounted on a stainless steel flush-mount tamper proof IP65 bracket. Where flush mount installation is not possible, a surface mounted stainless steel bracket shall be used subject to Client's approval.

#59 All Access Control equipment shall be durable and suitable for coastal area environments.

#60 Equipment installed in a hazardous area shall comply to ATEX standard.

#61 The Access Control System shall cater for future expansion.

#62 Access Controllers and readers shall be upgraded to the latest versions and still maintain compatibility with existing system.

#63 The Access Control shall have the capability to integrate to other systems such as visitor management module and SMS text messaging system.

#64 The Access Control shall be integrated to the Intrusion detection system to map alarm status dynamic objects on the ACS port layout screen for ease of alarm view, monitoring and acknowledgement.

#65 The ACS shall be integrated to the CCTV system for triggering alarm associated cameras live views and playback views during alarm status.

#66 The ACS shall be integrated with the fire and smoke detection systems for monitoring of fire alarms to unlock doors during an emergency and to map on the ACS port layout.

#67 Equipment fixing shall comply with the Transnet Group - Integrated Electronic Security and Related Systems Specification: General Specification.

#68 CAT6 Ethernet cabling and Mylar screened multicore interfacing cabling connections, as applicable, between all respective installations.

#69 Equipment fixing shall comply with the Transnet Group - Integrated Electronic Security and Related Systems Specification: General Specification.

7.1.2 Entrance Plaza

7.1.2.1 Field (Hardware)

#70 Entrance/exit vehicle lanes booms (per lane):

a. Boom shall be electronically operated via the Access Control System

b. Boom barrier equipment shall conform to the minimum requirements in the specification: Transnet Group – Integrated Electronic Security and Related Systems Specification: Access Control Hardware System.

c. Shall be able to handle a high volume of traffic and have a 100% duty cycle

d. Shall have 1-entry biometric reader for light vehicles mounted as per security layout drawing

e. Shall have 1-entry biometric reader for heavy vehicles mounted as per security layout drawing

f. Shall have full length boom arm to allow for cars and trucks

g. Shall have red/green LED traffic signal lights (robots)

h. Shall have flushed mount electric operating spike barriers integrated to the boom gate

i. Shall have loop detector

j. Boom controller will have LCD user interface for simple setup and easy maintenance

k. Should be suitable for coastal area environments

l. Manual control of booms should possible on the boom’s controller when Access Control System is not working.

#71 Full-height pedestrian double turnstiles:

a. The full height turnstile equipment shall conform to the minimum requirements in the specification: Transnet Group – Integrated Electronic Security and Related Systems Specification: Access Control Hardware System.

b. handle high volumes of traffic & heavy-duty solenoids rated for continuous duty cycle to ensure optimum reliability

c. 4 arm (90º) – with arms designed to ensure a single entry or exit

d. Zinc plated for corrosion resistance

e. Rotor arms shall be of similar shape as the ones in the existing Port East Entrance Plaza

f. The person is captured in a mantrap where a reader is positioned. If the person has no valid access, the turnstile arms are locked in position by solenoids

g. Integral wire ways with draw wires in place – no exposed wires

h. Shall have one entry and one exit biometric readers mounted the turnstile (dual direction access)

i. Shall be compatible and linked with Port entrance Access Control System

j. Shall be capable to link to Access Control System for fault reporting

k. Mechanical key override – clockwise/anticlockwise

l. Built-in Fail Safe/Fail Secure changeover options

m. Anti-tamper design and maintenance free

#72 Outdoor half-height / waist-high pedestrian turnstiles:

a. The half-height turnstile shall be installed per lane for passage pedestrians

b. Shall handle high volumes of traffic & is 100% duty rated

c. The full height turnstile equipment shall conform to the minimum requirements in the specification: Transnet Group – Integrated Electronic Security and Related Systems Specification: Access Control Hardware System.

d. 3 wing (120°) stainless steel

e. Zinc plated for corrosion resistance

f. Shall have one entry/exit biometric reader mounted on the turnstile (single direction access)

g. Shall be compatible and linked with the Port entrance Access Control System

h. Built-in Fail Safe/Fail Secure changeover options

i. Anti-tamper design and maintenance free

#73 The buildings' main entrance doors to the outside the port shall have a full Access Control comprising of:

a. 1-Entry and 1-exit biometric readers (with time and attendance)

b. Break-glass unit for exit during emergency

c. Emergency key switch where required

d. 500kg or higher monitored maglock with door status signal (ML600-M)

e. A single leaf door shall have one maglock

f. A double leaf door shall have two maglocks

#74 For offices and general areas where full Access Control is required, the access portal shall have:

a. 1-Entry and 1-exit proximity readers (with a keypad)
b. Break-glass unit for exit during emergency
c. Monitored maglock with door status signal LEDs
d. A single leaf door shall have one maglock
e. A double leaf door shall have two maglocks

#75 All IT rooms and critical rooms shall have:

a. 1-Entry and 1-exit biometric readers (without time and attendance)
b. Break-glass unit for exit during emergency
c. Emergency key switch where required
d. Monitored maglock with door status LEDs
e. Door monitor embedded Maglock to lock and monitor door status
f. A single leaf door shall have one maglock
g. A double leaf door shall have two maglocks

#76 Controller Unit (Lanes):

a. Shall communicate via TCP/IP to the central control system
b. Shall be able to operate independently of the server
c. Shall be housed in a control-box which shall be installed in the building in the Server room or secure location approved by the *Client*.
d. The controller shall be connected to the access switches in the Server room or the one in the Health office building.
e. Each lane shall have a controller interfaced with the boom-gate and the boom-gate readers
f. The half-height turnstile per lane shall either terminate to the boom-gate controller or be assigned its own controller.
g. Only one or two controllers shall be assigned per lane.
h. Controllers shall be installed with integrated UPS, battery-pack for back-up power.
i. Controller and back-up power supply shall be housed in a lockable box enclosure.
j. Shall have the following properties;
    i. Shall take a minimum of 4 readers
    ii. Number of Cards: 50000 (expandable to 250000)
    iii. Bookings/templates storable and pins: 50000
    iv. Doors per controller: 4 (expandable to 8)
    v. Readers per controller: 4 (expandable to 8)
    vi. I/O per controller: 16 supervised inputs / 8 outputs
    vii. Communication: Ethernet network interface (fixed IP recommended) and RS485 network reader bus

viii. Enclosure / Housing: powder coated aluminium, IP54, tamper-proof & monitored, lockable (key)

#77 Door Controller (buildings):

a. Shall communicate via TCP/IP to the central control system

b. Shall be able to operate independently of the server

c. Shall be housed in a enclosure box which shall be installed in the building on a secure side of the door inside the ceiling or on the wall above a specific door.

d. The door controller shall be connected to the access switch in the buildings as shown on the network layout drawings

e. Only one or two controllers shall be assigned per room or door.

f. Controllers shall be installed with integrated UPS, battery-pack for back-up power.

g. Controller and back-up power supply shall be housed in a lockable box enclosure box (size and material of box subject to *Client* approval).

h. Shall have the following properties;

i. Shall take a minimum of 4 readers

ii. Number of Cards: 50000 (expandable to 250000)

iii. Bookings/templates storable and pins: 50000

iv. Doors per controller: 4 (expandable to 8)

v. Readers per controller: 4 (expandable to 8)

vi. I/O per controller: 16 supervised inputs / 8 outputs

vii. Communication: Ethernet network interface (fixed IP recommended) and RS485 network reader bus

viii. Enclosure / Housing: powder coated aluminium, IP54, tamper-proof & monitored, lockable (key)

#78 **Input Terminals/ Output Terminals**

a. Where input/ output modules are required for installation instead of door controllers, the I/O devices shall conform to the minimum requirements in the Transnet Group - Integrated Electronic Security and Related Systems Specification: Access Control System Part 6.2.

#79 Biometric reader:

a. *Client* preferred make is XMP-TMC (Babylon product) or latest subject to *Client* approval

b. It shall have fingerprint scanner, Led display, proximity card reader and no keypad

c. Shall be tamper proof

d. Biometric reader shall be connected to the Access Control System via a door controller, where applicable.

#80 Card readers

a. Shall be able to read cards already used on the port (both card types if possible)

b. The reader shall be connected to the Access Control System via a door controller.

a. *Client* preferred make is XMP-TMC (Babylon) or latest subject to *Client* approval

b. Shall be of Multi-Mode Multi-Discipline type, which can read the following (and latest) 125kHz and 13.56MHz tags on the same Reader and must be able to read cards already used on the port

- 1.7.9.3 125kHz EM Marin
- 1.7.9.4 125kHz Impro Hi Tag (read/write)
- 1.7.9.5 125kHz Impro proprietary Tags (1074 and 2074)
- 1.7.9.6 125kHz HID Tags (H10301, H10302 and H10304)
- 1.7.9.7 13.56MHz HID iClass Tags (ISO 15693-2)
- 1.7.9.8 13.56MHz Sony FeliCa Tags (ISO 18092)
- 1.7.9.9 13.56MHz Phillips MIFARE® Tags. (ISO 14443A)

c. The reader shall be connected to the Access Control System via a door controller.

d. The card readers support infield firmware upgrade and feature Zero Down-time firmware upgrades.

e. Card readers shall be approved by the *Client* and Engineer regarding appearance, final finish, and mounting detail. Card readers shall be adaptable for surface and/or flush mounting.

f. Shall have the following properties;

i. Case: ABS material (impact-proofed housing) and tamper proof

ii. Typical Read Range: (subject to *Client* approval)

iii. Protection type: IP 65

iv. Signalling: minimum 3 LED statuses, buzzer

#81 Break glass unit;

c. Break glass unit and magnetic locks shall be connected to the controller for the specific door.

a. Shall have Manual key resettable actuator with resettable element

b. Legend & logo: BG cover “EMERGENCY DOOR RELEASE” , BG window “Emergency Break Glass” including “PRESS HERE” logo

c. Shall be surface mount

d. With hinged clear plastic protective cover

#82 Magnetic Lock:

a. Maglock shall be monitored (with LED, Hall effect IC and NO/NC relay)

b. Maglock shall be fail safe

c. Doors shall be assessed for the correct bracket prior installation

d. 600kg or higher holding force

e. Dual voltage 12 & 24VDC

f. MOV (metal oxide varistor) Surge protection

g. CE Approved

#83 Door Monitor/ Open Sensor

a. Shall use on roller shutter doors

b. Waterproof die-cast zinc construction

c. Surface mounting on concrete floor

d. 25mm Take and 55mm break

#84 **Fingerprint-enrolment-station**

a. Shall be installed in the Security Control room in the BTS building

b. Shall be compatible with the Access Control System installed

c. Will be used for the enrolment and verification of fingerprints

d. Shall allow a minimum of four fingerprints to be stored

e. Shall have the following properties;

- Connection: USB 2.0/3.0 and Ethernet RJ45
- Power supply: via USB-interface and power supply via power adapter
- Sensor technology: Optical

7.1.2.2 Monitoring

#85 All Access Control System shall be monitored and controlled from Emendi Building and the New entrance Plaza Supervisor office.

#86 The new Entrance plaza shall be provided with 2 client workstations (pc tower, 1 screen, 1 usb keyboard and 1 usb mouse). 1 workstation shall be installed in the Security Supervisor office and the other in the Main building reception desk (Registration office).

#87 The client workstations shall have the Babylon software to use by the security personnel to control and monitor Access Control System in the Entrance plaza.

#88 The Contractor shall provide an Access Control Server machine (1 pc rackmount tower, 1 rackmount KVM unit with an additional usb mouse) that installed in the Entrance Plaza admin building server room or Emendi building (depends on *Client* preference), where possible system data shall be shared with the existing system server data on the Port.

#89 The system shall be integrated to the existing Babylon XMP Access Control System server sitting in the Emendi building/ North Entrance Plaza.

#90 Additional licences shall be provided by Contractor where required by the Server.

#91 Client workstation to be installed in the new entrance plaza shall have the same graphics and configurations as the existing East entrance plaza.

#92 The contractor shall install the new system, configure, upgrade system where required and integrate the system to the existing Babylon Access Control System at the Port.

#93 Additional licences shall be provided by *Contractor* where required by the system, server or workstations.

#94 Access Control Server Minimum requirements

a. *Client* preferred brand is Dell or similar

b. 1U Rack Server

c. Intel Xeon 3.0GHz processor

d. 1x 16GB RAM

e. 2 x Gigabit Ethernet LAN ports

f. 4x 2TB Hot-plug Hard Drive

g. Dual, Hot-plug Power Supply (1+1)

h. Windows Server 2012, Standard Edition R2

#95 Access Control System Operator client PC minimum requirements

a. Rackmount and free-standing compatible Workstation CPU Tower

b. Intel Core i7 (12MB Cache, 3.0GHz) latest generation

c. 16GB Memory, 512GB SSD

d. 2x1000BaseT NIC

e. Graphics: NVIDIA(R) 2GB, and

f. OS: Windows 10 64 bit (shall be Transnet approved OS software) compatible with active directory and the Access Control and CCTV software.

g. Come with 2 24" Colour LCD screens (with a resolution of 1080p)

h. Come with wired keyboard (usb), wired optical mouse (usb) and a PTZ joystick

#96 Where the minimum requirements stipulated above are found not aligning with the Access Control System and CCTV system requirements, Contractor shall advice *Client* accordingly and make necessary changes.

#97 Monitor– 24" LED Monitor

a. Display: 24" LED Backlight

b. Designed for 24/7 operation

c. 4K Resolution

d. 16:9 aspect ratio

e. 1000:1 contrast ratio

f. Audio: Built-in Speakers

g. Inputs: VGA, HDMI

#98 Events Log Printer

a. A high quality Network capable Laser Printer shall be supplied, installed and commissioned as part of this contract, for use with the management workstation in order to generate user defined management reports.

b. Page feed capable of accepting paper at least up to 242 mm (A4) wide. Single page paper shall be used to allow users to print out historical events and system activity.

c. Shall conform to minimum requirements in Transnet Group - Integrated Electronic Security and Related Systems Specification: Access Control System Part 6.2, but of latest version.

d. The printer shall incorporate a visible control panel with LED indication for power on, paper out and ready.

e. The printer shall be installed and configured into the Supervisor client workstation to be installed within the Supervisor Office in the Entrance Plaza admin building.

f. The printer shall be supplied with both power and data cables of suitable length to suit the location. In addition, the printer shall be set up complete with one full box of paper and two spare cartridges.

7.1.2.3 Software

#99 All Access Control Systems software and firmware shall be the same make as the North entrance plaza or latest which is subject to approval from *Client*.

#100 The Access Control System software shall cater for future expansion

#101 Contractor shall supply and install operating system software for workstations and servers (OS may be sourced from Employer).

#102 Contractor shall supply and install Access Control Systems software and licences for servers, workstations and field equipment including additional licences where required.

#103 Access Control Software Minimum requirements

a. Developed for Windows 10, 2012, 2016 and latest
b. Multi-user capability and network support via TCP/IP
c. Online monitoring of all connected devices
d. Roll call and muster reporting
e. Security lockdown
f. Integration of monitoring and control *functions* within the building management access automation system
g. Unlimited number of graphics to visualize alarms and processes
h. Video log
i. Optional user-defined Time Recording and Accounting
j. Guard tour patrol system for monitoring e.g. security guards at appointed checkpoints
k. Transmission of alarms via e-mail or text message
l. Workflow
m. Integrated SNMP server
n. Open software interface feature to enable communication with third-party systems (e.g. SAP® R/3® HR via TCP/IP)
o. Optional Visitor management software
p. Integrated module for badge layout definition
q. Graphical user interface for creating, modifying or deleting cardholder records and access profiles

7.1.2.4 Power Supply

#104 The Access Control System shall be powered from the UPS

#105 Controllers shall be connected to UPS power through battery pack power supply which shall be mounted next to the controller box

#106 Power supply shall conform to requirements in Transnet Group – Integrated Electronic Security And Related Systems Specification Part-6.2 Access Control System

#107 Auxiliary systems and components such as UPS, Surge Protection and Power Supply Unit shall conform to the Transnet Group – Integrated Electronic Security And Related Systems Specification - Auxiliary And Related System

7.1.3 Berth B100

7.1.3.1 Field (Hardware)

#108 The Access Control System at the Berth B100 shall be of the same make as the North Entrance Plaza in 71.2.

#109 All Access Control portals and equipment at the Berth B100 shall be monitored and controlled remotely from the Emendi building, New North Entrance Plaza and locally only via individual access cards (issued by TNPA).

#110 The Berth 100 Access Control System shall interface to current existing Babylon system used at the port.

#111 Entrance/exit vehicle lane barrier boom-gates:

a. Boom shall be electronically operated via the Access Control System
b. Boom barrier equipment shall conform to the minimum requirements in the specification: Transnet Group – Integrated Electronic Security and Related Systems Specification: Access Control Hardware System.
c. Shall be able to handle a high volume of traffic and have a 100% duty cycle
d. Shall have 1-entry proximity reader for light vehicles mounted on gooseneck as per security layout drawing
e. Shall have 1-entry proximity reader for heavy vehicles mounted on gooseneck as per security layout drawing (same gooseneck as above)
f. Shall have full length boom to allow for cars and trucks
g. Shall have loop detector
h. Manual control of booms should be possible on the boom's controller when Access Control System is not working
i. Boom controller will have LCD user interface for simple setup and easy maintenance
j. Should be suitable for coastal area environments

#112 The buildings' main entrance doors shall have a full Access Control comprising of:

a. 1-Entry and 1-exit biometric readers (with time and attendance feature)
b. Break-glass unit for exit during emergency
c. Emergency key switch where required
d. 600kg or higher monitored maglock with door status signal (ML1200-M)
e. A single leaf door shall have one maglock
f. A double leaf door shall have two maglocks

#113 For offices and general areas where full Access Control is required, the access portal shall have:

a. 1-Entry and 1-exit proximity readers (with a keypad)
b. Break-glass unit for exit during emergency
c. 600kg or higher monitored maglock with door status signal (ML1200-M)
d. A single leaf door shall have one maglock

e. A double leaf door shall have two maglocks

#114 All IT rooms and critical rooms shall have Access Control, same as #112, without the requirement for time and attendance feature.

#115 Over-ride entry key-switch shall be installed in emergency, electrical or critical areas as per layouts.

#116 Biometric reader requirements same as listed in 7.1.2.1

#117 Card readers requirements same as listed in 7.1.2.1

#118 Door Controller; requirements same as listed in 7.1.2.1

#119 Door break-glass; requirements same as listed in 7.1.2.1

#120 Magnetic Lock requirements same as listed in 7.1.2.1

#121 Door monitor requirements same as listed in 7.1.2.1

7.1.4 Intercom

#122 Where indicated on the drawings door intercom systems shall be installed at the B100 gate and buildings to enable communication between the gate and B100 control room.

#123 The intercom system shall be of IoIP type and powered via PoE

#124 Master station shall be Voice-actuated or press-to-talk communication through the handset, with hands free response from the called sub.

#125 Intercom system shall conform to requirements stipulated in the Transnet Group – Integrated Electronic Security And Related Systems Specification Part 6,5 Intercom System

#126 **Desk-phone Master/Sub-Master station shall consist of the following**:

a. Master station shall be installed in the Berth B100 Control Room and interfaced to control room switch
b. Sub-master station shall be installed in the Berth B100 guardhouse and interfaced to guardhouse Access switch
c. Shall come with handset for private communication
d. Shall have chime tone volume control

#127 Intercom Door Station

a. Shall be installed at the gate entrance and interfaced to guardhouse switch
b. Shall be flush mount or surface mount where not possible
c. Hands free communication
d. Pole mount bracket with rain-cover/sunshield

7.1.4.1 Monitoring

#128 The Access Control System at the Berth B100 shall be integrated to the Port's Existing Babylon Access Control System and the North Entrance Plaza system.

#129 The Current Babylon Access Control System software at the Emendi building, East Entrance Plaza and the new North Entrance Plaza shall be used to control and monitor the Access Control at Berth B100.

#130 The system shall be integrated to the existing Babylon XMP Access Control System server sitting in the Emendi building/ North Entrance Plaza.

#131 Client workstation to be installed in the new entrance plaza shall have the same graphics and configurations as the existing East entrance plaza.

#132 The contractor shall add graphics and drivers, configure, upgrade system (subject to *Client* Approval) where required and integrate the system to the existing Babylon Access Control System at the Port.

#133 Additional licences shall be provided by *Contractor* where required by the existing system servers and workstations.

#134 The Access Control System software shall cater for future expansion.

7.1.4.2 Power Supply

#135 Power requirements shall be the same as in section 7.1.2.4.

7.1.5 Interface with Fire Detection System

#136 The Security system shall have the capability to interface with the Building monitoring and Fire alarm system. Thus the Situation Management and/or Access Control system should be able to accept signals in a form of voltage free contacts and Ethernet/serial data from the BMS and Fire alarm systems, and to provide (where required) control outputs in the form of voltage free contacts to these systems.

#137 A dedicated input should be available on the ACS controller which is designated as a fire alarm input, on receipt of a voltage free contact from the fire detection system this input will then trigger all portals under controller to unlock automatically without the involvement of an operator.

#138 An Ethernet/serial card should be added in the fire detection system to integrate the fire detection system on the Situation Management/ Access Control system for monitoring and displaying fire detection sensors and panel alarms.

7.2 CCTV Security System

7.2.1 General

#139 The CCTV system to be installed shall be compatible with the current CCTV system currently used at the Port which is monitored from Emendi Building – Security Control room with the NiceVision Enterprise system.

#140 The existing Port CCTV system and also *Client* preferred systems for the project are as follows;

a. Camera make: Bosch cameras

b. CCTV Software: NiceVision enterprise

c. Server and Storage: Dell® PowerEdge NVR

#141 Contractor shall provide a CCTV system (software and hardware) that is *Client* preferred or can propose a different brand hardware that is similar and can integrate to the existing system (any different brand proposed by the Contractor shall be subject to *Client* approval).

#142 The CCTV system shall conform to the Transnet Group - Integrated Electronic Security and Related Systems Specification: HD IP Video surveillance system, but with the consideration for latest technology. Where the specification conflicts with the requirements of this document then this document shall take precedence.

#143 The equipment selection will conform to Transnet ICT Equipment Standardization Specification.

#144 The main function of the system shall be for the following key functions:

a. Real time surveillance

b. Recording of real time events and historical video data for video evidence of a security event and

c. Provide a deterrent to criminal and unacceptable behaviour.

#145 CCTV hardware and software shall be compatible with the current existing system used at the port.

#146 CCTV cameras shall be installed at all access points and critical areas within the buildings.

#147 The system shall incorporate as standard motion detection video analytics and have activities recorded and stored.

#148 The CCTV network shall be secure against both physical and network intrusion. The contractor shall provide an effective network protection and securing strategy.

#149 Video storage capacity shall be considered at the beginning of the design process of the CCTV system to ensure additional equipment and additional storage requirements needed for the new system to operate at optimal performance level is catered for.

#150 The system shall be IP based.

#151 The system shall be available 24/7.

#152 The system shall be capable of unlimited expansion for the addition or modification of video inputs.

#153 CCTV equipment network settings such as IP address and mask will be provided by *Client* upon Request.

7.2.2 Cameras

#154 Suitable lenses shall be selected to accomplish the monitoring functions for each camera at its point of installation.

#155 The CCTV system cameras shall produce sharp, detailed and stable images on the monitor in sufficient detail to provide positive identification of individuals within the protected areas under all conditions of light.

#156 All fixed CCTV cameras shall be PoE powered.

#157 Dome cameras shall be used for indoor monitoring

a. Cameras shall be strategically placed to monitor critical access doors, passage ways and storage rooms.

#158 Fixed box (c-mount) or bullet cameras shall be used to monitor outdoor areas

a. Cameras shall be strategically placed to monitor gates, perimeter, parking and access roads.

#159 Where required, wide coverage public areas shall be viewed with PTZ cameras, to provide close up images and tracking of events.

#160 The CCTV shall operate in all light conditions, including low light conditions, and shall automatically compensate for changing light conditions.

#161 Where a camera must operate in total darkness, the nature of the possible events will be analysed to determine whether the situation requires a special application camera such as one that uses infra-red illumination or thermal.

#162 The CCTV system shall be interfaced with the intercom system and the Access Control System depending on the requirements of the specific installation.

#163 The system shall provide alarm condition detection/activation and camera network status.

#164 **Camera Types** referenced below, can be found on the Transnet Group - Integrated Electronic Security and Related Systems Specification: HD IP Video surveillance system.

#165 All indoor dome cameras will be at least full High Definition (FHD) 4.0MP resolution. These cameras shall be selected for suitability for internal and external Surveillance. Camera shall have minimum requirements of Camera Type 1b.

#166 All outdoor cameras will be at least full High Definition (FHD) 4.0MP resolution. The cameras shall be selected for suitability for internal and external Surveillance with minimum requirements of camera Type 6b.

#167 Facial recognition cameras will be at least full High Definition (FHD) 4.0MP resolution with integrated IR illuminator. The cameras shall be selected for suitability for external Surveillance with minimum requirements of camera Type 6b.

#168 As per design drawings, fixed IP Thermal Cameras of minimum specification of 640 x 480 resolution shall be used to monitor the port perimeter, and they shall be mounted at 3m or 6m height based on assessment of the Field of View.

#169 Automatic Licence Plate Recognition (ALPR) cameras shall have these minimum requirements;

a. Camera shall be installed and focus adjusted so that license plate should cover at least 15-20% of camera field of view

b. IP FHD with camera Type-7a minimum requirements

c. Vandal resistant pole mount accessories and surge protection

#170 Outdoor FHD PTZ cameras minimum requirements;

a. Cameras shall be mounted on 9m pole

b. Minimum specification: 2MP@30fps, 30x, high WDR

c. All Port perimeter PTZ cameras will have IR illuminators

#171 Dual (thermal + video PTZ) cameras (640 x 480, 2MP) shall be used to monitor for fire detection at the Berth B100 site.

#172 All cameras mounted/ installed in hazardous area zones shall have explosion-proof housings with explosion proof certification.

7.2.3 Camera Mount and Housing

#173 External cameras shall have IP66 rated housings and function satisfactorily in all weather conditions.

#174 Perimeter cameras shall be mounted on top of suitable camera masts at required heights for better monitoring (PTZ at 9m, fixed at 3m or 6m for perimeter).

#175 Thermal cameras in perimeter shall be mounted on 6m high Mast.

#176 Where both cameras types are required on the same pole, the 9m pole will be used, with the fixed camera mounted at 3m height.

#177 Camera masts shall be mounted on suitably sized and constructed bases to withstand the mass of the masts and any wind moments on the masts.

#178 All ceiling mount cameras shall be mounted with in-ceiling mount kits, and no wires shall be exposed.

#179 Cabling for all outdoor installations shall be run through galvanized steel conduit pipes or flexible steel conduit, no PVC pipes shall be used. Contractor to refer to referenced specification for further guidance.

#180 Plinths must be designed and constructed to support these masts.

#181 All steel Camera masts shall be earthed.

#182 Camera masts and poles shall be selected and designed with guidance from the Transnet Security Camera mast specification.

7.2.4 East Entrance Plaza

#183 Cameras on the lanes are installed as;

a. 1-LPR: for licence plate recognition
b. 1- Facial recognition IR cameras for trucks
c. 2- Facial recognition IR cameras for cars
d. 1-fixed camera to monitor the top of the trucks
e. 1-fixed camera to monitor passengers walking through the half-turnstile

#184 There shall be 2-PTZ cameras on 9m Masts with a homing position towards the lanes on either side

#185 1-PTZ cameras on the 9m masts shall be homed towards outside the port

#186 There shall be fixed cameras monitoring people passing through the full height turnstile

#187 Inside the building there shall be FHD dome cameras mounted on the ceiling monitoring main entrances and the general areas in the buildings

7.2.5 East Bank Substation

#188 1-Fixed FHD camera shall be installed on 3m mast to monitor vehicles entering/exiting the station.

#189 Fixed and PTZ cameras shall be used on perimeter boundaries.

#190 Perimeter cameras shall be mounted on top of suitable camera masts at required heights for better monitoring (9m masts for the PTZ, 3m mast for the fixed cameras).

#191 Where adequate lighting is not provided, infrared cameras shall be used.

#192 Inside the substation there shall be FHD fixed cameras installed only inside sensitive areas as depicted in the layout drawing.

#193 All cameras shall be PoE powered, and they shall connected to switch in the Substation rack 1.

#194 Where required, perimeter JB will be provided to house media converters for cameras installed at distance longer than 90m from the security rack.

7.2.6 Berth B100

#195 Two sets of cameras shall be installed on this site, one set for surveillance and the other for operation.

#196 The cameras for surveillance shall be installed as follows;

a. 2- entry facial recognition IR cameras for cars and trucks installed on a gooseneck for cars entering the site.
b. 2- exit facial recognition IR cameras for cars and trucks installed on a gooseneck for cars exiting the site.
c. Fixed FHD dome cameras shall be strategically installed in the buildings to monitor main entrance doors, general passages and sensitive rooms within the buildings.
d. Fixed and PTZ cameras shall be used on perimeter boundaries.

#197 Perimeter cameras shall be mounted on top of suitable camera masts at required heights for better monitoring (9m masts for the PTZ, 3m mast for the fixed cameras or the height of the structure).

#198 The cameras for operations shall be installed as follows;

a. Two thermal/normal-view PTZ cameras shall be installed on 3m mast to monitor fire signatures.

b. One additional normal PTZ camera shall be installed 9m mast next to these thermal cameras to have a general view of the sensitive area.

c. Since these cameras are installed in a hazardous zone, then they shall be installed in explosion proof housings.

d. The field junction box housing the switch connecting these cameras shall be on an explosion proof enclosure or installed outside the hazardous zone area.

#199 The surveillance cameras on the site will be controlled and monitored from the Main Control room at the Emendi building at the Port.

#200 The operational cameras installed on site shall be monitored and controlled from a client workstation installed in the control building.

#201 The Emendi building shall also have a view on these cameras, but the control building workstation shall take precedence on the control of the cameras.

7.2.7 Main Roads

#202 There shall be PTZ FHD cameras on 9m masts installed along the roads to have a general view of the roads.

#203 A fibre cable (installed by others) shall run to connect these cameras on the network ring.

7.2.8 Perimeter Fence

#204 There shall be fixed thermal FHD cameras mounted on 6m masts along the perimeter fence boundary.

#205 There shall be PTZ (with infrared light) FHD cameras on 9m masts installed to have a general of the perimeter.

#206 A fibre cable (installed by others) shall run to connect these cameras on the network ring.

#207 Transnet standard street and parking lights shall be sufficient for camera lighting.

7.2.9 Monitoring Station

#208 The CCTV system shall be integrated to the existing port CCTV system where the cameras will be monitored from the Emendi building by authorised security personnel.

#209 Camera setting and configurations shall be the same as the port existing CCTV system

#210 All CCTV cameras connected to the system shall digitally record for a minimum of 30 days and additional storage shall be considered for event recording.

#211 All abnormalities shall be digitally recorded for a period of no less than 30 days, and shall be capable of being used appropriately by the police in evidence and stored, copied and viewed without interfering with recording.

#212 The monitoring workstation and their access authorisation shall be as follows;

		CCTV Monitoring From			
		Emendi Building	East Entrance Plaza	Berth B100 Control Building	North Entrance Plaza
Mo nit	East Entrance Plaza	X	X		

	Substation	X			
	Berth B100	X		X	
	Main Roads	X			
	Perimeter Fence	X	X		

#213 A client workstation shall be installed in the Security supervisor office in the main building of the east entrance plaza to monitor the entrance plaza and perimeter as shown in the table above.

#214 Another client workstation shall be installed in the Berth B100 Control building to monitor the operational cameras on the Berth.

#215 Client workstation hardware shall conform to Transnet standards and support active directory.

#216 Operating system for the client workstation shall be provided by Transnet and all software in the client station shall confirm to the Transnet ICT standards.

#217 Minimum Workstation requirements for the B100 client workstation machine shall be as follows;

a. Rackmount and free-standing compatible Workstation CPU Tower
b. Intel Core i7 (12MB Cache, 3.0GHz) latest generation
c. 16GB Memory, 512GB SSD
d. 2x1000BaseT NIC
e. Graphics: NVIDIA(R) 2GB, and
f. Transnet approved OS software) compatible with active directory
g. Come with 2 24" Colour LCD screens (with a resolution of 1080p)
h. Come with wired keyboard (usb), wired optical mouse (usb) and a PTZ joystick

#218 For the Entrance Plaza the same workstation used for Access Control shall be used for monitoring the CCTV in the Supervisor's Office.

#219 Workstation in the Entrance Plaza workstation shall cater for 3 monitors, 2 for monitoring CCTV and 1 for the purpose of displaying Access Control. All connected in the same workstation.

7.2.10 Video Storage

#220 The system shall be capable of unlimited expansion for the addition or modification of video inputs.

#221 Whereby recording space is not enough, this shall be expanded to cater for the additional cameras.

#222 All required licences, firmware compatibility and legacy equipment interface requirement shall be provided by the contractor.

#223 Contractor shall first make an assessment on the current available storage capacity.

#224 The *Contractor* shall be responsible to integrate all the new cameras in the existing NVRs and software, then setup to be as per existing configurations.

#225 Video footage for the Berth B100 cameras shall be stored at the Emendi building server.

#226 Substation CCTV footage shall be stored at the Emendi building server.

#227 Main roads and Perimeter fence CCTV footage shall be stored at the entrance plaza and Emendi building.

#228 Entrance plaza footage shall be stored on the Entrance plaza server and the Emendi building server.

#229 Contractor shall supply NVR with minimum requirements of a Dell® PowerEdge R730xd NVR (NVR-R-2-2-96TB) which be installed either at Emendi building or Entrance plaza admin building.

7.2.11 Communication and Cabling

#230 All cables and conductors, except fibre optic cables, that act as a control, communication, or signal lines shall include surge protection.

#231 The CCTV network shall be secure against both physical and network intrusion. The contractor shall provide an effective network protection and securing strategy.

#232 CCTV network equipment and recording information shall be access controlled.

#233 Horizontal cabling of CCTV equipment shall be a responsibility of the *Contractor*.

#234 All CCTV equipment shall use CAT6 cabling or Fibre where required.

#235 Jointing of cabling shall not be allowed.

#236 All CAT6 cabling shall be no more than 90m

#237 CCTV network equipment and recording information shall be access controlled.

7.2.12 Power Supply

#238 The CCTV system including all cameras shall be powered from a UPS.

#239 Auxiliary systems and components such as UPS, Surge Protection and Power Supply Unit shall conform to the Transnet Group – Integrated Electronic Security And Related Systems Specification - Auxiliary And Related System

7.3 Public Announcement System

7.3.1 General

#240 The PA system shall form part of the emergency alert system for the building, operating automatically or manually to alert occupants to a hazard which may require evacuation in a safe and orderly manner. Therefore the PA shall be capable to:

a. Alert occupant during a fire hazard when fire has been detected.

b. Announce pre-programmed emergency alerts.

c. Announce general manual messages.

7.3.2 PA System Requirements

#241 The system shall integrate with the Fire detection system to auto engage fire alert alarm messages

#242 Failure of a single amplifier or loudspeaker circuit shall not result in total loss of coverage in the loudspeaker zone served.

a. The monitoring system specified should indicate the failure of an amplifier or of a loudspeaker circuit.

b. Contractor should advise whether two separate loudspeaker circuit in a zone is necessary or not, but the final decision lies with the *Client* Transnet.

#243 All messages shall be clear, short, unambiguous and as far as practicable pre-planned.

#244 The system design shall make it inherently impossible for an external source to corrupt or derange the store or its contents.

#245 The system shall be capable of being divided into emergency loudspeaker zones if required by the evacuation procedure.

#246 Unless otherwise advised by the *Client*, the following event priority levels will be used:

a. Evacuate - potentially life-threatening situation needing immediate evacuation.

b. Alert - dangerous situation nearby requiring warning of pending evacuation.

c. Non-emergency - operational messages, e.g. system test, etc.

7.3.3 Entrance Plaza

#247 The PA system main controller and amplifier shall be installed in a cabinet or rack in the main building server room.

#248 A remote desk station shall be provided in the main building reception desk to make announcements.

#249 The PA system shall be linked with fire monitoring system for emergency alarms.

7.3.4 Berth B100

#250 The PA system main controller and amplifier shall be installed in a cabinet in the control room.

#251 A microphone on the main controller shall be used to make announcements on the site.

#252 The PA system shall be linked with fire monitoring system for emergency alarms.

7.3.5 Field Hardware Controllers

#253 The PA system main controller and amplifier shall be installed in a cabinet or rack in the main building server room.

#254 UPS power (by Others) and battery back-up shall be provided and shall last at least 6 hours.

#255 All outdoor equipment shall be IP66 rated, or at least installed in a field enclosure that complies

#256 Shall be Manufactured from corrosion free materials

#257 Failure of one Controller shall not affect any other.

#258 Perform all the functions of the relevant/related area/s and/or zone/s

#259 These system elements should be mounted such that detection is expected before any components of the system are reached by the intruder.

#260 Controllers and other field devices shall not be mounted on the fence fabric but shall installed in field boxes a distance from the perimeter.

#261 System shall cater for future expansion.

7.3.6 Power Supply

#262 The system shall be powered via UPS

#263 If the building is to be evacuated following primary power failure, a secondary power supply shall be provided. This shall be capable of operating the system in the emergency mode for a period equal to twice the evacuation time determined by the appropriate authority for the building. In any event, the secondary power supply shall be capable of powering the system for a minimum of 30 min.

#264 Auxiliary systems and components such as UPS, Surge Protection and Power Supply Unit shall conform to the Transnet Group – Integrated Electronic Security And Related Systems Specification - Auxiliary And Related System

7.4 Perimeter Intruder Detection System

7.4.1 General

#265 PIDS systems shall be installed on the perimeter fence of the Port to detect the presence of an intruder attempting to breach for entry or exit.

#266 The Contractor shall do the detailed design, supply, installation, commissioning, configuration and integration of all equipment, software and database for the PID System.

#267 The PIDS to provided shall be Fibre Optic-cable Intruder Detection System (FOIDS systems Type-2 on the Transnet specification) which will be mounted on the palisade fence to achieve intruder detection on the perimeter.

#268 Contractor can propose an alternative technology that can outperform the FOIDS, subject to approval by the *Client*.

#269 The PIDS shall be compatible with proposed new and existing Access Control system (Babylon TMC) and Port CCTV system.

#270 Contractor shall integrate the PIDS system to the existing and new Access Control system to allow for the response to and/or monitoring of all events, conditions, statuses and alarms and to exchange this and other relevant data with the indicated systems

#271 The PIDS shall also be integrated to the existing CCTV system to allow for the response to and/or monitoring of all events, conditions, statuses and alarms and to exchange this and other relevant data with the indicated systems alarm recording triggered by PIDS as well as for the FoV focus control of the PTZ cameras.

#272 The system implementing Contractor must be accredited and certified by the manufacturer (OEM) as an EXPERT (or equivalent) integrator, whether as a direct or indirect Contractor.

#273 The minimum technical requirements of the system shall be as per Transnet group – integrated electronic security and related systems specification Part 6.1 - Perimeter Intrusion Detection System (PIDS) specifically FOIDS systems Type-2. But with the latest software, hardware and improved performance and features.

#274 The PIDS shall installed along the Port of Ngqura Perimeter as indicated in the Perimeter design drawings in 5.2.

#275 Where there is a gate along the perimeter, IR beams (both wired) shall be provided across gate for intruder detection.

#276 Where there is a river or stream along the perimeter, a Radar technology Intruder Detection System should be considered.

#277 The system shall provide cost-effective linear protections for the perimeter zones.

#278 The systems shall be easy to set-up and install without test equipment and allow remote adjustment of operating parameters.

7.4.2 System Requirements

#279 The PIDS shall provide a continuous monitoring which is at minimum sensitive to vibration, flexing and compression.

#280 The system shall be able to detect the intruder and recognise the type of intrusion - (climbing, digging, breaking, etc)

#281 The fibre shall be mounted on the fence such that it is not visible to people in the unsecured area to avoid damage or theft of the cable.

#282 Tamper detection – the system shall be tamper proof and have tamper detection such that an alarm shall occur if:

a. Any system cabling is cut or shorted;

b. The sensor is rotated or repositioned; or

c. Any housing covers are removed.

#283 System must be fully configurable to be able to properly set the alarm threshold to minimize the potential of false alarms occurring.

#284 The performance of the system shall be unaffected by lightning or other electromagnetic interference.

#285 Controllers shall allow for ease of integration to the Access Control system either via the ACS I/O modules or Babylon system communication protocols (RS485 or Ethernet).

#286 Main controllers of the system shall be housed in the Entrance Plaza server or at Emendi Building server room.

#287 Detection zones shall be matched with perimeter CCTV FoV where available

7.4.3 Field Hardware Controllers

#288 System shall be powered with UPS power (provided by Others) and battery back-up which shall last at least 6 hours.

#289 All outdoor equipment shall be IP66 rated, or at least installed in a field enclosure that complies

#290 Shall be Manufactured from corrosion free materials

#291 Failure of one Controller shall not affect any other.

#292 Perform all the functions of the relevant/related area/s and/or zone/s

#293 These system elements should be mounted such that detection is expected before any components of the system are reached by the intruder.

#294 Controllers and other field devices shall not be mounted on the fence fabric but shall installed in field boxes with tamper protection at a distance from the perimeter.

#295 System shall cater for future expansion.

7.5 Physical Security Information Management (PSIM)/ Situation Management System

7.5.1 General

#296 The Contractor shall engage (or provide) the services of an approved specialist subcontractors and/or OEM's, to be approved by the Employer, as necessary to provide a Situation Management system that is required to incorporate all systems mentioned below to be monitored and controlled from one system.

#297 The system must be designed and optimized to integrate information from the other systems and present the necessary data to the operator to manually or automatically resolve the situation in real time via the system. The Software shall provide the necessary tools for situation management including data collection, verification, analysis, resolution, tracking and reporting.

#298 As a minimum the system shall be integrated or have the capability integrate to with the following systems:

a. ACS

b. CCTV

c. PIDS

d. BMS

e. Visitor Management system

f. Fire Detection and Suppression

g. Intercom

h. UPS and generator

i. Public Address System

#299 The Situation Management system shall be installed with its own server in the Emendi Building server room. Server requirements shall be the same prescribed for the Access Control System.

#300 The system shall be installed for Security Operators on client workstations at the Emendi Building Control Room, New East Entrance Plaza and the existing North Entrance Plaza.

#301 As a preference from Transnet the PSIM system shall be that is South African developed, produced and maintained.

#302 The system requirements shall be as described in the specifications;

a. Transnet Group – Integrated Electronic Security And Related Systems Specification Part-6 Section-22: Physical Security Information Management (PSIM)

b. NMPP Functional Design Specification – Situation Management

#303 Where the above specifications requirements clashes with one another or other related standards used on the project, the Contractor shall notify the Project Manager of such developments.

8 Spares, Tools And Consumables

8.1 General

#304 The Contractor shall provide critical and recommended spares, as prescribed by the OEMs, for all systems, including but not limited to network equipment (switches, SFPs, patch-leads, etc.), CCTV equipment (cameras, power supplies, brackets, etc.) ACS (end-devices, controllers, access cards, etc.), earthing and lighting protection systems (surge arresters and fuses and the like) and any similar installations.

8.2 Spares, Tools and Consumables required prior to Final Handover

#305 The Contractor shall supply all spares that are required for start-up and commissioning purposes and for the 12-month period after commissioning, as recommended by the specialist subcontractors/OEM's.

#306 The Contractor shall also supply all consumables required within 12 months after commissioning and any special maintenance tools, defined as tools that are not readily available from commercial tool suppliers.

#307 Prior to placement of orders, the Contractor shall submit his proposed list of spares, consumables and tools to the Employer for his review and approval.

#308 Each spare part shall be properly tagged with a weatherproof label, showing the manufacturer's unique part number, description of the part and expiry date for parts having a limited shelf life. Small items with the same part numbers shall be tagged and packed together in a plastic bag or box. The tag shall also be shown on the outside of the bag or box.

#309 The cost of the above spares, consumables and tools shall be included in the rates tendered by the Contractor.

8.3 Spares required after Final Handover

#310 The Contractor shall also provide to the Employer a list of all critical and recommended spares as prescribed by the specialist subcontractor/OEMs, which shall cover the operational requirements after final handover of the works. These lists shall include the following:

- Description of spare part.
- Supplier contact details.
- Suggested stock levels.
- Prices.
- Lead-times for ordering and delivery of such spares.

#311 The Employer may issue an instruction to the Contractor to supply and deliver spares for operation and maintenance of the equipment after final handover. Separate payments will be made by the Employer for the provision of such spares.