HIGH LEVEL SCOPE OF WORK

FOR

ASSET PERIMETER SECURITY ENHANCEMENT PROJECT

Table of Contents

1.0 EXECUTIVE SUMMARY

A recent security incident highlighted vulnerabilities in the perimeter security of an SPDC site and a significant change in the background threat picture.
The change in threat prompted a vulnerability assessment and gap-analysis to be conducted for all assets in the Niger Delta; emphasizing the minimum-security standards expected for critical national infrastructure.
The assessment presented an opportunity to re-assess where we are most vulnerable against the current threat picture and re-focus on the measures: we need to ensure our people and assets are safe and secure.
In light of the ongoing drive to deliver value-for-money, three recommendations were endorsed to provide practical minimum standards across 2 areas:

- Improving security – closing the vulnerability gaps, principally with addition Government Security Agency deployments.
- Physically hardening our assets in line with security principles and the layered deter, detect, delay and respond approach.

2.0 GENERAL INFORMATION

This concept design document covers the second improvement tier: focusing on securing key sites' perimeters with dedicated security CCTV, electronic access control and an associated security management and integration system (Genetec) and security control room. Where it is cost-effective to do so during CCTV installation, perimeter lighting should be uplifted where required. The sites nominated for perimeter hardening are: Soku, Gbaran, Okoloma, Imo River, Nun River, and Egbema.
It is SCiNDO's responsibility to deliver the exact quantities with drawings per location.

3.0 PURPOSE

The purpose of this document is to provide NAPIMS with the high level scope of work. It would be used by SPDC Security for project planning, JV transparency, and execution while the design team will utilize it for engineering design.
The document has been populated with key design information and thus sets out the considerations, basic data and guidelines on which the Engineering Design is based.
This document provides descriptions and conceptual specifications for the components that encompass the power supply system, CCTV system, access control, telecommunication devices and cable media for information technology infrastructure system. They are the minimum requirements for the infrastructure features as described within this document.

4.0 SITE OVERVIEW

Site locations:

All measurement lines are conceptual, but broadly denote the required camera / lighting line inside the existing perimeter fence. Quantities are currently a P50 estimate pending Dedicated Engineering Design (DED) completion, required to finalise Material Take-off (MTO) quantities. P50 estimated costs are benchmarked against similar works being undertaken in FOT via the Security Systems Enhancement Project (SSEP).

4.1 Priority 1

Soku

Requirements:

- Dedicated security cameras (mounted on collapsible poles) around measured perimeter

- Jetty oversight surveillance cameras

- Security Control Room

- Personnel access control turnstile

- Backend Security Management system (Genetec)

Estimated Quantities:

Genetec Security Management System (scaleable)	1
Security Control Room	1 build
Perimeter Lighting (poles)	150
CCTV (poles)	40
Entry Control Gate(s)	1 turnstile

Estimated Cost: USD8,380,714.74

Long Lead Items Estimate: USD4,541,953.49

Requirements:

- Dedicated security cameras (mounted on collapsible poles) around measured perimeter

- Jetty oversight surveillance cameras

- Personnel access control turnstile and CCTV coverage

- Automated vehicle gate with access control and CCTV coverage

- Security Control Room

- Backend Security Management system (Genetec)

Estimated Quantities:

Genetec Security Management System (scaleable)	1
Access Controlled Security Control Room	1 room configuration
Perimeter Lighting (poles)	290
CCTV (poles)	80
Access Controlled Entry Control Gate(s)	Entry & Exit Vehicle gates 2 pedestrian turnstiles

Estimated Cost: USD11,174,286.32

Long Lead Items Estimate: USD6,055,937.99

Nun River

Requirements:

- Dedicated security cameras around measured perimeter

- Personnel access control turnstile and CCTV coverage

- Security Control Room

- Backend Security Management system (Genetec)

Estimated Quantities:

Genetec Security Management System (scaleable)	1
Access Controlled Security Control Room	1
Perimeter Lighting (poles)	42
CCTV (poles)	13
Access Controlled Entry Gate(s)	1 turnstile

Estimated Cost: USD2,793,571.58

Long Lead Items Estimate: USD1,513,984.50

4.2 Priority 2

Imo River

Requirements:

- Dedicated security cameras around measured perimeter

- Personnel access control turnstile and CCTV coverage

- Automated vehicle gate with access control and CCTV coverage

- Security Control Room

- Backend Security Management system (Genetec)

Estimated Quantities:

Genetec Security Management System (scaleable)	1
Access Controlled Security Control Room	1
Perimeter Lighting (poles)	92
CCTV (poles)	23
Access Controlled Entry Control Gate(s)	Entry and exit vehicle gates and 2 turnstiles

Estimated Cost: USD4,655,952.63

Long Lead Items Estimate: USD2,523,307.50

Requirements:

- Dedicated security cameras (mounted on collapsible poles) around measured perimeter

- Personnel access control turnstile and CCTV coverage

- Automated vehicle gate with access control and CCTV coverage

- Security Control Room

- Backend Security Management system (Genetec)

Estimated Quantities:

Genetec Security Management System (scaleable)	1
Access Controlled Security Control Room	1
Perimeter Lighting (poles)	100
CCTV (poles)	28
Access Controlled Entry Control Gate(s)	Entry and Exit vehicle gates and 2 turnstiles

Estimated Cost: USD6,518,333.69

Long Lead Items Estimate: USD3,532,630.50

Egbema

Requirements:

- Dedicated security cameras around measured perimeter

- Personnel access control turnstile and CCTV coverage

- Automated vehicle gate with access control and CCTV coverage

- Security Control Room

- Backend Security Management system (Genetec)

Estimated Quantities:

Genetec Security Management System (scaleable)	1
Access Controlled Security Control Room	1
Perimeter Lighting (poles)	50
CCTV (poles)	14
Access Controlled Entry Control Gate(s)	Entry and exit vehicle gates and 2 turnstiles

Estimated Cost: USD2,793,571.58

Long Lead Items Estimate: USD1,513,984.50

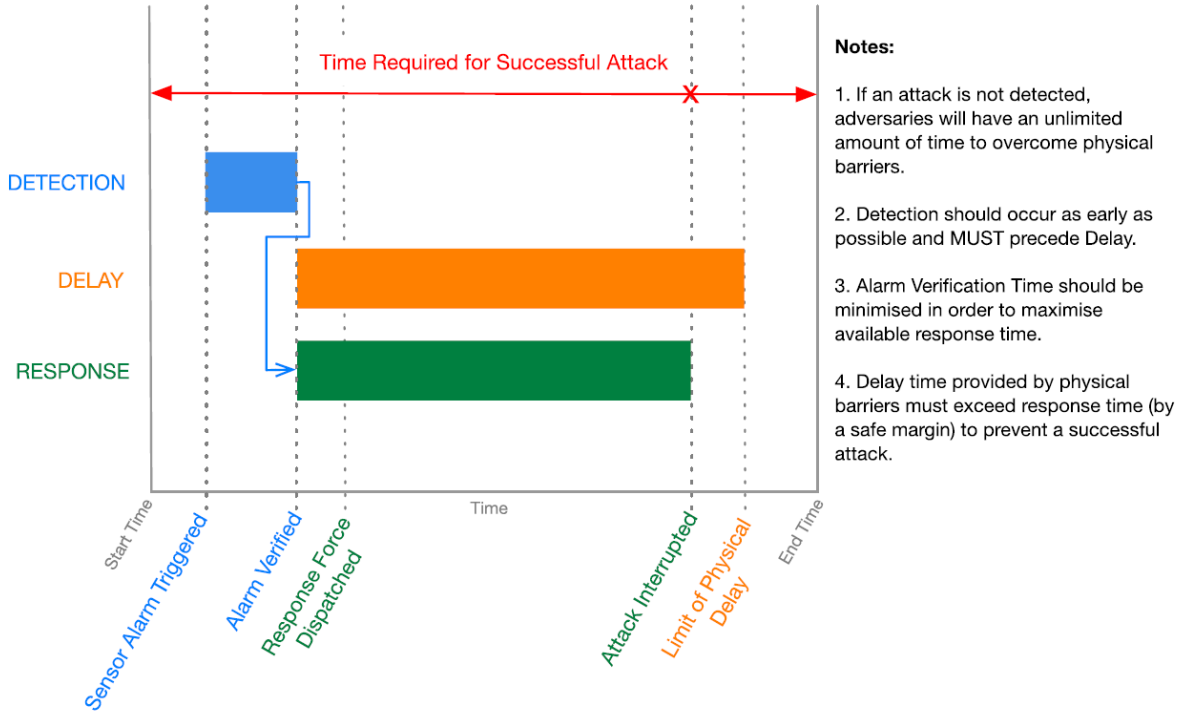
5.0 SCOPE AND CONCEPT
5.1 SCOPE

Design and detailed engineering drawings – Required for Soku, Gbaran, Egbema, Belema, Okoloma, Nun River and Imo River	- Foundations for lighting and CCTV poles around perimeter and entry control point(s) - Pit and ducts or direct bury for required electrical and data conduits (around perimeter, hubbed to TER/Security Control Room)
	- Power to perimeter and entry control point lighting and CCTV - Power to Security Control Room - Potential power uplift in TER for additional servers - Failover supplies: UPS / automatic changeover switch to secondary generator (where applicable)
	- Dedicated perimeter security CCTV camera with motion detection (not FIDS) - Electronic Access Control / POB System (Personnel and [where applicable] vehicle) at primary Entry Control Point(s) and doors to high risk/value rooms/buildings (Control Room/TER) - Enterprise Genetec security management system (integration to the central system) - SCR (screen, consoles, transmission links, structured office cabling) - LAN/WAN/FOC/SOC/Equipment Cabinet and connectivity with PHC IA - Training
	- Addition of effective gates/turnstiles where required - Security Control Room (SCR) – new or nominated room re-design (unless an appropriately sized room can be allocated and modified)

5.2 CONCEPT SELECTED FOR EACH FACILITY

As well as providing a Deterrance, a security system must deliver the requisite level of Detection, Delay and Response (DDR) performance to be effective. If there is a deficiency in any one of these areas, the asset will be vulnerable to successful attack as illustrated in the following diagram:

Figure 1. Detection, Delay and Response Performance



The overall design strategy is summarized as follows:

a. Implement electronic sensors that provide persistent, 24/7 detection coverage of all nominated assets.

b. Provide intelligent video surveillance capable of providing alarm verification and facilitating a rapid response. This implies automated detection, with video analytics providing 'push-alerts' to the security control room.

c. Remove the reliance upon manual Entry Control Procedures by implementing automated barriers and policy-based electronic access control.

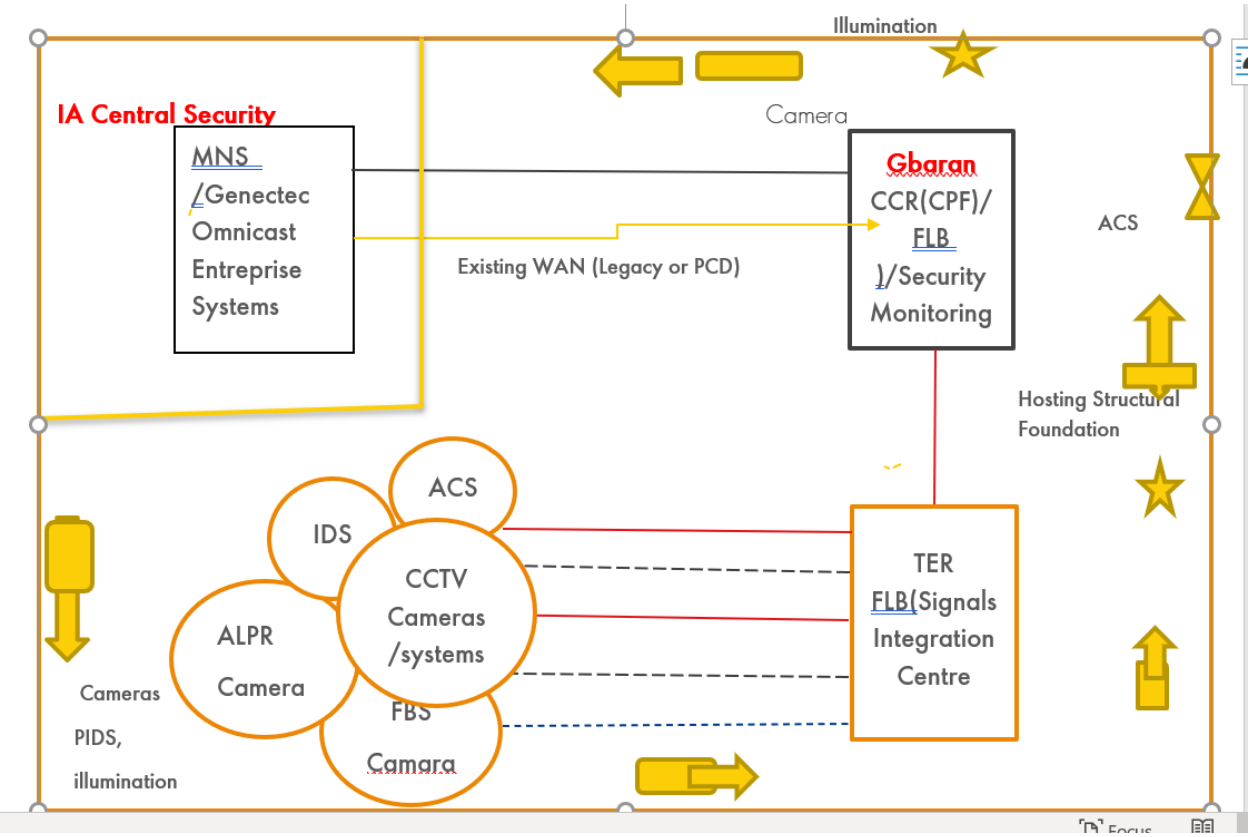
d. Ensure that all personnel and – where applicable – vehicles are authorized to do so.

e. Upgrade and extend existing video surveillance to ensure all vulnerable points are covered.

f. Use additional physical barriers to increase delay time faced by adversaries; providing enough time for a response force to intervene and prevent damage to assets.

g. Implement a robust Command, Control and Communications (C3) capability that allow a rapid, targeted and efficient response to incidents; installing Security Control Rooms (SCRs) at key C3 nodes, with electronic Access Control and centralized POB capability.

6.0 BASIC SCOPE SCHEMATIC



7.0 DESIGN BASIS AND REQUIREMENTS

GENERAL REQUIREMENTS

The project objective is to design the optimal security surveillance system based on industry standard standards and to build a fit for purpose.

In achieving the above objectives, the following sub-objectives will apply:
Design in accordance with the following documents:

- CSDMCSR006 Video Surveillance.docx (shell.com)
- CSDMCSR007 Perimeter Intruder Detection System (PIDS) and Security Fencing.docx (shell.com)
- Shell Standard Scope of Works Security System Integrator Video Surveillance Platform

Due to the revision-state of the corporate guidance above, the following step-outs are endorsed:

- The mandated security management and integration system is Genetec.
- Where an equipment make and model has been specified, the most recent equivalent model must be used.
- As all sites have an existing fenceline, the required sterile zone (demarcated with a secondary fence) is deemed too costly and impractical to deliver to brownfield sites, and is therefore not in scope
- Industry video surveillance guidance dates a 5-6 year lifecycle for associated hardware, after which the system can be considered outdated and a system upgrade or renewal can be initiated.

The Security Systems on the listed facilities shall consist of the following sub-systems:

- Access Control and POB System;
- Closed Circuit Television (CCTV);
- Marine Floating Barriers (where applicable)

PIDS False Alarm Rate (FAR)

False alarms should be minimized in order to maintain operator confidence in the system and ensure genuine alarms are easily identified. Calculated by dividing the number of false alarms by the number of testing days multiplied by the total length of PIDS in Km; industry reference target level is equal to or less than once per kilometer per 24 hours with video alarm verification. The current FIDS system – typically suited to medium risk sites – is often fouled by overgrowth, and also does not provide the required probability of detection.

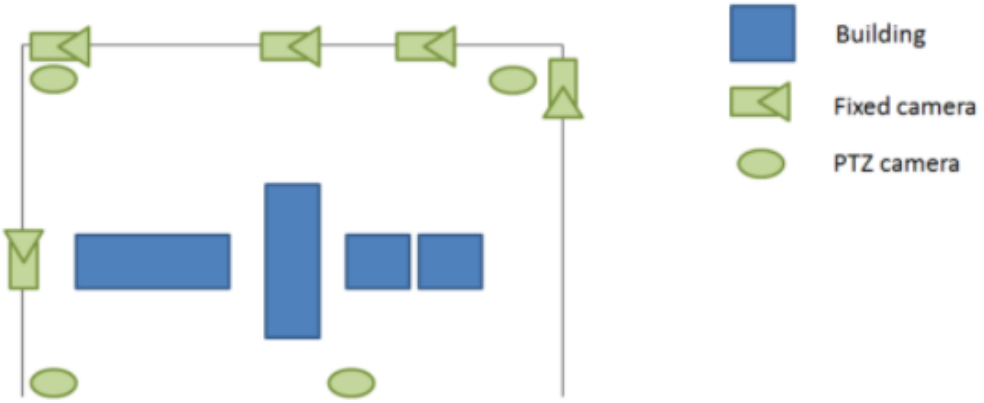
PIDS Probability of Detection (PoD)

In order to provide a reliable and quantifiable level of detection, the required target level for a high risk site is greater than or equal to 95%, and is deemed applicable to the entire perimeter.

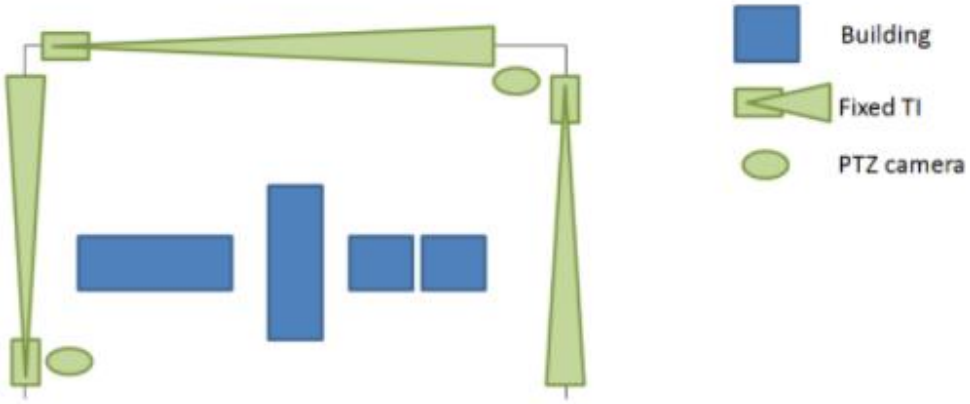
PIDS and Verification Selection

The most suitable PIDS sensor for a high risk site with a single fence is fixed thermal analytics, with video verification provided by pan tilt zoom (PTZ) surveillance cameras. However, such cameras are comparatively costly, and – should one fail – longer areas of fence-line are unprotected pending repair. Consequently, it is assessed that a line of day/night low-light fixed cameras is the preferred option, with thermal cameras used by exception where the topography is unsuitable for the required groundworks.

Fixed and PTZ Camera Layered Security



Use of fixed Thermal Imaging cameras in conjunction with PTZ cameras where it is topographically impractical to install day/night cameras along the fenceline



Security Management and Integration System. As a Corporate Shell requirement, the integrated Security Management System must be Genetec federated security centre (including Shell-imaged Streamvault servers with failover directory, Omnicast enterprise (for CCTV) and 30 days recording capacity, Synergis (access control system), Genetec advantage, Genetec security desk client connection). Genetec must be installed by an accredited integrator

Event-Driven Video and Alarm Management. In addition to providing the main Video Control and Monitoring platform, Genetec will integrate other security systems and devices into a single operator

environment. This allows external alarm sources from all types of security systems to trigger associated video coverage of the alarm to be automatically displayed in the control room, and allow the operator to quickly assess the cause of the alarm and initiate the appropriate response. In this respect video monitoring should be Event-Driven as much as possible, thereby reducing the requirement for manual monitoring of surveillance feeds, increasing operator efficiency and reducing operator fatigue.

Integration with other security systems must include ACS and video analytics

In both cases an alarm or event from these systems should appear in the Operator Console and automatically trigger the associated video cameras to be displayed on alarm monitors in the control room. The VSMS should also provide the capability for automatic pre-alarm and post-alarm recording at maximum frame-rate and resolution, with both the live video stream and of the event and also a play back video of the initial alarm activation, displayed concurrently on the video wall (low/no bezel 55" screens in a 2x2 square block configuration with video wall controller).

At least one black screen should be used for high priority alarms whereby an image is only displayed when the event-driven alarm is triggered.

Illumination

As well as providing a deterrent, a suitably illuminated fenceline allows responding security personnel to check for incursion attempts. The standard for fenceline illumination is an unbroken light corridor of 5 lux (when measured at the darkest point between light sources), with a minimum of 200 lux at site entrances and pedestrian barriers. Where work is required to install CCTV and access control works, lighting should also be uplifted.

Example of good perimeter illumination:

The mounting poles should be a minimum of 2 m inside the perimeter fence to ensure that they do not act as climbing aids to an intruder. If possible, the lighting poles should be pivoted to assist maintenance.

Communications

It is recommended that all security systems data transmission is via a dedicated security LAN installed as part of this project and incorporating the following:

a. Fibre Optic and Ethernet Transmission for camera systems.

b. Failover Core Switches.

c. Encryption and Firewall with Intrusion Prevention.

d. Connection to Shell WAN for remote monitoring.

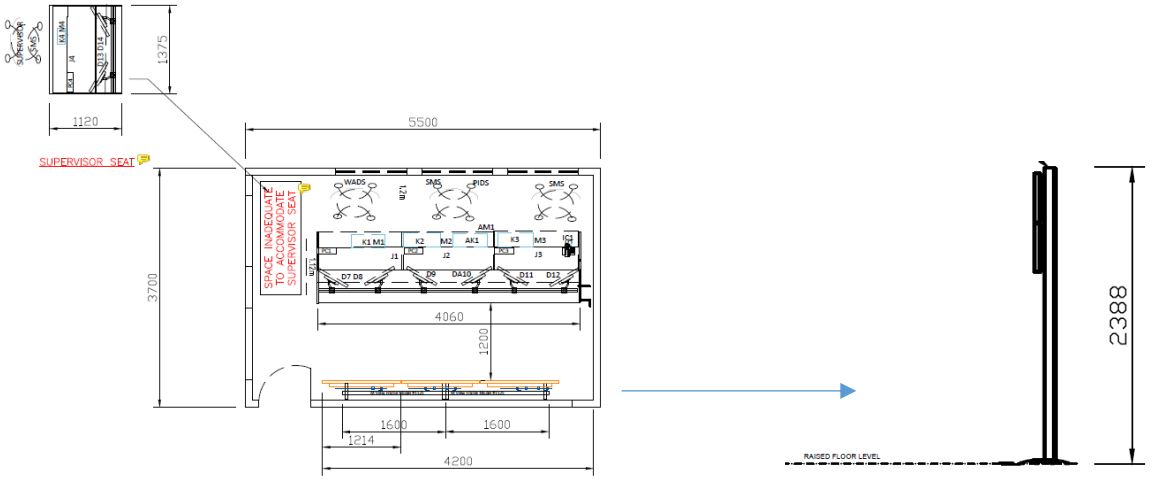
This will ensure that adequate bandwidth and Quality of Service is always available for security systems transmission; as such, the SCR can make full use of high-resolution imagery as part of the detection and monitoring function. Where impractical to deploy fibre, data reach back will be via point-to-point data communications.

Security Control Room (SCR)

The focal point of security sensors and communications will be the security console located as either a dedicated footprint within the Main Control Room or bespoke SCR. If security DSS/Spy already operates out of a dedicated space, it should be considered for modification. Most sites will require a minimum 2-seat option (CCTV/WADS operator and supervisor); however those with a larger access control requirement (generally those with vehicle access) shall require 3-seats (CCTV, ACS and supervisor).

Minimum Dimensions:

While the plan view overleaf depicts 3 desks, one can be removed to fit a side-facing supervisor's desk. Where space is available, the supervisor should sit behind the operator with full view of all displays. All sites shall require the CCTV (middle) desk, and sites with vehicle access shall require a dedicated ACS (right) desk. Regarding wall displays, a 4 x 55" screen display in 2 x 2 configuration is required (rather than 6 in the diagram below); one of which is required as an alert-push display. For height: >2.39m is required above floor level is required on which to mount the screen frame:



a. Associated Workstations must be Shell GID with at least 2-factor identification.

b. The security operator(s) must have visibility of surveillance screens, including camera screens, and wide area overview. Where CCTV is set up for alert detection, a screen should be dedicated for push-alerts. Access Control System summary screen must also be available.

c. All control rooms are restricted areas and should be accessible only to authorised personnel (with electronic access control). Administrators and Operators should have individual log-in and password details, with two-factor authentication: work stations should be GID.

Physical Access Control

Having provided a virtual tripwire around the perimeter, attention must be applied to pedestrian and vehicular access, which is to be considered an extension of the fenceline. Full height turnstiles with electronic access control are required at the entry control point. Also, there must be no option for personnel to bypass the turnstile by walking through the vehicle gates. Consequently, automated full-height vehicle gates (default position closed) are required behind the existing manual gates – this also removes the potential of coercion or collusion with the guard.

Electronic Access Control

The preferred method of access control is biometrics (face or iris), as this considerably reduces the chance of unauthorized access via a stolen, lost or borrowed identity card. However, at the time of publication, a suitable variant has not been identified. Plans should proceed with EV1 card readers, but be forward compatible with biometric technologies. The priority for access control is at the site entry control point(s), however high risk locations (offices, accommodation, control room, TER) should also be protected.

Mustering

The ability to autonomously muster and account for personnel is a critical requirement for managing a serious security/HSE incident. An electronic mustering / POB system shall be provided via mobile handset badge-readers and centralized dashboard.

8.0 INTERFACE WITH CENTRAL SECURITY SYSTEM

The security management system (Genetec) installed at each site shall be able to integrate with the central Omnicast enterprise system at PH I.A.

Where economically practicable, all sites' existing process safety cameras should be integrated with Genetec's Omnicast video management system. However, this requirement is secondary to the main security scope.

9.0 BACKUP INFORMATION - SPECIFICATIONS

Camera Specifications

Camera Type 1. Fixed visible surveillance. Preferred observation of the fence-line using pole-mounted fixed cameras with video analytics to provide 100% detection coverage. Resolution 1080p 25/30fps with Forensic WDR and Lightfinder. Must be installed such that a person occupies more than 10% of screen height (target image height) at any point around the perimeter. Typically mounted on a 6m pivoted lattice tower. Recommended camera is the Axis Q1615 MkIII (or Bosch equivalent) mounted within Ziztel ZCAM6-AXV (non-hazardous area) or ZCAM2-AXV (for hazardous areas) outdoor housings, illustrated below:

Camera Type 2. Where it is impractical to install a line of type 1 cameras along the fence-line, a thermal camera should be used to help ensure a high probability of detection and low false alarm rate. Advantage: longer range; disadvantage: larger sector loss if defective. Type: fixed thermal camera with uncooled VOx microbolometer. Typically mounted on a 6m pivoted lattic tower. Must be installed such that a human target is no less than 3 pixels per meter along its detection axis: capable of 50-600m depending on lens selection. Recommended camera is the FLIR FC-Series mounted within the ZCAM3-TI-669 hazardous outdoor housing, illustrated below:

Camera Type 3. Secondary PTZ Camera for assessment and verification of video analytics alarms, as well as tracking of targets to facilitate a response force to intervene. Enough cameras must be sited to ensure that a person occupies more than 25% of screen height (target image height) at any point around the perimeter. Typically mounted on a 8m pivoted lattice tower; dual mounted with a fixed camera, but top-mounted to ensure 360° coverage. Recommended camera is the Axis Q1615 MkIII (or Bosch equivalent) mounted within a PTZ positioning system (Ziztel ZCAM4 for hazardous areas; ZCAM8 for non-hazardous), illustrated overleaf:

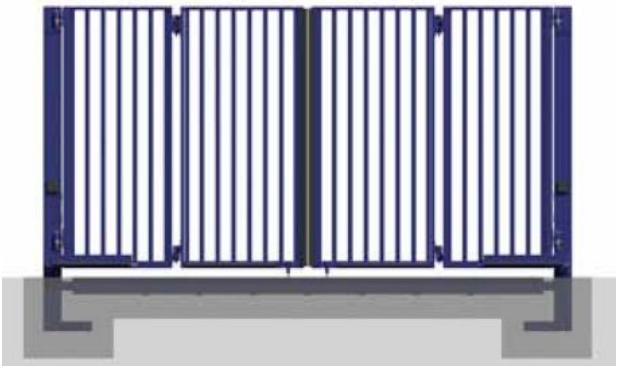
Camera Type 4. Pedestrian Access Control coverage. Fixed dome cameras providing coverage of entry and exit points, located such that a person occupies 100% of screen at doorway/turnstile. Sited above the badging point for face capture. Target resolution of more than 200 pixels per meter. 1080p resolution; min Frame rate 25/30 fps, configured at 12/15 fps during non-alarm conditions. Recommended camera is the Axis Q3515-LVE (or Bosch equivalent), illustrated below:

Camera Type 5. Entry and exit lane fixed Vehicle Overview Camera. Sited such that a vehicle occupies more than 50% of the screen height at barrier. Minimum 1080p resolution, and greater than 100 pixels on vehicle number plate, at a frame rate of at least 25/30 fps. Recommended camera is the Axis P1455-LE IR bullet camera (or Bosch equivalent), illustrated below:

Camera Type 6. Fixed camera coverage of open areas where suspicious activity may occur – identified for coverage of jetty areas (Soku, Gbaran, Belema). Sited such that a person occupies greater than 5% of screen height anywhere in the coverage area. Of note, this should be backed up by a PTZ (type 3) camera for assessment purposes. Recommended camera is the Axis P1447-LE (or Bosch equivalent) network camera with Optimized IR, Forensic WDR and Lightfinder, illustrated overleaf:

Gate 1. Full Height Security Turnstile. A heavy-heavy full-height turnstile should be considered as part of the perimeter fenceline: a galvanized 18-gauge steel physical barrier that allows entry to approved personnel at a rate of 15-20 per minute. The recommended product is the Boon Edam Turnlock 100 (illustrated below) fitted with electronic access control badge readers. Gates are bi-directional, allowing both entry and exit; however in sites with heavy footfall dedicated entry and exit turnstiles should be installed to avoid rush hour congestion. Note that entry and exit points should have dedicated security CCTV coverage (entry and exit) and well lit (at least 200 lux).

Gate 2. Full Height Automated Vehicle Gate. Bi-folding speed gate, ideal for brownfield sites where there is limited area for the gate to open and close (behind the existing manual gate). Required for Egbema, Gbaran, Okoloma and Imo River). Secures apertures up to 10m. Recommended gate is the Frontier Pitts Bi-Folding Speed Gates (basic version illustrated below) with security weldmesh infill; Dutyman MkII actuator and the following safety features: vehicle detector loops, safety photocell beams, traffic lights, flashing beacons and safety edge.



Concept of operation: vehicle passengers must leave the vehicle and proceed through the full height turnstile (covered drop-off and queuing area recommended). The driver activates the gate via a goose-neck stand-mounted badge reader. Camera type 5 should be used to cover entry and exit lanes.

Preventative maintenance schedules and parts should be included in the service level agreement.

Signage. Appropriate signage should be installed at regular intervals along the outer perimeter fence (for example every 50 m). The signage should inform people that it is a restricted area, identify any hazards such as BTC and notify people that video surveillance is in operation:

Through-life maintenance. The four components of capability are Manpower, Equipment, Training and Sustainability. Without a sustainable maintenance programme the capability will fail. A Service Level Agreement support contract is required to coincide with commissioning.

Minimum CCTV maintenance SLA times are as follows:

	Maximum Repair/Replacement Times		Maximum Repair/Replacement Times	
Description	**Low**	**Description**		**Description**
Video Surveillance Management System	24 hours	12 hours	6 hours	2 hours (on-site support)
Individual Cameras and Devices	7 days	5 days	1 day	2 hours (on-site spares)

Minimum Access Control System and associated gate SLA times are as follows:

Requirement	**Maximum SLA Response Time**		
	Medium	**High**	**Very High**
System Outage/Major System Fault	2 days	1 day	12 hours
Minor System Fault	7 days	5 days	2 days
Critical Component Failure/Replacement (Sensor, Assessment Camera)	5 days	2 days	12 hours
Auxiliary Component Failure/Replacement	7 days	5 days	2 days

For MOC: Regular tests should be conducted to ensure that key components are functioning to full specification. Details of tests should be recorded and retained. Camera output should be checked on at least a monthly basis to ensure the quality of imagery. Cameras and any associated wiring

should be made tamper proof with protective covering and tamper alarms employed where available. Cabling connections should be checked regularly, both physically with inspections and electronically to ensure they are performing to specification.

10% of equipment should be procured and made available as ready-use spares.