

 Eskom	<b>Report</b>	<b>Technology</b>
---	---------------	-------------------

Title: **Scope of work for Integrated Security System – Weskusfleur Substation** Unique Identifier: **240-170000066**

Alternative Reference Number: **N/A**

Area of Applicability: **Engineering**



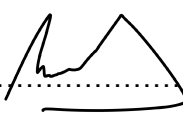
Documentation Type: **Report**

Revision: **1**

Total Pages: **21**

Next Review Date: **N/A**

Disclosure Classification: **CONTROLLED DISCLOSURE**

Compiled by	Functional Responsibility	Authorised by
		
.....	.....	.....
<b>Donald Moshoeshe</b>	<b>Cornelius Naidoo</b>	<b>Richard McCurrach</b>
<b>Engineer- PTMC</b>	<b>Manager - Telecoms T&amp;S CoE</b>	<b>Senior Manager – PTM&amp;C</b>
Date: ...28/05/2020.....	Date: 2020/05/28	Date: 31 May 2020
.....	.....	.....

## **CONTENTS**

	<b>Page</b>
<b>1. INTRODUCTION .....</b>	<b>4</b>
<b>2. SUPPORTING CLAUSES .....</b>	<b>4</b>
2.1 SCOPE .....	4
2.1.1 Purpose .....	4
2.1.2 Applicability .....	4
2.2 NORMATIVE/INFORMATIVE REFERENCES .....	4
2.2.1 Normative .....	4
2.2.2 Informative .....	4
2.3 DEFINITIONS .....	5
2.3.1 Disclosure Classification .....	5
2.4 ABBREVIATIONS .....	5
2.5 ROLES AND RESPONSIBILITIES .....	5
2.6 PROCESS FOR MONITORING .....	6
2.7 RELATED/SUPPORTING DOCUMENTS .....	6
<b>3. PROJECT SCOPE .....</b>	<b>6</b>
3.1 GENERAL SCOPE .....	6
3.2 ACCESS CONTROL SYSTEM (IACS) .....	6
3.2.1 IACS high level devices positioning and architecture philosophy .....	6
3.3 CCTV SYSTEM WITH INTRUDER DETECTION .....	6
3.4 NON-LETHAL ELECTRIFIED FENCE .....	6
3.5 INTEGRATED SECURITY SYSTEM FUNCTIONALITY .....	7
3.5.1 Site Zoning .....	7
3.5.2 Site Zone 1: General area .....	7
3.5.3 Site Zone 2: Support buildings and storage areas .....	8
3.5.4 Site Zone 3: High risk or critical areas .....	8
3.6 ALARMING REQUIREMENTS .....	9
3.7 SITE MONITORING .....	9
3.8 COMMUNICATIONS REQUIREMENTS .....	10
3.9 POWER SUPPLY REQUIREMENTS .....	10
3.9.1 Standby power systems .....	10
3.10 CABLING AND TRENCHING .....	11
3.11 SUPPLIER SERVICES & ORGANISATION EXPERIENCE .....	12
3.11.1 Warrantee and support .....	12
3.11.2 Organisation Experience .....	12
3.12 SYSTEM DESIGN METHODOLOGY .....	12
3.12.1 Functional Design Specification/System Design Report for IACS .....	13
3.12.2 Functional Design Specification/System Design Report for CCTV system with intruder detection .....	14
3.12.3 Functional Design Specification/System Design Report for NLEPDS .....	15
3.12.4 Functional Design Specification/System Design Report for PA system .....	16
3.12.5 Integration Functional Design Specification/System Design Report (Basic Design as per PTM&C SOW) .....	16
<b>4. SYSTEM EVALUATION, DEMONSTRATION AND DESIGN PRESENTATION .....</b>	<b>16</b>
<b>5. DETAIL DESIGN REPORT FOR THE INTEGRATED SECURITY SYSTEM .....</b>	<b>16</b>
<b>6. AUTHORISATION .....</b>	<b>17</b>
<b>7. REVISIONS .....</b>	<b>17</b>
<b>8. DEVELOPMENT TEAM .....</b>	<b>17</b>
<b>9. ACKNOWLEDGEMENTS .....</b>	<b>17</b>
<b>ANNEX A: ALARMING CAUSE AND EFFECT MATRIX .....</b>	<b>18</b>

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

ANNEX B: DETAILED DESIGN REPORT INDEX FOR INTEGRATED SECURITY SYSTEM ..... 20

FIGURES

Figure 1: Generic Access Control system devices interconnectivity ..... 13  
Figure 2: Generic CCTV system devices interconnectivity ..... 14  
Figure 3: Generic electric fence devices interconnectivity ..... 15

TABLES

Table 1: Site Zoning..... 7  
Table 2: Technical Standards for Standby Power Systems equipment ..... 11

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## **1. INTRODUCTION**

This document provides an overview of Eskom's requirements for the design, supply, installation and commissioning of an Integrated Security System at Weskusfleur Substation. The Integrated Security System shall be an integration of the CCTV system with intruder detection, access control system, non-lethal electrified fence/Non-Lethal Energized Perimeter Detection System and public address system. The document outlines design objectives to be fulfilled by the Integrated Security Solution and provides an overview of the envisaged system functionality in addition to the requirements stipulated in the accompanying technical specifications.

## **2. SUPPORTING CLAUSES**

### **2.1 SCOPE**

This scope of work is to be read in conjunction with the High Level Scope of Work – PTM&C Equipment for Weskusfleur Power Station (240-170000104).

#### **2.1.1 Purpose**

The document serves as a technical scope for an integrated security system at Weskusfleur Substation and stipulates technical details and deliverables for the project.

#### **2.1.2 Applicability**

This document is applicable to Weskusfleur Substation.

### **2.2 NORMATIVE/INFORMATIVE REFERENCES**

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

#### **2.2.1 Normative**

- [1] ISO 9001 Quality Management Systems.
- [2] 240-102220945 Specification for Integrated Access Control System for Eskom sites
- [3] 240-91190304 Specification for CCTV Surveillance with Intruder Detection
- [4] 240-86738968 Specification for Integrated Security Alarm System for Protection of Eskom
- [5] 240-86738968 Specification for Integrated Security Alarm System for Protection of Eskom Installations and its subsidiaries
- [6] 240-64720986 Emergency Preparedness Public Address System – For Large Area Deployment
- [7] 240-53114248 Thyristor and Switch Mode Charger, AC/DC to DC/AC Converters and Inverter/Uninterruptible Power Supplies Standard.
- [8] 240-78980848 Specification for Non-Lethal Energized Perimeter Detection System (NLEPDS) for protection of Eskom installations and its subsidiaries
- [9] 240-170000104 High Level Scope of Work – PTM&C Equipment for Weskusfleur Power Station
- [10] 240-170000100 Technical evaluation criteria for the supply of Weskusfleur PTM&C equipment

#### **2.2.2 Informative**

- [11] 240-836884419 PTM&C Technology Development

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## 2.3 DEFINITIONS

Definition	Description
<b>Tender</b>	A tender refers to an open or closed competitive request for quotations / prices against a clearly defined scope / specification.

### 2.3.1 Disclosure Classification

**Controlled disclosure:** controlled disclosure to external parties (either enforced by law, or discretionary).

## 2.4 ABBREVIATIONS

Abbreviation	Description
AC	Alternating Current
CCTV	Closed Circuit Television
DC	Direct Current
DVR/NVR	Digital Video Recorder/Network Video Recorder
GUI	Graphical User Interface
IACS	Integrated Access Control System
TCP/IP	Transmission Control Protocol/Internet Protocol
FAT	Factory Acceptance Test
SAT	Site Acceptance Test
LAN	Local Area Network
MCB	Miniature Circuit Breaker
PA system	Public Address System
PIR	Passive Infrared
PTZ	Pent Tilt Zoom
SAT	Site Acceptance Test
UPS	Uninterruptable Power Supply
WAN	Wide Area Network
NLEPDS	Non-Lethal Energized Perimeter Detection System otherwise commonly known as non-lethal electrified fence

## 2.5 ROLES AND RESPONSIBILITIES

- 1) Tenderers shall use this document together with other accompanying technical documents referenced above when tendering for the Integrated Security System for Weskusfleur.
- 2) Transmission security shall approve standard operating procedures for the whole system which to be provide by the Tenderer.
- 3) The tenderer is responsible for identifying and providing the required training to Eskom personnel to support and operate the system.

### CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## **2.6 PROCESS FOR MONITORING**

Not Applicable

## **2.7 RELATED/SUPPORTING DOCUMENTS**

## **3. PROJECT SCOPE**

### **3.1 GENERAL SCOPE**

This security scope for the project includes additional requirements for an integrated security system comprising of an Access Control System, CCTV system with Intruder detection, Non-Lethal Electrified Fence and PA system. The contractor shall design, manufacture, supply, develop user documentation, perform testing at works, deliver, install, and commission the Integrated Security System and associated equipment (hardware/software etc.) at Weskusfleur Substation according to the associated technical specifications.

**Note 1:** This PTM&C security scope does not include provision of site security during construction.

**Note 2:** The access control building, the local security room, security control room, and the security building shall be considered as the same building as the guard house.

### **3.2 ACCESS CONTROL SYSTEM (IACS)**

Refer to section 16.3 of 240-170000104 for detailed requirements for Access control system.

#### **3.2.1 IACS high level devices positioning and architecture philosophy**

- a) The contractor is required to submit a detailed design depicting the proposed architecture and narratives of how the IACS functional requirements will be achieved. The implemented architecture for IACS should comply with principles outlined in the technical standards for IACS [2] .
- b) In addition to ensuring that the installed system operates as required, the contractor is also required to ensure that the system can be upgraded for remote monitoring and control through the Eskom's WAN in future.

### **3.3 CCTV SYSTEM WITH INTRUDER DETECTION**

- a) Refer to section 16.4 of 240-170000104 for detailed requirements for CCTV system.
- b) Installed cameras to ensure that a continuous visibility is created along the perimeter by eliminating blind spots with one camera having the next camera within its field of view for effective monitoring.
- c) The contractor shall determine the required camera lens types that will ensure that the positioning of the cameras results in the most optimised and economical installation of the cameras at site.

### **3.4 NON-LETHAL ELECTRIFIED FENCE**

- a) Refer to section 16.6 of 240-170000104 for detailed requirements for electrified fence.

**Note:** Please note that the civils and mechanical components requested in 16.6 c) (anti-tunnelling, vegetation control slab, electric fence posts and gate) are to be include in the civil and mechanical design. Only the electrical components of the fence are to be included in the PTM&C security design (i.e. energizers, fence conductor, HT cables, display units, configuration unit, relay cards, gate motors and infrared units).

**CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

### 3.5 INTEGRATED SECURITY SYSTEM FUNCTIONALITY

a) Refer to section 16.9 of 240-170000104 for detailed requirements for integrated system functionality.

#### 3.5.1 Site Zoning

The site shall be zoned as follows:

**Table 1: Site Zoning**

Site Zone/ security level	Description	Area	Security measures
Zone 1	General area	<ul style="list-style-type: none"><li>Weskusfleur Inner perimeter (Open area)</li></ul>	<ul style="list-style-type: none"><li>Access Control on main entrances</li><li>Video surveillance</li><li>PA system</li></ul>
Zone 2	Support buildings and storage areas	<ul style="list-style-type: none"><li>Workshop</li></ul>	<ul style="list-style-type: none"><li>Alarm systems and Passive infrared sensors</li><li>Access Control on access points</li></ul>
Zone 3	High risk or critical areas	<ul style="list-style-type: none"><li>Guard House</li><li>Guard House Equipment Room</li><li>Battery Room</li><li>Carrier Room</li><li>Control building</li></ul>	<ul style="list-style-type: none"><li>Access control measures</li><li>Passive infrared beams</li><li>Video surveillance</li><li>PA system</li></ul>

#### 3.5.2 Site Zone 1: General area

- This is the outside area directly adjacent to the fences are monitored via the perimeter CCTV system.
- CCTV monitoring shall be conducted at the main vehicle entrance as an overview of the area and to serve as identification point for visitors.
- CCTV system to be installed on the perimeter in order to monitor and verify alarms on the fence pre-detection system and energized fence system.
- PTZ CCTV Cameras to be installed at strategic positions on the site and provide a controllable interface from where specific activities can be monitored remotely.
- A PA system shall be installed to communicate remotely and warn possible attackers as a deterrent.
- CCTV video analytics to be utilized as a pre-detection system on the outer perimeter fence.
- An intercom system with an integrated camera shall be installed at the gate as a point of communication between visitors and the site guards in the guard house at site.
- If the site is unmanned (no guards) the following interlocking shall apply: At the site gates entrance area an electronic Access Control reader consisting of a card and fingerprint/card reader shall be installed as initial verification of authorized personnel. Upon positive verification

#### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

all the gates should simultaneously open allowing the vehicle/person to enter the site. The gates should automatically close simultaneously 10 seconds after opening. If an object is detected preventing the gates from closing, an alarm should be triggered. When exiting the site, at the entrance area an electronic Access Control reader consisting of a card and fingerprint reader should be installed as initial verification of authorized personnel. Upon positive verification all the gates should simultaneously open allowing the vehicle/person to exit the site. The gates should automatically close 10 seconds after opening. If an object is detected preventing the gates from closing, an alarm should be triggered

- i) If the site is manned (guards at site) the following interlocking shall apply: An electronic Access Control reader consisting of a card and fingerprint reader shall be installed as initial verification of authorized personnel. Upon positive verification the energized fence gate will open after which the outer barrier gate will open to allow the vehicle inside the sally point. Upon entry into the sally point the outer barrier gate will close effectively locking the visitor in the sally point. At this time the guard will be able to interact with the visitor and conduct searching of the person and vehicle. Only after the guard has completed his duties will the guard exit the sally point at which time the guard has to tag on the inside of the guard house to verify the completion of his activities (The guard in turn will be required to tag on the inner perimeter pedestrian gate to enter the sally point, and then tag out of the sally point and only then tag in the guard house before the system will open, this logic followed will force the guard to enter the sally point and conduct the searching rather than just tagging a visitor in through the guardhouse point) when the visitor on his turn can then again tag in the reader in the sally point (Card reader only). At this time the inner gate will open to allow the visitor into the restricted area. Exiting of the site will be the reverse operation of the entry sequence

### **3.5.3 Site Zone 2: Support buildings and storage areas**

- a) Access control at all access points onto buildings and all buildings use an intrusion detection system which consists of a PIR and Door Contact to verify the status of the room when it is supposed to be unoccupied and subsequently generate an alarm if an intrusion is detected
- b) The intrusion system is to be automatically disarmed upon granting entry to a person through the IAC system and arming upon the exiting of such a person.

### **3.5.4 Site Zone 3: High risk or critical areas**

- a) At the entry points into these areas, biometric and card readers will be utilized as it is restricted areas and only personnel with Permit-To-Work are allowed inside this area. The biometrics is used to enforce this rule.
- b) All buildings shall use an intrusion detection system which consists of a PIR and Door Contact to verify the status of the room when it is supposed to be unoccupied and subsequently generate an alarm if an intrusion is detected. The intrusion system is to be automatically disarmed upon granting entry to a person through the IAC system and arming upon the exiting of such a person.
- c) HV Regulation require that the doors to the battery rooms remain open when occupied, the system will expect this open status and will generate an alarm if a person is detected inside the area even if it is an authorized person as the door is supposed to be in the open position.

**CONTROLLED DISCLOSURE**

- d) Rather than using PIR's to detect movement in the HV Yards, the CCTV system's Video Motion Detection System (VMD) will be utilized to perform the task as the area is too dangerous for the installation of PIR's. The VMD will function as the Intrusion detection system in this area. Two PTZ CCTV Cameras should be setup in a manner so as to sweep the respective fields of view in "patrol" mode and should generate alarms by utilizing Video Motion Detection.

### **3.6 ALARMING REQUIREMENTS**

- a) The alarming of the installed Integrated Security System shall form part of the disparate security systems installed at site to provide proactive coverage and monitoring of all protected areas i.e. Site perimeter, entrances, control room, HV yard and other strategic places within the protected site. The alarming shall be triggered by the following inputs:
- i. Due to Camera video analytics alarm detection on the zone(s)
  - ii. Alarm inputs from electric fence
  - iii. Alarm inputs from indoor Intrusion detection devices
  - iv. Alarm inputs from access control points
- b) The alarming of the system shall comply with alarming requirements of the disparate integrated technologies mentioned above, forming part of the integrated security system at site.
- c) The contractor is required to include the alarming functionality with the submitted detailed design including how the envisaged alarming will be achieved through integration of the disparate security technologies mentioned above.
- d) The alarming cause an effect matrix shall be as tabled in Annex A.

### **3.7 SITE MONITORING**

- a) There shall be a security manager workstation in the security building for local allocation and revoking of access rights and controlling of security workflows.
- b) There shall be a maintenance manager workstation in the security building for controlling of maintenance workflows.
- c) Some or all of the functions listed in item 1 and 2 above may be combined into a single physical workstation. The workstation software GUI shall be based on the operator log on credentials to be able to perform functions listed in item 1 and 2 above.
- d) The security alarms should be routed to zero control through the SCADA system. The system shall be scalable and have the capability of sending alarms and CCTV visuals to the remote off-site Security Control Centre and/or third party security Reaction Company (future).
- e) The system shall allow the Security Control Centre to be able to remotely control PTZ cameras at site (future).
- f) The system shall allow the remote Security Control Centre to have audio (via PA system) and data communication with the site. Including the ability to give audio warnings to over the PA system to the fence zone that detected an intrusion. (future)
- g) It shall be possible for the Security Control Centre to remotely request any of the stored event data or video streams in real time (future).

**CONTROLLED DISCLOSURE**

### **3.8 COMMUNICATIONS REQUIREMENTS**

- 1) IP based communication shall be supported for on-site communication.
- 2) The network shall provide redundancy in the event of path failure.
- 3) Single mode optical fibre is preferred as the physical transport medium of choice for on-site communication.
- 4) For indoor connections and outdoor connection distances below 5m, CAT5 or CAT6 UTP copper cable may be used.
- 5) The detailed design shall include the security LAN design used to facilitate communications between security system elements.

### **3.9 POWER SUPPLY REQUIREMENTS**

- 1) Back-up power shall be provided to power all security equipment in the event that primary power is lost (recommended standby time is 12 hours).
- 2) The security system shall be powered by AC supplied from the site's AC supply with an appropriately sized Uninterruptible Power Supply (UPS).
- 3) The UPS shall comply with the requirements of Thyristor and Switch Mode Charger, AC/DC to DC/AC Converters and Inverter/Uninterruptible Power Supplies Standard [5].
- 4) Power shall be distributed through the panel, so as to isolate the supply of the subsystems by means of appropriately sized MCBs. At a minimum, the following will be on separate supply circuits:
  - i. Perimeter Cameras
  - ii. Indoor cameras
  - iii. PA system devices
  - iv. Site controllers and server based equipment
  - v. Other security related equipment such as gate motors and electric fence energizers.
- 5) The system shall have a power failure indication that shall be sent through to the remote security control room (via SCADA alarm) should the AC supply be interrupted.

#### **3.9.1 Standby power systems**

The standby power systems requirements for security systems at Eskom sites shall comply with the following:

- a) The system design shall comply with the requirements of 240-91190294, DC & Auxiliary Supplies Philosophy.
- b) Security systems are required to ensure that the site is protected at all times, hence the standby time of these systems shall be in line with the overall required standby time for the site. The requirements of 240-118870219, Standby Power Systems Topology and Autonomy for Eskom sites, shall be adhered to.
- c) Standard or technically acceptable equipment shall be used. This equipment is available on Eskom National Contracts (ENCs) or recommended technically acceptable equipment lists.
- d) In the absence of ENCs for specific equipment or recommended technically acceptable equipment, the offered equipment shall comply with the technical standards as indicated in Table 2 below:

**CONTROLLED DISCLOSURE**

**Table 2: Technical Standards for Standby Power Systems equipment**

<b>Equipment</b>	<b>Technical Standard</b>
Nickel Cadmium Batteries	240-56360086, <i>Stationary Vented Nickel Cadmium Batteries Standard</i>
Vented Lead Acid Batteries	240-56360034, <i>Stationary Vented Lead Acid Batteries Standard</i>
Valve Regulated Lead Acid Batteries	240-51999453, <i>Standard Specification for Valve-Regulated Lead Acid Cells</i>
Power Electronics	240-53114248, <i>Thyristor and Switch Mode Chargers, AC/DC to DC/AC Converters and Inverter/Uninterruptible Power Supplies Standard</i>
Low Voltage Protective Devices, Cubicles and wiring	240-64139144, <i>AC Boards and Junction Boxes for Substations</i> 240-76628687, <i>AC/DC Reticulation Equipment for Breaker-and-a-Half Substations</i> 240-75658628, <i>Distribution Group's Specific Requirements for AC/DC Distribution Units</i>

### **3.10 CABLING AND TRENCHING**

- 1) The contractor shall provide detailed as built drawings indicating cable routes, installation locations of all equipment as part of the detailed design submission.
- 2) The contractor will be responsible for laying and terminating the cable from the peripheral devices to the control room.
- 3) Data and low voltage cable installations shall be separated from the mains power installations by a minimum of 500mm.
- 4) Where data and low voltage cabling has to cross power cabling, this shall always be at 90°
- 5) All wiring shall be concealed inside trunking or conduit. No exposed wiring will be accepted.
- 6) Cable runs next to devices that may cause electro-magnetic interference shall be avoided or suitable shielding provided.
- 7) Tension when pulling cables shall not exceed recommended safe values as specified by the cable manufacturers.
- 8) Supply and installation of all trunking, conduit, glands etc. form part of the contractor's scope of work.
- 9) Cable joints shall be avoided as far as practically possible.
- 10) An industry acceptable Source, destination cable marking system shall be used to mark all cables.

#### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

### **3.11 SUPPLIER SERVICES & ORGANISATION EXPERIENCE**

#### **3.11.1 Warrantee and support**

At minimum the Tenderer shall provide the following services as part of system(s) life cycle management:

- a) The system shall carry a minimum local (South African) warranty of 36 months with on-site, as well as telephonic, support from the date of the system being commissioned. After that, Eskom shall have the option to access ongoing support in terms of a subsequent agreement.
- b) The supplier must have a technician on call on a 24-hour basis for purposes of telephonic support.
- c) Supplier spares holding should include minimum replacement spares to restore service of the system in its entirety.
- d) All support shall also include all firmware upgrades of the initial system version installed over the operational life of the system.
- e) The support shall include first-line-level maintenance training.
- f) The supplier shall also provide operator training on site to the end user.
- g) Product support must include national, as well as international, support through the local branch.
- h) The supplier shall be willing to enter into an SLA with Eskom.
- i) The supplier should have a history of supplying products of this nature in South Africa for a minimum period of five years.
- j) The supplier is to provide a list of reference sites where the product on offer has been installed and the year of implementation.

#### **3.11.2 Organisation Experience**

- a) Tenderer must submit company organogram, indicating team composition(s).
- b) List of similar projects must be provided.
- c) CVs for the company and staff must be submitted with the following experience / competencies:
  - i. Experience in designing and installation of Access Control systems.
  - ii. Experience in designing and installation of CCTV systems.
  - iii. Experience in designing and installation of PA systems
  - iv. Experience in design and installation of NLEPDS (A registration Certificate with department of Labour for Electric Fence System Installer must be submitted).
  - v. Experience designing integrated security systems
  - vi. Experience and in TCP/IP networks.

### **3.12 SYSTEM DESIGN METHODOLOGY**

The methodology provides a framework to ensure that functional requirements for the security systems are incorporated in the system design as per Eskom's Technology Development standard and the technical standards.

**CONTROLLED DISCLOSURE**

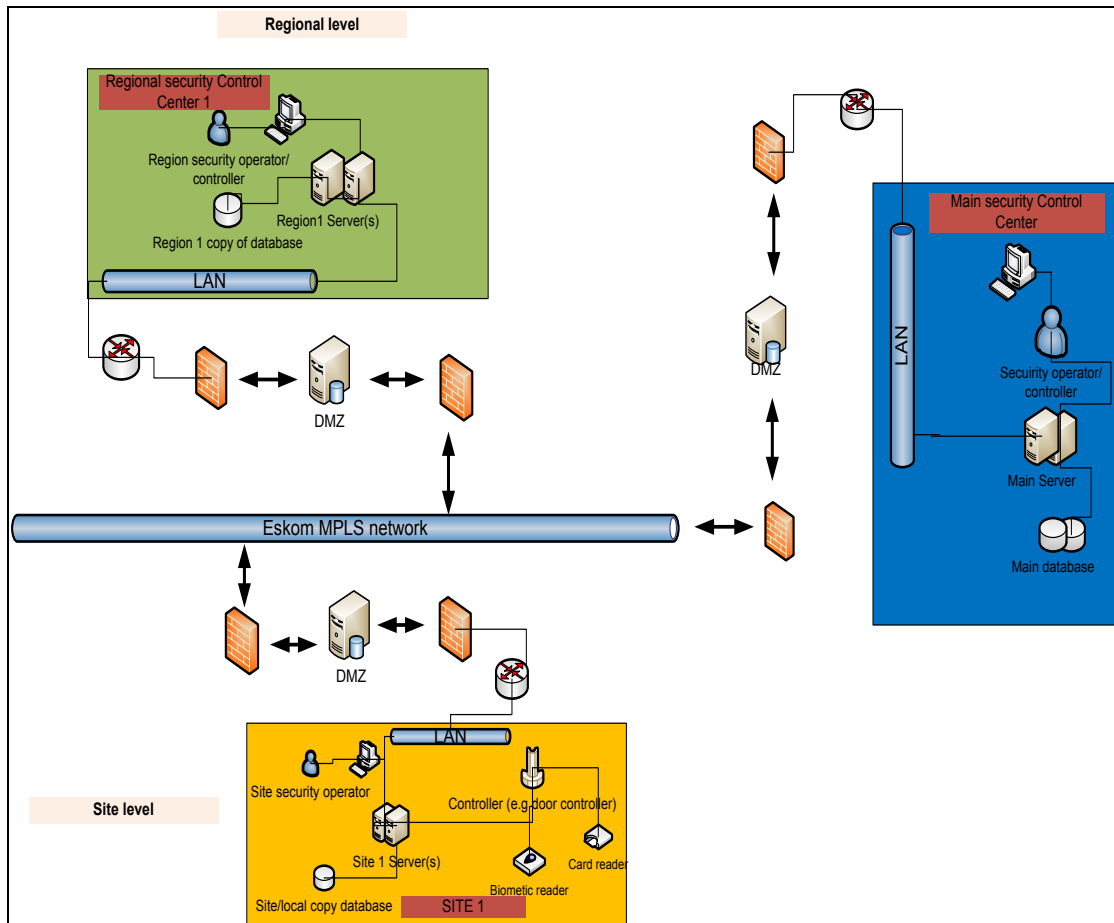
The tenderer is required to produce and submit Functional Specifications and a System Design Reports. The Functional Specification details Eskom's functional requirements in the context of the products that are offered by the Tenderer. The System Design Report documents the design that has been developed in order to meet the requirements as specified in the Functional Specifications and the scope of work.

*Note 1: The Functional Specifications and the System Design Reports can be combined as one document (Basic design as per PTM&C SOW).*

*Note 2: The diagrams depicted below are not the detailed designs of the required systems; they are generic representation of device interconnectivity to guide the designs. The Contractors are required to submit detailed schematics depicting detailed designs for the proposed systems.*

### 3.12.1 Functional Design Specification/System Design Report for IACS

The tenderer is required to produce and submit a Functional Specification and a System Design Report for the Integrated Access Control System (IACS). At minimum, the System design report shall cover the functional and interconnection details of system components as depicted in Figure 1 below:



**Figure 1: Generic Access Control system devices interconnectivity**

As per the figure above, at minimum the Functional Design Specification and System Design Report shall cover the functional and interconnection details of system components below in line with the standard for IACS and the scope of work.

- a) Servers
- b) Clint stations

**CONTROLLED DISCLOSURE**

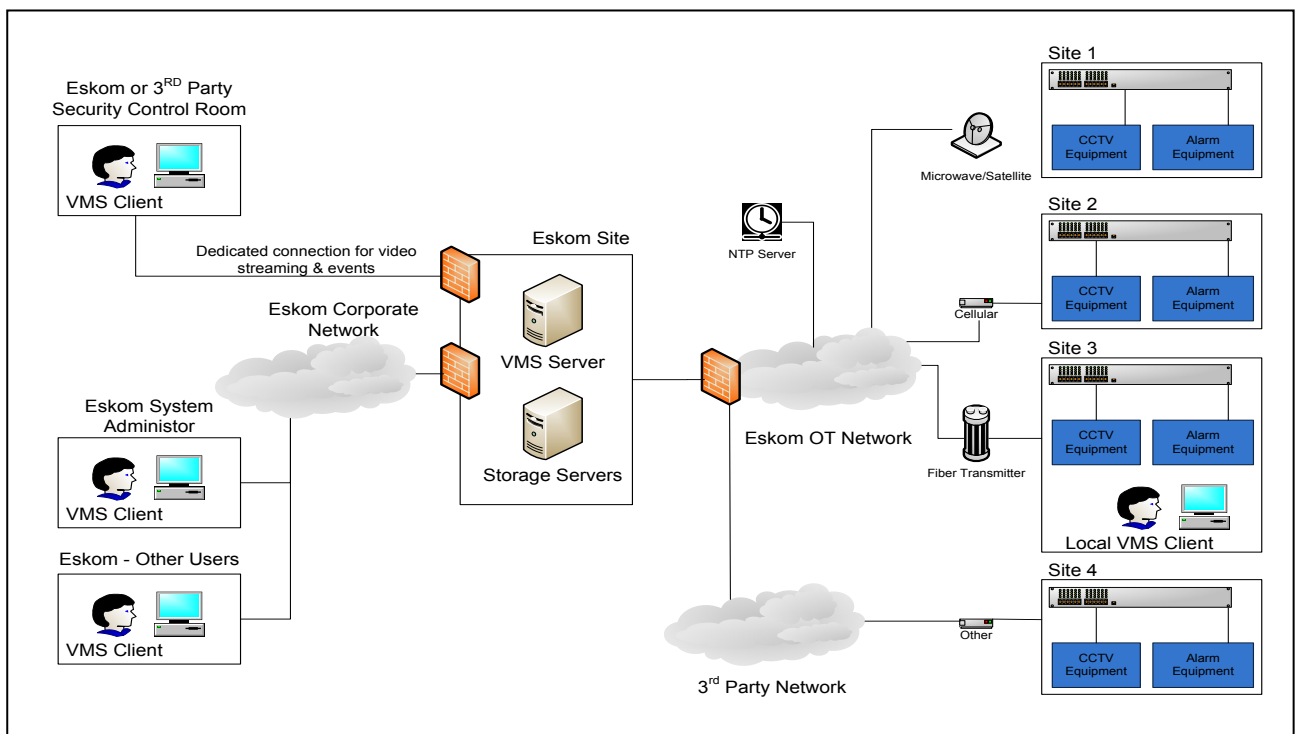
When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

- c) Communication and networking infrastructure (for local and remote communication)
- d) Card readers and biometric readers
- e) Controllers
- f) Graphical User Interface details
- g) System Alarming capability
- h) Power supply details
- i) Cabling details (communication and power cables)

*Note: For this project the scope is only limited to site level deployment, but the system shall be designed to be scalable to allow remote monitoring and control without any reengineering.*

### 3.12.2 Functional Design Specification/System Design Report for CCTV system

The tenderer is required to produce and submit a Functional Specification and a System Design Report for the CCTV system with intruder detection. At minimum, the System design report shall cover the functional and interconnection details of system components as depicted in Figure 2 below:



**Figure 2: Generic CCTV system devices interconnectivity**

As per the figure above, at minimum the Functional Design Specification and System Design Report shall cover the functional and interconnection details of system components below in line with the standard for CCTV system and the scope of work document.

- i. Cameras (indoor cameras, perimeter cameras and PTZs)
- ii. DVR/NVR including recording and streaming details
- iii. System Servers

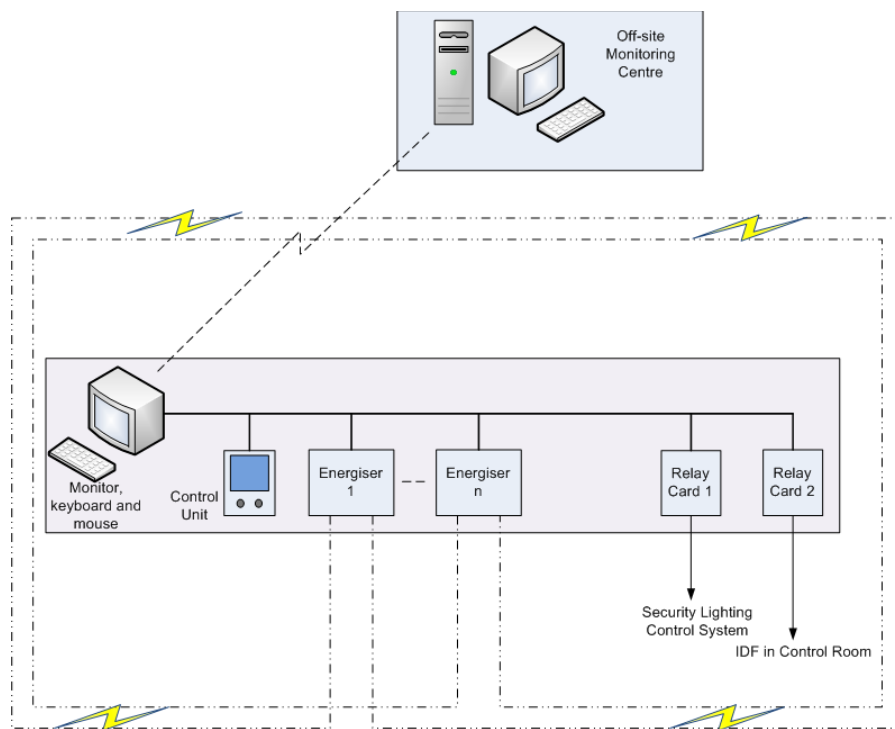
**CONTROLLED DISCLOSURE**

- iv. Communication and networking infrastructure (for local and remote communication)
- v. System Alarming capability
- vi. Power supply details including power backup
- vii. Cabling details (communication and power cables)
- viii. Video storage details
- ix. System Bandwidth details

*Note: For this project the scope is only limited to site level deployment, but the system shall be designed to be scalable to allow remote monitoring and control without any reengineering.*

### **3.12.3 Functional Design Specification/System Design Report for NLEPDS**

The tenderer is required to produce and submit a Functional Specification and a System Design Report for the Non-lethal energized perimeter detection system. At minimum, the System design report shall cover the functional and interconnection details of system components as depicted in Figure 3 below:



**Figure 3: Generic electric fence devices interconnectivity**

As per the figure above, at minimum the Functional Design Specification and System Design Report shall cover the functional and interconnection details of system components below in line with the standard for NLEPDS system and the scope of work.

- a) Electric fence conductors
- b) Power supply
- c) Configuration PC / Controller
- d) User interface / Display unit
- e) Synchronising equipment/mechanism

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

- f) Relay cards
- g) Communication infrastructure
- h) Energizer(s)

The Tenderer shall submit the compliance certifications for the following standards for verification of system compliance for acceptance testing:

- i. SANS 60335-2-76

*Note: The Functional Specification and the System Design Report shall cover only the electrical and electronic functionality. This scope excludes Anti-tunnelling, vegetation control slab and erection of pole, this will be provided by the civil contractor and a detailed drawing will be provided for the civils and mechanical installations.*

### **3.12.4 Functional Design Specification/System Design Report for PA system**

The tenderer is required to produce and submit a Functional Specification and a System Design Report for the Public Address (PA) system. At minimum, the System design report shall cover the functional and interconnection details of system components below in line with the standard for PA systems and:

- i. routers
- ii. modems
- iii. switches
- iv. patch panels
- v. speakers
- vi. Management system computer & monitors

*Note: For this project the scope is only limited to site level deployment, but the system shall be designed to be scalable to allow remote monitoring and control without any reengineering.*

### **3.12.5 Integration Functional Design Specification/System Design Report (Basic Design as per PTM&C SOW)**

- a) The tenderer is required to produce and submit an Integration Functional Specification and a System Design Report covering the integration of the disparate systems above into a unified security solution.
- b) Refer to section 16.9.1 for detailed requirements for the integration functional specification/system design report.

## **4. SYSTEM EVALUATION, DEMONSTRATION AND DESIGN PRESENTATION**

- a) Evaluations will be conducted as per 240-170000100.
- b) The appointed contractor will be required to demonstrate how the different functional and technical requirements have been incorporated in the proposed design as part of FAT and SAT tests. FAT and SAT procedures shall be provided by the Contractor for Eskom's review (minimum tests as per section 3.16 of Eskom spec 240-91190304).

## **5. DETAIL DESIGN REPORT FOR THE INTEGRATED SECURITY SYSTEM**

- a) The detail design report shall contain requirements as per the index in Annexure B.

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## **6. AUTHORISATION**

This document has been seen and accepted by:

<b>Name &amp; Surname</b>	<b>Designation</b>
Richard McCurrach	Senior Manager – PTM&C
Cornelius Naidoo	Manager - Telecommunications Technology and Support
Tony Sheerin	Manager – Project Planning and Support

## **7. REVISIONS**

<b>Date</b>	<b>Rev.</b>	<b>Compiler</b>	<b>Remarks</b>
May 2020	1	R Moshoeshoe.	First issue

## **8. DEVELOPMENT TEAM**

The following people were involved in the development of this document:

## **9. ACKNOWLEDGEMENTS**

Not applicable

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

### ANNEX A: ALARMING CAUSE AND EFFECT MATRIX

	Unauthorised Access					Authorised Access
	Breach physical perimeter fence or virtual perimeter fence by smart cameras/beams/etc.	Outdoor Sensor Triggers	Camera Outdoor Protected Area Triggers	Indoor Sensor Triggers	Camera Indoor Protected Area Trigger	
Perimeter flood lights activated at night only	✓					
Substation flood lights activated at night only	✓	✓	✓	✓		
Security floodlights activated at night only	✓	✓	✓	✓		
Control Room lights 24hr				✓	✓	
Switch Room lights 24hr				✓	✓	
Any other indoor room				✓	✓	
DVR/NVR record footage	✓	✓	✓	✓	✓	✓
Alarm signals(text and video) sent to Security Control Centre	✓	✓	✓	✓	✓	

**Scope of work for Integrated Security System-  
Weskusfleur Substation**

Unique Identifier: **240-170000066**

Revision: **1**

Page: **19 of 21**

	Unauthorised Access					Authorised Access
	Breach physical perimeter fence or virtual perimeter fence by smart cameras/beams/etc.	Outdoor Sensor Triggers	Camera Outdoor Protected Area Triggers	Indoor Sensor Triggers	Camera Indoor Protected Area Trigger	
PTZ tracking sent to Security Control	✓	✓	✓			
PA System recorded message activated	✓			✓	✓	
PA System Security Control operated if positive alarm verified	✓	✓		✓	✓	
Alarm System Zones triggered	✓	✓	✓	✓	✓	
Alarm Zone events sent to Security Control	✓	✓	✓	✓	✓	
Indoor Siren automatically activated				✓		
Strobe light automatically activated	✓	✓	✓	✓	✓	

## **ANNEX B: DETAILED DESIGN REPORT INDEX FOR INTEGRATED SECURITY SYSTEM**

1. Overview of functional specification
2. Scope of work
3. High Level Integration
  - a. Local vs remote monitoring and control capabilities
  - b. Software and network config files.
  - c. Cause and effect matrices (e.g. if alarm on fence, lights and image sent to control)
4. System Architecture ( to include Logical and physical design, networking and bandwidth requirements, Information flow, Physical security information management, User access profile management and enrolment process, cyber security controls e.g. firewalls, DMZ, System support remote access authentication etc.)
5. Lifespan of System and product software versions (include 10 year life span support)
6. Recommended Maintenance (Procedures, Spares and FMECA- Failure mode effects and criticality analysis, tools and test equipment, training requirements-engineering and field operations)
7. System commission and acceptance testing procedure (commissioning results to be provided prior to system handover (minimum tests as per section 3.16 of Eskom spec 240-91190304).
8. Appendix A – Drawings
  - Site layout
  - CCT Field of view
  - Site Security Zoning
  - System Configuration
  - Security LAN and Fibre Reticulation
  - Cable and trench layout
  - Power reticulation
  - Control Panels
  - Electric fence and energiser
  - Kimberly control drawings/configuration
9. Appendix B – Equipment Specification
  - Access Control & Intrusion Detection
  - Camera Surveillance System
  - Alarm System (if it is a separate controller)
  - Lighting Control System ( if it is a separate controller)
  - PA system (if it is a separate controller)
  - Electric fence and Energiser (If it is a separate controller)
  - Physical security information management
  - Data storage equipment on site and at Kimberly
10. Appendix C – Datasheets
  - Access Controllers
  - Card Readers
  - Biometric Readers
  - Maglocks
  - Break Glass Units

### **CONTROLLED DISCLOSURE**

- Door Contacts
- PIR Sensors
- Power Supplies (including UPS sizing)
- Intercoms
- Cameras
- Video Recorders
- Client Workstations
- Network Switches
- Fibre Converters
- Enclosures & Racks
- PA systems
- Security LAN and firewalls

11. 10 Appendix C- Bill of Materials