Eskom	Standard	Technology

Title: **SPECIFICATION FOR INTEGRATED SECURITY ALARM SYSTEM FOR PROTECTION OF ESKOM INSTALLATIONS AND ITS SUBSIDIARIES**

Unique Identifier:	**240-86738968**
Alternative Reference Number:	**<n/a>**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**2**
Total Pages:	**36**
Next Review Date:	**August 2025**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Donald Moshoeshoe	**Prince Moyo**	**Dr Titus Mathe**
Engineer	**General Manager: Power Delivery Engineering**	**General Manager: Asset Management**
Date: 22/07/2020	Date: 3/08/2020	Date: 03 August 2020

Supported by SCOT/SC

Richard McCurrach

PTM&C TC Chairperson

Date: 22 July 2020

PCM Reference: **240-43542545**

SCOT Study Committee Number/Name: **: Part 16 – DC & Auxiliary Supplies**

Content

Page

1. Introduction 4
2. Supporting clauses 4
   - 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 5
   - 2.3 Definitions 5
     - 2.3.1 General 5
     - 2.3.2 Disclosure classification 5
   - 2.4 Abbreviations 5
   - 2.5 Roles and responsibilities 6
   - 2.6 Process for monitoring 6
   - 2.7 Related/supporting documents 6
3. General 6
   - 3.1 General requirements 7
   - 3.2 Operating conditions 7
     - 3.2.1 General operating conditions 7
     - 3.2.2 Resistance to corrosion 7
     - 3.2.3 Environmental tests 7
4. Operational requirements 8
   - 4.1 System integration 8
     - 4.1.1 Alarm triggers 8
     - 4.1.2 Integration with PA system 8
     - 4.1.3 Integration with pre-detection sensors 8
     - 4.1.4 Integration with panic buttons 8
     - 4.1.5 Integration with security lighting 9
     - 4.1.6 Integration with other electronic security systems 9
     - 4.1.7 Arming and Disarming system 9
     - 4.1.8 Unauthorized access 9
     - 4.1.9 False or Nuisance alarm 9
     - 4.1.10 Integrated Alarm management 10
   - 4.2 The integrating system / controller shall: 10
   - 4.3 Alarms and indications 11
   - 4.4 Monitoring and Control 11
5. Electrical requirements 11
   - 5.1 Power Supply 11
   - 5.2 Communication 12
   - 5.3 Electrical safety 12
6. Physical requirements 13
   - 6.1 General construction requirements 13
   - 6.2 Tamper protection 13
   - 6.3 Physical safety 13

7. EMC 13
8. Noise 14
9. Cyber security 14
10. Earthing 14
11. Functional requirements for pre-detection sensors 14
12. System life-cycle 14
13. Warranty and support 14
14. Markings, Labelling and packaging 15
15. Documentation and drawings 15
16. Testing 16
17. Authorization 16
18. Revisions 16
19. Development team 16
20. Acknowledgement 16
Annex A – Alarm system cause and effect matrix 17
Annex B – Technical Schedule A&B 19

Tables

Table 1: Technical Standards for Standby Power Systems equipment 12

1. Introduction

The aim of this standard is to prescribe the minimum requirements for security alarm system that Eskom and its subsidiaries shall comply with to protect its installations.

2. Supporting clauses

2.1 Scope

This document outlines the requirements to be complied with for security alarm system for Eskom installations and its subsidiaries.

2.1.1 Purpose

This standard is a technical document that specifies functional, operational performance and other technical requirements that shall be met to meet the requirements of security alarm system for the protection of Eskom installations.

2.1.2 Applicability

This specification shall apply throughout Eskom Holdings Limited, its divisions, subsidiaries and entities wherein Eskom has a controlling interest.

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

The following documents contain provisions that, through reference in the text, constitute requirements of this specification. At the time of publication, the edition indicated was valid. All controlled documents are subject to revision, and parties to agreements based on this specification are encouraged to investigate the possibility of applying the most recent edition of the documents listed below. Information on currently valid national and international standards and specifications can be obtained from the Information Centre and Eskom Documentation Centre at Megawatt Park.

[1] ISO 9001, Quality Management Systems.

[2] SANS 2220-2-1 Electrical security systems, Part 2-1: Access control systems: General characteristics

[3] SANS 2220-1-1 Electrical security systems, Intruder alarm systems – General requirements

[4] SANS 2220-1-7 Electrical security systems, Electrical alarm systems: Power units

[5] SANS 2220-2-2 Electrical security systems, Access control systems - Central processor

[6] 240-83684419 PTM&C Technology development

[7] 240-102220945 Specification for Integrated Access Control System (IACS) for Eskom sites

[8] 240-78980848 Specification for Non-lethal Energized Perimeter Detection System (NLEPDS) for protection of Eskom installations and its subsidiaries

[9] 240-139282493 Security lighting for Eskom applications

[10] 240-106871262 Security systems technologies roadmap

[11] 240-170000098 Security public address system for substations and Telecoms high sites

[12] 240-170000096 Physical security integration standard

[13] 240-91190304 Specification for CCTV surveillance with intruder detection

[14] 240-55410927 Cyber Security Standard For Operational Technology

[15] 240-68111223 Goods information: standard networking devices for the substation environment standard

[16] 240-146054527 Information and Communications Technology Network Security Framework

[17] 240-70732888 Fibre optic cable system acceptance testing

[18] 240-94136376 IP voice and data network design guide

[19] 240-170000086 Roles and Accountabilities for Lifecycle Management of Physical Security Systems in the Transmission Division

2.2.2 Informative

None

2.3 Definitions

2.3.1 General

Definition	Description
Integrating System/ Controller	Component of the Alarm system responsible for integrating and controlling the functioning of the alarm system and its subsystems.
Local controller	A person that is locally situated at a protected side at the Access Control Building who is responsible for controlling the system.
Remote controller	A person that is situated at a remote security control centre who is responsible for controlling the system.

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
A	Ampere
AC	Alternating current
CCTV	Closed-Circuit Television
DC	Direct Current
DVR	Digital Video Recorder
EMC	Electromagnetic Compatibility
h	Hours
HV	High Voltage
I/O	Input/output
ICASA	Independent Communications Authority of South Africa
IP rating	Ingress Protection rating
MTBF	Mean Time Between Failures

Abbreviation	Description
A	Ampere
PA system	Public Address system
PC	Personal Computer
PTZ	Pan – Tilt - Zoom
SANS	South African National Standards
SCADA	supervisory control and data acquisition
V	Volts

2.5 Roles and responsibilities

a) The Security Technologies Care Group shall ensure that the technology developed is adequate for application across Eskom sites where it will be utilized.

b) Group security shall be responsible for auditing to ensure compliance with the requirements of this standard.

c) The procurement team shall utilise this document for the enquiry process and during the product development phase.

d) Substation Maintenance personnel shall be responsible for maintenance of equipment as per the standard.

2.6 Process for monitoring

Security Technologies care group shall ensure that this standard remains up to date.

2.7 Related/supporting documents

Not applicable.

3. General

The alarm system forms an integral part of the security system to provide proactive detection, surveillance coverage and alarm monitoring of all areas around site perimeters, entrances, all gates, guard rooms, control rooms, battery rooms, HV yard strategic places, strategic spares rooms etc. as determined by Eskom. The system will facilitate for local and remote surveillances of security related signals, effective crime pre-detection, live event monitoring, investigations, provision of management information, reviewing, profiling, data storage data retrieval, and the provision of evidence admissible in legal and disciplinary proceedings. The system will further facilitate the following:-

a) Enable safety of individuals at Eskom sites;

b) Reduction of manned guarding;

c) Supplement manned guarding by making them more efficient at Eskom sites;

d) To monitor persons entering and leaving Eskom sites ;

e) To detect intruders entering Eskom sites illegally;

f) Enable intrusion pre-detection in the following areas(but not limited to):-

1) HV yard strategic places,

2) Tunnelling underneath the site perimeter barrier fences and walls,

3) Separation of electric fence conductors,

4) Cutting and climbing over site perimeter barrier fences,

5) Digging underneath, breaking though the site perimeter barrier fences and walls.

3.1 General requirements

The alarm system shall comply to the following general requirements

a) Comply with requirements of SANS 2220-1-1.

b) Comply with the requirements of SANS 2220-2-2.

c) Still operate in the event of a main power failure.

d) Be either fail safe or fail secure, as required.

e) Incorporate a management reporting function.

f) Have visual and/or audible indicating equipment.

g) Be capable of accommodating traffic data flow even at peak data traffic periods.

h) Be capable of distinguishing between a specified number of different geographic areas and be capable of maintaining the validity of specific time zones.

i) Be able to generate alarms for any type of hazard to which the protected area or its occupants may be subjected.

j) Allow entry to the system parameters by password only and there shall be at least three levels of password to allow three levels of access with at least 10 unique usernames and passwords per access level as defined below:-

1) Level 1 access (Reader): the user can only view the alarms.

2) Level 2 access (Operator): the user is able to view and acknowledge the alarms.

3) Level 3 access (Administrator): the user has full access rights which include changing the configuration parameters of the system.

3.2 Operating conditions

3.2.1 General operating conditions

a) All the elements of the alarm system shall be able to function in all climatic conditions prevailing in South Africa with the minimum environmental conditions below, without the performance being out of limits or the life cycle being shortened:

b) Altitude: 0 – 2500 meters

c) Ambient temperature: -10 to + 55 °C

d) Relative humidity: 0 to 100 % outdoors, 5 to 95% indoors in the specified temperature range.

3.2.2 Resistance to corrosion

a) The components of the system shall be inherently corrosion resistant.

3.2.3 Environmental tests

a) Environmental tests on the alarm system detector shall be conducted in accordance with 5.4 of SANS2220-1-1, during and after the test the detector shall not be adversely affected, it shall not be damaged and it shall not generate an alarm.

4. Operational requirements

4.1 System integration

a) The alarm system shall be able to integrate with all Eskom's electronic security systems. The alarm configuration for the different applications will be different based on the applicable physical security design standards, site specific threat and risk assessment, security plan, environment and business operations.

4.1.1 Alarm triggers

a) Alarm triggers of the integrated alarm system shall occur as a result of the following triggers (but not limited to:-

1) Due to Camera video analytics alarm detection on the site zone(s);
2) Noise in the guarded zones;
3) Alarm inputs from electric fence;
4) Alarm inputs from infrared sensors;
5) Alarm inputs from microwave beams;
6) Alarm inputs from panic buttons;
7) Alarm input from fibre optic sensors(s);
8) Alarm inputs from access control points.

a) Integration with CCTV cameras

b) For effective alarm monitoring and proactive accurate response, the alarm system shall be interoperable with the following camera functionalities and triggers:

1) Built-in video motion analytics detection ,
2) Audio detection ,
3) Active tampering ,
4) I/O connections
5) Alarm and event management.

4.1.2 Integration with PA system

a) To ensure Interoperability with the PA system, the alarm system shall trigger the automated voice recordings of the PA system and enable operators to speak to intruders.

4.1.3 Integration with pre-detection sensors

a) The alarm system shall be interoperable with the pre-detection sensors and shall be triggered by the following sensors (at minimum):-

1) Infrared beams along the site perimeter and in the strategic places of the protected site.
2) Microwave beams in the selected strategic place of the protected site.
3) Fibre optic sensors at strategic places of the projected site.

4.1.4 Integration with panic buttons

a) A panic button may be installed to alert the security control room operators with a distress signal should an incident occur at a protected site.

b) There may be an option for both portable wireless panic buttons and fixed panic buttons installed at strategic areas.

c) The alarm condition or status shall continue until the panic button is manually reset.

4.1.5 Integration with security lighting

a) When an alarm is triggered, the security lighting of the zone that triggered the alarm shall immediately be switched on.

4.1.6 Integration with other electronic security systems

a) The system shall be able to integrate with any other electronic security system not mentioned above

4.1.7 Arming and Disarming system

a) The system should be able to arm and disarm on presentation of a valid access control medium.

b) System should be able to be armed both manually and via a remote control.

c) The remote shall have a minimum of four buttons / key combinations below:

1) Alarm system activation / deactivation;

2) Open electric gate (When installed);

3) Open the maglock to the relay house door (Where implemented);

4) Panic Button to alert the security control room operators with a distress signal when an incident occurs. .

d) It shall be possible to arm and disarm the intruder detection system from inside a vehicle outside the gate of the protected site.

e) There shall be high brightness LEDs to indicate alarm status (armed or disarmed). An LED should be mounted at each entry point in such a way that it is clearly visible even in bright sunlight.

f) It shall be possible to detect the following scenarios when the system is armed:

1) Unauthorised access to protected site;

2) A panic button (if installed) is pressed;

3) AC fail;

4) Periodic test signals to confirm system is operational.

4.1.8 Unauthorized access

a) The alarm system shall be triggered by either of the following which could indicate unauthorised access:

1) Unrecognised card being used at the card reader;

2) Panic button being pressed;

3) Control centre issuing an alarm instruction;

4) Cameras and pre-detection sensors detecting violation.

4.1.9 False or Nuisance alarm

a) The system should be designed in such a way that nuisance alarms are minimised, by using the following methods at minimum:-

1) Use high quality sensors;

2) Place sensors strategically;

3) Use ‘double knock’ design.

4.1.10 Integrated Alarm management

a) During the alarm situation(s) the following shall take place:-

1) Lights shall be immediately switched on, in that particular alarmed zone(s).

2) PTZ camera(s) shall immediately zoom into the alarmed zone(s).

3) Siren(s) shall sound on site in the control room(s).

4) Video recording shall commence immediately.

5) Alarm zone(s) shall be immediately displayed in all the working station(s), PCs, video wall(s).

6) Two way inbuilt audio system shall be immediately activated for operator(s) to speak to the intruder(s) using the PA system.

7) Where applicable and in line with applicable legal requirements, pepper sprays shall be ready for spraying into the culprits.

8) Recorded videos may be sent via emails and cell phones.

9) Each violation shall be reported to the control centre and notified to the security controller.

10) The security controller shall be able to confirm the arrival of the responders on site following an alarm event.

11) The system cause and effect matrix shall be as the table in Annex A.

Note: The order/sequence in which the above events occur shall be settable and changeable.

4.2 The integrating system / controller shall:

a) Collect information from intrusion detection systems, access control and video surveillance devices (at a minimum).

b) Contain circuitry that provides interface with the peripheral devices by means of industry standard open communications protocol.

c) Maintain a real-time sequential record of reader events, alarm events and all operator programming events that are date and time stamped to the nearest second. These events shall be stored in such a format that it is possible for other operators to sort and analyse them.

d) Have a transaction memory and shall be able to store information over a three month period or 10000 transactions.

e) Have a transaction memory to store information at an offsite central server over a longer period (over 6 months).

f) Have the output capability to send information to the intruder detector systems, tamper protection devices and power supply unit to reset once an alarm has been acknowledged by the security control centre.

g) Have input capability to monitor intruder detector alarm signals, tamper protection devices and power supply unit alarms.

h) Have interface capability with the communication unit in order to send alarm signals to the security control room and receive instructions to reset the alarm condition.

i) Provide an interface for connection to access control devices such as a reader controller and access control controller.

j) The system shall be configurable to have a decision making process at the controller so that controller transaction time does not exceed 1s.

k) The controller shall be menu driven and display status of all monitored points simultaneously.

l) To change settings on the controller the operator shall use a unique username and password. Each operator‘s transaction on the controller shall be recorded together with the date and time.

m) Where access control and intruder alarm monitoring is on the same central processor, the controller shall simultaneously handle message traffic from the readers, intruder alarm system and operational functions such as file maintenance, time updating and real time output control updating, and the output capability to send information to the access control system.

n) The system shall have the input capability to monitor access control system signals. The alarm signal shall have the highest priority and shall override other activities. It shall be possible to recall and execute the last transaction prior to the alarm condition.

4.3 Alarms and indications

a) The system shall be designed to ensure a clear and unambiguous indication of the origin of the alarm signal. The site and sensor (zone number and description) triggered should be clear e.g. Simmerpan Substation, Zone 5 – HV yard.

b) User shall be able to add a text label to the site and to each sensor ‘zone’.

c) In combined systems, alarm signalling and action relating to safety of life shall be given priority.

d) When the alarm system is set, all detection and signalling circuits used to transmit an alarm condition shall be monitored for faults other than those equivalent to an alarm.

e) The system shall be self-diagnostic such that if a fault occurs in the communication or part of the alarms system which would prevent the transmission of any alarm condition, an alarm or fault condition shall be generated at the monitoring centres(locally and remotely).

f) The local and remote controllers shall be able to view and respond to alarms.

g) The alarm condition generated by a detector shall be sustained for a configurable duration.

h) Depending on the site the alarm system is installed, it shall be possible to specify the information to be transmitted and the action to be taken on the receipt of alarm, fault, test or other signals.

i) The alarm system shall be able to show alarm status indications both locally and remotely.

4.4 Monitoring and Control

a) The alarm system shall be able to receive alarming instruction from security controller and sensors such as security lights, PA systems, Doors, CCTV, panic buttons or any other electronic security system at site.

b) The security control centre shall be able to remotely issue alarming instructions to the alarming system.

c) It shall be possible for the security control centre to monitor and control the system both locally and remotely.

d) The local and remote controllers shall be able to schedule equipment operation.

5. Electrical requirements

5.1 Power Supply

a) All system equipment shall be housed in 19-inch equipment cabinets as specified in the Eskom standard 240-60725641. This specification covers the earthing requirements in the cabinet as well.

b) The existing standby power systems at site shall be used as the primary standby power source, provided that the standby time (autonomy) requirements of the site are not adversely affected.

c) In cases where the above is not possible, the standby power systems requirements for security systems at Eskom sites shall comply with the following:

1) The system design shall comply with the requirements of 240-91190294, DC & Auxiliary Supplies Philosophy.

2) 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.

3) Standard or technically acceptable equipment shall be used. This equipment is available on Eskom National Contracts (ENCs) or recommended technically acceptable equipment lists.

4) 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 1 below:

Table 1: Technical Standards for Standby Power Systems equipment

Equipment	Technical standard
Nickel cadmium batteries	240-56360086 – Stationary Vented Nickel Cadmium Batteries Standard
Vented lead acid batteries	240-56360034 – Stationary Vented Lead Acid Batteries Standard
Valve-regulated lead acid batteries	240-51999453 – Standard Specification for Valve-Regulated Lead Acid Cells
Power electronics	240-53114248 – Thyristor and Switch Mode Chargers, AC/DC to DC/AC Converters, and Inverter/Uninterruptible Power Supplies Standard
Low-voltage protective devices, cubicles, and wiring	240-64139144 – AC Boards and Junction Boxes for Substations 240-76628687 – AC/DC Reticulation Equipment for Breaker-and-a-Half Substations 240-75658628 – Distribution Group's Specific Requirements for AC/DC Distribution Units

d) The system shall have an additional power failure alarm indication that shall be sent through to the Eskom control room via SCADA should the power supply be interrupted.

5.2 Communication

a) The integrated alarm system shall be an IP based smart solution with capability to integrate with other security systems through industry open communication protocols.

b) The alarm system shall be designed and constructed to accommodate a communication module that allows for communication between site where the system is installed and the remote security control centre (Zero control or Regional security control center).

5.3 Electrical safety

a) Any container for batteries shall be so constructed that the battery terminals are protected against inadvertent contact with metal parts.

b) A power unit for the alarm system shall be so constructed that electronics and electrical circuits are protected against hazards caused by battery charging, accidental electrolyte spillage, fumes or explosive gas.

c) All electrical components shall be protected against excess current and short-circuit by adequately rated overload protective devices.

d) In combined systems, alarm signalling and actions relating to safety of life shall be given priority.

e) The system shall be protected against transients and lightning surges.

f) The electrical installation shall comply with SANS 10142.

6. Physical requirements

6.1 General construction requirements

a) Construction of Intruder alarm system shall comply with 3.1.1 of SANS 2220-1-1.

b) The IP rating of enclosures for alarm system equipment installed outdoors shall be IP53.

c) The IP rating of enclosures for alarm system equipment installed indoors shall be IP51.

d) The enclosures shall provide protection of persons against access to hazardous parts by preventing or limiting the ingress of a part of the human body or an object held by a person.

e) The enclosures shall provide protection of equipment against the ingress of solid foreign objects.

f) Protection against dust shall be provided.

g) Protection against jetting water for shall be provided.

h) Protection against high voltage apparatus shall be provided.

i) Protection against bad weather conditions shall be provided.

j) Enclosures shall provide the acceptable degree of protection against moisture.

k) The mean time between failures (MTBF) of the alarm system detector shall be at least 60 000h.

6.2 Tamper protection

a) The alarm system detector shall have tamper device(s), it shall not be possible to adjust the detector without operating the tamper device(s).

b) Tamper protection for alarm system detector shall comply with 5.6 of SANS 2220-1-1.

c) It shall not be possible to alter the enclosure arrangements of the detector or to change its existing area of detection coverage or detection range without causing an alarm condition.

d) It shall not be possible to gain access to the electrical circuits, adjustment controls or tamper detection device without causing the tamper detection device to generate an alarm signal.

e) It shall not be possible to interfere with the operation of the detector by disconnecting or short circuiting any interconnecting circuit of the detector system. The system shall be monitored and an alarm condition signalled when alarm or tamper information is prevented from being transmitted.

f) It shall not be possible to disable the tamper detection device by means of normally available tools such as knives or screwdrivers.

6.3 Physical safety

a) The mechanical construction of any part of the system shall be such that injury caused by mechanical instability or by moving parts, protruding or sharp edges is prevented.

b) Enclosures shall be so constructed and mounted such that electrical tests and operations are possible without the removal of the devices from their mounting.

c) It shall not be possible to adjust the devices or their housing without operating the tamper detection device(s).

7. EMC

a) The alarm system shall comply with the relevant EMC standards regulated by ICASA.

b) The alarm systems shall comply to the requirements for limits of electromagnetic interference given in the regulations published in terms of the Telecommunications Act, 1996 (Act No. 103 of 1996).

c) Signal, voltage and electromagnetic radiation levels in readily accessible areas shall not be dangerous.

8. Noise

a) Noise levels for power unit of the alarm system shall comply with 3.4 of SANS 2220-1-7.

9. Cyber security

a) The system shall comply with all the requirements of Eskom's Cyber Security Standard for operational technology (document number 240-55410927).

b) The system shall not be susceptible to cyber-attacks and unauthorised remote access.

10. Earthing

a) The system shall be earthed as per Eskom's earthing standards

11. Functional requirements for pre-detection sensors

a) Alarms shall be generated by a perimeter detection system.

b) The perimeter detection system shall create an 'invisible wall' which encapsulates the entire perimeter of the yard, so that there are no areas where an intruder may enter the site undetected.

c) There shall be no 'dead spots' in the invisible wall. Where a method of detection has an inherent dead spot, the dead spot of each device shall be covered by another device (e.g. Cameras with overlapping fields of view).

d) The perimeter detection method should be divided into zones matching the areas covered by the perimeter cameras and fence zones.

e) Pre-detection sensors shall be triggered by vibration detection of the following:

1) beneath the site barrier fences and walls to sense digging;

2) on the site barrier fences and walls to sense breaking through the barriers/walls;

3) on top of the site barrier fences and walls to detect climbing

f) The sensitivity of the pre-detection system shall be configurable/tunable to limit nuisance alarms. The supplier shall provide details of how the system limits the nuisance alarms.

g) The system shall comply with the requirements of integrated alarm management listed above.

12. System life-cycle

a) The minimum system life-cycle of the proposed product must be ten (10) years.

b) The life-cycle of the product must be further supported in terms of spares availability for a minimum period of seven (7) years after discontinuation of the product

13. Warranty and support

a) The system shall carry a minimum local (South African) warranty of 36 months with on-site as well as telephonic support from date of the system being commissioned. Eskom shall thereafter have the option to access on-going 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 maintenance.

f) The supplier shall also provide operator training to enable the installation, calibration and maintenance of the equipment by Eskom personnel or appointed contractors.

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 at least a minimum period of five (5) years.

j) The supplier to provide a list of reference sites where the product on offer has been installed and the year of implementation.

14. Markings, Labelling and packaging

a) The alarm system components shall be marked with the following information:

1) The manufacture's name;

2) The model identification;

3) The rated supply voltage and frequency and the rated current;

4) Identification of terminals and leads by means of numbers, colours or other.

15. Documentation and drawings

a) The system shall be supplied together with the following documentation:

1) Performance characteristics;

2) Certificate of compliance;

3) Eskom Maintenance Standards and Task Manuals

4) Power supply requirements;

5) Wiring and mounting instructions;

6) Output ratings;

7) Instructions for adjustments, including specification of any special tools required;

8) Installation, commissioning and maintenance procedures;

9) Advice on how to avoid inappropriate use and potential false operation of equipment;

10) If the manner of installing components is not obvious, each component of an alarm system shall be supplied together with instructions for the installation of the component. Any component that may be damaged by reversal of the input polarity shall have this fact stated clearly in the instructions.

11) Drawings provided shall include the following:

i. All modules and circuit diagrams;

ii. Schematic diagrams;

iii. Installation drawings.

12) All training requirements shall be specified.

16. Testing

a) The supplier shall avail themselves for Site Acceptance Testing at site after installation.

b) All test procedures required to ensure the correct functioning shall be specified with a list of required test equipment and tools.

17. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Karen Pillay	Senior Manager- Security Solutions - Physical
Barry Clayton	Middle Manager - Transmission
Sikelela Mkhabela	Senior Manager - Distribution
Machiel Viljoen	Senior Manager - Generation
Kashveer Jagdaw	DC & Auxiliary Supplies SC Chairperson
Prudence Madiba	Senior Manager – Electrical and C&I Engineering
Cornelius Naidoo	Manager- Telecoms T&S CoE
Lenah Mothatha	Senior Manager – Transmission
Riaan Venter	Middle Manager – Civil and Structural COE

18. Revisions

Date	Rev	Compiler	Remarks
Aug 2020	2	R Moshoeshoe	- Updated power supply requirements to include reference to DC systems standards. - Included requirements for pre-detection sensors - Added technical schedule A&B - Included Alarm system cause and effect matrix and integrated alarming functionality
April 2015	1	R Moshoeshoe	- First issue

19. Development team

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

- Thomas Jacobs
- Tejin Gosai
- Albertus Hendriks

20. Acknowledgement

Not applicable.

Annex A – Alarm system 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 Center	✓	✓	✓	✓	✓	

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 – Technical Schedule A&B

TECHNICAL SCHEDULES A AND B FOR Specification for Integrated security alarm system 240-86738968

Schedule B: Guarantees, compliance, and technical particulars of equipment offered

- The clauses and numbering in this table are not necessarily the verbatim clauses as per 240-86738968. Therefore it is OBLIGATORY on the TENDERER to review the applicable clauses in 240-86738968 in order to provide an informed response.
- When completing the Schedule B and the References section, The Tenderer is required to state clearly, for each clause that requires a statement of compliance, with one of the following options:

a) Comply – Confirmation of FULL Compliance to all clauses of the applicable section of the Technical Standard. No deviations

b) Partially Comply – Confirmation of PARTIAL Compliance and that FULL Compliance is not possible. Deviations taken.

c) Do Not Comply - Conformation of Non-Compliance to ALL requirements in the applicable section

- Reference to evidence in the form of datasheets, equipment manuals, drawings, hyperlinks shall be included in the References section
- Where there are any deviations taken from the clauses in the applicable section, these should be indicated under the References and Deviations section

	Description	**Schedule A**	**Schedule B**	**References/Statement (supporting evidence) & Deviations**	**Comments**
3	**General**				
3.1	**General requirements** The system shall comply with the following general requirements:				
a)	Comply with requirements of SANS 2220-1-1.	comply			

b)	Comply with the requirements of SANS 2220-2-2.	comply			
c	Still operate in the event of a main power failure.	comply			
d)	Be either fail safe or fail secure, as required.	comply			
e)	Incorporate a management reporting function.	comply			
f)	have visual and/or audible indicating equipment.	comply			
g)	Be capable of accommodating traffic data flow even at peak data traffic periods.	comply			
h)	Be capable of distinguishing between a specified number of different geographic areas and be capable of maintaining the validity of specific time zones.	comply			
i)	Be able to generate alarms for any type of hazard to which the protected area or its occupants may be subjected.	Comply			
j)	Allow entry to the system parameters by password only and there shall be at least three levels of password to allow three levels of access	comply			
3.2	**Operating conditions**				
3.2.1	**General operating conditions**				

a)	All the elements of the alarm system shall be able to function in all climatic conditions prevailing in South Africa with the minimum environmental conditions below, without the performance being out of limits or the life cycle being shortened:	comply			
b)	Altitude: 0 – 2500 meters	comply			
c)	Ambient temperature: -10 to + 55 °C	comply			
d)	Relative humidity: 0 to 100 % outdoors, 5 to 95% indoors in the specified temperature range.	comply			
3.2.2	**Resistance to corrosion**				
a)	The components of the system shall be inherently corrosion resistant.	comply			
3.2.3	**Environmental tests**				
a)	Environmental tests on the alarm system detector shall be conducted in accordance with 5.4 of SANS2220-1-1, during and after the test the detector shall not be adversely affected, it shall not be damaged and it shall not generate an alarm.	comply			
4	**Operational requirements**				
4.1	**System integration**				
a)	The alarm system shall be able to integrate with all Eskom's electronic security systems.	comply			

4.1.2	**Alarm triggers**				
a)	Alarm triggers of the integrated alarm system shall occur as a result of the following triggers (but not limited to:- i. Due to Camera video analytics alarm detection on the site zone(s); ii. Noise in the guarded zones; iii. Alarm inputs from electric fence; iv. Alarm inputs from infrared sensors; v. Alarm inputs from microwave beams; vi. Alarm inputs from panic buttons; vii. Alarm input from fibre optic sensors(s); viii. Alarm inputs from access control points.	comply			
4.1.3	**Integration with CCTV cameras**				
a)	For effective alarm monitoring and proactive accurate response, the alarm system shall be interoperable with the following camera functionalities and triggers: i. Built-in video motion analytics detection ii. Audio detection iii. Active tampering iv. I/O connections v. Alarm and event management.	comply			

4.1.4	**Integration with PA system**				
a)	To ensure Interoperability with the PA system, the alarm system shall trigger the automated voice recordings of the PA system and enable operators to speak to intruders.	comply			
4.1.5	**Integration with pre-detection sensors**				
a)	The alarm system shall be interoperable with the pre-detection sensors and shall be triggered by the following sensors (at minimum):- i. Infrared beams along the site perimeter and in the strategic places of the protected site. ii. Microwave beams in the selected strategic place of the protected site. iii. Fibre optic sensors at strategic places of the projected site.	comply			
4.1.6	**Integration with panic buttons**				
a)	A panic button may be installed to alert the security control room operators with a distress signal should an incident occur at a protected site.	Comply			
b)	There may be an option for both portable wireless panic buttons and fixed panic buttons installed at strategic areas.	comply			

c)	The alarm condition or status shall continue until the panic button is manually reset.	comply			
4.1.7	**Integration with security lighting**				
a)	When an alarm is triggered, the security lighting of the zone that triggered the alarm shall immediately be switched on.	comply			
4.1.8	**Integration with other electronic security systems**				
a)	The system shall be able to integrate with any other electronic security system not mentioned above	comply			
4.1.9	**Arming and Disarming system**				
a)	The system should be able to arm and disarm on presentation of a valid access control medium.	comply			
b)	System should be able to be armed both manually and via a remote control.	comply			
c)	The remote shall have a minimum of four buttons / key combinations below: 5) Alarm system activation / deactivation; 6) Open electric gate (When installed); 7) Open the maglock to the relay house door (Where implemented);	comply			

	8) Panic Button to alert the security control room operators with a distress signal when an incident occurs				
d)	It shall be possible to arm and disarm the intruder detection system from inside a vehicle outside the gate of the protected site.	comply			
e)	There shall be high brightness LEDs to indicate alarm status (armed or disarmed). An LED should be mounted at each entry point in such a way that it is clearly visible even in bright sunlight.	comply			
f)	It shall be possible to detect the following scenarios when the system is armed: 5) Unauthorised access to protected site; 6) A panic button (if installed) is pressed; 7) AC fail; 8) Periodic test signals to confirm system is operational.	comply			
4.1.10	**Unauthorized access**				
a)	The alarm system shall be triggered by either of the following which could indicate unauthorised access: 5) Unrecognised card being used at the card reader; 6) Panic button being pressed; 7) Control centre issuing an alarm instruction;	comply			

	8) Cameras and pre-detection sensors detecting violation.				
4.1.11	**False or Nuisance alarm**				
a)	The system should be designed in such a way that nuisance alarms are minimised, by using the following methods at minimum:- 1) Use high quality sensors; 2) Place sensors strategically; 3) Use 'double knock' design.				
4.1.12	**Integrated Alarm management**				
a)	During the alarm situation(s) the actions listed in section 4.1.12 of 240-86738968 shall take place	comply			
4.2	**The integrating system / controller shall:**				
a)	Collect information from intrusion detection systems, access control and video surveillance devices (at a minimum).	comply			
b)	Contain circuitry that provides interface with the peripheral devices by means of industry standard open communications protocol.	comply			
c)	Maintain a real-time sequential record of reader events, alarm events and all operator programming events that are date and time stamped to the nearest second.	comply			

d)	Have a transaction memory and shall be able to store information over a three month period or 10000 transactions.	comply			
e)	Have a transaction memory to store information at an offsite central server over a longer period (over 6 months).	comply			
f)	Have the output capability to send information to the intruder detector systems, tamper protection devices and power supply unit to reset once an alarm has been acknowledged by the security control centre.	comply			
g)	Have input capability to monitor intruder detector alarm signals, tamper protection devices and power supply unit alarms.	comply			
h)	Have interface capability with the communication unit in order to send alarm signals to the security control room and receive instructions to reset the alarm condition.	comply			
i)	Provide an interface for connection to access control devices such as a reader controller and access control controller.	comply			
j)	The system shall be configurable to have a decision making process at the controller so that controller transaction time does not exceed 1s.	comply			
k)	The controller shall be menu driven and display status of all monitored points simultaneously.	comply			

l)	To change settings on the controller the operator shall use a unique username and password. Each operator‘s transaction on the controller shall be recorded together with the date and time.	comply			
m)	Where access control and intruder alarm monitoring is on the same central processor, the controller shall simultaneously handle message traffic from the readers, intruder alarm system and operational functions such as file maintenance, time updating and real time output control updating, and the output capability to send information to the access control system.	comply			
n)	The system shall have the input capability to monitor access control system signals. The alarm signal shall have the highest priority and shall override other activities. It shall be possible to recall and execute the last transaction prior to the alarm condition.	comply			
4.3	Comply to alarms and indications requirements listed in section 4.3 of 240-86738968	comply			

4.4	**Monitoring and Control**				
a)	The alarm system shall be able to receive alarming instruction from security controller and sensors such as security lights, PA systems, Doors, CCTV, panic buttons or any other electronic security system at site.	comply			
b)	The security control centre shall be able to remotely issue alarming instructions to the alarming system.	comply			
c)	It shall be possible for the security control centre to monitor and control the system both locally and remotely.	comply			
d)	The local and remote controllers shall be able to schedule equipment operation.	comply			
5	**Electrical requirements**				
5.1	**Power Supply**				
a)	All system equipment shall be housed in 19-inch equipment cabinets as specified in the Eskom standard 240-60725641. This specification covers the earthing requirements in the cabinet as well.	comply			

b)	The existing standby power systems at site shall be used as the primary standby power source, provided that the standby time (autonomy) requirements of the site are not adversely affected.	comply			
c)	Standby power systems requirements shall comply to requirements listed in section 5.1 (c) of 240-86738968	comply			
d)	The system shall have an additional power failure alarm indication that shall be sent through to the Eskom control room via SCADA should the power supply be interrupted.	comply			
5.2	**Communication**				
a)	The integrated alarm system shall be an IP based smart solution with capability to integrate with other security systems through industry open communication protocols.	comply			
b)	The alarm system shall be designed and constructed to accommodate a communication module that allows for communication between site where the system is installed and the remote security control centre (Zero control or Regional security control centre).	comply			
5.3	**Electrical safety**				

a)	Any container for batteries shall be so constructed that the battery terminals are protected against inadvertent contact with metal parts.	comply			
b)	A power unit for the alarm system shall be so constructed that electronics and electrical circuits are protected against hazards caused by battery charging, accidental electrolyte spillage, fumes or explosive gas.	comply			
c)	All electrical components shall be protected against excess current and short-circuit by adequately rated overload protective devices.	comply			
d)	In combined systems, alarm signalling and actions relating to safety of life shall be given priority.	comply			
e)	The system shall be protected against transients and lightning surges.	comply			
f)	The electrical installation shall comply with SANS 10142.	comply			
6	**Physical requirements**				
6.1	Comply to general construction requirements listed in section 6.1 of 240-86738968	comply			
6.2	Comply to tamper protection requirements listed in section 6.2 of 240-86738968	comply			
6.3	Comply to physical safety requirements listed in section 6.3 of 240-86738968	comply			

7	**EMC**				
a)	The alarm system shall comply with the relevant EMC standards regulated by ICASA.	comply			
b)	The alarm systems shall comply to the requirements for limits of electromagnetic interference given in the regulations published in terms of the Telecommunications Act, 1996 (Act No. 103 of 1996).	comply			
c)	Signal, voltage and electromagnetic radiation levels in readily accessible areas shall not be dangerous.	comply			
8	**Noise**				
a)	Noise levels for power unit of the alarm system shall comply with 3.4 of SANS 2220-1-7.				
9	**Cyber security**				
a)	The system shall comply with all the requirements of Eskom's Cyber Security Standard for operational technology (document number 240-55410927).	comply			
b)	The system shall not be susceptible to cyber-attacks and unauthorised remote access.	comply			
10	**Earthing**				

a)	The system shall be earthed as per Eskom's earthing standards	comply			
11	**Functional requirements for pre-detection sensors**				
a)	Alarms shall be generated by a perimeter detection system.	comply			
b)	The perimeter detection system shall create an 'invisible wall' which encapsulates the entire perimeter of the yard, so that there are no areas where an intruder may enter the site undetected	comply			
c)	There shall be no 'dead spots' in the invisible wall. Where a method of detection has an inherent dead spot, the dead spot of each device shall be covered by another device (e.g. Cameras with overlapping fields of view).	comply			
d)	The perimeter detection method should be divided into zones matching the areas covered by the perimeter cameras and fence zones.	comply			
e)	Pre-detection sensors shall be triggered by vibration detection of the following: 1) beneath the site barrier fences and walls to sense digging; 2) on the site barrier fences and walls to sense breaking through the barriers/walls;	comply			

	3) on top of the site barrier fences and walls to detect climbing				
f)	The sensitivity of the pre-detection system shall be configurable/tunable to limit nuisance alarms. The supplier shall provide details of how the system limits the nuisance alarms.	comply			
g)	The system shall comply with the requirements of integrated alarm management listed in 240-86738968	comply			
12	**System life-cycle**				
a)	The minimum system life-cycle of the proposed product must be ten (10) years.	comply			
b)	The life-cycle of the product must be further supported in terms of spares availability for a minimum period of seven (7) years after discontinuation of the product	comply			
13	**Warranty and support**				
a)	The system shall carry a minimum local (South African) warranty of 36 months with on-site as well as telephonic support from date of the system being commissioned. Eskom shall thereafter have the option to access on-going support in terms of a subsequent agreement.	comply			
b)	The supplier must have a technician on call on a 24-hour basis for purposes of telephonic support.	comply			

c)	Supplier spares holding should include minimum replacement spares to restore service of the system in its entirety.	comply			
d)	All support shall also include all firmware upgrades of the initial system version installed over the operational life of the system.	comply			
e)	The support shall include first line maintenance	comply			
f)	The supplier shall also provide operator training to enable the installation, calibration and maintenance of the equipment by Eskom personnel or appointed contractors.	comply			
g)	Product support must include national as well as international support through the local branch.	comply			
h)	The supplier shall be willing to enter into an SLA with Eskom	comply			
i)	The supplier should have a history of supplying products of this nature in South Africa for at least a minimum period of five (5) years.	Comply			
j)	The supplier to provide a list of reference sites where the product on offer has been installed and the year of implementation.	comply			
14	**Markings, Labelling and packaging**				
a)	The alarm system components shall be marked with the following information:	comply			

	5) The manufacture's name; 6) The model identification; 7) The rated supply voltage and frequency and the rated current; 8) Identification of terminals and leads by means of numbers, colours or other.				
15	**Documentation and drawings**				
a)	The system shall be supplied with documentation and drawings listed in section 15 of 240-86738968	comply			
16	**Testing**				
a)	The supplier shall avail themselves for Site Acceptance Testing at site after installation.	comply			
b)	All test procedures required to ensure the correct functioning shall be specified with a list of required test equipment and tools.	comply			