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:	**1**
Total Pages:	**19**
Next Review Date:	**April 2020**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Donald Moshoeshoe	**Thomas Jacobs**	**Willy Majola**
Engineer	**DC & Auxiliary Supplies SC Chairperson**	**Engineering SGM**
Date: 10 April 2015	Date: 10 April 2015	Date: 16/4/2015

Supported by SCOT/SC

Richard McCurrach

PTM&C TC Chairperson

Date: 16/4/2015

PCM Reference: **240-43542545**

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

Content

Figures

Tables

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

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

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

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

[5] TST41-877, Transmission Substations Design Earthing Standard

[6] 240-55410927, Cyber Security Standard For Operational Technology

2.2.2 Informative

[7] ISO 9001, Quality Management Systems.

[8] 32-644, Eskom documentation management standard

[9] 474-65, Operating manual of the Steering Committee of Technologies (SCOT)

[10] 34-1613, Specification for CCTV surveillance and camera system installations at distribution substations

[11] 34-1430, Procedure for first line maintenance of security system at substations

[12] DISSCABL1, Specification for Intruder Alarm Systems Used At Distribution Substations

[13] DST0045, Standard for Security Requirements At Distribution Substations and Buildings

[14] 34-1617, Specification for Infrared Detectors At Distribution Substations

[15] 34-1618, Specification for Electronic Access Control At Distribution Substations

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
AC	Alternating current
Ah	Ampere hour
CCTV	Closed-Circuit Television
DC	Direct Current
DVR	Digital Video Recorder
EBI	Enterprise Buildings Integrator
EMC	Electromagnetic Compatibility
h	Hours
HV	High Voltage
Hz	Hertz
I/O	Input/output
ICASA	Independent Communications Authority of South Africa
Id	Identification
IP rating	Ingress Protection rating
km	kilometres
LED	Light Emitting Diode
MCB	Miniature Circuit Breaker
MTBF	Mean Time Between Failures

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

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

Group Security risk analysis will determine the effectiveness of this standard.

2.7 Related/supporting documents

Not applicable

3. General

The alarm system forms an integral part of the IP surveillance system to provide proactive 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 control rooms IP surveillance signals monitoring, effective crime pre-detection, live event monitoring, investigations, provision of management information, reviewing, profiling, data storage (digital), data retrieval, and the provision of evidence admissible in legal and disciplinary proceedings. The system will further facilitate the following:-

- Enable safety of individuals at Eskom sites;
- Reduction of manned guarding;
- Supplement manned guarding by making them more efficient at National key points;
- To monitor persons entering and leaving Eskom sites ;
- To provide visual confirmation of intruders activating alarms;
- To provide information on false alarms;

- Enable intrusion pre-detection in the following areas:-
  - o HV yard strategic places,
  - o Tunnelling underneath the electric fence,
  - o Separation of electric fences,
  - o Cutting and climbing over perimeter outer barrier fences,
  - o Digging underneath, breaking though and climbing over the outer barrier walls.

3.1 General requirements:

The alarm system shall:

1) Comply with requirements of SANS 2220-1-1.
2) Comply with the requirements of SANS 2220-2-2.
3) ensure controlled access to and exit from a controlled area and be capable of recording each transaction.
4) allow easy access for purposes of servicing while restricting opportunities for deliberate interference.
5) still operate in the event of a main power failure.
6) be either fail safe or fail secure, as required.
7) incorporate a management reporting function.
8) have keyboard entry to access control system software by password.
9) have visual and/or audible indicating equipment.
10) have signalling interface (modem).
11) be capable of accommodating traffic data flow even at peak data traffic periods.
12) be capable of distinguishing between a specified number of different geographic areas and be capable of maintaining the validity of specific time zones.
13) be able to generate alarms for any type of hazard to which the protected area or its occupants may be subjected.
14) 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:
    a) level 1 access (reader) : the user can only view the alarms.
    b) level 2 access (Operator) : the user is able to view and acknowledge the alarms.
    c) level 3 access (Administrator) : the user has full access rights which includes changing the configuration parameters of the system.

3.2 Operating conditions

3.2.1 General operating conditions

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:

3.2.1.1 Altitude

0 – 2500 meters

3.2.1.2 Ambient temperature

-10 to + 55 °C

3.2.1.3 Relative humidity

Up to 100 % outdoors, 5 to 95% indoors in the specified temperature range.

3.2.2 Resistance to corrosion

The components of the system shall be inherently corrosion resistant.

3.2.3 Environmental tests

3.2.3.1 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. Applicable sites

Table 1 shows different Eskom sites where the Alarm system may be used (but not limited thereto).

Table 1: Applicable sites for installation of alarm system

Generation Coal Fired Power Stations	Distribution Customer Network Centres
Generation Nuclear Power Stations	Customer Service Hubs
Generation Peaking Hydro Power Stations	Data Centres
Generation Peaking Open Cycle Gas Turbine Power Stations	National and Regional Security Control Centre
Generation Renewable Power Stations	Mobile Construction Sites
Transmission Substations	Customer Call Centres
Transmission National Control	Real Estate Office Complexes
Distribution Substations	Real Estate Campuses
Distribution Control Centres	Real Estate Office Blocks
Distribution Warehouses	Telecommunications Sites

NOTE: There should be a portable, quick deploy systems that could be deployed at construction sites, high risks sites awaiting permanent installation or sites where the permanent alarm is faulty and awaiting maintenance.

5. Operational requirements

5.1 System integration

EBI is Eskom standard security system integration platform. All Eskom security systems hardware and software design must comply and be compatible to all EBI requirements. The alarm system must be integratable 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.

5.1.1 Alarm triggers

Alarm triggers on the integrated alarm system shall occur as follows:-

a) Due to Camera video analytics alarm detection on the zone(s);

b) Noise in the guarded zones;

c) Alarm inputs from electric fence;

d) Alarm inputs from infrared sensors;

e) Alarm inputs from microwave beams;

f) Alarm inputs from panic buttons;

g) Alarm input from fibre optic sensors(s);

h) Alarm inputs from access control points.

5.1.2 Integration with CCTV cameras

For effective alarm monitoring and proactive accurate response, all cameras shall be equipped with the following features which will enable the network cameras to be constantly on guard in analysing alarm inputs and activating sirens in the control rooms while zooming into the alarm(s) spot(s) :-

a) Built-in video motion analytic detection system,

b) Audio detection alarm,

c) Active tampering alarm,

d) I/O connections. Some inputs will be used for the purposes of electric fence alarm relay outputs, sensors alarm triggers etc.,

e) Alarm and event management.

5.1.3 Integration with PA system

Audio detection will facilitate for the following activities:-

a) Operators to listen for sounds in the guarded areas and react accordingly.

b) Operators to speak to intruders.

c) Communication at the access points (entrances to the protected sites) etc.

5.1.4 Integration with pre-detection sensors

Pre-detection sensing will occur as follows:-

a) Infrared along the perimeter and in the strategic places of the protected site.

b) Microwave beams in the selected strategic place of the protected site.

c) Fibre optic sensors will be installed as follows:-

i. Beneath, inside middle and top of the outer barrier wall to sense digging, intrusion through the wall and climbing over the wall.

ii. On the outer barrier fence.

iii. Underneath electric fence and in-between conductors in order to sense digging as well as separation of the conductors.

5.1.5 Integration with panic buttons

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

5.1.5.2 There shall be an option for both portable wireless panic buttons and fixed panic buttons installed at strategic areas.

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

5.1.5.4 The panic button function shall be operational over the entire area of the protected site.

5.1.6 Integration with other electronic security systems

5.1.6.1 The system shall be integratable with any other electronic security system.

5.1.7 Arming and Disarming system

5.1.7.1 System should be able to be armed via a remote control.

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

a) Alarm system activation / deactivation;

b) Open electric gate (When installed);

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

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

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

5.1.7.4 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.

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

a) Unauthorised access to protected site;

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

c) Authorised access;

d) AC fail;

e) Periodic test signals to confirm system is operational.

5.1.7.6 Unauthorized access

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

a) Unrecognised card being used at the card reader;

b) Panic button being pressed;

c) Control centre issuing an alarm instruction;

d) Cameras and alarm sensors detecting violation.

5.1.7.7 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:-

   i. Use high quality sensors;

   ii. Place sensors strategically;

   iii. Use ‘double knock’ design.

5.1.8 Integrated Alarm management

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

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

5.1.8.2 PTZ camera(s) shall immediately zoom into that zone(s).

5.1.8.3 Siren(s) shall sound in the control room(s).

5.1.8.4 Video recording shall commence immediately.

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

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

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

5.1.8.8 Recorded videos shall be sent via emails and cell phones.

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

5.1.8.10 The operator shall be able to use information available, as well as the site history to decide on a response.

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

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

5.2 The integrating system / controller shall:

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

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

c) Maintain a real-time sequential record (on the hard disk) of reader events, alarm events and all operator programming events and 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 one month period or 1000 transactions.

e) Have a transaction memory to store information at an offsite central server over a longer period (over 3 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 configured 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 access 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. As well as 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.

5.3 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.

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 the minimum of 1s 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.

5.4 Monitoring and Controls

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.

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.

e) The alarm system shall have a signalling interface (modem, fibre, microwave etc.) to enable operators to easily monitor sites remotely.

5.4.1 Access Control Medium

5.4.1.1 The preferred access control medium, e.g. smart cards, biometric system, remotes, etc. will depend on the security risk of the protected site.

5.4.1.2 Each authorized person shall receive an access control medium which will link the employee to a specific code internally programmed on the access control medium.

5.4.1.3 Each Eskom personnel shall be able to use a single access control medium for all sites to which they have access.

5.4.1.4 The access control medium shall be remotely programmable allowing for Eskom personnel to be able to authorise and unauthorise the access control medium holder per site. There will be some Eskom personnel with access to sites in a specific area. Other personnel will have access to all sites.

5.4.1.5 Should an access control medium get lost or stolen or a person with an access control medium no longer be authorized, the specific code linked to the access control medium shall be removed off the database and be blocked by the intruder detection system with immediate effect.

5.4.1.6 The system shall be able to store information for 1000 different access control media.

5.4.1.7 It shall be possible to give different access levels to different access control media. e.g. Remote 1 can only use the panic function, but not arm/disarm the system. Remote 2 can arm/disarm and have panic function.

5.4.1.8 It shall be possible to change the access levels for the access control medium from a central location. i.e. if a new access control medium is to be added to all/ some sites it should be possible to add this access control medium on a central server which will 'push' the changes to all the remote alarm panels.

5.4.1.9 The access control medium shall be robust and water resistant.

5.4.1.10 The access control medium shall have a transmission distance of 100 m. It should be possible to install repeaters to extend this distance at large sites.

5.4.1.11 Access control medium should have a unique ID so that the record of arming and disarming is logged to a specific access control medium.

5.4.1.12 At least 999 unique access control media shall be able to be used per site.

5.4.1.13 A record shall be kept of who each access control medium has been allocated to.

5.4.1.14 It shall be possible to limit which access control media have access to which alarm systems.

6. Electrical requirements

6.1 Power Supply

Two power supply solutions shall be provided for the system. Option A will operate off 110V DC and will be connected to the relay house 110V DC supply which has battery backup. Option B is to use the 220V AC supply from the site and shall include battery backup/UPS for all system devices.

The responsible Eskom DC engineer shall be consulted on a per site basis to determine which power supply system will be used. Option A be installed whenever possible since this arrangement leverages off the battery maintenance processes already in place. Option B will be used when site battery capacity is not sufficient to supply the added load of the alarm system. For both options the standing time for backup power is 12 hours at sites within 200kms of responsible Eskom DC section, 18 hours at sites more than 200kms from responsible Eskom DC section.

NOTE: Both power supply designs shall be available.

6.1.1 Option A: 110V DC

6.1.1.1 The security system shall be powered by 110V supplied from the site's DC supply. In the event of a power failure the system will be supplied by the site's battery backup.

6.1.1.2 The security system shall be supplied by an appropriately sized supply cable and MCB from the site's DC panel.

6.1.1.3 MCB on the AC/DC panel shall be clearly labelled 'Security' to indicate the use.

6.1.1.4 Power will 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:

a) Intruder detection system;

b) Perimeter Cameras;

c) DVR, Indoor cameras and PTZ;

d) Perimeter detection system (if separate from perimeter cameras).

6.1.1.5 Sufficient surge protection shall be installed to protect the system from surges propagating from the supply, as well as from equipment in the yard.

6.1.1.6 The system shall have a power failure alarm indication that shall be sent through to the security control room should the AC supply be interrupted.

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

Figure 1 below shows how the power shall be distributed to the installed alarm system equipment:

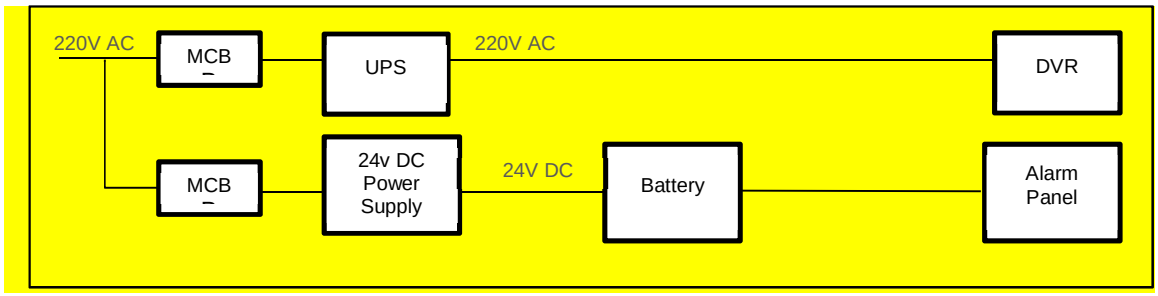

Figure 1: Power distribution to the connected alarm panel

6.1.2 Option B: 220V AC

6.1.2.1 The security system shall be powered by 220V AC supplied from the site's AC supply with an appropriately sized Uninterruptable Power Supply.

6.1.2.2 The security system will be supplied by an appropriately sized supply cable and MCB from the site's AC panel.

6.1.2.3 MCB on the AC/DC panel shall be clearly labelled 'Security' to indicate the use.

6.1.2.4 Power will 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:

a) Intruder detection system;

b) Perimeter Cameras;

c) DVR, Indoor cameras and PTZ;

d) Perimeter detection system (if separate from perimeter cameras).

6.1.2.5 An uninterruptible power supply (UPS) shall be installed to supply the entire CCTV and intruder detection system for a minimum of 12 hours at sites within 200kms of the responsible Eskom DC section, and for a minimum of 18 hours at sites more than 200kms from the responsible Eskom DC section.

6.1.2.6 Batteries other than the UPS batteries are not recommended but where individual subsystems have their own battery backup, these shall not be fed by the UPS. This is to prevent the UPS from charging these batteries in the event of a power failure. The batteries shall provide backup for the time specified above.

6.1.2.7 Sufficient surge protection shall be installed to protect the security system from surges propagating from the supply, as well as from equipment in the yard.

6.1.2.8 The system shall have a power failure intruder detection indication that shall be sent through to the security control room should the AC supply be interrupted.

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

6.1.2.10 The power supply used shall comply with the requirements of SANS 2220-1-7.

6.2 Communication

a) The integrated alarm system shall be an IP based smart solution with capability to integrate with the EBI system integration platform.

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.

6.3 Electrical safety

6.3.1 General electrical safety

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

6.3.1.2 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.

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

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

6.3.1.5 The system shall be protected against transients and lightning surges.

7. Physical requirements

7.1 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 (detectors, outdoor sensors, sirens, PA Speaker, Alarm Status LED) 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.

7.2 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.

7.3 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).

8. EMC

a) The alarm system shall comply to 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.

9. Noise

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

10. 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.

11. Earthing

a) The system shall be earthed to Eskom's earth-mat as per Eskom's earthing standards/specifications and drawings e.g. TST41-877, etc.

12. Maintenance

a) The alarm system shall be designed to provide easy access for maintenance and servicing purpose.

b) Maintenance procedures shall be provided

c) The estimated maintenance frequency and durations shall be specified

d) A repair procedure shall be specified (e.g. on site repair, bring in repair, fixed price exchange) and shall include current costs and time to repair.

e) Spares shall be available 10 years even after the model has been discontinued.

f) The system shall have a minimum of two years guarantee.

g) Faulty equipment shall be replaced within the first year of installation.

h) A warranty repair schedule shall be provided.

i) A 10% spares holding is required.

13. Markings, Labelling and packaging

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

a) the manufacture's name;

b) the model identification;

c) the rated supply voltage and frequency and the rated current;

d) identification of terminals and leads by means of numbers, colours or other.

14. Documentation and drawings

The system shall be supplied together with the following documentation:

a) Performance characteristics;

b) Power supply requirements;

c) Wiring and mounting instructions;

d) Output ratings;

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

f) Installation, commissioning and maintenance procedures;

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

h) 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.

i) Drawings provided shall include the following:

1) All modules and circuit diagrams;

2) Schematic diagrams;

3) Installation drawings.

15. Testing

a) Factory acceptance tests (FAT) will be conducted at supplier premises or at a venue agreed with Eskom.

b) Eskom staff will perform site acceptance tests (SAT).

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

16. Training

a) Product specific training is required to enable the installation, calibration and maintenance of the equipment by Eskom personnel or appointed contractors.

b) The training shall be a supplier-accredited course to ensure correct installation and use of the equipment within Eskom.

c) All training requirements shall be specified.

17. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Willy Majola	Engineering SGM
Prince Moyo	Power Delivery Engineering GM
Danie Odendaal	Plant Engineering GM
Richard McCurrach	Senior Manager – PTM&C CoE
Amelia Mtshali	PTM&C – Metering, DC & Security technology & Support Manager (Acting)
Thomas Jacobs	DC & Auxiliary Supplies SC Chairperson
Andre Bekker	Security Technologies CG Chairperson
Prudence Madiba	Senior Manager – Electrical and C&I Engineering
Elekanyani Ndlovu	Middle Manager – Electrical Plant COE
Martin Strauss	Senior Manager- Group Security
Karen Pillay	Middle Manager- Group Security

18. Revisions

Date	Rev	Compiler	Remarks
April 2015	1	R Moshoeshoe	First issue

19. Development team

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

- Donald Moshoeshoe
- Thomas Jacobs
- Sandi Ndamase

20. Acknowledgement

N/A