

Title: **ANTI-THEFT VIBRATION
SENSOR AND ALARM SYSTEM**

Unique Identifier: **240-170000156**

Alternative Reference Number: **<n/a>**

Area of Applicability: **Engineering**

Documentation Type: **Standard**


Revision: **1**

Total Pages: **16**

Next Review Date: **May 2026**

Disclosure Classification: **Controlled
Disclosure**

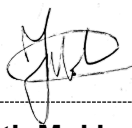
Compiled by



Ockert Fourie
Senior Engineer - LES

Date: 04 May 2021


Supported by



Faith Mokhonoana
**Middle Manager – LES
Inland Cluster**

Date: 04 May 2021

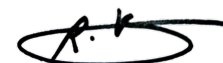
Authorized by



Riaz Vajeth
Senior Manager- LES

Date: 4 May 2021

Supported by SCOT SC



Riaz Vajeth
SCOT SC Chairperson

Date: 4 May 2021

Eskom Stakeholders Consulted:

<u>Name</u>	<u>Functional Responsibility</u>
Cornelius Naidoo	Telecommunications T&S CoE Manager
Moses Tebele	Chief Engineer Eskom Grids
Julie Cheerkoot	Middle Manager Security
Nicolaas de Klerk	Senior Engineer Eskom Dx
Shaun Solomon	Chief Advisor IT

*each of the above technical leaders where supported by their relevant teams

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.....	5
2.2.1 Normative.....	5
2.2.2 Informative.....	5
2.3 Definitions	5
2.3.1 General	5
2.3.2 Disclosure classification.....	6
2.4 Abbreviations	6
2.5 Roles and responsibilities.....	6
2.6 Process for monitoring.....	7
2.7 Related/supporting documents.....	7
3. Operating Conditions.....	7
4. Option selection.....	7
5. Technical Requirements.....	8
5.1 Theft Monitoring Device/Unit	8
5.1.1 General	8
5.1.2 Communication	9
5.1.3 Power	10
5.1.4 Enclosure	10
5.1.5 Time Synchronization	11
5.1.6 Visual	11
5.1.7 Audio	11
5.1.8 Electromagnetic Compatibility (EMC)	12
5.2 Data Monitoring System	13
5.2.1 General	13
5.2.2 Alert Notifications.....	14
5.2.3 Communication	15
5.3 Documentation	15
6. Authorization	16
7. Revisions.....	16
8. Development team	16
9. Acknowledgements	16

1. Introduction

Tower member theft on lattice towers is a serious issue in Eskom Transmission and Distribution and there have been various methods applied to try and combat the issue experienced. Some of these methods include:

- Marking of members with the Eskom logo.
- Installing swaged type bolts under and up to the anti-climbing device (ACD).
- Upgrading the ACD on lattice towers, etc.

Although these methods were effective in some way, they did not curb or successfully prevent the theft of members on lattice-type towers. Theft of tower members poses a serious problem for Eskom Transmission and Distribution as the risk of a complete tower collapse increases, and with that the chances of a lengthy line outage. As a result of this, there is a continuous requirement to replace these stolen and/or damaged tower members. These member theft incidents can sometimes go unnoticed for a period of time due to inspection and maintenance schedules. In some cases, it has led to a worst-case scenario where a complete replacement of the tower and its supporting components was required after it has collapsed as a direct result of tower member theft. The collapse of a tower not only poses a risk to public safety but also to the continuity of power supply. The situation will also have a huge financial implication for Eskom.

With the current anti-theft measures in place, as mentioned above, thieves are forced to cut the members using grinders, cutting torches, hacksaws, etc. in an attempt to steal the members. This cutting action produces a vibration frequency within an identifiable band. These vibration device will detect that the structure is experiencing a vibration frequency within a specified band, it will send out an alert to a central control system to dispatch armed response to the affected site. This alert will be accompanied by either a still image from a camera or a short audio recording (depending on the system selection) in an attempt to take care of false alerts and to positively confirm theft activity at the site. This activity can then be communicated to the relevant Grids to ensure the maintenance of the structures takes place timeously.

2. Supporting clauses

2.1 Scope

This document provides guidance to Eskom Transmission and Distribution when procuring anti-theft vibration detection devices. The standard covers requirements set out for the device with supporting components to be installed on the tower, the data monitoring system to be installed at a central control room as well as the accompanying documentation to be received from the supplier.

2.1.1 Purpose

This document provides guidance to Eskom Transmission and Distribution when procuring anti-theft vibration detection devices.

2.1.2 Applicability

This document applies to Eskom Transmission and Distribution Division

2.2 Normative/informative references

2.2.1 Normative

- [1] IEC 60529: degrees of protection provided by enclosure (IP Code)
- [2] IEC 61000 part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test
- [3] 240 – 55410927 Cyber security standard for operational technology
- [4] IEC 61000 part 4-4: Testing and measurement techniques – Electrical fast transient/ burst immunity test
- [5] IEC 61000 part 4-5: Testing and measurement techniques – Surge immunity test
- [6] IEC 61000 part 4-8: Testing and measurement techniques – Power frequency magnetic immunity test
- [7] IEC 61000 part 4-16: Testing and measurement techniques – Test for immunity to conducted, common mode disturbances in frequency range 0 Hz to 150 kHz

2.2.2 Informative

IEC 61000 part 5-6: Installation and Mitigation Guidelines – Mitigation of External EM Influences

IEC 61000 part 6-5: Generic standards – Immunity for equipment used in power station and substation environment

NRS 083-1: Code of practice for the application of electromagnetic compatibility (EMC) standards and guidelines in electricity utility networks: Part 1 Equipment Standards

NRS 083-2: Electromagnetic compatibility (EMC) in electricity utility networks: Part 2 Substation design and equipment installation practices

NRS 083-3: Electromagnetic compatibility (EMC) in electricity utility networks: Part 3 Secondary equipment installations in substation rooms - Illustrations

2.3 Definitions

2.3.1 General

Definition	Description
Controller	A person based at the security control room responsible for the 24/7 monitoring of the entire system
Activities	A condition in which a person is illegally attempting to remove components attached to Eskom infrastructure.
Control room	A room serving at a central place where a large facility or physically dispensed services can be monitored and controlled
Supplier	In this document the supplier indicates the person/company that tenders for the contract and that supplies the device

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
°C	Degrees Celsius
3G	Third generation cellular data communication
ACD	Anti-Climb Device
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
FOV	Field of View
GPRS	General Packet Radio Service
GPS	Global positioning system
GSM	Global System for Mobile Communications
Hz	Hertz
ICASA	Independent Communications Authority of South Africa
kV	Kilovolt
kW/m ²	Kilowatt per square meter
mm	Millimetre
OHS	Occupational Health and Safety
PSIM	Physical Security Information Management
RFI	Radio Frequency Interference
SIM	Subscriber identification module (sim card)
UV	Ultraviolet
LES	Lines Engineering Services
CoE	Centre of Excellence

2.5 Roles and responsibilities

- It is the responsibility of the compiler to ensure that this document is presented at the relevant Scot SC, LMF and is authorised.
- Lines Engineering Services are responsible for the technical content of this document and the future revisions.
- The Lines & Servitude manager should ensure that these requirements in this report is suitable for specific line installations.

ESKOM COPYRIGHT PROTECTED

- The Lines & Servitudes manager is responsible for the maintenance and good working order of the alarm devices.
- Eskom Telecommunications is responsible for the specification relating to the communication of the device.
- Eskom Zero Control (Eskom Security) is responsible for the monitoring of the system and dispatching of necessary personnel to respond to the alarms on the towers.
- Eskom IT is responsible for the interface of the software at Zero Control.

2.6 Process for monitoring

Not applicable.

2.7 Related/supporting documents

- a) 240-681079090: Tower member theft alarm anti-theft device
- b) 240-133062091: Central grid vibration sensor project for tower member theft

3. Operating Conditions

The equipment shall be suitable for outdoor installation and use on lattice-type structures up to 765 kV. The Equipment shall be designed to operate satisfactorily when subjected to the following operating conditions:

In the vicinity of power lines with the following voltage range	Up to 765 kV
System frequency	50 Hz
Altitude	0 m to 2500 m above sea level
Ambient temperature	from -15 °C to 50 °C
Maximum relative humidity	100 %
Mean annual value of solar radiation	1,0 kW/m ²

4. Option selection

The supplier's device shall be capable to cater for all three options described below and conform to the requirements specified in section 5 of this report.

- a) Vibration detection only
- b) Vibration detection + audio recordings
- c) Vibration detection + Visual image

ESKOM COPYRIGHT PROTECTED

5. Technical Requirements

A conceptual process flow of the anti-theft vibration detection device and alarm system is illustrated in Figure 5-1.

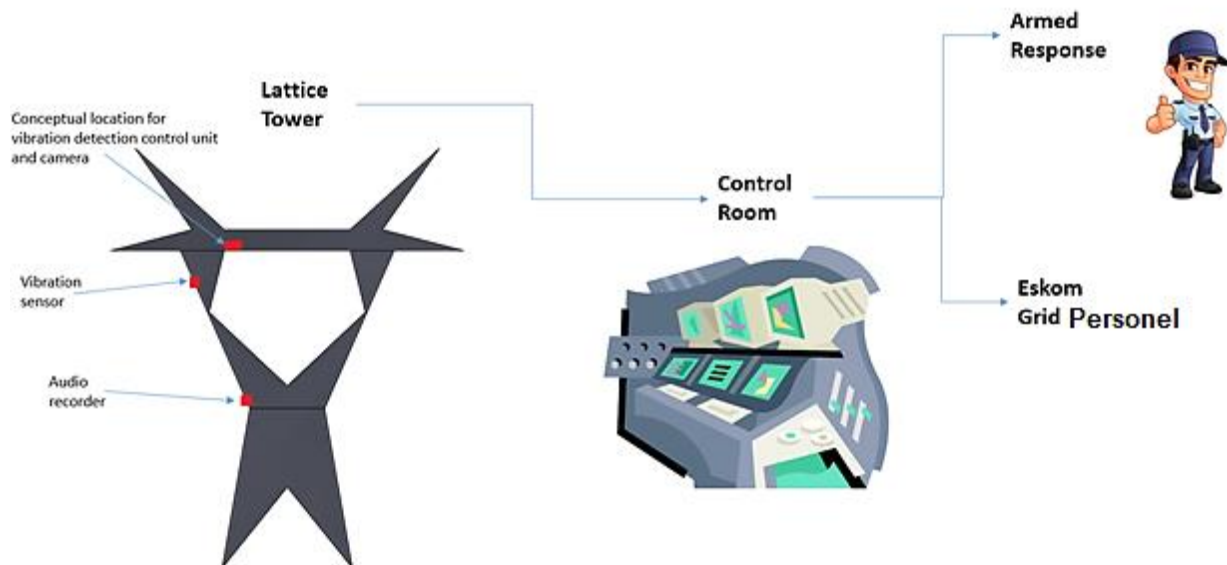


Figure 5-1: Process flow of the anti-theft vibration detection device and alarm system

5.1 Theft Monitoring Device/Unit

5.1.1 General

- a) The unit shall be able to sense all activities occurring at any part of the tower structure when installed at or above the bottom phase cross-arm of the structure that requires protection.
- b) The unit shall detect suspected theft of steel tower members, which occurs in a mode of the following, but is not limited to:
 - 1) Unbolting of the steel member
 - 2) Cutting of the steel member by hacksaw
 - 3) Cutting of the steel member by grinder
- c) The supplier shall clearly state and demonstrate how each mode of theft will be detected during the day and at night.
- d) The unit shall also be able to sense and communicate to the Data Monitoring System any form of tampering of the unit itself.
- e) The unit shall be equipped to handle all of the options described in section 4 to monitor activities on the tower and send alerts to the Controller to view and make appropriate decisions as described in clause **Visual** and **5.1.7**.
- f) The unit shall continue to transmit the alert notifications until the controller has acknowledged a receipt of the alert on the Data Monitoring System.
- g) The supplier shall specify technical parameters like:

ESKOM COPYRIGHT PROTECTED

- 1) Power output
 - 2) Modulation
 - 3) Bandwidth
 - 4) Theoretical achievable Uplink/Downlink data rates
 - 5) The maximum number of sensors that can be monitored per unit.
- h) The supplier shall fully disclose any EMI and RFI mitigation measures from other transmitting devices in the area, as well as from the power system in close proximity.
- i) The unit shall have a built-in GPS location in order to ensure that the location of the unit can be known at any given time.
- j) The unit shall have self-diagnostics to report at least the following:
- 1) Heartbeat/Health check
 - 2) Low battery
 - 3) Battery voltage
 - 4) GPS location
- k) Each unit shall have a collect, repair/replace, re-install, re-commission, and operational support guarantee to ensure a continuous operation of the unit after commissioning.
- l) The installation and maintenance of the devices, in most cases, should occur while the line is live; therefore, the person responsible for the installation and maintenance of the devices should have the required OHS authorisation.
- m) The device should have the capability to log at least 10 events in a memory
- n) All devices installed on Eskom infrastructure is to be owned by Eskom, including sim cards.

5.1.2 Communication

- a) The unit shall communicate wirelessly to the Data Monitoring System. The unit shall be type approved by **ICASA** for use in South Africa. Supplier to provide a type approval certificate.
- b) The system shall use any available wireless technology as a means of communication. The system shall be GPRS and 3G capable.
- c) When making use of a sim card, the card will be embedded in the communication device to deter thieves from targeting the units.
- d) Supplier to ensure communication in areas where cellular coverage is known to be minimal and/or not available. If provided by a non-GSM cellular service provider, provide ICASA telecoms service provider license details.
- e) The unit shall communicate to the Data Monitoring System (detailed in section 5.2 below) all detected activity on tower steel members on a 24/7 basis.
- f) The unit together with the Data Monitoring System shall ensure that suspected theft activities are detected and displayed for the Controller to view as quickly as possible and within a maximum of 2 minutes of the activity occurring.

-
- g) Should the need arise where the controller requires further verification of the activity alert at the tower, the controller should be able to request additional verification from the audio or video device (depending on the system installed). The unit shall respond accordingly through the Data Monitoring System.
 - h) The unit shall be configurable remotely to perform setting changes.
 - i) The device shall conform to Eskom cybersecurity standards for operational technology [3] with AES-256 and IPsec as a minimum.
 - j) When the device detects that the alarm event cannot be sent, it should store the alert information in its memory and try every 5min to resend the event from the device memory until successful alert has been sent.
 - k) In the case that the device detects that the alarm event cannot be sent, it should send a text sms after the second (2nd) failed attempt to a designated number to inform that person of a possible alert.

5.1.3 Power

- a) The unit shall be powered by a suitable battery that can last a minimum of 7 days without being charged;
- b) The microprocessor can be switched into a dormant mode, and only woken up at specified intervals, which should be in line with the sampling rate requirements
- c) Battery/batteries can be charged by solar panel or any other form of charging such as magnetic induction from the current unbalances of the power line phases, or through electric field, taking into consideration that towers are located in remote areas where no electrical services are available;
- d) The solar panel or related charging mechanism shall be supplied with the unit or built into the unit as would be the case for magnetic field or electric field energy harvesting, but not in a way that will produce corona;
- e) The solar panel or related charging shall be able to fully charge the unit battery from the lowest point to maximum within 8 hours;
- f) Battery temperature operating range shall be -15 °C to 60 °C;
- g) The battery shall have a minimum life span of 3 years and easily replaceable at the tower after this period.

5.1.4 Enclosure

- a) The enclosure shall have a minimum rating of IP 65 [1], while still catering for radio or cellular or wifi communication signals to be sent from and received by the unit;
- b) Eskom Holdings name shall be embedded on the outside of the enclosure along with the manufacturer's details;
- c) All components shall be mounted inside the enclosure, unless a specific statement in this document requires a component to be mounted on the outside (i.e. battery, communicator, sensors, and antennae) without causing corona (Eskom may insist on a corona test).
- d) All exposed non-metallic parts to be UV-stabilised for at least 10 years and details of UV additives used shall be provided with the bid.

- e) All metal parts shall have corrosion protection and stainless steel shall be used for all fasteners in order to ensure operation of equipment for a period of at least 10 years or more.
- f) Magnets as an alternative attaching method could be considered.
- g) Enclosure shall be metal, except in areas where radio Wi-Fi or cellular communication antennae may have to be fitted,

5.1.5 Time Synchronization

- a) The unit shall be equipped with a real-time clock (RTC) with leap year support.
- b) The time source in the unit shall have an inherent accuracy of better than 250ms during any 24h period. This means that time lost or gained during a 24h period shall not be > 250ms.
- c) The RTC battery shall provide at least 7 days of total stand by time.
- d) The battery should not need replacing more often than every 10 years under normal operating conditions.

5.1.6 Visual

Each unit shall take still images(when this option is selected) when activities on the towers are detected and send the images to the data monitoring station for the Controller to analyse and make decisions on whether to send armed response personnel or not. The camera used for visual images shall comply with the following:

- a) The camera shall have a Field of View (FOV) and focal point to fit the shortest and tallest structure on the specified line to be able to see the entire footprint of the steel structure. If more than one line is specified, each line will be evaluated individually.
- b) Capture still images day and night;
- c) Images quality should be transferable over at least GPRS, but still, be sufficient that will allow the Controller to make a decision on whether such activity needs to be investigated by the field armed security personnel;
- d) No lighting in the visible spectrum such as flashlights shall be used to take images as this will easily allow suspects to identify the structures where their activities are monitored.

5.1.7 Audio

Each unit shall take an audio recording (when this option is selected) of at least 10s when activities on the towers are detected and send the recording to the data monitoring station for the Controller to analyse and make decisions on whether to send armed response personnel or not. The units shall not emit any audible noise when suspected activities occur as this will have a similar effect as described above.

- a) General mono-directional audio microphone for recording.
- b) Audio compression SPEEX Codec or similar, 16Bit, 80-8000 Hz
- c) Audio inputs 1 x line in (0-2 Vpp, nominal 0.775 Vpp) or Mic in (electret or electrostatic microphone)

5.1.8 Electromagnetic Compatibility (EMC)

The vibration detection control unit should be able to withstand the following EMC requirements as stated in Table 5-1, column 7, to withstand the interference environment that it will be installed in.

Table 5-1: EMC requirements

REFERENCED STANDARD	IEC 61000-6-5 SIGNAL PORT TYPES					HARDENED LEVELS (All signal ports)
	ENCLOSURE PORTS	SIGNAL PORTS	AC INPUT POWER PORTS	DC INPUT POWER PORTS	EARTH PORT	
IEC 61000-4- 2 ESD	3 (8kV Air, 6kV Contact)					4 (15kV Air, 8kV Contact)
IEC 61000-4- 3 Radiated RFI	3 (10 V/m)					X (35 V/m) IEEE C37.90.2
IEC 61000-4- 4 Fast transient burst		4 (2kV/ 1kV)	4 (2kV/ 1kV)	4 (2kV/ 1kV)	4 (2kV/ 1kV)	4 (2kV/ 1kV)
IEC 61000-4- 5 Surge		3 (2kV/1k V)	4 (2kV/1kV)	3 (2kV/1kV)	3 (2kV/1k V)	4 (4kV/ 2kV)
IEC 61000-4- 6 Induced RFI		3 (10V)	3 (10V)	3 (10V)	3 (10V)	3 10V = 140 dB(uV)

ESKOM COPYRIGHT PROTECTED

IEC 61000-4- 8 Magnetic field	2 (3A/m)					4 (40 A/m continuous) 1000 A/m for 1s
IEC 61000-4- 11 Voltage dips ac power			30% for 1 cycle			30% for 1 cycle
IEC 61000-4- 12 Damped ocillatory		2 (1kV/0.5 kV)	3 (2.5kV/1kV)	3 (2.5kV/1kV)		3 (2.5kV/1kV)
IEC 61000-4- 16 Main frequenc y		4 30V continuo us 300V for 1s		4 30V continuous 300V for 1s		4 30V continuous 300V for 1s
IEC 61000-4- 17 AC ripple				10%		10%
IEC 61000-4- 29 Voltage dips DC power				30% & 60% for 100ms		30% & 60% for 100ms

5.2 Data Monitoring System

5.2.1 General

- a) The Data Monitoring System shall be installed at a designated Eskom control room.

ESKOM COPYRIGHT PROTECTED

-
- b) The system shall remotely receive alert information from the field theft monitoring units and send such information to the theft monitoring control room where it will be verified by the controller if it is a positive alarm.
 - c) The system shall be able to provide basic information relating to the field unit status (such as battery check, battery recharge system check, heartbeat, location).
 - d) The system must be able to record every transaction into a database that should be accessible to authorised personnel. Different levels of security should be assigned to allow for administrative rights and read only rights. This information should be easily exported to MS Excel format to provide management information. Records of all armed/disarmed, alarm activities and setting changes shall be recorded. Storage for data to comply with legal requirements.
 - e) Since most problems related to the alert system are false alarms, the supplier shall demonstrate how false alarms are eliminated.
 - f) The application software shall operate in either a stand-alone mode with the capability to operate in a client/server mode within a data centre environment. All networking and server cabinets to be provided by the supplier.
 - g) Proposals should clearly indicate recovery strategy and contingency plan in the event of an application failure and the system information including configurations shall be backed up at least twice in a month.
 - h) The supplier shall provide details of the backup strategy and off-site storage procedures.
 - i) The application software shall be compatible with the Microsoft Windows 10 operating system.
 - j) The supplier shall provide a System Engineer who will be responsible for programming and reconfiguration of the system.
 - k) All infrastructure at the Eskom Control centre is to be owned by Eskom, including any IP on the monitoring system.
 - l) The supplier shall state provision made for integration into a Physical Security Information Management (PSIM) using an appropriate 'Middleware' technology such as Oracle Fusion and provide information on similar products supported by the application.
 - m) The minimum requirements for display screens shall be 21 inches on all data monitoring/viewing stations.

5.2.2 Alert Notifications

- a) The System shall be able to disseminate alert data from individual theft monitoring units and provide the following basic information to the monitoring/viewing stations:
 - 1) Type of event (System, Incident, or Administrative).
 - 2) Date and time of the event in format CCYY/MM/DD; hh:mm:ss.
 - 3) Name of the reporting device.
 - 4) Location of the reporting device in the form of GPS coordinates.
- b) The system shall be able to aggregate the data in graphical presentation with the option of Geographical Information System (GIS) integration.

-
- c) Alert messages shall be colour coded (e.g. yellow, green, orange, red, etc.) on display screens to indicate the status of the alert, this will be defined in pre-determined business rules during the configuration of the system after the contract have been awarded.

5.2.3 Communication

- a) The system shall be able to automatically poll each unit at least once every 24 hours to confirm both its health status and GPS coordinates and send alert information to the control station for all units that have no heartbeat or that has changed location when compared to the previous known position.
- b) The system shall allow a system administrator with the appropriate user-level authorization and two-way factor authentication to remotely configure all field units including arming/on, disarming/off of each unit, and setting changes. This is necessary in cases where maintenance is taking place on the structures and if modifications needs be made on the device.
- c) The system shall automatically check and verify the heartbeat and location of the field units every time when a field unit is armed/re-armed and send an alert to the control monitoring/viewing station. This is to ensure that movement of the field units, while the field units are disarmed/switched-off, are detected.
- d) The system shall also allow the Administrator or Operator to be able to remotely activate or suspend from alarming groups along a length of line the entire platform/units within a specific geographic location or individual units as required for line maintenance.

5.3 Documentation

- a) Full technical and descriptive details, relating to all the items offered in this enquiry, shall be submitted in order for the offer to be fully evaluated. This shall include the following:
- 1) Full technical details of the proposed system which shall include:
 - i Method of communication between unit and central master station;
 - ii Types of sensor used and how detection is done;
 - iii Cost of the System operation;
 - iv Installation requirements;
 - v Operation requirements;
 - vi Method of false signal elimination;
 - vii Expected failure rate as a percentage of Units installed.
 - 2) Details of quality assurance procedures; and
 - 3) Drawings; etc.
- b) The supplier shall submit recommendation documents on how to inspect, test and maintain the theft monitoring units and Data Monitoring System in a good operating condition.
- c) The supplier shall also submit documents on recommended minimum spares.
- d) Failure to submit such information may preclude further consideration of the bid.

ESKOM COPYRIGHT PROTECTED

- e) The successful supplier will be required to obtain design review (Engineering and IT) governance approval for both the basic design as well as the detail design.
- f) All design documents to provide in Eskom approved formats.

6. Authorization

Name and surname	Designation
Riaz Vajeth	Chairman of Lines Scot SC; Senior Manager LES

7. Revisions

Date	Rev	Compiler	Remarks
May 2021	1	OJ Fourie	Device Specification

8. Development team

The following people were involved in the write up of the technical content of this document:

- Ockert Fourie
- Bertie Jacobs
- Cornelius Naidoo
- Matthew Taljaard
- Roy Hubbard
- Arthur Burger
- Nicolaas de Klerk
- Tejin Gosai
- Shaun Solomon
- Craig Moran
- Julie Cheerkoot

9. Acknowledgements

Eskom appreciates the feedback and reference documents from Ethekwini Municipality.