Eskom	Standard	Transmission

Title: **MAINTENANCE STANDARD FOR TRANSMISSION ELECTRONIC PHYSICAL SECURITY SYSTEMS**

Unique Identifier:	**240-170001130**
Alternative Reference Number:	**<n/a>**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**1**
Total Pages:	**61**
Next Review Date:	**May 2029**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Donald Moshoeshoe	**Cornelius Naidoo**	**Judith Malinga**
Chief Engineer – PTM&C	**Middle Manager – Telecoms & Physical Security T&S**	**Senior Manager – PTM&C**
Date: 15/07/2024	Date: 16/7/2024	Date: 22/07/2024

Supported by SCOT/SC

Judith Malinga

Metering, DC & Security SC Chairperson

Date: 22/07/2024

PCM Reference: **240-45920887**

SCOT Study Committee Number/Name: **Metering, DC & Security SC**

Content

Tables

1. Introduction

There is a requirement to document maintenance strategies, which define maintenance that is applicable to the Eskom Transmission and Telecoms Physical Security assets. The initiatives to standardize the engineering design processes dictated that a Maintenance Strategy should be compiled including specifying asset classes/systems. PTM&C Physical Security technologies and support (T&S) was tasked with developing a maintenance standard for secondary plant physical security systems which specifies maintenance requirements for the asset classes and systems.

further to the above, this Maintenance Strategy is also developed to take cognizance of the original design intent of each asset class, and thus, to define the maintenance requirements of each asset class.

The strategy also indicates how maintenance triggers may be affected based on the specific asset functional location (the asset environment, usage, and health). In addition, an ageing analysis indicates intended design life, asset ageing mechanisms, specific asset health indices and calculations to determine useful remnant life. This also serves as primary input to the asset health, technical and economic end-of-life assessments.

2. Supporting clauses

2.1 Scope

This Maintenance Engineering Strategy is applicable to the secondary plant physical security systems in Eskom's Transmission division. All minimum maintenance activities are described down to the lowest level at which Eskom performs maintenance along with the triggers for said maintenance activities and the associated logistics requirements.

The condition monitoring and maintenance activities are prescribed based on the outcome of the asset health analysis, the FMECA and the ageing analyses. Triggers for these maintenance activities are developed based on the criticality assessment and may be influenced by the plant functional location to execute maintenance more often, whilst complying with the minimum requirements provided. Where training or task manuals are deemed necessary, these need to be developed and are indicated as such.

Aging analysis is performed to indicate the operational life of the plant and factors that contribute to the acceleration of the life of that plant. Asset health indicators are developed, and the associated remnant life calculations given.

The scope of this strategy includes:

- Maintenance requirements (Test and Inspection requirements, Preventative Maintenance based on condition / duty, Preventative Maintenance based on time and, Corrective maintenance.
- Maintenance logistic requirements (maintenance spares, special tools and facilities)
- Asset Health requirements
- Asset performance requirements
- Manage Asset Excursion

2.1.1 Purpose

The purpose of this document is to stipulate the maintenance requirements for the secondary plant physical security systems installed at Eskom Transmission substations and Telecoms sites.

Each physical security system asset, in each specific functional location, needs to have consistent asset health monitoring. The asset health monitoring ensures that the appropriate capital, and operational investments, can be made, at the appropriate times, to sustain the operational capability of the asset.

2.1.2 Applicability

This document is applicable to Eskom Transmission and Telecoms sites.

2.2 Normative/informative references

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

2.2.1 Normative

[1] ISO 9001 Quality Management Systems

[2] Act No. 85 Occupational Health and Safety Act, 1993

[3] 240-44509543 Process Control Manual (PCM) for Design System

[4] 240-45920887 Process Control Manual (PCM) for Maintenance of Design Base

[5] 240-45921037 Process Control Manual (PCM) for Optimized Operational Asset Performance

[6] 240-45920941 Process Control Manual (PCM) for Manage Asset Excursion

[7] SANS 1125 Room Air Conditioners and Heat Pumps

[8] SANS 54511 Air Conditioners, Liquid Chilling Packages and Heat Pumps with Electrically Driven Compressors for Space Heating and Cooling

[9] 240-61182655 Maintenance Standard for Substation Electrical Components

[10] 240-171000171 Commissioning guideline for secondary plant physical security systems

[11] 240-180100001 Secondary plant security systems maintenance procedure

[12] 240-170000086 Roles and accountabilities for lifecycle management of physical security systems in the Transmission division

[13] 240-171000100 Training Requirements for physical Security Systems (PSS)

2.2.2 Informative

[14] 240-49230046 Failure Mode and Effects Analysis Guideline

[15] 240-49230148 Maintenance and Logistics Support Design Guideline

[16] 24-49230067 Life Data Analysis Guideline

[17] 240-55922824 Substation Layout Design Guideline

2.3 Definitions

2.3.1 General

Definition	Description
Alarm and Detection System	The system sensors are deployed at strategic locations on the site that requires monitoring and local and / or remote alarms are triggered in the event of any movement in restricted zones within the protected site.
Asset	Any infrastructure that has been established to enable the generation, transmission, distribution, and sale of electricity.

CCTV System	Closed-circuit television (CCTV), also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. Detection of any movement is either done via an external sensor or via video analytics. The footage is used to confirm any unauthorised entry and also for record purposes
Condition monitoring	The monitoring or diagnostic activity that is used to predict or foresee equipment failures (EPRI).
Corrective Maintenance	The maintenance carried out after a failure has occurred and intended to restore an item to a state in which it can perform its required function.
Failure Causes	The circumstances during design, manufacture or use which have led to failure (IEEE). Failure causes describes why, but not how, equipment fails. Failure causes are rarely the root causes of failures and are defined at the level at which maintenance is performed.
Functional Importance – Critical	Applicable to an asset that must operate, as designed, in order: • to meet to meet legal requirements; or • to meet regulatory requirements; or • to ensure safety of people; or • to prevent irreversible environmental harm; or • to prevent economic loss (net profit) of > R99 million; or • to ensure continuity of supply, where not doing so would imply failure to meet one of the above points in the Eskom or public domain.
Functional Importance – Economic	Applicable to an asset which must operate, as designed, in order • to ensure continued income through the provision of services and accurate billing; or • to prevent damage to, or accelerated ageing of asset resulting in economic loss, • such that any economic losses (net profit) are limited to between R100,000 and R1 million.
Functional Importance – Run to Failure	Applicable to an asset where the consequences of failure are acceptable, without preventative maintenance being performed, for a period of time until normal inspection and test activities will determine the failure and correction actions can be carried out. Economic losses are limited to < R100,000.
Functional Importance – Significant	Applicable to an asset which must operate, as designed, in order • to prevent impact on personnel and public; or • to prevent measurable impact on environment; or • to prevent damage to, or accelerated ageing of asset resulting in economic loss; or • to ensure continued income through the provision of services and accurate billing; or • to protect the Eskom brand and reputation, • such that any economic losses (net profit) are limited to between R1 million – R99 million.
Failure Mechanism	The physical, chemical or other process that results in failure. **Note:** The circumstance that induces or activates the process is termed the root cause of failure (IEEE).

Failure Mode	The effect by which a failure is observed to occur (IEEE). A failure mode describes how, but not why, equipment fails.
Failure rate	The actual or expected number of failures in a specified time or specified number of operations.
Integrated Access Control System	It is an electronic system that aims to collaborate and align efforts across the logical and physical security domains in an effort to standardise access control.
Maintenance Engineering Strategy	Maintenance Engineering Strategy refers to the engineering performed during the design process (logistic support analysis) to define the maintenance requirements of the System, Structure or Component (SSC) that serve as primary input to the maintenance execution strategy. This typically include the following: minimum critical spares requirements; maintenance tasks definition; in-service inspection and test requirements; maintenance periodicities and triggers; training requirements; facilities; expected SSC life, etc.
HV Yard	Shall mean any outdoor area enclosed in a safety fence, in which is situated any combination of transforming, switching and / or linking apparatus, together with any associated strung or solid busbar arrangement.
Maintenance Template	A pre-selected set of maintenance tasks for an equipment type, environment, application, etc. These are developed using a logic tree analysis. Maintenance template improves efficiency of task selection (EPRI).
Non-lethal Energised Fence	An electrified physical barrier with an access gate consisting of bare wires erected around the site perimeter against the trespass of persons or animals. The bare wires carry pulses of electric current generated by an energiser to provide a non-lethal shock to deter potential intruders. The system can also detect and alarm any physical interfering with the wires via local – and remote graphical users interfaces (PCs). The structure also includes anti-tunnelling and vegetation slabs.
Power over Ethernet (POE)	Power over Ethernet (PoE switches provide PoE power and network connectivity over twisted-pair wire to access points, surveillance cameras, and other IoT devices)
Public Address System	A public address system (PA system) is an electronic system comprising microphones, amplifiers, loudspeakers, and related equipment. It increases the apparent volume (loudness) of a human voice, musical instrument, or other acoustic sound source or recorded sound or music. In the security context it is used to deter any unauthorised person from entering the site.
Preventative Maintenance	The maintenance carried out at predetermined intervals or corresponding to prescribed criteria (such as measured condition or number of operations). Preventive maintenance is intended to reduce the probability of failure and or, the performance degradation of an item.
Security Control Centres	These are monitoring and control centres where security alarms and CCTV footage are monitored and needed response/s initiated from. The alarms and CCTV footage can be aggregated to a national security control centre that can initiate requisite actions from a national perspective.
Security Lighting	The lights that are installed along the site perimeter for security purposes. This system is integrated with the Non-lethal Energised Fence system to light up specific zones where unauthorised access is detected.

Substation	A site on which is situated any transforming, switching or linking apparatus forming part of the Power System and on which no generating equipment is situated, other than auxiliary generating sets. The term "substation" includes compressor stations, distribution stations, capacitor stations and switching stations.

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
APM	Asset Performance Management
OEM	Original Equipment Manufacturer
CM	Corrective Maintenance
CMMS	Computerized Maintenance Management System
CoE	Centre of Excellence
EPRI	Electric Power Research Institute
FAT	Factory Acceptance Test
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
IEEE	Institute of Electrical and Electronics Engineers
OU	Operational Unit
PID	Perimeter Intrusion Detection
PM	Preventative Maintenance
POE	Power over Ethernet
PSIM	Physical Security Information Management System
SAT	Site Acceptance Test
SSC	System, Structure or Component
TPS	Transmission Physical Security

2.5 Roles and responsibilities

a) The Manager –Design Base Asset Maintenance is responsible for the consistency and process of compiling this maintenance strategy.

b) Transmission Grids & Telecoms Regions are accountable for developing Maintenance Plans in line with this maintenance standard and the subsequent scheduling, work execution and capturing of the relevant information as specified by this standard and job plans and / or task list in the CMMS's.

c) Transmission Grids and Telecoms Regions are responsible for the implementation, operation, and maintenance of the Transmission Physical Security (TPS) systems.

d) The Transmission Grids and Telecoms Regions are responsible for the selection of asset specific maintenance execution strategies per individual asset.

e) Where Transmission Grids and Telecoms Regions cannot comply with any of the specified requirements, such deviations shall be managed as per the Manage Asset Excursion process.

f) Any other secondary plant physical security systems maintenance document developed must comply with the requirements of this maintenance standard.

g) In the absence of an Asset Performance Management (APM) tool, the Manager – Design Base Asset Maintenance is accountable to provide templates which allows for manual implementation of the requirements of this standard.

h) Transmission Security– Responsible for auditing the physical security systems and ensure that the systems are installed and maintained according to the associated installation and maintenance standards.

i) Customers – Responsible for providing the current and future requirements. Customers shall participate in the standards development through SCOT.

2.6 Process for monitoring

The Manager – Design Base Asset Maintenance will monitor the effectiveness and consistency of adoption of this standard through established report formats which will be sent to the Transmission Grids & Telecoms Regions to provide the required information.

2.7 Related/supporting documents

Not applicable.

3. Requirements

3.1 Asset identification

This Transmission Physical Security maintenance standard includes the following systems:

a) Chassis and its peripherals (including fan(s))

b) Electric fence energizers

c) Access control system controllers and motors

d) Alarm system controllers

e) CCTV system DVRs/NVRs and cameras

f) Public address system controllers

g) Perimeter intrusion pre-detection system controllers

h) Intercom systems controllers

i) Physical security Information Management Systems (PSIM)

Note: The word chassis in this document is used in general terms to refer to a housing for security equipment modules.

Table 1 below shows the core components of the currently installed security systems with their associated OEM's.

Table 1: Typical physical Security systems installed

Equipment category: Electric fence energizers	
Typical Equipment Installed	**OEM**
BS120 energizer	Stinger electronics
M28S energizer	Nemtek
Druid 28 LCD energizer	Nemtek
Stealth Master M28SM energizer	Nemtek
M18 energizer	Nemtek
JVA Z18 energizer	Stafix
Equipment category: Gate motors	
Typical Equipment Installed	**OEM**
D10 sliding gate motor	Centurion systems
Vector 500 sliding gate motor	Centurion systems
24VDC elite sliding gate motor	Hansa
Equipment category: Access control systems	
TBS alarm system	TBS
Net2 plus ACS controller	Paxton
Equipment category: Alarm systems	
Typical equipment installed	**OEM**
SP 6000 alarm system	Paradox
INTEGRA + 64 controller	Satel
DCS alarm system	DCS
Orisec alarm system	Orisec
Equipment category: CCTV Systems	
Typical equipment installed	**OEM**
Uniview video surveillance system	Uniview Technologies
Alhua video surveillance system	Alhua
Equipment category: Public Address System	
Typical equipment installed	**OEM**
TOA PA system	TOA Electronics
Equipment category: Intercom systems	
Typical equipment installed	**OEM**

Akuvox intercom system	Akuvox
Equipment category: Intrusion Pre-detection Systems	
Typical equipment installed	**OEM**
Moduteq WI-I PIDS	Moduteq
Equipment category: Security Management systems	
Typical equipment installed	**OEM**
Winguard PSIM system	Advancis

Note: detailed list of typical equipment installed is included in Annex B

3.2 Design intent

Maintenance requirements contribute to achieving the design intent, i.e. what the maintenance should sustain. In order to accurately specify the maintenance requirements, it is necessary to understand the design intent in terms of the intended purpose:

The purpose of each Transmission Physical Security asset or component needs to be known to provide maintenance to each component and to the overall physical security.

Table 2: Physical security systems descriptions

Security System		Design Intent
Electric Fence System	a.	Also referred to as Non-Lethal Energised Perimeter Detection System (NLEPDS), the electric fence system secures Eskom property and ensures the safety of personnel and assets. It secures what's inside the protected area.
	b.	The electric fence system is an excellent security deterrent to burglary, vandalism and trespassing. It restricts ease of unauthorised entry to the protected area by the outside parties.
	c.	It provides a non-lethal electric shock to a human or animal that touches any of the positive and negative conductor wires simultaneously. The shock delivers sufficient joules to provide severe discomfort to the subject, it is low in current (the lethal component) and high in voltage (the shock discomfort component).
	d.	A quality electric fence system provides a standby service time that is equivalent to the standby time of the protected site when the site AC power is down.
	e.	The electric fence system communicates the location/zone of the intruder or disturbance along the protected site perimeter to the control room (both locally and remotely).
Access Control system	f.	The Access Control Systems (ACS) provides access to authorised employees and contractors using access cards, remote control units and the finger printing (biometric scanning).
	g.	The sliding gate system is a key component to provide authorised delivery, entry and exiting of tools, equipment, and construction raw materials.
	h.	Ensures that only authorised persons are allowed in certain zones and that personnel are allowed in certain work locations based on their operational roles.
CCTV System	i.	Provides a visual monitoring of activities in and around the protected site in real time.
	j.	Provides visual monitoring without a person having to be there and possibly in a dangerous situation

	k.	Provides more effective communication of information that surpasses human to-human communication of information at a time. The visual information can provide live information to multiple parties simultaneously.
	l.	Provides pan, tilt, zoom, wide angled view, thermal detection functionalities which allow for a situation to be analysed and action taken accordingly, much quicker.
Public address system	m.	Referred to as PA system - is an electronic system comprising of microphones, amplifiers, loudspeakers, and related equipment. It increases the apparent volume (loudness) of a human voice, musical instrument, or other acoustic sound source or recorded sound or music.
	n.	Provides a deterrence to intruders from trespassing, stealing or vandalising.
	o.	Provides a further legally required warning to trespassers, thieves, and vandalisers.
Intrusion Pre-Detection System	p.	The intrusion pre-detection sensors provide detection of intrusion prior to intruders gaining access to the protected sites and issues a warning to the local security office and at the remote security control Centre.
Intercom System	q.	The intercom system provides a means to communicate effectively with colleagues that are not within hearing range.
	r.	The perimeter intercom warns intruders that they are trespassing and that they need to move away from the protected site.
Security information management system (PSIM)	s.	PSIM (Physical Security Information Management system) is a category of software that provides a platform and applications created by middleware developers, designed to integrate multiple unconnected security applications and devices and control them through one comprehensive user interface.
	t.	The PSIM integrates the hardware and the software components (that can practically be integrated) into an effective security management system.
	u.	The PSIM is a major contributor towards reaching the intended design life of the substation facility components.
Switch	v.	Small form-factor pluggable (Transceiver Modules support Ethernet, Sonet / SDH and Fibre Channel applications)
	w.	Power over Ethernet switches provide PoE power and network connectivity over twisted-pair wire to access points, surveillance cameras, and other IoT devices)
Firewall	x.	The firewalls provide safety for the IP communication and prevent hackers from illegally accessing the security data.
Server	y.	The server systems provide storage facilities for the video recordings.

3.3 Maintenance Engineering Strategy

The TPS Maintenance Strategy refers to the original engineering design intent, to identify the asset care that each component requires:

a) Maintenance task determination

b) Asset and maintenance data required

c) Identify the required Task manuals

d) Maintenance spares

e) Facilities and training requirements

3.3.1 Maintenance Task Determination

a) The generic maintenance activities and triggers are derived from the FMECA study, (refer to Appendix A).

b) The maintenance activities from the FMECA studies are collated and grouped into different tasks in the maintenance activity (refer to table 3 below).

c) The Maintenance tasks are created based on the following:

i. Common outage requirements for the maintenance to be undertaken. (The Electricity requirements / **what** is required)

ii. Common craft requirements for the maintenance to be undertaken. (The skill required / **who** may perform the duty)

iii. Common trigger requirements as to when the maintenance must be undertaken. (The timing requirements / **when** it must be done)

d) These tasks become job plan titles and task list titles in SAP.

e) The activities form the job operational steps in job plans / task lists

Table 3: Maintenance activities

Equipment Class:		Physical Security Systems									
Equipment Sub Class:											
Equipment Sub Class Family:											
Trigger Modifiers		Permutations	1	2	3	4	5		Key		
	Functional Importance	Critical	X	X					1M	One monthly	
		Significant			X	X			6M	Once every six months	
		Economic					X		1Y	Once every year	
	Environment	Harsh		X	X						
		Mild	X			X	X				
Activity No	Maintenance Activities	FMECA Ref No	Trigger (Time and/or Status)					Outage Y/N	Manual Y/N	Quality Criteria	
Condition Monitoring											
1	Visual Inspection of dust on ventilation pores of the chassis and kiosks	1.2	3Y	2Y	3Y	2Y	3Y	N	Y	The dust shall not clog the breathing pores of the chassis and kiosks	
2	Visual Inspection of dust on fans	1.3	3Y	2Y	3Y	2Y	3Y	N	Y	There must be no built-up dust deposits on the fan blades	

3	Visual Inspection of the mechanical condition of fans	1.3	3Y	2Y	3Y	2Y	3Y	N	Y	The fans shall run smoothly without funny noise. The sound must suggest that the fans are not being overworked.
4	Visual Inspection of chassis to cabinet earth ground connections and cabinet (gland plate) to station earth connection	1.1	3Y	2Y	3Y	2Y	3Y	N	Y	The chassis must be earthed to the ground copper bar of the cabinet and the cabinet must be earthed (gland plate) to station earth.
5	Visual Inspection for surge arrestor condition	1.8,1.12	3Y	2Y	3Y	2Y	3Y	N	Y	The surge arresters must not be blown.
6	Visual Inspection of cables and mechanical condition of connectors	1.13,1.14,1.15	3Y	2Y	3Y	2Y	3Y	N	Y	Cables radius must be within the acceptable standard stipulated in the installation guides. Connectors must not be bent and squeezed by the cabinet door.
7	Visual Inspection of latches of the modules and cables latching clips	1.7,1.9,1.11	3Y	2Y	3Y	2Y	3Y	N	Y	Module latches must be locked.
8	Visual Inspection of the cable labels	1.13	3Y	2Y	3Y	2Y	3Y	N	Y	Cables must be labelled as per the standard.
9	Measurement of the ambient temperature and humidity	1.4	3Y	2Y	3Y	2Y	3Y	N	Y	The ambient temperature where the equipment is operating must meet the OEM requirements.

10	Perform active hot standby fail over test for the PSIM	1.16	2Y	1Y	2Y	1Y	2Y	N	Y	When the main PSIM server is disconnected, the standby server shall take over the Security management responsibilities without a glitch and human intervention.
Preventive Maintenance based on Time										
11	Cleaning of dust on ventilation pores of the chassis	1.2	Failed chassis dust inspection	Failed chassis dust inspection	Failed chassis dust inspection	Failed chassis dust inspection	Failed chassis dust inspection	N	Y	The chassis must be clean with no dust deposits on the surface
12	Cleaning of dust on fans	1.3	Failed fan dust inspection	Failed fan dust inspection	Failed fan dust inspection	Failed fan dust inspection	Failed fan dust inspection	Y	Y	The fans must be clean with no dust
13	Update of PSIM software patches and antivirus on the clients	1.16,1.18	1M	1M	1M	1M	1M	Y	Y	The firmware and the PSIM software patches shall be up-to-date as per the OEM. Antivirus on the PSIM client machines shall be up-to-date.

14	Generate on site and off site PSIM backups	1.16,1.18	1M	1M	1M	1M	1M	N	Y	PSIM backups shall be generated and be stored on site and also off site.
Corrective Maintenance:										
15	Inspect and clean dust on ventilation pores of the chassis	1.2	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	N	Y	In the case of temperature/ heating equipment alarm, the dust on the chassis must be cleaned
16	Inspect and clean dust on the fans	1.3	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Y	In the case of temperature alarm/ heating equipment, the dust on the fans must be cleaned

17	Inspect and replace the damaged chassis. Ensure that the chassis ground connection is installed correctly. Cabinet must be earthed (gland plate) to station earth.	1.1	Alarm, failed services	Alarm, failed services	Alarm, failed services	Alarm, failed services	Alarm, failed services	Y	Y	A new chassis must be installed and the chassis to ground connection must be installed correctly. Cabinet must be earthed (gland plate) to station earth.
18	Inspect, test and replace the damaged surge arrestors	1.12	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Y	New surge arresters shall be installed if the installed one is blown.
19	Inspect and replace the damaged connectors	1.15	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Y	New cables and connectors shall be installed and cables be bent at acceptable radius.

20	Inspect and replace the damaged chassis	1.1	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Y	A new chassis must be installed. Circuits created on the new chassis must be tested as per the ATPs.
21	Inspect, test and replace the damaged module	1.5,1.6,1.7,1.8,1.9,1.10,1.11	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Y	A new module must be installed. Circuits created on a new module must be tested as per the ATPs.
22	Inspect and tighten the latches of the modules and cables latching clips	1.7,1.9,1.11	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Y	No modules shall have open latches, the lathes must be locked
23	Inspect and replace the damaged cables. Label the installed cables.	1.13	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Y	Damaged cables shall be replaced and labelled.
24	Set or repair the air conditioner for the correct temperature and humidity	1.4	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Y	The air conditioner shall be set to the OEM temperature requirements.

25	Inspect, test and swap out the damaged PSIM hardware	1.16,1.17	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Y	Y	A new PSIM hardware must be installed.
26	Fix the PSIM network errors	1.19	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Y	Y	PSIM shall have visibility of the network and also be able to provision services.

Note: the outage mentioned in the table above refers to the associated security system outage, not the substation electrical system outage. The services refer to security systems services.

3.3.2 Required task manuals

If the specific equipment requires an installation manual, it should be available from the CMMS. All the kinds of maintenance (Scheduled preventive, Condition preventive, corrective and statutory maintenance) on each equipment type, should be referred to in the FMECA table and in the maintenance activity table. The CMMS, the FMECA, and Maintenance Activity tables should all be updated and referred to. This will prevent maintenance activities being neglected or 'falling through the cracks'. Refer to the secondary plant security maintenance procedure (240-180100001) for equipment specific checks.

Table 4: Task manuals

Task Manual	Task	Intent
Routine inspections	Routine inspections	Visual inspections: • Visual Inspection of dust on ventilation pores of the chassis/kiosks • Visual Inspection of dust on fans • Visual Inspection of the mechanical condition of fans (funny noises) • Visual inspection of chassis to cabinet copper earth bar connections and cabinet (gland plate) to station earth connection. • Visual Inspection for surge arrestor condition • Visual Inspection of cables and mechanical condition of connectors • Visual Inspection of latches of the modules and cables latching clips • Visual Inspection of the cable labels • Measurement of the ambient temperature and humidity • Performance of PSIM active hot standby fail over test
PSIM Backups and software upgrades	PSIM backups and software upgrades	• Update of PSIM software patches and antivirus on the client machines • Generate on site and off-site PSIM backups (at least two geographical locations)
Corrective maintenance	Corrective maintenance	• Inspect and clean dust on ventilation pores of the chassis • Inspect and clean dust on the fans • Inspect and replace the damaged chassis. Ensure that the earth connection is installed correctly. The cabinet must be earthed (gland plate) to station earth. • Inspect, test and replace the damaged surge arrestors • Inspect and replace the damaged connectors • Inspect, test and replace the damaged modules • Inspect and tighten the latches of the modules and cables latching clips • Inspect and replace the damaged cables. Label the installed cables.

		• Set or repair the air conditioner in the ACB equipment room for the correct temperature and humidity. • Inspect, test and swap out the damaged PSIM hardware • Fix the PSIM errors

3.3.3 Maintenance spares

3.3.3.1 Critical spares

Table 5 below lists the critical maintenance spares group for Transmission physical security systems.

Table 5: Transmission physical security systems critical spares

Item	Description
1.	Power supply modules, associated OEM power cables and power supply trays
2.	Controllers for respective systems (alarm system, PA system, ACS, IPDS, fence systems etc)
3.	Physical Security Information Management system (PSIM) servers
4.	Physical Security Integrated Management (PSIM) Client machines
5.	2.24 mm galvanised steel Fence conductor
6.	Energizers
7.	12V 7AH batteries
8.	NVRs/DVRs
9.	24V DC sliding gate motors
10.	24V motor chargers
11.	Two button ET TX remote (434Mhz)
12.	4 Button ET TX remote (434 Mhz)
13.	lightning & surge protection units
14.	Cameras
15.	Biometric readers and card readers
16.	Keypads for respective systems (alarm system, PA system, ACS, IPDS, fence systems etc)

3.3.3.2 Non-critical Spares

Table 6 shows the list of electronic physical security systems equipment noncritical spares:

Table 6: Transmission physical security systems non-critical spares

Item	Description
1.	Mounting brackets

Item	Description
2.	accessories (e.g. zoning boards, connectors, ferrules)

a) OU's / Grids are to determine the stock levels required based on:

i. failure rates,

ii. on hand availability of spares and market availability of spares and

iii. lead time for spares

b) These three determinants: the CMMS, the FMECA table and the Maintenance Activity table, should be the major input into the maintenance spares holding decisions.

c) Another determinant shall be the recommended spares holding from the OEMs and the installers (OEM's recommended installers).

3.3.4 Facilities and training material

The training requirements for this maintenance standard, forms part of the general inspection and care requirement for each component. The physical security training modules will ensure that the asset maintenance is executed properly, and safely, by skilled, and competent, staff. Skills shall be continuously developed and maintained to adequately maintain the physical security of all transmission related infrastructure. Refer to the guideline for training requirements for physical security systems (240-171000100) for detailed training requirements.

3.4 Maintenance Execution Strategy

a) The Maintenance Execution Strategy refers to the asset specific maintenance tasks and triggers, which the Grids and OUs use, for the creation of Maintenance Plans.

b) An asset risk framework (Asset classification) is adopted, which is based on:

i. defined Asset Conditions (health),

ii. Environmental conditions,

iii. Usage / Duty Cycle, and

iv. Functional importance (That is the criticality, based on, the consequence of failure and other Operational factors)

c) The asset risk framework falls within the parameters of this TPS Maintenance Strategy.

d) To select the optimal maintenance triggers for the creation of PM tasks, the following components of the maintenance execution strategy are to be carried out:

i. Asset classification

ii. Maintenance task selection

3.4.1 Asset classification

In order to ensure that the Operating Units and Grids classify individual assets in a consistently similar manner, tables are provided below.

Questions to be answered below are designed to lead to the most appropriate maintenance strategy for TPS equipment. The first 'Yes' answer will determine the classification of the TPS equipment, and the remaining questions, for that section, are to be ignored.

Table 7: Asset classification

A. Functional Importance	Critical	Significant	Economical
In the equipment directly impacting the Centralised operational and functional capabilities to integrate multiple unconnected security applications and devices and control them through one comprehensive user interface?	Yes		
Is the equipment directly impacting site level subsystems control functions?		Yes	
Is the answer to questions above 'No'?			Yes

B. Operating Environment	Harsh	Mild
Is the equipment installed outside the access control building (ACB) equipment room (or similar room) with uncontrolled temperature, dust, and humidity?	Yes	
Is the equipment installed inside the access control building (ACB) equipment room (or similar room) with controlled temperature, dust, and humidity?		Yes

3.4.2 Maintenance task selection

a) The Maintenance tasks in Table 8 below, are created based on the maintenance task determination.

b) The maintenance task table is used by the maintenance planner, to identify maintenance tasks & triggers for the PM tasks. These PM tasks need to be created in the CMMS, for each asset, which this standard applies to.

c) The Interpretation of the maintenance task table is as follows:

i. **Trigger Modifiers:** The trigger modifiers determine the Asset Classification tables (refer to table 7 above). Trigger modifiers determine maintenance frequencies.

ii. **Permutations:** The permutations are a combination of the response options to the different trigger modifiers. An asset can either be in a harsh or a mild environment, but never in both.

iii. **No's 1,2,3…..n:** Each of these numbers represent a unique maintenance execution strategy for the asset class. Each maintenance task is subsequently referenced to the column where this number lies.

iv. **Maintenance Tasks:** Maintenance tasks represent a grouping of maintenance activities.

v. **FMECA: reference**: The FMECA reference provides the link between the maintenance tasks and the FMECA study in appendix A.

vi. **Trigger**: The trigger indicates whether the maintenance should be carried out or not. The yes or no decision is based on:

- The condition status
- The time based (elapsed time since last maintenance) or
- Run to failure (where corrective maintenance is initiated).

vii. **Key:** The maintenance key is a legend for the maintenance frequencies identified. For instance, 6M means that the maintenance task needs to be carried out every six months.

viii. **Outage:** A 'Y' indicates that a security system outage is required to carry out the maintenance task.

ix. **Skills level:** Where specified, this indicates whether specialised skills are required to carry out a specific task or not. (Y/N)

Table 8: Maintenance Tasks

Equipment Class:		Electronic physical security systems									
Equipment Sub Class:											
Equipment Sub Class Family:											
Trigger Modifiers		**Permutations**	**1**	**2**	**3**	**4**	**5**		**Key**		
	Functional Importance	Critical	X	X					1 M	One monthly	
		Significant			X	X			6 M	Once every six months	
		Economic					X		1Y	Once every year	
									2Y	Once every two years	
	Environment	Harsh		X		X					
		Mild	X		X		X				

Ref	**Routine inspections**	**Activity No**	**Trigger (Time and/or Status)**					**Outage Y/N**	**Skill Level**
1	**Routine inspections**	1,2,3,4,5,6,7,8,9,10,11,12	3Y	2Y	3Y	2Y	3Y	N	Field Technician
2	**PSIM Backups and software upgrades**	13,14	1M	1M	1M	1M	1M	N	PSIM administrator
3	**Inspect and clean dust on ventilation pores of the chassis**	15	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	N	Field Technician

4	**Inspect and clean dust on the fans**	16	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Equipment qualified installer
5	**Inspect and replace the damaged chassis. Ensure that the chassis to cabinet copper earth bar connection is installed correctly. The cabinet must be earthed (gland plate) to the station earth.**	17	Alarm, failed services	Alarm, failed services	Alarm, failed services	Alarm, failed services	Alarm, failed services	Y	Equipment qualified installer
6	**Inspect, test and replace the damaged surge arrestors**	18	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Equipment qualified installer
7	**Inspect and replace the damaged connectors**	19	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Equipment qualified installer
8	**Inspect, test and replace the damaged module**	21	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Equipment qualified installer
9	**Inspect and tighten the latches of the modules and cables latching clips**	22	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Equipment qualified installer
10	**Inspect and replace the damaged cables. Label the installed cables.**	23	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Equipment qualified installer

11	**Set or repair the air conditioner for the correct temperature and humidity**	24	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Alarm, failed services, substandard performance	Y	Field Technician
12	**Inspect, test and swap out the damaged PSIM hardware**	25	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Y	Equipment qualified installer
13	**Fix the PSIM errors**	26	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Alarm, failed services, network visibility lost	Y	Equipment qualified installer

The following is the breakdown of equipment maintenance tasks:

3.4.3 Routine inspection

The following activities constitute the routine inspection maintenance task:

a) Check the clogging of dust on the ventilation pores of the chassis

b) Check the clogging of dust on the fans

c) Check the mechanical condition of fans by listening to the abnormal noise and speed

d) Check the chassis to cabinet copper earth bar connection and ensure that earth connection is in place. The cabinet must be earthed (gland plate) to the station earth.

e) Check the surge arrestor condition to ensure that the surge arrester is not blown and is installed properly.

f) Check the cables condition and mechanical condition of connectors

g) Check the latches of the modules and cables latching clips

h) Check if all the cables are labelled as per the standard

i) Measure the ambient temperature and humidity in the room where equipment is installed

j) Perform PSIM active hot standby test

3.4.4 Preventative Maintenance

The following activities constitute the preventative maintenance task:

a) Generate on site and off site PSIM backups

b) Upgrade software, check licences, firmware and update antivirus on PSIM client machines

3.4.5 Corrective Maintenance

The following activities constitute the corrective maintenance task. All the replaced equipment including the provisioned circuits shall be tested as per equipment ATPs:

a) Inspect and clean dust on ventilation pores of the chassis

b) Inspect and clean dust on the fans

c) Inspect and replace the damaged chassis. Ensure that the chassis is earthed correctly to the cabinet copper earth bar. Cabinet must be earthed (gland plate) to the station earth.

d) Inspect, test and replace the damaged surge arrestors

e) Inspect and replace the damaged connectors

f) Inspect, test and replace the damaged modules

g) Inspect and tighten the latches of the modules and cables latching clips

h) Inspect and replace the damaged cables. Label the installed cables.

i) Set or repair the air conditioner in the ACB equipment room for the correct temperature and humidity

j) Inspect, test and swap out the damaged PSIM hardware. Should it be necessary, recover the configuration from the backups.

k) Fix the PSIM errors

3.5 Plant, maintenance and test data to be recorded

The following minimum asset data must be captured in the Computerized Maintenance Management System (CMMS) to suitably describe the asset.

3.5.1 General Supplier/OEM data

As a general rule, the OEM information (asset data) of all physical security systems equipment listed in the CMMS should include the following information:

a) OEM
b) Global and Local Website
c) Physical Address / Area in RSA
d) Name of Product Specialist
e) Product Specialist Mobile Number
f) RSA Support Email
g) WhatsApp Contact / Emergency / After Hours Number
h) Name of Salesperson
i) Landline Telephone Number
j) Salesperson Mobile Number
k) Salesperson Email Address
l) Recommended Spares Holding
m) General OEM and Supplier Recommendations

3.5.2 General equipment data

a) Broad Category of Equipment Type
b) Equipment make and Model number
c) Equipment Picture
d) Manufacturing Year
e) Installation and commissioning date
f) Site name
g) Floor/building name
h) IP address
i) Serial number
j) MTBF / Mean Time Between Failures
k) Currently Installed Firmware version (software)
l) When any patches or upgrade will be or were required, and if that patch is still available.
m) Product (hardware and software) Obsolete Date / When product support ends
n) Operating Power
o) Rated Voltage

3.5.3 NLEPDS

The NLEPDS equipment should have the following additional information listed in the CMMS:

a) Energizer type

b) Date the new battery was installed and expected operating life

3.5.4 CCTV system

The CCTV equipment should have the following additional information listed in the CMMS:

a) NVR type

b) NVR name

c) Camera type

d) Camera name

3.5.5 Gate motors

a) Gate motor make and model

b) Motor mechanism (swing/sliding)

3.5.6 Access Control Systems (ACS)

The access control system should have the following additional information listed in the CMMS:

a) ACS controller type

b) Type of card/biometric reader

c) Controller name

d) Controller position

3.5.7 Alarm systems

The alarm system equipment should have the following additional information listed in the CMMS:

a) Alarm panel type

b) Alarm panel name

c) Alarm panel position

3.5.8 Public Address System

The public address system equipment should have the following additional information listed in the CMMS:

a) Speaker type

b) Speaker names

c) Speaker position

3.5.9 Intercom Systems

The intercom systems should have the following additional information listed in the CMMS:

a) Floor/building name

b) Device

3.5.10 Perimeter intrusion detection systems (PIDS)

The PIDS should have the following additional information listed in the CMMS:

a) Sensor/detector type

b) Detector zone

3.5.11 Firewalls

The firewalls should have the following additional information listed in the CMMS:

a) Firewall Model
b) Firewall Name
c) Firewall position
d) Operating system installed

3.5.12 PSIM system Servers

The PSIM servers should have the following additional information listed in the CMMS:

a) Server model

b) Server name

c) Server position

d) Operating system installed

3.5.13 Workstations

The workstations should have the following additional information listed in the CMMS:

a) Floor/building position

b) Workstation model

c) Workstation name

d) Operating system installed

3.5.14 Switches

The switches should have the following additional information listed in the CMMS:

a) Floor/building position

b) Switch type

c) Switch name

d) Switch position

3.5.15 Inspections and Tests (IT), Preventative Maintenance (PM), Corrective Maintenance (CM) and Investigation (I) Data

The following minimum plant data shall be captured in the CMMS to suitably capture what is noted during inspections and tests (including Factory Acceptance Test (FAT) and Site Acceptance Test (SAT) where relevant to a specific asset), preventive and corrective maintenance as well as investigations, if relevant.

Table 9: CMMS plant data

Maintenance task/data	Data type	Source	Source activity
1. Routine inspection			
1.1 Clogging of dust on the ventilation pores of the chasses	Good/bad condition	Report	I
1.2 Clogging of dust on the fan	Good/bad condition	Report	I
1.3 Fan condition	Good/bad condition	Report	I
1.4 Chassis and cabinet earthing	Good /bad condition	Report	I
1.5 Surge arrestor condition	Good/bad condition	Report	I
1.6 Cables and connectors condition	Good/bad condition	Report	I
1.7 Latches of the modules and cables latching clips	Loose/tight	Report	I
1.8 Cable labels as per the standard	Acceptable/ not acceptable	Report	I
1.9 Ambient temperature and humidity	Degrees Celsius, %: No	Report	IT
1.10 Active hot standby failover test	Pass/fail	Report	IT
2. **PSIM backups**			
2.1 On site and off site PSIM backups	Pass/Fail	Report	IT
3. **Preventative Maintenance**			
3.1 Cleaning of dust on ventilation pores of the chassis	Report	Report	PM
3.2 Cleaning of dust on fans	Report	Report	PM
3.3 Dispatch PSIM software patches and antivirus on the clients	Report	Report	PM
4. **Corrective maintenance**			
4.1 Inspect and clean dust on ventilation pores of the chassis	Report	Report	CM
4.2 Inspect and clean dust on the fans	Report	Report	CM
4.3 Inspect and replace the damaged chassis. Ensure that the earth connection is installed correctly. The cabinet must be earthed (gland plate) to the station earth.	Report	Report	SAT
4.4 Inspect, test and replace the damaged surge arrestors	Report	Report	SAT
4.5 Inspect and replace the damaged connectors	Report	Report	SAT

Maintenance task/data	Data type	Source	Source activity
4.6 Inspect, test and replace the damaged modules	Report	Report	SAT
4.7 Inspect and tighten the latches of the modules and cables latching clips	Report	Report	SAT
4.8 Inspect and replace the damaged cables. Label the installed cables.	Report	Report	SAT
4.9 Set or repair the air conditioner for the correct temperature and humidity	Report	Report	SAT
4.10 Inspect, test and swap out the damaged PSIM hardware	Report	Report	SAT
4.11 Fix the PSIM errors	Report	Report	SAT

Note: Refer to 240-180100001 for a guideline on maintenance tasks for the respective security systems.

3.6 Asset Performance

Asset performance measures should be introduced to monitor and report performance of the Physical Security Systems. This should include both manual monitoring by grid personnel together with the automated reporting capability of the physical security information management system (PSIM).

3.6.1 Failure causes to be recorded in performance management systems

To enable the trending of failure causes and to monitor the effectiveness of the Maintenance Engineering and Execution Strategies in preventing failures, it is required that incidents be investigated and the root cause/s of the failures be determined and captured in the appropriate systems. Standard failure causes, as identified in the FMECA, are listed below such that these specific names can be captured in the CMMS and Performance Management System.

Table 10: Failure causes

Component	Failure mode	Root cause
Physical Electric fence	1. Fence/supports damaged or missing	Vandalism and environmental damage
	2. Circuitry failure	Poor workmanship and environmental damage
Electric fence electricity	1. Energiser not working	PC board failure / AC supply / setup incorrectly / zone setup faulty
	2. Fence wires touching	Break in / poor workmanship / poor material
	3. Break in a wire	Break in / poor workmanship / poor material
	4. Grounding insufficient	Insufficient grounding rod / poor connections
	5. Fence/supports damaged or missing	Vandalism and environmental damage
	6. Circuitry failure	Poor workmanship and environmental damage
ACS sliding gate motor	1. Not working	No AC supply / battery dead / poor communication wiring

	2. Partial open and close	Incorrect software settings / hardware settings / stop function
	3. Wheel not connecting to the sliding gate rack	Sprocket wheel incorrectly mounted / gate rack buckled
Biometric reader	1. Not providing access	Fingerprint not registered / database not picking it up / wiring is damaged
Card reader	1. Not providing access	Card not registered / database not picking it up / wiring is damaged
Storage controller	1. Not providing access	Database corrupted / rack hardware damaged
Alarm system	1. No sound	Speaker blown
	1. No sound	Wiring chewed by rodents / damaged
	1. No sound	Amplifier damaged
	1. No sound	Alarm detection faulty
CCTV system	1. No picture	Wiring is damaged
	2. No thermal image	Thermal camera is damaged
	3. No PTZ function	The PTZ camera is damaged
	4. No recording	NVR damaged
PA system	1. Not giving the intruder warning	speaker / wiring / automated detection
Perimeter vibration detectors	1. No wifi connection	Modem faulty / lightning damaged / end of life
	2. Sensor out of position	Poor workmanship / loose screw
	3. Doesn't detect vibration	Working component damaged / end of life
Intercom system	Failure	Microphone / wiring / speaker / battery / AC failed
PSIM system	1. General Failure	Various components failed
	1. Hardware failure	Severs damaged
	2. Software failure	Management software corrupted
Switches	1. Hardware failure	Switch ports broken/
	2. Software failure	Switch not properly configured
Firewalls	1. Hardware failure	Firewall damaged
	2. Software failure	Fire rules non properly configured

3.7 Manage Asset Excursions

a) Asset excursions are a result of assets being operated outside of their design tolerances due to either maintenance deficiencies or network incidents. Each identified excursion must be assessed to determine the risk to the specific asset and the impact on the current maintenance execution strategy.

b) The above impact assessment is critical in order to determine if additional inspections and or tests are required or if a planned maintenance outage is required to be broad forward. Asset excursions should be managed as per the Process Control Manual (PCM) for Manage Asset Excursion (240-45920941).

3.8 Asset health

3.8.1 Design life expectancy and failure issues

a) The lifetime expectancy of an electric fence system, with perfect maintenance, is 20 years.

b) The lifespan of a typical alarm system with its associated electronic components, is four to five years. However, many companies and homeowners keep their alarm systems for around 10 years.

c) The other security systems, like the intercom systems, the pre-detection systems, and the public address systems, have a similar 5-year lifetime cycle, mainly due to improving technology.

d) Access Control Systems (ACS) expected lifetime is 10 years or more behind mainstream technology.

e) Cameras will last anywhere from 5 years or more. Good security cameras can last 10 years or even longer.

3.8.2 Condition assessment techniques

The conditions of all the Transmission Physical Security System assets are determined through visual inspections and functionality tests.

3.8.3 Condition rating

a) Computing the Asset Health Index for the Transmission Security Systems will require developing end-of-life criteria. Each criterion represents a factor critical in determining the asset's condition relative to end-of-life.

b) The condition assessment and rating process includes visual inspections and/or functionality tests and detailed reviews of maintenance records and diagnostic test reports extracted from Eskom's asset management system databases. In addition to maintenance histories, these databases should contain information about operating requirements and conditions, defects, failures, and spares. In assessing the information available against end-of-life criteria, condition state is rated A through to E. For this asset class, letter condition ratings have the following general meanings:

i. "A" means the component is in "as new" condition;

ii. "B" means the component has some minor problems or evidence of aging;

iii. "C" means the component has many minor problems or a major problem that requires attention;

iv. "D" means the component has many problems and the potential for major failure; and

v. "E" means the component has completely failed or is damaged or degraded beyond repair.

c) The specific definitions are used for each condition rating (i.e., A to E) in the assessment of each system component. An equivalent rating score is awarded for each assessment outcome based on the scoring guideline provided in table 11 below.

Table 11: Condition rating score guideline

Condition rating	Condition rating score
A	4
B	3
C	2
D	1
E	0

Note: Each equipment type has a number of specific conditions/factors that it is dependent on.

Table 12: Equipment Types and their typical Condition/factor Dependency

	Security System	"Dependent on" Condition/Factor
1	Electric Fence System	i. Operating environment (inland vs coastal environment)
		ii. Physical fence conductor type (e.g steel vs aluminium)
		iii. Energizer battery
		iv. Energizer performance
2	Access Control Systems	i. Power supply / battery
		ii. Remote control performance
		iii. Biometric/card readers sensitivity/performance
		iv. Remote functionality
3	Alarm System	i. Panic buttons
		ii. Audio of the alarm
		iii. Remote alarming
		iv. Incident recording
		v. Nuisance alarms/accuracy
4	CCTV systems	i. Camera Lens condition
		ii. Control function (e.g PTZ zoom)
		iii. Recording
		iv. Storage
		v. Bandwidth and video compression efficiency
5	Public address system	i. Microphone and speaker conditions
		ii. Amplifiers
		iii. Speaker mounting
6	Intrusion Pre-detection system	i. Sensor's accuracy/nuisance prevention
		ii. Sensor density (count)
		iii. Mode of detection vs operating environment (e.g., vibration sensors in mining areas)

7	Intercom systems	i.	Microphones
		ii.	speakers
		iii.	Audio clarity
8	Physical Security Information Management system (PSIM)	i.	All subsystems operational (integrability)
		ii.	Accuracy in recording
		iii.	Report generation automation
		iv.	Network resources utilization (e.g service prioritization)
9	Switches	i.	Hardware
		ii.	Software
		iii.	Efficiency in traffic switching/routing
10	Firewalls	i.	Hardware
		ii.	Software
		iii.	Security efficiency (security rules management)
11	Servers	iv.	Hardware
		v.	Software
12	All	vi.	Wiring, power supply, earthing, environmental conditions, fault currents, lighting strikes

d) In addition to the equipment Condition/factor dependency, it is necessary to define an overall asset health index formula, the asset health index of an item depends on a number of variables below:

i. **Maintenance**: This speaks to the operation of the equipment and weather it can be adjusted to operate within specification or not.

ii. **Spares**: This refers to the availability of spares.

iii. **Skills**: This refers to the availability of skills required to carry out the maintenance required.

iv. **OEM Support**: This refers to the availability of OEM support.

v. **Failure Rate**: This refers to the performance history of the equipment.

Table 13: Maintenance

Maintenance	Condition Rating	Rating Score
Indicate operate within specifications / No adjustments necessary	A	4
Indicate operate marginally outside specifications / Minor adjustments needed	B	3
Indicate operate outside specifications / Adjustments needed	C	2
Indicate operate significantly outside specifications / Adjusted and are marginally within specification	D	1
Indicate operate significantly outside specifications / Cannot be adjusted to be within specification	E	0

Table 14: Spares

Spares	Condition Rating	Rating Score
Spares readily available / short lead times / reasonable cost	A	4
Spares available / long lead times / reasonable cost	B	3
Spares available / long lead times / excessive cost	C	2
Spares shortlisted for discontinuation by manufacturer	D	1
No spare parts available	E	0

Table 15: Skills

Skills	Condition Rating	Rating Score
Available	A	2
Very Limited	B	1
Not Available	C	0

Table 16: OEM Support

OEM Support	Condition Rating	Rating Score
Support from OEM (contract in place)	A	3
Support from Local Supplier	B	2
Support from within Eskom	C	1
No support available	D	0

Table 17: Failure Rate

Failure Rate	Condition Rating	Rating Score
0 Failures past 2 years	A	4
1 Failures past 2 years	B	3
2 Failures past 2 years	C	2
3 Failures past 2 years	D	1
4+ Failures past 2 years	E	0

e) Each of the variables above is then weighted as seen in Table 19 below.

Table 18: Variable Weighting

Asset Health Contributing Factor	**Weighting**
Maintenance (needed to fall within spec)	3
Spares (availability)	1
Skills (availability)	2
OEM (support availability)	5
Failure Rate (over the past 2 years)	4

f) The health index for Transmission Physical Security is then calculated by applying the combined condition scoring weight distribution as indicated in Table 19 below:

Table 19: Overall Transmission Physical Security health index scale

Variable Item No.	Health index criteria	Weight	Condition rating	Maximum score
1	Maintenance	3	A,B,C,D,E / (4,3,2,1,0)	12
2	Spares	1	A,B,C,D,E / (4,3,2,1,0)	4
3	Skills	2	A,B,C / (2,1,0)	4
4	OEM Support	5	A,B,C,D / (3,2,1,0)	15
5	Failure Rate	4	A,B,C,D,E / (4,3,2,1,0)	16
Max. Score: 51 (Calculate percentage result)				

3.8.4 End of life criteria

The actual condition score calculated above is divided by the max score to determine the end-of-life percentage. This asset health index rating provides the end-of-life criteria for the TPS systems.

Table 20: Asset health index scale

Health index	Condition	Description	Requirements
85 - 100	Very Good	Some ageing or minor deterioration of a limited number of components	Normal maintenance
70 - 85	Good	Significant deterioration of some components	Normal maintenance
50 - 70	Fair	Widespread significant deterioration or serious deterioration of specific components	Update maintenance execution strategy as per section 3.4
30 - 50	Poor	Widespread serious deterioration	Start planning process to replace or rebuild considering risk and consequences of failure
0 - 30	Very Poor	Extensive serious deterioration	At end-of-life, immediately assess risk; replace or rebuild based on assessment.

4. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Remone Govender	Middle Manager - Group Security
Justice Ramanyoga	Middle Manager DX security
Monette Heath	Middle Manager GX security
Melvin Murugen	Middle Manager TX security
Judith Malinga	Senior Manager – PTM&C Engineering
Aletta Mashao	Senior Manager – PTM&C DX
Christoph Kohlmeyer	Senior Manager – GX Engineering (Acting)
Sikelela Mkhabela	Senior Manager – DX Network Operations
Alison Maseko	Senior Manager - Eskom Telecommunications

Cornelius Naidoo	Middle Manager – Telecommunication and Physical Security T&S
Johan Pieterse	Chief Engineer – TX Secondary Plant, Work Planning and Centralised Services

5. Revisions

Date	Rev.	Compiler	Remarks
July 2024	1	Donald Moshoeshoe	First revision

6. Development Team

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

- Donald Moshoeshoe
- Vernon Dinkleman

7. Acknowledgements

The compilers of the voice and data maintenance standard (240-143239708), the structure and some sections of this standard where derived from this document.

Annex A – Maintenance analysis

A.1 FMECA worksheet

The table below document the details of the FMECA process to indicate the reasoning as to the identified maintenance activities and logistics requirements. Note that a criticality assessment may have to be included for each Functional Importance, Health, Usage or Environment row that is included in **Error! Reference source not found.**, if the Consequence or Probability is dependent on these. The yellow areas are completed as part of the Maintenance Engineering Strategy and the green areas as part of the Maintenance Execution Strategy. 'Local' and 'Next Higher' Failure Effects are relevant to the Maintenance Engineering Strategy only and are specific to the asset class/system for which the strategy is being developed. 'End' Failure Effects are relevant to the Maintenance Execution Strategy and documented in the context of the effect on the overall security system/station.

Table A.1: FMECA Worksheet

FMEA									**Criticality (Risk) Assessment**									**Outcome**
Ref	**Function / item**	**Failure mode**	**Failure mechanism / cause**	**Failure effects**			**Detection method**	**Compensating provisions**	**Environment**	**Mild**				**Harsh**				**Maintenance Determination / Recommendation**
				Local	Next Higher	End			Functional Importance	Critical	Significant	Economic	Run to failure	Critical	Significant	Economic	Run to failure	
1.1	Chassis	Chassis electrical damage	Surge	Chassis damage	No visibility of some data points on the PSIM	All data points connected to the node are not visible on the PSIM	Loss of datapoints alarm shows on the PSIM at zero control	None	Probability1	A				B				
									Consequence2	4	3	2	1	4	3	2	1	1. Swap out the damaged chassis and ensure that it is earthed according to the installation standard.
									Risk3	IV	IV	IV	IV	III	II	IV	IV	

																The cabinet must be earthed (gland plate) to the station earth.
1.2		Chassis overheating	Dust clogging on ventilation pores of the chassis	Chassis shutdown	No visibility of some data points on the PSIM	All data points connected to the node are not visible on the PSIM	Lost of datapoints alarm shows on the PSIM at zero control	None	Probability1	A				B				
									Consequence2	4	3	2	1	4	3	2	1	1. Visual inspections 2. Clean the dust on the ventilation pores of the chassis
									Risk3	IV	IV	IV	IV	III	II	IV	IV	
1.3			Fan mechanical failure due to dust	Chassis shutdown	No visibility of some data points on the PSIM	All data points connected to the node are not visible on the PSIM	Lost of datapoints alarm shows on the PSIM at zero control	None	Probability1	A				B				
									Consequence2	4	3	2	1	4	3	2	1	1. Inspections 2. Clean and test the fan

																	3. Swap out the damaged fan
								Risk3	IV	IV	IV	IV	III	II	IV	IV	
								Probability1	A				B				
								Consequence2	4	3	2	1	4	3	2	1	1. Inspections
																	2. Measure the ambient temperature
1.4			Ambient temperature above the allowed maximum temperature	Chassis shutdown	No visibility of some data points on the PSIM	All data points/zones connected to the node are not visible on the PSIM	Lost of datapoints alarm shows on the PSIM at zero control	None									3. Set or repair the air conditioner
								Risk3	IV	IV	IV	IV	III	II	IV	IV	
1.5								Probability1	A				A				

	Site Security Control modules	Corrupted software, loss of memory or configs	Software errors/bug, flat battery for the memory	Loss data points, Loss of node	Faulty control data point alarm shows on PSIM at zero control or complete loss of Node	All data points/zones connected to the node are not visible on the PSIM	Faulty control module datapoint alarm shows on the PSIM at zero control or complete node disappearance	Control module redundancy (e.g multiple synchronised energizers)	Consequence2	4	3	2	1	4	3	2	1	1. Swap out the faulty control modules
									Risk3	IV	IV	IV	IV	IV	IV	IV	IV	
1.6	Sub system controllers	Electrical damage	Surge	Module not powered	Faulty module alarm shows on the PSIM	All data points/zones connected to the module are not visible on the PSIM	Faulty datapoints alarm shows on the PSIM at zero control	Limited module redundancy	Probability2	A				B				
									Consequence1	4	3	2	1	4	3	2	1	1.Inspections to identify the correct use of surge arrestors where required 2.Tests the module
									Risk0	IV	IV	IV	IV	III	II	IV	IV	2. Swap out the damaged aggregation module
1.7		Bad contact	Damaged module contact	Module not recognised by the chassis	Faulty data point alarm shows on the PSIM	All data points/zones connected to the module are not visible on the PSIM	Faulty data point alarm shows on the PSIM at zero control	Limited module redundancy	Probability3	A				B				
									Consequence2	4	3	2	1	4	3	2	1	1. Inspection 2. Test the module.

									Risk1	IV	IV	IV	IV	III	II	IV	IV	3. Swap out the damaged aggregation module
1.8	Sensors and readers	Electrical damage	Surge	Module not powered	Faulty module/data point alarm shows on the PSIM	All data points connected to the module are not visible on the PSIM	Faulty module/data point alarm shows on the PSIM at zero control	Limited module redundancy	Probability0	A				B					
									Consequence1	4	3	2	1	4	3	2	1	1. Visual inspections to identify the correct use of surge arrestors where required 2. Test the module.
									Risk0	IV	IV	IV	IV	III	II	IV	IV	3. Swap out the damaged service module
1.9		Bad contact	Module not properly inserted	Module not recognised by the chassis	Faulty module/data point alarm shows on the PSIM	All data points connected to the module are not visible on the PSIM	Faulty module/data point alarm shows on the PSIM at zero control	Limited module redundancy	Probability1	A				A					
									Consequence0	4	3	2	1	4	3	2	1	1.Visual inspections
									Risk1	IV	IV	IV	IV	IV	IV	IV	IV	2. Insert the modules properly and lock the module latches

1.10	Interfacing modules	Electrical damage	Surge	Module not powered	Faulty module/data point alarm shows on the PSIM	All data points connected to the module are not visible on the PSIM	Faulty module/data point alarm shows on the PSIM at zero control	None	Probability1	A				B				
									Consequence0	4	3	2	1	4	3	2	1	1.Visual inspections
									Risk1	IV	IV	IV	IV	III	II	IV	IV	2. Swap out the damaged module
1.11		Bad contact	Module not properly inserted	Module not recognised by the chassis	Faulty module/data point alarm shows on the PSIM	All data points connected to the module are not visible on the PSIM	Faulty module/data point alarm shows on the PSIM at zero control	None	Probability0	A				A				
									Consequence1	4	3	2	1	4	3	2	1	1.Visual inspections
									Risk2	IV	IV	IV	IV	III	II	IV	IV	2. Insert the module properly and lock the module latches
1.12	Surge protection	Electrical damage	Surge	Surge protector blown	Faulty module/data point alarm shows on the PSIM	All data points connected to the module are not visible on the PSIM	Faulty module/data point alarm shows on the PSIM at zero control	Limited module redundancy	Probability1	A				B				
									Consequence2	4	3	2	1	4	3	2	1	1.Visual inspections
									Risk3	IV	IV	IV	IV	III	II	IV	IV	2. Swap out the blown surge protector
1.13	Cables	Damaged cables	Cables bent beyond the acceptable radius or	loss of nodes/data points	Faulty module/data point alarm	All data points connected to the module are not visible on the PSIM	Faulty module/data point alarm shows on the	Limited module redundancy	Probability3	A				A				
									Consequence2	4	3	2	1	4	3	2	1	1. Visual inspections

			damaged by rodents		shows on the PSIM		PSIM at zero control		Risk1	IV	IV	IV	IV	IV	IV	IV	IV	2. Replace the damaged cables and ensure that the cables are labelled correctly.
1.14	Connectors	Loose connectors	connectors loose due to tempering	loss of nodes/data points	Faulty module/data point alarm shows on the PSIM	All data points connected to the module are not visible on the PSIM	Faulty module/data point alarm shows on the PSIM at zero control	Limited module redundancy	Probability2	A				A				
									Consequence2	4	3	2	1	4	3	2	1	1. Visual inspections 2. Fasten the loose connectors
									Risk0	IV	IV	IV	IV	IV	IV	IV	IV	
1.15		Damaged connectors	Damaged connector due to improper handling	loss of nodes/data points	Faulty module/data point alarm shows on the PSIM	All data points connected to the module are not visible on the PSIM	Faulty module/data point alarm shows on the PSIM at zero control	Limited module redundancy	Probability1	A				A				
									Consequence2	4	3	2	1	4	3	2	1	1. Visual inspections 2. Test the connectors 3. Replace the damaged connectors
									Risk1	IV	IV	IV	IV	IV	IV	IV	IV	

1.16	PSIM System	Server hardware failure	Surge	PSIM server damaged	Data points/location/site server visibility lost at zero control	Zero loses control of the location/site server but data points are still running.	Location server and data points lost on the Zero Control PSIM screens	Redundant PSIM server	Probability0	A				B				
									Consequence1	4	3	2	1	4	3	2	1	1. Inspection 2. Make sure that software patches are up to date 3. Make sure that the PSIM back ups are in place. 4.Test the server 5. Swap out the damaged hardware
									Risk1	IV	IV	IV	IV	III	II	IV	IV	6. Perform the PSIM failover test
1.17		Client machine failure	Surge	Client machine damaged	Faulty module/data point alarm shows on the PSIM	All data points connected to the module are not visible on the PSIM	Faulty module/data point alarm shows on the PSIM at zero control	Multiple client machines	Probability0	A				B				
									Consequence1	4	3	2	1	4	3	2	1	1. Inspection 2. Test the client machine

																	3. Swap out the damaged client machine
									Risk1	IV	IV	IV	IV	III	II	IV	IV	
1.18		Software failure	Software bug	PSIM server disconnected, PSIM not behaving as expected, one or more PSIM client machines disconnected	Data points/location/site server visibility lost at zero control	Zero loses control of the location/site server but data points are still running.	Location server and data points lost on the Zero Control PSIM screens	Redundant PSIM server, multiple client machines	Probability1	B				B				
									Consequence2	4	3	2	1	4	3	2	1	1. Test and establish if the issue is with software or network 2. Make sure that software patches are up to date 3. Make sure that the PSIM back ups are in place.
									Risk1	III	II	IV	IV	III	II	IV	IV	4. Fix the software issues
1.19		Network failure	Network configuration errors	PSIM server disconnected, PSIM not behaving as expected, one or more	Data points/location/site server visibility lost at	Zero loses control of the location/site server but data points	Location server and data points lost on the Zero Control PSIM screens	Redundant PSIM server, multiple client machines	Probability1	B				B				
									Consequence2	4	3	2	1	4	3	2	1	1.Test and establish if the

				PSIM client machines disconnected	zero control	are still running.													issue is with software or network 2. Fix the PSIM errors
									Risk1	III	II	IV	IV	III	II	IV	IV		

Note: The estimated risk and consequence rating on this table is based on subjective assessment and should be used as a guideline only, improvement on future revisions of this standard shall include accurate qualitative assessment of the risk and consequence categorising for the associated asset class.

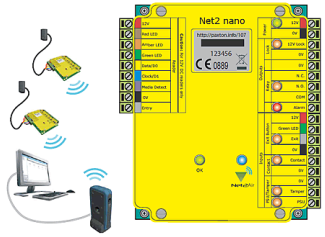
Annex B - Typical physical Security systems installed

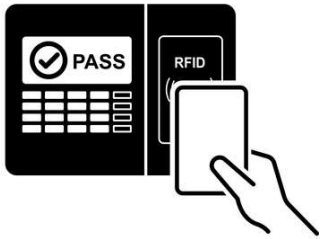
Table B1: Typical physical Security systems installed (detailed information)

SYSTEM NO.	SYSTEM	COMPONENT DESCRIPTION	OEM	OEM MODEL	Picture
1	Electric Fence Systems	Energizer	Stinger	Stinger BS120 energizer	
	Electric Fence Systems	Energizer	Stinger	Stinger BS102 energizer	

	Electric Fence Systems	Energizer	Staffix		
	Electric Fence Systems	Energizer	Staffix	Staffix JVA Z18 energiser	
	Electric Fence Systems	Energizer	Nemtek	Nemtek M28S energiser	
	Electric Fence Systems	Energizer	Nemtek	Nemtek M18 energiser	

	Electric Fence Systems	Energizer	Nemtek	Nemtek Stealth Master M28SM	
2	Access Control Systems (ACS)	Sliding Gate Motor	Centurion	Centurion D10 sliding gate motor	
	Access Control Systems (ACS)	Sliding Gate Motor	Centurion	Centurion vector 500 motor	
	Access Control Systems (ACS)	Sliding Gate Motor	Hansa	Hansa 24VDC sliding gate motor	

	Access Control Systems (ACS)	Swing Arm Gate Motor	King right Motors	Modus Articulated Motors	 
	Access Control Systems (ACS)	Biometric Readers	TBS	TBS 2DS TCOM4 biometric readers	
	Access Control Systems (ACS)	Access Controller	Paxton	Paxton NeT2 Plus	
	Access Control Systems (ACS)	Access Controller	HikVision	DSK2600G Series	

	Access Control Systems (ACS)	Card reader gate control	Previously OEH	CS500 Controller (decomissioned - card reader to open /close gate)	
3	Alarm systems	Burglar Alarm System	SATEL	SATEL INTEGRA PLUS 64 Controller	
	Alarm systems	Burglar Alarm System	Paradox	Paradox SP 6000	
	Alarm systems	Burglar Alarm System	DCS	DSC PC1616	

	Alarm systems	Burglar Alarm System	Fidelity ADT	Fidelity ADT	
	Alarm systems	Burglar Alarm System	ORISEC	ORISEC ZP20	
	Alarm systems	Burglar Alarm System	Motorola	Motorola ACE 3600	
4	CCTV systems	Cameras	Uniview	UNIVIEW IPC32345A-DZK Dome Camera	

	CCTV systems	Cameras	Uniview	UNIVIEW IPC264EA-HDZK Bullet Camera	
	CCTV systems	Cameras	Uniview	UNIVIEW TIC2621SR-F3-4F4AC-VD Thermal Camera	
	CCTV systems	Cameras	Uniview	UNIVIEW IPC6852ER-X45-VF PTZ Camera	
	CCTV systems	NVR	Uniview	Uniview 516-128 NVR Network Video Recorder	

	CCTV systems	Cameras	Alhua Technologies	Alhua Technologies	
5	Public Adress System	Speaker	TOA	TAO IP-A1SC15 speakers	
6	Intrusion Pre-detection Systems	Vibration Detectors	Moduteq	WI-I PIDS	
7	Intercom Systems	Intercom (gate to sec room)	Akuvox	Akuvox R20A smart intercom	

	Intercom Systems	Intercom (gate to sec room)	Akuvox	AKUVOX C315S	
8	Intercom Systems	Intercom (gate to sec room)	Honeywell		
	Intercom Systems	Intercom (gate to sec room)	Advancis	Advancis	
	Security Management systems	PSIM System	Advancis	Winguard	

9	Switches	Core -, IPNet-, POE-, Switch & Video Recorder	Huawei	HUAWEI 24 PORT SFP(CORE SWITCH)	
	Switches	Core -, IPNet-, POE-, Switch & Video Recorder	Huawei	Huawei IPINET SWITCH	
	Switches	Core -, IPNet-, POE-, Switch & Video Recorder	Huawei	Huawei 24 PORT POE SWITCH	
	Switches	Core -, IPNet-, POE-, Switch & Video Recorder	Huawei	Huawei NVR516-128	

10	Firewalls	Network Firewall	Fortigate	Fortigate FG-40F	
11	Server System	Servers	Huawei	Huawei Server	
	Server System	Servers	Dell	Dell Server