Eskom	Standard	Technology

Title: **PHYSICAL SECURITY SYSTEMS TECHNOLOGY ROADMAP**

Unique Identifier:	**240-106871262**
Alternative Reference Number:	**<n/a>**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**2**
Total Pages:	**20**
Next Review Date:	**May 2026**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Donald Moshoeshoe	**Naresh Hari**	**Dr. Titus Mathe**
Engineer – PTM&C	**General Manager: Transmission Engineering**	**General Manager: Group Technology**
Date: 28/06/2021	Date: 2021-07-20	Date: 2021-08-26

Supported by SCOT/SC

Kashveer Jagdaw

SCOT/SC Chairperson

Date: 28/06/2021

PCM Reference: **240-45541534**

SCOT Study Committee Number/Name: **Part 16: DC & Auxiliary Supplies SC – Security Systems CG**

Content

Tables

1. Introduction

Eskom currently deploys various physical security technology solutions to safeguard its employees and assets by monitoring access to Eskom sites as well as detecting and preventing unauthorised access to these sites.

World technology trends are changing and business requirements are continuously evolving, it is therefore imperative to identify, assess and evaluate currently available viable security technologies that can meet current and future business objectives.

The objective of this technology roadmap is to assess current physical security technologies within Eskom, and also to make projections for future technology implementations to cater for Eskom's security requirements.

Note: In this document security systems/technologies shall refers to physical security systems/technologies.

2. Supporting clauses

2.1 Scope

The scope of this document is the development of technology roadmap for physical security technologies which include the following:

a) Access Control Systems

b) Detection and Alarm Systems

c) Video Surveillance Systems

d) Deterrent Systems

   1) Illumination/Lighting Systems

   2) Public Address Systems

   3) Fences

e) Tracking Technologies

f) Remote Monitoring Centres / Command Centres

This document provides an overall physical security roadmap, the different physical security solutions deployed at specific sites will depend on factors such as the site/equipment network importance, security risk assessment of the site and the availability of supporting services (e.g. telecommunications, response teams, etc.) at the site.

2.1.1 Purpose

The purpose of the Security Technology Roadmap is to document current physical security requirements in Eskom and the technologies deployed to address them, the document further makes projections of viable technologies that will be deployed in future in line with envisioned technology migration and evolving business requirements.

2.1.2 Applicability

This document shall apply throughout Eskom Holdings Limited Divisions.

2.2 Normative/informative references

2.2.1 Normative

[1] ISO 9001, Quality Management Systems.

[2] 240-49910527, Procedure for Plan and Select Technologies

[3] 240-170000086 Roles and Accountabilities for Lifecycle Management of Physical Security Systems in the Transmission Division

[4] 240-55410927 Cyber Security Standard for Operational Technology

[5] 240-56927206 Eskom Holdings Corporate Plan 2020/21 – 2022/23 Rev 10

2.2.2 Informative

None

2.3 Definitions

2.3.1 General

Definition	Description
Access Control System (ACS)	It is a system that aims to collaborate and align efforts across the electronic, logical and physical security domains in an effort to control access to sites.
Pan-tilt-zoom (PTZ) camera	A pan-tilt-zoom (PTZ) camera works by moving the camera in different directions to get a whole picture of the surveillance area and zooming in for further detail of security events. The pan, tilt, and zoom capabilities make it possible to monitor large areas with a single camera while getting great detail at the same time.
Physical security	Is defined as all those measures that involve the use of physical and technological aids in the protection of assets. It is a set of tangible countermeasures designed to control the access and egress and to prevent the interruption of operations.
PSIM	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.
Public Address System	Referred to as 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.

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
ACS	Access Control System
CCTV	Close Circuit Television
CG	Care Group
CoE	Centre of Excellence
DVR	Digital Video Recorder
Dx	Distribution
ENC	Eskom National Contract
Gx	Generation

Abbreviation	Description
HR	Human Resource
HV	High Voltage
IACS	Integrated Access Control System
IM	Information Management
IT	Information Technology
NVR	Network Video Recorder
OU	Operating Unit
PA	Public Address
PSIM	Physical Security Information Management
PTZ	Pan-Tilt-Zoom
R,T&D	Research, Testing and Development
SC	Study committee
SCOT	Steering Committee of Technology
Tx	Transmission
UAV	Unmanned aerial vehicle

2.5 Roles and responsibilities

The Physical Security Systems CG that operates under the DC & Auxiliary Supplies SC is represented by all Eskom stakeholders that have a vested interest in security systems.

The roles and responsibilities as outlined in [3] shall be applicable to ensure that the objectives of this document are supported and implemented.

The progress in meeting these roadmap objectives shall be reviewed by the Security Systems CG and necessary actions instigated to ensure compliance.

2.6 Process for monitoring

The implementation of the roadmap objectives shall be monitored by the Security Systems CG.

2.7 Related/supporting documents

Not Applicable

3. Technology Roadmap

A roadmap is a plan intended to achieve a particular goal or function. It defines a plan that matches short –, medium – and long term goals with specific technology solutions to help achieve those goals.

The plan not only addresses how to identify, evaluate and select new technologies, but more importantly how to implement, operate, maintain and decommission the deployed technologies sustainably.

Currently deployed technologies will be evaluated against requirements as to how best those requirements are being met – future technologies will be evaluated against how the requirements can be met better. There must be a tangible benefit for changing to new technologies as the business implications can be significant. Technology change should also be done in a phased approach to limit the degree of business disruption. There must be awareness of what new challenges can be introduced with the adoption of new technologies – is the business ready to accommodate them – what business infrastructure or support processes need to be in place to gain the best benefits.

The deployment of security technologies must be in line with Eskom's cyber security standard [4] to ensure that the Operational Technology networks and systems in Eskom are protected from cyber-attacks.

3.1 Methodology

The following methodology was followed to develop the technology roadmap:

a) Reviewing Eskom's purpose, mission and vision statements. Understanding the company's Strategic Imperatives and 5-year Priorities

b) Identifying ways in which the management of the security systems and technologies can support the aforementioned objectives

c) Reviewing and re-examining the current technology status and activities

d) Future candidate technology assessment and selection

e) Selecting focus technologies

f) Develop new objective statements for focus technologies

g) Develop Technology Implementation Plan

3.2 Eskom Mission, Strategy, Imperatives and Goals

Eskom's purpose is as per Eskom Holdings Corporate Plan [5].

3.3 Access Control System

3.3.1 Overview

Access Control revolves around the technologies deployed to manage access to Eskom sites.

3.3.2 Current situation

Currently Access control at most Eskom sites is managed using the traditional lock-and-key and electronic systems that are mostly used with access cards or remotes issued to individuals and programmed with codes that will allow access to a limited number of sites – normally in line with the area the individual is authorized to operate in. These systems are highly ineffective in that they do not provide real-time information of who enters and exits Eskom sites. The systems are also not able to authenticate users' rights of access to different sites/areas.

3.3.3 Business requirements

The Access Control System (ACS) needs to be deployed at all Eskom sites with various levels of checks in line with the importance (criticality) of the site.

Future systems need to achieve the following business objectives:

- Having an integrated access control system which will allow stakeholders to know in near real-time, who is entering and exiting Eskom sites.
- To enable and revoke access permission to different sites from a central server which is integrated with the HR system.

- To allow the use of a single coded device to access all sites.
- To prevent unauthorized people; who are not adequately trained to operate in hazardous environments from entering the area; thereby reducing the risk of fatalities and injuries.
- To have a reliable availability of information (date and time stamped) and audit trails of security related data and records to assist in investigations related to security breach.
- To have an effective incidents management across Eskom where alarms and events data are monitored from a centralized security control area.

3.3.4 World trends and use of technology

- Trends in integrated access control evolve around the unification of different platforms and the optimal use of integrated systems to make better and faster decisions. Migration of services to the cloud is also becoming a reality whilst taking data privacy into consideration. Better and more reliable biometrics is gaining momentum in ensuring that people are correctly identified. The use of contactless biometric access control systems is a growing trend. Access control technologies exist that automatically restricts/prohibit access if certain requirements are not met (e.g. wearing of masks, out-of-tolerance body temperature).

3.3.5 Technology development plan

This section of the roadmap describes the “road” that the Access Control System in Eskom will take over the next 5 to 10 years.

For many years, the traditional lock-and-key and electronic systems that are used with coded access devices have been used for Access Control in Eskom. A challenge with these technologies is that they are inefficient in providing the required real-time information related to access/exit to Eskom sites in line with Eskom’s vision of having Access Control systems that can be integrated with near real-time data and access to different sites/areas.

The EBI platform from Honeywell was previously selected as the heart of the IAC system. Eskom rolled out the heart of the Integrated Access Control system (IACS) comprising several remote servers with the main server situated at MWP. The EBI system has been identified as a legacy technology and Eskom will phase it out in the next 5 years. An audit will be conducted to investigate the levels of implementation and investment made on the system to guide the phase out strategy.

The business has opted for an open architecture approach. An Integrated Access Control System (IACS) capable of integrating with CCTV, HVAC, building management systems and other security / business subsystems to provide a unified security management system is envisioned to address the shortcomings associated with the legacy lock-and-key Access Control System . There are sites where the traditional lock-and-key system will continue to be used as shown in the Table 1 due to their remoteness and limitations mentioned below:

- The telecommunications infrastructure not being available to ensure data transfer between field devices and the security control centres.
- IT/IM systems not being available
- Budget constraints

The expected Access Control technology migration in Eskom is indicated in Table 1. The Integrated access Control system standard will be in line with SCOT procedure for technology development. An enquiry will be issued for associated field devices and associated management systems. This will be followed by pilots and standardization.

Table 1: Development plan for Access Control system

Technology	Technology Development Time Frame									
	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Lock-and-key										
Standalone (fragmented) Access Control Systems										
Open architecture Integrated Access Control										
EBI system										
Notes The result of an audit investigation will determine the strategy to be used to phase out the EBI system										
Key:	Literature/market scans, Research	Pilots	Standardisation	Ready for implementation	Technology Discontinued					

3.3.6 Implementation plan for Access Control System (ACS) technologies

This section of the roadmap describes the implementation plan for the ACS to ensure that the business has all resources to support deployed technologies effectively and optimise the return-on-investment. The technology will be implemented in a phased release approach to minimise impact to business operations.

The primary reasons for the adoption of this phased release approach are:

- The phased approach will address quick wins for the business while still planning and conceptualising the value chain, whereas a big bang approach will delay delivery of key priorities, which directly impacts business expectations
- Security Management is ever evolving and hence an incremental approach is best suited to ensure the application of key learnings from each phase incrementally while leveraging on the best suited technology.
- The phased release will allow Eskom to explore the various deployment methodologies and arrive at a ‘best fit’ option for the national roll-out of other functionality and systems in Eskom, by means of a global template/enterprise approach.
- This approach will further assist to reduce the risk of huge upfront capital investments and ensure probability of success compared to a big bang approach that has large capital investment and higher risks of failure.

Table 2 below depicts high level time frames for the implementation of the Integrated Access Control System in Eskom.

Table 2: IACS implementation plan

Activity	Implementation Time Frame									
	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Product evaluation and contract										
Training										
Maintenance Strategy										
Phased releases										

3.4 Detection and alarming

3.4.1 Overview

The alarm system forms an integral part of the security system to provide proactive alarm monitoring of all areas around site perimeters, entrances, all gates, guard rooms, control rooms, battery rooms, HV yard strategic places, strategic spares rooms etc.

The detection system enables intrusion pre-detection at strategic areas as determined by Eskom.

3.4.2 Current situation

Eskom deploys alarm systems as part of the security systems to provide proactive alarm monitoring at its sites.

Used detection technologies include non-lethal energised fences, vibration sensors, intrusion detection beams, CCTV with advanced video analytics and passive / active motion sensors.

The systems are used for pre-detection in the following typical applications:-

- HV yard strategic places,
- Tunnelling underneath the fences,
- Separation of electric fence conductors,
- Cutting and climbing over perimeter barrier fences,
- Digging underneath, breaking though and climbing over the barrier walls.

3.4.3 Business requirements

The business requires a technology that will cater for the following future requirements:

- Enable safety of individuals at Eskom sites.
- Reduction of manned guarding.
- A technology that will supplement manned guarding by making them more efficient especially at sites that are classified as National Key Points.
- Systems that can be integrated with other deployed security technologies like CCTV to provide a unified security solution.
- Technologies that can reliably detect unauthorised entry to any Eskom site with the least amount of nuisance alarms.
- Detection and alarming systems to detect the unauthorized movement of Eskom assets e.g. cables, power lines, lattice structure members, pole mounted transformers, batteries, pylon/tower members, etc.

3.4.4 World trends and use of technology

- Exterior sensors

These are mainly used to detect intruders crossing a boundary of a protected area. Exterior sensors performance is based on probability of detection, the sensor's susceptibility to unwanted alarms (due to changing environmental conditions), and the sensor's vulnerability to defeat. Technologies used include fence-mounted vibration sensors (fibre optic or ported co-axial), electric fields, capacitance sensors, buried sensors, line-of-sight sensors (using microwaves or infrared), camera video analytics, radar (with analytics) and seismic sensors.

- Interior sensors

These are used to detect an intruder penetrating or moving inside a protected area. Sensing technologies based on vibration, sounds, ultrasonic, magnetic switching, microwaves, infrared and video analytics are used.

- Video analytics using video footage combined with artificial intelligence (AI) to reliably detect intruders are also becoming prevalent.

3.4.5 Technology development plan

This section of the roadmap describes the "road" that the Detection and Alarming technologies in Eskom will take over the next 5 to 10 years.

The expected Detection and Alarming technologies migration in Eskom is indicated in Table 3 below.

Table 3: Detection and Alarming technologies development plan

Technology	Technology Development Time Frame																			
	2021		2022		2023		2024		2025		2026		2027		2028		2029		2030	
Non-lethal electrified fence																				
Line-of-sight sensors (using microwaves or infrared)																				
Vibration detection with alarm system																				
Video analytics																				
Radar's and volumetric sensing, electric fields, capacitance sensors, buried sensors																				

Key:	Literature/market scans, Research	Pilots	Standardisation	Ready for implementation	Technology Discontinued

3.4.5.1 Short term developmental plans (1- 3 years)

- Effective implementation and integration of detection and alarming systems with other deployed security technologies like CCTV etc.
- Deploying cameras with video analytics functionality.
- Detection and alarming systems to detect the unauthorized movement of Eskom assets e.g. cables, power lines, lattice structure members, pole mounted transformers, batteries, pylon/tower members, etc.
- Integrating new detection and alarming technologies with legacy technologies and planning the phasing out of these legacy technologies.

3.4.5.2 Medium term developmental plans (3 -5 years)

- Research new detection technologies e.g. volumetric sensing, radar systems, vibration sensors, advanced analytics.
- Review the application of intrusion detection beams (microwave, infrared).
- Technology to monitor staff movement on site.

3.4.6 Implementation plan

The implementation of the technology will be guided by the minimum security requirements taking into consideration the criticality of sites/assets and compliance to security requirements for sites which are classified as National Key Points. Essential infrastructure shortcomings and the cost to make such services available will also be a guide in terms of what detection and alarming technology to deploy.

In order for the detection and alarming technologies to be effective, the following conditions need to be met:

- Adequate telecommunications infrastructure must be available to ensure data transfer between field devices, servers and security control centers;
- The security control centers must be manned and operational to manage security related alarms;

- The IT/IM systems must be in place and sustainable;
- Armed response teams must be available to apprehend intruders.

Table 4 below depicts a high level implementation plan for the detection and alarming technologies

Table 4: Implementation time frames for Detection and Alarming technologies

Activity	Implementation Time Frame																			
	2021		2022		2023		2024		2025		2026		2027		2028		2029		2030	
Product evaluation and contract																				
Training																				
Maintenance Strategy																				
Rollout																				

Notes:

2021 - 2023:

- Technology Group to have Technical specifications and associated technical evaluation criteria available.

2023 – 2030

- Prepare for enquiry to establish ENCs
- Issue enquiry and evaluate tenders
- Establish ENCs
- Training on equipment to be included

3.5 Video Surveillance

3.5.1 Overview

Surveillance is the monitoring of the behaviour, activities, or other changing information, usually of people/equipment for the purpose of influencing, managing, directing, or protecting them.

The objective of CCTV is to promote safety and to render an additional, cost effective visual intelligence medium to assist personnel in making decisions with regards to security. The visual environment created by CCTV will assist in deterring potential intruders, as well as guide security personnel, thus reducing the risk of danger to human life and assets. CCTV surveillance forms part of the total security system which incorporates fences, intruder detection systems, site access control, and human response teams.

3.5.2 Current situation

Both IP and analogue (fixed and PTZ) cameras are used either along the perimeter or indoors at Eskom sites. Depending on the purpose / application, surveillance technologies used include normal day/night cameras and thermal cameras. CCTV technology is currently utilised exclusively for security purposes.

3.5.3 Business requirements

Eskom requires a technology that will provide reliable security information (video footage, audio clips, etc.) and offer auditable security related data to assist in investigations related to security breach as well as reduction in losses due to theft and vandalism related incidents. Some of the business requirements include:

- The use of intelligent video surveillance systems that can monitor and report (autonomously) on anomalies or out-of-bound conditions that require intervention;
- Systems that allow threats to be monitored, detected, observed, recognised and in some cases even identified under various environmental conditions;
- The technology should be able to be integrated with other security systems.

3.5.4 World trends and use of technology

Some of the world trends for surveillance technologies are:

- On-board video analytics and integration of unidirectional and bidirectional audio;
- Edge storage on camera, complementing centralized DVR/NVR storage;
- Optimised compression techniques for better transmission across low bandwidth telecommunication channels;
- Use of drones/Unmanned aerial vehicles (UAVs).

3.5.5 Technology development plan

This section of the roadmap describes the "road" that the Video surveillance technology in Eskom will take over the next 5 – 10 years.

Table 5 below depicts the envisioned development for the surveillance technology in Eskom.

Table 5: Development time frames for video surveillance technology

Technology	Technology Development Time Frame									
	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Optical cameras										
Thermal cameras										
Physical security video surveillance systems to support condition monitoring of plant										

Key:	Literature/market scans, Research	Pilots	Standardisation	Ready for implementation	Technology Discontinued

3.5.5.1 Short term development plan (1- 3 years)

- Review and assess the effective use of currently deployed systems.
- Evaluating the viability of employing thermal cameras.

3.5.5.2 Medium term development plan (3 - 5 years)

- Research into the latest camera technologies and their capabilities to operate effectively under various extreme environmental conditions.
- Investigate how cameras can be used to support other functions at site besides security, e.g. condition monitoring of plant, etc.

3.5.5.3 Long term development plan (5 - 10 years)

- Use of and effective integration of image recognition software to allow access control, etc.
- Research the use of real-time satellite footage e.g. Google Earth.

3.5.6 Implementation plan

The video surveillance is a multidisciplinary technology that requires collaborated inputs from different departments including Power Delivery Engineering, Group IT, Group Security, Regional Security Sections / departments and Eskom Telecoms for it to be developed. In order for the video surveillance systems to be deployed effectively, the following requirements must be catered for:

- Adequate telecommunications infrastructure must be available to ensure effective data transfer between field devices and the Security control centers;
- Security control centers must be in place (staffed) and operational to manage the system;
- The IT/IM systems must be in place;
- Proper installation, testing and commissioning of installed equipment to ensure that they serve the intended purpose;
- There must be trained field staff to support the system.

Table 6 below depicts a high level implementation plan for the video surveillance technology in Eskom:

Table 6: Implementation time frame for video surveillance technology

Activity	Implementation Time Frame																			
	2021		2022		2023		2024		2025		2026		2027		2028		2029		2030	
Product evaluation and contract																				
Training																				
Maintenance Strategy																				
Rollout																				

Notes

2021 - 2022:

- Technology Group to have Technical specifications updated.
- Prepare for enquiry to establish ENCs

2023 – 2030 :

- Issue enquiry and evaluate tenders
- Establish ENCs
- Training on equipment to be included

3.6 Deterrence Systems

3.6.1 Overview

The main purpose of deterrent methods is to discourage assailants and to convince potential attackers that a successful attack is unlikely due to a strong defence system. They serve to prevent, or at least delay attacks, and also act as a psychological deterrent by defining the perimeter of the facility and making intrusions seem more difficult.

3.6.2 Current situation

Currently Eskom deploys different methods of deterrence including perimeter fences, security lighting, non-lethal electrified fences, visible guarding and PA systems, basically every physical evidence that indicates that the plant is been monitored / protected. These systems are used in conjunction with other security technologies such as CCTV to provide a unified security solution at Eskom sites.

Note: Deterrent gas systems was discontinued due safety concerns.

3.6.3 Business requirements

The business requires deterrence methods/systems that are effective, these systems must also have reduced maintenance requirements especially for remote sites that are not easily accessible. The deployed systems must achieve the security objectives below:

- They must serve as visual demarcation of Eskom assets.

- They must discourage potential intruders from entering/vandalising Eskom sites.

With intruders becoming more familiar with currently deployed deterrence methods, it is necessary to investigate the deterrence value of existing methods and also research on other legal/socially acceptable deterrence methods.

3.6.4 World trends and use of technology

Some of the trends include the following:

- Sound bomb as means of deterring intruders, but further investigations are necessary to analyse ecological impact/friendliness especially at sites that have noise level restrictions that are not in remote areas.
- Use of pepper spray.
- Use of hardened equipment that can resist normal penetration attempts.
- Use of drones.

3.6.5 Technology development plan

This section of the roadmap describes the “road” that the Deterrence technology in Eskom will take over the next 5 – 10 years.

Table 7 below depicts envisioned timelines for the development of deterrence technologies

Table 7: Development time frame for Deterrence technologies

Technology	**Technology Development Time Frame**									
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**2028**	**2029**	**2030**
Perimeter fences and walls										
Security lighting										
Non-lethal electrified fences										
Visible guarding with response										
PA systems										
Sound bomb										
Pepper spray										

Notes:

3 years:

- Implementation of technical specifications for fences
- Implementation of effective known deterrence methods; e.g. PA Systems, etc.

3 – 5 years:

- Investigating the deterrence value of existing methods
- Research on other legal / socially acceptable methods

Key:	Literature/market scans, Research	Pilots	Standardisation	Ready for implementation	Technology Discontinued

3.6.6 Implementation plan

The table below depicts a high level implementation plan for the Deterrence technologies in Eskom

Table 8: Implementation time frame for Deterrence systems

Activity	Implementation Time Frame																			
	2021		2022		2023		2024		2025		2026		2027		2028		2029		2030	
Product evaluation and contract																				
Training																				
Maintenance Strategy																				
Rollout																				

3.7 Tracking systems

3.7.1 Overview

Tracking technology provides ability to track the location and movement of Eskom assets as well as tagging of high value portable devices and other mobile assets to monitor their movement.

3.7.2 Current situation

Tracking devices are not yet standardised for usage in Eskom.

3.7.3 Business requirements

The tracking technology is required to cater for the following requirements:

- Ability to track the location and movement of Eskom assets.
- Inconspicuous tags that can be easily applied with long expected battery life.
- Tagging of high value portable devices and other mobile assets to monitor their movement.
- Reduction in losses due to prevention of assets getting lost/stolen.

3.7.4 World trends and use of technology

- Tagging of high value portable devices and other mobile assets to monitor their movement.
- Wireless mobile panic buttons with movement tracking.

3.7.5 Technology development plan

This section of the roadmap describes the “road” that the Tracking technology in Eskom will take over the next 5 – 10 years.

Table 9 below depicts envisioned time frame for development of tracking systems in Eskom.

Table 9: Development time frame for Tracking systems

Technology	Technology Development Time Frame									
	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Tracking Systems										

Key:	Literature/market scans, Research	Pilots	Standardisation	Ready for implementation	Technology Discontinued

3.7.6 Implementation plan

The table below depicts a high level implementation plan for the Tracking technologies in Eskom

Table 10: Implementation plan for tracking systems

Activity	Implementation Time Frame																	
	2021		2022		2023		2024		2025		2026		2027		2028		2029		2030	
Product evaluation and contract																				
Training																				
Maintenance Strategy																				
Rollout																				

3.8 Security Monitoring/Control Centres

3.8.1 Overview

Security monitoring centres will be used to integrate and monitor security feeds, access control and alarms from various Eskom sites including Transmission sites, Distribution sites, Eskom telecoms sites etc.

3.8.2 Current situation

Some Eskom Security Monitoring Centres exist, but mostly 3rd party centres are used. Security related alarms and video streams are routed to the Main Control centre with other network alarms such as ones relating to protection of primary plant equipment. Due to the perceived higher priority of these other alarms, the security related alarms are often not attended to in a timely manner.

3.8.3 Business requirements

The objective is to send video images and alarms to the centralized security monitoring centers, this will enable a quick efficient response in case of a security incident occurring. The monitoring centres will bring the following benefits:

- Improvement in the management of physical access to Eskom sites.
- Improve the safety and security of Eskom assets;
- Establish an audit trail of access to Eskom facilities;
- The monitoring centres should enable an integrated management of security technologies including CCTV system, access control system, alarms, PA systems etc. providing a unified security management system.
- Having an integrated view in near real-time, of who is entering and exiting Eskom sites.
- Reliable availability of information and audit trails of security related data such as photographs, biometrics, visitor management records and entry/exit records to assist in investigations related to security breaches.
- Use of security management systems that use standard protocols and can be used to monitor and control the different security technologies used by Eskom.

3.8.4 World trends and use of technology

Deployment of security control centres that are based on open system architecture to allow various security technologies to be integrated into unified and scalable security platforms.

3.8.5 Technology development plan

This section of the roadmap describes the “road” that the security monitoring centres in Eskom will take over the next 5 – 10 years.

Due to their complexity and big scale, the security control centres development will take a collaborated effort involving different Eskom departments including Engineering, Group IT, Group security, Real Estate and Regional Security Sections / departments.

There also exists a number of dependencies which the system relies on to be effectively developed, these include:

- Availability of IT/IM systems – servers.
- Telecommunications infrastructure being in place.
- Monitored systems should be installed and fully functional and integratable, these include CCTV systems, access control systems, alarms PA systems etc.

A project has been raised to pilot a Security Control Center together with the associated Physical Security Information Management System (PSIM). Through this pilot project, the following business requirements will be tested and used as benchmark for future implementations:

- Enterprise-wide integration of physical security systems.
- Collect and correlate data from multiple unconnected or diverse security subsystems and components.
- Manage incidents in real time.
- Create real-time dashboards and reports.
- Present site-relevant information in a GIS (Geographical Information System) format to enhance situational awareness.
- Manage the information flow between the security control centre and its associated physical security systems.
- Classify incidents, apply the appropriate response and create alarms and notifications.
- Manage incident response and escalate to the level of response needed.
- Investigate user security profiles and behaviours.
- Replay any event or incident from the stored database for further investigation.

After the pilot project different SCC’s (Security Control Centres) will exist, i.e. RSCCs (Regional Security Control Centres) and NSCCs (National Security Control Centres). These Control Centres will make use of Eskom-owned Data Centre facilities and connect via Eskom-owned Telecommunications infrastructure.

Table 11 below shows envisioned development times for the Security Control Centers.

Table 11: Development time frame for Security Control Centres

Technology	Technology Development Time Frame									
	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Security Monitoring/Control centres including PSIM										

Key:	Literature/market scans, Research	Pilots	Standardisation	Ready for implementation	Technology Discontinued

3.8.6 Implementation plan

The implementation of the Security control centres will be in line with the security systems strategy as determined by Eskom.

4. Authorization

This document has been seen and accepted by:

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

5. Revisions

Date	Rev	Compiler	Remarks
May 2021	2	R Moshoeshoe	• Changed document title from Security Systems Technology Roadmap to Physical Security Systems Technology roadmap • Updated the Technology development time frames • Updated strategy for the EBI technology regarding its phasing out as the legacy technology • Updated details for Security Monitoring/Control Centres and PSIM
April 2016	1	T Jacobs	First issue

6. Development team

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

- Thomas Jacobs
- Victor Lehobo
- Albertus Hendriks
- Moeried Jattiem
- Monette Heath
- Cornelius Naidoo
- Tejin Gosai
- Bradley Taaibosch

- Andre Van Den Berg
- Cornelius Visagie
- Craig Moran
- Shaun Solomon
- Chris Van Reenen

7. Acknowledgements

Not applicable.