

 Eskom	Standard	Technology
------------------------------------------------------------------------------------------------	-----------------	-------------------

Title: **SPECIFICATION FOR
INTEGRATED ACCESS
CONTROL SYSTEM (IACS) FOR
ESKOM SITES**

Unique Identifier: **240-102220945**

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

Area of Applicability: **Engineering**

Documentation Type: **Standard**

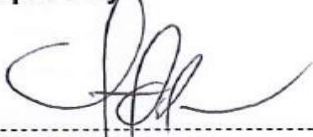
Revision: **1**

Total Pages: **40**

Next Review Date: **September 2021**

Disclosure Classification: **Controlled
Disclosure**

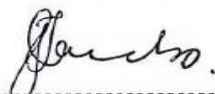
Compiled by



Donald Moshoeshe
Engineer

Date: 18 August 2016

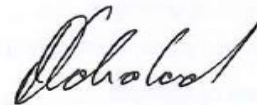
Approved by



Thomas Jacobs
**DC & Auxiliary Supplies SC
Chairperson**

Date: 18 August 2016

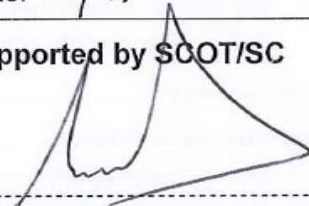
Authorized by



Danie Odendaal
Engineering SGM (Acting)

Date: 9/9/2016

Supported by SCOT/SC



Richard McCurrach
PTM&C TC Chairperson

Date: 31/8/2016

Content

	Page
1. Introduction	5
2. Supporting clauses	5
2.1 Scope	5
2.1.1 Purpose	5
2.1.2 Applicability	5
2.2 Normative/informative references	5
2.2.1 Normative	5
2.2.2 Informative	6
2.3 Definitions	6
2.3.1 General	6
2.3.2 Disclosure classification	7
2.4 Abbreviations	7
2.5 Roles and responsibilities	9
2.6 Process for monitoring	9
2.7 Related/supporting documents	9
3. Access control systems classification	10
3.1 General	10
3.2 Class 1 — Common code	10
3.3 Class 2 — Common access card	10
3.4 Class 3 — System coded access card	10
3.5 Class 4 — Unique access card	10
3.6 Class 5 — Unique access card and personal identification number (PIN)	10
3.7 Application of ACS class types	10
4. System role players/actors	11
5. Operational requirements	11
5.1 General operational requirements	11
6. Access Control Models	13
7. System architecture	13
8. Communication and network requirements	15
8.1 General communication requirements	15
8.2 Supported communication standards	16
8.3 Bandwidth requirements	16
8.3.1 Bandwidth estimations	16
9. Cyber security	17
10. Hardware requirements	17
10.1 Server requirements	17
10.2 Registration stations	18
10.3 Client stations	19
10.4 Readers and reader controllers (for both outdoor and indoor use)	19
10.4.1 General	19
10.4.2 Card readers	20
10.4.3 Biometric readers	20
10.4.4 Reader controllers	20

ESKOM COPYRIGHT PROTECTED

10.5	Goosenecks	21
10.6	Access cards	21
10.7	Barriers	22
10.7.1	Doors.....	23
10.7.2	Gates.....	24
10.7.3	Vehicle stoppers	24
11.	Integration requirements.....	25
11.1	General.....	25
12.	Buildings access control	25
13.	Reporting	25
13.1	Attendance Register.....	25
13.2	Visitor reports	26
13.2.1	Visitor/Host registration information	26
13.3	Additional Reports	29
13.4	Graphical User Interface Requirements.....	30
13.4.1	Functional GUI Requirements.....	30
13.4.2	Additional GUI alarm requirements.....	31
13.5	Databases	31
13.5.1	General database requirements	31
13.5.2	Database structure.....	32
14.	Alarms.....	32
15.	Power supply	33
16.	Cabling requirements	33
17.	Physical requirements	34
17.1	Tamper protection	34
17.2	Ingress protection.....	34
17.3	Safety	35
18.	Environmental requirements	35
18.1	General.....	35
18.2	Operating conditions	35
18.3	EMC requirements	35
18.4	Earthing.....	35
19.	Labelling and numbering	36
20.	Markings	36
21.	Inspections and methods of tests	36
22.	Miscellaneous requirements.....	36
22.1	Spares	36
22.2	Tools and test equipment.....	37
22.3	Training	37
22.4	Warranty.....	37
22.5	Repairs	38
22.6	Support contract requirements.....	38
23.	Authorization.....	38
24.	Revisions	39

25. Development team	39
26. Acknowledgements	40

Tables

Table 1: Application of ACS class types	11
Table 2: IACS role players/actors	11
Table 3: System bandwidth estimations for Regional Centres	17
Table 4: Visitor reports requirements	26
Table 5: Preregistration information/fields	26
Table 6: Registration (Check in/out) Fields	28

1. Introduction

A surge in crime related incidents at Eskom sites has prompted a mandate to initiate a Security Improvement Plan (SIP). The increasing threat to the safety and security of people, information and assets is impacting Eskom operations and its ability to deliver a world class service, and in turn, public confidence in Eskom. The safety of people and the integrity of information and assets is a key priority in Eskom.

An Integrated Access Control System (IACS) is a combination of business processes, policies and technologies that will allow the organization to provide secure, scalable and robust future-proof solutions that are able to flexibly be deployed as security requirements evolve. The Integrated Access Control System is aimed at improving and effectively managing physical access control and physical security at Eskom sites. The purpose of the integrated system is also to allow users the ability to achieve maximum benefit from each individual system whilst reducing the time, cost as well as risk that comes with operating and maintaining a number of individual, stand-alone systems.

Access control is about managing access rights of individuals, visitors into various sites and facilities. It is about granting and limiting permissions to Employees, visitors, contractors in and out of various areas, e.g., secure and non-secure areas and how these must be managed. This includes lockdown of facilities, lockout of facilities, emergencies, etc.

An Integrated Access Control System is a solution that consists of hardware and software designed to control entry into selected areas and manage movement of people/vehicles within. The system must be agnostic to the choice of field equipment technologies as well as the type of data carriers/ credentials for system users.

The main components of an Integrated Access Control System are the system software, electromagnetic hardware, electronic hardware and system users.

2. Supporting clauses

2.1 Scope

2.1.1 Purpose

Purpose of this document is to outline the technical specifications for the Eskom standard Integrated Access Control System (IACS) for procurement of Access Control Systems at Eskom sites that will integrate to the existing Integrated Access Control System backbone.

2.1.2 Applicability

This document shall apply throughout Eskom Holdings SOC Limited Divisions and subsidiaries.

2.2 Normative/informative references

The following documents contain provisions that, through reference in text, constitute requirements of this specification. At the time of publication, the editions indicated were valid. These documents are subject to revision, parties using this document are encouraged to apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

- [1] ISO 9001 Quality Management Systems.
- [2] SANS 2220-2-1 - Access control systems Part 2-1: General characteristics
- [3] SANS 2220-2-2 - Access control systems Part 2-2: Central processors
- [4] SANS 2220-2-3 - Access control systems Part 2-3: Card readers
- [5] SANS 2220-2-4 - Access control systems Part 2-4: Reader controllers

-
- [6] SANS 2220-2-5 - Access control systems Part 2-5: Biometric readers
 - [7] SANS 2220-2-6 - Access control systems Part 2-6: Access cards
 - [8] SANS 2220-1-7 - Electrical security systems Part 1.7: Intruder alarm systems: Power units
 - [9] SANS 61000-1-2 - Electromagnetic compatibility (EMC) Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena
 - [10] 240-55410927 - Cyber security standard for Operational Technology
 - [11] 240-55683502- Definition of Operational Technology (OT) and OT / IT Collaboration Accountabilities
 - [12] 240 – 56872313 - Radio Station Earthing and Bonding
 - [13] 240 – 56356396 - Earthing and Lightning Protection Standard
 - [14] TST41-877 - Transmission Substation Design Earthing Standard
 - [15] 240-56360034 - Stationary Vented Lead Acid Standard
 - [16] 240-56360086 - Stationary Vented Nickel Cadmium Batteries Standard
 - [17] 240-51999453 - Specification for Valve Regulated Lead Acid Cells
 - [18] 32-1203 - Eskom Telecommunications User Requirements Specification
 - [19] 240-94136376 - IP Voice and Data Network Design Guideline
 - [20] 240-79669677 - Demilitarised Zone (DMZ) designs for Operational Technology
 - [21] 240-46264031 – Fibre Optic Design Standard – Part 2: Substations
 - [22] 32-438 - Information Security Systems Classification Standard
 - [23] IEC 62645 - Nuclear Power Plants – Instrumentation and Control Systems-Requirements for Security Programme for Computer-based Systems
 - [24] 240-71432150 - Plant Labelling and Equipment Description Standard
 - [25] 240-86738968 - Specification for Integrated Security Alarm System for Protection of Eskom Installations and its Subsidiaries

2.2.2 Informative

- [26] 240-78980848 - Specification for Non-Lethal Energized Perimeter Detection System (NLEPDS) for protection of Eskom Installations and its subsidiaries
- [27] 240-79537982 - Security Threat and Risk Assessments
- [28] 240-44175038 - Control of Non-Conforming Product or Service Procedure
- [29] 240-91190304 - Specification for CCTV Surveillance with Intruder Detection
- [30] 240-56737448 - Fire Detection and Life Safety Design Standard
- [31] 240-64720986 - Emergency Preparedness Public Address System - For Large Area Deployment
- [32] 240-64636794 - Standard for Wiring and Cable Marking in Substations
- [33] 240-70413291 - Specification for Electrical Terminal Blocks

2.3 Definitions

2.3.1 General

Definition	Description
------------	-------------

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

Definition	Description
Critical Asset	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electricity supply network.
Critical cyber assets	Cyber assets essential to the reliable operation of critical assets.
Cyber Asset	Programmable electronic devices and communication networks including hardware, software, and data.
Cyber Security	<p>Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:</p> <ul style="list-style-type: none"> • Availability • Integrity, which may include authenticity and non-repudiation • Confidentiality
Fail Safe	A device or practice that in the event of a specific type of failure, responds or results in a way that will cause no harm, or at least minimizes harm, to other devices or to personnel
Fail Secure	A device which, if (or when) it fails, does so in a way that will cause no harm or at least a minimum of harm to other devices or danger to personnel, and doesn't cause the system to be insecure
Gooseneck	Pedestal used to install card readers or intercoms at drive-up and pedestrian access points

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
A	Ampere
AC	Alternating Current
ACS	Access Control System
AES	Advanced Encryption Standard
API	Application Programming Interface
BACnet	Building Automation and Control Networks
CAD	Computer Aided Design
CCTV	Closed circuit television

ESKOM COPYRIGHT PROTECTED

Abbreviation	Description
DC	Direct Current
DDE	Dynamic Data Exchange
DVR	Digital Video Recorder
Dx	Distribution
EMC	Electro-magnetic Coupling
FAT	Factory Acceptance Test
GIOP	General Inter-ORB Protocol
GUI	Graphical user interface
Gx	Generation
h	hour
HD	High definition
HR	Human resources
HTML	Hypertext Mark-up Language
HV	High Voltage
HVAC	Heating, Ventilation and air Conditioning
IAC	Integrated Access Control
IACS	Integrated Access Control System
ICMP	Internet Control Message Protocol
ID	Identity Document
IEC	International Electrotechnical Commission
IP	Internet Protocol
IT	Information Technology
kg	Kilogram
km	Kilometre
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LonWorks	Local Operating Network
m	meter
mA	milliampere
mm	millimetre
MPLS	Multiprotocol Label Switching
MTBF	Mean Time Between Failures
MWP	Megawatt Park
NSCC	National Security Control Centre
NVR	Network Video Recorder

Abbreviation	Description
ODBC	Open Database Connectivity
OMA	Outdoor Morpho Access
OPC	Open Protocol Communications
OT	Operational Technology
PA	Public Address
PIN	Personal Identification Number
PIR	Passive Infrared Sensor
POE	Power Over Ethernet
RMU	Ring Main Unit
SANS	South African National Standard
SAT	Site Acceptance Test
SIP	Security Improvement Plan
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
TSL	Transport Layer Security
Tx	Transmission
UDP	User Datagram Protocol
UPS	Uninterruptable Power Supply
VIP	Very Important Person
VLAN	Virtual Local Area Network
WAN	Wide Area Network

2.5 Roles and responsibilities

- a) The Security Systems Care Group shall ensure that the technology developed is adequate for application across Eskom sites where it will be utilized.
- b) Group security shall be responsible for auditing to ensure compliance with the requirements of this standard.
- c) The procurement team shall utilise this document for the enquiry process and during the product development phase.

2.6 Process for monitoring

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

2.7 Related/supporting documents

Not applicable.

3. Access control systems classification

3.1 General

The requirements of the Access Control System are based on what the needs of Eskom are as the client. Access control systems are classified by the degree of security they provide and security requirements from the client in accordance with Global Accepted Security Standards. The supplier of the system shall indicate the classification of the system in accordance with Global Accepted Security Standards; 4.1 of SANS 2220-2-1, the classification being related to the nature of the risk, level of security that the client has specified and the level of security that is provided. In the classification of the systems below, other access control data carrier technologies such as Biometrics may be used instead of a card.

3.2 Class 1 — Common code

A class 1 access control system shall allow access to persons who key in a single common code. The code may be alphabetic, numeric or alphanumeric.

3.3 Class 2 — Common access card

In a class 2 access control system, each card shall have the same encoded data chosen from at least 10 000 possibilities.

3.4 Class 3 — System coded access card

In a class 3 access control system, each card shall have a system code chosen from at least 200 possibilities and an individual code chosen from at least 10 000 possibilities. It shall be possible to add cards to or delete cards from the system. The cards shall not be accepted by any system other than the one in which they are intended to operate. This class of access control system shall incorporate a central control and monitoring system whereby the central processor software can be used to generate reports on the status of any card.

3.5 Class 4 — Unique access card

In a class 4 access control system, it shall be possible to decentralize the intelligence. Each card shall have a code chosen from at least ten million possibilities and any attempt to change or modify the code shall destroy the card. It shall be possible to add cards to or delete cards from the system.

The cards shall not be accepted by any system other than the one in which they are intended to operate.

This class of access control system shall incorporate a central control and monitoring system whereby the central processor software can be used to generate reports on the status of any card.

3.6 Class 5 — Unique access card and personal identification number (PIN)

A class 5 access control system shall have at least the same features as a class 4 system but shall also use a PIN of at least four digits or use biometrics.

3.7 Application of ACS class types

The ACS classes defined above should be used in protecting classified systems in Table 1 below as classified in the Information Security Systems Classification standard (unique identifier: 32-438) and the Cyber Security Standard for Operational Technology (unique identifier: 240-55410927). The standards define the classification scheme to indicate the need, priorities and degree of protection that should be afforded to the system based on the confidentiality, integrity and availability requirements of the system.

Table 1: Application of ACS class types

Access Control System class	System classification levels (Availability, Integrity, Confidentiality) as classified in 32-438	Cyber Assets Classification as classified in 240-55410927
Class 1	Low, low, Public	Cyber Asset
Class 2	Moderate, Moderate, Controlled Disclosure	Cyber Asset
Class 3	High, Moderate/High, Controlled Disclosure/ Confidential	Essential Cyber Asset
Class 4	High, High, Confidential	Critical Cyber Asset
Class 5	High, High, Secret/Top Secret	Critical Cyber Asset

4. System role players/actors

The system should have role players/actors that interact with the IACS as defined in Table 2 below:

Table 2: IACS role players/actors

Actor	Role(s)
Security Manager	<ol style="list-style-type: none"> 1. This is the owner of the system. 2. Site / zone update, setup and configuration of IACS accordingly with the ongoing needs of the organization. 3. Generates Reports to Manage Security and Investigate.
Access Area Operator	Facilitate and allow/deny access/exit to site
Reception Operator	Enrol/Register a Visitor
Registration Operator	Enrol/Register an Employee or Contractor
Employee	<ol style="list-style-type: none"> 1. Pre-Register visitors 2. Host a visitor 3. Visitor to another Eskom site 4. Card Holder
Visitor	External Visitor, Employee visiting another Eskom site, Card Holder
Security Administrator	On instruction of the Security Manager, he/she can set the Site / zone update, setup and configuration of IACS.
IT Administrator	IT System monitoring, troubleshooting and escalates access control issues
Security Control Room Operator	Attend to alarms; Monitor and Escalate Alarms

5. Operational requirements

5.1 General operational requirements

The IACS must primarily cater for Eskom's integration requirements and must form the basis to engage with all the disparate systems in the physical security environment.

The IACS (Integrated Access Control System) shall be the standard Physical Access Control across Eskom with capabilities to integrate with but not limited to CCTV, Lifts, Canteen Management System, Transportation System, Building Management Systems and other security / business subsystems to provide a unified security management system.

The system shall be capable of providing access control for Corporate Offices and any other Eskom buildings, Power Stations, Dx and Tx substations, Mini substations, Sites under construction, Control Rooms, Technical Services Centres, Customer Walk-in Centres, Laboratories, Water treatment plants, Visitor Centres, Stores, Workshops, Canteens, Medical Centres, Fire Stations, Boardrooms, Conference facilities, Eskom Telecommunications Radio Sites, Maintenance or service centres, Server Rooms, Gyms, Kitchens, Boarding/Accommodation and Bus areas. In addition to providing access control to different site types, the system shall also be able to provide access control to equipment requiring restricted access such as metering kiosks and RMU(s). The integrated Access Control system shall achieve the following general requirements:

- 1) The system shall be able to transfer data to SAP for Time and attendance data.
- 2) Each user authorization shall be uniquely definable.
- 3) Operator terminals shall be protected by terminal security such as password policy.
- 4) All actions on the system shall be traceable and auditable. These actions must be kept for a minimum period of 90 days.
- 5) The system shall allow for an allocated employee number (unique number) to be changed when a contractor or visitor becomes a permanent employee with Eskom (i.e. a scenario must be allowed for whereby a person can initially be registered as a visitor/contractor and then upgraded to permanent employee status, without having to re-register the person).
- 6) The system shall be able to automatically disable a visitor or contractor on the required date of termination as entered by the registrar on the registration facility at the date of registering.
- 7) A visitor shall be disabled after leaving the site or designated place of visit/work, this function must be reversible whereby a person can be enabled should he require entering the premises again. Depending on the specified elapsed time after the initial authorisation was granted, to allow return access the full process of authorisation must be followed, otherwise a verification process must be followed.
- 8) The system shall have a full anti-pass back facility to control the flow of personnel from one zone to the other, (i.e. once a person has successfully fingerprinted and has passed through the access control point, access must be blocked in terms of the zone he has just left – i.e. preventing a scenario whereby a person can allow another person through an access control point based on his fingerprint).
- 9) High risk areas access shall be granted only to personnel working in that area. Additional access shall only be granted if the necessary approval has been given by the responsible person of that area and shall be automatically disabled as soon as that person leaves the area.
- 10) The system shall allow for overrides, interlocking and other functions as they become necessary to operate and optimize the system by the administrator at a remote location.
- 11) The system shall be able to interface with existing software packages and therefore an open protocol software platform will be required.
- 12) It shall be possible for the operator to bypass anti-pass back rules selectively such as one host having multiple visitors.
- 13) The system shall have lockdown functionality in emergency situations.
- 14) System shall allow for online changes to be made.
- 15) Real-time online debugging shall be possible.
- 16) The system shall be either fail safe or fail secure, as required.
- 17) The application for change or update of access shall be completed on a standardised eForm.
- 18) There shall be a dedicated “Master” station to assist in roll call in the event of an evacuation. Indicating who was in the building at the time of evacuation and if all are accounted for at the assembly point.

- 19) The system shall have a built in Fitness For Duty (FFD) program or interface to the FFD program. FFD is a program that qualifies persons for access to certain areas on condition that they have successfully qualified for entry to area, e.g. Plant Induction Training (PIT), radiation workers, medically fit, not blacklisted, etc.
- 20) Reporting functionality for the system shall comply with the requirements of section 13 of this document.

6. Access Control Models

The system should be able to enforce access through the following types of controls

- 1) Attribute-based Access Control (ABAC)
- 2) Discretionary Access Control (DAC)
- 3) History-Based Access Control (HBAC)
- 4) Identity-Based Access Control (IBAC)
- 5) Mandatory Access Control (MAC)
- 6) Organization-Based Access control (OrBAC)
- 7) Role-Based Access Control (RBAC)

7. System architecture

The system should have a distributed architecture with tiered model comprising Primary Servers, Regional Servers and Site Servers as depicted in Figure 1 below, with the exception of nuclear sites where security control can only be done at site level.

Note: For details on DMZ designs refer to 240-79669677 - Demilitarised Zone (DMZ) designs for Operational Technology standard

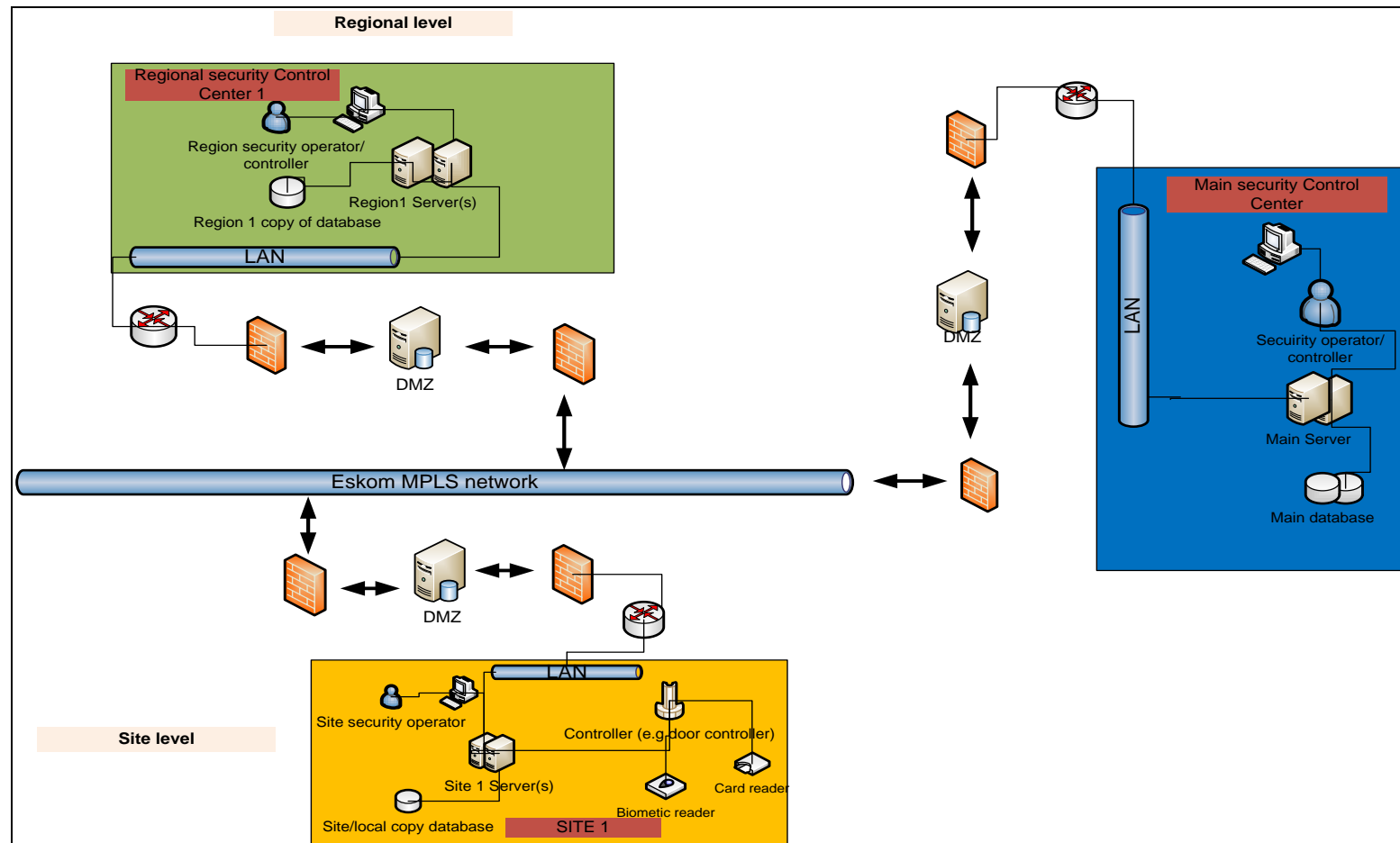


Figure 1: High Level ACS Architecture

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

- 1) There shall be a primary server hosted at the main Security control centre which shall act as a single source for all Eskom's card Holder data.
- 2) The primary server shall have redundancy with real time synchronisation with the secondary/ back-up server.
- 3) At regional level there shall be regional servers connected to the Primary server via the Eskom Telecoms IP network.
- 4) The regional servers shall have real time synchronisation of card holder information with the Primary server. These servers shall have a daily full server backup.
- 5) At site level (where applicable), there shall be site server(s) installed with various security end point devices. The sites server(s) shall be capable of operating in isolation if it loses connectivity to the regional sever to ensure business continuity.
- 6) Firewalls and servers shall be managed by Eskom to ensure confidentiality and integrity of information. Where a third-party is appointed for management of firewalls and servers, there shall be a non-disclosure agreement signed between Eskom and the third-party and Eskom shall be approached for approval of any planned upgrades or changes before they are implemented.

8. Communication and network requirements

8.1 General communication requirements

- 1) Suppliers shall ensure that the system is capable of using Eskom's existing communication infrastructure.
- 2) The network infrastructure shall adhere to the principles laid out in the following documents which will be made available to the contracted supplier:
 - a) 240-55410927 - Cyber Security Standard for Operational Technology
 - b) 240-55683502 - Definition of Operational Technology (OT) and OT / IT Collaboration Accountabilities
 - c) 32-1203 – Eskom Telecommunications User Requirements Specification
 - d) 240-94136376 - IP Voice and Data Network Design Guideline.
 - e) 240-46264031 – Fibre Optic Design Standard – Part 2: Substations.
 - f) IEC 62645 Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Security Programme for Computer-based Systems.
- 3) The network provided shall link all the controller servers and client stations on site with 99.99 % availability.
- 4) The system shall allow IP to IP connection between the servers.
- 5) The system shall allow multi-casting for distributing status information between servers.
- 6) The servers shall be time synchronised.
- 7) There shall be LAN points for servers with connectivity to IAC VLAN.
- 8) There shall be bus communication provision from servers to IACS field devices.
- 9) Servers shall be configured with static IP addresses.
- 10) All reader controllers shall have interface capabilities stipulated under section 4.1.3 of SANS 2220-2-4.

- 11) The System shall at minimum cater for Ethernet 10/100/1000 with auto negotiation, the supplier shall also indicate if their equipment supports the following I/O ports:
- a) RS-232
 - b) RS-485
 - c) Wiegand in/out
 - d) TTL in/out
 - e) Modem (to provide alternative Comms where there is no network infrastructure installed).

8.2 Supported communication standards

- 1) The system shall support open communication standards/protocols that will enable it to be integrated to the existing IACS backbone infrastructure. At minimum the following standards shall be supported:
- a) TCP/IP
 - b) HTML
 - c) LonWorks
 - d) BACnet
 - e) OPC
 - f) MODBUS
 - g) ODBC
 - h) Wiegand
 - i) UDP
 - j) DDE
 - k) GIOP
 - l) TSL/SSL
 - m) ICMP
 - n) SOAP

8.3 Bandwidth requirements

- a) Bandwidth allocation for the system shall comply with the requirements of Eskom Telecommunications User Requirement Specification (Unique identifier: 32-1203).
- b) Suppliers shall state the required bandwidth to link the ACS systems at sites to the existing Dedicated VLAN infrastructure allocated for the IACS in line with international Security Standards. Eskom Telecoms network infrastructure will be provided to connect the sites to the main security network.

8.3.1 Bandwidth estimations

8.3.1.1 Eskom's vision is to have regional security control centres. Table 3 below depicts estimated minimum bandwidth requirements that should be catered for, per day between the regional points of presence on MPLS.

Table 3: System bandwidth estimations for Regional Centres

Region	Estimated number of users	Estimated minimum bandwidth required (in Kbps)
MWP	10758	512
Witbank	10838	512
Simmerpan	11980	512
Mkondeni	3079	512
East London	2296	512
Polokwane	2422	512
Bloemfontein	2717	512
Belville	5459	512

8.3.1.2 For specific sites in the respective regions, the bandwidth required shall be determined in consultation with the Eskom Telecomms department and factors such as criticality of the site, clocking bandwidth, bandwidth for graphic displays etc. will be taken into consideration.

9. Cyber security

- 1) The system shall comply with Eskom' Cyber Security standard for Operational Technology (Unique identifier: 240-55410927).
- 2) The system shall comply with the requirements of Demilitarised Zone (DMZ) designs for Operational Technology (Unique identifier: 240-79669677).
- 3) For nuclear sites the system shall comply with site specific cyber security procedures and programs. This includes allowing a limited number and nature of external connections to the system. Preference shall be given to solutions that use physical layer data diodes. There shall be no incoming data streams to the security system with the exception of the stations GPS clock and limited data from the FFD system. As a minimum these links shall go through a Deep packet inspection.

10. Hardware requirements

10.1 Server requirements

- 1) The server shall comply with the requirements of SANS 2220-2-2.
- 2) There shall be a primary server where all the system configurations and event data is stored.
- 3) There shall be a redundant sever which is a mirror of the primary server. This server is used in case of primary server failure.
- 4) There shall be a regional server(s) containing configurations and access control data for the region.
- 5) There shall be a test server which is a mirror of the primary server. The function of this server is to perform all testing related activities before moving the changes into production.
- 6) There shall be synchronization between field devices and server network such that transaction records are automatically uploaded from each reader to the relevant database.
- 7) The server shall automatically back up data, this data shall be stored for a minimum period of 36 months.
- 8) There shall be LAN points for servers with connectivity to the IAC VLAN.
- 9) There shall be servers that handle administration at each site that can be diverted to a central server that is situated at the security control centre.

ESKOM COPYRIGHT PROTECTED

- 10) The server shall be able to handle the automatic deletion of visitor and contractor account/profile after the expiry date.
- 11) The server shall be able to handle the deletion and removal of redundant account/profile based on information received from an administrator workstation.
- 12) Cabinets with minimum IP 65 rating shall be used for servers. These shall be housed inside the nearest restricted building such as guard house or access control building.
- 13) The server shall have 99.99 % availability.
- 14) The server shall be of a modular design.
- 15) The server shall contain a real-time clock circuit synched with a GPS time clock, capable of maintaining and displaying real time (month, day, hour, minute and second).
- 16) Interface between the server and the peripheral devices (such as readers and reader controllers) shall be by means of a standard communications protocol.
- 17) The server shall allow entry to the system parameters by password only, and there shall be at least three levels of password to allow three levels of access.
- 18) The server software shall maintain a real-time sequential record (on the hard disk) of reader events, alarm events and all operator programming events. If so required, these events shall be stored in such a format that it is possible for other operators to sort and analyse them.
- 19) The sizing of the servers shall be guided by the following factors:
 - a) Number of estimated card holders per site
 - b) Estimated transactions per cardholder per day
 - c) Amount of space (in GB) that the transactions information will require per month
 - d) The retention period of the information and the capacity (in GB) that will be required for retaining this information.
 - e) Storage for event management data
 - f) Storage for log files
 - g) Storage for backups and installation media

10.2 Registration stations

- 1) The Security Manager shall be the owner and main operator of the system responsible to provide any changes and permissions to the system.
- 2) Upon positive screening and security vetting of the employee by HR, then the employee can proceed to the Security Manager to be issued with a card or credential valid for 1-year. The registration facility shall enable the Security Manager to be able to register, disable, enable and change personnel details of employees, Visitors and other personnel onto the access control system for them to be able to gain access into the approved areas as approved by the security management team.
- 3) A full audit-trail shall be provided for all registration transactions.
- 4) Registration shall be fingerprint protected – i.e. the access control administrator shall be required to fingerprint in order to login to the registration application.
- 5) The registration stations shall be integrated to the database where the access control data is kept.
- 6) Permanent employees shall only be registered once authorization has been given. Registration should only be authorised when an Identity document and employee number (unique number) are produced by the employee.
- 7) Visitors shall only be authorised for registration when a valid identity document is produced and confirmation from the Eskom employee been visited has been received.

ESKOM COPYRIGHT PROTECTED

- 8) Contractors shall only be authorised for registration after producing a valid labour requisition form with start and end date captured and a valid identity document. There shall be automatic lockout after completion of the work related to the contract.
- 9) Permanent employee's access rights shall only be disabled on request from the Security and/or HR department.
- 10) Visitors' access rights shall be disabled by the access control auto-disabling function at the end of the scheduled visiting time/period and/or at the return of the visitor access card in the drop box.
- 11) Contractors' and sub-contractors access rights shall be disabled once the term that is recorded expires. A reminder shall be generated by the system 48 hours prior to disabling the access rights. This reminder shall be sent to HR department, affected contractors and project managers.
- 12) The HR department shall notify the systems administrator to extend or terminate the access rights, the system shall generate automated reminders to the HR department and system administrators for access rights expiry dates.

10.3 Client stations

- 1) The IACS shall use a client/server architecture
- 2) The client stations shall be used by the operator to view alarm/events and manage the system. This client station shall have a standard Eskom desktop image loaded.
- 3) The reception stations shall be used by the operator to manage visitors. This reception station shall have a standard Eskom desktop image loaded.
- 4) The software installed on the client stations shall cater for the following requirements:
 - a) Screen modification programs.
 - b) Menu modification programs
 - c) Keyboard modification programs
 - d) Colour modification programs
 - e) Icon menu modification programs
 - f) System monitor programs
 - g) Logbook reset program
 - h) Graphical font modification program
 - i) System message modification program

10.4 Readers and reader controllers (for both outdoor and indoor use)

10.4.1 General

- 1) It shall be possible to assign to any reader an IN or OUT function in any geographic area or any combination of areas.
- 2) It shall be possible for the operator to declare any reader as either card only, card plus biometrics, card plus PIN, or to switch from one state to the other. The central processor shall automatically do the necessary status checking and send the appropriate command to the reader controller.
- 3) It shall be possible to attach an identifier to each reader to assist in identifying reader locations for record purposes.
- 4) It shall be possible to assign to any reader a time and attendance function. This function shall be independent of the access control function. Time and attendance events shall be recorded sequentially in a separate record.

- 5) It shall be possible for the processor software to enable or disable any reader at any time or to switch from one state to the other. The central processor shall generate a report showing which readers are currently enabled or disabled. There shall be an audit trail of the user who completed the change and authorization.

10.4.2 Card readers

- 1) Card readers shall comply with requirements of SANS 2220-2-3.
- 2) A card reader shall accept cards presented to it through proximity, or long distance reading or remote controls linked to access cards such that systems can be armed/disarmed and access be granted without exiting the vehicles at sites located in risky areas.
- 3) The reader shall use visual confirmation e.g. light-emitting diodes to show whether access was granted or denied. The response shall be within 100 milliseconds of presentation of the access card.
- 4) If a PIN keypad is included in a card reader, access shall only be granted when the card and its associated PIN have been validated.
- 5) The readers shall be capable of reading access cards and send data to an associated interface.
- 6) A card reader shall be capable of indicating failures as well as an alarm condition.

10.4.3 Biometric readers

- 1) Biometric readers shall comply with requirements of SANS 2220-2-5.
- 2) A biometric device shall contain a sensor that recognizes a person's physical characteristics, such as the following:
 - a) fingerprints;
 - b) hand geometry (finger position and length);
 - c) retina patterns;
 - d) voice patterns; or
 - e) signature
- 3) If a PIN keypad (from which a personal identification number can be entered) is used, access shall only be granted on validation of both the PIN and the measured physical characteristics.
- 4) There shall be biometric readers capable of requesting biometric validation after presentation of the access card, after which it shall send data to an associated interface.
- 5) The MTBF (mean time between failures) of biometric readers shall comply with section 4.1.5 of SANS 2220-2-5.
- 6) If a biometric reader is connected to a central processor, it shall be by means of standard communications protocol.
- 7) The biometric device shall comply with all relevant health and safety requirements and regulations.
- 8) Markings for biometric readers shall comply with section 5 of SANS 2220-2-5.

10.4.4 Reader controllers

- 1) Reader controllers shall comply with requirements of SANS 2220-2-4.
- 2) A reader controller shall be used where a reader cannot be connected directly to a central processor.
- 3) Construction of reader controllers shall comply with section 4.1.1 of SANS 2220-2-4.

- 4) The MTBF (mean time between failures) (guaranteed by the supplier) of a reader controller (assessed in accordance with IEC 60050-191 and IEC 60300 (all relevant parts)) under normal operating conditions shall be at least 8 000 h.
- 5) A site server shall be used to control all reader controllers for a site.
- 6) The reader/door controller must keep a local copy of the access control lists and logs, so that stand-alone operation is possible for a defined time in the event of a communications failure.

10.5 Goosenecks

- 1) Goosenecks with base plate and front mounting shall be provided, for cars these goosenecks shall be 1.1 meters high and for trucks these shall be 1.83 meters high.
- 2) Goosenecks for double height shall be provided.
- 3) The goosenecks shall be fitted with rain covers.
- 4) There shall be provision for removable goosenecks, where certain lanes might be utilised for extra heavy vehicle access.

10.6 Access cards

- 1) Access cards shall comply with the requirements of SANS 2220-2-6.
- 2) Access shall be available in the formats below:
 - a) swipe cards
 - b) contact cards
 - c) passive proximity cards
 - d) active proximity cards
- 3) Access cards shall be Eskom's approved corporate identity template and be made of a durable material that can display the following information, as required:
 - a) an ID photograph;
 - b) Employee number (unique number);
 - c) a company logo;
 - d) name and other information of bearer (e.g. vehicle permit information).
- 4) Card printers shall be used to print the employee details and card layout directly to the cards before issuing.
- 5) The standard card format shall at minimum have 128 Bit Encryption.
- 6) The cards shall have support for random ID, each card shall have a unique serial number printed on the card.
- 7) Dimensions of access cards shall comply with section 4.1.2 of SANS 2220-2-6.
- 8) An ACS card encoder shall be used to encode cards by loading the required information regarding the card owner before issuing of the card. Any attempt to change the code shall destroy the card.
- 9) A photograph of the card holder shall be captured using a digital HD camera before issuing the card.
- 10) The card shall be water resistant and resistant to wear and tear caused by extended use.
- 11) The location of the contacts and the microchip shall not cause surface irregularities on the back of the card or in the magnetic strip area.
- 12) It shall be possible to print a list of all card numbers and their cardholder names which conform to a combination of specific and non-specific parameters.

ESKOM COPYRIGHT PROTECTED

- 13) When so required, the central processor shall be able to provide a print-out of all activities of a card.

10.7 Barriers

- 1) A barrier shall be one of the following devices intended to prevent unauthorized access to a controlled area:
 - a) an access booth;
 - b) a door (with door closer or monitor or both);
 - c) a vehicle boom;
 - d) a vehicle gate;
 - e) a vehicle stopper;
 - f) a turnstile.
- 2) A barrier shall at minimum, consist of the following components:
 - a) a physical barrier;
 - b) a detection unit, this can be used to detect an object in the path of the barrier which could obstruct the barrier movement;
 - c) an interface to a control unit operated manually or by some access control facility;
 - d) a barrier status device, and
 - e) a tamper protection device.
- 3) The mean time between failures (MTBF) of a barrier shall be such that, under normal operating conditions, there are at least 100 000 operations with specified maintenance and 50 000 operations without maintenance. In the case of barriers of width more than 4 m and up to 10 m, the number of operations shall be 50 % of the above, and in the case of barriers of width more than 10 m, the number of operations shall be as specified by the manufacturer.
- 4) When an access booth is tested in accordance with section 6.3 of SANS 2220-2-7, the mechanism shall be activated by the access control system and an override switch. In the case of a power failure, the outside door of the booth shall unlock automatically, and the inside door shall lock automatically. The booth shall have a preset timer to relock the door if the booth was not used within 30 s after a door has been unlocked.
- 5) A panic/emergency alarm facility shall be provided on the inside of the booth, to allow any person trapped inside the booth to initiate an alarm.
- 6) If a booth malfunctions, it shall be possible to unlock the door from the outside with an emergency key override.
- 7) A barrier shall have the necessary potential free contacts to indicate status (open/closed).
- 8) A cubicle shall be so constructed that it is possible to anchor the booth to a solid base by means such as expanding bolts.
- 9) A class 4 or class 5 access control system using an access booth shall have a system to detect when more than one person is using the booth. In such a case, access shall not be granted.
- 10) The operating mechanism of the access booth shall have a locked cover equipped with a tamper protection switch.
- 11) Turnstiles and booms
 - a) Turnstiles shall comply with section 4.7 of SANS 2220-2-7.

- b) A vehicle boom shall consist of the following components:
 - i. an enclosure for the operating mechanism;
 - ii. a boom;
 - iii. detector loops;
 - iv. a warning device;
 - v. a mechanical crank;
 - vi. an operating mechanism;
 - vii. a boom rest (for a boom longer than 4 m).
- c) The boom shall be activated by electronic means such as a reader controller.
- d) The enclosure of an operating mechanism for a boom shall at minimum comply with the requirements of class IP45 of SANS 60529.
- e) There shall be provision for single and double height turnstiles.
- f) A drop box shall be used for visitors to capture the card on exit.
- g) Vehicle barriers with ground loop sensors shall be installed.
- h) At vehicle entrances dual height gooseneck pedestals with rain covers for biometric readers shall be installed.
- i) Detector loops shall be so constructed that they can be buried in a road to detect vehicle movement. The boom shall close only after the vehicle has moved over the loop. The boom shall lower 30 s after it has been raised. The sensitivity of the detector loops shall be adjustable.
- j) Each boom shall incorporate a warning device such as lights or a siren, to indicate when the boom is in operation (opening or closing).
- k) In case of a power failure, it shall be possible to mechanically raise and lower the boom.
- l) The bearings of the boom shall be self-lubricating and maintenance free.
- m) Interface modules shall be installed for boom gates. They shall be mounted inside one of the boom enclosures behind the maintenance lid, mounted on din rail.

10.7.1 Doors

- 1) There shall be door monitors used to monitor the status of the door.
- 2) Electromagnetic locks with minimum 5000N holding force shall be used, the maglocks shall be released with an authorized access card, pin and/or biometric input.
- 3) Door closers shall be used to keep the doors closed and locked.
- 4) All doors shall be fitted with a resettable break Glass unit/pushbutton. When the break glass/pushbutton is triggered, an alarm shall be activated which shall override the door access control and keep the door unlocked. The break glass/pushbutton shall only be used during emergencies.
- 5) An electronic push bar shall be used on the fire exit doors to open the emergency escape from within the building. An emergency alarm should also be triggered by the opening of the emergency escapes.
- 6) Manual key overrides shall be installed for all critical doors (e.g. emergency doors); these should be wired in line with the break glass/pushbutton unit to cut power to any connected locks. The manual key overrides shall be mounted in such a way that they will not be vandalised or operated by unauthorised people.

- 7) For automated doors, the door movement shall stop when the door meets an obstruction, e.g. a person, and an obstruction alarm signal shall be initiated.
- 8) There shall be a provision for exit pushbuttons.
- 9) All bearings of the doors shall be self-lubricating and maintenance free.
- 10) There shall be an interface mounted inside a central enclosure where multiple doors are access controlled within a small geographical area.
- 11) There shall be an electronic door contact for door status indication purposes.

10.7.2 Gates

10.7.2.1 Vehicle gates

- 1) Motorized or hydraulic vehicle gates shall have the following components:
 - a) an enclosure for the operating mechanism;
 - b) an operating mechanism consisting, for example, of
 - i. an electric motor for electrically operated gates, or
 - ii. a pump complete with gears and valves for hydraulically operated gates;
 - c) a control box (for electronic control or key switch operation);
 - d) a status detector mechanism;
 - e) an obstruction detector mechanism; and
 - f) a warning device.
- 2) There shall be an enclosure with locked cover that gives access to the operating mechanism, gears, etc. The cover shall be equipped with a tamper protection switch, and shall comply with the requirements for class IP45 of SANS 60529.
- 3) The operating mechanism shall be so constructed that a person could not physically move it from the closed to the open position without using special tools.
- 4) A sliding gate drive shall move the gate at a speed of at least 10 m per minute.
- 5) A swinging gate drive shall move the gate by 90° in not more than 20 s.
- 6) The status detector mechanism shall indicate correctly whether the gate is open or closed.
- 7) The vehicle gate movement shall stop when the gate meets an obstruction, e.g. a vehicle, and an obstruction alarm signal shall be initiated.
- 8) Each vehicle gate shall incorporate a warning device such as lights or a siren, to indicate when the gate is in operation (opening or closing).

10.7.2.2 Pedestrian gates

- 1) The gate shall have a status detector mechanism to indicate correctly whether the gate is open or closed.
- 2) The control box shall have a locked cover that gives access to the electronic components. The operation of the gate shall be initiated by means of a PIN code, biometric reader, card reader or key switch attached to the control box.

10.7.3 Vehicle stoppers

- 1) A vehicle stopper shall comply with requirements of section 4.6 of SANS 2220-2-7.

11. Integration requirements

11.1 General

The IACS shall primarily cater for Eskom's integration requirements and shall form the basis to engage with all the disparate systems in the physical security environment.

The IACS (Integrated Access Control System) shall be the standard Physical Access Control System across Eskom with capabilities to integrate with but not limited to CCTV, Lifts, Canteen Management System, Transportation System, Building Management Systems and other security / business subsystems to provide a unified security management system.

Eskom aims to develop a detailed integration standard which will outline the integration requirements between all security technologies deployed as its sites. The IACS shall be adaptable to cater for future integration requirements that Eskom will stipulate and at minimum it shall be integratable with the following systems:

- 1) Intrusion Detection system
- 2) Electric Fence system
- 3) Intercom and Public Address systems
- 4) CCTV system
- 5) Security Lighting system
- 6) Guard Tour system
- 7) Fire Detection system

12. Buildings access control

- 1) All entry points into buildings shall be secured by the Access Control system.
- 2) Where viable, windows should be protected by burglar proofing, apart from areas where HV Regulations require otherwise.
- 3) All non-automated doors shall be fitted with a suitable grade security lock.
- 4) In the administration buildings all offices shall have security gates installed on the doors, a suitable key control system shall be introduced to manage access to offices and the safekeeping of duplicate keys.

13. Reporting

The Integrated Access Control System shall have Reporting capability. The system should have a set of standard off the shelf reports. The system must allow for custom development of reports. The business requirement is to build a set of custom reports that are specific to the Eskom environment and these reports should be a standard set of reports for any Eskom site nationally. Both standard and custom reports should have capability of being scheduled to run at specific dates and times and/or recurring. The system is required to contain functionality for reports to be e-mailed from within the application. The reports are required to have an export / save functionality for at least xls, csv, and pdf file formats.

13.1 Attendance Register

- 1) A field labelled "Flexible time" should be added to the report as this is currently contained in the manual attendance register form. Managers and staff often agree on Flexible time and the hours. This information is passed onto the HR department. A "yes / no" value should populate the Flexible Time field to indicate to a person looking at the report that the individual has an earlier / later start and end time due to the flexible time agreement.

- 2) A field labelled "Leave" must be added to the report as this is currently contained in the manual attendance register form. A "yes / no" value should populate the Leave field to indicate to a person looking at the report that the individual is not just absent from work but on Leave. This should integrate with SAP so leave is automatically filled in.
- 3) A field labelled "Leave Type" must be added to the report to enable Management viewing the report to understand whether a person is on their Annual leave or sick leave etc.

13.2 Visitor reports

- 1) Visitor reports should cater for the requirements in Table 4 below:

Table 4: Visitor reports requirements

Report Name	Description
Pre-registered visitors report	To provide a list of visitors that are / have been pre-registered
Visit History report	To provide a list of visitors that have visited a site or all sites in a specific period
Visitors per Host report	To show the visitors that a host has had over a specific period of time
Visits per Visitor report	To show a visitor and their visits to a / all Eskom sites
Visitor Details report	To display all the captured details of a visitor from registration / enrolment
Visitor Statistical report	<ol style="list-style-type: none"> To indicate the number of visitors and visits per building, area and use of parking facilities. To provide management Information database about the visits to the sites and visitor patterns To assist to optimise the visitor process by evaluating registration durations of previous visits, which can allow management to create a reference point and the effects of optimisation of the process can be determined.

13.2.1 Visitor/Host registration information

The system shall cater for information fields depicted in Table 5 and Table 6 below on information forms and databases to facilitate the ACS searches.

13.2.1.1 Pre-registration information

Table 5: Preregistration information/fields

Required Capability	Importance	Mandatory
Form Attributes	L/M/H	
Main Menu		
Search	H	
Pre-registered Visitors	H	
Previous Visitors	H	
Visitor Personal Info		
Visitor Last Name	H	X
Visitor First Name	H	X

ESKOM COPYRIGHT PROTECTED

**SPECIFICATION FOR INTEGRATED
ACCESS CONTROL SYSTEM (IACS) FOR
ESKOM SITES**
Unique Identifier: **240-102220945**Revision: **1**Page: **27 of 40**

Required Capability	Importance	Mandatory
Visitor Company	M	
Date of Birth	M	X
ID / Passport Number	H	X
Telephone Number	M	X
Cell / Mobile Number	H	X
E-Mail Address	M	
Date of Visit	H	X
Time of Visit	H	X
Vehicle Registration	H	X
Duration of visit	L	
Meeting Room	M	
Reason for Visit	M	X
Comments / Notes	M	
Visitor Host Details		
Name Search		
Advanced Search		
First Name	H	X
Last Name	H	X
Unique Number	H	X
Telephone Number	H	X
Cell / Mobile Number	H	X
E-Mail Address	L	
Office / Site / Location	H	
Host Advanced Search Options		
Visitor Last Name	H	
Visitor Name	L	
Unique Number	H	
Mobile Number	M	
Visitor Type Selection		
Employee / Contractor registering External Visitor	H	
Employee / Contractor visiting other site	H	

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

13.2.1.2 Registration (Check in/out) Fields

Table 6: Registration (Check in/out) Fields

Required Capability	Importance	Mandatory
Form Attributes	L/M/H	
Main Menu		
Search	H	
Pre-registered Visitors	H	
Previous Visitors	H	
Current Visitors	H	
Current Cards	M	
Visitor Personal Info		
Visitor Last Name	H	X
Visitor First Name	H	X
Visitor Company	M	
Date of Birth	M	X
ID / Passport Number	H	X
Telephone Number	M	X
Cell / Mobile Number	H	X
E-Mail Address	M	
Date of Visit	H	X
Time of Visit	H	X
Vehicle Registration	H	X
Duration of visit	L	
Meeting Room	M	
Reason for Visit	M	X
Comments / Notes	M	
Capture / Import Photograph	H	
Visitor Host Details		
Name Search		
Advanced Search		
First Name	H	X
Last Name	H	X
Unique Number	H	X
Telephone Number	H	X
Cell / Mobile Number	H	X

ESKOM COPYRIGHT PROTECTED

Required Capability	Importance	Mandatory
E-Mail Address	L	
Type of Employee	H	
Office / Site / Location	H	
Host Advanced Search		
Visitor Last Name	H	
Visitor Name	L	
Unique Number	H	
Mobile Number	M	
Card Details		
Card Number	H	
Commence Date and Time	H	
Expiry Date and Time	H	
Host Card Number	H	
Visit Menu		
Start Visit	H	
Place Visit On Hold (Suspend)	H	
End Visit	H	
Delete Visit	H	

13.3 Additional Reports

The Business requires report(s) to provide information regarding volumes. E.g. Number of people that have been through the visitor gate in a specific time period. Business would be able to understand the number of employees, contractors and visitors by using filters on this report. The value is that business would be able to understand the high traffic areas and which hardware / equipment is working more often and may need servicing or inspection more often.

The business requirement is for an Access Denied Report to be created. This must show the number of "Access Denied" attempts in a specific time period. It should also list each individual that has been denied access in the report. This will enable the business to conduct more training if necessary as the information would be indicative of how many people are possibly having problems at biometric fingerprint readers.

An Alarms Report must be created so that management as well as operations have a clear view of the number of alarms that have been reported on the system. The Alarms report must also show the number of alarms that have been acknowledged and those that are not acknowledged. The report should break down alarms into the various levels of alarms that have been already defined e.g. High and Low priority.

13.4 Graphical User Interface Requirements

13.4.1 Functional GUI Requirements

- 1) The GUI must implement a role-based access and privilege model so that classes of users can be given access to functions appropriate to their assigned organisational responsibilities.
- 2) The GUI should primarily contain floor plan views per site. Alarms page / window should form part of screen to allow the user both graphical and data alarms to select from.
- 3) The GUI must cater for utilising photos as the background where icons can be mapped onto it. E.g. a picture of a zone with icons of readers and controllers mapped over the picture.
- 4) The GUI must cater for importing drawing files of various types such as CAD files.
- 5) The GUI must cater for multiple floor levels – as required for buildings with more than a single floor.
- 6) The GUI should have the capability to display more than 1 screen (floor plan) at a time (split screens).
- 7) The GUI must cater for 3 dimensional models and views with related controls to navigate through the model. This requirement should be based on the site type and criticality.
- 8) The GUI must include a zoom function which allows for both zoom in and zoom out on floor plan views and 3 dimensional views.
- 9) The GUI must allow for colours to be configurable for the layouts. E.g. Floor plan line colours can be green against a black background.
- 10) The system must cater for integration of various modules into this GUI. Readers, controllers, access points, cameras, intrusion detection system and other security and BMS related hardware devices must be mapped/displayed on the GUI. The user should be able to select from a drop down list of various components to get a dynamic view of the same. E.g. if “Readers” were selected then the floor plan should only display the readers on that floor
- 11) All icons mapped on the GUI must be linked with the actual hardware devices installed in the field/building/site. The linking of this must include details such as the state of the device, the alarm state if any and last person that has accessed that point if it is a reader. There must be capability of using a pop-up screen to view this status.
- 12) The level of detail should be at a door level, i.e. the operator does not have to have a view of the server, and converter connected to the door. The alarm should bring up details of what the hardware /tamper alert is.
- 13) The GUI should contain different icon types/styles for different equipment e.g. camera, reader, controller.
- 14) The GUI must have colour coding for hardware items depicted, i.e. use colour coding to indicate the status of hardware items.
- 15) Alarms must be 3 colours:
 - a) Red for high priority
 - b) Yellow for medium priority
 - c) Blue for low priority
- 16) The GUI must display all access points that are open e.g. doors, turnstiles especially in the case of an evacuation. A separate colour code should be used for this. Text should be displayed as well indicating emergency.
- 17) A flashing GUI icon should be used when a hardware failure occurs or an alarm is triggered at any specific point. The flashing should not stop until the alarm / failure has been acknowledged / opened.

- 18) A hardware failure or alarm should have an audible alarm sound together with the flashing icon. The alarm sound should increase automatically after every 2 minutes that the alarm has not been acknowledged / opened. This must be configurable to use for only certain alarm types / levels e.g. High Priority alarms
- 19) The GUI should have a configurable threshold of the number of unacknowledged alarms and an automatic escalation via the e-mail / SMS gateway.
- 20) The GUI should have manual and automated methods of SMS and emailing alarms, especially for high priority alarms.
- 21) The GUI must allow for clicking on the icons (cameras, readers, controllers, power supply etc.) that have been mapped on the interface. The system must then respond by opening details of the linked camera/reader/controller/power supply etc. The icon focus must return back to its original point on the map after closing this details screen.
- 22) Access to live and recorded camera footages must be possible from the camera links on the GUI.
- 23) The GUI should have an emergency contact list that the operators can quickly access in order to attend to an alarm.
- 24) On acknowledging/opening an alarm the GUI should display procedures to attending to the alarm. For each alarm type these may differ as there are different threat levels in the business and therefore should be configurable per alarm type.
- 25) The GUI should have the ability to capture sticky notes / comments to alarms and escalations.
- 26) The GUI should have both touch screen and keyboard/mouse/joystick device input/control.
- 27) Must show different zones and the number of people in each zone should be listed in the zone.

13.4.2 Additional GUI alarm requirements

- 1) Alarms should be displayed in real-time with the icons.
- 2) Linked readers/controllers/power supplies etc. must open within 100 milliseconds requesting it to open.
- 3) Cameras should open in 100 milliseconds on a local site at 15 frames per second speed.
- 4) It must cope with high volume of alarms and events between 8am-5pm, Mondays – Fridays.
- 5) 500 unacknowledged alarms must result in an escalation to the Security Manager.

13.5 Databases

13.5.1 General database requirements

- 1) Database shall provide for regular reports and specific database queries, these should be viewable both locally (onsite) and also retrievable remotely from security control centre(s).
- 2) Copies of reports from the database shall be kept for at least three years or as long as required for legal proceedings.
- 3) The system shall allow for Logbook entries with the following as minimum features:
 - a) Alarm logbook for alarmed events generated by the system or peripheral devices
 - b) System logbook for all actions performed on the system
 - c) Event logbook for all events generated by the peripheral devices or by programs that are started up automatically in the background
 - d) Access logbook from all the readers
 - e) Time logbook for all time management related readings received from all the readers

- f) Trend logbooks
 - g) Error logbook which is used for system errors as well for unauthorized access requests
 - h) Visitor logbook
 - i) Video logbook
- 4) Database reports shall provide for the following functions:
- a) Time and Attendance
 - b) Personnel tracking (Individual's historical movements to and from the various access points)
 - c) Date and time movements of Individuals or groups through the system

13.5.2 Database structure

- 1) The database shall allow for the following information to be included:
- a) Eskom employee number (unique number)
 - b) Access ID (this shall be generated automatically by the system)
 - c) Full names and surnames
 - d) ID Number
 - e) Selection of access levels whereby the level where access is required is selected at the registration facility
- 2) The employee status shall be either of the following:
- a) Eskom employee
 - b) Sub-contractor
 - c) Visitor
 - d) Contractor
 - e) Security services
 - f) Vendor (to be used for regular visitor)

14. Alarms

- 1) The system alarms shall comply with Specification for Integrated security Alarm system for protection of Eskom installations and its subsidiaries (240-86738968).
- 2) Where access control and alarm monitoring are carried out on the same central display screen, the central display screen shall:
- a) Serve as a logged message output device and an operator's screen;
 - b) Be capable of being used as an alarm display terminal;
 - c) Be able to view the alarm display and other displays concurrently ; and
 - d) While the screen is being used by the operator for card or system programming, allow logging to occur.
- 3) Error messages shall cause a beep tone to be sounded. The message shall stand until the error is acknowledged by the operator. All events printed on the printer shall include the time of the event to the nearest second, and details of the event.

- 4) System shall have the following alarms capabilities:
 - a) Alarm handling screen
 - b) Graphics associated with alarms
 - c) Alarm classification
 - d) Report back facility why the alarm occurred
 - e) Logging of all transactions in the alarm logbook

15. Power supply

- 1) The power unit of an access control system shall comply with the requirements of SANS 2220-1-7.
- 2) All backup supplies shall comply with 240-53114248, Thyristor and switch mode chargers, AC/DC to DC/AC converters and inverter/uninterruptable power supplies standard.
- 3) The batteries used shall comply with the following standards:
 - a) 240-56360034, Stationary Vented Lead Acid Standard
 - b) 240-56360086, Stationary Vented Nickel Cadmium Batteries Standard
 - c) 240-51999453, Specification for Valve Regulated Lead Acid Cells
- 4) There shall be an intelligent power supply that monitors incoming power, battery status and only supply power to the servers.
- 5) There shall be a backup battery that ensures at least 24 hours autonomy.
- 6) The system shall still operate in the event of a main power failure.
- 7) Each system or subsystem shall have a dedicated circuit breaker and supply circuit.
- 8) There shall be UPS with sufficient capacity to support all ACS equipment for a minimum of 8 hours.
- 9) Electro-magnetic radiation from the UPS shall not affect the operation of other electronic equipment in the equipment room
- 10) The battery system shall be maintenance free with a 5 year guarantee.

16. Cabling requirements

- 1) Cables shall comply with the requirements of Eskom's Standard for Wiring and Cable marking in Substations (240-64636794).
- 2) Terminal blocks shall be in accordance with Eskom standard 240-70413291, Specification for Electrical Terminal Blocks.
- 3) All wiring shall be concealed inside trunking or conduit. No exposed wiring will be accepted except at sites where suitable cable trays are installed.
- 4) Cabling in roof or floor voids shall be installed in cable trays. Where cable trays are not available or viable, conduit will be acceptable.
- 5) Cabling in trays shall be tied off at a maximum of 1.5m interval.
- 6) Data and low voltage (0-48V DC/AC) cable installations shall be separated from mains power installations by a minimum of 500mm.
- 7) Where data and low voltage cabling has to cross power cabling, this shall always be at 90° angles.
- 8) Cabling in manholes shall be kept above the manhole floor level to avoid water contact.
- 9) Cable shall be handled with care and not pulled with excessive force that may cause internal damage.

- 10) The installer must adhere to the drawings and specifications at all times. Where a discrepancy exists between a drawing and these specifications, the higher of the two standards is to be followed.
- 11) The installation contractor shall provide detailed as built drawings indicating cable routes, installation locations and unique equipment identifiers on completion of each logical section of an installation.
- 12) Cables are not to be bent at a radius of less than four times the diameter of the cable or tighter than specified by the manufacturer.
- 13) There shall be no cables running next to devices that may cause electro-magnetic interference.
- 14) Tensioning of cables shall not exceed 10kg.
- 15) Correct wiring schematic shall be followed.
- 16) All wiring shall be terminated with bootlace ferrules of the appropriate size and colour to match the cable.
- 17) All bootlace ferrules shall be properly crimped and shall have good mechanical and electrical connection.
- 18) A dedicated ferrule crimper when crimping bootlace ferrules shall be used. The use of side-cutters, pliers or other tools for crimping is not acceptable.
- 19) No short circuits shall be caused when cutting cables.
- 20) Where cables are laid in trenches, they shall be armoured.
- 21) Cable trenches shall be excavated according to the Standard Technical Specification. Trenches shall be 600 mm deep measured from average ground level to the top of the upper sleeve or cable. Contractors shall allow for the excavation, bedding, laying of cables and sleeves and graded back-filling of all trenches as specified.
- 22) Where any power reticulation work has been undertaken, contractors shall make provision to submit an approved reticulation certificate issued by an authorised electrical Contractor.
- 23) With respect to site cabling, no cable joints shall be accepted between buildings and control room. In the event that the distance exceeds the length of a standard cable drum, the Project Manager's ruling shall be obtained. The Project Manager will then determine where the cable may be joined and which jointing materials would be acceptable. The Contractor shall indicate the positions of all joints on the final as-built Drawings.

17. Physical requirements

17.1 Tamper protection

- 1) Tamper protection for the electrical components of the IACS shall be in accordance with section 4.10 of SANS 2220-2-1 such that the following shall not be possible:
 - a) To alter the enclosure arrangement without causing an alarm signal to be generated;
 - b) To gain access to the electrical circuits, adjustment controls and temper protection devices without the tamper protection device causing the component to generate an alarm signal.
 - c) To disable the tamper protection device by means of normally available tools such as knives, pliers and screw drivers.

Compliance is checked in accordance with section 6 of SANS 2220-2-2: *tamper protection test*

17.2 Ingress protection

The enclosures for the electrical and electronic circuits shall, unless otherwise specified, provide protection of class IP65 in accordance with SANS 60529.

ESKOM COPYRIGHT PROTECTED

17.3 Safety

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

18. Environmental requirements

18.1 General

- 1) Access cards shall comply with environmental requirements of 4.2 of SANS 2220-2-6.
- 2) Biometric readers shall comply with environmental requirements of 4.2 of SANS 2220-2-5.
- 3) Servers/central processors shall comply with environmental requirements of 4.2 of SANS 2220-2-2.
- 4) Card readers shall comply with environmental requirements of 4.2 of SANS 2220-2-3.
- 5) Barriers shall comply with environmental requirements of 4.8 of SANS 2220-2-7.

18.2 Operating conditions

- 1) All the elements of the IACS shall be able to function within the conditions below, without the performance being out of limits or the life cycle being shortened:
 - a) Ambient temperature : -10 to +°55C
 - b) Altitude: 0 to 2500 meters
 - c) Relative humidity: Up to 100% outdoors, 5 to 95% indoors
- 2) The system and associated equipment shall be protected against dust and any other coastal condition such as corrosion.
- 3) Mechanical shock and vibration shall not affect the functioning of the system and associated equipment for its life cycle.
- 4) Protection shall be provided for short or long term over voltages or under voltages, impulses, transients, spikes, surges, brownouts, mains borne interference's or power failures and the equipment shall be suitable for continuous and reliable operation under these circumstances.
- 5) The equipment shall not generate any interference, which could hinder its own performance or the performance of the other equipment in its vicinity.
- 6) All servers shall be installed in purpose built cabinets, they should not be placed in non-dedicated cupboards or floor.

18.3 EMC requirements

- 1) Signal, voltage and electromagnetic radiation levels in readily accessible areas shall not be dangerous.
- 2) System and its components shall comply with requirements of SANS 61000-1-2.

18.4 Earthing

- 1) The Earthing of the system shall comply with Eskom's earthing standards below:
 - a) 240 – 56872313 – Radio Station Earthing and Bonding.
 - b) 240 – 56356396 – Earthing and Lightning Protection Standard.
 - c) TST41-877 - Transmission Substation Design Earthing Standard.

19. Labelling and numbering

- 1) Terminal boxes and terminals shall be numbered and labelled accordingly in line with the approved labelling standards specific to area of applicability.
- 2) Numbering and labelling of system components shall be executed in such a way that it can be guaranteed that a maintenance artisan can trace wiring (cores) with the as-built information only.
- 3) Labelling at power stations, excluding nuclear power stations shall comply with requirements of Plant Labelling and Equipment Description Standard (240-71432150).
- 4) Labelling at Transmission sites shall comply with requirements of Standard for Labelling of Secondary Plant Equipment (240-62362652).

20. Markings

- 1) Markings for access cards shall comply with section 5 of SANS 2220-2-6.
- 2) Markings for biometric readers shall comply with section 5 of SANS 2220-2-5.
- 3) Markings for servers/central processors shall comply with section 5 of SANS 2220-2-2.
- 4) Markings for card readers shall comply with section 5 of SANS 2220-2-3.
- 5) Markings for barriers shall comply with section 5 of SANS 2220-2-7.

21. Inspections and methods of tests

- 1) Inspections and methods of test for servers/central processors shall comply with section 6 of SANS 2220-2-2.
- 2) Card reader inspections and methods of tests shall comply with section 6 of SANS 2220-2-3.
- 3) Inspection and tests methods for biometric readers shall comply with section 6 of SANS 2220-2-5.
- 4) Inspection and methods of tests for reader controllers shall comply with section 6 of SANS 2220-2-4.
- 5) Inspections and methods of tests for access cards shall comply with section 6 of SANS 2220-2-6.
- 6) Inspections and methods of tests for barriers shall comply with section 6 of SANS 2220-2-7.

22. Miscellaneous requirements

22.1 Spares

- 1) **Costs:** The contractor shall provide a priced spares breakdown for each item of equipment. The level of breakdown shall be compatible with the maintenance policy of field replacement of faulty subunits or modules.
- 2) **Licensing:** The supplier shall indicate explicitly any licence conditions for associated software, what the duration of the licence is, and whether periodic payments would have to be made.
- 3) **Recommended list of spares:** The supplier shall provide a recommended list of spares that Eskom should hold. The quantity of such spares will be a function of the installed base and MFBF figures. The supplier shall furnish Eskom with the MTBF figures for items on the list of spares.
- 4) There shall be provision for direct replacement spares to be obtained from the manufactures.
- 5) There shall be a formal OEM support and agent agreement letter provided by the supplier for local availability of spares and repair services.
- 6) There shall be a provision for Eskom to Establish contracts with external companies to facilitate the repairs of faulty equipment.

- 7) There shall be a provision to keep portable (non-strategic) spares in strategic stores and dispatched when required.
- 8) There shall be provision to keep critical spares at minimum levels as identified by the custodians in the critical spares stores.
- 9) For emergency replacements where it could be difficult to wait for the spares to be dispatched, there shall be a provision to keep the spares at local stores.
- 10) There shall be provision to channel the spares from grids and other stake holders via an identified stores custodian who will exchange the faulty spare for the working one and send the faulty one for repairs at the expense of the grid/customer for replenishment purposes.
- 11) Lead time to replace a spare shall be a day, at maximum.
- 12) Suppliers shall notify Eskom before they discontinue or modify any part of the system to allow procurement arrangements for the installed spares base.

22.2 Tools and test equipment

- 1) Cost of test equipment: The supplier shall provide a price list of the test equipment that is considered necessary to perform on-site maintenance and fault-finding on all offered equipment. Test sets that are proprietary to the manufacturer shall only be recommended where commercial general-purpose test equipment cannot be employed, or where its use would be uneconomic.
- 2) Cost of tools, etc.: The contractor shall supply a price list of the special tools, connector cords, outriggers, card extenders, etc. that are considered necessary to perform on-site maintenance and fault-finding on all offered equipment.

22.3 Training

- 1) Courses: Training courses for Eskom technicians shall be provided in the Republic of South Africa. Such courses will be separately ordered from time to time as needs dictate.
- 2) Course structure: Courses shall be structured on a modular basis by individual equipment, such that a series of modules may be run consecutively to meet the needs of a particular group of trainees. The modules shall cover the operation of the equipment to block diagram level, testing, commissioning, and fault-finding to field-removable module level. Management system software training is also required.
- 3) Course training venues: Unless the training needs to be provided in a specialized facility in South Africa, it is desirable that courses be conducted at various Eskom centres around the country where both classrooms and student accommodation exist.

22.4 Warranty

- 1) Duration: Suppliers shall state the warranty period on all offered equipment and the terms thereof.
- 2) Fault investigations: It will not be practical to require the contractor to attend to every on-site fault. It is a requirement, therefore, that the supplier accepts that on-site fault investigation shall be carried out by Eskom technicians with the warranty remaining intact. Only in the event of obscure faults will the supplier be required to send staff to site. Removed units, subunits or modules will be returned to the contractor for repair or replacement under the terms of the Warranty. Technicians working on the equipment shall undergo the supplier provided training in terms of 22.3 of this specification.
- 3) Limitations: The supplier shall indicate explicitly whether the equipment is limited in any way by licences and/or software maintenance agreements. In addition, the supplier shall include in the price the cost of all features, capabilities and capacities (i.e. will one have to pay for extra licences when either scaling up the deployment, or to get full functionality).

- 4) Support: The supplier shall indicate available options and costs for maintenances, upgrades, etc. of the offered equipment. In addition, the supplier shall furnish Eskom with technology roadmaps for the offered equipment. The supplier shall have a technology migration plan that will allow the system to evolve with technology developments and the new technology should still be integratable with the legacy equipment.

22.5 Repairs

- 1) Repair service: The supplier shall provide a repair service for faulty units, subunits and modules removed from site by Eskom technicians. This service shall form part of the support service called for in 22.6. The period for which this service will run after equipment manufacture discontinuation date will be specified, in line with 22.6.
- 2) Turnaround times: Within the contracted repair turnaround time, the supplier shall return to Eskom either the repaired item or a replacement thereof. In the case of a repaired item, a brief report, detailing the work carried out and components replaced, shall be included with the item. Historical records of repairs to units shall be maintained.
- 3) Warranties: Repaired items shall be warranted against a repetition of the same fault for a period of three months from the date of return.

22.6 Support contract requirements

- 1) Repairs: The contractor shall provide unlimited repairs to Eskom's spares holding by providing a repair and return service on any of the offered equipment.
- 2) Guarantees: The contractor shall provide the repair and return service on equipment that has gone faulty and is outside of the warranty period on an **as and when** required basis.
- 3) Turnaround time: The turnaround time for the repair and return service shall be thirty (30) calendar days.
- 4) On-site support: The contractor shall provide a minimum of 20 h per month on-site support.
- 5) Standby service: The contractor shall provide a 24 h standby service.
- 6) Down-line support: The contractor shall provide a technical assistance and support service for second and third line maintenance locally.
- 7) Ongoing software support: The contractor shall provide software updates, patches and/or firmware when they become available.
- 8) On-the-job training: The contractor must first apply the updates on one system element in conjunction with a representative of Eskom. Thereafter, Eskom may either choose to apply the updates or may ask the contractor to effect the updates in the rest of the system elements.
- 9) Troubleshooting meetings: Formal meetings where technical problems can be documented and be driven to conclusion shall be held as and when required.
- 10) After-sales support: The contractor, when requested, shall provide an installation and commissioning service on an additional time and material basis where required.

23. Authorization

This document has been seen and accepted by:

Name	Designation	<u>Email</u> address
Tebogo Rakau	Divisional Executive: Security Division	RakauJT@eskom.co.za
Danie Odendaal	Engineering SGM (acting)	OdendaDP@eskom.co.za
Prince Moyo	Power Delivery Engineering GM	MoyoP@eskom.co.za

ESKOM COPYRIGHT PROTECTED

Name	Designation	Email address
Tebogo Rakau	Divisional Executive: Security Division	RakauJT@eskom.co.za
Richard McCurrach	Senior Manager – PTM&C CoE	McCurrR@eskom.co.za
Amelia Mtshali	Metering, DC & Security Technologies Manager – PTM&C CoE	Amelia.mtshali@eskom.co.za
Karen Pillay	Manager – (Security Design, Advisory and Projects)	PillayK@eskom.co.za
Yashil Narandas	Middle Manager - Group IT – Project Delivery	NarandY@eskom.co.za
Prudence Madiba	Senior Manager Electrical and C&I Engineering	MadibaRP@eskom.co.za
Lungile Malaza	Middle Manager – Electrical Plant COE	MalazaLP@eskom.co.za
Marius van Rensburg	Senior Manager – Transmission	vRensbMa@eskom.co.za
Paul Grobler	Chief Engineer – Transmission	GroblePP@eskom.co.za
Sikelela Mkhabela	Senior Manager – Distribution	MkhabeS@eskom.co.za
Ashwin Pillay	Senior Manager – PTM	PillayAS@eskom.co.za
Alison Maseko	Senior Manager – Transmission	MasekoAN@eskom.co.za
Cornelius Visagie	Chief Technologist – Group Technology – PEIC C&I	VisagiCJ@eskom.co.za

24. Revisions

Date	Rev	Compiler	Remarks
Sept 2016	1	R Moshoeshoe	First issue

25. Development team

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

- Donald Moshoeshoe
- Thomas Jacobs
- Sandi Ndamase
- Jorge Nunes
- George Jordaan
- Ben Janse Van Nieuwenhuizen
- Trevor Pope
- Sally Levesque
- Zwelandile Mbebe
- Justice Ramanyoga
- Koos Pretorius
- Matthew Taljaard

ESKOM COPYRIGHT PROTECTED

- Paul Grobler
- Leon Drotsche
- Anton Naude
- Zameka Qabaka
- Alan Jones

26. Acknowledgements

- Group security
- Security Care Group