Eskom	Standard	Technology

Title: **SPECIFICATION FOR CCTV SURVEILLANCE WITH INTRUDER DETECTION**

Unique Identifier:	**240-91190304**
Alternative Reference Number:	**34-1613, DISSCABM6**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**2**
Total Pages:	**115**
Next Review Date:	**March 2026**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Albert Hendriks	**Prince Moyo**	**Dr. Titus Mathe**
Engineer	**General Manager: Transmission Engineering**	**General Manager: Group Technology**
Date: 09/02/2021	Date: 23 February 2021	Date: 2021-03-09

Supported by SCOT/SC

Richard McCurrach

PTM&C TC Chairperson

Date: 10 Feb 2021

PCM Reference: **<xxxxxx>**

SCOT Study Committee Number/Name: **Security Technology**

Content

Page

1. Introduction 6
2. Supporting clauses 6
   - 2.1 Scope 6
     - 2.1.1 Purpose 6
     - 2.1.2 Applicability 6
   - 2.2 Normative / Informative references 6
     - 2.2.1 Normative 6
     - 2.2.2 Informative 7
   - 2.3 Definitions 7
     - 2.3.1 General 7
     - 2.3.2 Disclosure classification 8
   - 2.4 Abbreviations 8
   - 2.5 Roles and responsibilities 9
   - 2.6 Process for monitoring 9
   - 2.7 Related/supporting documents 9
3. Requirements 9
   - 3.1 Objective 9
   - 3.2 Protection of Information 9
   - 3.3 Note on Product Choice 10
   - 3.4 CCTV System Overview 10
   - 3.5 Design and Installation Process Overview 10
     - 3.5.1 Site Specific Requirement Specification 12
     - 3.5.2 Design and Tender 13
     - 3.5.3 Tender Technical Evaluation 15
     - 3.5.4 Factory Acceptance Test 16
     - 3.5.5 Installation of System 17
     - 3.5.6 Commissioning of System 17
     - 3.5.7 Documentation 17
   - 3.6 Installation 18
   - 3.7 System Level 19
     - 3.7.1 System Overview 19
     - 3.7.2 Operation - Unauthorised Access 21
     - 3.7.3 Warrantee and Certification 22
     - 3.7.4 General Physical Requirements 22
     - 3.7.5 General Electrical Requirements 23
     - 3.7.6 Cable routes in control plant / equipment rooms: 24
     - 3.7.7 Outdoor Cables and Trenching in Substations 24
     - 3.7.8 Security Cabinet 25
     - 3.7.9 Backup Power Supply 26
     - 3.7.10 Communication 28
     - 3.7.11 PA System 29
     - 3.7.12 Time Synchronisation 29
   - 3.8 Intruder Detection System 30
     - 3.8.1 Indoor Detection 30
     - 3.8.2 Alarm System Operation 30

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.

3.8.3 Lighting Integration 31
3.9 Yard 31
3.9.1 Overview 31
3.9.2 Perimeter Camera System Layout 32
3.9.3 Perimeter Detection System 34
3.9.4 Yard Installation 35
3.10 CCTV Surveillance System 37
3.10.1 Camera Purpose 37
3.10.2 General Camera Requirements 39
3.10.3 General Requirements for Outdoor Cameras 41
3.10.4 Fixed Thermal perimeter cameras 42
3.10.5 Fixed perimeter cameras – non thermal 43
3.10.6 PTZ camera 43
3.10.7 Indoor Cameras 45
3.10.8 Digital Video Recorder / Network Video Recorder 46
3.11 Video Management System (VMS) 49
3.11.1 Introduction 49
3.11.2 Location and Architecture 49
3.11.3 Network and Connections 50
3.11.4 Features 51
3.11.5 Network Security 51
3.11.6 Video Recording and Streaming 52
3.11.7 Event Management 53
3.11.8 Usability 53
3.11.9 Hardware 54
3.11.10 Training and Support 54
3.12 Security Control Room 54
3.12.1 Security Control Room Operators 54
3.12.2 Records 55
3.13 Legal and Evidentiary Aspects 55
3.13.1 Overview 55
3.13.2 Application 56
3.13.3 Rules applicable to digital images 56
3.13.4 Procedures when handling evidence 57
3.13.5 Physical handling of Storage Media 57
3.13.6 Information for Eskom 58
3.13.7 Period for which day-to-day data shall be preserved 58
3.13.8 General evidentiary requirements 58
3.13.9 Pro-Forma Statements 59
3.14 Operation 59
3.14.1 Standard Operating Procedure 59
3.14.2 Continuous Improvement 59
3.15 Maintenance 60
3.15.1 Introduction – Maintenance Contracts 60
3.15.2 VMS System Maintenance 61
3.15.3 Ad hoc Maintenance (Faults) 61
3.16 Testing 61
3.16.1 Introduction 61
3.16.2 Tender Demonstration Tests 62

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.

3.16.3 Factory Acceptance Tests 63
3.16.4 Site Acceptance Tests 64
3.16.5 Alarm System Tests 65
3.16.6 PA System Tests 66
3.16.7 Floodlight Tests 66
3.16.8 Intruder Detection Tests 67
3.16.9 Yard Intruder Detection Tests 67
3.16.10 Indoor Intruder Detection Tests 67
3.16.11 Site Intruder Detection Soak Tests 68
3.16.12 Camera Functional Tests 68
3.16.13 PTZ Camera 71
3.16.14 DVR Acceptance Tests 72
3.16.15 VMS Acceptance Tests 74
4. Authorization 74
5. Revisions 75
6. Development team 75
7. Acknowledgements 75
Annex A – Discussion of video analytics 76
Annex B – Typical maintenance check list 77
Annex C – System Performance 79
Annex D – Introduction to Rotakin Test Target 80
Annex E – Affidavit 81
Annex F – Functional Acceptance Test Sheets 82

Figures

Figure 1: Design and Installation Process (pg1) 11
Figure 2: Design and Installation Process (pg2) 12
Figure 3: Example of Camera Placement, FOV and Purpose 15
Figure 4: Functional Block Diagram of CCTV System 20
Figure 5: Unauthorised Access Flow of Information [20] 22
Figure 6: Cable Trench Layout 24
Figure 7: Example of Poorly Organised Security Equipment Cabinet 25
Figure 8: Example of Well Organised Security Equipment Cabinet 25
Figure 9: Preferred Power Distribution, Using Backup Power from the Site 27
Figure 10: Incorrectly Distributed Option 2 Power, Battery Downstream from UPS 28
Figure 11: Correctly Distributed Option 2 Power, Battery Parallel to UPS 28
Figure 12: Examples of Various Layouts of Perimeter Cameras 33
Figure 13: General Layout of Perimeter Camera System bundled with Intelligent Video Analytics for Detection - creates an 'invisible wall' with no gaps 34
Figure 14: Exposed soil due to poor workmanship 36
Figure 15: Camera and Metal Enclosure Mounted on Concrete Pole 36

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.

Figure 16: Illustration of CCTV categorisation based on screen height [25] 38
Figure 17: Indoor camera inside room....46
Figure 18: VMS Network Architecture 50
Figure 19: Design and Tender Phases....62
Figure 20: Comparative Effectiveness of Backlight Compensation of Different Cameras [27] 63
Figure 21: Factory Acceptance Phase 63
Figure 22: Site Acceptance Phase 64
Figure 23: Example of Measured Horizontal Field of View of a Camera 69
Figure 24: Example of Measured Vertical Field of View of a Camera....69
Figure 25: Example of Camera Report: Note that only the Recognition Column has been completed 70
Figure 26: Example of measured Field of View of PTZ Pre-set Positions 72
Figure D.1: Rotakin Test Target 80

Tables

Table 1: CCTV categories 37
Table 2: Relative Size of Person on Screen....37
Table 3: Example of Camera Purpose and Conditions at a Specific Site 39
Table 4: Minimum Manufacturer Specifications for Cameras....40
Table 5: Additional Minimum Manufacturer Specifications for Outdoor Cameras....42
Table 6: Additional Minimum Manufacturer Specifications for Thermal Cameras 42
Table 7: Additional Minimum Manufacturer Specifications – Fixed Perimeter Cameras 43
Table 8: Additional Minimum Manufacturer Specifications for PTZ Cameras....45
Table 9: Additional Minimum Manufacturer Specifications for Indoor Cameras 46

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. Introduction

This specification sets out the physical, technical, functional requirements for integrated CCTV surveillance used at Eskom facilities. This document is intended for Operating Units, Engineering, Protective Services and Risk Management. The document includes testing and maintenance procedures.

2. Supporting clauses

2.1 Scope

This specification focusses on the application of CCTV at substations. The principles outlined here can also be implemented at Eskom offices, telecommunication sites and power stations. It should shall be applied when designing and evaluating CCTV security systems for substations, for Eskom facilities.

This document does not apply to cameras used for non-security purposes such as fire detection and operating. However many of the principles of design, testing and commissioning apply to CCTV in general and could be used to inform the design or specification of non-security CCTV systems.

2.1.1 Purpose

This specification sets out Eskom's physical, technical and functional requirements for CCTV surveillance used in Eskom.

2.1.2 Applicability

This document shall apply throughout Eskom Holdings Limited Divisions. This document is intended for Operating Units, Project Engineering, Protective Services and Risk Management.

2.2 Normative / Informative references

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

2.2.1 Normative

[1] ISO 9001, Quality Management Systems.

[2] 34-304, Generic Substation Design

[3] 240-86738968 - Standard for Security Alarm Systems for Protection of Eskom Installations and its Subsidiaries

[4] IEC 60255-1, Measuring relays and protection equipment – Part 1: Common requirements

[5] IEC 60721-3-3, Classification of groups of environmental parameters and their severities – Stationary use at weather protected locations

[6] SANS 10222-5-2, Electrical security installations Part 5-2: CCTV installations – Application guidelines.

[7] 240-55410927, Cyber security standard for Operational Technology

[8] 240-55683502 Definition of operational technology (OT) and OT / IT collaboration accountabilities

[9] 34-1430,Procedure for first line maintenance of Security systems at substations

[10] 240-44175038,Control of Non-Conforming Product or Service Procedure

[11] 34-1617 Specification for Infrared Detectors Used at Distribution Substations

[12] IEC 60721-3-3 Classification of groups of environmental parameters and their severities – Stationary use at weather protected locations

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] DISPVADR2 REV0: 2007, Procedure for first line maintenance of security systems at substations.

[14] 240-44175038, Control of Non-Conforming Product or Service Procedure

[15] 240-79537982, Security Threat and Risk Assessments

[16] SANS 10222-5-1-1, Part 5-1-1: CCTV installations — CCTV surveillance systems for use in security applications — Operational requirements

[17] 240-64636794, Standard for Wiring and Cable Marking in Substations

[18] 240-70413291, Specification for Electrical Terminal Blocks

[19] D-DT-0011, Pole, Spun Conc Str/Light Assem 5.7m

[20] D-DT0012, Pole, Spun Conc Str/Light Assem 7.2m

[21] D-DT-0332, LV and MV Foundation Pole Arrangement

[22] 240-79669677: Demilitarised Zone (DMZ) Designs For Operational Technology

[23] 240-55863502: Definition of OT and OT/IT Collaboration Accountabilities

[24] IEEE 1613-2009: IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations

2.2.2 Informative

[25] CCTV Operational Requirements Manual, UK Home Office, N Cohen, J Gattuso & K MacLennan-Brown

[26] Usability 101: Introduction to Usability, http://www.nngroup.com/articles/usability-101-introduction-to-usability/ (accessed 2015/02/21), J Nielsen

[27] Panasonic iPro 6 Series: Full Review, http://www.securityelectronicsandnetworks.com/articles/2014/04/30/panasonic-ipro-6-series-full-review, (accessed 2015/02/25)

[28] DISPAVACE8, The Management of Electronic And Physical Protection Measures

2.3 Definitions

2.3.1 General

Definition	Description
Balun	An electrical device that converts between a balanced signal and an unbalanced signal. Used in the CCTV industry to transmit analogue signals over UTP cable instead of coaxial cable.
CCTV camera	The unit that contains an imaging device that produces a video signal from an optical image.
CCTV control unit	The equipment used to control and monitor the operational functions of a CCTV system.
CCTV equipment	The unit that contains a CCTV camera, lens and ancillary equipment.
CCTV surveillance system	A system that consists of camera equipment as well as any monitoring and associated equipment for transmission and controlling purposes that is necessary for surveillance of a defined security zone.
Charged coupling device	A charge-coupled device (CCD) is a light-sensitive integrated circuit that stores and displays the data for an image in such a way that each pixel (picture element) in the image is converted into an electrical charge, the intensity of which is related to a colour in the colour spectrum

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
CS Mount	The configuration used to mount lenses.
Customer Network Centre (CNC)	Eskom field office typically consisting of offices, warehousing, workshops and outdoor storage areas.
Digital Video Recorder (DVR)	Device with the primary function of recording video footage from CCTV cameras. May also include a number of other features. For simplicity this document uses the term 'DVR' to refer to a DVR or NVR since both devices perform the same function.
Microbolometer	An uncooled thermal sensor used as a detector in thermal cameras.
Network Video Recorder (NVR)	A Digital Video Recorder which is connected to a network rather than directly to cameras. For simplicity this document uses the term 'DVR' to refer to a DVR or NVR since both devices perform the same function.
Nuisance Alarm	Alarm generated when a detection system triggers for something other than an intruder (e.g. a bird sets off an alarm). Note: The term 'nuisance alarm' is used rather than the more common 'false alarm'. This is because 'false' implies that the sensor is broken whereas 'nuisance' indicates that the sensor did detect something (e.g. a bird), but not the thing that it is installed to detect (human intruder).
Operational Technology (OT)	OT is the technology that is used to operate, monitor and control the power system.. (As opposed to Information Technology (IT) which is the infrastructure used for corporate services). For further clarification see Eskom Standard 240-55683502[8]
Video Analytics	An electronic method of automatically analysing video images to detect specific types of events (more advanced than Video Motion Detection).
Video Management System	Software used to connect to multiple DVRs or NVRs and view the footage from the attached cameras.
Video motion detection	An electronic method of detecting a change in the field of view of a camera.

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
AGC	Automatic gain control
AI	Automatic Iris
BLC	Back light compensation
CCD	Charged coupling device
CCTV	Closed circuit television
CNC	Customer Network Centre
DVR	Digital video recorder

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.

Abbreviation	Description
EI	Electronic Iris
FPS	Frames per second
NTP	Network Time Protocol
OT	Operational Technology
PA	Public address
PCR	Project Change Request
PTZ	Pan, tilt and zoom
UPS	Uninterruptible power supply
UTP	Unshielded Twisted Pair
VDU	Video display unit
VMD	Video motion detection
VMS	Video Management System
VPN	Virtual private network
WDR	Wide dynamic range

2.5 Roles and responsibilities

Security systems design engineers shall utilise this document as the basis for the enquiry process and during the product development phase.

Protective Services shall use this document to guide maintenance of installed CCVTV systems.

2.6 Process for monitoring

The security technology and support department will monitor compliance to this standard.

2.7 Related/supporting documents

This document supersedes DSP34-1613, DISSCABM6 and SCSSCABM6

3. Requirements

3.1 Objective

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.

3.2 Protection of Information

The installation & maintenance contractor shall not disclose any particulars of the project including this specification or the CCTV surveillance system to any other party or authority without written consent from Eskom.

All persons required to work on the site shall be made known to Eskom and may be required to have their security cleared prior to commencement of work and access to the site.

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.

3.3 Note on Product Choice

This document applies to going out on tender without a List of Approved Products (LAP). The supplier is free to tender with whatever make/model of equipment they believe is most able to meet the requirements of this specification.

There may however be cases where a site/region wishes to issue a List of Approved Products. This would be a list of equipment (make and model) which Eskom has proven, through experience or testing, can meet the requirements of this specification. Reasons for this may include ensuring compatibility with equipment already installed, and to leveraging off experience and training already within the business.

Should a LAP based tender be used, the functional requirements of this document would remain the same. However less vigorous testing of the equipment would be necessary. The tender documents should reflect which parts of this document would be relevant to the tender and what designs and practical evaluations will be applicable. It is recommended that the suppliers still be required to demonstrate an understanding of the equipment to be used, and how to use it effectively to achieve the security goals.

This document assumes that a non-LAP tender will be followed, i.e. the supplier will choose the products to be used.

3.4 CCTV System Overview

The use of CCTV surveillance systems enhance the visual monitoring of sites due to characteristics such as digital transmission of video, as well as digital storage of video for litigation purposes. A CCTV surveillance system provides a means to store and transmit visual footage of incidents within the site which can then be reviewed and analysed in detail.

The CCTV installations at Eskom sites are primarily intended for verification purposes, i.e. the visuals should be of such a quality that an observer can, with a high degree of certainty, determine whether there are intruders, the number of intruders, their actions and any equipment they may be carrying such as saws, guns, etc.

Should an intrusion incident occur, the intruder detection system shall be triggered by means of intruder detection units (typically video analytics on the perimeter cameras). The alarms and visuals shall be stored on site as well as transmitted to an assigned security alarm control room where the security personnel can assess the situation and then take the necessary responsive actions. The operators in the security control room shall have full control over the camera units, as well as have access to a public address (PA) system and outdoor lights installed at the site. This will enable the operator to obtain visuals of an intruder, as well as provide the operator a means of warding the intruder off via the PA system.

The communication link between the site DVR and the security control room shall be by means of a dedicated and secure communication medium between the sites and the security control room and take place over Eskom's telecommunications network. Communication media may include fibre (2Mbps bandwidth), microwave and satellite. GPRS shall only be used when higher bandwidth options are not available. Though the Eskom telecommunication network is preferred, 3rd party communications infrastructure may be used if necessary.

3.5 Design and Installation Process Overview

The design and installation process illustrated in Figures 1 and 2 shall be followed at any new CCTV site to ensure that the system installed is able to deliver the level of security required.

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.

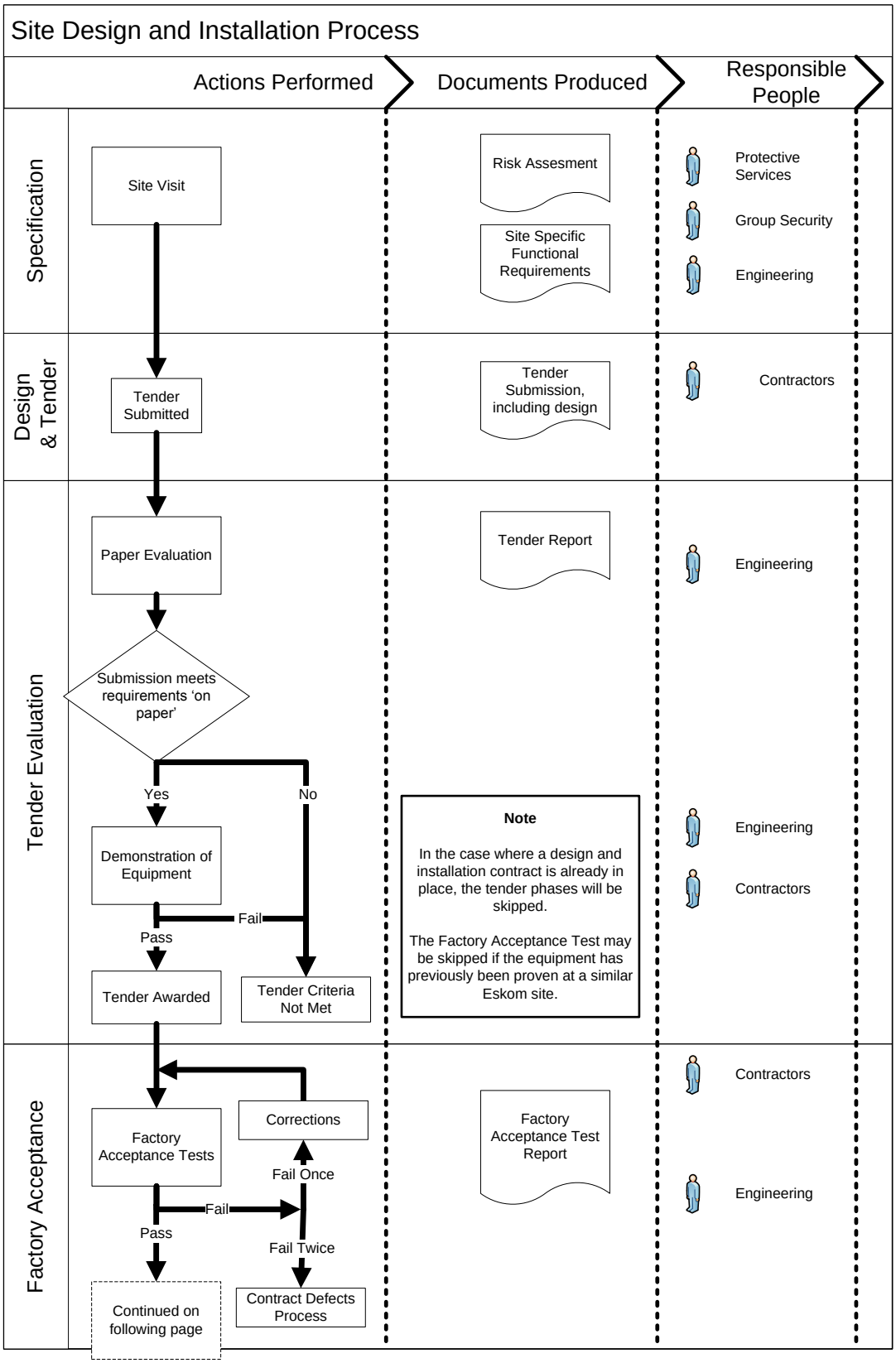


Figure 1: Design and Installation Process (pg1)

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.

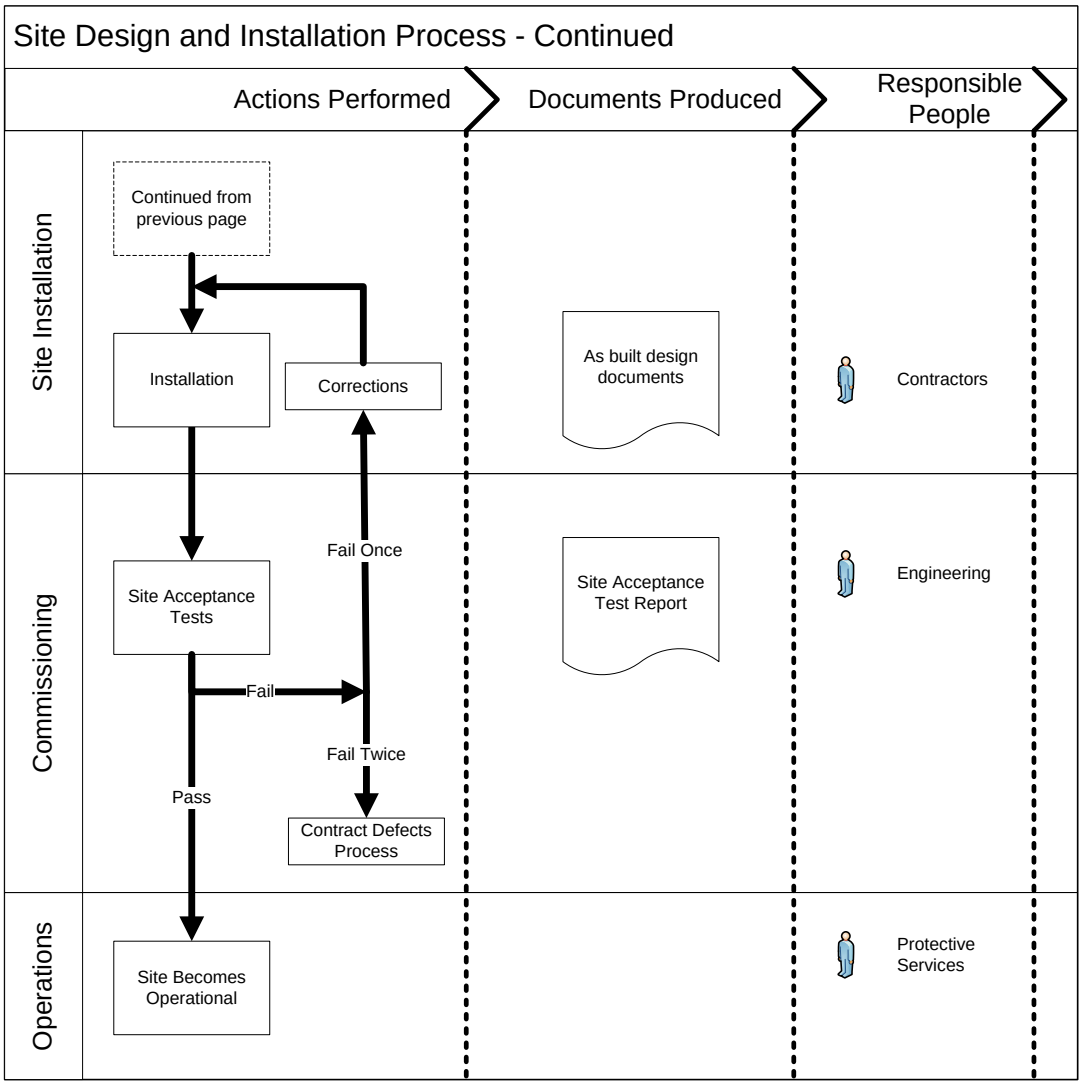


Figure 2: Design and Installation Process (pg2)

3.5.1 Site Specific Requirement Specification

A careful examination of the requirements of each site is essential before deciding on the level of security to implement at a site. The first step of the design process is therefore a site visit by a member of Eskom Group Security to determine the security risks at the site. From this visit a Risk Assessment and Site Specific Functional Requirement document will be drawn up highlighting the risks and recommending the level of security needed at the site. The Eskom document 240-79537982[15] outlines the process for security threat and risk assessments. The relevant group Security Generic Physical Security Design (PSD) shall also be applied.

Note that the site visit should include other security which may be needed to be installed or refurbished. For example should there be an additional fence, additional locking mechanism or burglar guards installed? At some sites it may be determined that these security measures are sufficient and CCTV is not necessary.

If CCTV is required at a site, site specific CCTV functional requirements shall be drawn up. This document is compiled by Engineering based on a site visit and the Risk Assessment. The functional requirements shall take into account what needs to be secured at a site and the risks and challenges associated with the site's unique layout. The site specific functional requirement document should include:

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) Where detection, observation, recognition and identification are needed from cameras?
2) Where detection will be needed
3) Whether monitoring of the CCTV will be onsite, offsite, or both.
4) The communications mediums available to the site from an offsite security control room.
5) The expected response time of armed response to the site.
6) Any potential blind spots due to the site layout and geography.
7) Suggested zones for the alarm and CCTV system
8) Eskom shall identify the floor space for the security cabinet or provide space in an existing panel.

3.5.2 Design and Tender

Once the CCTV functional requirements documents have been finalised the detailed design can begin. Where a contractor has not already been appointed for security systems installations, this design will be submitted as part of the tender process. Where a contract for a number of CCTV sites has already been put in place, the design phase may mean adapting a generic design for the particular site being secured.

Since not all aspects of the design are required at time of tender, the design documents required at time of tender and at time of final design are specified separately, below.

Eskom may choose to do the design in-house, in which case some, or all of the design documents will be provided by Eskom.

3.5.2.1 Tender Design Requirements

The design document shall include:

a) The equipment (make and model) to be used

b) Electronic copies of all equipment data sheets. This should include user and installation manuals if possible.

c) An overall system diagram showing the interconnections between equipment.

   1) Connections between equipment shall be labelled with communication protocol (RS485, TCP/IP, NO/NC contact) or voltage level.

   2) For tender this does not need to include wiring colours/numbers and terminal names/numbers.

d) The proposed design for both backup power solutions shall be included (see section 3.7.9)

   1) 110V DC Power design.

   2) 220V AC Power Option:

      i. Show expected backup time including calculations.

      ii. Include Make, Model and Capacity of batteries to be used

e) A site layout (see Figure 3) showing:

   1) The placement of all cameras and detection equipment

   2) The purpose of each camera

   3) The expected vertical and horizontal fields of view of all cameras. This may be calculated manually or by using camera CAD software.

   4) The detection area of all detection equipment

   5) The various alarm zones on the site, with zone name and number

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.

6) The routes for cabling to outdoor equipment and motorized gate through existing cable trenches and dedicated trenches. Cable exit points shall be clearly marked.

7) Cable and wire numbering philosophy and methodology.

8) The position of the security cabinet

9) Position of yard/junction boxes.

f) A list of equipment in the security cabinet.

g) A list of equipment to be in yard boxes (if used).

3.5.2.2 Final Design Requirements

The design document shall include:

a) The equipment (make and model) to be used

b) Electronic copies of all equipment data sheets. This should include user and installation manuals if possible.

c) An overall system diagram showing the interconnections between equipment.

1) Connections between equipment should be labelled with communication protocol (RS485, TCP/IP, NO/NC contact) or voltage level.

2) Final Design: Wiring colours and numbers and terminal names/numbers to be indicated for all connections.

d) Power supply details including:

1) The power supply point(s) to be used, including MCB numbers.

2) The backup power solution to be used at the site (see section 3.7.9)

e) If the preferred 110V DC power option the following shall be included (arranged by Eskom representative):

1) Document from the relevant DC engineer confirming that the 110V DC supply can be used for the CCTV system. This document should include calculations that show that the site backup power requirements can still be achieved with the additional load of the CCTV system.

f) If the 220V AC Power Option is to be used then the following will be supplied:

1) Expected backup time including calculations.

2) Make, Model and Capacity of batteries to be used

g) A site layout (see Figure 3) showing:

1) The placement of all cameras and detection equipment

2) The purpose of each camera

3) The expected field of view of all cameras

4) The detection area of all detection equipment

5) The various alarm zones on the site, with zone name and number

6) The routes for indoor cabling, clearly marking the trunking or overhead racks to be used / installed.

7) The routes for cabling to outdoor equipment and motorized gate through existing cable trenches and dedicated trenches. Cable exit points shall be clearly marked.

8) Cable and wire numbering philosophy and methodology.

9) The position of the security cabinet

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.

10) Position of yard/junction boxes.

h) The layout of equipment in the security cabinet.

i) The layout of equipment in yard boxed (if used).

j) The design document shall be accepted by an Eskom Security Systems Engineer before any installation begins.

k) The site specific Health and Safety plan shall be accepted by an Eskom Health and Safety practitioner before any installation begins.

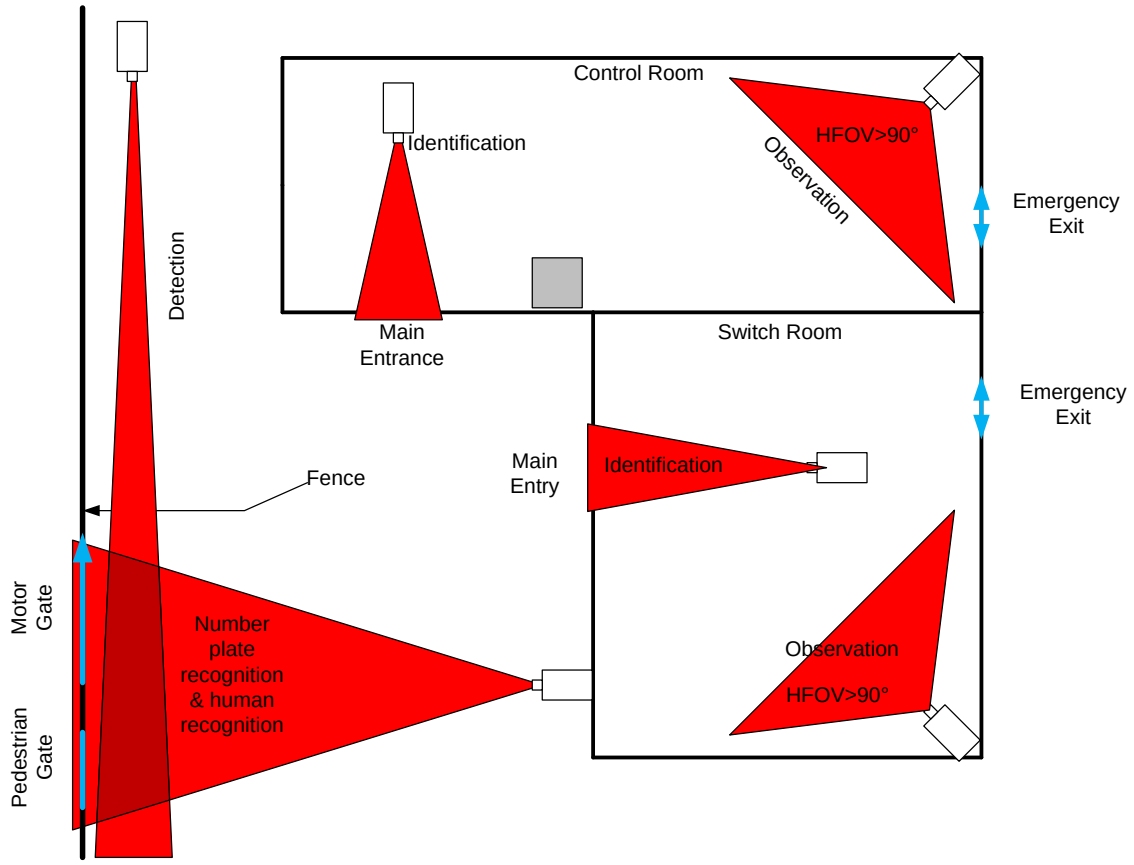


Figure 3: Example of Camera Placement, FOV and Purpose

3.5.3 Tender Technical Evaluation

The tender technical evaluation shall work in conjunction with the Eskom commercial process and shall consist of two steps:

3.5.3.1 Paper Evaluation

The submission shall be evaluated against the CCTV functional requirements Document based on the tender proposal documents and the specification sheets of the proposed equipment.

3.5.3.2 Practical Evaluation

Functional testing of the chosen equipment is crucial to ensure that equipment is able to meet the CCTV functional requirements. Comparing datasheets is not sufficient; the proposed equipment needs to be tested in a simulated environment to ensure it can meet all requirements.

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.

If the design submitted meets the CCTV functional requirements 'on paper' then a demonstration of the equipment shall be arranged as the next stage of functional evaluation.

3.5.3.2.1 Presentation

Companies meeting the Paper Evaluation requirements will be required to do a presentation of their proposed design. The presentation should:

a) Give an overview of the proposed design

b) Highlight advantages of the proposed solution as far as it will enable Eskom to secure it's sites from intruders

c) Demonstrate an in depth technical knowledge of and familiarity with the equipment to be used.

d) Demonstrate how equipment will work together to provide the security level required.

e) The suppliers ability to support the equipment when technical issues are encountered

f) Examples of similar installations which the tenderer has done

g) Eskom evaluators may ask questions regarding the proposed solution.

3.5.3.2.2 Demonstration of Equipment

A demonstration of the equipment shall be arranged.

The procedure for the Tender Demonstration Tests can be found in section 0.

Once a contract has been placed, any design changes shall be subject to additional demonstration tests before Eskom approves the change.

An equipment demonstration may also be required if there is an existing CCTV contract, but the site design proposes a piece of equipment that has not previously been used on an Eskom site.

3.5.3.2.3 Site Visit

Each tenderer shall arrange for an Eskom representative(s) to view a site where they have done a similar installation.

The site visit will be evaluated based on:

a) Quality of installation. Cables routed neatly, cabinets organised, cabling labelled.

b) Ability of cameras to operate as expected

c) Effectiveness of intruder detection used.

d) It is acknowledged that maintenance of the system is the system owner's responsibility and the condition of equipment and cabling at time of visit may not be a true reflection of the quality at the time of handover.

3.5.4 Factory Acceptance Test

Once the tender has been awarded and the purchase order for the term contract / site installation has been placed, Factory Acceptance Tests shall be performed. In the case where there is an existing term contract, and the equipment and system setup has been proven at previous Eskom installations, the factory acceptance test need only be done when the contract is established. This shall be at the discretion of the responsible Eskom engineer. The site where the equipment has been previously proven shall be documented.

The procedure for the Factory Acceptance Tests can be found in section 0

If the Factory Acceptance Tests are not met after corrections have been made, the relevant contract defects process shall be followed.

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.

3.5.5 Installation of System

The CCTV design shall be signed off as accepted by Eskom's appointed Project Engineer before installation of the system can begin. No work may begin on site without design approval from Eskom and a site kick off meeting.

The system shall be installed according to the appropriate manufacturer and Eskom specifications.

Detailed installation specifications can be found in section 3.6 of this document.

Any changes to the design made during the course of installation shall be approved by the Project Engineer via a project change request (PCR) or a formal site instruction and reflected in the as-built design documents.

3.5.6 Commissioning of System

Commissioning of the System includes adjusting all necessary settings to ensure that the installation meets the CCTV functional requirements. This requires explicit testing of the system including the simulation of incidents in all lighting conditions (sunrise, full sun, sunset, night). Commissioning tests include testing the interface between the CCTV system and the security control room (off site and on site).

The site will not be accepted until Site Acceptance Tests prove that the installation meets all requirements as set out in the site specific functional requirements.

The procedure for the Site Acceptance Tests can be found in section 0.

If the Site Acceptance Tests are not met after corrections have been made, the relevant contract defects process shall be followed.

3.5.7 Documentation

On completion of the installation the contractor shall provide Eskom with the following documentation:

a) Detailed as-built drawings of the installation including the following:

   1) A site layout diagram indicating the position of all equipment and devices installed. A complete cable block and wiring diagram with cable & wire numbers

   2) A site layout diagram indicating the position of all equipment and devices installed

   3) Coverage plots of the areas covered by intruder detectors and a list and description of each zone.

   4) Coverage plots of the areas covered by cameras' fields of view

   5) Alarm system zones

b) Manuals and training for the CCTV surveillance system. The manuals shall include the following:

   1) An overview of the CCTV and intruder detection system, including the equipment block schematic

   2) The functions and features of each item of equipment.

   3) Individual operating instructions for each item of equipment.

   4) Detailed operating instructions for all modes of operation of the CCTV system.

c) Manufacturer's technical and maintenance specifications for each item of equipment installed.

d) All documents shall be provided in soft and hard copy. Drawings softcopies shall be provided in as CAD files in .dwg format. Other soft copy documents shall be provided as pdfs.

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.

e) All system and camera settings shall be recorded, so that they can be confirmed and reproduced as required.

1) Where possible these settings and configurations shall consist of backup files which can be loaded onto the relevant equipment in the case of malfunction or replacement.

2) Where the equipment does not allow for softcopy backups, an electronic document listing the settings may be provided.

3.6 Installation

a) To ensure quality workmanship and sound installation practice, it is imperative that the contractor adheres to the specifications and standards supplied by Eskom. Should there be any uncertainty with regards to the specifications; the contractor is to contact the Eskom employee responsible for the project for guidance.

b) Only contractors with experience in CCTV and alarm system installations shall do installations. To this end the tenderer shall provide a CV of relevant experience and references.

c) All installers shall adhere to the OHS Act (Occupational Health and Safety Act) of 1970 when installing the system. Contractors and sub-contractors shall meet the requirements specified by Eskom Health and Safety specifications

d) All equipment shall have a mechanical earth connected to the site earth according to Eskom standards.

e) All equipment shall be designed and specified for a minimum realisable operational life 10 years under the prevailing environmental conditions unless otherwise agreed to by Eskom during the tender evaluation stage.

f) Consideration must be given for the minimum working and electrical clearances of overhead equipment – see Eskom Specification 34-304 - Substations, Section 2: Generic Substation Design [2] - section 4.5.1.2

g) All equipment shall be labelled in accordance with the design diagrams, with durable, weather resistant labels.

h) Cable and wiring marking shall be in accordance with Eskom standard 240-64636794, Standard for Wiring and Cable Marking in Substations.

i) All cables and wires shall be marked with a unique identification, at all terminations, in accordance with the cabling and wiring diagrams supplied.

j) All of the splices and connections shall be mechanically secure and shall provide electrical contact without stress on connections and terminals. Splicing is strongly discouraged but if unavoidable, splices used shall have insulation equivalent to that of the wires being joined.

k) Any hole which insulated conductors pass through shall be provided with a smooth, rounded bushing, or shall have smooth, rounded surfaces upon which the insulated conductors may bear.

l) Wireways shall be smooth and free from sharp edges, burrs, fins, or moving parts that may damage wiring.

m) All internal wiring connections shall be made with a solder lug or pressure terminal connector

n) A terminal lug shall be arranged such that in any position it cannot contact the metal enclosure, non-energized accessible metal parts or other electrical circuits. Alternatively the shank of the lug shall be provided with insulation equivalent to that of the conductor.

o) Terminal blocks shall be in accordance with Eskom standard 240-70413291, Specification for Electrical Terminal Blocks.

p) The CCTV installation shall be signed off as accepted by Eskom's appointed Project Engineer for the security system installation.

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.

3.7 System Level

3.7.1 System Overview

The CCTV system consists of various subsystems. A functional block diagram of the CCTV system illustrating the main subsystems and the interaction between the subsystems is provided in 4 below. The CCTV system has components both on and off site. What follows is a brief explanation of the system as a whole, detailed descriptions of each subsystem can be found later in the document.

3.7.1.1 On site

At each site being protected, various subsystems connect to create an integrated security system. These subsystems will differ from site to site but may include:

a) Physical deterrents such as fences

b) Outdoor perimeter detection provided by a number of technologies

c) Indoor intruder detection provided by a number of technologies

d) Surveillance cameras (indoor and outdoor)

e) Lighting systems

f) Access control equipment

g) Other devices such as sirens, public address systems or alarm system status LEDs

These subsystems will communicate with various controllers (DVR, Alarm panel, PA controller etc.) using a combination of hardwired contacts and communication busses (RS232, Ethernet, proprietary protocols etc.). These controllers will communicate with each as necessary to create a system which can meet the functional requirements set forth in this document. At manned sites there may also be a security monitoring station on site from which CCTV and alarms can be viewed.

The security equipment cabinet shall also serve as the point of power distribution for the security equipment which may need a variety of combination of AC and DC power at various voltage levels.

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.

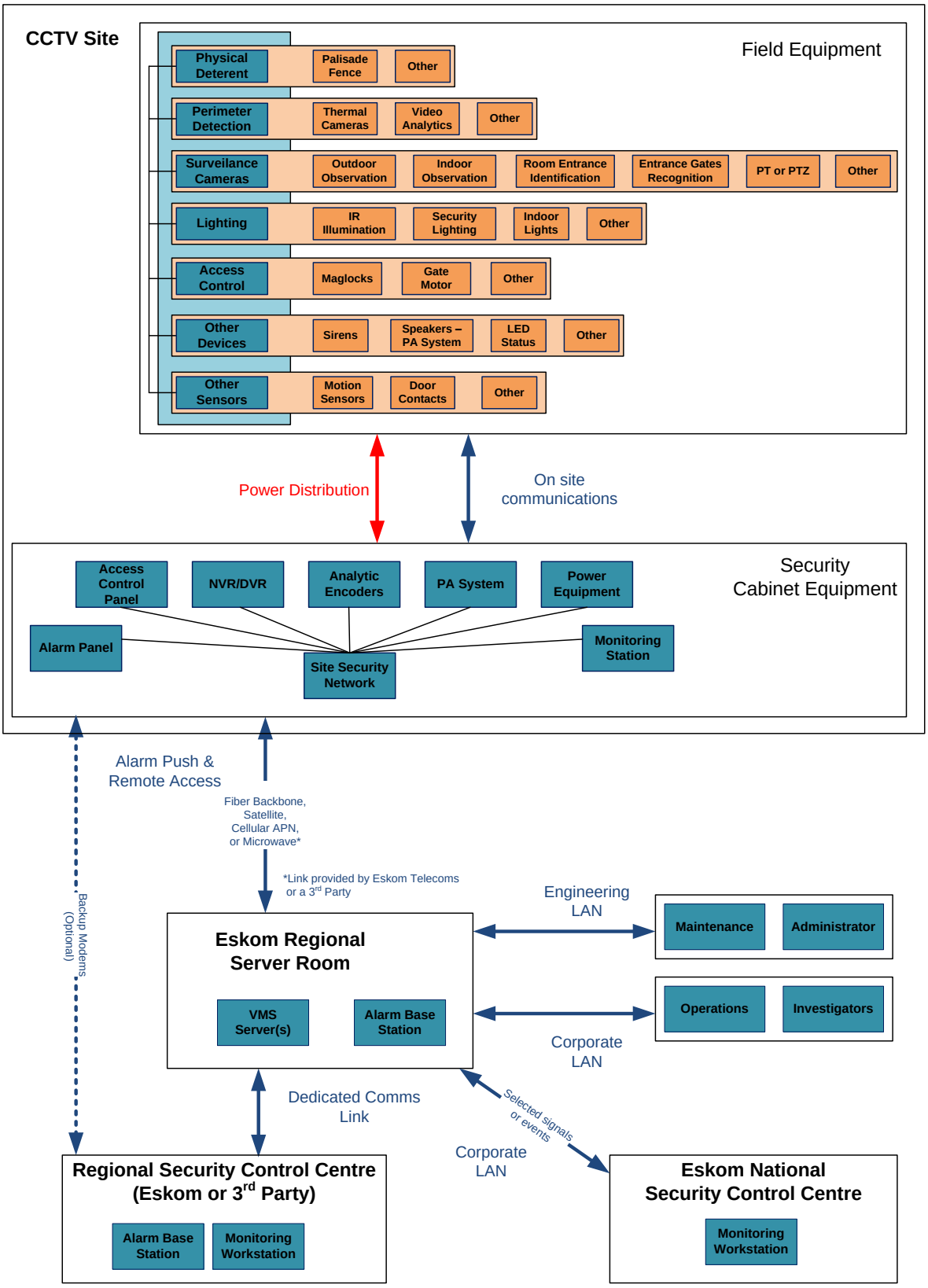


Figure 4: Functional Block Diagram of CCTV System

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.

3.7.1.2 Eskom Local OT Security Server

All sites with CCTV systems will communicate with a Local OU Security Server. This server shall be owned and hosted by Eskom. VMS server software will be housed here as well as other server related equipment such as alarm base stations. Housing the system at an Eskom site ensures that Eskom has control over the server equipment and prevents Eskom from being locked into using a specific service provider for remote security monitoring. All sites in the OU will connect to this Local OU Security Server via a combination of available communication channels. WAN communications may be provided by Eskom or a third party. The Local OU Security Server shall be suitably protected by physical and network access control (secure room, user rights, firewalls etc.).

Standalone sites such as Power Stations may be designed with an onsite Local OU Security Server. If necessary due to budget/resource availability, the server can be hosted at a third party (see 3.11.2.1 for details).

3.7.1.3 Local Security Control Centre

The Local Security Control Centre shall be responsible for responding to alarms from sites and managing incidents on site using the CCTV data from site. Ideally the Local Security Control Centre should be an Eskom manned centre, but budget and resource restraints may necessitate that the control centre be provided by a third party. Network security between any 3rd parties and the Eskom Network shall be designed and controlled by Eskom. Details of the activities of the Local Security Control Centre can be found in section 3.12 - Security Control Room.

The Security Control Centre shall use approved VMS client software to connect to the Eskom OT Security Server, thereby receiving all alarm signals from the various sites (black screen monitoring). The Local Control Centre shall also be able to receive video on demand from the sites via the OT Security Server.

The connection between the Local OT Security Server and the Local Security Control Centre shall be a dedicated link (e.g. a Diginet line / microwave link). There may also be a backup links directly between the Local Security Control Centre and sites if this is deemed necessary.

3.7.1.4 National Security Control Centre

Eskom intends to establish an Eskom National Security Control Centre from which selected security incidents can be managed and monitored. A communication link would be established from the local OU security servers to the National Control Centre server via the Eskom corporate LAN. Selected signals or events would then be directed to the National Security Control Centre. It shall be possible to escalate events from the Local Security Control Centre to the National Security Control Centre.

3.7.1.5 Engineering and Operational Access

Eskom engineers shall be able to connect to the Local OT Security Server remotely from the Eskom Engineering (OT) LAN to perform maintenance and administrative tasks on the system.

Members of Eskom Group Security shall be able to connect to the OT security server remotely from the Eskom corporate network in order to perform operational tasks (check up-time of systems, confirm sites are being armed etc.) and investigations (view footage and alarm logs etc.).

This remote access shall be restricted to those who have explicitly been granted access rights.

3.7.2 Operation - Unauthorised Access

The figure below depicts the sequence of events that the security alarm system and personnel shall follow during unauthorised access to the protected site[3].The CCTV system needs to enable this sequence of events can take place.

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.

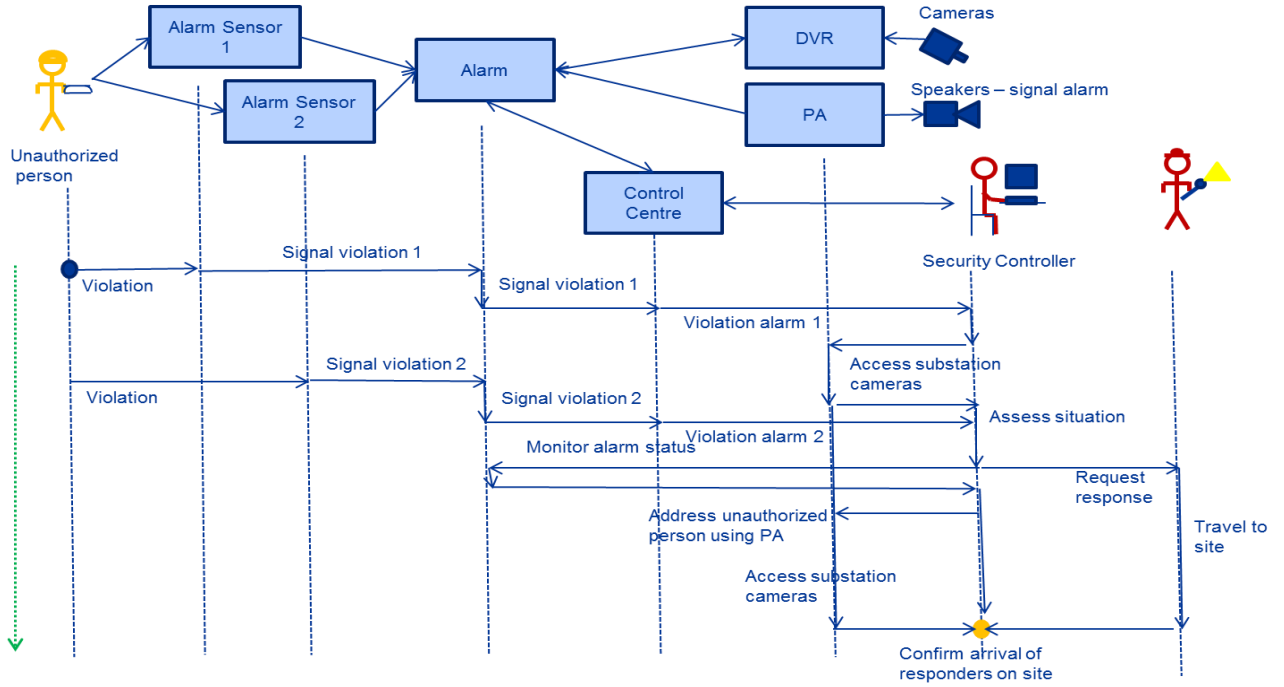


Figure 5: Unauthorised Access Flow of Information [20]

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

1) Attempt to disarm system by unauthorised user.

2) Panic button been pressed.

3) Control centre issuing an alarm instruction due to unauthorised access

4) Cameras and alarm sensors detecting violation.

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

c) The security controller shall be able to address the unauthorised person using the Public Address System.

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

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

3.7.3 Warrantee and Certification

a) All equipment installed shall be subject to the OEM warrantee.

b) Contractor shall provide proof that technicians have been trained and certified to install and configure the CCTV equipment specified.

c) There shall be an agreement from the OEM that the OEM supports the tender offering and will continue to support the product if the tenderer defaults.

3.7.4 General Physical Requirements

All installed equipment shall meet the following mechanical requirements:

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.

3.7.4.1 Environmental conditions

All equipment shall be designed for application in 'special' environmental conditions as follows (adapted from Table 2 of IEC 60255-1[4]):

a) Ambient air temperature: -25 °C to +55 °C (installed indoors); or -25 °C to +70 °C (installed outdoors, within enclosures).

b) Altitude: < 2 500 m

c) Pollution: Location in urban areas with industrial activities and without special precautions to minimize the presence of sand or dust (conditions as per classes 3C2 and 3S2 in IEC 60721-3-3[12]).

d) Relative humidity (24h average): 98%

e) All outside equipment Including fasteners and supports should be corrosion resistant and appropriate for the environment on site

f) After fabrication, metal surfaces including doors and removable covers shall be prepared and finished with corrosion protection.

g) Paint work damaged during transport and delivery shall be made good as per manufacturer repair specification at no cost to Eskom. If site re-painting is necessary, the equipment and labels shall be carefully masked and any overpaint which occurs in spite of the masking must be removed. If the damage is not repairable, Eskom reserves the right to return the equipment.

h) All nuts, bolts and washers use for the construction to be stainless steel. Screws can be cadmium plated.

i) Further environmental protection may be needed e.g. Equipment installed at a coal power station or in a mining area will need added dust protection.

j) Convection cooled (fan-less) equipment are strongly preferred. If fans are used, they shall be speed controlled and the electronics shall be isolated and conformal coated to protect against dust ingress.

3.7.5 General Electrical Requirements

All installed equipment shall meet the following electrical requirements:

a) The expected life of equipment under conditions specified (section 3.7.4.1 above) shall be a minimum of 5 years.

b) All power cable shall be appropriately sized to ensure voltage drops along cable runs remain within the operating specifications of the equipment being powered.

c) All equipment shall be effectively protected against overvoltage due to lighting strikes or switching surges by strategically placed surge arrestors

d) Descriptive cable markings shall be used as agreed to with Eskom. These shall be reflected on the drawings. See section 3.6 for more details.

e) Cable selection and routing shall always be done in such a way that operation of equipment is not affected by electrical interference. This may be achieved by separating power and communications cables, shielding of cables, or a combination of the two.

f) Equipment shall not be affected by electrostatic discharges that are applied directly to the equipment or to metal objects in the proximity of the equipment: All electronic equipment shall be a class 2 device as specified in IEEE 1613-2009, 8 *Electrostatic discharge tests*[24]

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.

3.7.6 Cable routes in control plant / equipment rooms:

a) Auxiliary power cables shall be laid in the control room power rack, away from communication cables.No conduit is needed on the rack.

b) Communications cables should use the control plant room communications rack. No conduit is needed on the rack.

c) Where cable racks are not available, cables may be routed along the wall or in PVC sleeves in the cable trench, at Eskom's discretion.

d) Where security cables are routed along the walls, they shall be in metal or plastic conduit.

e) Auxiliary power and communication cables shall be in separate conduit.

f) In substations, security cables shall not be routed in the ceiling.

g) If fibre optic leads are used they should be protected using sprague tubing when entering and exiting cable trays or panels.

h) Regional or site specific requirements may supersede the above cable route requirements.

3.7.7 Outdoor Cables and Trenching in Substations

a) Security cable should share control cable or lighting trenches where possible, where this is not possible, security cable trenches shall be dug.

b) The security cables shall enter the control plant room through the same path as control cables.

c) Security cable trenches shall be 0,5 m deep

d) All cables shall be armoured or laid in appropriately sized plastic conduit (e.g. HDPE, Kabelflex, whether in cable trenches or dedicated security trenches. The appropriate bends and connectors must be used for the conduit, according to manufacturer's instructions.

e) Security systems communication cables and auxiliary power cables shall not be laid in the same conduit unless using fibre communication or DC power.

f) Drilled holes in junction boxes shall be kept to a minimum and shall be appropriately sealed to prevent water ingress.

g) Care shall be taken when working with fibre optic cable so as to ensure the fibre is not damaged during installation or maintenance.

h) The stone layer shall be removed far enough from the cable trench excavation as illustrated in 6. The trench soil shall not be placed on top of any yard stone.

i) After the cables have been laid, the trenches must be backfilled with the original soil in layers not exceeding 300mm and properly compacted. Once the backfill is completed, the stone shall be replaced appropriately.

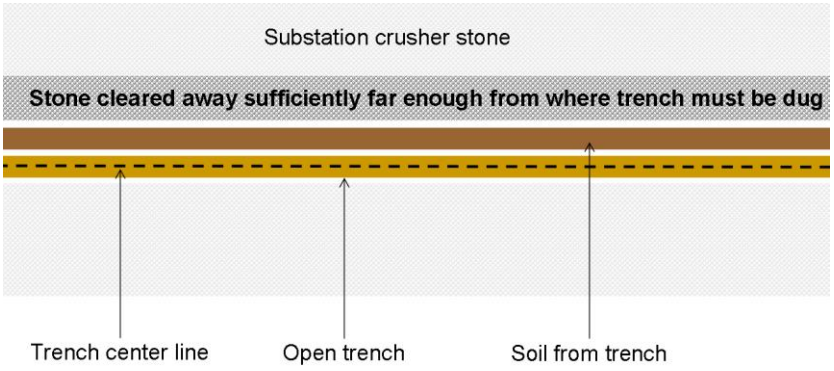


Figure 6: Cable Trench Layout

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.

3.7.8 Security Cabinet

The security cabinet/panel shall contain all the control equipment of the intruder detection and the surveillance system (digital video recorder (DVR), communication equipment, public address (PA) etc.). The cabinet shall be housed within a suitable access controlled equipment room; at substations this shall be the substation control plant room.

a) Cabinet shall be a freestanding swing frame panel or a freestanding server cabinet.

b) Cabinet shall be designed so as to limit dust ingress which could affect effective operation of equipment.

c) All points of cable entry shall be through glands so as to secure the cables.

d) Access to the inside of the cabinet shall be restricted and controlled by means a physical lock to which only authorized security personnel and Eskom employees from the Risk Department shall have access. Cabinet shall be alarmed for tempering and remain armed when main alarm system is disarmed. This is subject to regional requirements.

e) Cabinet design shall take into consideration airflow and heat distribution. Equipment shall be laid out such that units that generate the most heat are at the top.

f) There shall be a dedicated Aux power supply distribution module with a suitably sized incomer isolator and suitably sized load MCBs per piece of equipment.

g) The incomer supply DB MCB for this module must be correctly sized to protect the incomer cable in order to prevent nuisance trips.

h) Cables shall be neatly routed in trunking.

i) Cable ties or similar shall be used for cable management.

j) Where possible equipment in the security cabinet shall be 19 inch rack mountable or DIN rail mounted equipment. Where 19” or DIN rail mounting is not available, equipment shall be neatly secured on shelves.

k) Equipment or connection accessed regularly shall be accessible from the front of the panel or shall be wired to a terminal rack accessible from the front.

l) Equipment shall be suitably earthed to the cabinet, and the cabinet shall be earthed to the substation earth.

m) Eskom shall approve the layout design before the cabinet is populated.



Figure 7: Example of Poorly Organised Security Equipment Cabinet



Figure 8: Example of Well Organised Security Equipment Cabinet

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.

3.7.9 Backup Power Supply

Two power supply solutions shall be provided for the system.

Option A will operate off 110V DC and will be connected to the relay house 110V DC supply which has battery backup.

Option B is to use the 220V AC supply from the site and it shall include a battery backed up UPS for all security system devices.

The responsible Eskom DC design engineer shall be consulted on a per site basis to determine which power supply system will be used and to allocate connection MCB's on the main Distribution Board. Option A be installed whenever possible since this arrangement leverages off the battery maintenance processes already in place. Option B will be used when there is no site battery capacity or the capacity is not sufficient to supply the added load of the camera and alarm system. For both options the standing time for backup power is 12 hours at sites within 200kms of a responsible Eskom DC section, 18 hours at sites more than 200kms from a responsible Eskom DC section.

Both power supply design options shall be available.

3.7.9.1 Option A: 110V DC

a) The security system shall be powered by 110V supplied from the site's DC supply. In the event of a power failure the system will be supplied by the substation's battery and / or generator backup.

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

c) The MCB used on the AC/DC panel shall be clearly labelled 'Security'.

d) Power will be distributed through the panel so as to isolate the supply of the subsystems by means of appropriately sized MCBs. At a minimum the following will be on separate supply circuits:

   1) Intruder detection system

   2) Perimeter Cameras

   3) DVR, Indoor cameras and PTZ

   4) Perimeter detection system (if separate from perimeter cameras)

   5) Other security related equipment such as motorized gates or electric fences.

e) Figure 9 below, shows an overview of the power distribution for option A. This should be adapted according to the equipment being used.

f) All equipment shall meet the specifications of sections 3.7.3 - Warrantee and Certification, 3.7.4 - General Physical Requirements, and 3.7.5 - General Electrical Requirements.

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.

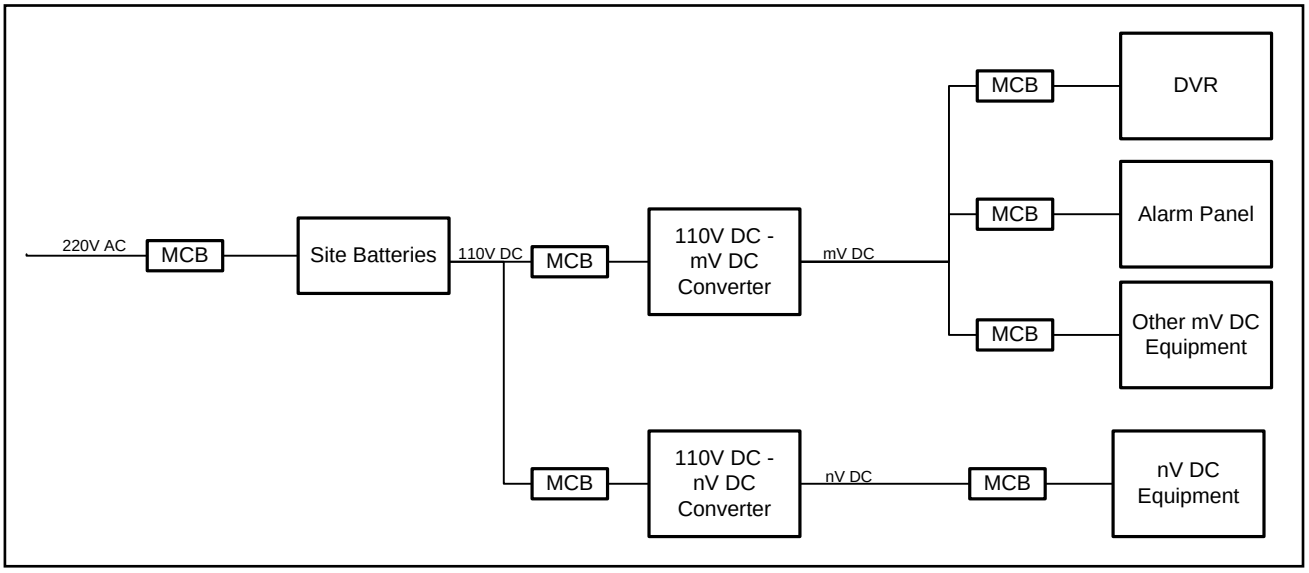


Figure 9: Preferred Power Distribution, Using Backup Power from the Site

3.7.9.2 Option B: 220V AC

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

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

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

d) Power will be distributed through the panel so as to isolate the supply of the subsystems by means of appropriately sized MCBs. At a minimum the following will be on separate supply circuits:

1) Intruder detection system

2) Perimeter Cameras

3) DVR, Indoor cameras and PTZ

4) Perimeter detection system (if separate from perimeter cameras)

5) Other security related equipment such as motorized gates or electric fences.

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

f) CCTV system batteries in addition to UPS batteries are not recommended. If CCTV system batteries are unavoidable then individual subsystems that have their own battery backup, these shall not be fed by the UPS. This is to prevent the UPS from charging these batteries in the event of a power failure (See figures 10 and 11). Any CCTV system batteries used shall provide backup for the time specified in section e) above.

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

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

i) Figure 11 below, gives an overview of the power distribution for option B. This should be adapted according to the equipment being used. DC voltages shown are examples; other DC or AC voltages may be used as necessary.

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.

j) All equipment shall meet the specifications of sections 3.7.3 - Warrantee and Certification, 3.7.4 - General Physical Requirements, and 3.7.5 - General Electrical Requirements.

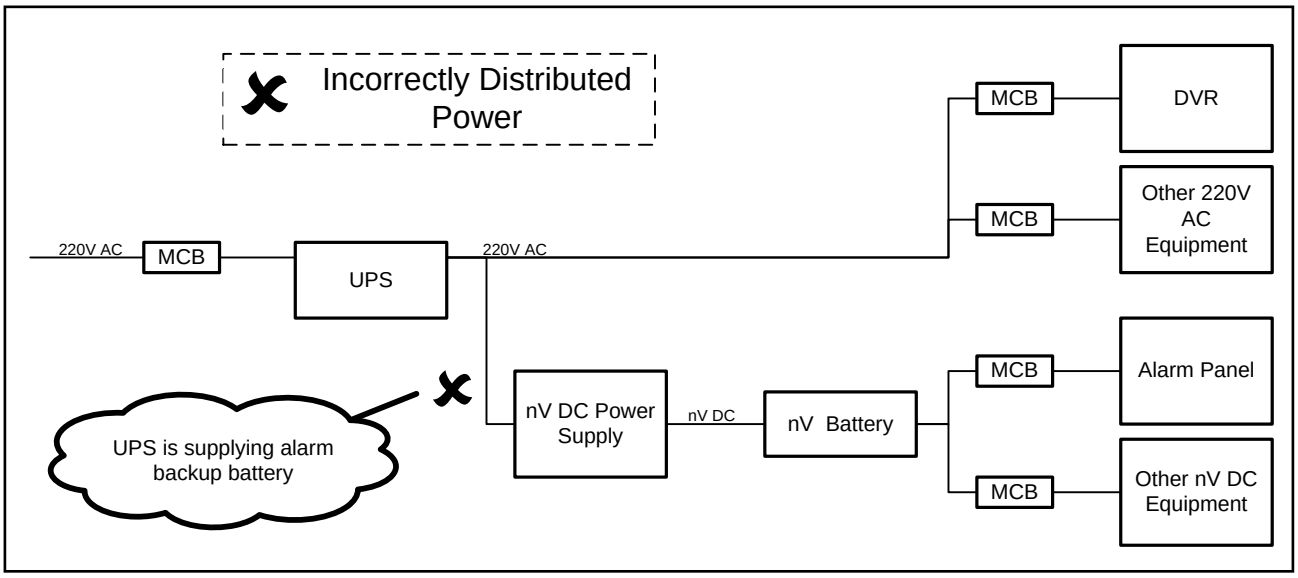


Figure 10: Incorrectly Distributed Option 2 Power, Battery Downstream from UPS

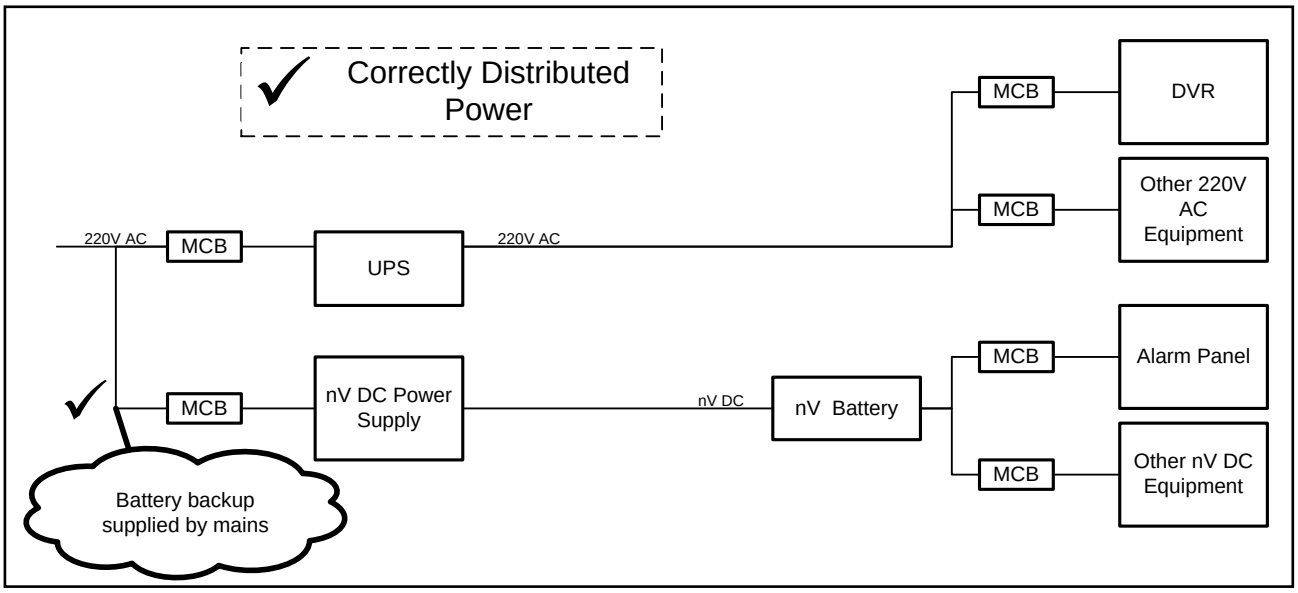


Figure 11: Correctly Distributed Option 2 Power, Battery Parallel to UPS

3.7.10 Communication

a) A connection from the site to the Eskom local OT security server shall provide the means of communication to the control centre for, alarms and live viewing.

b) The connection shall also be used for remotely configuring equipment and downloading of recorded footage

c) The communication link between the site and the security control room shall be by means of a dedicated and secure communication medium between the sites and the security control room.

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.

d) Communication shall take place over Eskom's telecommunications network if at all possible.

1) When specifying a new site Eskom Telecoms will be consulted to determine the feasibility of using (or establishing) an Eskom Telecoms link to the site.

2) Eskom Telecoms will be consulted before going out on tender and communications available shall be stated at tender phase.

3) The priority and risk at the site shall be taken into account when deciding whether or not to increase bandwidth available for security

e) Though the Eskom telecommunication network is preferred, 3rd party communications infrastructure may be used if necessary.

f) The communication medium will be fibre (2Mbps bandwidth) where possible and satellite or microwave where fibre is not installed.

g) As a last resort, if a higher bandwidth connection is not possible, GPRS may be used for communications provided equipment is specified and configured to be operated over the lower bandwidth.

h) The communication link shall be established according to the latest Eskom specification DISSCZAA2: CCTV Satellite Telecommunication Specification for Distribution Substations.

i) The connection from the security equipment to the Eskom Telecoms network shall be Ethernet and use RJ45 connectors.

j) Eskom to provide all IP addresses to be used for on-site LAN.

3.7.11 PA System

The PA system shall provide the means by which the security control room personnel shall communicate audibly over a speaker system. The communication to the speakers shall be by means of an audio module connected to or forming part of the DVR.

A traditional PA system with amplifier may be used, or a Network Horn Speaker, which communicates using TCP/IP. Cost and ease of installation should be taken into account when choosing between the two types.

The PA system shall meet all specifications listed in section 3.7.4 – General Physical Requirements and section 3.7.5 - General Electrical Requirements. Additional requirements are listed below.

a) If using a traditional PA, A power amplifier with a minimum of 25W RMS X 2 channels output power shall be installed to power the speakers with amplifier size that matches.

b) The speakers shall be weatherproof, environmental, corrosion and vandalism resistant as well as UV resistant.

c) The speakers shall be installed under the overhang of the building's roof where possible.

d) The audio from the speakers shall be clearly audible throughout the whole yard and be able to handle an alarm siren without distortion.

e) Additional speakers shall be added if necessary

f) Speaker setup shall take into account local residents in urban areas.

3.7.12 Time Synchronisation

a) In order accurately analyse recordings of incidents, and for providing reliable evidence, recorded footage needs to be time stamped with an accurate date and time stamp.

b) The preferred method of time synchronization is using GPS. If a site has a GPS time signal, it should be used for the security system.

c) At a single site, all cameras shall be time synced to within 1s of each other. This time syncing may be provided by the DVR or other timing device.

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.

d) Different sites shall be synchronised so that the difference between the times at different sites is less than 10s. This synchronisation may happen via an NTP clock or the central video management system (VMS).

e) The central NTP clock or VMS system shall get its time from a GPS signal.

3.8 Intruder Detection System

3.8.1 Indoor Detection

a) There shall be intruder detection in all buildings and rooms which the risk assessment indicates should be protected. At substations this will include all rooms of the relay house and switch rooms.

b) The sensors shall be placed so as to detect intrusion through any door or window leading into the building or by which access can be gained into the secured area.

c) Intruder detection may be in the form of movement detection (e.g. passive infrared sensors (PIRs), video analytics); door and window detection (e.g. Reed switches), or some combination of sensors.

d) Intruder detection shall be located as to detect unauthorised entry through any door or window in the building.

e) Battery rooms holding lead acid batteries are a zone 2 hazardous location with specific rules governing work in the room. For this reason battery rooms shall not have CCTV or alarm equipment installed inside, but rather a door contact installed on the outside of all doors and windows to detect unauthorised entry.

3.8.2 Alarm System Operation

a) The alarm system shall meet the requirements of Eskom specification 240-86738968 - Standard for Security Alarm Systems for Protection of Eskom Installations and its Subsidiaries [3]. In addition, the alarm system shall support the following when integrated with the CCTV:

b) When an alarm is generated by the alarm system, the CCTV system shall detect the alarm and know what zone was triggered in ordered to trigger the relevant cameras for that zone.

c) The alarm system shall receive trigger signals from CCTV video analytics in addition to triggers from the site's traditional security sensors.

d) For redundancy alarm signals shall be sent to the Local OT security server through the CCTV system (to the VMS) and well as through the alarm system (to the alarm base station).

e) The intruder detection system shall be able to control relay contacts which can be connected to the gate motor for opening and closing the gate.

f) Should the intruder detection system be triggered at night, the site's LED floodlights shall be activated for a period of 15 minutes. Night can be determined by a means of day/night sensor or a clock timer. See section 3.8.3 below for more details.

g) When the alarm is deactivated, a signal shall be sent through to the security control room identifying the employee who disarmed the site.

h) Alarm system activation / deactivation shall be confirmed by means of audio sound over the speaker system as well as indicator LED(s) visible from inside the relay house and from the outside the gate of the site.

i) Activation/deactivation of the intruder detection system shall activate/deactivate perimeter detection and internal building protection whether the detection is on the cameras or alarm sensors.

j) Each activation / deactivation of the alarm system shall be date and time stamped and recorded by the alarm system.

k) The system shall use remote controls to activate and deactivate the system as specified by 240-86738968 or per the technology already being used in the region.

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.

3.8.3 Lighting Integration

Yard lighting at Eskom substations have yard operating lights consisting of floodlights which provide enough light for work in the HV yard to be performed safely during low light conditions. These lights are not however designed to provide lighting on the perimeter of the site and as such do not provide suitable light for cameras.

Due to Eskom's drive to save energy, at many substations the floodlights remain off at night. Although the floodlights are not designed to illuminate the whole site, they can be useful as a deterrent to intruders and to guide armed response when they arrive at the site.

a) Should the alarm be triggered, all of the floodlights shall be switched on simultaneously to act as a deterrent as well as provide light for the PTZ camera. The floodlights shall be controllable (switch on / off) from within the security control room.

b) The flood lights shall be triggered to turn on when the alarm is triggered at night.

c) The system shall determine when it is night either by means of a day/night sensor, or based on the time of day.

d) Unless otherwise decided by the operating unit, the floodlights shall be off at all times except when the alarm is triggered.

e) The floodlights shall still be able to be operated manually by a person on site.

f) The lights shall be powered via a timer module to ensure that lights are not left burning. The timer shall be set to 15 minutes. This timer will only come into effect when lights are turned on by alarm or security control room; when lights are turned on by person on site, they shall remain on, until turned off by person on site.

3.9 Yard

3.9.1 Overview

a) The main outdoor area to be covered by the CCTV and intruder detection system shall be along the perimeter of the site yard within the boundary fence.

b) There shall be a thorough analysis of the site's layout before installing any cameras and perimeter detection to ensure that the entire site perimeter has been covered. Once installed, the entire system will be tested to ensure that this intended coverage has been achieved (See sections 3.16.10 - Indoor Intruder Detection Tests and 3.16.12 -Camera Functional Test).

c) The intention is for the perimeter detection system to detect when an intruder crosses the boundary of the site and the camera system to be used to verify that a person has crossed the boundary. It is recommended that the perimeter detection be provided by video analytics, either as part of the camera / DVR, or as an add-on feature to the camera system. See Section 3.9.3.

d) One or more PTZ cameras shall be installed so as to view the majority of the yard. The intention of the PTZ system is to automatically track intruders, providing information to the security monitoring centre which can be used to deter the intruder and guide armed response. At smaller, lower risk sites, the PTZ may be omitted to save costs. At other sites it may prove more feasible to use strategically placed fixed cameras instead of the PTZ.

e) A fixed camera shall be positioned so as to have a clear view of the main entrance gate. The intention of the gate camera is to recognise people and vehicles entering the site.

f) To prevent damage to the camera and ensure good picture quality, cameras shall not be placed in a direction such that they will be exposed to intense beams of light from the floodlights or direct sunlight.

g) Visible notification shall be placed at entrances and on the outside of the perimeter fence of the premises to notify persons entering the premises, that they may be subjected to CCTV surveillance. At substations the date of placement of such notices shall be recorded in the substation logbook.

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.

3.9.2 Perimeter Camera System Layout

a) The installation of fixed cameras shall be done primarily to cover the inside perimeter of the site yard.

b) The purpose of the perimeter cameras is detection (See section 3.9.1 for a discussion of camera purpose). Perimeter cameras shall provide control room operators a method to confirm when an alarm is generated that an intruder has breached / approached the perimeter.

c) At selected sites it may be appropriate for the cameras field of view to cover the outside perimeter of the fence, supporting detection before the perimeter is breached. This will depend on detection method used and the likelihood of false alarms from movement just outside the perimeter.

d) There shall be a thorough analysis of the site's layout before installing any cameras and perimeter detection to ensure that the entire site perimeter has been covered. This must include mapping each camera's field of view and range of view on the site layout drawings to ensure that the perimeter is 100% covered.

e) The view of the camera shall be free of any hindering obstacles such as walls, trees or buildings.

f) The installation of cameras shall be done so as not to hinder existing vehicle accessibility paths to the installed power plant.

g) The recommended arrangement of cameras within a generic substation yard is illustrated in Figure 12. Achieving coverage of the yard fence need not always be by means of a camera installed parallel to the yard fence. This is especially the case where the layout of the yard is not square. The requirement is only to have visuals of all enclosing fences of the yard, be it a parallel visual along the span of fence or at an angle facing.

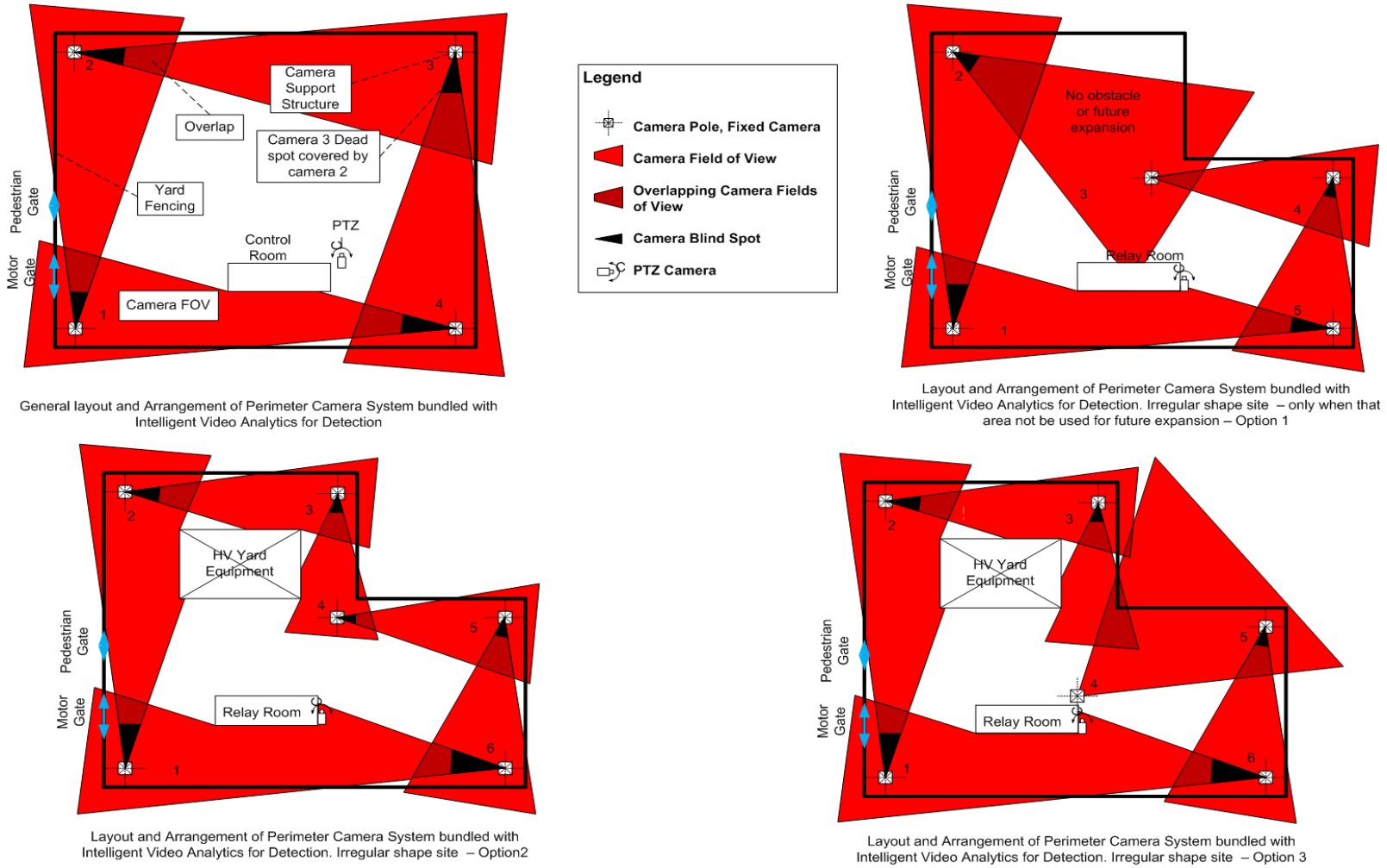
h) Where it is possible to obtain visuals at an angle of the fence, it shall be ensured that there is no obstacle between the camera and the face of the fence being monitored.

i) Every camera has a 'dead spot' directly in front of it, where it will not be able to see. The size of this dead spot is determined by height and angle at which the camera is mounted, and the camera's field of view. Perimeter cameras shall be arranged so that the dead spot of each camera is covered by the field of view of another camera as shown in 12.

j) Should there be obstacles or poor visuals, additional cameras shall be installed to cover the span of fence.

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.



General layout and Arrangement of Perimeter Camera System bundled with Intelligent Video Analytics for Detection

Layout and Arrangement of Perimeter Camera System bundled with Intelligent Video Analytics for Detection. Irregular shape site – only when that area not be used for future expansion – Option 1

Layout and Arrangement of Perimeter Camera System bundled with Intelligent Video Analytics for Detection. Irregular shape site – Option2

Layout and Arrangement of Perimeter Camera System bundled with Intelligent Video Analytics for Detection. Irregular shape site – Option 3

Figure 12: Examples of Various Layouts of Perimeter Cameras

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.

3.9.3 Perimeter Detection System

a) Alarms shall be generated by a perimeter detection system.

b) The use of microwave beam detection is strongly discouraged due to the prevalence of nuisance alarms.

c) It is preferred that the perimeter detection be provided by 'video analytics', either built into, or as an addition to, thermal perimeter cameras. Other detection methods (or combination of detection methods) may be used if they are able to meet the functional requirements specified here.

d) If Video analytics is used it should be 'advanced video analytics', able to analyse the footage, not simply video motion detection which only looks for changes in the picture. See 0 for the distinction between the two.

e) 'Edge' video analytics is preferred over server/DVR based video analytics. Edge video analytics happens on board the camera or on a device connected to each camera. Each camera therefore has a dedicated processor analysing its footage. Server or DVR based analytics uses one processor to analyse the feeds from a number of cameras, increasing the chance of poor performance. See 0 for more information.

f) The perimeter detection system shall create an 'invisible wall' which encapsulates the entire perimeter of the yard, so that there are no areas where an intruder may enter the site undetected.

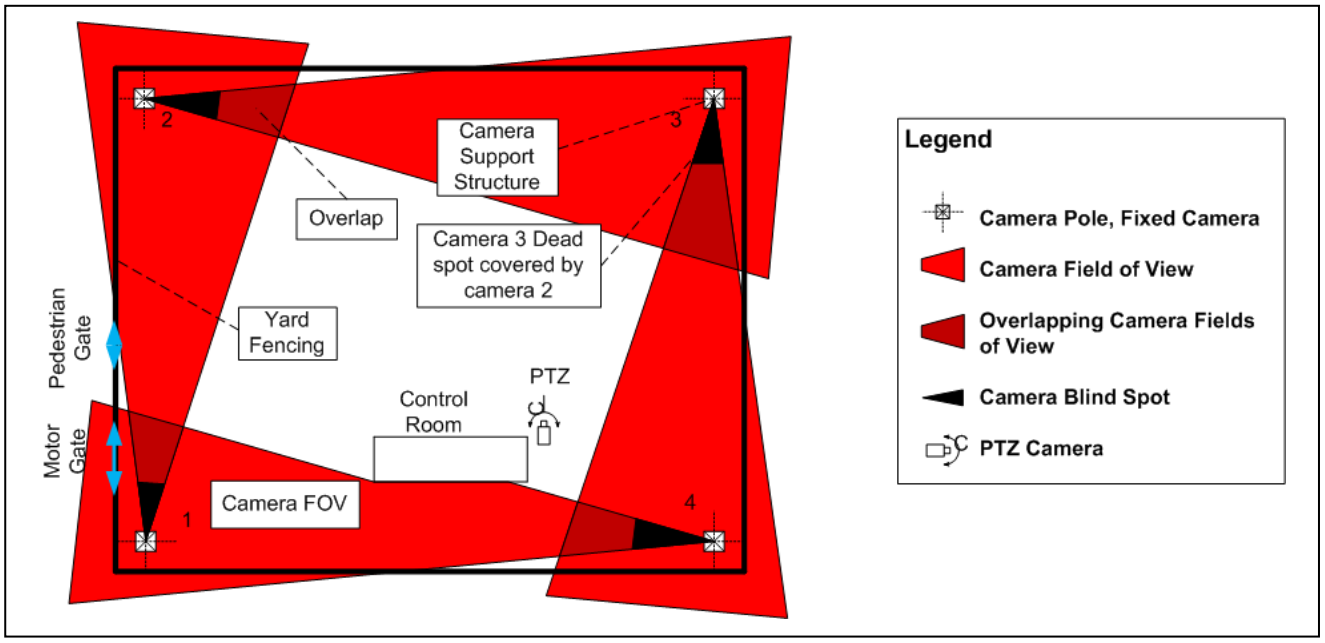


Figure 13: General Layout of Perimeter Camera System bundled with Intelligent Video Analytics for Detection - creates an 'invisible wall' with no gaps

g) There shall be no 'dead spots' in the invisible wall. Where a method of detection has an inherent dead spot, the dead spot of each device shall be covered by another device (e.g. Cameras with overlapping fields of view).

h) The perimeter detection method should be divided into zones matching the areas covered by the perimeter cameras. This shall enable the operators at the security control room to determine which area has been disturbed and which visual to use from the camera covering that section of fence where the incident occurred. Zone names must be the same on site as in the video management system at the security monitoring centre. These zones and zone names shall be reflected on the site layout provided with the system documentation.

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.

i) The perimeter detection system must generate an alarm when a human enters the monitored zone. It must be able to detect a person who is walking upright, walking hunched over, crawling or running.

j) The system must not trigger for the following:

1) Changes in light,

2) Movement of trees,

3) Small vibrations of the camera pole

4) Animals, especially birds (including large birds such as guinea fowl and egyptian geese),

5) Vehicles driving past the substation.

6) Weather conditions including rain, snow and dust storms.

k) The sensitivity of the perimeter detection system must be adjustable in order to configure the system to meet the conditions at specific sites.

l) The system must be able to operate in all lighting and weather conditions.

m) Nuisance alarms shall be limited to 7 nuisance alarms, per site, per 7 day period.

3.9.4 Yard Installation

3.9.4.1 Poles

a) Where lighting poles, buildings, or other suitable structures exist on the site in appropriate positions, these may be used to mount the cameras. If no existing structure is available, the cameras shall be mounted on poles.

b) Poles shall be steel reinforced 4.5m or 5.7m spun concrete poles according to Eskom drawings: D-DT-0010 or D-DT0011. Poles may be purchased on the Eskom ENC (Eskom National Contract) if one is in place at the time.

c) Poles to be installed as per manufacturer instructions so as to minimize vibration due to wind.

d) To prevent theft of cameras, the poles shall not be placed directly next to the fence, and anti-climbing devices shall be considered.

e) The pole shall be earthed via 50 x 3 mm earth tails, the earth tails shall be buried and welded to the base of the fence so as not to be easily visible. The join shall be painted the same colour as the fence to avoid theft of the copper earthing.

f) The earthing shall conform to the latest revision of the general earthing standards of copper joints as per D-DT-5240, sheets 2 and 6 (Annex C and Annex D)

g) Holes required for the fixing of the sensors and cameras may be drilled on-site and shall be appropriately sealed to prevent water ingress. Drilling can be minimised by using equipment that clamp securely onto the poles.

h) Prior to the installation of the support foundation, the stone layer shall be removed sufficiently far enough from where the foundation is to be cast. Any soil excavated from the foundation hole shall not be mixed with the yard stone as illustrated in 14, as it will lower the resistivity of the yard stone, altering the touch and step potentials within the yard and thus increasing the risk of danger to human life.

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.



Figure 14: Exposed soil due to poor workmanship

i) On completion of the installation, all excess soil shall be removed from the yard and the stone shall be replaced to cover the area surrounding the foundation. Any soil exposure due to the yard stone being replaced inappropriately is unacceptable.

j) All cabling be routed through the foundation of the cement pole. Drilled holes shall be kept to a minimum and shall be appropriately sealed to prevent water ingress.

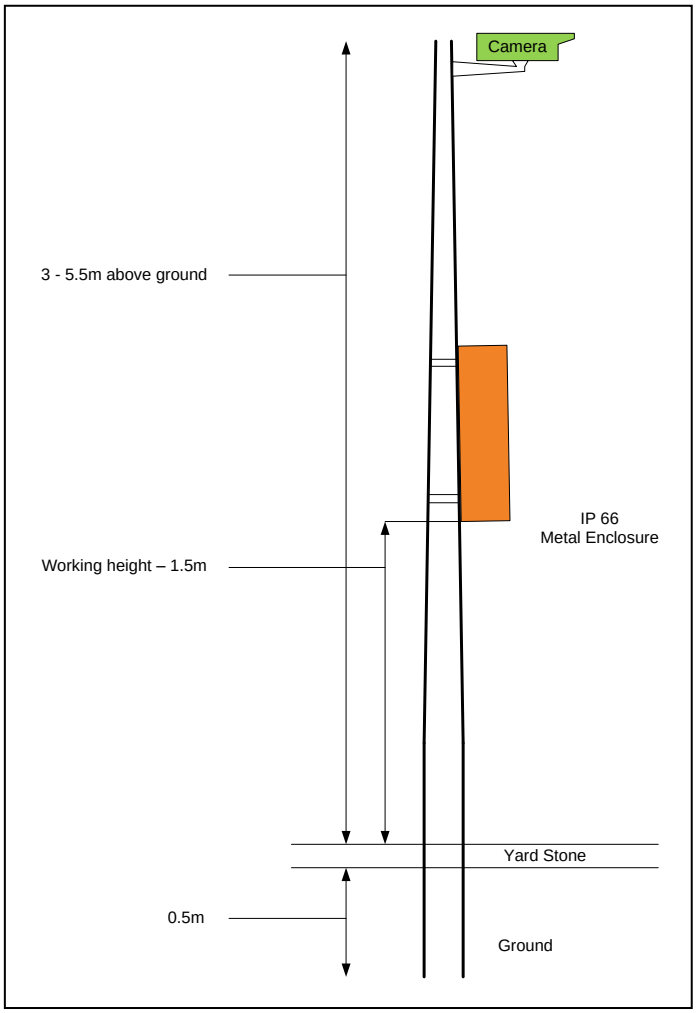


Figure 15: Camera and Metal Enclosure Mounted on Concrete Pole

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.

3.10 CCTV Surveillance System

The subcomponents of the surveillance system primarily consist of fixed perimeter cameras, gate cameras, PTZ cameras, indoor cameras and the security and site lighting. The requirements of each of these subcomponents are specified below. It is recommended that when any design is done, that it be taken into consideration that should the equipment need upgrading, that the existing infrastructure shall be able to incorporate new technologies.

IP or analogue cameras may be used provided they meet the technical and functional requirements specified here.

3.10.1 Camera Purpose

In order to test whether a camera is fit for purpose, it is essential that the purpose of this camera be defined.

The CCTV industry commonly uses specific categories to define the purpose of CCTV cameras. When a site is designed, the purpose of each camera must be clearly identified from the beginning. Table 1 below lists the 4 CCTV categories.

Table 1: CCTV categories

Purpose	Operational Requirement
Identification	Detail should be sufficient to enable the identity of an individual to be established beyond reasonable doubt. Camera footage alone should be enough to prosecute in court.
Recognition	A high degree of certainty whether or not an individual shown is the same as someone seen before. Camera footage could aid in prosecution along with other evidence.
Observation	Be able to observe what a person is doing.
Detection	Sufficient to determine with a high degree of certainty whether or not a person is present.

SANS 10222-5-2 Section 7.7 recommends specific relatives sizes for a human on screen depending on camera purpose, see Table 2 and Figure 16 below.

Table 2: Relative Size of Person on Screen

Category	% Screen Height on 600TVL Camera
Identification	120%
Recognition	50%
Observation	25%
Detection	10%

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.

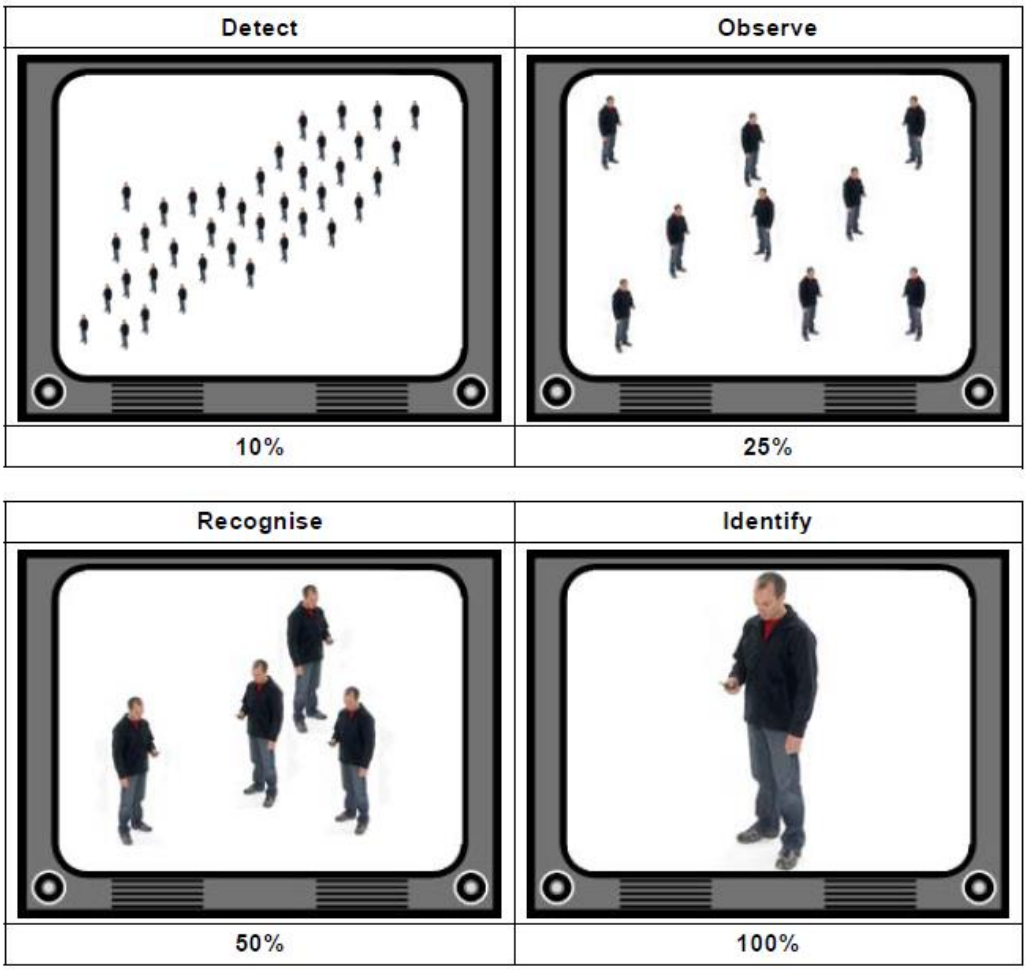


Figure 16: Illustration of CCTV categorisation based on screen height [25]

The functional test for whether a camera meets a particular category is to determine the percentage of the screen taken up by an average human. This can be done using the 1.6m Rotakin test target. The target is placed at the furthest distance that the camera is needed to see, and the percentage of the screen height taken up by the Rotakin on the CCTV display is measured. Where a Rotakin target is not available, a person of average height (about 1.6m) may be used as the test target. An introduction to the Rotakin target can be found in Annex D.

3.10.1.1 Each camera shall have a single, clearly defined purpose

It is tempting to try to reduce costs by using a single camera for more than one function (e.g. positioning a perimeter fence camera so that it can also see number plates at the gate). In practise, this results in a camera which cannot perform either purpose successfully. A single purpose must be stated for each camera and the camera must be tested against this. The purpose should consist of a category (detection, observation, recognition or identification), an area to be covered and a range of distances from the camera.

E.g.

“Camera 1 should detect intruders on the fence perimeter between 5 and 80m from the camera.

Camera 2 should provide identification of persons standing in the doorway.”

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.

Lighting conditions in which the camera should operate should also be stated.

Table 3 shows an example of a table used to log the intended purpose and operational conditions for each camera. All CCTV designs should include a similar table.

Table 3: Example of Camera Purpose and Conditions at a Specific Site

Camera	Purpose	Distance/place	Lighting Conditions
1	Detection of intruders	5m	Outside, some ambient light.
2	Observation of intruders approaching transformer 3	10m	Indoor fluorescent, lights remain on at night.
3	Recognition of intruders entering building	2m	Bright backlighting through doorway.

3.10.2 General Camera Requirements

a) Cameras shall meet all specifications listed in sections:

1) 3.7.3 - Warrantee and Certification

2) 3.7.4 - General Physical Requirements

3) 3.7.5 - General Electrical Requirements

b) Additional requirements for all camera types are listed below.

c) Further requirements for specific camera types can be found in sections 3.10.4 to 3.10.7.

3.10.2.1 General

a) Cameras may be analogue or IP cameras

b) Before installation begins the camera layout, including expected fields of view and dead spots, shall be documented and signed off by an Eskom Engineer.

3.10.2.2 Cables

a) Choice of cables shall be based on camera manufacturer recommendations.

b) Either fibre or electrical signals may be used for camera communication. Cost should be considered when choosing between Cat 5 and fibre communication cables. In high EMF environments CAT6 or fibre should be considered.

c) Where electrical cables are used they should be unshielded twisted pair (UTP) cable, such as CAT5. UTP cabling is cost efficient, has high noise immunity, lower loss per length than coax and allows for high quality long range transmission.

d) For analogue cameras a UTP balun connector may be implemented for the cabling between the camera and the DVR. Cat5 is recommended over coaxial cable as it is thin and flexible cable making it easy to string between walls. Due to its smaller size, more cat5 lines can be run through a conduit than with coax cable. If necessary, active balun connectors may be used to transmit signals over larger distances.

e) Cable selection and routing shall always be done in such a way that operation of cameras is not affected by interference. This may be achieved by separating AC power cables from communication cables, shielding cables, or a combination of the two. It should not be necessary to separate DC power from communication cables. It should not be necessary to separate fibre communication cables from AC power cables.

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.

3.10.2.3 Installation

a) The installation of the camera and brackets shall be as indicated in the manufacturer's guidelines.

b) Brackets used to secure the camera shall be robust and shall minimize vibration.

c) Brackets shall be capable of being "lock tight" to reduce the possibility of accidentally moving.

d) All brackets shall be "cable managed" so that cable entering the housing is enclosed within the bracket from the support to the housing, allowing no cable to be exposed.

e) The cables shall be marked with at least the camera name and number.

f) Dome and PTZ cameras shall be mounted with appropriate brackets which prevent the pole from being in the camera's field of view.

3.10.2.4 Manufacturer Specifications

The manufacturer's specifications for all cameras shall at minimum meet the requirements in Table 4 below.

Note that meeting the minimum requirements 'on paper' does not necessarily mean that a camera can perform as necessary. For this reason the demonstration of equipment (described in section 3.5.3.2) is essential when evaluating CCTV cameras.

Table 4: Minimum Manufacturer Specifications for Cameras

Characteristic	Description	Requirements
1) Automatic Gain Control (AGC)	Automatic gain control (AGC) increases the cameras sensitivity automatically when the ambient light deteriorates.	At least 30dB.
2) Back Light Compensation (BLC)	Electronically compensates for high background lighting to give details which would normally be silhouetted.	Back light compensation must be implemented.
3) Coverage Distance	The distance covered visually between a fixed camera's position and the next camera.	The camera's specified coverage distance shall be 10% further than is required by the site security design.
4) Frames Frequency	The number of frames per second (fps).	Minimum 8 fps
5) Lens	A camera lens is a curved piece of transparent glass that focuses the image in a camera. A camera lens is not a single lens, but a combination of lenses to bend the light entering the camera in such a way that it can be captured.	The lens shall be chosen to suit the application and the functional requirements of the site.
6) ONVIF Compliance	ONVIF (Open Network Video Interface Forum) is an international specification with the aim of 'promoting and developing global standards for interfaces of IP-based physical security products.	If cameras are IP Cameras, they shall be ONVIF compliant. It must however be noted that ONVIF compliance does not guarantee compatibility between systems.
7) Image Format	The approximate size of a camera image detection device.	1/3 inch or larger
8) Remotely Configurable	Ability to change camera settings through a network.	All cameras settings (except focal length and focus) shall be remotely configurable, either via the DVR, or directly using Ethernet.

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.

Characteristic	Description	Requirements
9) Resolution	Resolution determines picture quality. The higher the resolution the better the picture quality.	A minimum horizontal resolution of 600 TV lines or 800 pixels.
10) Signal to Noise Ratio (SNR)	The ratio between useful television signal and disturbing noise signal.	The signal to noise ratio shall be ≥ 52dB.
11) White Balance Control (WBC)	Automatically adjusts a colour camera's colour to maintain white areas.	Camera shall implement wide dynamic range and white balance control functionality to compensate for bright areas.
12) Wide Dynamic Range	Ability of camera to provide clear images when there are very light and very dark areas simultaneously in the camera's field of view.	Camera shall have Wide Dynamic Range

3.10.3 General Requirements for Outdoor Cameras

Outdoor cameras shall meet all specifications listed in section 3.10.2 – General Camera Requirements, additional requirements are listed below:

3.10.3.1 General

a) As far as possible, outdoor cameras shall be positioned “North to South” in order to avoid sunlight on the lens. In some cases this is not possible; therefore all cameras shall have wide dynamic range (WDR) functionality.

3.10.3.2 Cables

a) The power cable shall be steel wire armoured cable.

3.10.3.3 Installation

a) The camera shall be well protected from the elements and vandalism by mounting it within an appropriate housing.

b) The camera housing shall have an IP rating of at least 65.

c) The camera housing shall have a sun visor and be steel constructed.

d) The camera housing shall be weather-proof, environmental, corrosion and vandalism resistant as well as UV resistant.

e) Harsh environments such as coal power plants may require a harsh environment housing. Similarly cameras at coastal sites will need added corrosion protection.

f) If necessary, a junction box with a minimum rating of IP 65 may be installed on the camera support pole. The junction box shall be used to protect any connections and additional equipment necessary for the camera operation. Equipment housed in the junction box should be kept to a minimum; as much equipment as possible shall be housed in the equipment room / relay house.

g) If used, the junction box shall be mounted on the cement pole support, below the camera.

h) If used, the junction box shall be lockable (lock and key, not a panel key) and alarmed.

i) All openings of the housing and junction box, used as well as unused, shall be properly sealed to prevent any water or insects from entering the housing.

3.10.3.4 Manufacturer Specifications

In addition to meeting the requirements of 4, outdoor cameras shall at minimum meet the requirements in 55 below.

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.

NOTE: Meeting the minimum requirements 'on paper' does not necessarily mean that a camera can perform as necessary. For this reason the demonstration of equipment (described in section 3.5.3.2) is essential when evaluating CCTV cameras.

Table 5: Additional Minimum Manufacturer Specifications for Outdoor Cameras

Characteristic	Description	Requirements
Sun Damage Resistance	Resistance of sensor to thermal damage from the sun.	Camera sensor shall be protected from sun damage. Mechanical Shutters are susceptible to failure and will not be accepted.

3.10.4 Fixed Thermal perimeter cameras

3.10.4.1 Introduction

The purpose of perimeter cameras is to provide confirmation of an intruder when an alarm is generated by the perimeter intruder detection system. Since even the best perimeter detection will generate some false alarms, resources can be better managed if intrusion confirmed before armed response is sent to a site.

Since the images from good thermal cameras are not affected by weather conditions (fog, rain, snow), or glare, it is preferred that the perimeter cameras be thermal. It is also preferred that these thermal cameras provide perimeter detection using 'video analytics', either built into, or as an addition to, the perimeter cameras. Other detection methods (or combination of detection methods) may be used if they are able to meet the functional requirements specified here.

3.10.4.2 Specifications

Thermal cameras shall meet all specifications listed in section 3.10.2 - General Camera Requirements, and section 3.10.3 - General Requirements for Outdoor Cameras.

If video analytics on the cameras is used as a method of intruder detection, the video analytics shall meet all specifications listed in 3.9.3 - Perimeter Detection System.

Additional requirements for thermal cameras are listed below:

a) Thermal perimeter cameras shall be installed along the perimeter of the site yard as described in section 3.9.2 above.

3.10.4.3 Manufacturer Specifications

In addition to meeting the requirements of Tables 4, and 5, thermal cameras shall at minimum meet the requirements in Table 6 below.

Note that meeting the minimum requirements 'on paper' does not necessarily mean that a camera can perform as necessary. For this reason the demonstration of equipment (described in section 3.5.3.2) is essential when evaluating CCTV cameras.

Table 6: Additional Minimum Manufacturer Specifications for Thermal Cameras

Characteristic	Description	Requirements
Detector Type	Sensor used to detect thermal radiation	Uncooled micro bolometer
Automatic Gain Control (AGC)	Increases the camera's sensitivity automatically when the ambient heat deteriorates.	Must have Automatic Gain Control
Resolution	Resolution determines picture quality. The higher the resolution the better the picture quality.	At least 320 x 240

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.

Characteristic	Description	Requirements
Thermal Sensitivity	Minimum change in temperature which the detector can differentiate between.	<100mK

3.10.5 Fixed perimeter cameras – non thermal

Fixed cameras shall meet all specifications listed in section 3.7.4 – General Camera Requirements, and section 3.10.3 - General Requirements for Outdoor Cameras.

Additional requirements are listed below:

a) Fixed cameras shall be installed along the perimeter of the site yard as described in section 3.9.2 above.

b) If non thermal perimeter cameras are to be used, the design must explicitly address how the effects of weather will be mitigated.

3.10.5.1 Manufacturer Specifications

In addition to meeting the requirements of Tables 4, and 5, fixed perimeter outdoor cameras shall at minimum meet the requirements in Table 7 below.

NOTE: That meeting the minimum requirements 'on paper' does not necessarily mean that a camera can perform as necessary. For this reason the demonstration of equipment (described in section 3.5.3.2) is essential when evaluating CCTV cameras.

Table 7: Additional Minimum Manufacturer Specifications – Fixed Perimeter Cameras

Characteristic	Description	Requirements
Infrared	Lighting in invisible frequency spectrum used for low-lighting conditions.	Use 850 or 940nm wavelength Distance covered must match application.
Sensitivity	Minimum light level required to get a usable / acceptable video picture.	The minimum sensitivity shall be 0.0002 lux for colour images and 0.00002 lux for monochrome images.

3.10.6 PTZ camera

3.10.6.1 Introduction

The purpose of the PTZ cameras is to track intruders in order to help response teams pinpoint the location of intruders. Intruder tracking can be automatic or manual.

If method of perimeter detection is visual, it is less necessary to have PTZ cameras since the presence of intruders will already have been confirmed visually.

If however perimeter detection is non visual, and there are no corresponding perimeter cameras, then the use of one or more PTZ(s) is recommended if possible.

PTZ cameras are an expensive piece of equipment and should only be installed if it is possible to achieve their primary objective of assisting response teams or onsite security. If communications to the site are over GPRS, then the latency of communications will likely render manual control of the PTZ impossible. In this case automatic tracking and preset positions shall be used. Regardless of the communication medium, the feasibility of using the PTZ shall be tested per site. If it is not possible to control the PTZ effectively to track a suspect, then a PTZ shall not be installed. In this case more fixed cameras can be installed to cover strategic areas.

PTZ cameras should be seen as an optional piece of equipment to be used only where it can add value.

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.

3.10.6.2 Installation

a) One or more PTZ cameras may be installed within the yard depending on the risk and the layout of the site.

b) The PTZ camera shall be positioned in the yard in such a way as to cover the majority of the critical points. Positioning shall be site dependent and shall be informed by the site PSD,

c) In the case where there are no perimeter cameras, the perimeters are the critical points to be covered by the PTZ.

d) Where there are perimeter cameras the critical points to be covered by the PTZ are:

1) Cable trenches,

2) Building Entrance

3) Gate entrances

4) Minisubs, RMUs or Metering Kiosks.

5) Outdoor storage areas

e) The PTZ camera unit shall be installed in one of the following manners:

1) On a 7.2m or 9.1m Eskom approved cement pole (See D-DT-0011& D-DT0012 for guidance). The installation shall be done according to the latest revision of D-DT-0332 (LV and MV Foundation Pole Arrangement).

2) A steel pole attached to a building. SANS 1431 grade 300WA or 4360 grade 43A steel shall be used.

3) A bracket attached to an already installed Eskom lighting mast.

3.10.6.3 Specification

PTZ cameras shall meet all specifications listed in section 3.10.2 - General Camera Requirements, and section 3.10.3 - General Requirements for Outdoor Cameras. Additional requirements are listed below:

a) The PTZ's zooming capabilities shall be powerful enough to meet the purpose of the PTZ

b) The PTZ camera shall be remotely controllable by an operator to pan, tilt, zoom, focus, mobilize the iris, switch the camera on/off and place the camera in a pre-set position.

c) The PTZ camera shall be controlled by a hardwired cable.

d) If there are no perimeter cameras then the PTZ shall be able to see the perimeter by means of thermal imaging or a built in infrared spotlight.

e) The PTZ shall have preset positions. When a preset position is chosen by the controller, the PTZ shall immediately go to that position.

f) Preset positions shall include zoom level.

g) It shall be possible to label the preset positions with a descriptive name.

h) The PTZ shall be capable of having at least 10 pre-sets.

i) Preset positions at each site shall include all gates, doors, various points on the perimeter boundary and high risk assets (trenches, transformers, rolls of cable).

3.10.6.4 Operation

a) It is preferable that the PTZ have built in analytics and be set to 'patrol' the yard during normal operation.

b) If the PTZ does not have analytics then during normal operation it should be set to a useful 'home' position (e.g. gate).

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.

c) When an alarm triggers the PTZ shall zoom into the area where the alarm happened. If a person is detected, the PTZ shall follow the motion of that person.

d) The control signals from an operator shall take preference over the patrol and tracking functions.

e) Preset positions at each site shall include all critical points on the site.

3.10.6.5 Manufacturer Specifications

In addition to meeting the requirements of Table 4, and 5, PTZ shall at minimum meet the requirements in Table 8 below.

Note: That meeting the minimum requirements 'on paper' does not necessarily mean that a camera can perform as necessary. For this reason the demonstration of equipment (described in section 3.5.3.2) is essential when evaluating CCTV cameras.

Table 8: Additional Minimum Manufacturer Specifications for PTZ Cameras

Characteristic	Description	Requirements
Pan Speed	Speed at which the PTZ camera can pan the full 360°	Minimum 6° per second
Pan Range	Angle through which the PTZ can pan	360 º
Tilt Range	Angle through which the PTZ can tilt	Minimum 90º (-10º +80º)
Optical Zoom	Range of focal lengths through which the camera can zoom without reducing resolution	Minimum 3.2mm – 138.5mm (43x) (Site dependent)
Digital Zoom	Maximum that camera can zoom while decreasing the resolution.	Minimum 16x
Light Sensitivity	Minimum light level required to get a usable / acceptable video picture.	The minimum sensitivity shall be 0.0007 lux for colour images and 0.000007 lux for monochrome images.

3.10.7 Indoor Cameras

When deemed necessary by the site risk assessment, indoor cameras shall be used inside building on the site. At substations, indoor cameras shall be installed in control plant rooms and switch rooms.

Indoor cameras shall meet all specifications listed in section 3.10.2 - General Camera Requirements. Additional requirements are listed below:

3.10.7.1 General

a) The camera field of view shall include the entrance to the room/building as the point of interest. Where there is more than one entrance, more indoor cameras may be necessary, as determined by the risk assessment.

b) Indoor cameras may be dome, fixed or bullet cameras

c) Indoor cameras shall have infrared lighting.

d) The purpose of the camera shall be observation and / or identification in the case of forced entry depending on the site requirements. Depending on the bandwidth available it may be appropriate to have observation quality on the live stream and identification quality only on recordings.

e) Backlight compensation with wide dynamic is particularly necessary for cameras looking at entrances. The effectiveness of these features must be tested at time of day when the sun in most directly shining into the entrance. If tests show that the backlight compensation is not sufficient then lighting shall be used to achieve the camera's purpose.

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.

3.10.7.2 Placement and Installation

a) Indoor cameras may be ceiling or wall mounted depending on the site.

b) The camera shall be housed in a vandal proof housing with an IP rating of at least 51.

c) The camera field of view shall be adjustable via an adjustable bracket or built in manual pan-tilt mechanism.



Figure 17: Indoor camera inside room

3.10.7.3 Manufacturer Specifications

In addition to meeting the requirements of Table 4, indoors cameras shall at minimum meet the requirements in Table 9 below.

Note: Meeting the minimum requirements 'on paper' does not necessarily mean that a camera can perform as necessary. For this reason the demonstration of equipment (described in section 3.5.3.2) is essential when evaluating CCTV cameras.

Table 9: Additional Minimum Manufacturer Specifications for Indoor Cameras

Characteristic	Description	Requirements
Day/Night Function	Ability to compensate for poor lighting conditions	Camera shall have day/night function
Electronic Shutter (ES)	Compensates for moderate light changes in indoor applications without the use of auto iris lenses.	Electronic shutters shall be used.
Infrared	Lighting in invisible frequency spectrum used for low-lighting conditions.	Camera shall have infrared.
Minimum illumination	Minimum light level required to get a usable / acceptable video picture.	The minimum illumination shall be 0.0002 lux for colour images and 0 lux for monochrome images.

3.10.8 Digital Video Recorder / Network Video Recorder

a) A Digital video recorder (DVR) or Network Video Recorder (NVR) shall be used to record relevant video footage as well as to allow access to live streaming footage from the security control room. For simplicity, this document uses the term 'DVR' to refer to either a DVR or NVR, since both devices perform the same function.

b) The DVR shall be integrated with the alarms from both the perimeter detection system and the indoor intruder detection system and shall connect to the Video Management System.

c) The DVR shall meet all specifications listed in section 3.7.4 – General Physical Requirements, and section 3.7.5 - General Electrical Requirements. Additional requirements for DVRs are listed below.

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.

3.10.8.1 DVR Functionality

a) In the event of an alarm being triggered (from camera or intrusion detection system) when the system is armed the system shall:

1) Record footage from relevant cameras. Relevant cameras are those with a field of view of the triggered zone and may include PTZ cameras or fixed cameras adjacent to the triggered zone depending on the site.

2) The footage recorded shall be for 5s second before the event triggered, the time of the actual event (however long motion is detected by the camera) and at least a 15 second post event time period. This recording shall be at the full resolution of the camera.

3) Send a signal to the Security Control Room, including the zone that was triggered.

4) Send short video clip / series of still pictures from the camera covering the zone where the alarm triggered to the security control room. This shall be at a resolution suitable for the communication medium used. The quality of the footage received at the security control room shall be such that the controller can clearly identify whether the intruder detection was triggered by a human (detection).

5) Allow for the security control room to remotely access the site in order to stream live footage from the system. This live streaming may be at a lower resolution than the recorded footage, but shall be of a high enough resolution to allow for observation by the controllers.

6) Allow for the security control room to operate any PTZ cameras installed on site, including using pre-set positions.

7) Allow for the controller to speak over the PA system or play a pre-recorded message on site.

b) In the event of movement being detected when the system is not armed, the system shall:

1) Record footage from relevant cameras for 5s second before the event, the time of the actual event (For however long motion is detected by the camera) and at least a 15 second post event time period. This recording shall be at the full resolution of the camera.

3.10.8.2 Compatibility:

a) The DVR shall be able to integrate with a wide range of cameras from different manufacturers.

b) The DVR shall be ONVIF compliant. It must however be noted that ONVIF compliance does not guarantee compatibility between systems.

c) The DVR shall allow for simultaneous use of different model cameras with different resolutions.

3.10.8.3 Recording and streaming

a) It shall be possible to configure the DVR to record on any motion event or only when an alarm event is generated.

b) Simultaneous recording on site and streaming to the security control room shall be possible.

c) It shall be possible to stream video at a lower resolution and frame rate than the footage is recorded on site.

d) Recording: Shall be such that identification can be achieved on cameras with identification as the purpose.

e) All footage shall be time and date stamped

f) It shall be possible to search events and recorded footage based on a combination of date, time, event and motion in a specific part of the camera's field of view

g) The recording media shall be a removable, hot swappable and lockable.

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.

h) All footage shall be kept for a minimum of 30 days. To achieve this, the hard drive size should initially be calculated to be large enough to store 30 hours of continuous recording from all cameras. After 30 days of normal event based operation on site, the hard drive space used shall be checked and the hard drive upgraded if necessary.

i) It shall be possible to 'flag' important footage so that it will not be overwritten.

j) When the hard drive is full, the DVR shall continue to record by overwriting the oldest recordings first. Flagged footage shall not be overwritten.

3.10.8.4 Frame Rate

a) The frame rate shall be adjustable

b) A frame rate of at least 25fps shall be achievable by the DVR

c) Recommended frame rate for streaming video: 2-5 fps

d) Recommended frame rate for recordings: 6fps or larger

3.10.8.5 Video Compression

a) Compression standards such as H. 264, MPEG4 or equivalent may be used for streamed video

b) A compression standards such as MJPEG or equivalent may be used for streamed video

c) Video compression shall be used appropriately such that the specified purpose of each camera (detection/observation/recognition/identification) can be achieved for recordings and streaming of footage (for further information on camera purpose see section 3.10.1)

3.10.8.6 Time Sync

a) The DVR shall enable the syncing of time between sites, and between cameras as specified in section 3.7.12

3.10.8.7 Remote Connections

a) It shall be possible to remotely view live or recorded video over the network (with appropriate access rights).

b) It shall be possible to configure all DVR settings over the network (with appropriate access rights).

c) It shall be possible to download recordings on site or offsite.

3.10.8.8 Video Monitor

a) It shall be possible to plug a Video Monitor into the DVR (site specific)

3.10.8.9 Security

a) The DVR shall be password protected.

b) The DVR shall cater for a minimum of 10 individual users with assigned access rights.

c) There shall be a minimum of 2 access levels:

1) Level 1 shall provide viewing of footage only, with no ability to delete footage or view or change settings.

2) Level 2 shall provide full administrative rights.

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.

3.10.8.10 Hardware and I/O connections

a) The DVR shall have input contacts for connecting to alarm signals from the alarm system

b) It is recommended that DVR have an ‘error’ output which will output a signal to the alarm system if there is an error with the DVR.

c) DVR shall have an on off switch and status LED

3.10.8.11 System Logging:

a) The DVR shall keep a time stamped electronic log of the following:

1) User who has logged in to make changes.

2) Changes made

3) System Errors

4) Interruption of Camera feeds

3.11 Video Management System (VMS)

3.11.1 Introduction

A video management system (VMS) is the software which allows one to view and manage the CTTV cameras at multiple sites. It is the VMS which operators at the security control room will be using to receive alarms from sites, receive short clips of incidents and through which they will connect to remote sites to view live streaming video. The VMS is the central tool to being able to detect and respond to security incidents on site.

3.11.2 Location and Architecture

In regions where an Eskom security control room for remote sites is not available, the security control shall be manned and hosted by a contractor. It is however imperative that Eskom still remains in control of the VMS infrastructure and is not locked into using one service provider indefinitely. For this reason a distributed architecture shall be used for the security network allowing for the VMS system to be used from multiple secure sites. This architecture is illustrated in 18 below.

The network infrastructure shall adhere to the principles laid out in the following Eskom Documents:

a) 240-55410927 - Cyber Security Standard for Operational Technology[7]

b) 240-55683502 - Definition of Operational Technology (OT) and OT / IT Collaboration Accountabilities[8]

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.

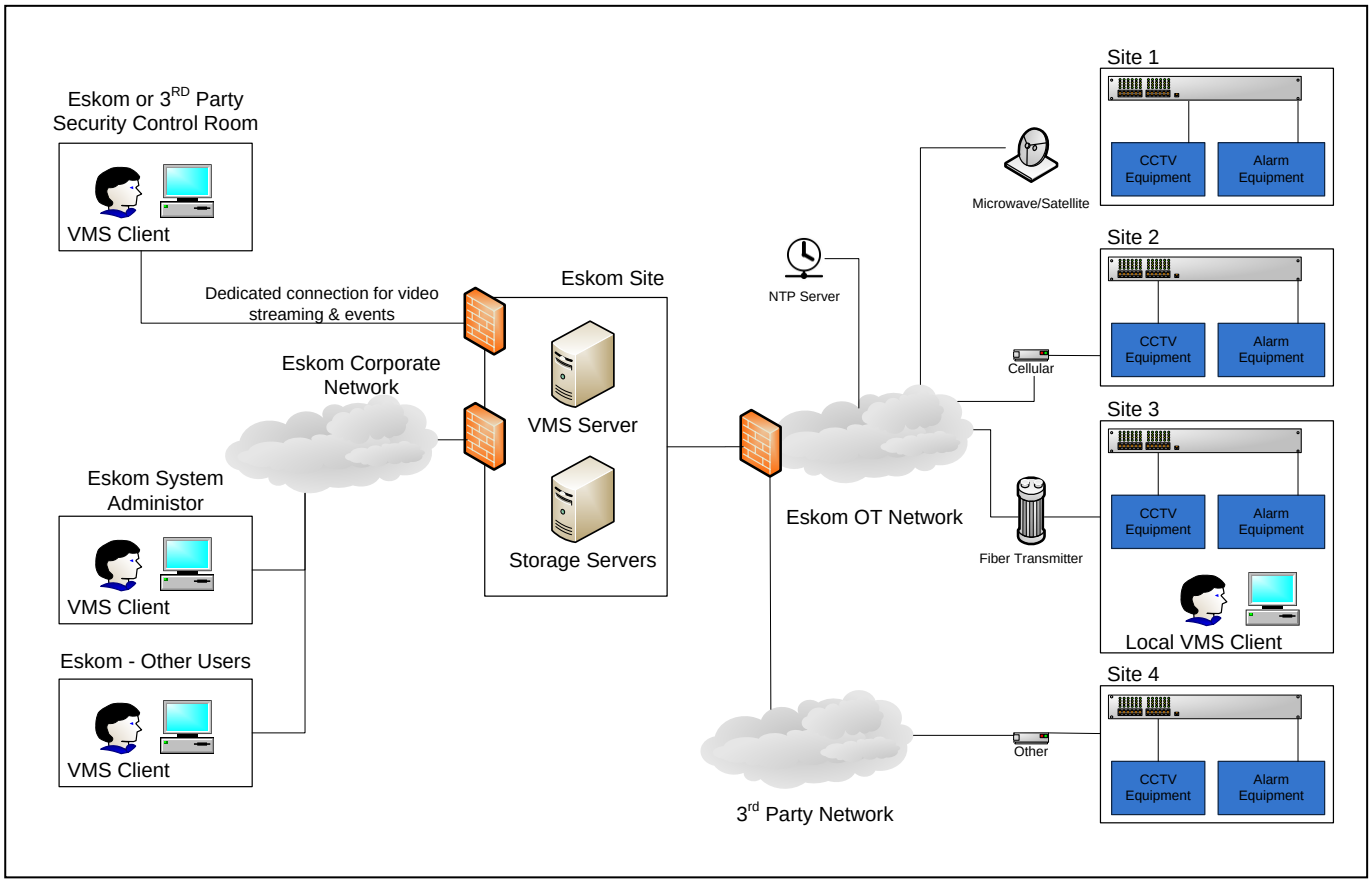


Figure 18: VMS Network Architecture

3.11.2.1 Hosting Server at a Third Party – Exceptional Case

There may be cases where, due to budget, infrastructure or resource restraints, it is not feasible for the server to be hosted by Eskom. In such cases the VMS server may be hosted by a third party.

However the following shall be in place:

a) An agreement with the third party as to who owns the following when the contract expires:

1) Server(s)

2) VMS software license

3) Configuration data

4) Recordings

5) Logs

b) A strategy for moving monitoring of sites to a different third party, or Eskom premises when the contract expires.

3.11.3 Network and Connections

a) The VMS shall connect to CCTV cameras and DVRs via the Eskom OT network, a third party network, or a combination of the two.

b) The VMS shall be capable of a ‘Client-Server’ configuration. The server shall be housed at an Eskom site and the security control room shall connect to the server using client software, over a secure, dedicated link.

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.

c) Authorised Eskom employees using the client software shall be able to connect to the server via the Eskom Corporate Network.

d) The VMS system shall be able to connect to a minimum of 500 sites and 4000 cameras. Not all installations will need this many connections, but it shall be possible to upgrade the system to accommodate these numbers.

e) The VMS design shall cater for failover and allow for a redundant architecture.

f) The system shall allow for at least 5 simultaneous client connections.

g) The frame rate and resolution of camera connections shall be reduced in order to provide smooth footage over the communication medium.

3.11.4 Features

a) The VMS shall be able to connect to a wide range of CCTV NVRs and DVRs.

b) Where there are already CCTV components installed, the VMS shall be compatible with the existing install base of CCTV equipment. As part of the enquiry documentation Eskom shall provide a list of CCTV equipment installed.

c) The VMS system shall be ONVIF Compliant. It must however be noted that ONVIF compliance does not guarantee compatibility between systems.

d) Be able to connect to cameras with a wide range of different resolutions (from CIF (352x240) to 5 Megapixel). Typically the higher resolutions will only be used when monitoring is on site.

e) All security control room activities as described in section 3.12 Security Control Room, shall be possible using the VMS system.

f) The VMS system shall allow for Access Control integration.

g) The VMS shall be linked to an NTP/SNTP timeserver to synchronise the time on the VMS system.

h) The VMS shall be able to operate as a time server to synchronise the times of downstream systems at remote sites.

i) Shall allow an administrator to make customizable reports on events, system status etc.

j) The VMS shall allow the security control room operators to view whether a site is armed or disarmed.

k) It shall be possible to draw up a list of all sites which are disarmed.

3.11.5 Network Security

a) The system shall comply with 240-55410927: Cyber Security Standard for Operational Technology which serves to guide the implementation of Cyber Security principles in the OT environment

b) All connections to the Eskom OT networks shall be firewalled as per 240-79669677: Demilitarised Zone (DMZ) Designs For Operational Technology

c) All connections to the Eskom corporate network shall be firewalled and approved by Eskom Group IT.

d) Remote Access to the Eskom network shall adhere to 32-273: Information Security – IT/OT and Third Party Remote Access Standard.

e) The Engineering design shall follow both IT and OT governance processes as per 240-55863502: Definition of OT and OT/IT Collaboration Accountabilities.

f) The VMS shall allow for individual, password protected user rights.

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.

g) There shall be a minimum of 2 access levels:

1) Level 1 shall provide viewing of footage only, with no ability to delete footage or view and change network settings.

2) Level 2 shall provide full administrative rights.

h) The system shall keep a time and date stamped log of all logon events

i) The system shall keep a log of all administrative changes made on the system, including who made the change.

3.11.6 Video Recording and Streaming

a) The primary purpose of the VMS shall be to view live footage. Due to network constraints the primary place for saved recordings shall be on site. However, for investigation and training purposes, it shall be possible for the VMS to record footage which has been streamed to the security control room and to export that footage.

b) The VMS shall support simultaneous recording and streaming of footage.

c) The VMS shall support streaming at a wide range of resolutions, depending on the network bandwidth and the camera being connected to.

d) The VMS shall enable different client workstations to stream from different cameras simultaneously.

e) The VMS shall enable a continuous streaming ‘video wall’. This shall be customizable, allowing for resizable viewing panes.

f) The VMS shall support recording and playback of files using H.264, MPEG and MJPEG video compression

g) The VMS shall be able to trigger recordings based on: Schedule, Manual trigger, alarm, event

h) Be able to stream and record using various frame rates (8fps -25fps). Typically the higher frame rates will only be used for live footage when monitoring is on site.

i) The VMS shall be able to use a wide range of different communication links to different sites. This will range from poor 3G connections, to high latency satellite, to fibres. It shall be possible to cater for different frame rates and resolutions per site depending on the bandwidth and cost of the communication medium.

j) All recordings shall be electronically watermarked and show time and date.

k) It shall be possible to search events and recorded footage based on a combination of date, time, event and motion in a specific part of the camera’s field of view

l) Playback in slow motion and at high speed shall be possible.

m) The player shall allow for multichannel playback, which allows users to play recorded video from several cameras simultaneously. This is useful if tracking suspects moving on a site.

n) The system shall be able to perform mass export of archived footage.

o) It shall be possible to ‘cut’ footage to export only the portion of footage that is of interest

p) As a guideline, the system shall cater for at least 7 days of continuous recordings from each of the security control room monitors, streaming from 5 of the highest frame rate and resolution cameras installed.

Example

The security control room has 2 people monitoring sites from separate workstations. The highest resolution cameras installed are 1Mpx cameras streaming at 10fps

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.

Calculation

Determine file size of 1 hour of footage: Either record an hour of footage, or use one of the many 'CCTV file size calculators' available online.

Approximate size of 1 hour of footage in H.264 = 1.5G

Approximate size of 7 days of footage: 252G

Approximate size of 7 days of footage for 5 x 1Mpx cameras = 1.26T~1.25T

So, for two monitoring stations you will need 2.5T of hard drive space.

a) It shall be possible to 'flag' important footage so that it will not be overwritten.

b) When the hard drive is full, the oldest recordings shall be overwritten first. Flagged footage shall not be overwritten.

3.11.7 Event Management

The VMS shall:

a) Support 'black screen monitoring': In normal state, no video is shown. When an alarm triggers at a site the controller sees a series of still images or a short video clip of the zone where the alarm was triggered. The controller can then choose to stream video from the site.

b) Support an event queue to allow the management and acknowledgment of multiple alarm events.

c) It shall be possible to look at a new event without having acknowledged a previous event.

d) Support PTZ control including PTZ pre-set positions.

e) Allow the transmission of voice from the controller to the PA system on site.

f) Allow for the controller to control lights at the site.

g) Allow controller to view the location of alarms and cameras on a site layout

h) Allow controller to view the location and status of all sites on a map

i) Enable comments from controller to be linked to an event.

j) It shall be possible to 'escalate' incidents to another workstation running the client software e.g. another controller or an Eskom National Security Control Centre.

k) Log events and actions for auditing purposes

l) A highly recommended feature is the ability of the VMS system to track movement and highlight which area of the camera field of view has triggered an alarm (This could be software based or a feature of the cameras or video analytics on site).

3.11.8 Usability

The VMS system shall have high usability (be 'user friendly'). Usability is a difficult thing to quantify but can be broadly defined as consisting of [26] :

a) Learnability: How easy is it for users to accomplish basic tasks the first time they encounter the design?

b) Efficiency: Once users have learned the design, how quickly can they perform tasks?

c) Memorability: When users return to the design after a period of not using it, how easily can they re-establish proficiency?

d) Errors: How many errors do users make, how severe are these errors, and how easily can they recover from the errors?

e) Satisfaction: How pleasant is it to use the design?

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.

Before choosing a VMS system Eskom shall view a demonstration of the VMS product. The service provider shall be able to demonstrate all of the features specified above, this shall include administrative tasks as well as security control room tasks. The evaluator(s) shall use the system themselves as part of this demonstration rather than simply being shown the system in operation.

3.11.9 Hardware

a) Server shall meet Eskom IT requirements for servers including:

1) An HP server shall be used

2) Server shall be 19” rack mountable

3) The operating system shall be Window Server 2008 r2

4) Symantec antivirus shall be installed (can be provided by Eskom IT support)

5) Server shall connect to Eskom IT servers for antivirus and Windows security updates.

b) Server shall meet with the VMS manufacturer’s hardware requirements.

c) Server shall be housed in a secure, access controlled environment.

3.11.10 Training and Support

a) There shall be local support for the VMS product.

b) Product support in the closest City to the installation

c) The tenderer shall provide Eskom with details of their support network as well as the service levels in terms of turnaround time to attend to technical problems.

d) Operator and administrator training shall be provided

e) Documentation on the hardware installation shall be provided (see section b)

f) Instruction manuals shall be provided (see section b)

3.12 Security Control Room

The CCTV surveillance shall be monitored by Eskom staff or an Eskom approved security company located within a secured central security control room. The security control room shall be equipped such that the security control room operators shall, for each site, be able to:

a) Select each individual camera within the site to view footage from the respective camera.

b) Operate additional lighting installed.

c) Select a program to sequentially switch the cameras.

d) Operate the zoom, pan and tilt throughout the complete range of each PTZ camera installed.

e) Operate the PA systems installed in the respective sites.

3.12.1 Security Control Room Operators

While the system equipment may perform optimally, any failure on the operator’s part will lead to a performance degradation of the entire CCTV surveillance system. When selecting security control room operators there are various skills that need to be taken into account.

a) The security control room operators shall have the ability to work under pressure, have vigilant capabilities and maintain the ability to perform under widely fluctuating work levels.

b) Operators should be well trained so that they are fully conversant with the use of all items of equipment and are able to deal with any operational circumstances that might confront them.

c) Operator training shall include coping with equipment malfunction.

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.

d) Operators shall be trained to operate the remote PA system.

e) Operators shall be trained in the verbal procedure to be followed when addressing an intruder via the PA system.

f) The functions of security control room operators shall include being able to operate each camera in order to:

1) Obtain individual camera views as well as the duration.

2) Make adjustments to attain the appropriate lighting for the specific camera.

3) Select a program to sequentially switch the cameras.

4) Operate the pan-and-tilt and zoom applications throughout the complete range, where fitted.

5) Use the on screen menu with crisp, sharp images that do not deteriorate with usage or downloading.

3.12.2 Records

For record purposes, the security control room shall have a maintenance/repair logbook. This logbook may be software based or paper based. The security control room operators shall record the following in a chronological order:

a) Date and time.

b) Fault specific details.

c) Fault notification to responsible Eskom employee.

d) Any re-notification.

e) Commencement date and time of repairs / inspections / maintenance.

f) Completion date and time of repairs / inspections / maintenance.

g) Signature of responsible Eskom employee, next to each new entry.

h) Replacement spares required and installed.

i) CCTV and intruder detection equipment maintenance contractor attendance log details for routine and breakdown maintenance.

j) The language medium shall be in English.

3.13 Legal and Evidentiary Aspects

During an incident investigation, the visual footage captured by the CCTV surveillance system is of crucial importance regarding the investigation. The following protocols in the handling of recorded visual footage or other material that has evidential value shall be adhered to.

3.13.1 Overview

The rules of law governing litigation and the proof of facts are the Law of Evidence. Substantive law lays down what has to be proved, the rules of evidence relate to the manner of proof. The law of evidence is part of the common law and has not been codified. In terms of the Criminal Procedure Act, 51 of 1977, the law of evidence in South Africa consists of English Law as it existed on 30 May 1961, except as amended by statute and interpreted by the courts.

For purposes of the admissibility of CCTV the statutes relating thereto are:

a) Criminal Procedure Act, 51 of 1977;

b) Law of Evidence Amendment Act, 54 of 1988;

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.

c) Electronic Communications and Transactions Act, 25 of 2002;

d) The Constitution of South Africa

3.13.2 Application

Of these acts the Electronic Communications and Transactions Act is applicable to computer generated evidence and therefore the admissibility of CCTV. The following is pertinent to CCTV evidence and shall be adhered to by any person handling any evidence to be used in a court of law.

a) There are no specific rules or legislation dealing with admissibility of video recordings.

b) Video recordings are admissible and the court will determine what weight should be attached to this evidence.

c) Digital images are readily subject to alteration, more so than with analogue recordings. The court will therefore scrutinise the evidence with a great degree of circumspection.

d) It is of paramount importance that the original recording is safeguarded (tag and bag procedure for master copy) and produced for the court's inspection as proof that the evidence was not tampered with.

e) The chain of evidence from original recording to production in court must be well-documented and the witnesses available to testify.

f) All enhancements, screen-grabs or stills should be able to relate to the original recording, but should not be made from the original. All computer- related work should be done from copies; the original is to be kept solely for the court as the master copy.

g) Only suitably qualified experts in the field of computer-generated images can be allowed to work with the copies and testify in court.

h) The court will make the final judgment on the weight to be attached to the videos, not the experts. Authentication is required to demonstrate that the evidence is what the proponent claims. Authenticating a traditional picture typically includes testimony regarding the basis of the witness' knowledge of the scene depicted; that he or she recognizes the scene in the video or DVD, and that it is a true and accurate depiction of the scene at the relevant time. Assuming there are no other bars to the admission of the picture, it should be admitted into evidence.

3.13.3 Rules applicable to digital images

The use of digital cameras and images for evidence are regulated by the Electronic Communications and Transactions Act 25 of 2002. It is essential to establish a reliable chain of custody in order to demonstrate the integrity of images to be introduced as evidence. The chain of custody shall be the personnel monitoring and controlling the CCTV surveillance and intruder detection system at the security control room. The chain of custody shall be able to prove:

a) How the data images were captured.

b) When, where and how the images were stored.

c) Who had access to the data images from the time they were captured until introduced as evidence.

d) Any details on whether or not the data images had been enhanced and how.

e) The personnel shall be able to provide evidence of the integrity/authenticity of physical evidence, from the time of its recording until it is presented.

Anyone who handled any physical evidence, even momentarily, may be called to testify as to when, where, and from whom it was received; what was done with it; to which it was surrendered, and the specific time and date and the reason therefore.

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.

The longer the chain of custody, the greater the risk. Any disruption in the chain of custody may cause evidence to be rejected. Even if it is admitted, a disruption can weaken or destroy its probative value. It is thus very important to stress the need to furnish proof of the exact location evidence was found and its condition throughout all the processes until being presented. This is essential in the event of a dispute concerning the value of evidence. The chain of custody shall include proof of the following:

a) The evidence being submitted is the same as that captured.

b) The absence of any opportunity to alter or replace evidence.

c) Any changes in the condition of evidence (exhibits) can be rationally explained.

3.13.4 Procedures when handling evidence

a) Security personnel shall take steps to help ensure that evidence will be admissible in a court of law.

b) Security personnel shall rely on standard protocols and operating procedures to ensure that all image evidence, digital, photographic or video will be handled in the same manner.

c) Image handling procedures shall be standardized and access to digital images shall be strictly controlled.

d) Original digital images shall always be preserved in their original format by saving the image on a hard drive, a CD or with image security software.

e) Should a photograph be enhanced for investigation or demonstrative purposes, the enhanced image shall not replace the original, but shall rather be saved as a separate image.

3.13.5 Physical handling of Storage Media

3.13.5.1 Handling

The persons involved in handling any video footage stored on storage media (DVD, CD, flash drive or other) shall be:

a) The person in control of the data capturing and storing system.

b) The Investigating Officer (IO).

c) All other authorized persons having custody of the original recorded evidence.

3.13.5.2 Procedures

a) Immediately after an incident, the media shall be extracted by one authorised user of the system, in the presence of the IO.

b) If it is impracticable to have copies made first, the images shall be shown to the IO.

c) The IO must formally seize the media in terms of the section 20 of the Criminal Procedure Act (Act 51 of 1977).

d) Immediately after copies have been made of the media, both the original and/or further duplicates shall be “bagged and tagged”. Special evidence bags approved by the SAPS shall be provided for this purpose.

e) The original recording shall be kept in secure and safe custody as an exhibit for evidentiary purposes only.

f) Two duplicates of the original media shall be made/downloaded, one for investigative purposes and one for safekeeping by Eskom.

g) Selected images may be printed for investigative purposes.

h) It is advisable that two persons be present at the making of duplicates and/or prints for corroboration.

i) Duplicates shall be made on “read-only” media, as this will ensure that it cannot be altered.

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.

j) The original recording shall be kept in a safe to which there is restricted access. Any handover or changes to custodian(s) must be recorded in the security logbook and in affidavit form when required (See Annex E)

k) Any custodian of data evidence shall ensure that his/her statement is taken by the investigator.

l) Care shall be taken that potential witnesses do not gain access to images.

3.13.6 Information for Eskom

A copy of data recorded of any criminal incident shall be forwarded to the appropriate Eskom personnel. Its shall be placed in a separate envelope, marked as prescribed and accompanied by a covering letter/note with the following information

a) The relevant SAPS case Number.

b) A full description of the crime incident, e.g. Armed Robbery, Attempted Armed Robbery, Burglary, etc. date, time and place.

c) The rank and name of the investigating official, including his/her telephone and fax number.

d) A brief summary of the incident, including all relevant facts considered necessary for the accurate analysis of the details such as similarities with other incidents, etc.

e) A full description of all other exhibits, the way it was marked, packed and sealed.

3.13.7 Period for which day-to-day data shall be preserved

Day to day image recordings shall be kept for a period of 30 day, bearing in mind the prescription of three years for civil claims. Copies of recordings of incidents picked up from the 30 day database shall be kept for at least three years or as long as required for legal proceedings.

3.13.8 General evidentiary requirements

The following are requirements to avoid pitfalls in retaining the integrity of physical evidence:

a) The least possible number of authorised persons shall handle evidence.

b) In the event of evidence being taken from the charge of the investigator, full particulars of the person taking it, the date and time, the reason and the person returning it on a specific date shall be recorded.

c) Full particulars of all persons handling the exhibit shall also be recorded (names and identity numbers).

d) A written letter of acknowledgement shall be obtained from the recipient.

e) All media items of evidence shall be uniquely “bagged and tagged”.

f) Marks of identification shall not be made on the exhibits as it can influence the evidential value thereof. The best way to mark the items is by tagging, labelling or placing the items into a container and then marking the container.

g) Should there be more than one exhibit (media), it shall all be separately “bagged and tagged”.

h) Precautionary measures shall be taken to prevent media from getting mixed-up. Annotations shall also be made of who found the exhibit, and where and from which recording device it was extracted.

i) Media shall be protected from exposure to harmful conditions.

j) Any apparent tampering shall be recorded and brought to the presiding officer’s attention.

k) Statements shall be obtained from the supplier and/or installer of the CCTV system covering the requirements of section 15 (3) of the ECT Act (23 0f 2002).

l) Any person who prints a photograph from digital media shall, in affidavit form, state that the photograph is a true reflection of the data contained on the electronic media, and the affidavit shall accompany the photographs.

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.

m) In order for the SAPS to view evidence, the footage has to be saved in a format that can be opened in Adobe Photoshop Premier.

n) Discreet timeslots have to be identified on the specific media, indicating exactly when the incident took place to avoid unnecessary time wasted on searching for such incidents.

3.13.9 Pro-Forma Statements

Any enhancements required should be restricted to experts, who should testify to this regard. Pro-forma statements from such experts can be taken and submitted to court and they only have to testify when required by the court.

3.14 Operation

3.14.1 Standard Operating Procedure

Standard operating procedures (SOP) shall be drawn up in consultation with Protective Services and Group Security in order to determine how the system will be used and by whom.

Activities which shall be covered by standard operating procedures shall include:

a) Procedure for security control room to follow on receiving an event

b) Procedure to be followed when collecting video footage to be used as evidence

c) Procedure to be followed to report and address faulty CCTV equipment

d) Procedure to be followed when making changes to the CCTV system

3.14.2 Continuous Improvement

Installed equipment is still only a tool to be used by people and will not add value unless the people operating the equipment are able to use it effectively.

For this reason simulated incidents (dry runs) shall be done on a regular basis. The frequency of these shall be determined in consultation with Eskom Group Security. The intention of the simulated incident is to:

a) Test the SOP

b) Test the competence of people involved in response

c) Test security control room and armed response

d) Identify actions for improvement. These may include:

   1) Changing the SOP

   2) Providing More Training

   3) Changing how system operates

   4) Changing the equipment being used at this or future installations.

   5) Changing service provider

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.

3.15 Maintenance

3.15.1 Introduction – Maintenance Contracts

a) All installations shall be accompanied by a 1 year maintenance contract.

b) After this 1 year period one of the following must be in place:

1) A maintenance contract with a supplier

2) A maintenance plan for Eskom to do maintenance work.

3.15.1.1 Routine First Line Maintenance – CCTV SystemFrequency

Each site shall receive routine site maintenance 4 times per year (approximately 3 month's interval between services).

There may be cases where this quarterly maintenance is not achievable (e.g. substations in remote areas). In such a case the routine may be adjusted as follows:

a) A subset of the maintenance tasks may be carried out by non-security staff during other regular maintenance (e.g. at a substation, the CNC could add the dusting of the camera lenses to their list of monthly maintenance activities).

b) The frequency of extensive first line maintenance may be reduced to bi-annually or annually.

c) The results of the monthly VMS tests (b) shall be used to indicate the necessity for re-active maintenance.

3.15.1.2 Procedure

A maintenance schedule and procedure shall be drawn up and followed. This schedule shall be a combination of all of the following:

a) The maintenance schedule provided by the CCTV system provider (see section 3.5.7c).

b) Eskom document 34-1430 - Procedure for First Line Maintenance of Security Systems at Substations [9] Sections 5.2.10 - CCTV, and 5.2.5 – Floodlighting.

c) Additional Maintenance activities:

1) Functional test of all equipment on site, including signals to and from the security control room.

2) Adjustment of equipment (especially cameras) where necessary

3) Cleaning of equipment

4) Inspection for wear and tear

5) Applying any Eskom approved firmware updates or settings changes.

3.15.1.3 Remedial Actions and Documentation

a) Any equipment, etc. failures must be immediately reported to Eskom.

b) All routine maintenance shall be documented and these records shall be held by Eskom for a minimum of 3 years.

c) Annex B has an example of a typical quarterly site maintenance check list

d) On completion of each inspection and maintenance service, the contractor shall present, for the customer's signature, an acceptance certificate which will be a condition for invoice payment.

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.

3.15.2 VMS System Maintenance

a) Regular update of antivirus and operating system on the VMS server shall be done either automatically or manually (automatic is preferred).

b) The security control room shall conduct a comprehensive maintenance check on the entire system once a month. At each site it should be confirmed that:

1) All cameras can be connected to

2) Footage can be streamed from site

3) The picture quality is acceptable for security control room operation.

4) PTZ cameras can be controlled from security control room

5) Lights can be activated from security control room

c) A monthly report will be presented to Eskom security services on an agreed date each month stating the health of each site.

d) Any equipment, etc. failures shall be immediately reported to Eskom.

3.15.3 Ad hoc Maintenance (Faults)

a) All equipment identified as faulty shall be brought to the attention of Eskom.

b) There shall be a clear, documented, process for reporting faults on the security system, including expected timelines and names of responsible people.

c) Response will be required on the same day unless otherwise negotiated.

d) In the case of an emergency, meaning a situation with life threatening consequences or situation that will cause damage to property or equipment, Eskom representative will state clearly that this is an “Emergency situation and immediate response will be required.

e) The service provider can as part of the contract render a repair service of faulty equipment at a rate & condition submitted. This process will be finalised at the contract awarding stage.

f) On arrival at site, the contractor’s field staff will first report to the contractor’s security control centre and Eskom representative on site if applicable.

g) Once the repair or replacement is completed, relevant Site Acceptance Tests shall be conducted and documented before the work shall be signed as accepted by Eskom (see Section 3.16.4).

h) On completion of each inspection and maintenance service, the contractor shall present, for the customer’s signature, an acceptance certificate which will be a condition for invoice payment.

i) Equipment replaced on site remains the property of Eskom and this original (broken) equipment must be returned with the invoice for these services. Payment of this invoice is thus subject to compliance.

j) All equipment that fails within the warranty period will be replaced at the contractor’s expense.

k) All equipment replaced will have a new full warranty period as with the original installed equipment.

l) Equipment repaired will have a pro rata warranty as agreed to upfront – at tender award stage.

3.16 Testing

3.16.1 Introduction

As discussed in the Design and Installation Process Overview (section 3.5), it is imperative that the CCTV system be thoroughly tested to ensure that it meets the functional requirements of the site. This is important for a number of reasons:

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.

a) A large number of different pieces of equipment need to interface with each other to achieve the specified functions.

b) Each piece of equipment can be configured in a variety of different ways depending on the objective.

c) It is impossible to know how a CCTV system will perform based on manufacturer's specifications alone; a field test is needed to be sure that each camera can provide the visuals required.

It is also prudent to identify any non-conformances as early in the design and installation process as possible. For this reason a number of functional tests shall be performed at various stages of the design and installation life cycle.

As introduced in the installation process discussion (section 3.5), the various testing phases which shall be implemented are:

- Tender Demonstration Tests
- Factory Acceptance Tests
- Tests during Commissioning
- Site Acceptance Tests

The most comprehensive of these testing phases shall be the Site Acceptance Test. The process for all preliminary testing phases shall be adapted from the final Site Acceptance Test. What follows is a description of each phase and how it shall be adapted from the Site Acceptance Test. The Site Acceptance Tests to be carried out before site handover are then discussed in detail.

3.16.2 Tender Demonstration Tests

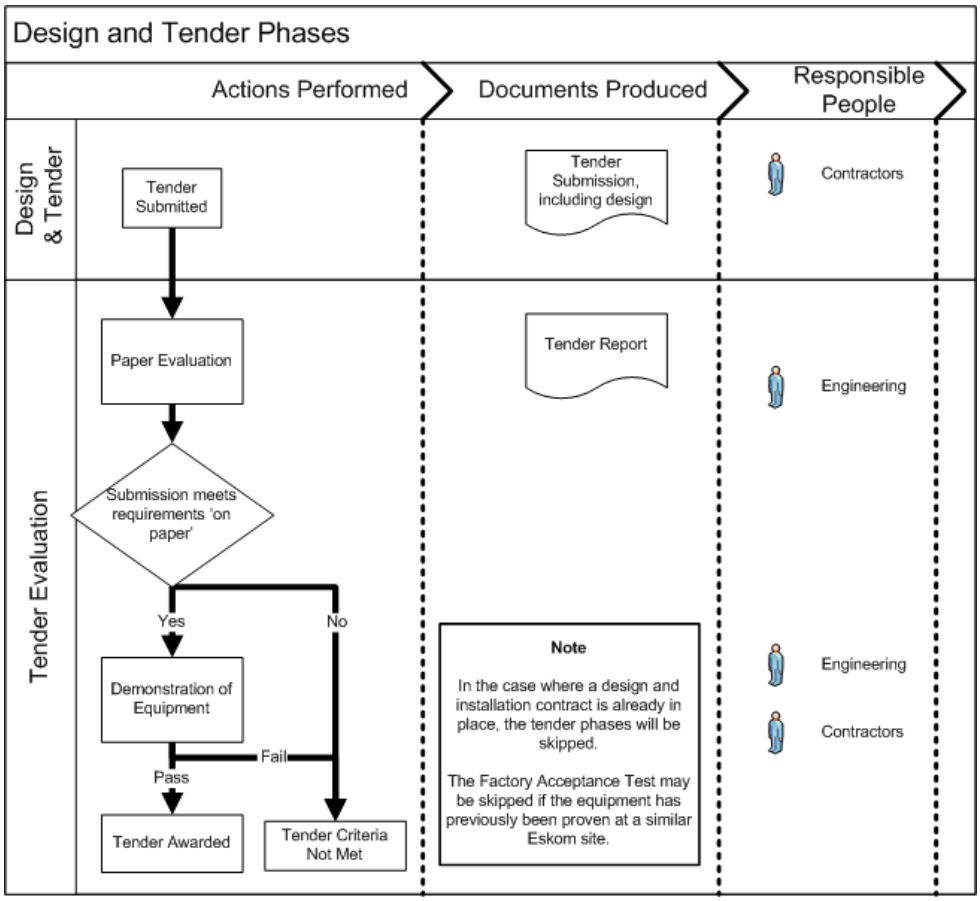


Figure 19: Design and Tender Phases

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.

3.16.2.1 Introduction

In order to evaluate a tender submission, one needs to evaluate the equipment put forward in the tender. All tender submissions shall first be subject to a 'paper evaluation'. If the proposal meets the requirements 'on paper', then the company who submitted the tender shall then arrange a demonstration to demonstrate how the system will meet these requirements. This is particularly important for cameras, since the same description could be very differently implemented by two different suppliers. For example two cameras might both have back light compensation, but one may produce a better image than another in backlit conditions (See 20 below).



Figure 20: Comparative Effectiveness of Backlight Compensation of Different Cameras [27]

3.16.2.2 Testing Procedure

The purpose of testing at the tender phase is to test whether the equipment proposed is capable of meeting the specifications. To this end, each piece of equipment needs to be demonstrated to meet the functional requirements. These tests need not be carried out on site. They may be carried out on equipment already installed on a 3rd party site by the tenderer or setup for demonstration purposes. Before the demonstration, the tenderer will be given details of the tests to be performed. The test should be based on the proposed design. For example company A proposes using camera x to cover a distance of 100m. Company B proposes that camera Y be installed every 50m to cover the 100m distance. Camera X will therefore be tested to a distance of 120m and Camera Y to a distance of 60m.

3.16.2.3 Evaluation

If a piece of equipment/system does not pass a test, the demonstrator will be allowed to retune/reconfigure the stem/equipment. If, when retested, the system still fails, the equipment shall not be retested.

3.16.3 Factory Acceptance Tests

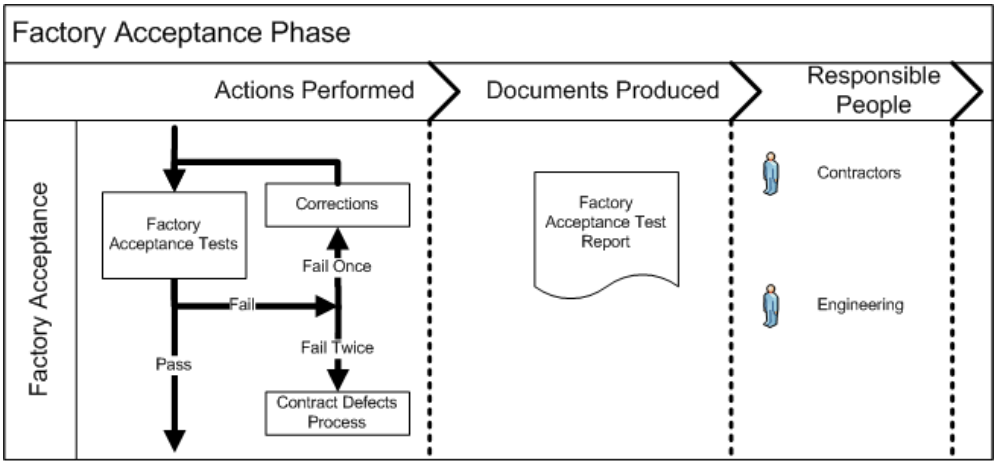


Figure 21: Factory Acceptance Phase

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.

3.16.3.1 Introduction

Factory acceptance testing helps to save time in the field by ensuring that equipment is correctly configured, before taking it to site. This is especially important when implementing a new design. Although the system was tested at tender stage to check that individual components can meet the spec (sensor A generates an alarm when intruder detected; Camera A can record at X frame rate), the system as a whole will now be tested (When sensor A is triggered, a signal is sent to the DVR which starts to record the feed from Camera A).

3.16.3.2 Testing Procedure

The supplier will be required to show that the equipment (which has not yet been installed) has been configured and connected in such a way that the functional requirements can be met.

3.16.3.3 Evaluation

If a piece of equipment/system does not pass a test, the supplier will be allowed to retune/reconfigure the system/equipment. If, when retested, the system still fails, the supplier will be allowed to make minor redesigns / equipment changes where necessary (subject to governance procedures). If, after redesign the requirements can still not be met, the non-conformance process shall be followed [14]. This may ultimately lead to the cancellation of the contract.

3.16.4 Site Acceptance Tests

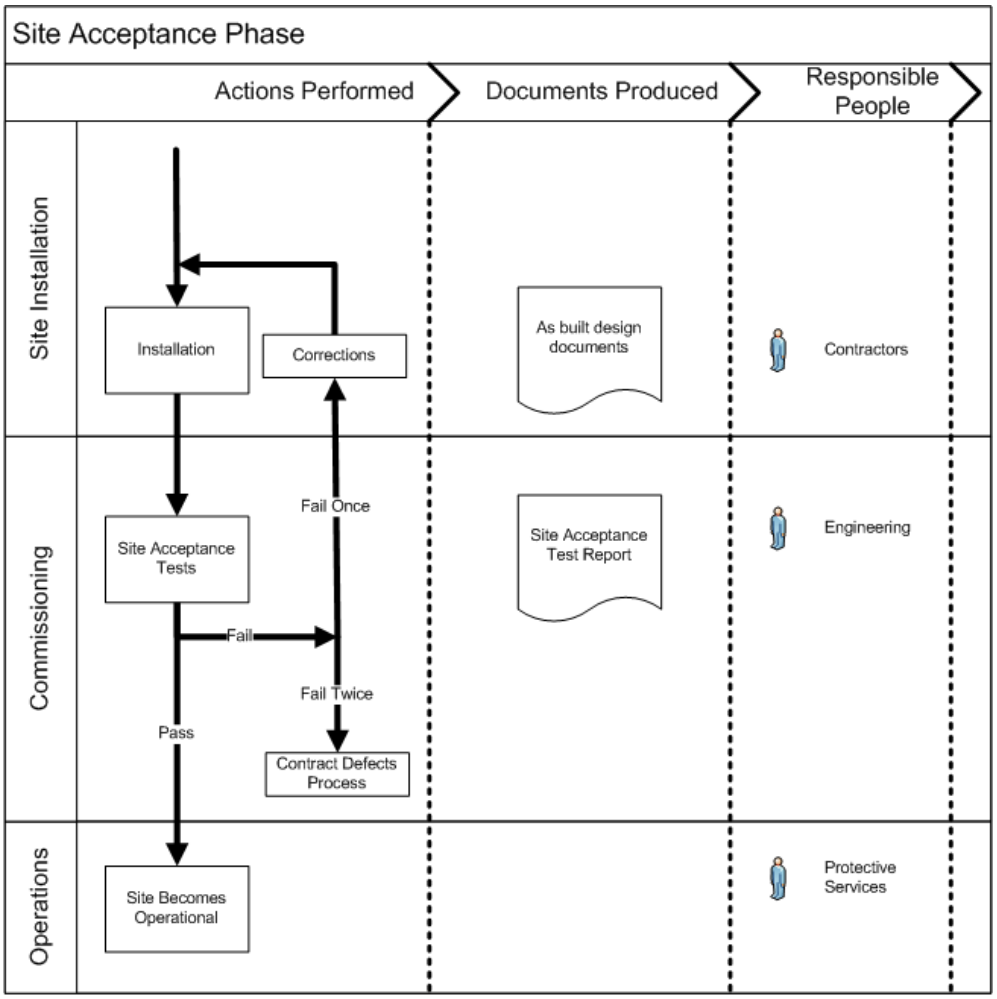


Figure 22: Site Acceptance Phase

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.

3.16.4.1 Description

In order to ensure that all aspects of the CCTV and intruder detection system are thoroughly evaluated and tested, it is required that the acceptance test procedure (ATP) as stipulated below shall be performed for each of the components / functionalities. The system will only be accepted once the required test is passed successfully for each respective component / functionality described in the ATP. For each test performed, there is a qualification table that shall be filled in (See Annex F). Based on the results in the qualification table, the component / functionality shall be deemed acceptable or not.

The Project Manager and / or duly appointed representative, may inspect and test the various portions of the work at any time and shall have full power to reject all or any portion of the work considered to be defective or inferior in quality of material, workmanship or design. The appointed contractor shall replace any portion of the work so rejected immediately, unless in the opinion of the Project Manager, the work rejected can be so treated and repaired as to render it fit for incorporation in the system.

3.16.4.2 Testing Procedure

3.16.4.2.1 Evaluation

If a piece of equipment/system does not pass a test, the supplier will be allowed to retune/reconfigure the system/equipment. If, when retested, the system still fails, the supplier will be allowed to make minor redesigns / equipment changes where necessary (and subject to governance procedures). If, after implementing the design changes, the requirements can still not be met, the non-conformance process shall be followed [14] which may ultimately lead to the cancelling of the contract.

3.16.5 Alarm System Tests

3.16.5.1 Test Procedure

The following shall be tested on the alarm system:

a) Test and map the detection range of all intrusion sensors.

b) Test that zones are mapped and labelled correctly

c) Test the alarm sends a signal back to the security control room with the correct site and zone triggered.

d) Test that the alarm status (armed/disarmed) is visible at the security control room

e) Test that the remote control is able to arm and disarm the alarm system from inside a car outside the gate of the site.

f) Test that the remote control is able to arm and disarm the alarm system from inside a car outside the gate of the substation.

g) Test that the remote control is able to open the motorised gate from inside a car outside the gate of the site (if installed).

h) Test that when armed, the status LED is clearly visible from the gate of the substation in bright sunlight.

i) Test that there is an audible confirmation from the siren when the system is armed and disarmed

j) Test that the alarm panic button works over 80% of the site

k) Test that the keypad is operational including keypad panics.

l) Confirm that triggering alarms in each zone trigger recording on the appropriate camera(s).

m) Confirm that all passwords and pin codes have been changed from the default setting.

n) Infrared detectors shall be tested against 34-1617 - Specification for Infrared Detectors Used at Distribution Substations[11]

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.

o) If using Power Option B, 220V AC (see 0): Turn off the AC MCB to the security panel and confirm that the system continues to run normally.

3.16.5.2 Test Qualification

The alarm system tests shall be documented. Should the test be failed, the alarm system shall be retuned and retested. Should the test be failed again, the system shall be reconfigured and corrective action shall be taken to ensure the test is passed successfully.

3.16.6 PA System Tests

3.16.6.1 Test Procedure

The PA system shall be tested from within the site equipment room, as well as from the security control room. A quality microphone shall be used for the test so as to not influence the results of the test.

a) An employee shall speak over the PA system while another employee shall stand in the yard to listen and determine the clarity of the PA system.

b) A sentence shall be said over the system while an employee is positioned at each corner of the site, on all corners of the site and at any identified critical positions where there may be obstacles or obstructions that may buffer, distort or echo the audio coming from the speakers.

c) The employee shall confirm whether the sentences heard were the same as what was said. This shall be done by writing down what was heard and correlating on completion of the test.

d) Verify whether the clarity and volume of the audio is acceptable and can be well distinguished from any surrounding noise that may exist in the area such as transformer hum and corona noise.

e) The same test as mentioned above shall be conducted from within the security control room.

f) The test shall be repeated with the person speaking from offsite at the regional control room.

3.16.6.2 Test Qualification

The PA system Test Sheet in Annex F shall be used to document the PA system clarity test. Should the test be failed, the system shall be retuned and retested. Should the test be failed again, the system shall be reconfigured and corrective action shall be taken to ensure the test is passed successfully.

3.16.7 Floodlight Tests

3.16.7.1 Test Procedure

The installed LED floodlights shall be tested from both the site and security control room via the intruder detection panel.

a) Verify whether all of the lights are working properly.

b) Verify whether all the lights are activated when the alarm is activated / deactivated / triggered.

c) Verify whether the lights can be remotely switched on / off from within the security control room.

d) Verify whether the lights' timer modules are correctly functioning and that the lights remain on for a period no longer than 15 minutes.

e) Verify that the floodlights do not shine directly into any cameras.

f) Verify that the lights aren't causing excessive light pollution (e.g. shining onto a nearby situated house).

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.

3.16.7.2 Test Qualification

The Functional Floodlight System Test in Annex F shall be used to document the floodlight illumination test. Should the test be failed, the system shall be retuned and retested. Should the test be failed again, the system shall be reconfigured and corrective action shall be taken to ensure the test is passed successfully.

3.16.8 Intruder Detection Tests

When testing the intruder detection system, one needs to test that detection is achieved, but also that minimal nuisance alarms are generated (Soak Test).

3.16.9 Yard Intruder Detection Tests

3.16.9.1 Test Procedure

This test may be adapted according to the detection technology used. It shall always ensure that there is no point where an intruder may enter the site without being detected.

a) The test shall be performed by crossing the protected zone/virtual fence at multiple points.

b) The test shall be done by walking upright, hunched and crawling through the protected zone.

c) The distance at which the test shall start is from just before the detector's anticipated blind spot (if any).

d) Cross the area covered by the detection system, increasing in intervals of 10m from the detector's location.

e) Cross the area where there are distinct depressions and elevations.

f) Verify detection for each crossing of the protected zone.

g) Verify that upon detection, the camera records for 5 seconds before the event, and 15s after movement stops.

h) Verify that the footage to the security control room is suitable for confirming an intrusion.

i) Verify that it is not possible for an intruder to jump over or crawl under a detection zone.

3.16.9.2 Test Qualification

Either The Yard Intruder Detection Test sheet or The Yard Intruder Video Analytics Detection Test sheet (Annex F) shall be used to document each sensor in the yard intruder detection system.

Should the test be failed, the sensor shall be retuned and retested. Should the test be failed again, the sensor shall be reconfigured and corrective action shall be taken to ensure the test is passed successfully.

Once all sensors on a site have been tested for human detection, a site soak test shall be performed for 1 week to ensure that no more than 7 nuisance alarms are generated for the site per 7 day period (see (sections 3.16.11 & 3.16.11.2 below).

3.16.10 Indoor Intruder Detection Tests

3.16.10.1 Test Procedure

This test may be adapted according to the detection technology used. It shall always ensure that there is no point where an intruder may enter the building without being detected.

a) The test shall be performed by entering/simulating entrance into the building via every potential point of entry (doors, windows, air vent, ceiling etc.)

b) The test shall be done by walking upright, hunched and crawling through/just in front of the potential point of entry.

c) Verify detection for each potential entry point.

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.

d) Verify that upon detection, the camera records for 5 seconds before trigger happened and 15 seconds after movement stops.

e) Verify that the footage to the security control room is suitable for confirming an intrusion.

3.16.10.2 Test Qualification

Either the Indoor Intruder Detection Test sheet or The Indoor Intruder Video Analytics Detection Test sheet (Annex F) shall be used to document each sensor in the building intruder detection system.

Should the test be failed, the sensor shall be retuned and retested. Should the test be failed again, the sensor shall be reconfigured and corrective action shall be taken to ensure the test is passed successfully.

Once all sensors on a site have been tested for human detection, a site soak test shall be performed for 1 week to ensure that no more than 7 nuisance alarms are generated for the site per 7 day period (see (sections 3.16.11 & 3.16.11.2 below).

3.16.11 Site Intruder Detection Soak Tests

3.16.11.1 Test Procedure

Once all site intruder detection sensors (yard and building) have qualified individually, the Yard Detection Intruder Detection Site Soak Test (Annex F) shall be used to test the system as a whole for nuisance alarms.

The site shall be armed for a period of 1 week and all activations of the alarm during that week shall be noted.

For the site to pass there shall be less than 7 nuisance alarms in the 7 day period.

3.16.11.2 Test Qualification

Should a 7 day soak test indicate that the site generates more than 7 alarms in a 7 day period; the sensor(s) generating the majority of nuisance alarms shall be reconfigured. The Yard Intruder Detection Test shall then be repeated on the returned sensor(s) to ensure they still accurately detect intruders. The Intruder Detection Site Soak Test shall then be repeated. Should the soak test be failed again, the sensor(s) shall be reconfigured and corrective action shall be taken to ensure that both the intruder detection and soak tests are passed successfully.

3.16.12 Camera Functional Tests

Each camera shall be tested against its intended purpose (see section 3.10.1 for further information on camera purpose).

Cameras intended for observation, recognition or identification shall be tested as described in this section. These tests can be used for indoor or outdoor cameras.

Cameras intended for detection shall be considered intruder detection devices and shall be tested against the tests described in sections 3.16.8 to 3.16.11 above.

3.16.12.1 Test Procedure

Where available the Rotakin Test target shall be used for testing all cameras. An introduction the Rotakin Test Target can be found in Figure 12. Where a Rotakin or similar testing chart is not available, a person of average height (about 1.6m) shall be used as the target for the tests. Instead of the Rotakin number and letter ratings, a rating of poor/sufficient/excellent can be used.

a) The test shall be performed in the day and then repeated at night.

b) The day and night tests shall be repeated for all viewing media to be used. I.e. if the footage is to be recorded and viewed from a security control room, the tests shall be done based on control room footage and then repeated for recorded footage.

c) The target shall be placed at the furthest point to be covered and the percentage height of the screen taken up by the target shall be determined.

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.

d) The resolution achieved shall be tested using the Rotakin Bands or a rating of 'poor/sufficient/excellent'

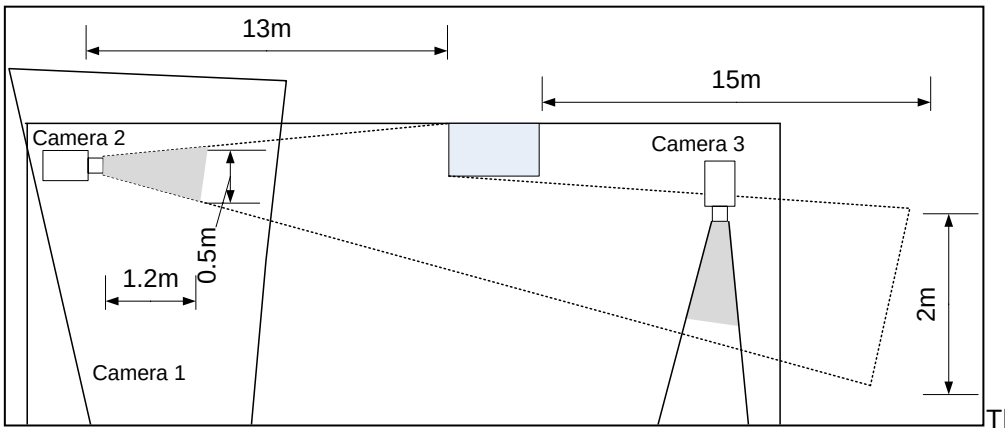
e) The frame rate achieved shall be tested using the Rotakin Bands or a rating of 'poor/sufficient/excellent'

f) The depth of focus achieved shall be tested using the Rotakin Bands or a rating of 'poor/sufficient/excellent'. (Not necessary for observation cameras)

g) The colour quality achieved shall be tested using a scale of 1-10.

h) Cameras intended for recognition or identification: The ability of a viewer to recognise/identify a human or number plate shall be tested using the Rotakin or a human/number plate.

i) A walk test shall be used to confirm the horizontal field of view of each camera expected from the design document. A measuring wheel shall be used to determine exact dimensions of the field of view achieved. The design document shall be redlined and updated based on the measurements. A single sketch may be used to show the horizontal field of view of all cameras on a site / in an area.



The

Figure 23: Example of Measured Horizontal Field of View of a Camera

j) A walk test shall be used to confirm the vertical field of view of each camera. A measuring wheel shall be used to determine exact dimensions of the field of view achieved. Obstacles and other cameras in field of view shall be included in the sketch. The design document shall be redlined and updated based on the measurements.

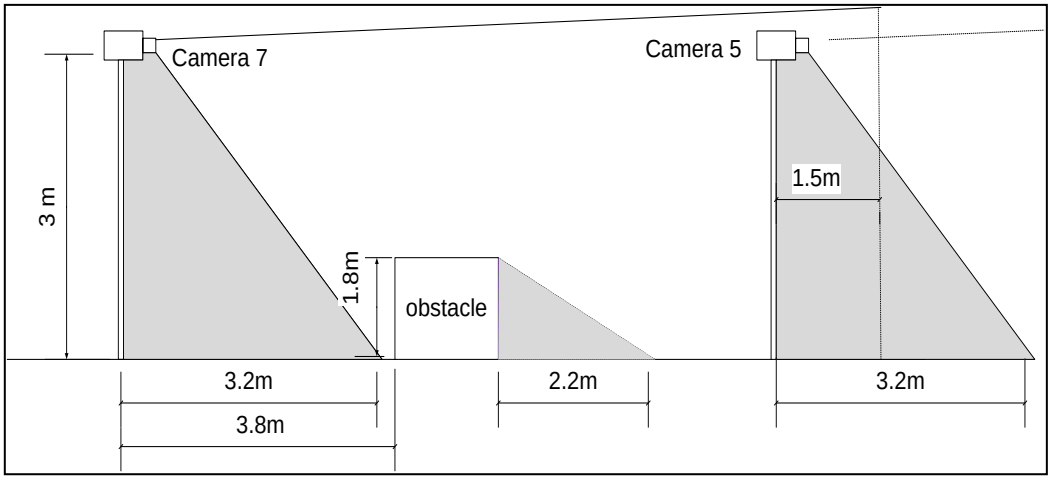


Figure 24: Example of Measured Vertical Field of View of a Camera

k) Time stamped snapshots shall be taken from each camera in the day and at night to be provided for handover purposes and future reference.

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.

3.16.12.2 Test Qualification

The Functional CCTV Test sheet (**Annex F**) shall be used to document each camera on the site.

The Test sheet consists of 6 sections with a summary of each section's results on the cover page.

Each camera shall be tested against its purpose. The test sheet shows the qualification criteria for each camera purpose so only the column corresponding to the camera's purpose needs to be completed (See 25 below for an example).

Functional CCTV Camera Test

Eskom

Section 2 of 6 : Rotakin Test - Recorded Footage

Site:	Heidelberg	Camera Number:	5
Auditor:	Sally Levesque		
Date: Day Test	14/4/2015	Time: Day Test	11:00
Date: Night Test	16/4/2015	Time: Night Test	20:00

(On Site Recordings) / Off site Recordings			
Comms Medium (if off site):	Fibre / GPRS / Satellite		
Recording File Format:	.avi	Recording Resolution:	1024 x 768
File size of 1 minute of recorded footage:	100Mb		

* Rotakin target to be placed at the furthest area to be protected
* Complete for each camera seperately (except detection cameras)
* Only complete the column corresponding to the camera's purpose
*Camera used for detection should be tested using the Camera Detection Test Sheets

Purpose of Camera:		Observation	(Recognition) & Numberplates	Identification
Expected percentage of screen height taken up by rotakin target		25%	50%	100%
Actual percentage of screen height taken up by rotakin target			65%	
Resolution Expected (Rotakin Bands):		F-H	A-B	A-B
Resolution Achieved:	Day		A	
	Night		B	
Frame Rate Expected (Rotakin Motion Band):		3-4	4-5	4-5
Frame Rate Achieved:			4	
Depth of Focus Expected at point of interest (Depth of Focus Circle):		NA	85%	85%
% Depth of Focus Achieved	Day	NA	85%	
	Night	NA	85%	
Colour Band Rating: (Excellent 10-9),(Very Good 8-7),(Good 6-5), (Poor 4-3),(Bad 2-1)				
Colour Band:	Day	NA	6	
Number Plate Recognition:	Day	NA	NA	NA
	Night	NA	NA	NA

Recorded Footage Rotakin results:

Day Test :	(Pass) / Fail	Night Test :	(Pass) / Fail

page 2 of 6

Figure 25: Example of Camera Report: Note that only the Recognition Column has been completed

Should the test be failed, the camera shall be retuned and retested. Should the test be failed again, the camera shall be reconfigured and corrective action shall be taken to ensure the test is passed successfully.

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.

3.16.13 PTZ Camera

3.16.13.1 Introduction

As discussed in 3.10.6.1, PTZ cameras are an expensive piece of equipment and should only be installed if it is possible to achieve their primary objective of assisting response teams or onsite security. If the tests detailed below show that it is not possible to control the PTZ effectively to track a suspect (either manually or automatically), then a PTZ shall not be installed. In this case more fixed cameras can be installed to cover strategic areas.

3.16.13.2 PTZ Control Test

The control of the PTZ cameras shall be tested from within the equipment room, as well as from the security control room.

a) Pan the PTZ camera 360º clock wise, as well as counter clockwise.

b) Verify whether the PTZ can pan in both directions without judder and excessive delay and overshoot.

c) Verify whether a panning angular velocity is equal to or greater than 6º per sec.

d) Tilt the PTZ camera over the camera's full range.

e) Verify whether the camera is capable of tilting a full 180º.

f) Verify whether the camera is capable of optically zooming in on an object with at least 35 times magnification.

3.16.13.3 PTZ Camera Coverage Test

The PTZ camera shall also be tested to verify that it can be effectively used to enable the security control room to gather real-time information about incidents on site, and co-ordinate the response to any intrusions.

A Rotakin, similar testing chart, or person of average height (about 1.6m) shall be used as the target for the tests.

a) The test shall be performed in the day and then repeated at night.

b) The day and night tests shall be repeated for all viewing media to be used i.e. if the footage is to be recorded, and viewed from a security control room, then the tests must be done based on live control room footage, and then repeated for recorded footage.

c) The target shall be placed at each of the areas to be covered by the PTZ preset positions and the effectiveness of the PTZ footage at that preset will be evaluated.

d) If PTZ tracking is available it shall be tested by a person walking and running between various positions on the site.

e) The percentage height of the screen taken up by the target shall be determined.

f) The resolution achieved shall be tested using the Rotakin Bands or a rating of 'poor/sufficient/excellent'

g) The frame rate achieved shall be tested using the Rotakin Bands or a rating of 'poor/sufficient/excellent'

h) The depth of focus achieved shall be tested using the Rotakin Bands or a rating of 'poor/sufficient/excellent'. (Not necessary for observation cameras)

i) The colour quality achieved shall be tested using a scale of 1-10.

j) Cameras intended for recognition or identification: The ability of a viewer to recognise/identify a human or number plate shall be tested using the Rotakin or a human/number plate.

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.

k) A walk test shall be used to determine and sketch the horizontal field of view and area of focus of each preset position. A measuring wheel shall be used to determine exact dimensions of the field of view achieved. Figure 26 below shows an example sketch.

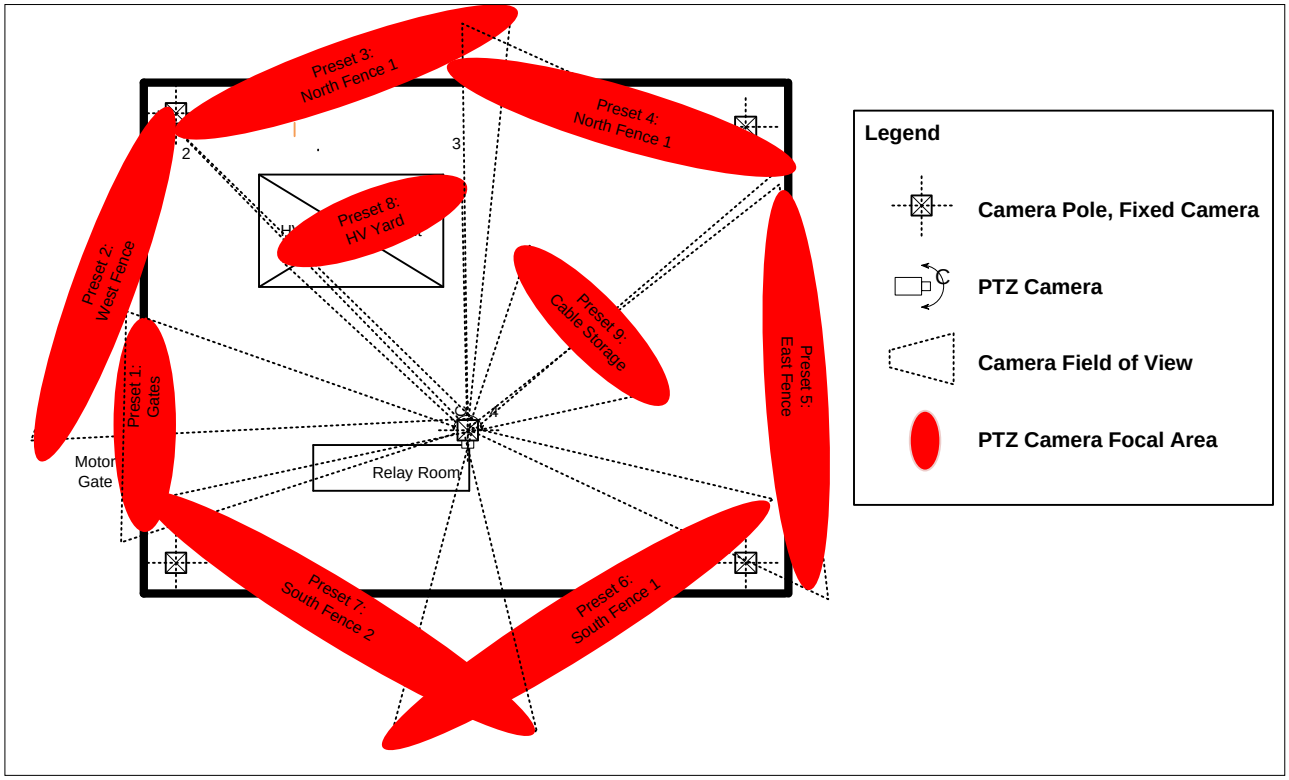


Figure 26: Example of measured Field of View of PTZ Pre-set Positions

l) Time stamped snapshots shall be taken from each camera in the day and at night to be provided for handover purposes and future reference.

m) The ability of the camera to compensate for glare from the sun shall be tested by facing the PTZ towards the sun.

n) The ability of the controller to manually operate the pan, tilt and zoom functions in real time from the security control room shall be tested and scored using a scale of 1-4.

3.16.13.4 PTZ Camera Coverage Test Qualification

The PTZ Functional Test sheet (**Annex F**) shall be used to document the testing of each PTZ on the site.

The Test sheet consists of 5 sections with a summary of each section's results on the cover page.

Should the test be failed, the system shall be retuned and retested. Should the test be failed again, the system shall be reconfigured and corrective action shall be taken to ensure the test is passed successfully

3.16.14 DVR Acceptance Tests

3.16.14.1 DVR Test Procedure

The DVR shall be tested to ensure that it is capable of meeting all requirements and has been configured correctly.

a) An incident on site shall be simulated and the following verified:

1) DVR Records for 5s second before the event, the time of the actual event and 15s second after motion stops

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.

2) Alarm signal is sent to security control room

3) A short video clip / series of still pictures from the camera covering the zone where the alarm triggered is sent to the security control room.

4) Clip is a lower resolution so that the video or pictures may be sent via GPRS.

5) The quality of the clip received at the security control room is such that the controller can clearly identify whether the intruder detection was triggered by a human.

6) Security control room is able to stream footage from site

7) Streamed footage allows for observation of site by security control room.

8) Security control room is able to operate PTZ cameras on site

9) Security control room is able to access PTZ pre-set positions

10) Security control room is able to speak over the PA system

11) Security control room is able to play pre-recorded message over PA System

b) It shall be verified that recordings made on the DVR meet the following requirements:

i. DVR can simultaneously record and stream footage

1) Recordings are electronically watermarked

2) Recordings show correct time and date

3) The DVR is able to trigger recordings based on schedule, manual trigger or alarm

4) It is possible to search recorded events based on date and time; event; motion in specific area; or a combination.

5) Playback in slow motion is possible

6) Playback at high speed is possible

7) Users can play recorded video from several cameras simultaneously

8) It is possible to ‘cut’ footage to export only the portion of footage that is of interest

9) All cameras on site are synced to within 1 second of DVR time

10) DVR time is synced to within 1 min of VMS time.

c) It shall be verified that the DVR has the following network security features:

1) Access Level 1:

i. Can perform all operator tasks

ii. No ability to delete footage

iii. No ability to view and change network or configuration settings.

2) Access Level 2:

i. Has full admin rights

ii. Can view a time and date stamped log of all logon events

iii. Can view a log of all administrative changes made on the system, including who made the change.

iv. Authorised Eskom employees using the client software are able to connect to the server via the Eskom Corporate Network.

d) The quality of streaming video obtained at the security control room shall be evaluated..

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.

e) For tender evaluations or evaluation of new DVR models the following shall also be tested:

1) The quality of streaming video obtained video across all potential telecoms media (GPRS, Fibre, Microwave, Satellite etc.)

2) The general usability of the user interface in terms of: efficiency memorability, errors, and user satisfaction (See section 3.11.8).

3.16.14.2 DVR Test Qualification

The DVR / NVR System Tests in Annex F shall be used to document the VMS test. Should the test be failed, the system shall be reconfigured and retested. Should the test be failed again, the system shall be reconfigured and corrective action shall be taken to ensure the test is passed successfully.

3.16.15 VMS Acceptance Tests

3.16.15.1 VMS Test Procedure

The ability of the VMS system to meet all requirements as specified in section 3.11 shall be tested.

The ability of the VMS to enable the security control room activities described in 3.12 shall be tested.

The VMS system shall be operated by the evaluator in order to get a first-hand understanding of how user friendly the system is.

The activities shall be demonstrated while connected to at least one live site:

3.16.15.2 VMS Test Qualification

The Video Management System Test in Annex F shall be used to document the VMS test. Should the test be failed, the system shall be reconfigured and retested. Should the test be failed again, the system shall be reconfigured and corrective action shall be taken to ensure the test is passed successfully. In the event that the retuned system cannot deliver the functions originally specified, Eskom shall consider changing to a different VMS system.

4. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Prince Moyo	Power Delivery Engineering GM
Richard McCurrach	PTM&C TC Chairperson
Amelia Mtshali	Metering, DC & Security Technologies Manager (Acting) – PTM&C CoE
Prudence Madiba	Senior Manager Electrical and C&I Engineering
Lungile Malaza	Middle Manager – Electrical Plant COE
Martin Strauss	Senior Manager – Group Security
Karen Pillay	Manager - Security Design, Advisory & Projects
T Jacobs	DC Auxiliary Supplies SC Chairperson

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.

5. Revisions

Date	Rev.	Compiler	Remarks
Feb 2021	2	A Hendriks	There are no changes to the document's technical content. Learnings from the Bernina Security Project will be used to improve the document and it will become the blueprint for future implementations.
March 2016	1	S Levesque	Comments from the Workshop held on 11 Dec 2015 incorporated. Final version authorised. Specification revised due to newer technologies, and extended to cover all Eskom buildings and all divisions. Document number changed from 34-1613 to 240-91190304
Nov 2011	0	S Sivasamy	Specification revised due to newer technologies, as well as increased implementation of CCTV and alarm systems within Distribution substations. Document number DISSCABM6 changed to 34-1613
Jan 2004	0	SM Dhlamini	Document reference number changed from SCS to DIS

6. Development team

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

- Sally Levesque, Engineer
- Albert Hendriks, Engineer
- Thomas Jacobs, Chief Engineer

7. Acknowledgements

The author would like to thank everybody who contributed by means of comments and participation during the workshop.

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.

Annex A – Discussion of video analytics

Distinction between video motion detection and video analytics

A distinction needs to be made between what this document refers to as Video Analytics and Video Motion Detection. The Table below should be used to determine if a solution offered is Video Motion Detection or Video Analytics. This specification calls for Video Analytics to be used for perimeter detection.

Video Motion Detection	Video Analytics
System looks for basic changes in the video being viewed	System does analysis of the changes being viewed to determine if they are of interest
Camera field of view can be split up into zones/blocks where movement should trigger an alarm	Camera field of view can be split up into zones/blocks where movement should trigger an alarm. In addition system can be told to trigger for any motion, human detection or vehicle detection
Will false trigger due to movements from trees, shaking of camera pole or changes in lighting.	Will not false trigger due to movements from trees, shaking of camera pole or changes in lighting.
Will not take into account that objects get smaller when further away. May not trigger on objects at a distance.	Will take into account the three dimensional field of view (objects are smaller further away). Adjusts the amount of movement to trigger an alarm depending on the distance.
Limited tracking capabilities	Can be used to guide a PT(Z) camera to track a moving object
Not an effective method of outdoor perimeter detection	Can be an effective method of outdoor perimeter detection when configured appropriately.

Comparison Between Server and Edge Video Analytics

Manufacturers take one of two approaches when implementing Video Analytics. These are known as ‘edge’ or ‘server’ analytics and refer to where the processing of the image data is done.

The Table below compares the two approaches.

Server Analytics	Edge Analytics
The video analytics processing is done on the DVR or similar server.	Analytics is done on a dedicated device or on-board the camera
Processing from all video feeds is done on a single machine.	Each device analyses the feed from a single camera, or a limited number of cameras.
Server may run other tasks in addition to analysing camera feeds (e.g. recording).	Processor is dedicated to analysing camera feed.
Server analytics will lag if communication between camera and server are not fast enough.	Edge analytics not subject to communication lag. Sends single alarm single back to alarm monitoring system.
Appropriate for indoor environment with little activity	Has enough processing power to effectively monitor an outdoor, or busy indoor environment.

Edge analytics are recommended over server analytics. However, as with all aspects of CCTV installations, thorough functional testing shall be done in order to determine the best solution for each site.

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.

Annex B – Typical maintenance check list

The following checklist shall be used as a guide for the development of a Site Maintenance check list. The list below shall be adapted to comply with the supplier's maintenance recommendations.

SECURITY SYSTEMS

Quarterly Routine SITE MAINTENANCE

Site:	
Maintenance performed by:	
Signed:	
Date:	
Does Security System Requires Follow up maintenance? (if yes, give details)	

Tick List

	Y	N	NA
1. Check battery voltage and condition of batteries.			
2. Inspect and clean all door and window contacts.			
3. Clean all 'passive infra-red' motion detector front covers dust & dirt and inspection of pulse settings and anti-tamper switches.			
4. Check and lubricate key switches if applicable.			
5. Inspect and clean power points such as plug in transformers and plug points.			
6. Check power supply to the control boxes.			
7. Visually inspect all cabling and joints for corrosion, breakages and dry joints.			
8. Visually inspect cabling and joints for corrosion in the control box.			
9. Inspect and check status of keypad.			
10. Test opening and closing of motorized gate if applicable.			
11. Inspect and clean smoke and heat detectors if they form part of the burglar alarm system.			
12. Test all zone alarms and panic signals with monitoring company.			
13. Test arm and dis-arm signals to monitoring company.			
14. Test all glass break detectors.			
15. Inspect, clean and align all active infra-red beams where necessary			
16. Clear all equipment of insects and spray all outdoor equipment with insect repellent.			

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.

	Y	N	NA
17. Clean all obstructions if interfering with infra-red/micro wave beams alignment causing nuisance alarms.			
18. Visually inspect electric fence energizers LED indicators for correct operation.			
19. Visually inspect electric fence to be clear of all vegetation & debris.			
20. Cleaning, servicing and refocus of all CCTV equipment.			
21. Check all connections and end of line terminations			
22. Check all mountings, brackets and housings			
23. Visual inspection of access controllers			
24. Test access control card readers & RF remotes functionality			
25. Check on site data recordings of access control system			
26. Turnstile card reader functionality			
27. Maintain turn stiles mechanism			
28. Vehicle boom – check functionality			
29. Check holding & loop detectors			
30. Maintain vehicle boom mechanism			
31. Gate access – check functionality			
32. Maintain gate mechanism			
33. Door access – check functionality			
34. Maintain door strike movement			
35. Maintain door closers & check for correct operation			
36. Video capturing on site – check data capturing and check that recordings are being kept for 30days.			
37. Compare footage to footage on file from commissioning			
38. Inspect all equipment related to CCTV re connectivity, e.g. Wiring, cabling, enclosures, etc.			
39. Check camera alignment and field of view.			
40. Check focus of all cameras			
41. Clean all camera lenses and covers			
42. Check mounting brackets, poles etc. for damage			
43. Test PA system			

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.

Annex C – System Performance

The following formulae shall be used to evaluate the performance of CCTV and Intruder detection systems and shall be calculated monthly (adapted from DISPAVACE8 [28]).

System Availability

System Availability shall be greater than 98%

$$\boldsymbol{System\ Availability} = \frac{(\boldsymbol{Total\ hours}) - (\boldsymbol{Total\ non\ operational\ hours})}{\boldsymbol{Total\ Hours}} \times \mathbf{100}$$

This can be calculated per site or per region

System Reliability

Monthly System Reliability shall be greater than 95%

$$\boldsymbol{Monthly\ System\ Reliability} = \frac{\boldsymbol{Number\ of\ Faults\ in\ a\ Month}}{\boldsymbol{Number\ of\ Systems\ Installed}} \times \mathbf{100}$$

This can be calculated per site or per region.

System Dependability

Any single zone of the alarm / detection system shall give no more than 7 false detections in any 7 day period.

To measure this as a KPI, the following formulae below shall be used.

Monthly System Dependability shall be greater than 85%

$$\boldsymbol{Per\ Site\ System\ Dependability} = \left(\mathbf{1} - \frac{\boldsymbol{Number\ of\ false\ alarms\ in\ a\ month}}{\mathbf{400}}\right)^{\mathbf{2}}$$

This calculation is per site. Per region, the System dependability is the average of the per site values.

NOTE: This formula was chosen so as to reflect the following:

- 0 false alarms is ideal – 100% Dependable
- 7 faults per 7 days is acceptable - 85% Dependable
- 30 faults per 7 days indicates a poorly functioning system – 50% Dependable
- 100 false alarms per 7 days indicates an unusable system – 0 % dependable

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.

Annex D – Introduction to Rotakin Test Target



Figure D.1: Rotakin Test Target

The Rotakin Target was developed by the British Home Office as a means to test CCTV camera performance. The use of the Rotakin Test Target or similar CCTV test chart is highly recommended during CCTV commissioning.

Where a Rotakin is not available, all tests can be adapted to be used with a human target, the difference being that the results will be more subjective.

SANS 10222-5-14[16] introduces the Rotakin Test Target as follows:

> **5.4.2** Although many of the problems might be the result of poor system design and specification, the final commissioning testing does not always make them apparent. The absence of a simple but reliable accepted performance standard was identified as a key issue. This has led to the development of a device called the ROTAKIN (see figure 1).
>
> **5.4.3** The ROTAKIN is a test target mounted on a stand. The target is a weatherproof panel measuring 1 600 mm x 400 mm, black in colour, and shaped at each end to represent the outline of a human head. It bears high contrast resolution bars and a wedge chart for static and dynamic resolution measurements. A camouflage cloth cover allows additional intruder detection in various positions with or without the stand.
>
> **5.4.4** A small battery driven motor shall rotate the target at 25 RPM. This is representative of a person moving quickly but stealthily. The complete kit is light and easily portable.
>
> **5.4.5** The ROTAKIN test target shall be used to carry out the following objective tests:
>
> a) the area covered by each camera, to detect and eliminate blind spots;
>
> b) the size of the target and if it is readily seen;
>
> c) the system response time and staff reaction;
>
> d) the visibility of target camouflage against a contrasting background;
>
> e) the effects of different types of scene illumination; and
>
> f) lens focus and adjustments.

More information on the Rotakin can be found at www.cctvinfocus.com.

SANS 10222-5-14[16] sections 5.4.10 – 5.4.19 describes a similar chart developed in Germany which may be used as an alternative to the Rotakin.

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.

Annex E – Affidavit

(Example of Affidavit Form for Security Personnel)

Affidavit

_____ declares under oath, as follows:

I, number_____, am a _____ at _____

I am in possession of a _____ degree (____) from the University of _____ (only if applicable)

On _____ the video/images was/were copied to

CD/DVD/ _____ by myself, this copy was marked "_____" and sealed in an evidence bag with number _____ and was kept at _____ for safe keeping purposes.

or / and

On _____ I received one (1) evidence bag with number _____ containing _____

or /and

On _____ I handed over one (1) evidence bag with

number _____to _____ for_____ (reason if applicable)

I know and understand the contents of this declaration. I have no objection to taking the prescribed oath. I consider the prescribed oath to be binding on my conscience.

_____ : NAME

I certify that the deponent has acknowledged that she/ he knows and understands the contents of this declaration which was sworn before me and deponent's signature was placed thereon in my presence at

_____(Place) on _____(date).

_____ : PERSONNEL NUMBER / ID NUMBER

COMMISSIONER OF OATHS

_____ : NAME

_____ : ADDRESS

_____ : RANK / POSITION

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.

Annex F – Functional Acceptance Test Sheets

The following pages are templates for functional acceptance reports for Demonstrations on Equipment, Factory Acceptance Tests (FAT) and Site Acceptance Tests (SAT). They may be edited to better fit the site requirements.

An Excel sheet containing all test sheets is available from the author.

List of Test Sheets:

1) FAT Summary
2) Functional PA System Test
3) Functional Floodlight System
4) Intruder Detection Test – Yard
5) Intruder Detection Test - Yard - Video Analytics
6) Intruder Detection Test – Indoors
7) Intruder Detection Test - Indoors - Video Analytics
8) Intruder Detection Soak Test
9) Functional CCTV Camera Test
10) Functional PTZ Camera Test
11) DVR / NVR Functional Acceptance Test
12) Video Management System Test

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.

Functional Acceptance Test CCTV Camera System

Summary of System Tests

Site:	
Auditor:	

Results Summary

Test	Result	Remarks
Alarm System	Pass / Fail	
PA System	Pass / Fail	
Floodlights	Pass / Fail	
Yard Detection	Pass / Fail	
Yard Detection - Cameras	Pass / Fail	
Indoor Detection	Pass / Fail	
Indoor Detection - Cameras	Pass / Fail	
Intruder Detection Soak Test	Pass / Fail	
CCTV Cameras	Pass / Fail	
Control Room Integration	Pass / Fail	

Overall	**Installation Accepted / Retuning Needed / Redesign Needed / NCR to be issued**		
Remarks			
Auditor's Signature:		Date:	

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.

Functional PA System Test

Site:		Auditor:	

Clarity Tests - Microphone on Site

Position	Sentence Spoken	Sentence Heard Correctly?
Corner 1		Yes / Almost / No
Corner 2		Yes / Almost / No
Corner 3		Yes / Almost / No
Corner 4		Yes / Almost / No
		Yes / Almost / No
		Yes / Almost / No
		Yes / Almost / No

Clarity Tests - Microphone at Offsite Control Room

Position	Sentence Spoken	Sentence Heard Correctly?
Corner 1		Yes / Almost / No
Corner 2		Yes / Almost / No
Corner 3		Yes / Almost / No
Corner 4		Yes / Almost / No
		Yes / Almost / No
		Yes / Almost / No
		Yes / Almost / No

Noise Pollution Tests

PA System should be barely audible from boundary of nearest residence.

Position	PA Audible?
	Yes / Barely / No
	Yes / Barely / No
	Yes / Barely / No

Results Summary

Test	Result	Remarks
Overall	**Pass / Fail**	

Auditor's Signature:			**Date:**	

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.

Functional PA System Test- Listener Sheet

Clarity Tests - Microphone on Site

Position	Sentence Heard	Sentence Heard Correctly?
Corner 1		
Corner 2		Yes / Almost / No
Corner 3		Yes / Almost / No
Corner 4		Yes / Almost / No
		Yes / Almost / No
		Yes / Almost / No
		Yes / Almost / No

Clarity Tests - Microphone at Offsite Control Room

Position	Sentence Heard	Sentence Heard Correctly?
Corner 1		Yes / Almost / No
Corner 2		Yes / Almost / No
Corner 3		Yes / Almost / No
Corner 4		Yes / Almost / No
		Yes / Almost / No
		Yes / Almost / No
		Yes / Almost / No

Noise Pollution Tests

Stand at boundary of nearest residence.

Position	PA Audible?
	Yes / Barely / No
	Yes / Barely / No
	Yes / Barely / No

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.

Functional Floodlight System Test

Site:	
Auditor:	
Flood light System Description	

Test Results

Requirement	Acceptable?
All floodlights functioning properly?	Yes / No
Alarm Activation	
Floodlights turn on automatically when alarm is activated at night?	Yes / No
Floodlights do not turn on when alarm is activated in the day?	Yes / No
When activated by alarm, floodlights automatically turn off after 15mins?	Yes / No
Security Contrl Room Activation	
Security control room can turn on the floodlights remotely?	Yes / No
When activated remotely, floodlights automatically turn off after 15mins?	Yes / No
On site activation	
Floodlights can be activated by person on site?	Yes / No
Floodlights remain on when activated by person on site? (Lights do not turn off automatically)	Yes / No
Floodlight Placement	
Floodlights do not shine directly into any cameras	Yes / No
Are lights causing excessive light pollution (e.g. shining into a nearby house)	Yes / No

Results Summary

Test	Result	Remarks
Overall	**Pass / Fail**	

Auditor's Signature:		**Date:**	

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.

Intruder Detection Test - Yard

Site:		Sensor Number:	
Auditor:		Zone:	

Description of detector position:	
Detector type, make and model:	
What activity is to be detected? :	
Risk of activity:	
Evident obstructions and blind spots:	
Potential causes of nuisance alarms (eg trees, wildlife, light changes)	

Perimeter Tests

Distance (Repeat Every 10m)	Person Detected?			
	Walking	Hunched	Crawling	Running
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No

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.

Elevations, Depressions

Description	Person Detected?			
	Walking	Hunched	Crawling	Running
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No

Potential Nuisance Alarms

Description	Nuisance Alarm Generated?
	Yes / No
	Yes / No
	Yes / No
	Yes / No

Blind Spots

Describe/sketch any obstructions or blind spots. Which other detectors covers these areas?

Camera Footage Recorded when Sensor Triggers

Camera Footage is recorded	Yes / No / NA
Camera footage is sufficient to confirm an intrusion?	Yes / No / NA
Camera recordss 5s before triggering and 15s after movement stops	Yes / No / NA

Results Summary

Test	Result	Remarks
Overall	**Pass / Fail**	

Auditor's Signature:		**Date:**	

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.

Intruder Detection Test - Yard - Video Analytics

Site:		Camera Number:	
Auditor:		Zone:	
Description of camera position:			
Camera Make and Model:			
CCD Size:		Lense:	
Light conditions under which the camera detection needs to be effective:			
What activity is to be detected? :			
Risk of activity:			
Evident obstructions and blind spots:			
Potential causes of nuisance alarms (eg trees, wildlife, light changes)			

Perimeter Tests

Distance (Repeat Every 10m)	Person Detected?							
	Walking		Hunched		Crawling		Running	
	Day	Night	Day	Night	Day	Night	Day	Night
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no

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.

Elevations, Depressions

Description	Person Detected?							
	Walking		Hunched		Crawling		Running	
	Day	Night	Day	Night	Day	Night	Day	Night
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no
	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no	yes / no

Potential Nuisance Alarms

Description	Nuisance Alarm Generated?
Headlights of passing car	Yes / No
Moving Shadows	Yes / No
Direct sunlight	Yes / No

Blind Spots

Describe/sketch any obstructions or blind spots. Which other detectors covers these areas?

Camera Footage when Sensor Triggers

Camera Footage is recorded	Yes / No / NA
Control Centre Camera footage is sufficient to confirm an intrusion?	Yes / No / NA
Camera records 5s before triggering and 15s after movement stops ?	Yes / No / NA

Results Summary

Test	Result	Remarks
Overall	**Pass / Fail**	

Auditor's Signature:		**Date:**	

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.

Intruder Detection Test - Indoors

Site:		Sensor Number:	
Auditor:		Zone:	
Description of detector position:			
Detector type, make and model:			
What activity is to be detected? :			
Risk of activity:			
Evident obstructions and blind spots:			
Potential causes of nuisance alarms (eg banners, piles of papers, light changes)			

Doors

Door	Person Detected?			
	Walking	Hunched	Crawling	Running
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No

Windows

Window	Person Detected?			
	Walking	Hunched	Crawling	Running
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No

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.

Other Potential Points of Entry

Entry Point	Person Detected?			
	Walking	Hunched	Crawling	Running
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No

Potential Nuisance Alarms

Description	Nuisance Alarm Generated?
	Yes / No
	Yes / No
	Yes / No
	Yes / No

Blind Spots

Describe/sketch any obstructions or blind spots. Which other detectors covers these areas?

Camera Footage Recorded when Sensor Triggers

Camera Footage is recorded	Yes / No / NA
Camera footage is sufficient to confirm an intrusion?	Yes / No / NA
Camera recordss 30s before triggering and 30s after movement stops	Yes / No / NA

Results Summary

Test	Result	Remarks
Overall	**Pass / Fail**	

Auditor's Signature:		**Date:**	

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.

Intruder Detection Test - Indoors - Video Analytics

Site:		Camera Number:	
Auditor:		Zone:	
Description of camera position:			
Camera Make and Model:			
CCD Size:		Lense:	
Light conditions under which the camera detection needs to be effective:			
What activity is to be detected? :			
Risk of activity:			
Evident obstructions and blind spots:			
Potential causes of nuisance alarms (eg banners, piles of papers, light changes)			

Doors

Door	Person Detected?			
	Walking	Hunched	Crawling	Running
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No

Windows

Window	Person Detected?			
	Walking	Hunched	Crawling	Running
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No

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.

Other Potential Points of Entry

Point of Entry	Person Detected?			
	Walking	Hunched	Crawling	Running
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No
	Yes / No	Yes / No	Yes / No	Yes / No

Potential Nuisance Alarms

Description	Nuisance Alarm Generated?
Headlights of passing car	Yes / No
Moving Shadows	Yes / No
Direct sunlight	Yes / No

Blind Spots

Describe/sketch any obstructions or blind spots. Which other detectors covers these areas?

Camera Footage when Sensor Triggers

Camera Footage is recorded	Yes / No / NA
Control Centre Camera footage is sufficient to confirm an intrusion?	Yes / No / NA
Camera records 5s before triggering and 15s after movement stops ?	Yes / No / NA

Results Summary

Test	Result	Remarks
Overall	**Pass / Fail**	
Auditor's Signature:		**Date:**

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.

Intruder Detection Soak Test

Site:			
Auditor:		Zone:	

This test is conducted for the site as a whole. The site shall be armed for a period of 1 week and all activations of the alarm during that week shall be noted.
For the site to pass there shall be less than 7 nuisance alarms in the 7 day period.

Day 1 of Soak Test		Day 7 of Soak Test	

Nuisance Alarm Acitivations

Date & Time	Zone	Detector	Notes
Total number of nuisance alarms			
Detectors to be re-tuned			

Results Summary

Test	Result	Remarks
Overall	**Pass / Fail**	
Auditor's Signature:		**Date:**

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.

Functional CCTV Camera Test

Section 1 of 7 : Camera and Site Details

Site:		Camera Number:	
Auditor:			
Camera Location:			
Camera Make and Model:			
CCD Size:		Lense:	
Camera Resolution:			
Activity is to be observed:			
Risk of activity:			
Purpose of Camera:	Observation	Recognition & Numberplates	Identification
Light conditions under which camera needs to be effective:			
Minimum Lux at target:		Distance to target:	
Evident obstructions and blind spots:			

Results Summary

Test	Result	Remarks
Section 2: Rotakin Test - Recorded	Pass / Fail	
Section 3: Rotakin Test - Live	Pass / Fail	
Section 4: Sun and Light Immunity	Pass / Fail	
Section 5: Human Face and Vehicle Number Plate	Pass / Fail / NA	
Section 6: Vertical Field of View	Pass / Fail	
Section 7: Horizontal Field of View	Pass / Fail	
Overall	**Pass / Fail**	
File names of time stamped snapshots taken during testing		
Auditor's Signature:		**Date:**

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.

Section 2 of 7 : Rotakin Test - Recorded Footage

Site:		Camera Number:	
Auditor:			
Date: Day Test		Time: Day Test	
Date: Night Test		Time: Night Test	

On Site Recordings / Off site Recordings		Comms Medium (if off site):	Fibre / GPRS / Satellite
Recording File Format:		Recording Resolution:	
File size of 1 minute of recorded footage:			
Time & date displayed correctly on footage?	Y / N	Camera name and number displayed correctly on footage?	Y / N

* Rotakin target to be placed at the furthest area to be protected
* Complete for each camera seperately (except detection cameras)
* Only complete the column corresponding to the camera's purpose
*Camera used for detection should be tested using the Camera Detection Test Sheets

Purpose of Camera:		Observation	Recognition & Numberplates	Identification
Expected percentage of screen height taken up by rotakin target		25%	50%	100%
Actual percentage of screen height taken up by rotakin target				
Resolution Expected (Rotakin Bands):		F-H	A-B	A-B
Resolution Achieved:	Day			
	Night			
Frame Rate Expected (Rotakin Motion Band):		3-4	4-5	4-5
Frame Rate Achieved:	Day			
	Night			
Depth of Focus Expected at point of interest (Depth of Focus Circle):		NA	85%	85%
% Depth of Focus Achieved	Day	NA		
	Night	NA		
Colour Band Rating: (Excellent 10-9),(Very Good 8-7),(Good 7-5), (Poor 4-3),(Bad 2-1)				
Colour Band:	Day	NA		
	Night			
Number Plate Recognition:	Day	NA		NA
	Night	NA		NA

Results - Recorded Footage :

Day Test :	Pass / Fail	Night Test :	Pass / Fail

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.

Section 3 of 7 : Rotakin Test - Live Viewing

Site:		Camera Number:	
Auditor:			
Date: Day Test		Time: Day Test	
Date: Night Test		Time: Night Test	

Live View on Site / Live View off Site			
Comms Medium (if off site):	Fibre / GPRS / Satellite		
Compression Format:		Live Stream Resolution	
Average bandwidth of live stream:			

* Rotakin target to be placed at the furthest area to be protected
* Complete for each camera seperately
* Only complete the column corresponding to the camera's purpose

Purpose of Camera:		Observation	Recognition & Numberplates	Identification
Expected percentage of screen height taken up by rotakin target		25%	50%	100%
Actual percentage of screen height taken up by rotakin target				
Resolution Expected (Rotakin Bands):		F-H	A-B	A-B
Resolution Achieved:	Day			
	Night			
Frame Rate Expected (Rotakin Motion Band):		3-4	4-5	4-5
Frame Rate Achieved:	Day			
	Night			
Depth of Focus Expected at point of interest (Depth of Focus Circle):		NA	85%	85%
% Depth of Focus Achieved	Day	NA		
	Night	NA		
Colour Band Rating: (Excellent 10-9),(Very Good 8-7),(Good 7-5), (Poor 4-3),(Bad 2-1)				
Colour Band:	Day	NA		
	Night			
Number Plate Recognition:	Day	NA		NA
	Night	NA		NA

Day Test :	Pass / Fail	Night Test :	Pass / Fail		

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.

Section 4 of 7 : Sun and Light Immunity

Site:		Camera Number:	
Auditor:			
Date: Day Test		Time: Day Test	
Date: Night Test		Time: Night Test	

Indoor, Door Cameras

Able to achieve recognition of person entering door with bright sun outside and no lighting inside?	Yes / No / NA

Outdoor Cameras

Able to achieve purpose when sun is in the camera field of view?	Yes / No / NA

Results - Sun and Light Immunity

Sun and Light immunity meet operationalrequirements?	Yes / No

Section 5 of 7 : Human Face and Vehicle Number Plates

** This test is not necessary when cameras are used for detection or observation*

Purpose of Camera:

Recorded Footage	Detection	Recognition	Number Plates	Identification
Live Viewing	Detection	Recognition	Number Plates	Identification

Test

		Recorded Footage		Live Viewing - Control Room		
		Test 1	Test 2	Test 1	Test 2	Result
Human Face	Day					Pass / Fail
	Night					Pass / Fail
Vehicle Number Plate	Day					Pass / Fail
	Night					Pass / Fail

Results - Human Face and Vehicle Number Plates

Face Identification meets operational requirements?	Yes / No / NA
Number Plate Identification meets operational requirements?	Yes / No / NA

ESKOM COPYRIGHT PROTECTED

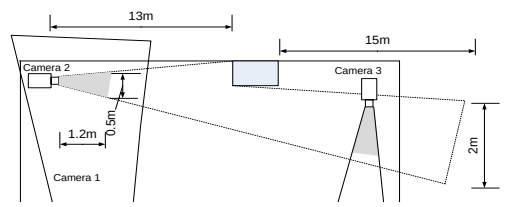
When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

Section 6 of 7: Camera Horizontal Field of View

Site:		Camera Number:	
Auditor:			
Date: Day Test		Time: Day Test	
Date: Night Test		Time: Night Test	

**Sketch camera field of view as achieved on site. Include Measurements. Include obstacles*
**Field of view must be determined in the day and at night.*
**Sketch the Worst Case Scenario*

eg



Horizontal Field of View meets operational requirements?	Yes / No	

ESKOM COPYRIGHT PROTECTED

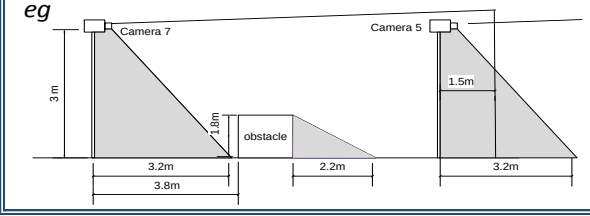
When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

Section 7 of 7: Camera Vertical Field of View

Site:		Camera Number:	
Auditor:			
Date: Day Test		Time: Day Test	
Date: Night Test		Time: Night Test	

**Sketch camera field of view as achieved on site. Include Measurements. Include obstacles and other cameras in field of view*
**Field of view must be determined in the day and at night.*
**Sketch the Worst Case Scenario*

eg



Horizontal Field of View meets operational requirements?	Yes / No	

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.

Functional PTZ Camera Test

Section 1 of 8 : Camera and Site Details

Site:		Camera Number:		Auditor:	
Camera Location:					
Camera Make and Model:		CCD Size:		Lense:	
Camera Resolution:					
Light conditions under which camera needs to be effective:					
Minimum Lux at target:		Distance to furthest target:			
Evident obstructions and blind spots:					

Results Summary

Test	Result	Remarks
Section 2: PTZ Control	Pass / Fail	
Section 3: Live View	Pass / Fail	
Section 4: Recorded Footage	Pass / Fail	
Section 5: Horizontal Field of View	Pass / Fail	
Overall:	**Pass / Fail**	
File names of time stamped snapshots taken during tests		
Auditor's Signature:		**Date:**

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.

Section 2 of 8 : PTZ Control Test

Site:		Camera Number:		Auditor:	
Date:					

* Tests to be done from control room

Live View on Site / Live View off Site	Comms Medium (if off site):	Fibre / GPRS / Satellite	Compression Format:

Results:

Function	Requirement	Result	Pass / Fail	Comment
Pan Range	360 °		Pass / Fail	
Pan Direction	Bidirectional		Pass / Fail	
Pan Velocity	≥ 6 ° per second		Pass / Fail	
Tilt	≥ 180°		Pass / Fail	
Optical Zoom	≥ 35 times		Pass / Fail	
Judder	Negligible		Pass / Fail	
Overshoot	Negligible		Pass / Fail	

Results - PTZ Control Test :

Day Test :	Pass / Fail	Comments	

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.

Site:		Camera Number:		Auditor:	

Section 3 of 8 : Live View

Date: Day Test		Time: Day Test		Date: Night Test		Time: Night Test	
Live View on Site / Live View off Site		Comms Medium (if off site):		Fibre / GPRS / Satellite		Compression Format	
Live Stream Resolution				Average bandwidth of live stream:			
Able to achieve purpose when sun is in the camera field of view?			Yes / No / NA				

* Complete detailed tests sheet - page 4

Results - Live View:

Day Test :	Pass / Fail	Night Test :	Pass / Fail

Section 4 of 8 : Recorded Footage Summary

Date: Day Test		Time: Day Test		Date: Night Test		Time: Night Test	
On Site Recordings / Off site Recordings		Comms Medium (if off site):		Fibre / GPRS / Satellite			
Recording File Format:		Recording Resolution:			File size of 1 minute of recorded footage:		
Time & date displayed correctly on footage?	Y / N	Camera name and number displayed correctly on footage?	Y / N	Preset Position Displayed on footage?	Y / N		

* Complete detailed tests sheet - page 5

Results - Recorded Footage :

Day Test :	Pass / Fail	Night Test :	Pass / Fail

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.

Section 5 of 8 : Live Tracking Tests

* Circle appropriate purpose for each place (O)bservation, (R)ecognition, (N)umber plates, (I)dentification.
* Zoom into the point of interest so that the target is at the appropriate screen percentage.

Place of interest			Purpose	Activity to be observed:	Risk of activity:	Preset Position Correct?	Camera Movement Smooth?	% Screen Height	Resolution Achieved	Frame Rate	Depth of Focus	Colour Band	Purpose Achieved?
PTZ Preset	Description												
1		Day	O / R / N										Y / N
		Night											Y / N
2		Day	O / R / N										Y / N
		Night											Y / N
3		Day	O / R / N										Y / N
		Night											Y / N
4		Day	O / R / N										Y / N
		Night											Y / N
5		Day	O / R / N										Y / N
		Night											Y / N
6		Day	O / R / N										Y / N
		Night											Y / N
7		Day	O / R / N										Y / N
		Night											Y / N
8		Day	O / R / N										Y / N
		Night											Y / N
9		Day	O / R / N										Y / N
		Night											Y / N
10		Day	O / R / N										Y / N
		Night											Y / N

Results - Live View:

Day Test :	Pass / Fail	Night Test :	Pass / Fail

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.

Section 6 of 8 : Recorded Footage Tests

* Circle appropriate purpose for each place (O)bservation, (R)ecognition, (N)umber plates, (Identification).
* Zoom into the point of interest so that the target is at the appropriate screen percentage.

Place of interest			Purpose	Activity to be observed:	Risk of activity:	% Screen Height	Resolution Achieved	Frame Rate	Depth of Focus	Colour Band	Purpose Achieved?
PTZ Preset	Description										
1		Day	O / R / N								Y / N
		Night									Y / N
2		Day	O / R / N								Y / N
		Night									Y / N
3		Day	O / R / N								Y / N
		Night									Y / N
4		Day	O / R / N								Y / N
		Night									Y / N
5		Day	O / R / N								Y / N
		Night									Y / N
6		Day	O / R / N								Y / N
		Night									Y / N
7		Day	O / R / N								Y / N
		Night									Y / N
8		Day	O / R / N								Y / N
		Night									Y / N
9		Day	O / R / N								Y / N
		Night									Y / N
10		Day	O / R / N								Y / N
		Night									Y / N

Results - Recorded Footage:

Day Test :	Pass / Fail	Night Test :	Pass / Fail

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.

Section 7 of 8 : PTZ Automatic TrackingTest

Site:		Camera Number:		Auditor:	
Date: Day Test		Time: Day Test		Date: Night Test		Time: Night Test	

* Viewing to be done from control room
* A person shall run and walk across various areas of the site with a focus on strategic areas.

	Fibre / GPRS / Satellite	Compression Format:	

Results:

Function	Requirement	Result	Pass / Fail	Comment
Judder (should be minimal)			Pass / Fail	
Overshoot (should be minimal)			Pass / Fail	
Tracks target walking across field of view			Pass / Fail	
Tracks target running across field of view			Pass / Fail	
Tracks target walking towards camera			Pass / Fail	
Tracks target walking towards away from camera			Pass / Fail	
Tracks target running towards camera			Pass / Fail	
Tracks target running towards away from camera			Pass / Fail	
Zooms As expected			Pass / Fail	

Results - PTZ Control Test :

Day Test :	Pass / Fail	Night Test :	Pass / Fail

ESKOM COPYRIGHT PROTECTED

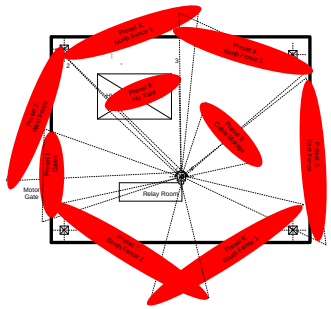
When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

Section 8 of 8: Camera Horizontal Field of View

Site:		Camera Number:		Auditor:	

**Sketch camera field of view as achieved for eaxh PTZ preset position. Number the preset Positions.*
**Include Measurements. Include obstacles*
**Field of view must be determined in the day and at night.*
**Sketch the Worst Case Scenario*

eg



Horizontal Field of View meets operational requirements?	Yes / No

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.

DVR / NVR

Functional Acceptance Test

Site:		Date:	
DVR Make and Model:		Auditor:	

Number of Connected Cameras		Comms Medium:	Fibre / GPRS / Satellite
Resolution and file types of recordings:			
Resolution and file types of short incident clips (if used):			
Resolution and file types of streaming video:			

Incident Operations

The following shall be demonstrated by simulating an incident at a site.

Requirement	Yes / No	Comments
Records for 5s second before the event, the time of the actual event and 15s seconds after motion stops	Y / N	
Signal is sent to Control Room	Y / N	
Sends short video clip / series of still pictures from the camera covering the zone where the alarm triggered to the security control room.	Y / N	
Clip is a lower resolution so that the video or pictures may be sent via GPRS.	Y / N	
The quality of the clip received at the control room is such that the controller can clearly identify whether the intruder detection was triggered by a human.	Y / N	
Control room is able to stream footage from site	Y / N	
Streamed footage allows for observation of site by control room.	Y / N	
Control room is able to operate PTZ	Y / N	
Control room is able to access PTZ preset positions	Y / N	
Control room is able to speak over the PA system	Y / N	
Control room is able to play pre-recorded message over PA System	Y / N	

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.

Recording

Requirement	Yes / No	User Friendly? (1-4)	Comments
DVR can simultaneously record and stream footage	Y / N		
Recordings are electronically watermarked	Y / N		
Recordings show correct time and date	Y / N		
The DVR is able to trigger recordings based on:	Y / N		
- schedule,	Y / N		
- manual trigger	Y / N		
- alarm	Y / N		
It is possible to search recorded events based on:	Y / N		
- date and time	Y / N		
- event	Y / N		
- motion in specific area	Y / N		
- combination of the above	Y / N		
Playback in slow motion is possible	Y / N		
Playback at high speed is possible	Y / N		
Users can play recorded video from several cameras simultaneously	Y / N		
It is possible to 'cut' footage to export only the portion of footage that is of interest	Y / N		
All cameras on site synced to within 1 second of DVR time	Y / N		
DVR time synced to within 1 min of VMS time?	Y / N		

Network Security

Requirement	Yes / No	User Friendly? (1-4)	Comments
Access Level 1:			
- Can perform all operator tasks	Y / N		
- No ability to delete footage	Y / N		
- No ability to view and change network	Y / N		
Access Level 2:	Y / N		
- Has full admin rights	Y / N		
Can view a time and date stamped log of all logon events	Y / N		
Can view a log of all administrative changes made on the system, including who made the change.	Y / N		
Authorised Eskom employees using the client software are able to connect to the server via the Eskom Corporate Network.	Y / N		
Authorised Control Room staff client software shall connects to the server via a dedicated connection	Y / N		

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.

Video Quality

Requirement	Rating	Comments
Streaming over GPRS	poor/ fair / excellent	
Streaming over fibre / satellite connection	poor/ fair / excellent	

General Usability

Evaluator to score the following based on their own user experience and experience watching others use the system.

1: Terrible
2: Poor
3: Meets expectations
4: Exceeds expectations

Requirement	Score (1-4)	Comments
Efficiency: Once users have learned the design, how quickly can they perform tasks?		
Memorability: When users return to the design after a period of not using it, how easily can they re-establish proficiency?		
Errors: How many errors do users make, how severe are these errors, and how easily can they recover from the errors?		
Satisfaction: How pleasant is it to use the design?		

Results Summary

Test	**Result**	**Remarks**
Overall	**Pass / Fail**	

Auditor's Signature:		**Date:**	

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.

Video Management System

Functional Acceptance Test

Site:		Date:	
VMS System:		Evaluator:	

The following shall be demonstrated on a live system.
In order to determine the user friendliness of the system, the Eskom evaluator shall operate the software with instructions from the contractor.

The following scoring system shall be used for 'user friendliness':

1: It is not possible to figure out how to do the activity without instructions. Activity is slow and requires many steps. System does not perform optimally.
2: Once the operator has been using the system for a while, the activity will be fairly easy and perform relatively well.
3: It is fairly easy to figure out how to do the activity. The system performs as expected.
4: It is easy to figure out how to do the activity. The system performs above expectations.

General Control Room Operations

	Yes / No	User Friendliness (0-4)	Comments
Operator can:			
Select an individual site	Y / N		
Select each camera at the site	Y / N		
Sequentially switch between cameras	Y / N		
Operate PTZ through full range	Y / N		
PTZ can be controlled using pre-set positions	Y / N		
Play recorded message on PA system	Y / N		
Speak using PA system	Y / N		
Start recordings of live footage	Y / N		
View recorded footage	Y / N		
View the location and status of all sites on a map	Y / N		

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.

Incident Operations

The following shall be demonstrated by simulating an incident at a site.

	Yes / No	User Friendliness (0-4)	Comments
In normal state, no video is shown.			
Alarm triggers at a site: controller sees a series of still images or a short video clip of the triggered zone.	Y / N		
The controller can choose to stream video from the site.	Y / N		
There is an event queue to allow the management and acknowledgment of multiple alarm events.	Y / N		
It is possible to look at a new event without having acknowledged a previous event.	Y / N		
Controller can view the location of alarms and cameras on a site layout	Y / N		
Controller can enter comments and link them to the event	Y / N		
It is possible to 'escalate' incidents to another workstation running the client software	Y / N		
Events and actions are logged for auditing purposes	Y / N		
VMS system can track movement and highlight which area of the camera field of view has triggered an alarm (recommended but not compulsary)	Y / N		

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.

Recording			
	Yes / No	User Friendliness (0-4)	Comments
VMS can simultaneously record and stream footage	Y / N		
Recordings are electronically watermarked	Y / N		
Recordings show correct time and date	Y / N		
The VMS is able to trigger recordings based on:	Y / N		
- schedule,	Y / N		
- manual trigger	Y / N		
- alarm	Y / N		
It is possible to search recorded events based on:	Y / N		
- date and time	Y / N		
- event	Y / N		
- motion in specific area	Y / N		
- combination of the above	Y / N		
Playback in slow motion is possible	Y / N		
Playback at high speed is possible	Y / N		
Users can play recorded video from several cameras simultaneously	Y / N		
It is possible to 'cut' footage to export only the portion of footage that is of interest	Y / N		

Infrastructure and Connections			
	Yes / No	User Friendliness (0-4)	Comments
Access Level 1:			
- Can perform all operator tasks	Y / N		
- No ability to delete footage	Y / N		
- No ability to view and change network settings.	Y / N		
Access Level 2:	Y / N		
- Has full admin rights	Y / N		
Can view a time and date stamped log of all logon events	Y / N		
Can view a log of all administrative changes made on the system, including who made the change.	Y / N		
Authorised Eskom employees using the client software are able to connect to the server via the Eskom Corporate	Y / N		
Authorised Control Room staff client software shall connects to the server via a dedicated connection	Y / N		

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.

Video Quality

	Rating	Comments
Streaming over GPRS	poor/ fair / excellent	
Streaming over fibre / satellite connection	poor/ fair / excellent	

General Usability

Evaluator to score the following based on their own user experience and experience watching others use the system.

1: Terrible
2: Poor
3: Meets expectations
4: Exceeds expectations

	Score (1-4)	Comments
Efficiency: Once users have learned the design, how quickly can they perform tasks?		
Memorability: When users return to the design after a period of not using it, how easily can they re-establish proficiency?		
Errors: How many errors do users make, how severe are these errors, and how easily can they recover from the errors?		
Satisfaction: How pleasant is it to use the design?		

Results Summary

Test	Result	Remarks
Overall	**Pass / Fail**	
Auditor's Signature:		**Date:**

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.