Eskom	Report	Technology

Title:	**SCOPE OF WORK FOR INTEGRATED PHYSICAL SECURITY SYSTEM**	Unique Identifier:	**240-170000258**
		Alternative Reference Number:	**<n/a>**
		Area of Applicability:	**Engineering**
		Documentation Type:	**Report**
		Revision:	**4**
		Total Pages:	**38**
		Next Review Date:	**n/a**
		Disclosure Classification:	**Controlled Disclosure**

Compiled by	**Functional Responsibility**	**Authorized by**
	Naidoo	
Donald Moshoeshoe	**Cornelius Naidoo**	**Judith Malinga**
Snr Engineer- PTM&C	**Middle Manager – Telecoms & Physical Security T&S**	**Senior Manager – PTM&C**
Date: 02/08/2023	Date: 7/8/2023	Date: 08/08/2023

PCM Reference: **PTM&C**

SCOT Study Committee Number/Name: **Part 16 - DC & Auxiliary Supplies**

Content

Tables

1. Introduction

There have been numerous security breaches at Eskom sites resulting in theft of Eskom assets. In order to prioritise people's safety and protect Eskom assets and installations, the review and improvement of physical security measures at these sites is necessary to ensure that current threats are appropriately mitigated, through the implementation of suitable security measures, systems and procedures. This document provides an overview of Eskom's requirements for the design, supply, installation and commissioning of an Integrated Security System at Eskom Substations and Telecoms sites.

2. Supporting Clauses

2.1 Scope

This document provides an overview of Eskom's requirements for the design, supply, installation and commissioning of an Integrated Physical Security System (IPSS) at Eskom substations. The Integrated Security System may be an integration of the CCTV system, intruder detection system, Access Control System (ACS), alarm system, public address (PA) system, Intrusion pre-detection system and interfaces to the Physical Security Information Management (PSIM) system (includes IT infrastructure) depending on site requirements. The document outlines business objectives to be fulfilled by the Integrated Security Solution and provides an overview of the envisaged system functionality. The Contractor shall use the accompanying technical specifications referenced together with details outlined in this document when tendering for the integrated security system.

Note: There might be projects where the scope of work includes only a subset of the systems mentioned above. In these instances the scope of work shall clearly indicate the excluded subsystems using the table in Annex C.

2.1.1 Purpose

The document serves as a technical scope for an integrated security system at Eskom substations and Telecoms sites and stipulates technical requirements and deliverables.

Note: The word Substation is used in generic terms in this document, this shall refer to any Eskom site where the requirements of this document are implemented.

2.1.2 Applicability

This document is applicable to Eskom Substations and Telecoms sites.

2.2 Normative/Informative References

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

2.2.1 Normative

[1] ISO 9001 Quality Management Systems.

[2] 240-102220945 Specification for Integrated Access Control System for Eskom sites

[3] 240-91190304 Specification for CCTV Surveillance with Intruder Detection

[4] 240-86738968 Specification for Integrated Security Alarm System for Protection of Eskom Installations and its subsidiaries

[5] 240-170000098 Security Public Address Systems for Substations and Telecoms high sites

[6] 240-170000096 Physical security integration standard

[7] 240-170000086 Roles and Accountabilities for Lifecycle Management of Physical Security Systems in the Transmission Division

[8] 240-170000257 Technical Evaluation Criteria for the Integrated Security System

[9] 240-60725641 Specification for Standard (19 inch) Equipment Cabinets

[10] 240-46264031 Fibre-Optic Design Standard – Part 2: Substations

[11] DEM2412993 & 2425114 LAD (Logical Architecture Definition) PAC (Physical Application Component) for Physical Security Information Management System(PSIM)

[12] Business Requirement Specification DEM_2412993 & 2425114 Tx and ET Security Monitoring System

[13] 240-170000691 Standard for Intrusion pre-detection systems used at Eskom sites

[14] 240-170000723 Generic Technical Requirements for Physical Security Technologies Contracts

[15] 240-171000171 Commissioning guideline for secondary plant physical security system

2.2.2 Informative

[16] 240-836884419 PTM&C Technology Development

[17] 240-78980848 Specification for Non-Lethal Energized Perimeter Detection System (NLEPDS) for protection of Eskom installations and its subsidiaries

2.3 Definitions

2.3.1 General

Definition	Description
Tender	A tender refers to an open or closed competitive request for quotations / prices against a clearly defined scope / specification.

2.3.2 Disclosure Classification

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

2.4 Abbreviations

Abbreviation	Description
AC	Alternating Current
AGA	Architecture Governance Assessment
CCTV	Closed Circuit Television
DC	Direct Current
DVR/NVR	Digital Video Recorder/Network Video Recorder
FAT	Factory Acceptance Test
GUI	Graphical User Interface
IACS	Integrated Access Control System
IPSS	Integrated Physical Security System
LAN	Local Area Network
MCB	Miniature Circuit Breaker
PA system	Public Address System
PIR	Passive Infrared

Abbreviation	Description
PSIM	Physical Security Information Management
PSIRA	Private Security Industry Regulatory Authority
PTZ	Pent Tilt Zoom
SAT	Site Acceptance Test
SM	Single Mode
TCP/IP	Transmission Control Protocol/Internet Protocol
UPS	Uninterruptable Power Supply
VMD	Video Motion Detection
WAN	Wide Area Network

2.5 Roles and Responsibilities

Roles shall be as outlined in 240-170000086

2.6 Process for monitoring

Not Applicable

2.7 Related/Supporting Documents

Not applicable

3. Project scope

3.1 General project scope

The scope includes requirements for an integrated security system comprising of an Access Control System, CCTV system, Intrusion pre-detection system, alarm system, public address (PA) system and interfaces to the PSIM system (includes IT Infrastructure).

The contractor shall design, manufacture, supply, develop user documentation, perform testing at works, deliver, install, and commission the Integrated Security System and associated equipment (hardware/software etc.) at the Substation/Telecoms site and Zero Control (Simmerpan, Germiston) according to the associated technical specifications.

The scope of work for the Contractor for the Integrated Security System will include the following:

a) Produce basic and detailed designs for the Integrated Security System. The detailed design must include detailed designs for the Access Control System, CCTV system, Intruder detection system, alarm system, the public address system and the PSIM system (includes IT Infrastructure).The design must also cover integration of these different systems and the NLEPDS (existing) into an Integrated Security System;

b) Present the proposed designs to PTM&C design review team (DRT) for acceptance;

c) Installation and configuration of substation security LAN Infrastructure;

d) Installation, configuration and commissioning of the CCTV system in totality on site as per Eskom standard (240-91190304);

e) Installation, configuration and commissioning of the Integrated Access Control System (IACS) in totality on site as per Eskom standard (240-102220945);

f) Installation, configuration and commissioning of intruder detection system in totality on site as per Eskom standard (240-91190304,240-86738968 & 240-170000096);

g) Installation, configuration and commissioning of alarm system in totality on site as per Eskom standard (240-86738968);

h) Installation, configuration and commissioning of public address system in totality on site as per Eskom standard (240-170000098);

i) Installation, configuration and commissioning of intrusion pre-detection system in totality on site as per Eskom standard (240-170000691);

j) Integration of the Access Control System (ACS), CCTV system, Intruder detection system, alarm system, public address system into an integrated security system (240-170000096) to interface with the PSIM system;

k) Provide services as per 240-170000723;

l) Installation, configuration and commissioning of interfaces to the Physical Security Information Management (PSIM), including firewall configuration and Telecoms circuit commissioning, for data collection, incidents management, data correlation, controlling functionality (CCTVs, IACS systems, PA systems, etc.) and provision of real-time dash boards and reports (refer to DEM2412993 & 2425114);

m) Conduct FAT and SAT tests before commissioning the complete integrated system;

n) Compile site as built drawings with electrical and engineering detail;

o) Create a Graphical User Interface (GUI) and behaviour models for the site;

p) Produce a detailed design report for the integrated security system as per the index in Annex B of this document;

Notes:

1) The generic site layouts in Annex D shall be used for typical site security zoning

3.2 Integrated Access Control System (IACS)

a) The Integrated access control system will be used to manage access rights of Eskom employees, visitors and contractors in and out of different areas at site.

b) The system will also be used to grant and limit access permissions in and out of areas such as secure and non-secure areas.

c) The offered system shall comply with requirements of Specification for Integrated Access Control System (IACS) for Eskom sites (240-102220945).

d) The system should support a tiered architecture which will allow monitoring of the site both locally and remotely comprising of field devices (biometric & card readers) at site level and system management servers at the remote security control room (zero control).

3.2.1 IACS devices layout

The envisaged Integrated Access Control devices for the site and their locations are shown in Table 1 below:

Table 1: IACS devices positioning

Area	Point	Device	Status Contact	Lock	Evacuation Device	Bypass
Main Gate (Inbound traffic)	Exterior Perimeter Fence (Gooseneck Mount)	Card Reader	Gate Status Contact	Electro Mechanical Lock	None	Mechanical Bypass

Area	Point	Device	Status Contact	Lock	Evacuation Device	Bypass
	Energized Fence Gate	Integrated with exterior gate automation	Gate Status Contact	Electro Mechanical Lock	None	Mechanical Bypass
	Inner Perimeter Fence (Gooseneck Mount)	Card + Biometric Reader	Gate Status Contact	Electro Mechanical Lock	None	Mechanical Bypass
Outbound Traffic	Exterior Perimeter Fence (Gooseneck Mount)	Card + Biometric Reader	Gate Status Contact	Electro Mechanical Lock	None	Mechanical Bypass
	Energized Fence Gate	Integrated with interior gate automation	Gate Status Contact	Electro Mechanical Lock	None	Mechanical Bypass
	Inner Perimeter Fence (Gooseneck Mount)	Card Reader	Gate Status Contact	Electro Mechanical Lock	Emergency Exit Button	Mechanical Bypass
Guard House	Entrance Door	Card + Biometric Reader (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Equipment Room Door (Inside)	Card + Biometric Reader (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
Control Room Buildings (	Office Door	Card Reader (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Control Room Entrance Door	Card + Biometric Reader	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Control Room Back Door (Emergency Exit)	Emergency exit break-bar	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Control Room Double Door	Card Reader (Inside only)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Battery Room	Card + Biometric (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Carrier Room	Card + Biometric (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
Office buildings & store rooms	Main entrances	Card + Biometric (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass

Note: Ideally the existing Eskom approved cards should be used for the new access control system. Eskom's approval shall be obtained before deciding on the access cards for the system.

3.2.2 IACS high level devices positioning and architecture philosophy

a) The contractor is required to submit a detailed design depicting the proposed architecture and narratives of how the IACS functional requirements will be achieved. The implemented architecture for IACS should comply with principles outlined in the technical standards for IACS [2].

b) In addition to ensuring that the installed system operates as required on site, the contractor is also required to ensure that the system enables remote monitoring and control through the Eskom's WAN.

3.3 CCTV system

a) A CCTV system shall be installed and the proposed system for the site is intended to provide the guards/ control room operators with a single point from where they can view and verify alarm events from the Intrusion detection system and energized fence triggers without having to physically respond to the alarm event in the case of a false/nuisance alarm and correctly assess and verify positive alarm events in the event of an attempted or successful intrusion attempt.

b) The offered system shall comply with requirements of Eskom standard for CCTV system (240-91190304).

c) The CCTV system shall be integrated with video analytics and automatically record any alarm event by means of the 30 seconds pre-event buffer, the actual event (for however long motion is detected by the camera) and at least a 30 seconds post event time period. The system shall utilize a video analytics system as pre-detection to automatically generate alarms and perform event recording.

d) It is proposed that static thermal cameras with video motion detection be installed along the perimeter of the Substation to provide both surveillance and detection functionality. In addition it is proposed that PTZ cameras be installed for zooming and recognition functionality.

e) The CCTV system shall be connected to the security LAN to enable event driven video streaming to the local security room and zero control (Simmerpan, Germiston).

f) A video intercom system must be installed at the main gate entrance and the audio feed and camera feed from the unit must be integrated into the local NVR to ensure both visual and audio recording of events. The purpose of this unit is to enable the security control room to interact with unannounced visitors and non-Eskom staff. The communication will be point-to-point between the gate and the security control room and will not be integrated with the gate control system.

g) The contractor shall determine the required camera lens types that will ensure that the positioning of the cameras results in the most optimised and economical installation of the cameras at site. This includes ensuring that a continuous visibility is created along the perimeter by eliminating blind spots with one camera having the next camera within its field of view for effective monitoring.

h) All steel poles and structures shall be hot-dipped galvanised.

3.3.1 CCTV System devices layout and positioning

The areas identified where CCTV devices (cameras) are to be installed are listed in Table 2 below. The cameras are to be positioned as per the site layout.

Table 2: CCTV cameras positioning

Area	Site location	Device(s)
Perimeter and Main Access Gate	Perimeter fence	Static thermal Cameras
		PTZ Cameras
	Access Gate	Static Cameras

Area	Site location	Device(s)
		Video Intercom
	Guard House	Interior Static Cameras
Control Room Building	Outside Battery Room entrance	Exterior static Cameras
	Control Room Door	Interior Static Cameras
	Control Room Emergency Exit	Interior Static Cameras
	Control Room Double Door	Exterior Static Cameras
	Carrier Room	Interior Static Cameras
Office buildings & store rooms	Main entrances	Exterior Static Cameras

3.4 Intruder Pre-detection system

a) Intrusion pre-detection units shall be installed in all areas of the substation including buildings, rooms and substation perimeter area which need to be protected.

b) The sensors shall be placed so as to effectively detect intrusion into the protected (secured) areas for the following:

i. Unauthorised movement around/inside a protected area at site

ii. Tunnelling underneath the fences,

iii. Separation of electric fence conductors,

iv. Cutting and climbing over perimeter barrier fences/walls,

v. Vibrations caused by Digging underneath, breaking through and climbing over the barrier fences/walls.

c) The Intrusion pre-detection system installed shall comply with the requirements of the standard for intrusion pre-detection systems used at Eskom sites (240-170000691).

3.4.1 Intrusion Pre-detection system devices layout and positioning

Table 3: Intruder detection devices positioning

Area	Point	Device(s)
Guard House	Server Room	Interior PIRs
Control Room Buildings	Outside Office Door	Door Contact
	Office Interior	Interior PIRs
	Battery Room Door	Door Contact
	Battery Room	Interior PIRs
	Control Room Door	Door Contact
	Control Room Emergency Exit	Door Contact
	Control Room	Interior PIRs
	Building interior	Interior PIR
	Carrier Room	Interior PIR
Office buildings & store rooms	Main entrances	Door Contact
Substation Perimeter	On each perimeter camera	Intrusion detection analytics

Substation Perimeter	Outer wall/barrier fences	Exterior intruder pre-detection system (Contractor to propose a system)

Note: The use of passive infrared (PIR) units is not recommended for exterior use due to prevalence of nuisance alarms associated with the units.

3.5 Public Address System

a) The installation of a PA system is required in order to engage potential intruders and issue warnings.

b) The PA system shall be able to be remotely and locally operated when necessary.

c) The system must be operable via the guard house and remotely via the responsible control rooms to warn would be attackers of the restriction of access to the site.

d) Voice recordings shall be synchronized with the cameras and recorder on the local NVR via a suitable audio input to ensure synchronization of events.

e) The installed PA system shall comply with the requirements of technical specification for Public Address Systems (240-170000098).

3.5.1 PA system devices layout and positioning

The speakers shall be mounted on the existing perimeter light masts around the site perimeter where feasible.

3.6 Alarm system

a) The alarm system shall be installed and will form an integral part of the other security systems installed at site to provide proactive coverage and monitoring of all protected areas i.e. Site perimeter, entrances, buildings, HV yard and other strategic places within the substation. The alarm system shall be triggered by the following inputs:

   1) Due to Camera video analytics alarm detection on the zone(s).
   2) Alarm inputs from electric fence.
   3) Alarm inputs from Intrusion pre-detection devices.
   4) Alarm inputs from access control points.

b) The installed alarm system shall comply with the requirements of Specification for Integrated Security Alarm System for Protection of Eskom Installations and its subsidiaries (identifier: 240-86738968) and alarming requirements of other integrating technologies mentioned above, forming part of the integrated security system at site.

3.7 System integration

a) The subsystems outlined above are required to be integrated into a unified integrated security system in line with Eskom’s technical specification for security systems integration (240-170000096).

b) The integrated system shall achieve the cause the effect matrix requirements in site zoning below and in tabled Annex A.

3.7.1 Site Zoning

The table below shows a typical site zoning:

Table 4: Site Zoning

Site Zone/ security level	Description	Area	Security measures

Zone 1	General area	• Substation Inner perimeter (Open area)	• Access Control on main entrances • Video surveillance • Intrusion pre-detection system • PA system • Alarm system
Zone 2	High risk or critical areas	• Entrance area • Guard House • Guard House Equipment Room • Battery Room • Carrier Room • Control building	• Access control measures • Passive infrared beams • Video surveillance • PA system • Alarm system

3.7.1.1 Site Zone 1: General area

a) This is the outside area directly adjacent to the fences are monitored via the perimeter CCTV system.

b) CCTV monitoring shall be conducted at the main vehicle entrance as an overview of the area and to serve as identification point for visitors.

c) CCTV system to be installed on the perimeter in order to monitor and verify alarms on the perimeter intruder detection system and energized fence system.

d) PTZ CCTV Cameras to be installed at strategic positions on the site and provide a controllable interface from where specific activities can be monitored both locally and remotely.

e) A PA system shall be installed to communicate remotely and warn possible attackers as a deterrent.

f) An intruder -pre-detection system is to be installed on the outer barrier to act as the first line of detection.

g) CCTV video analytics to be utilized as an additional pre-detection system along the site perimeter.

h) An intercom system with an integrated camera shall be installed at the gate as a point of communication between visitors and the site guards in the guard house at site.

i) Rather than using PIR's to detect movement in the HV Yards, the CCTV system's Video Motion Detection System (VMD) will be utilized to perform the task. The VMD will function as the Intrusion detection system in this area. PTZ CCTV Cameras should be setup in a manner so as to sweep the respective fields of view in "patrol" mode and should generate alarms by utilizing Video Motion Detection.

j) An alarm system to alarm for any intrusions detected.

k) If the site is unmanned (no guards) the following interlocking shall apply: At the site gates entrance area an electronic Access Control reader consisting of a card and fingerprint/card reader shall be installed as initial verification of authorized personnel. Upon positive verification all the gates should simultaneously open allowing the vehicle/person to enter the site. The gates should automatically close simultaneously 10 seconds after opening. If an object is detected preventing the gates from closing, an alarm should be triggered. When exiting the site, at the entrance area an electronic Access Control reader consisting of a card and fingerprint reader should be installed as initial verification of authorized personnel. Upon positive verification all the gates should simultaneously open allowing the vehicle/person to exit the site. The gates should automatically close 10 seconds after opening. If an object is detected preventing the gates from closing, an alarm should be triggered.

l) If the site is manned (guards at site) the following interlocking shall apply: An electronic Access Control reader consisting of a card and fingerprint reader shall be installed as initial verification of authorized personnel. Upon positive verification the energized fence gate will open after which the outer barrier gate will open to allow the vehicle inside the sally point. Upon entry into the sally point the outer barrier gate will close effectively locking the visitor in the sally point. At this time the guard will be able to interact with the visitor and conduct searching of the person and vehicle. Only after the guard has completed his duties will the guard exit the sally point at which time the guard has to tag on the inside of the guard house to verify the completion of his activities (The guard in turn will be required to tag on the inner perimeter pedestrian gate to enter the sally point, and then tag out of the sally point and only then tag in the guard house before the system will open, this logic followed will force the guard to enter the sally point and conduct the searching rather than just tagging a visitor in through the guardhouse point) when the visitor on his turn can then again tag in the reader in the sally point (Card reader only). At this time the inner gate will open to allow the visitor into the restricted area. Exiting of the site will be the reverse operation of the entry sequence.

3.7.1.2 Site Zone 2: High risk or critical areas

a) At the entry points into these areas, biometric and card readers will be utilized as it is restricted areas and only personnel with Permit-To-Work are allowed inside this area. The biometrics is used to enforce this rule.

b) All buildings shall use an intrusion detection system which consists of a PIR and Door Contact to verify the status of the room when it is supposed to be unoccupied and subsequently generate an alarm if an intrusion is detected. The intrusion system is to be automatically disarmed upon granting entry to a person through the IAC system and arming upon the exiting of such a person.

c) HV Regulation require that the doors to the battery rooms remain open when occupied, the system will expect this open status and will generate an alarm if a person is detected inside the area even if it is an authorized person as the door is supposed to be in the open position.

d) An alarm system to alarm for any intrusions detected.

Note: The generic site layouts in Annex D shall be used to depict site zoning

3.8 Site monitoring

a) There shall be a security manager workstation at site in the security building for local allocation and revoking of access rights and controlling of security workflows.

b) There shall be a maintenance manager workstation in the security building for controlling of maintenance workflows.

c) Some or all of the functions listed in item (a) and (b) above may be combined into a single physical workstation. The workstation software GUI shall be based on the operator log on credentials to be able to perform functions listed in item (a) and (b) above.

d) The security alarms and CCTV visuals should be routed to remote Security Control Centre (zero control) through the Eskom WAN.

e) The system shall allow the remote Security Control Centre to be able to remotely control PTZ cameras at site.

f) The system shall allow the remote Security Control Centre to have audio (via PA system) and data communication with the site. Including the ability to give audio warnings over the PA system to the security zone that detected an intrusion.

g) It shall be possible for the Security Control Centre to remotely retrieve any of the stored event data or video streams in real time.

3.9 Communication

a) The network shall provide redundancy in the event of path failure.

b) Single mode optical fibre is preferred as the physical transport medium of choice for on-site communication. The installation shall conform to Eskom standard, 240-46264031.

c) For indoor connections and outdoor connection distances below 5m, CAT5e/CAT6 UTP copper cable may be used.

d) The detailed design shall include the security LAN design used to facilitate communications between security system elements.

e) The IT Infrastructure (LAN, cabling, servers, etc.) design shall be detailed in the IT documentation.

f) The Ethernet communication channel on the Eskom Telecomms WAN (multiplexer) shall be specified for a minimum 10/100/1000 Base-T with auto negotiation. The interface can be a RJ45 connector using a CAT5e/CAT 6 cable or a fibre optic cable.

3.10 PSIM requirements

a) The centralized PSIM infrastructure is located at Zero Control in Simmerpan, of which the design shall be defined in the detailed design stage of the project (refer to LAD and BRS: DEM_2412993 & 2425114). For this enquiry the Tenderers are required to supply, install, configure and commission interfaces for integration to the PSIM system already installed at Zero Control in Germiston, refer to Annex E of this document for PSIM interfaces integration requirements and guideline.

3.11 Power supply requirements

a) All system servers shall be housed in 19-inch equipment cabinets as specified in the Eskom standard 240-60725641. This specification covers the earthing requirements in the cabinet as well.

b) Power shall 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) Perimeter Cameras
   2) Indoor cameras
   3) PA system devices
   4) Site controllers and server based equipment
   5) Other security related equipment such as gate motors and electric fence energizers.

c) The system shall have a power failure indication that shall be sent through to the remote security control room should the supply be interrupted.

d) The existing power systems at site shall be used as the primary power sources, provided that the standby time (autonomy) requirements of the site are not adversely affected.

e) Tenderers are required to propose a suitable standby power system sized appropriately to handle the expected system load. Eskom may however decide to utilise the existing standby batteries at site.

3.12 Cabling and trenching

a) The contractor shall provide detailed as built drawings indicating cable routes, installation locations of all equipment as part of the detailed design submission.

b) The contractor will be responsible for laying and terminating the cable from the peripheral devices to the control room.

c) Data and low voltage cable installations shall be separated from the mains power installations by a minimum of 500mm.

d) Where data and low voltage cabling has to cross power cabling, this shall always be at 90°

e) All wiring shall be concealed inside trunking or conduit. No exposed wiring will be accepted.

f) Cable runs next to devices that may cause electro-magnetic interference shall be avoided or suitable shielding provided.

g) Tension when pulling cables shall not exceed recommended safe values as specified by the cable manufacturers.

h) Supply and installation of all trunking, conduit, glands etc. form part of the contractor’s scope of work.

i) Cable joints shall be avoided as far as practically possible.

j) An industry acceptable Source, destination cable marking system shall be used to mark all cables.

3.13 Project technical services

a) Tenderer shall provide services outlined in 240-170000723 Generic Technical Requirements for Physical Security Technologies Contracts.
b) Tenderer to include a 5 year training, support, repair and maintenance as part of the project solution.

3.13.1 Organisation Experience

a) Tenderer must submit company organogram, indicating team composition(s).

b) List of similar projects must be provided.

c) CVs for the company and staff must be submitted with the following experience / competencies:

    1) Experience in design and installation of Alarms system.

    2) Experience in design and installation CCTV Systems, maintenance & associated communication network system fault finding.

    3) Experience in design and installation of Access Control Systems (IACS).

    4) Experience in design and installation of PA Systems.

    5) Experience in design and installation of Intrusion pre-detection Systems.

    6) Experience in design and installation of an Integrated Security System.

    7) Experience in design and installation of the IT Infrastructure and PSIM.

d) Project Lead Engineer that is professionally registered (Pr Eng/Pr Tech) with ECSA (Engineering Council of South Africa) that will sign off the entire design.

e) Experience in providing training on all the components in the Integrated Security System

3.14 Technical returnables and index

a) The index in Annex F of this document provides a guideline of how the technical returnables should be indexed by the Tenderers.

b) The supplier shall produce and submit a detailed design report for the integrated security system as per the index in Annex B of this document.

4. Authorisation

This document has been seen and accepted by:

Name and surname	Designation
Mario Peterson	Middle Manager (Acting) – PTM&C Project Engineering and Support

5. Revisions

Date	Rev	Compiler	Remarks
August 2023	4	R Moshoeshoe	Corrected references in scope selection annexure
April 2023	3	R Moshoeshoe	Included requirements for PSIM interfaces
June 2022	2	R Moshoeshoe	Included requirements for intrusion pre-detection system
June 2021	1	R Moshoeshoe.	First issue

6. Development team

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

- Chris Van Reenen
- Victor Lehobo
- Phelokazi Ndlovu

7. Acknowledgements

Not applicable

Annex A – Integrated Alarming cause and effect matrix

	Unauthorised Access					**Authorised Access**
	Breach physical perimeter fence or virtual perimeter fence by smart cameras/ beams/etc.	**Outdoor Sensor Triggers**	**Camera Outdoor Protected Area Triggers**	**Indoor Sensor Triggers**	**Camera Indoor Protected Area Trigger**	
Perimeter flood lights activated at night only	✓					
Substation flood lights activated at night only	✓	✓	✓	✓		
Security floodlights activated at night only	✓	✓	✓	✓		
Control Room lights 24hr				✓	✓	
Switch Room lights 24hr				✓	✓	
Any other indoor room				✓	✓	
DVR/NVR record footage	✓	✓	✓	✓	✓	✓
Alarm signals(text and video) sent to Security Control Centre	✓	✓	✓	✓	✓	
PTZ tracking sent to Security Control	✓	✓	✓			
PA System recorded message activated	✓			✓	✓	
PA System Security Control operated if positive alarm verified	✓	✓		✓	✓	

	Unauthorised Access					**Authorised Access**
	Breach physical perimeter fence or virtual perimeter fence by smart cameras/ beams/etc.	**Outdoor Sensor Triggers**	**Camera Outdoor Protected Area Triggers**	**Indoor Sensor Triggers**	**Camera Indoor Protected Area Trigger**	
Alarm System Zones triggered	✓	✓	✓	✓	✓	
Alarm Zone events sent to Security Control	✓	✓	✓	✓	✓	
Indoor Siren automatically activated				✓		
Strobe light automatically activated	✓	✓	✓	✓	✓	

Annex B – Detailed design report index for integrated security system

a) Overview of functional specification

b) Scope of work

c) High Level Integration

  1) Local vs remote monitoring and control capabilities

  2) Software and network config files.

  3) Cause and effect matrices (e.g. if alarm on fence, lights and image sent to control)

d) System Architecture (to include Logical and physical design, networking and bandwidth requirements, Information flow, Physical security information management, User access profile management and enrolment process, cyber security controls e.g. firewalls, DMZ, System support remote access authentication etc.)

e) Lifespan of System and product software versions (include 10 year life span support)

f) Recommended Maintenance (Procedures, Spares and FMECA- Failure mode effects and criticality analysis, tools and test equipment, training requirements-engineering and field operations)

g) System commission and acceptance testing procedure (commissioning results to be provided prior to system handover (minimum tests shall be as per 240-171000171).

h) Annex A – Drawings

  - Site layout
  - CCT Field of view
  - Site Security Zoning
  - System Configuration
  - Security LAN and Fibre Reticulation
  - Cable and trench layout
  - Power reticulation
  - Control Panels
  - Electric fence and energiser
  - Security control room drawings/configuration

i) Annex B – Equipment Specification

  - Access Control & Intrusion Detection
  - Camera Surveillance System
  - Alarm System (if it is a separate controller)
  - Lighting Control System (if it is a separate controller)
  - PA system (if it is a separate controller
  - Electric fence and Energiser (If it is a separate controller)
  - Physical security information management
  - Data storage equipment on site and at Remote Security Control room

j) Annex C – Datasheets

- Access Controllers
- Card Readers
- Biometric Readers
- Maglocks
- Break Glass Units
- Door Contacts

k) PIR Sensors

- Power Supplies (including UPS sizing)
- Intercoms
- Cameras
- Video Recorders
- Client Workstations
- Network Switches
- Fibre Converters
- Enclosures & Racks
- PA systems
- Security LAN and firewalls

l) Annex C- Bill of Materials

Annex C – IPSS Project Scope Selection

Lead Engineer:		**Tel:**	
Lead Engineer's Department:			
Project name:			
Project No/WBS.:			
Region /Grid			
Substation/ET site:			
Offsite Security Control Centre:			

The table below shall be used to indicate systems that are included in the project scope:

System	Generic sections of scope of work (240-170000258) - applicable to all Systems	Applicable sections in the generic scope of work (240-170000258)	System included in the Project Scope (yes/No)
Integrated Access Control System(IACS)	3.1, 3.7, 3.8, 3.9, 3.11, 3,12, 3.13, 3.14	3.2 & Generic sections	
CCTV System		3.3 & Generic sections	
Intrusion pre-detection System		3.4 & Generic sections	
Public Address System		3.5 & Generic sections	
Alarm System		3.6 & Generic sections	
Interfaces to PSIM system		3.10	

Note:

1. Where a system is not included as part of the project scope, details relating to such a system shall be treated as information only and should be excluded from the project costing.
2. Where the project scope includes the NLEPDS refer to 240-170000192 & 240-134779125.
3. Where there is no requirement to interface to PSIM, it will reflect as not applicable for implementation but the design must still comply to the requirements as per the IT documentation ([11] and [12]). Instead of Bernina, the LAD and BRS documents shall be read as applicable to the substation referred to in this scope of work.

	Name	**Designation**	**Signature**	**Date**
Project Scope verified by:				
Project Scope Approved by:				

Annex D: Typical site layout

The generic site layout below shall be used for a typical site zoning

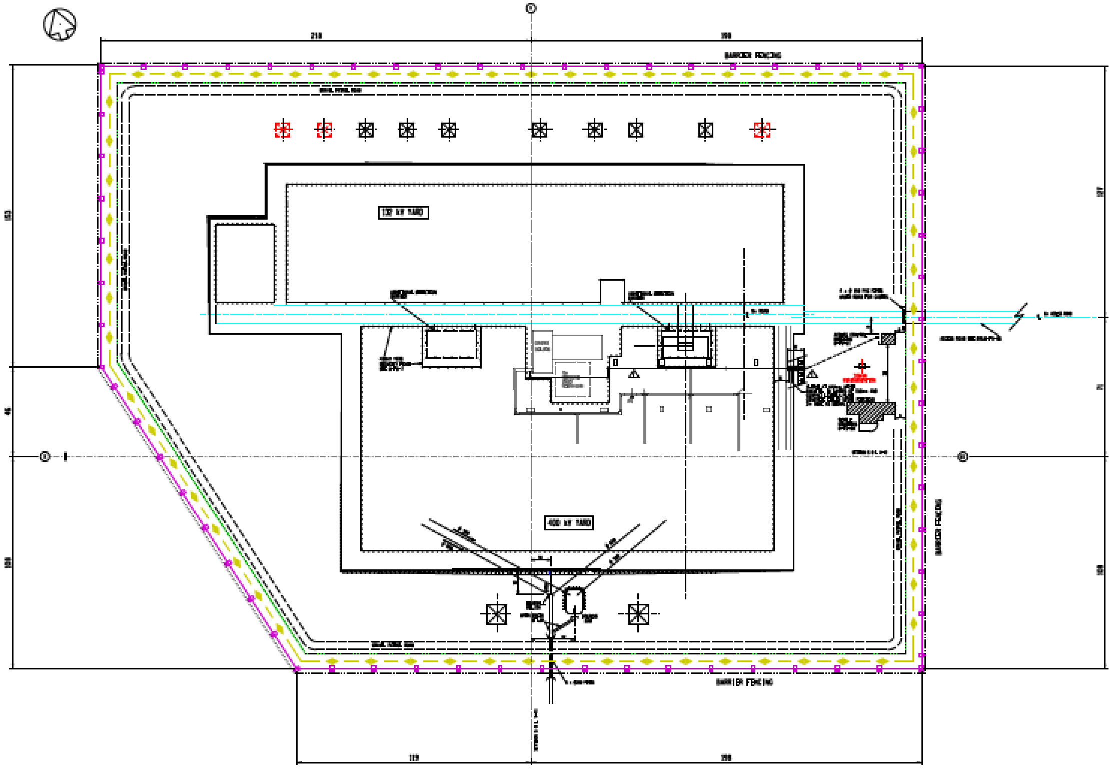


Figure D1: Typical site layout Tx Substation (refer to drawing THE22P02-SE-42)

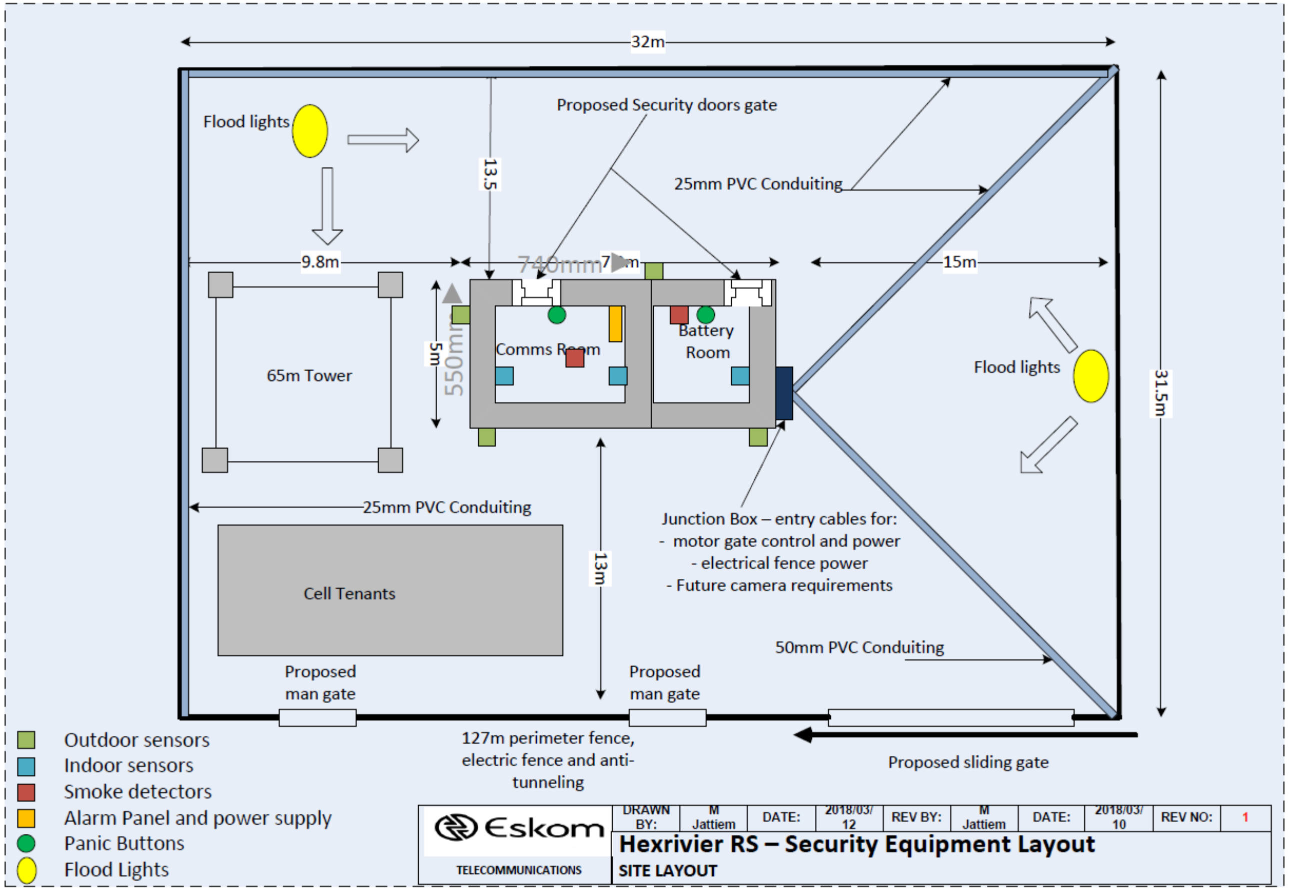


Figure D2: Typical site layout for ET Site

Annex E: PSIM interface integration requirements and guideline

1. Introduction

The Physical Security Information Management (PSIM) system and its centralised infrastructure for Eskom Transmission is installed at the Security Control Centre (Zero Control) at Simmerpan Complex in Germiston. Any security projects that require security remote monitoring and control shall use this guideline on how to interface to the existing installed PSIM system to standardise and streamline the monitoring infrastructure optimally.

2. PSIM capabilities and features

a) The installed PSIM system provides a software-based platform that is scalable and has modular system architecture that enables multiple vendors to integrate their subsystems (e.g., CCTV, access control, intrusion pre-detection, public address, alarm system etc) to it.

b) The PSIM system software is a licensed model and allows further future extensions (functional and capacity-related). The software's licensing scheme shall be based on the number of subsystems/clients/servers installed as well as on the functionalities of the PSIM system and the total number of installed devices.

c) The system uses the Client-Server model to monitor all connected sub-systems and enables bidirectional communication i.e. receiving and transmitting information and events to and from the connected systems

d) The system manages (Accept/Defer/Fetch/Assign/Complete) the events received from the sub-systems either individually or in a grouped presentation.

e) The system offers a user interface and operating concept in modern Windows style.

f) In the network mode, devices can be connected to any workstation within the system. The linkage with PSIM is established via pure software interface modules. The workstations can work independently, i.e. in case of an interruption of the server connection, the events registered by local systems are still displayed.

g) The system has capability to link-up to bus systems such as EIB/KNX, LON, Interbus

h) The system allows the connection of phone and intercom systems via proprietary interfaces as well as standard protocols such as CSTA, TAPI and SIP

i) Customized control panels for various device linkages are available.

3. Subsystem interfacing requirements

The proposed sub-systems shall at minimum have the following capabilities in order to interface to the installed PSIM:

a) All systems and devices connected to the PSIM System shall communicate their status and alarms and be able to receive control instructions/sequences using IP networking.

b) Project data shall supply graphical and textual information with instructions and measures as well as scheduled commands. In addition, personalized operating rights shall be assigned to each data point. With help of the information provided in the graphics and texts the event handling shall then be completed through taking actions and entering comments interactively.

c) All sent or received telegrams shall be logged for each device/sub system interface.

d) In addition to the regular workstations (full clients), a web access for display of events and control of connected subsystems shall be possible cross-platform.

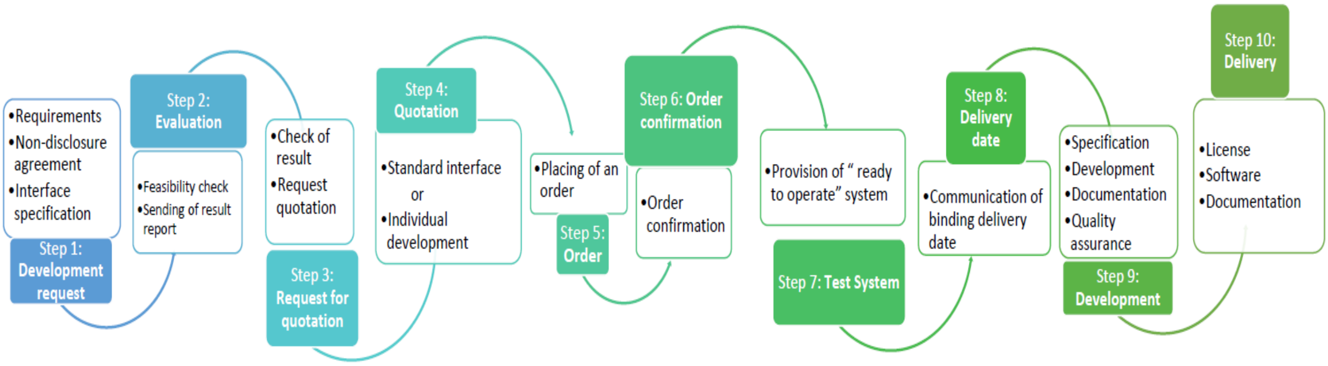
e) The web access shall be realized browser-independently based on HTML and JavaScript and without any manual installation (e.g. of plug-ins).

f) The system’s software needs to communicate bi-directionally.

***Important to note for adding of subsystems:** The PSIM System has been designed to enable a centrally controlled interaction between security, building and information management systems, however it shall not replace any installed single system. (The integration extent always depends on the capability of the SDK (Software Development Kit) supplied by the device manufacturer.*

4. Interface development process

a) The figure below shows the process that shall be followed by the Suppliers and PSIM OEM for provision/development of interface to link site level systems to the PSIM at Zero Control. Suppliers shall include the associated cost of all the works included in this process in their costing.



RACI

Responsible party	Steps
Contractor	1, 3, 5, 7,
PSIM OEM	2, 4, 6, 8, 9, 10

Figure 3: PSIM interface provision/development process

b) The table below shall be populated to provide details for the subsystems and associated devices to start the evaluation process depicted above.

Subsystem	Vendor	Model	Panel/Device Qty.
CCTV system			
Alarm system			
Intrusion pre-detection system			
Access Control system			
Public address system			
Site Integration system (where applicable)			
Other			

5. Supported interfaces

Below is a list of interfaces supported by the current PSIM at Zero Control. When the PSIM System integrates to third party systems, the Suppliers shall include the optional additional modules and licenses if it is found in the current interface list as well as the possibility for future extensions with further optional modules not on the list.

a) Generic Interfaces

Serial IN-SST
Serial OUT-SST
Generic OUT-IP
GenIO

b) Standardized Interfaces

BACnetClient	KNX
EIB	LON Bus (via Gateway)
ESPA 4.4.4	Modbus RTU
ESPA-X	Modbus IP
Interbus	OPC DA 2.0 Server / Client
IP Check	OPC UA

c) Network Management

APC ISX-Manager (via Modbus)	Generic SNMP Protocol
HP Open View Service Desk	SNMPv3

EMKA	barox switches (via SNMP)

d) Key Management

Deister – Key Management System
Gantner – Leisure Key Management
Kemas – Key Management Systems

e) Media Control

Russound CAV 6.6

f) Weather Data

Vaisala – WINDCAP

g) Radiation Detection

GIHMM – Gamma Detector (via ModbusIP)

h) General Alarm system

ABI – MC1500
Bosch – UGM 2005 / 2010 / 2020 / 2040
Esser (Honeywell) – BMZ 8000 via SEI
Esser (Honeywell) – BMZ IQ8 Control via SEI
Securiton – SecuriPro
Siemens – SM80
Siemens – SM88 (SM-PORT, FRK, FRK-B)

i) Fire Alarm Systems

Advanced Electronics – MX 4000 / MX 5000	Hekatron – BMZ 340
Autronica – BS 420	Hertek – PENTA Series
Bosch – UGM 2005 / 2010 / 2020 / 2040	IFAM – FAT
Bosch – FPA 5000	Kentec Electronics Limited – Taktis MCE
Cerberus Algorex – FC700A	Notifier (Honeywell) – AM 2000 / AM 4000 / AM 6000 / AM 8000
Cerberus Algorex – CS11 (DMS 7000)	Notifier (Honeywell) – ID 2000
CEAG (Cooper), DF6000	Notifier (Honeywell) – NF 3000 / 5000 / ID 3000

Consilium – Consilium Common Platform (CCP)	Minimax – FMZ 4100 / 5000 (via MX2 Protocol)
Cooper CF1100 / CF 3000 / DF 6000	Morley – Standard Morley Protocol
Detectomat – detect 3004 und 3016	NSC – Solution F1
Detectomat – DC3500	Panasonic – EBL 128/512 via EBLnet
Eltek Fire & Safety (Honeywell) – FireWin	Protec – 6400
ESMI (Schneider Electric) – FX 3NET	Sauter – AVEO flex
Esser (Honeywell) – Esser N 3007 / 3008	Schrack – Integral via B3-USI4-Modul
Esser (Honeywell) – Esser 8000 / 8007 / 8008	Schrack – Integral via B5-LAN-Modul
Esser (Honeywell) – Esser 8000 / IQ8 / Flex-ES	Schrack – MAXIMA
GE – FP2000	Siemens – Cerberus FS720 (FC722, FC724)
Global Security – JunoNET Panel	Telenot – Comfire 3000-4 Plus
Hekatron – Integral via BX-USI4	Telenot – Hifire 4100
Hekatron – Integral via BX-NETX	Total Walther (Tyco) – Zettler BMCI
Hekatron – Integral from B5-SCUA (via LAN on Board)	Total Walther (Tyco) – Zettler Fast 2000
Securiton – SecuriFire via B3-USI4-Modul	Total Walther (Tyco) – Zettler Expert
Securiton – SecuriFire via B5-LAN-Modul	Total Walther (Tyco) – Zettler Profile
Siemens – SigmaSys D-100 / SM80 / SM88	Total Walther (Tyco) – Zettler ZETFAS/LOUT (via FILNET)
Siemens – FS20 (FC2020, FC2040, FC2060) via BACnet	Total Walther (Tyco) – Zettler ZETAPLEX-FSK (via AED)
Siemens – FS20 (FC2020, FC2040, FC2060) via	Total Walther (Tyco) – Zettler ZX / MZX
UNIPOS – FS5200	Wagner – Titanus Rack Sens
Wagner – FPA5000	Wagner – Titanus Super Sens
Wagner – Titanus Micro Sens	Wagner – Titanus Top Sens
Wagner – Titanus Pro Sens	

j) Intrusion Detection Systems

ABI – MC1500 / MMP1	Esser (Honeywell) – EMA 5007 / all system types via SEI
Alphatronics – UNii	Europlex – 3GS
Aritech – CD Max	GE – ATS MasterPanel
Bosch – NZ 300	Honeywell – Galaxy Dimension (via Microtech)
Bosch – UEZ / BZ500	Satel – Integra 256 Plus
Bosch – MAP 5000	Napco Security Technologies – Napco Gemini
Bosch – UGM 2005 / 2010 / 2020	Novar (Honeywell) – EMZ 561 (MB16, MB100, MB256, MB256plus) via IGIS-LOOP
Effeff – EMZ 561 (–> Novar/Honeywell)	Novar (Honeywell) – EMZ 561 (MB16, MB100, MB256, MB256plus) via IGIS-LAN
Effeff – DEZ 9000	Novar (Honeywell) – EMZ 561 (MB16, MB100, MB256, MB256plus) via WinMAG (OPC)
Esser (Honeywell) – DEZ 9000	Novar (Honeywell) – MB24, MB48, MB100 via module 013211.10
Novar (Honeywell) – MB-Secure via ISOM API	Siemens – Security detection system SM88
Nox Systems – Nox	Siemens SPC
Paradox – Imperial	Sonax – Varus
Plettac – GSE 63	Sonax – Z 3000
RISCO Group – ProSYS/LightSYS	Telenot – complex 400H
Rokonet (RISCO) – ProSYS	Telenot – Hiplex8400h
Securiton – SecuriPro	Total Walther (Tyco) – ZETADRESS 300
Siemens – Guarto	Total Walther (Tyco) – ZETADRESS 1000/2000
Siemens – Sintony Si400 / Si420	Total Walther (Tyco) – ZETADRESS 5000
Siemens – Transliner Cerberus IK 500 / IC 1000	UTC FS – ATS1000A / ATSx500A
UTC FS – ATS MasterPanel	Vanderbilt – SPC (43xx,53xx,63xx) via FlexC

k) Receiving stations

Digifon – Receiving Station	Telenot – ÜZ7500, comXline
effeff (Honeywell) – DEZ 9000	Telesignal – Receiving Station
MS MIKROPROZESSOR-SYSTEME – MSD 4000	Tyco – Surgard
Telenot – T508, T608	Vanovost – Receiving Station

l) Access control systems

AHB Systeme GmbH – AHB	Genetec – GenetecSecurity
Touchless Biometric Solutions (TBS)	Xtralis – VSK / FOXnet
Autec – UBI (via UBI2 / UBI3 protocol)	Hirsch/Identiv – Velocity
Bosch – AMCAC	Honeywell – IQMultiAccess
Bosch – Miditec	Honeywell – Pro-Watch
Continental Access – CardAccess 3000	Inner Range – Integriti
CEM Systems – AC2000	Interautomation – CASA
Dorma – Matrix	Interflex – 6010
EAL – AtsLink	Interflex – 6020
effeff (Honeywell) – Multiaccess	Interflex – 6040
ENGIE Fabricom – I-CARDS	ISONAS
EVVA – ATS	Johnson Controls – Cardkey Pegasys / Pegasys 2000
Gantner – GAT ACE 3000 / 7000	KABA – EXOS 9300 / B-COMM / B-COMM Java
Gantner – Gantner AC	Keyprocessor – iProtect
Gantner – GTS6200	PCS – DEXICON
Gantner – LAS	Primion – AC
GE – FacilityCommander (FCWnx)	Roger – RACS 4
Keyscan – System 7 / Vantage	SDS
Lenel – OnGuard	SALTO
Miditec (OPC UA)	Siemens – SiPass / SiPort / SPC
Nedap – AEOS	Softcon – CR355
Pascom – Pascom	Software House (Tyco) – C·CURE 800 / 8000
Paxton – Net2	TDS – CoreAccess
Software House (Tyco) – C·CURE 9000	TripleEye – TiSM

Stanley – PAC	Xtralis – S2000
Syntegro – Synguard	

m) Escape routes

Dorma – TMS
effeff (Assa Abloy) – BCM 925
effeff (Assa Abloy) – 970 TSBC
GEZE – GEZE
Microconsult – Escape door control

n) Emergency Exits / Emergency Lighting

CEAG – ZB96
Inotec – INOTEC CPS
Kaufel – viaFlex Emergency Lighting Systems

o) Perimeter protection

CIAS ELETTRONICA – IB-SYSTEM IP	Sick – Laser sensor (via SOPAS OPC Server)
Elbit Systems – MIVNIT	Sicurit – HyperPower SMS (compatible with all Sicurit PIDS)
ELFAR – ELFAR Smart Fence Driver	Smart Microwaves
Feldhaus-Uhlenbrock – AL-5	Sorhea – G-FENCE, KAPIRIS III, MAXIRIS III, SOLARIS, APIRIS
Future Fibre Technologies – CAMS 3	Southwest Microwave – Intrepid MicroPoint I
Haverkamp – MicroGARD	Southwest Microwave – INTREPID II
Senstar	Sysco – Sona5 / Sona IP
SenSys – FiberSenSys	Titze – PIDS
WI-I PIDS	

p) Personal Security / Communication / Pager

Ascom Pager Systems	Pager connection via ESPA 4.4.4
Ascom PNA	Schmidt Funktechnik – Telestech 2000 PNA
Ascom SMS	TAPI Interface
Ascom Tek 900	Tetronik – DAKS (via ESPA-X)
Blick Pager Systems	vi2vi – viTrack

Bosch – D6801 – Pager	Voice Modem
Bosch – PS6000 (via UPC6000 / BID)	Voice Modem with Text-to-Speech Funktion (SAPI5)
Cinterion – TC35, MC52/55, CT63	Voxtron – AgenTel
ComPlan Emergency server	WAV-Out Modul
CSTA – TK-Standard	Funkwerk (Funktel) – Dect Secury System (DSS) – PNA
E-Mail, Fax	Funkwerk (Funktel) – RP201, D6801, OCP – Pager
Felsenmeer – gsm (s, s plus, s Ex, s Ex plus)	MOXA G2111 – GSM-Modem
Felsenmeer – D.A.N Shalosh	Optro – OPTRO-2000 SL-N

q) Intercom / Nurse Call

2N (via SIP)	Gehrke – 4000 SA
Behnke – S20 (incl. video)	Gehrke – NeuroKom IP
Combird – SyrinX	Metasec (incl. video)
Commend – GE 300, 700, 800 and VirtuoSIS	Schrack Seconet – VISOCALL IP
Efe – Cell communication system	Zenitel Stentofon – AlphaCom / AlphaDisp / MPC
Esser (Honeywell) – Ackermann IPC	Total Walther (Tyco) – Zettler Medicall 800/800IP

r) Video System

American Dynamics – AKS Matrix Switching Systems (MSS)	Bosch – VideoJet 10 / 100 / 8000 / 8008
American Dynamics (Tyco) – HybridDVR	Bosch – VideoJet X10 / X20 / X40
American Dynamics (Tyco) – Intellex DVR	Bosch – VIP 10 / 1000
American Dynamics (Tyco) – VideoEdge	Bosch – VIP-X
Artec Technologies – Multieye (Multieye SDK)	Bosch – Video Recording Manager (VRM)
Aventura – Video Management Systems	Bosch – VIDOS Lite Monitor Wall
AverMedia – AverDigi DVR	Bosch – VIDOS-NVR 4.00
Avigilon – Avigilon HD CCTV System	Bosch – Bosch Video Management System (BVMS)
Axis – Network Cameras (VAPIX Version 2)	Bosch (Philips) – LTC8x00 video matrix
Axxonsoft – Intellect	Cathexis – Cathexis DVR
Bosch – Network Cameras (via BoschVideoSDK Version 5 / 6)	Condev – Condev VKS

Bosch – Dinion IP	Convision – Convision Camera server
Bosch – DiBos 8.4	Dahua – Dahua Digital Video Systems
Bosch – Divar 2	Dallmeier – DallmeierAPI
Bosch – Divar XF	Dedicated Micros – Video remote transmission DVST
Bosch – FlexiDome IP	DEKOM – DiViCro
Dallmeier – PView	Digifort – Digifort IP Video Management System
Dallmeier – PView2	Digivod – Digivod VMS
Dallmeier – DIS 2	Ernitec – System 500M / 1000M
Dallmeier – Leo	EverFocus – EDR 410/810/920/1620/1640 DVR
Dallmeier – Panomera	FLIR – LatitudeVMS
Dallmeier – SMAVIA	Genetec – Security Center
Geovision – Geovision Active-X Version 6.0 & 7.100	Geutebrück – Video matrix (GST)
Geutebrück – G-Core	Geutebrück – Multiscope II
Geutebrück – GeViSoft	Geutebrück – Reporter
Geutebrück – GeViScope	Geutebrück – Video control system Mbeg
Griffid – Digital Video Surveillance System	Panasonic – NVR ND200 / ND300 / ND300A / ND400
HeiTel / Xtralis – HeiTel Server	Panasonic – DVR HD309 / HD316A / HD350 / HD616 / HD716
Hikvision – HikCentral Professional (HCP)	Panasonic – Network cameras and converter (PS-API)
Hikvision – Net Video Recorder DS-7716NI-I4/16P	Panasonic – InsightAPI
HiTRON Systems – HiTRON NVR	Pelco – Endura
Honeywell – MAX 1000 VKS	PKE – Avasys Video
IndigoVision – IndigoVisionSDK	Qognify (Seetec) – Cayuga (Version 6)
IndigoVision – NVR	Qognify (Seetec) – Seetec Version 5
Kodicom – CCTV Cameras	Schille – SiVMS
Linke – SYSn 96 KP VKS	Senstar – Symphony
March Networks – 6700, 8000 and Command	SightLogix – SightSensor HD / NS / TC
March Networks – 4000 C Series Hybrid NVRs	Siemens Siveillance™ Video
March Networks – ESM	Siemens – SiNVR

Milestone – XProtect 2020 R3 (Express/+, Professional/+, Expert and Corporate) via MIPSDK	Siemens – Simatrix
Mirasys – Video Management	Siemens – Sistore AX / MX / CX / SX
Mobotix – Hub	Siemens – Siemens VKS
Mobotix – Network Cameras	Simplex – Simplex Multiplexer VKS
Netavis – Observer II	Sony – NVR (Network Surveillance Server)
NICE – Alpha System digital video	Sony – RZ30N
Odetics – DVMD32	Sony – RZ30P
TEB – Digipryn	Vanderbilt – Eventys Range NVR DVR
Tyco – AKS Matrix Switching Systems (MSS)	Vanderbilt – NVR DS-7200 / 7600
Tyco – ExacqVision VMS (via ADSDK)	VDG – Diva / Sense
Tyco – ExacqVision VMS (via evAPI-SDK)	Vicon – VDR 704 / 708 / 716
Tyco – HybridDVR	Videv – Video crossbar Euroline
Tyco – Intellex DVR	Videv – Euromax 250 / 500 / 2000
Tyco – VideoEdge	Vigilant – NetView II
UTC – TruVision	VisiOprime – FX / FXL / PXL
VSCS – Video Security Control System	XTralis – HeiTel Server
XTralis – Foxnet	

s) Video Controller

Axis – Axis joysticks T8311 / T8312 / T8313	Panasonic – Video control unit
Dallmeier – Video Management Center	General USB joystick interface
Geutebrück MBeg	VideoTec DCZ Joystick
Mobotix – MobotixEventStream	

t) Video Analysis

Ipsotek – VISuite
MATE – Video detection
Visapix – Video detection

u) Video Wall Management

Barco CMS
Eyevis – eyecon

VuWall – VuWall

v) Public Address System

Bosch – Praesideo
Dynacord – Promatrix 4000 / 8000
G+M – G+M Acoustics system
Esser (Honeywell) – Variodyn D1
Siemens – Novigo
Siemens – Cerberus PACE
TOA – NX-100

w) Gas Detection

Winter – WinPro
Honeywell – Analytics Zellweger System 57

x) Building Management (BM)

Beckhoff – ADS / TwinCAT System
Bosch – AMCIO
Decision Industrial Interface Digital I/O
EIB/KNX (b+b OpenEIB switch)
Kieback & Peter GLT via OPC
Klöckner Möller – Lighting Control
LON Bus (via Gateway)
Modbus RTU
Total Walther (Tyco) – Zettler AED Concentrators
Modbus IP
Phoenix Contact Interbus Remotekopplung (TCP/IP and/or modem)
Siemens – Desigo Insight
Siemens – Desigo CC
Siemens Visonik
Siemens WinCC via OPC
Wago (LON, Ethernet, CAN, Profibus, etc.)
Wikon FEWIS Remote Digital/Analog I/O
Total Walther (Tyco) – Zettler L-Out Module via Fil-Net

y) Leak Detection

Frogsys – Liquid leak detection
Tyco – Trace Tek – Leak Detection Systems

z) Occupant Management

ADV-Vollzug
BASISWEB

GEW-Database
IVV

aa) Parking Management

Scheidt & Bachmann
SkiData – sweb Control

bb) Misc. Interfaces

Advancis – Virtual	CSV Import/Export
Airthings – Airthings	Dart – SNMPv3
ASCII interface	Disruptive Technologies – Disruptive IoT
Bild + Ton (Hifi Remote-Control)	DWG / DXF Import
Candid – SekurZone (License Plate Recognition)	ELREHA – VPR-19000
Cara – Cash Register System	Flight Information System
Fortecho Solutions – Fortecho	Johnson Controls – MetasysOPC
Freshworks – Freshdesk	KTG GmbH – SecuScan (Under Vehicle Monitoring System)
EuroImmun – EJDB Transponder System	Logprinter
HP Open View Service Desk	Microsoft – SystemInfo
Intergraph – I/CAD (Incident Management System)	MIGRA – Migra/Migan display
NIS LCD-display	Siemens – SICAM1703
OnSolve	TeleRadio Engineering – UVSS & VLPR (Under Vehicle Surveillance System & Licence Plate Recognition System)
Planon – Planon Web Services	TNO – Effects

Annex F: Technical returnables index

The index below is a guideline of how the technical returnables and supporting information should be indexed.

1. Valid PSIRA registration certificate.
2. Completed Technical Schedules A/B related to 240-86738968 as per Annex A of 240-170000257 including supporting information/evidence.
3. Completed Technical Schedules A/B related to technical specification 240-91190304 as per Annex B of 240-170000257 including supporting information/evidence.
4. Completed Technical Schedules A/B related to technical specification 240-102220945 as per Annex C of 240-170000257 including supporting information/evidence.
5. Completed Technical Schedules A/B related to technical specification 240-170000098 as per Annex D of 240-170000257 including supporting information/evidence.
6. Completed Technical Schedules A/B related to technical specification 240-170000691 as per Annex E of 240-170000257 including supporting information/evidence.
7. Completed Technical Schedules A/B related to technical specification 240-170000096 as per Annex F of 240-170000257 including supporting information/evidence.
8. Completed Technical Schedule A/B related to specification 240-17000723 as per Annex G of 240-170000257 including supporting information/evidence.
9. Detailed design report as per index in Annex B of this document (240- 170000258)