Sentech STP Radiokop Campus

DETAIL TECHNICAL SPECIFICATION FOR ALL ELECTRONIC EQUIPMENT

ANNEXURE 2

PART C3, Section 1

TENDER FOR, DESIGN, INSTALL AND MAINTENANCE FOR
ACCESS CONTROL AND CCTV SURVEILLANCE SYSTEM

TABLE OF CONTENTS

PART1 – SENTECH STP RADIOKOP CAMPUS

SCOPE

This tender document details the system requirements for the design, manufacture, supply, installation and commissioning of the systems as specified in this tender document for Sentech STP Campus at Radiokop.
An Intelligent Security Control system solution must be offered for the project.
The system must be designed in line with South African Government National Key Point act, with emphasis on implementation of International Standards.

This specification must be read in conjunction with the Bill of Quantity document attached and our marked up building drawings

The scope of the electronic security on the SENTECH Campus will be the following:

- Personnel Access Control
- Visitor Access Control
- Vehicle Access Control
- Fever Scanning for Covid-19
- Door Monitoring System
- CCTV surveillance System
- DSIM Platform

1 DESIGN METHODOLOGY

Pedestrian Flow

Pedestrian access to the Campus will be semi-restricted via the main entrance Gate turnstiles that will be installed in the new security entrance next to the traffic entrance booms

Pedestrian flow through the internal site will be controlled via bio-metric access controlled doors, booths and hip height turnstiles

All visitors shall report to the new gate security enrolment station where they will be scanned for fever and if normal their biometrics (Facial) will be enrolled onto the access control system. Permitting them restricted access to a specific area before being directed to the main reception area. While being escorted by an employee. Paraplegic visitors shall follow the same root but will gain access via the paraplegic gate next to the turnstiles

All staff's biometrics (Facial) shall be permanently enrolled onto the access controlled system. The specific enrolment shall be pre-programmed in order to allow access at:

- Vehicle access booms
- Different buildings on site(Green area)
- Red area Zone 1 and Zone 2
- Remote sites
- Turnstiles
- Booths

Vehicle Flow

Vehicle access to the Campus **will** only be allowed through the main vehicle entrance in Octave St Radiokop Honeydew

All vehicle entrances will be lockable at night.

A VIP/Visitors parking area will be provided to the right of the boom entrance at the main gate. The VIP/visitors parking area will be solely for VIP/visitors parking and access **will** be restricted via an access controlled boom. Visitor Boom will be controlled by the security guard at the gate by means of a RF control button.

Security Level Designation

The following levels of security have been established:

2 LEVEL1: BOUNDARY SECURITY

Definition

Boundary Security

- ClearVu fence is installed around boundary
- Limited External CCTV surveillance is provided and will be extended in future

3 LEVEL2:SITE SECURITY

Definition

The Site Security will include the following:

- Internal Green area buildings
- Internal Red area(KU Band Area and C Band)
- Vehicle entrance from Octave St
- Contractors entrance from Strutt St on the Western Side

Security Measures

- Access Control Enrolment of the personnel, visitors and contractors to site and buildings will be done at the new security gatehouse once built but will be done at the main building reception to start with.
- Fever screening will be done at all entry points into buildings.
- Vehicle traffic booms with biometric in/out
- CCTV Surveillance on entrance/exit lanes
- Entry and Exit LPR cameras
- Full height Biometric controlled Industrial turnstiles at entrance (next to booms in Octave St)
- Single and Dual Biometric controlled booths in Red Area
- X-ray equipment (hand bags and delivery)at main gate turnstiles
- All parcels carried by visitors **will** be subject to X-Ray Screening at the main reception
- Full height walk through metal detectors at main gate after the turnstiles

- Turnstiles with paraplegic gate will be installed at Main building reception.

4 LEVEL 3:KU BAND NKP (RED AREA)

Definition

The Internal Campus is classified as a National Key Point (NKP)site

Security Measures

- CCTV Surveillance - Cameras shall be strategically positioned throughout the site and buildings . All cameras will be in accordance with SANS 10222-5-1-4.
- Physical security by SENTECH at building entrance
- All doors will be monitored
- Fire access will be fitted by sound bombs
- Biometric access will be required to gain access to office areas as indicated on our drawings .
- Biometric access control controllers are to be fitted to the secure side of the building/door
- Fever screening will be done at all entry points into buildings.
- CCTV Surveillance at all entrances and exits - Cameras are fitted on the secure side of all access doors.
- Security booths will be installed where shown on our drawings
  - KU-Band building one Sigle booth unit on the north side and a Double booth unit at the south main area

Security Control Room

A new security control room will be established in the red area to monitor the Campus. The control room equipment room will accommodate the access control systems file server as well as other system, i.e. Video Wall, Monitors, PC's, Digital Recording etc.

The control room will be linked to an off-site control and response centre

Access to Plantrooms

Access to critical Plant rooms will be via access controlled doors. A biometric In/Out access system shall be implemented at each plant room door.

No provision was made for access control at:

- UPS rooms
- Generator rooms
- Sub-station rooms

Only door status will be monitored

PART 2 FUNCTIONAL REQUIREMENTS FOR ELECTRONIC SECURITY

5 GENERAL

5.1 This specification calls for the supply, installation and commissioning of a complete, integrated security system in accordance with appropriate local and international standards and the technical and performance criteria set out in this document.

5.2 This specification covers:

(a) Access Control

(b) Intruder Alarm System

(c) Alarms Management

(d) Photo ID Badging

(e) Visitor Management

(f) Guard Tour

(g) Perimeter security

(h) Fever screening systems at entrances.

5.3 The system is to be supplied with all equipment, hardware, software, cabling and ancillary services as required to provide an integrated system complete and functional in all respects. The tenderers are to familiarise themselves with all matters related to such requirements and to account for such in the tendered price.

5.4 Other security system components not included in this specification shall be fully integrated with this integrated security system.

5.5 It is the responsibility of the tenderer to obtain clarification of all matters in which doubt exists as to the exact intent of this document or in which a conflict appears to have arisen. Such information must be obtained prior to the closing and lodging of tenders.

5.6 The response shall clearly detail all pricing for components, cabling, installation, engineering, training, commissioning, setting to work, and 24 months comprehensive warranty.

5.7 The tenderer must include as part of the tender submission a complete, clause-by-clause response.

5.8 Access control with facial recognition has always been a challenge but now it is a simple and convenient way for access control.

5.9 It also creates an unparalleled security environment with enhanced efficiency and advanced technology.

5.10 With the Covid-19 issue that we are facing the facial recognition system allows for an Access Control with contactless verification that is more sanitary and convenient in a busy precinct environment like Sentech.

5.11 Fingerprint biometric readers is a huge risk for microbe transmissions by direct and indirect contact, has some issues with people that has poor minutia points for fingerprint templates and can't be used when people are wearing gloves.

5.12 Facial recognition removes all these concerns in one single go, and it is the future of access control.

5.13 Fever scanning was implemented to prevent the spread of Covid -19 and must form part of an integrated solution.

6 RESPONSE FORMAT

6.1 The tenderer shall respond to each clause with one of the following responses. Should the tender wish to clarify or amplify the response, then the clarification or amplification shall not change the given meaning of the response statement.

6.2

Response	**Meaning**
Complies	The equipment/system offered complies fully in all respects with the specification clause.
Substantially Complies	The equipment/system offered does not comply fully but offers most or a substantial part of the requirements of the particular clause. Compliance in excess of 75% of the requirement qualifies for this category. Areas of non-compliance must be clearly identified and explained.
Partially Complies	The equipment/system offered provides only a part of the requirements of the clause. Less than 75% compliance with the clause should invoke this response. Areas of non-compliance must be clearly identified and explained.
Does Not Comply	The equipment/system offered does not provide the requirements of the particular clause.
Accepted	The Tenderer understands and accepts the conditions imposed or enunciated by the particular clause, and has included provision for such in the tender.
Not Accepted	The Tenderer does not accept the condition imposed by the particular clause and as such is not included in the tender. Reasons for non-acceptance must be given.

6.3 The consultant and Sentech reserves the right to accept or reject any tender where clauses are tagged.

7 PRODUCT COMPETENCE

7.1 The successful tenderer will be required to demonstrate their competence to supply, install, commission, and maintain the product line proposed in the tender submission as follows:

7.1.1 Provide a letter of reference from the product manufacturer confirming the tenderer's status with the manufacturer, advising:

(a) Exclusive or non-exclusive agreement to provide the system in the geographical territory for this specific project.

(b) The tenderer will be fully supported by the manufacturer (accredited) in meeting the requirements of this specification.

7.2 The tenderer shall provide evidence of competency in carrying out the following areas of work:

(a) System design

(b) Installation management

(c) System configuration

(d) System commissioning

(e) System maintenance

7.3 When working on the system, each employee of the successful tenderer that will be working on Sentech's system will be certified (up to date accreditation) showing evidence of current manufacturer factory training, indicating the level of training.

8 FUNCTIONAL OVERVIEW

8.1 The Security Management System (The System) shall allow multi-site configuration able to be managed by one or more of the connected sites.

8.2 The same access control system must be able to be extended to all Sentech's remote towers.

8.3 It shall include (but not be limited to) the following:

(a) Access control

(b) Alarms management

(c) Cardholder management

(d) CCTV integration

(e) Integrated Visitor Management

(f) Guard Tour

(g) Perimeter deterrent and detection integration

(h) Fever screening systems at entrances.

8.4 The System shall control access through nominated doors having electric locking door status monitoring and biometric access control readers. Access rights associated with a presented access token or biometric identifier shall be checked for validity based on token or identifier, access area, access time and any other access management function defined in this specification, as stored in intelligent field controllers. Access shall be granted or denied dependant on fever scanning result and the access privilege. Access rights shall be programmed in a variety of ways to allow flexibility as defined elsewhere in this specification.

8.5 The System shall provide access control in elevators (on some of our remote sites) enabling access to any combination of floors over specified time periods. The interface to the elevator manufacturer's equipment shall be by either low level interface (relay outputs) or by a high level (data) interface.

8.6 The System shall monitor the condition of inputs. The System shall be able to be programmed to apply a variety of conditions to the way in which these inputs are monitored and shall enunciate the condition of such inputs in accordance with such programming.

8.7 The System shall provide a fully functional intruder alarm system including entry and exit delays where intruder detection sensors are connected to system inputs. The Intruder Alarm Systems component shall be fully integrated with the Access Control aspects of the system. It shall be possible to set (secure) or unset (unsecure) areas from any access control reader associated with an area, access control reader with keypad, Alarms Management Terminal, or as required from defined central control locations.

8.8 The System shall provide an integrated software facility for the design and production of photo ID cards.

8.9 The System shall be OPC AE (Alarms and Events) and OPC DA (Data Access) compliant, enabling integration of event, status and override data with external OPC compliant automation and business systems.

8.10 The System shall allow data exchange with other applications using XML protocols for schedule changes and card record changes.

8.11 The System shall support the BACnet communications protocol.

8.12 The System shall support a Web Service to allow an external system create remove and modify cardholders, including assigning access rights.

8.13 The System shall support a Web Service to allow an external system to create and modify visits and visitors.

8.14 The System shall support APIs to allow external systems to receive events from The System, and pass events to The System.

8.15 The System shall support the Simple Network Management Protocol (SNMP) protocol.

8.16 All system communications must be totally integrated with either existing or new LAN/WAN networks. Tenderers must make themselves familiar with the specific requirements for this project.

8.17 Connection to Intelligent Field Controllers (FCs) shall be achieved using cabling supporting the TCP/IP protocol. The network connection must be on-board the FC. Interface transceiver units (Ethernet to RS485, RS232 etc) are not acceptable.

8.18 The System and Intelligent Field Controllers shall have IPv6 address support.

8.19 Remote FCs not permanently connected to the network can be connected via a PSTN service, using TCP/IP protocols.

(a) Connection from the remote FC to the server shall be either via dialup to an Internet Service Provider (ISP) using encrypted TCP/IP, and then via an approved firewall through into the IT environment or via dialup directly to a RAS connection on the Server.

8.20 All system software upgrades shall be downloadable through the network to the FC, readers and I/O devices.

8.21 All data communication between The System and FCs shall be encrypted using an industry standard symmetric encryption algorithm equivalent to 256-bit AES or stronger.

8.22 All data communication The System and FCs shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall be equivalent to 1024-bit RSA or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours.

8.23 All data communication between FCs shall be encrypted using an industry standard symmetric encryption algorithm equivalent to 256-bit AES or stronger.

8.24 All data communication between FCs shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall be equivalent to 1024-bit RSA or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours.

8.25 All data communication between FCs and Edge Devices such as readers and I/O devices shall be encrypted using an industry standard symmetric encryption algorithm equivalent to 128-bit AES or stronger.

8.26 All data communication between FCs and Edge Devices such as readers and I/O devices shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall be equivalent to elliptic curve ECC P-256 or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours.

8.27 The System shall report all events to the operator(s) as configured and shall produce and maintain a log of all system events, alarms and operator actions.

8.28 The System shall provide a means for an operator to extract information relative to the event log and system configuration and produce this information in the form of printed reports, emailed reports directly from The System itself, screen displays or exported files.

8.29 The System shall provide for a Windows based User Interface with Site Plans and interactive icons representing the location and real-time status of Access Control, and Alarm Monitoring equipment.

8.30 The System shall provide emergency evacuation reporting.

8.31 The System shall be designed and manufactured by a reputable company who shall be certified under the ISO 9001:2008 (or later) quality procedures.

8.32 Where applicable, equipment shall have the following approvals:

(a) FCC Part 15

(b) CE approval BS EN 50130-4 Alarm Systems Electromagnetic Compatibility (Immunity)

(c) CE approval BS EN 55022 Emissions

(d) UL294 Access control

(e) UL1076 Burglar Alarms

(f) ULC-ORD-C1076

8.33 Encoders and readers shall also meet:

(a) CE ETS 300 683 Short Range Devices

(b) C-Tick AS/NZS 4251 Generic Emission Standard

(c) C-Tick RFS29

8.34 The System software shall be written in a fully structured, fully validated and commercially available language that provides a strictly controlled development environment.

8.35 The user interface for operational management of site security shall be developed using Microsoft .NET and Windows Presentation Foundation (WPF) development tools.

8.36 Comprehensive backup and archiving facilities shall be incorporated as an integral part of the system software.

8.37 The System shall include divisioning suitable for multi-tenanted buildings. Operators shall only be able to access those parts of the system which fall within their division and operator privileges.

8.38 FCs must support peer to peer communications for input and output communications between-FCs. Systems that require the main server for communications between panels are unacceptable.

9 SYSTEM SERVERS AND WORKSTATION HARDWARE

9.1 The server and workstation equipment shall support the Microsoft Windows environment as described in this section.

9.2 The server shall be of the Microsoft operating system. Operating systems such as Linux, Unix, and OS X shall not be acceptable.

9.3 The operating system used by the system server shall be Microsoft Windows 2012 Server (64 bit), Microsoft Windows 7 Professional/Ultimate/Enterprise or Windows 8.1 Pro

9.4 The tenderer should list any other supported Microsoft Server versions.

9.5 The operating system used by workstations shall be Microsoft Windows 7 Professional/Ultimate/Enterprise or 8.1 Pro (64 bit).

9.6 The tenderer should list any other supported Microsoft operating system versions.

9.7 The database engine shall be:

(a) Microsoft SQL Server 2012 (64 bit) or

(b) Microsoft SQL Server 2012 Express (64 bit).

9.7.2 The tenderer should list any other supported Microsoft SQL Server versions.

9.8 Workstations shall support multi-monitor operation, allowing an operator to set up one or more monitors for each workstation.

9.9 Workstation display resolution shall be a minimum of 720P. 1080P shall also be supported. Dragging the view onto a higher resolution monitor shall cause the view to resize, taking advantage of the higher resolution.

9.10 Manual Deployment using installation media shall also be supported.

9.11 It shall be possible for an operator to run a workstation solely from files stored on and run from a USB memory device and without requiring any pre-installation of vendor software on the PC.

10 LICENSING

10.1 If system licensing is required, the license to use the system shall allow usage in perpetuity.

10.2 Details of the license model shall be provided in the tender response.

10.3 Licensing shall permit all operational requirements for a specific system. This shall include but not limited to:

10.3.1 The live (operational) system.

10.3.2 Temporary test installations used for investigating configuration options or new software releases.

10.3.3 Secondary installations required for standby operation.

10.4 Updating of license content to make changes to existing licensed items shall not require a server restart.

10.5 It is acceptable to require a restart to allow incorporating additional items to the license.

10.6 The license content shall be detailed in a user window.

11 SYSTEM REQUIREMENTS

11.1 The system shall be in commercial operation with the same or similar configuration as detailed in this specification and shall be available for inspection. A reference list of such similarly configured systems and details of contact persons shall be submitted with the tender response.

11.2 The system described in this specification must have the following capacity as a minimum:

(a)	Configured Workstations	Unlimited
(b)	Graphical Site Plans	Unlimited
(c)	Access Readers	Unlimited
(d)	Elevators	10 elevators each with up to 75 levels
(e)	Fully Supervised 4 state Alarm Inputs	Unlimited
(f)	Output relays	Unlimited
(g)	Access Control Zones	Unlimited
(h)	Schedules per day	100
(i)	Schedule categories	50
(j)	Holiday days	30
(k)	Operators	Unlimited
(l)	Concurrent Operator Sessions	Unlimited
(m)	Cardholders	Unlimited
(n)	Cardholder Issue Levels	15
(o)	Cardholder Personal Data Fields	64

11.3 The system architecture shall be a tiered system consisting of:

(a) One or more installations of the head-end software application operating on computer servers and operator workstations.

(b) Intelligent Field Controllers (FCs) managing the system in a distributed intelligence format.

(c) Semi-intelligent sub-units (outputs, inputs, readers, etc) which rely on FCs to function.

12 CENTRAL CONTROL AND SYSTEM MANAGEMENT SOFTWARE

12.1 The Central Management System (CMS) shall use the Microsoft Windows operating system as defined previously. The version of Microsoft Windows shall be a currently supported version.

12.2 The system database shall be a version of Microsoft SQL Server appropriate for the system size required. The version of Microsoft SQL Server shall be a currently supported version as defined previously.

12.3 The system shall be OPC enabled in accordance with the current OPC specification for OPC AE (Alarms and Events) and OPC DA (Data Access).

12.4 The central server shall employ a high quality personal or server computer incorporating current generation design and components. It shall be of a Microsoft approved model for operation with current versions of Microsoft Windows operating systems. The PC specifications, including processor speed, internal memory and hard disk size shall be specified by the supplier and must be sufficient to meet or exceed the specified system requirements.

12.5 The system shall be capable of supporting a minimum of 20 PC based operator workstations simultaneously running. Operator workstations running terminal emulation software will not be accepted.

12.6 The system shall automatically log and time/date-stamp all events within the system including intruder alarm set/unset events, access control events, operator actions and activity.

12.7 The central control software shall be easy to use, make extensive use of menus and windows and require a minimum of operator training to operate the system proficiently. Systems requiring a script/program language approach to configure the system will not be accepted.

12.8 The central control must be capable of receiving simultaneous alarm signals from a number of remote locations without loss or excessive delay in their presentation to the operator. Any authorised operator should be allowed to acknowledge, view and/or process an alarm from any screen.

12.9 The central control shall be fitted with a real time clock, the accuracy of which shall be preserved over the period of main power supply failure. Synchronisation between the central control and Ethernet connected FCs shall be automatic and not require operator intervention.

12.10 Operator selection of processing tasks shall be via menu selections. Authorised Operators shall be able to process alarms, produce reports and modify database records without degrading system performance.

12.11 The following is the minimum operational and monitoring facilities required. The ability to:

(a) Program either a group or individual card readers with access control parameters, without affecting other card readers.

(b) Program the access criteria for individual Cardholders or groups of Cardholders.

(c) Store at least 64 non-access control data fields for each cardholder. The names of these ‘Personal Data’ fields shall be user-definable.

(d) Authorise or de-authorise a Cardholder in the system with the result reflected immediately throughout all readers in the system.

(e) Enable a ‘Card Trace’ against selected Cardholders so that an alarm is raised each and every time that cardholder presents their access card or token.

(f) Pre-program holidays so that different access criteria apply compared to normal working days. The system must have a capacity to set at least 400 holiday days.

(g) Recognise and manage regional holiday requirements

(h) Define as many access zones as there are card readers fitted.

(i) Allow or disallow individual Cardholder access to any one, or group of card readers, in real time.

(j) Log all system and operator activity to hard disk as they occur.

(k) Program alarm response instructions into the system so that these are presented to the Operator when processing an alarm event.

(l) Enable an Operator to enter messages against alarm events. This shall be configurable to be compulsory based on the operator who is logged on.

(m) Configure user-definable hot keys to allow the operator to enter commonly used comments when entering messages related to alarms. For example, F1 = False Alarm, F2 = User Error, etc.

(n) Temporarily override a Cardholder’s, or group of Cardholder’s pre-programmed access criteria.

12.12 The central control shall display a one-line plain language event message for every activity event (alarm or otherwise) occurring in the system. All activity logged shall be time and date stamped to the nearest second (hh:mm:ss). On having the appropriate operator authorisation it shall be possible to drill down into the properties of each component that makes up that event for future details. The event message shall advise:

i. Time of event created at the Intelligent Field Controller.

ii. Time of the event received at the central control system.

iii. Action.

iv. Successful or unsuccessful.

v. If the transaction is unsuccessful, the reasons for the denial.

(a) This includes but is not restricted to the following items:

i. All card or facial attempts.

ii. All door alarms.

iii. All operator activity including log on, log off, alarm response messages and any alteration of system data files.

iv. All alarm monitoring activations.

v. All communications link failures.

12.13 Time schedules for different ‘day types’ shall be configurable.

12.14 Regional holidays shall be configurable to allow for regional variations.

12.15 The system shall provide a detailed operator help file. This help file shall provide operators with text, audio and video help instructions and tutorials.

12.16 The system shall allow for searching of items configured within the system based on the following:

(a) Item characteristics.

(b) Related items.

(c) Times related to events including the item.

12.17 The system shall integrate with Microsoft Active Directory enabling cardholder and user records to be fully synchronised on a real-time, bi-directional basis.

12.17.1 Integrations that use third party applications to synchronise between Microsoft Active Directory and the system shall not be acceptable.

13 MULTIPLE SERVER CONNECTIVITY

13.1 Systems based on multiple servers installed at several locations shall be supported.

13.2 Each server shall be capable of communicating directly with its local Intelligent Field Controllers (FCs).

13.3 Should a network failure occur between servers, they shall continue to communicate with their local FCs.

13.4 Should a network failure occur between servers, operators shall be able to continue to manage the local system connected to their respective servers. This includes (but is not limited to) the following functions:

13.4.1 Manage alarms

13.4.2 Override and manage doors

13.4.3 Arm and disarm alarms

13.4.4 Edit cardholders

13.4.5 Run reports

13.5 Alarms and events from all servers shall be able to be displayed on any or all of the system workstations.

13.6 The cardholder database shall be automatically replicated to all servers as a ‘global’ entity.

13.7 Replication of cardholder changes shall occur as changes are made and not batch processed.

13.8 Communication between servers shall be peer to peer.

13.9 The multiple server environment shall allow for evacuation reports for each site on the multiple server system to be generated on one server, for one or more remote servers.

13.10 Operator views and access privileges shall follow the same rules across multiple servers as apply within a single server.

13.11 Security system items configured on existing servers shall automatically be recognised by any servers added to the multiple server group. Likewise, system items configured on the server(s) being added shall be automatically recognised by the existing multiple server group.

13.12 Use of software interface custom written modules or scripts to connect servers into a multiple server configuration shall not be permitted.

13.13 Manual or script re-entry of data for existing servers into any new servers being added to the multiple server group shall not be permitted.

13.14 Synchronisation of data across all servers shall be an automatic real-time function not requiring operator intervention or initialising.

13.15 Should communication be lost between two or more servers, the individual servers shall continue to function independently and shall resynchronise all changes made whilst off line automatically.

13.16 Should a conflict occur resulting from two items being created in two or more servers whilst servers are off line then an alarm shall be raised when the servers are re-joined advising of the conflict.

13.17 Should an existing record be modified in two or more servers whilst the servers are off line then on reconnection, the modifications shall be carried out in time order of the modifications.

14 GRAPHICAL USER INTERFACE

14.1 Configuration Graphical User Interface

14.1.1 The system access shall be via a Graphical User Interface (GUI)

14.1.2 All functionality shall be managed via the GUI

14.1.3 Drop-down menus or intuitive buttons shall be provided to select all configuration functions.

14.1.4 System items (hardware items and software items) shall all have an associated properties menu to allow item configuration.

14.1.5 Configuration or operation using scripting or other forms of text-based programming will not be accepted.

14.2 Operator User Interface

14.2.1 In addition to the User Interface defined above, the Operator User Interface shall be provided as follows:

(a) Full screen, user configurable viewers, designed specifically for the task and the information needs of the operator.

(b) Default viewers shall be provided covering the primary site management functions of:

i. Events

ii. Alarm management

iii. Cardholder management

iv. Access management

v. Site monitoring

vi. Calendars and day schedules

vii. Macros

viii. Operator Management

ix. Site wide system changes

x. Reports

(c) The system shall allow customised viewers to enable operators to access information relevant to their task.

(d) The Operator User Interface shall be fully configurable by an operator with authorisation to configure viewers.

14.2.2 Each viewer shall consist of a navigation area and a panel area as detailed below.

(a) The navigation area shall provide a list of system information associated with the specific viewer.

i. It shall be possible to select and order the columns of data associated with alarm and cardholder viewers.

ii. Incremental searching shall be provided based on preselected data columns for cardholder viewers.

iii. Selection of a line item in the navigation area shall cause the associated tile data to be populated.

iv. Alarm viewer headers shall display the number of unprocessed alarms for each alarm.

(b) One or more data tiles shall be provided to display detailed data associated with the navigation area item selected.

i. Tiles shall be able to be created based on a range of default tiles provided for this purpose.

ii. Each tile shall be configurable with the required data fields as determined by the function of the tile

iii. Tiles shall be maximised by single click operation.

iv. When a tile has been maximised, other tiles shall remain visible in thumbnail format, allowing single click to restore them.

v. Where applicable, minimised tile icons shall display dynamic content.

14.2.3 There shall be provision for displaying URL pages in a window.

(a) The URL window shall allow either a URL address or PDF or TXT file to be selected.

(b) Navigation from the selected URL shall be configured either as:

i. Navigation enabled

ii. Restricted navigation (allowing navigation to links on the site but not away from the configured URL

iii. Navigation disabled.

(c) Auto refresh of the URL shall be configurable down to 1 minute resolution.

14.2.4 The event viewer shall have the following capabilities:

(a) Allow the operator to view events in real time.

(b) The displayed data columns shall be configurable.

(c) The columns shall be sortable.

(d) Auto scroll capability.

(e) Allow the operator to view historic events, even when they have been processed from the main viewer window.

i. Filter based on time/date.

ii. Filter based on the source of the event, i.e. door, input, output etc.

iii. The filtered events shall appear in the event window in the same manner as real time events.

iv. Display a count of the number of events which were found.

(f) Display information relevant to the event that has been selected. This is applicable to the real time event viewer and the historic event viewer:

i. Instructions for the operator.

ii. Details of the event.

iii. Site plan.

iv. Cardholder image (where appropriate to the event).

v. Video camera feed (where appropriate to the event).

vi. Recent event history for the door (where appropriate to the event).

vii. Recent event history for the cardholder (where appropriate to the event).

15 SITE PLANS AND GRAPHICS

15.1 It shall be possible to manage and monitor alarms, overrides, the general status of site items and open doors through the Graphical User Interface with the use of interactive real time dynamic site plans and icons.

15.2 Site plan usage shall support touch-screen technology.

15.3 All site plans stored on the server PC shall be automatically updated if amended at any of the networked workstations.

15.4 External drawings shall be imported into the system from external drawing software.

15.4.1 The ability to import following drawing formats, as a minimum, shall be supported:

(a) BMP

(b) WMF

(c) EMF

(d) JPEG

(e) GIF

(f) DXF (version 3 or above)

(g) AutoCAD

15.5 It shall be possible to assign icons to system functions and place these at any position on a site plan.

15.6 Provision for drawing lines and areas to form ‘objects’ shall be available. These objects shall be able to be associated with system items allowing system item status to be visually indicated by the object.

15.7 It shall be possible to place free text onto a site plan.

15.8 Site plans shall be ‘nested’ allowing a single action (mouse click on a current site plan icon) to move from one site plan to another.

15.9 The following functions should, as a minimum, be able to be executed by clicking on Site Plan icons:

(a) View the current status of a Door, Input or Output.

(b) Override a Door, Input or Output.

(c) Monitor and acknowledge an Alarm.

(d) Open an access controlled door.

(e) Move from one site plan to another.

(f) Activate an Intercom.

(g) Override an alarm, access or perimeter fence zone state.

(h) Generate a report.

15.10 Icon names shall use the item name by default but a shortened name shall be selectable so as not to clutter the site plan with text.

15.11 The size of the Icons shall be scalable.

15.12 A pre-designed set of icons covering basic access control functions shall be provided.

15.13 It shall be possible to design and load icons from external software for use in the system.

15.14 It shall be possible to design macro buttons to reside on site plans. On activation, macro buttons must be capable of performing multiple overrides for any site items simultaneously.

15.15 It shall be possible to click and drag over an area within a site plan or individually select items on a site plan in order to override their state in one action.

15.16 It shall be possible to search for, select and navigate through available site plans within a single window (tile) and to view, move backward or forward through the list of recently visited site plans.

15.17 It shall be possible to display the number of cardholders within zones in real-time. This should be in the form of a numerical display on the site plan.

15.18 By default, the numerical display shall be green when the zone is empty and red when it is occupied.

15.19 It shall be possible to alter the size, font and colour of the numerical display.

15.20 It shall be possible to display the names of the cardholders within the zones along with the entry time and a user definable field such as contact number, department, card expiry details etc.

15.21 It shall be possible to change the location of a cardholder via the software so as to reduce or increase the cardholder count within a zone without the need to physically present the card to a reader.

15.22 The system shall allow access zones to be monitored ‘on the fly’ whereby the operator can drag and drop an access zone icon from a list or the site plan onto the cardholder monitoring area to view the number of cardholders within that area.

15.23 The system shall capable of maintaining a text file in real-time which contains details of the cardholders within the zones. This may be used by third party software to monitor cardholder location for tracking or evacuation purposes.

15.24 The operator shall be able to generate a report by selecting an item on the site plan.

15.25 The report shall be in context to the icon that was selected.

15.26 The report shall be exportable from within the report builder to the following formats:

(a) Adobe PDF files (.PDF)

(b) Microsoft word file (.DOCX)

(c) Microsoft XPS file (.XPS)

(d) Microsoft Excel file (.XLSX)

(e) Pages saved as image files (.JPEG)

(f) CSV file with headers (.CSV)

(g) CSV file without headers (.CSV)

15.27 It shall be possible to email the report directly from within the report builder.

15.28 It shall be possible to view video cameras from multiple vendors within the same graphical user interface.

15.29 Where supported by the integrated video system, it shall be possible to operate camera controls such as:

(a) PTZ

(b) Pause

(c) Forward

(d) Rewind

15.30 It shall be possible to maximise a camera window.

15.31 Whilst a camera window is maximised, the other camera windows should be changed to live thumbnail images so as to ensure the operator is able to see activity in all cameras.

15.32 It shall be possible to drag a camera icon from a site plan into a video viewer so as to dynamically be able to view cameras in an ad hoc manner.

15.33 It shall be possible to drag a camera icon from a list into a video viewer so as to dynamically be able to view cameras in an ad hoc manner.

15.34 It shall be possible to find a camera from a search box.

15.35 The Graphics application shall allow the Operator to add, delete or modify graphic floor plans and add indicator ICONs to graphic floor plans that represent Controllers, input/output points, readers, or cameras located in the Campus. Formats for Graphics supported shall include: jpg; bmp; dxf; wmf; emf.

15.36 There shall be two Modes, Live and Design. The Live mode shall be used for real time monitoring. In addition, right clicking an ICON presents the Operator with a list of available Access or Control Functions that can be issued to the device. The Design mode allows the Operator to Define which Graphics are to be used, place ICONs on the Graphics, and define properties for each ICON.

15.37 There shall be a Pan and Zoom Viewer that provides a key plan that can be panned and scrolled by moving the red box, which indicates the current viewing area.

15.38 There shall be a Directory of available Graphics to easily select the desired Graphic to display.

15.39 The Graphics application shall display the real-time state and condition of Alarm Points and Doors. The Door ICONs shall change from a closed door ICON to an Open door ICON, representing that the door is open.

15.40 When the door is closed, a closed ICON will appear again.

15.41 The Alarm ICONs shall change from a closed contact ICON to an Open contact ICON, representing that the alarm device is active.

15.42 When the Alarm Device is restored to its normal condition, a closed contact ICON will appear again. The ICON will also display the Device Name and Alarm Condition that caused it to go into an Alarm condition.

15.43 The Colour of the ICON will also change based on whether it is in alarm or secure

16 FIELD HARDWARE

16.1 The Field Controller (FC) shall be the main controller in the field. The Security Management System (The System) shall communicate directly with all FCs.

16.2 Each FC shall be intelligent such that in the event of failure of power or communications to The System, for whatever reason, the system shall continue to allow or deny access based on full security criteria.

16.3 The FC shall store on-board all the security and access parameters to operate completely independently from the central control server. Systems that rely on the central control server for access decisions will not be considered.

16.4 The FC shall buffer activity data and immediately transmit it to the central control server upon reestablishment of communications.

16.5 Should communications fail with The System, each FC shall be capable of buffering up to 80,000 events.

16.6 All events shall be time-stamped at the FC at the time of occurrence.

16.7 Systems that only time stamp the event upon receipt at the central control PC shall not be acceptable.

16.8 The FC shall be capable of storing up to 500,000 card records with associated access criteria.

16.9 The system shall monitor input circuits and enunciate whether the circuit is Normal, Alarm, Open Circuit Tampered or Short Circuit Tampered as separate conditions.

16.10 A configurable range of end of line resistor values shall be supported as a software function to support pre-existing input circuits when required.

16.11 The use of any circuits using other than dual 4k7 end-of-line resistors must be approved by the consultant.

16.12 The FC shall include tamper protection for the front and the back of the panel. The front panel shall be tamper protected for door open, and the rear of the panel to detect if the panel has been removed from the wall. These shall use optical tamper detection. Mechanical tamper devices are not acceptable.

16.13 The FC shall incorporate an ARM 9 processor with at least 256 Megabytes of non-volatile FLASH EEPROM. The FC shall incorporate boot code in a protected sector of the flash memory. For software upgrades, all system software shall be downloaded from the central server over the network

16.14 The FC shall support direct download via USB to allow local upgrade of the FC.

16.14.1 The upgrade process shall only accept authenticated downloads via the USB port.

16.15 The FC shall operate from a separate battery backed 13.6V DC supply.

16.16 The FC shall continue to operate for at least 24 hours in the event of a mains supply failure.

16.17 The system shall be capable of automatically detecting and reporting a power failure, low battery and battery not connected.

16.18 FCs shall automatically restart and resume processing following a power failure.

16.19 FCs shall be fitted with ‘watchdog’ hardware and software to provide automatic detection and restart should the processor lock up.

16.20 The FC shall contain its own real time clock. The clock shall be synchronised with the central control server clock at least once per hour. The accuracy shall be such that the time difference between FCs shall not vary more than 0.5 second at any time.

16.21 The FC shall be allocated to a time zone appropriate to the FC location to cater for regionally and globally located FCs.

16.22 The FC shall have an on board Ethernet (TCP/IP) connection and driver supporting 10BaseT and 100BaseT operation. Third party plug-in RS485/Ethernet modules will not be accepted.

16.23 When specified, the FC shall support 100/1000BaseT.

16.24 The FC shall be fitted with 2 Ethernet ports providing an alternate communication capability.

16.25 The System and Intelligent Field Controllers shall have IPv6 address support.

16.26 The FC shall be provided with a pre-configured IP address to allow off-line initial configuration via a web browser application when required.

16.27 The FC shall support DNS (Domain Name Server) operation.

16.28 Should the primary DNS not be available, the FC shall be able to automatically establish contact with a secondary or tertiary DNS.

16.29 Should excessive network broadcast traffic occur (resulting from a denial of service attack or similar), an alarm shall be generated.

16.30 All data communication between The System and FCs shall be encrypted using an industry standard symmetric encryption algorithm equivalent to 256-bit AES or stronger.

16.31 Communication between The System and FCs shall be on-line and monitored for interruption.

16.32 The FC shall include one RS 232 multi-communications port.

16.33 The FC shall include one USB 2.0 port.

16.34 The FC shall support remote site dial-up.

16.35 Remote communication between the FCs and the remote devices shall use the switched telephone network circuits.

16.35.1 Incoming connection shall be via an ISP service.

16.35.2 Outgoing connections via modems connected to the customer LAN are not permitted, however dial-out directly from The System is allowed provided the modem is fixed to ‘non-answer’ mode.

16.36 The FC shall support a cellular module for alarm transmission to multiple alarm monitoring stations via a cellular network.

16.37 It shall be possible to view the FC status and configuration for commissioning and diagnostic purposes without the use of the central server software or other proprietary software. This may be achieved by the use of a conventional web browser. In high security applications, it must be possible to disable this feature at the FC.

16.38 The FC shall support logic functionality by way of configurable 'Logic Blocks'.

16.38.1 The FC logic functionality shall be able to be run independent of The System being online.

16.38.2 The following items shall be useable as inputs to Logic Blocks:

(a) Physical Input states

(b) Output states (both physical and logical)

(c) Door states

(d) Other Logic Block states

16.38.3 Up to 10 Logic Block input items shall be configurable in AND/OR combinations to cause an output to operate.

16.38.4 Up to 10 AND/OR rules shall be configurable for each item.

16.38.5 The Logic Block output shall be able to be configured as an internal (virtual) output, i.e. a state that can be on or off but does not require a physical relay.

16.38.6 The Logic Block output shall be able to be assigned to an external output.

16.38.7 The Logic Block output shall be able to be assigned as an input on one or more other Logic Blocks.

16.38.8 The Logic Block output timing shall be configurable to at least the following:

(a) Delay on

(b) Delay off

(c) Latched

(d) Pulse time

(e) Maximum on time

(f) Passthru

16.38.9 The FC Logic Block output shall be able to trigger actions across multiple FCs, independent of The System being online

16.39 A separate alarm message shall be transmitted to The System for at least the following alarm conditions. The alarm message shall be displayed in plain language text.

(a) Tamper

(b) Tamper Return to Normal

(c) Unit Stopped Responding

(d) Card error

(e) Maintenance Warning

(f) Alarm Sector State Change

(g) User Set

(h) User Unset

(i) Card Trace

(j) Wrong PIN

(k) Access Denied

(l) Duress

(m) Zone Count Maximum

(n) Zone Count Minimum

(o) Door Open Too Long

(p) Forced Door

(q) Door Not locked

(r) Power Failure

(s) System Reboot

(t) Intercom

16.40 The FCs shall communicate with and control the following equipment:

(a) Fever Reading equipment

(b) Facial Biometric access readers

(c) Card access readers with PIN keypads

(d) Elevator access equipment

(e) Alarm monitoring Input/Output panels and equipment

(f) Alarm response equipment

16.41 Any failure of a biometric reader unit and its communications with the FC shall be raised immediately as a high priority alarm and shall not cause the FC or other associated hardware to stop working correctly.

16.42 The FC shall communicate with remote devices (biometric readers, alarm equipment, elevator readers) using a fully encrypted data communications protocol. Unencrypted ASCII text or similar data transmissions are not acceptable.

16.43 All communications between the FCs and the remote devices must be check-digit coded to protect data from manipulation during transmission.

16.44 All communications links between the FCs and the remote devices shall be monitored such that an alarm is raised at the central control if the data being transmitted is corrupted or tampered with in any way.

16.45 All data communication between FCs shall be encrypted using an industry standard symmetric encryption algorithm equivalent to 256-bit AES or stronger.

16.46 All data communication between FCs shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall be equivalent to 1024-bit RSA or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours.

16.47 Communication between FCs and downstream devices shall support a high speed protocol of at least 1Mbit/second.

16.48 The FC shall support up to 10 high speed communication ports.

16.49 The FC shall support up to 80 devices comprising of a combination of readers, I/O devices and sensors.

16.50 The FC shall not necessarily support 80 devices of one type.

16.51 Devices connected to the high communication speed port shall contain a unique serial number.

16.52 When connected to an FC, the serial number of the device shall be reported to The System.

16.53 Once assigned to a function within an FC, if any attempt is made to substitute readers in the field without authorisation, an alarm shall be generated.

16.54 The FC shall support the Wiegand connections protocol, supporting up to 65,535 Bits.

16.54.1 Wiegand formats shall be configurable, allowing for:

(a) Number of Bits

(b) Facility/site code Bits

(c) Card number Bits

(d) Parity bit configuration

16.55 The FC shall have Open Supervised Device Protocol (OSDP) reader support.

16.56 The system shall provide relay output facilities that are system activated in response to alarm activations. Relay functions required are:

(a) Activate and latch a relay in response to an alarm. Relay to remain latched until alarm processed.

(b) Activate a relay for pre-set ‘pulse’ time. The relay to release after the ‘pulse’ time lapses.

(c) Relay activation to ‘mirror’ or ‘follow’ the alarm input activation.

16.57 The system shall incorporate relay outputs that can be activated according to time schedules, rather than alarm event. These outputs may be used to control lighting, heating, or to electronically lock or unlock non-monitored doors.

17 ACCESS CONTROL

17.1 The system shall provide complete flexibility and be capable of programming an unlimited combination of access control, security alarm and I/O parameters subject only to performance and memory limitations within the intelligent Field Controller (FC).

17.2 For ease of programming cardholders shall be grouped into access groups sharing the same access criteria.

17.3 Individual cardholders may be assigned with an extended door unlock time, as may be required by cardholders with a disability.

17.4 It shall be possible to assign an individual cardholder to an access group on a temporary basis with predetermined start and finish times.

17.4.1 During the period of temporary access, the cardholder shall have the rights of the group to which they have been assigned in addition to any permanent access rights they may have been assigned.

17.4.2 The access group details page shall display both permanent and temporary access members with the status of temporary members shown as:

(a) Pending (with the start and finish times)

(b) Active

(c) Expired

17.5 Any cardholder or access group in the system shall be able to be programmed to have access to any combination of controlled doors in the system with each period of access for each door controlled to within the nearest minute.

17.6 The FC shall check entry based on ALL of the following criteria:

(a) Fever reading below 37 degrees

(b) Correct site code

(c) Authorised card in database

(d) Correct issue number

(e) Authorised door / access zone

(f) Authorised time of day

(g) Valid card holder competencies (refer to the ‘Identity Analytics - Competencies’ section)

(h) Correct PIN (If PIN entry is required)

(i) Double entry (anti-passback, anti-tailgating or escort modes).

17.7 Anti-passback mode shall be able to be configured in any of the following modes:

(a) Disallow second access to an area if a valid exit has not previously been registered and generate an alarm (hard anti-passback).

(b) Allow second access to an area if a valid exit has not previously been registered but generate an alarm (soft anti-passback).

(c) Exclude specific Access Groups from the rules defined in (a) and (b) above.

(d) Anti-passback rules shall be able to be reset by either:

i. Automatically after a preset period after valid entry.

ii. Automatically at a standard time each day

iii. Automatically on exit from site

iv. Manually as an override.

(e) Must support Global Anti-passback allowing multiple access zones to be linked for the purpose of anti-passback, across multiple FCs utilising encrypted peer-to-peer communications.

(f) The FCs shall not rely on the server for anti-passback operation. Global anti-passback shall work across multiple FCs, even if the server is off line.

17.8 Anti-tailgate mode shall be able to be configured in any of the following modes:

(a) Disallow exit from an area if a valid access has not previously been registered and generate an alarm (hard anti-tailgate).

(b) Allow exit from an area if a valid access has not previously been registered but generate an alarm (soft anti-tailgate).

(c) Exclude specific Access Groups from the anti-tailgate rules.

(d) Anti-tailgate rules shall be able to be reset by either:

i. Automatically after a preset period after valid entry.

ii. Automatically at a standard time each day

iii. Manually as an over-ride.

(e) The FCs shall not rely on the server for anti-tailgate operation. Global anti-tailgate shall work across multiple FCs, even if the server is off line.

17.9 Every incorrect PIN attempt shall be notified at the central control as an alarm condition.

17.10 Each reader shall be capable of automatically switching the access mode of a door at different times of the day based on control parameters received from the Security Management System (The System). The following access criteria modes are required:

(a) Free access Door is unlocked. No card entry required.

(b) Secure access Door is locked. A successful card attempt is required for valid entry. Door re-secures after access attempt.

(c) **Secure + PIN access**

Door is locked. A successful card attempt and correct PIN number is required for valid entry. Door re-secures after access attempt.

i. The PIN number should be set for a minimum of between 4 to 8 digits in the system configuration.

ii. Cardholders may choose how long their PIN number is, as long as it meets the minimum length requirement.

(d) **Override from reader** Members of certain Access Groups shall be able to change the access and PINs mode of the door at certain times.

(e) **Dual Authorisation** Access is granted when two different but legitimate cards are presented within a given time frame.

(f) **Escort** A second card is required to be presented from a cardholder who is nominated in the 'Escort Access Group'.

(g) **Shared PIN Number** The System Operator determines what the PIN number will be and programs this into the system. Access is allowed through the door when the correct 4 digit PIN is entered.

17.11 Cardholder access reporting to The System and logging in the audit trail shall be configurable in two modes:

(a) Only when there has been a successful presentation of a valid access card , bio-face or token AND the door open sensor has detected the door has actually been opened.

(b) Whenever there has been a successful presentation of a valid access card or bio-face irrespective of whether the door has been opened.

17.12 Readers with integrated PIN pads, or fingerprint readers using identification shall provide an 'Entry under Duress' facility.

17.12.1 Duress shall be initiated by the cardholder either by the addition of a unique number to their PIN number, or by incrementing the last digit of their PIN number by one. Duress on fingerprint readers shall be initiated by the cardholder presenting their pre-enrolled 'Duress finger'.

17.12.2 There must be NO indication of a Duress entry at the reader.

17.12.3 A critical priority 'Duress Alarm' shall be displayed at the Security Management System.

17.12.4 It must be possible to configure the system such that duress or other selected critical alarms pop to the front of the display, ensuring immediate operator attention. The existence of other incoming alarms shall be visible to the operator but must not interrupt their current task.

17.13 Zone counting shall be available to provide real-time counting of cardholders in access zones.

17.13.1 The result of the number of cardholders in the zone being outside of the specified range(s) shall generate an event or an alarm, depending on system configuration.

17.13.2 The minimum and maximum numbers of cardholders in a zone before an event is generated shall be configurable.

17.13.3 It shall be possible to set up a 'grace time' (in seconds) to allow the zone count to be outside the minimum within the mid-range or outside the maximum number of cardholders, without generating an event.

17.13.4 It shall be possible to assign a specific message for each of the below minimum, mid-range or above maximum conditions.

17.13.5 It shall be possible to set up the system to prohibit one cardholder being allowed in a zone by:

(a) Requiring two valid but different cards to access a zone should the zone count reports zero cardholders in the zone.

(b) Requiring one card to access a zone should the zone count report two or more cards in the zone.

(c) Requiring one card to exit from a zone should the zone count report three or more cards in the zone.

(d) Requiring two valid but different cards to exit from a zone should the zone count report two people present.

(e) Prohibiting exit from a zone and generate an alarm if the zone count reports one person present.

17.13.6 It shall be possible to increment and decrement zone counting based on physical inputs not related to access events.

17.13.7 It shall be possible to increment and decrement zone counting based on logical inputs not related to access events.

17.13.8 It shall be possible to schedule an Access Zone for a 'First Card Unlock' mode, whereby the Access Zone is scheduled to go to Free Access, but only when a suitably privileged card is badged at the reader. All other cards will be granted access, but will not be able to set the door to Free Access unless they have the 'First card Unlock' privilege.

17.13.9 It shall be possible for suitably privileged cardholders to toggle the access mode of a reader between Free Access and Secure by badging their card at the reader twice in quick succession.

17.13.10 It shall be possible for suitably privileged cardholders to log on to a reader with a keypad either by a card badge or PIN number and change the access mode of the reader to either Free or Secure.

17.13.11 In addition to unlocking a door when granting access, it shall be possible to activate an additional output or macro which is uniquely related to the cardholder or access group to which they belong.

17.13.12 It shall be possible to 'lock down' specific areas of a site such that cardholders who would usually have access, are denied access. Cardholders with suitable privileges such as security personnel will still have access. The 'lock down' should be activated and/or cancelled by the following methods;

(a) Clicking an icon on the site plan.

(b) Automatically, based upon an event within the system.

(c) Automatically, based upon an input activation.

18 MOBILE CLIENT APPLICATION

18.1 The System shall have a mobile client application which allows operators to remotely manage the system via a smart phone or tablet (‘the Mobile Device’). Dedicated devices with a single hardware option shall not be acceptable.

18.2 The Mobile Device shall be able to manage system alarms.

18.2.1 Alarms shall be displayed in different colours to denote the priority.

18.2.2 The alarms shall flash when unacknowledged.

18.2.3 The alarms will cease to flash when acknowledged.

18.2.4 Display the following alarm status:

i. Active.

ii. Escalated.

iii. Multiple occurrences of the same alarm within a user-defined time frame.

18.2.5 View alarm details such as:

i. Priority.

ii. Source of the alarm, e.g. door, input, cardholder etc.

iii. Date/time.

iv. Alarm history.

18.2.6 Add notes to the alarm.

18.2.7 View alarm instructions.

18.2.8 When multiple instances of the same alarm occur, the Mobile Device will present alarms as a group and display the number of alarms in each group.

18.2.9 Acknowledge Alarms.

18.2.10 Process Alarms.

18.2.11 Filter alarms by (but not limited to) the following:

i. Priority.

ii. Acknowledged.

iii. Unacknowledged.

iv. Active.

v. Inactive.

vi. Division.

18.3 The Mobile Device shall be capable of monitoring the status of system items such as (but not limited to):

i. Doors.

ii. Access Zones.

iii. Alarms Zones.

iv. Fence Zones.

v. Macros.

18.4 It shall be possible to search for items by selecting from a list or entering part of the text relating to the item name.

18.5 The Mobile Device shall be able to override items such as (but not limited to):

i. Doors.

ii. Access Zones.

iii. Alarms Zones.

iv. Fence Zones.

v. Macros.

18.6 The Mobile Device shall be able to lock down an access zone such that all cardholder access is disabled, excluding specifically authorised cardholders. This may be required in case of a security emergency on the site.

18.7 The Mobile Device shall be able to manage cardholders.

18.7.1 It shall be possible to search for cardholders by selecting from a list or entering part of the text relating to the cardholder name.

18.7.2 It shall be possible to search for cardholders based on (but not limited to):

i. Card number.

ii. User defined Personal Information Field such as Company, Department, Employee ID, Licence plate etc.

18.7.3 The Mobile Device shall display (but not be limited to) the following cardholder information:

i. Name.

ii. The last entered zone, including date/time.

iii. Image.

iv. Access Groups.

v. User defined information such as Company, Department, Employee ID, Licence plate etc.

vi. Access Cards.

18.7.4 Fields such as email address, phone number etc. shall be hyperlinks to enable the operator to click on the field and automatically be taken to the email or phone application.

18.7.5 If a cardholder record is disabled, or lacking the correct access criteria, a highlighted message shall appear on the screen to alert the operator.

18.7.6 Is shall be possible to disable a cardholder record via the Mobile Device.

18.7.7 It shall be possible to conduct a spot check of cardholders whereby the operator can view the access credentials of the cardholder on the Mobile Reader and record whether the cardholder passes an ID check and has the appropriate access rights to their current location. The operator presses a ‘Pass’ or ‘Fail’ button and enters a reason. This information is logged at the central server.

18.8 Spot checks

18.8.1 It shall be possible to conduct a spot check of cardholders whereby the operator can view the access credentials of the cardholder on the Mobile Device and record whether the cardholder passes an ID check and has the appropriate access rights to their current location.

18.8.2 The operator shall select a ‘Pass’ or ‘Fail’ button which will be logged at the central server.

18.8.3 It shall be possible for the operator to select a pre-defined reason for the pass or fail.

18.8.4 It shall be possible for the operator to enter free text into a notes field.

18.8.5 It shall be possible to record the location of the operator to indicate where the spot check took place.

18.9 It shall be possible for the Mobile Device screen to lock after a preconfigured period of inactivity.

19 MOBILE READER

19.1 The system shall have a mobile reader module (‘the Mobile Reader’) to enhance the capabilities of the mobile client application.

19.2 The Mobile Reader shall be capable of reading Mifare cards and automatically displaying the cardholder details.

19.3 The Mobile Reader shall support (but not be limited to):

19.3.1 Mifare Plus.

19.3.2 Mifare DESFire.

19.3.3 Mifare Classic.

19.3.4 Facial Readers with Weigand output

19.4 It shall be possible for the Mobile Reader to log a cardholder into or out of an access zone in the same manner as if the cardholder presented their card to a fixed access control reader.

19.5 The cardholder credentials shall be authenticated by the system and displayed in the user interface, clearly indicating an access granted or denied decision.

19.6 Access granted and denied decisions shall be indicated by different audible tones.

19.7 It shall be possible to continuously read cards without pressing any additional ‘read card’ buttons. This shall be required when logging a large group of cardholder into or out of an access zones.

20 IDENTITY ANALYTICS - COMPETENCIES

20.1 Competencies shall be cardholder-based assignable attributes, used to determine if the cardholder is allowed access to specified areas based on factors relevant to the cardholder. The factors may be based on authority or skill levels or similar.

20.2 Multiple competency attributes may be assigned to one or more cardholder records.

20.3 Each competency will assume one of 4 different states:

(a) Active - The competency is currently valid for the cardholder.

(b) Expiry due - The competency is currently valid for the cardholder but will expire in a specified period.

i. A configurable message shall be displayed advising the cardholder that the competency is about to expire.

(c) Expired - The competency has been assigned to the cardholder but has expired.

(d) Disabled - The competency, is temporarily disabled (or overridden) for the cardholder.

i. A field shall be provided to store the reason for disabling a competency.

20.4 The competency states shall be configurable as ‘soft’ allowing access but generating an alarm; or ‘hard’ denying access, should a competency requirement not be met.

20.5 Each competency shall be individually set per cardholder

20.6 A field shall be provided to store the reason for disabling a competency.

20.7 Competencies shall be configured as required per access zone.

20.8 It shall be possible to exempt specific access groups from the requirement to meet specific competencies.

20.9 Denied access due to an invalid or missing competency shall be displayed to the user at the door reader.

20.10 Access permission based on competency criteria must be determined at the Intelligent Field Controller (FC), independent of the Server being on line.

20.11 The reason for denied access due to an invalid competency shall be displayed on the door reader or keypad.

20.12 Advanced warning of a cardholder’s competency about to expire shall be sent to the individual and/or other nominated persons via email.

20.13 Notice of a cardholder’s competency expiry shall be sent to the individual and/or other nominated persons via email.

20.14 A consolidated report detailing competency expiry warnings for cardholders shall be sent via email to the associated manager.

21 PRE-PROGRAMMED OVERRIDE MACROS

21.1 To allow for making changes to the system configuration on demand, it shall be possible to pre-configure the required changes and assign them to a macro action.

21.2 Macro actions shall be capable of (but not limited) the following;

21.2.1 Open doors.

21.2.2 Change door modes such as Free, Secure, Secure with PIN, Dual Authority.

21.2.3 Anti-Passback Forgive.

21.2.4 Active and release zone Lockdown (i.e deny access for cardholders during and emergency).

21.2.5 Reset the Cardholder count in a zone.

21.2.6 Switch an output on and off.

21.2.7 Activate the generation of pre-configured reports.

21.2.8 Start and stop a Guard Tour.

21.3 A macro shall be capable of activating multiple actions from within a single macro. There shall be no fixed limit to the number of actions that can be configured.

21.4 An operator shall be able to initiate the macro via either a menu item or by a site plan icon.

21.5 Macros shall be capable of being activated by any system events.

21.6 Macro configuration must be by the use of GUI features such as drop down lists and drag-and-drop techniques. The use of script language to write macros is not acceptable.

21.7 It shall be possible to initiate Macros based on a on a time schedule.

21.8 Macros shall be able to execute Microsoft Windows command line actions.

21.9 Up to 300 character variables shall be able to be specified for each command line

21.10 Each Macro shall be able to contain multiple command line entries

21.11 The configuration and execution of command line Macros shall be user account name and password protected. These user names and passwords shall be obscured on entry, and transmitted and stored at the central command system server in an encrypted format.

22 ON-LINE DOOR CONTROL

22.1 Access control for a door shall allow for the following features where specified:

(a) Access reader

(b) Emergency release switch input

(c) Reception control switch input

(d) Fever scanning control to stop people with high fever

22.2 Egress control for a door shall allow for the following features where specified:

(a) Exit reader

(b) Push button request to exit

(c) Emergency exit break-glass

22.3 A push button request to exit shall record the exit in the event database.

22.4 When requested by a valid means of access or egress, the door shall unlock for a preset period, after which the door shall relock.

22.4.1 If access or egress is completed prior to the pre-set time expiring, then the door shall relock immediately the door has closed.

22.4.2 The period of unlock shall be extended should a cardholder have a suitable privilege. This may be the case for a person with a disability.

22.5 All entry and exit methods shall be recorded in the event in the event database.

22.6 The door shall be monitored for both door open/closed and door unlocked/locked using concealed monitor switches appropriate for the door installation.

22.7 Where the door is a double door, the inactive door leaf shall also be monitored for door open/closed and door unlocked/locked. The inactive leaf door monitor switches may be connected as part of the active door leaf monitoring.

22.8 It shall be possible to configure the door in a way that generates a forced door alarm should the door be unlocked and/or opened without first being released by the system.

22.9 Should a door be left unlocked or open after a preset time, an alarm shall be generated reporting the condition.

22.10 The door open/unlocked warnings shall provide an audible warning at the door.

22.11 It shall be possible to disable the reader audible warning.

22.12 It shall be possible to generate the audible warning via a relay connected elsewhere in the system.

22.13 Should a valid request to access a door be generated and access not taken, it shall be possible to ignore the request (not record it as an entry event) and automatically re-secure the door after a preset time.

22.14 When a valid access through a door is undertaken, the door shall immediately re-secure on re-closing irrespective of the door unlock time.

22.15 The system shall have a ‘lockdown’ feature whereby cardholders who would usually have access to Access Zones are denied access.

22.15.1 It shall be possible to ‘lock-down’ an Access Zone based on any event within the system.

22.15.2 It shall be possible to assign specific cardholders the right to access a zone when the access zone is locked, whilst refusing access to all other cardholders.

22.16 It shall be possible to create an interlock relationship between groups of doors for situations such as ‘mantraps’ whereby a door cannot be opened until other doors or inputs are closed.

22.16.1 Up to 20 doors shall be included in any interlock group.

22.16.2 It shall be possible to configure interlock groups via GUI ‘drag and drop’ functionality without the requirement to write scripted logic.

22.16.3 It shall be possible to assign outputs that activate when the fever reader ,reads high which will interlock so as to advise cardholders and not open the door or turnstile.

22.17 The system shall support a challenge or video verification mode as specified below:

22.17.1 When a card is presented at a reader, images from the cardholder database (as many as required) shall be displayed in the challenge window.

22.17.2 Associated with the images, it shall be possible to display a video image from one or more assigned cameras.

22.17.3 In Challenge Mode it shall be possible to view a site plan showing the location and status of the controlled entry point and nearby items.

22.17.4 In Challenge Mode it shall be possible for the operator to view the status of the cardholder’s cards and competencies for the purpose of informing the cardholder, at the time of entry, if any expiries are imminent.

22.17.5 Specific personal data shall also be able to be displayed, associated with the cardholder (name details, department etc).

22.17.6 Associated with a challenge entry, the selection and layout on screen of cardholder images, cardholder personal data, cardholder card or competency status, site plans or video images must be configurable using simple drag and drop, or click and drag techniques to resize or reposition information.

22.17.7 The Challenge Mode shall be configurable to either:

(a) Automatically grant access to a valid card. In this case the system shall be able to display the current access decision (granted or denied) to the challenge operator.

(b) Require operator intervention to grant access to a valid cardholder.

22.17.8 Should a second challenge be requested while an unanswered challenge remains in the system, the second and subsequent challenges shall queue automatically awaiting response.

22.17.9 It shall be possible for an operator to view waiting challenge events and to select and process challenge events within the queue in any order they choose.

22.17.10 The system shall allow challenge events to be managed from a single full-screen view per operator or multiple filtered views, as dictated by the customer.

23 OFF-LINE DOOR CONTROL

23.1 Where specified, doors shall be managed using an off-line door locking system.

23.2 A single interface shall be provided that allows for administration and reporting including both the online and offline (or standalone) locking systems.

23.3 The off-line doors shall be fully integrated into the Access Control and Intruder Alarm System as described below:

23.3.1 Facial technology shall be contactless and compatable with Mifare Classic, Mifare Plus and Mifare DESFire, as required for all on-line doors ,booths, booms and turnstiles.

23.3.2 Encoding shall be carried out as a single encode operation for both on-line and off-line door readers.

23.3.3 Operational data shall be transferred between the integrated security system and off-line doors automatically, without the need for specific operator actions. This data shall include:

(a) Multiple levels of door low battery voltage alarms.

(b) Access activity from all doors.

(c) Disabled card information

(d) Changes to cardholder access privileges.

23.3.4 Assignment of access privileges for use in both online and offline doors shall be available through a single interface.

23.3.5 Access privileges based on the time of day shall be available (e.g. office hours versus after hours) or type of day (e.g. weekdays versus weekends) with full flexibility in specifying the time intervals or day types for any user.

23.3.6 It shall be possible to configure the system to ensure access updates for off-line doors are enforced within a given period of time, configurable as a minimum from 1 to 7 days.

23.3.7 Access privileges must not be stored at the door escutcheon (eliminating the need to update each door escutcheon when a user is added or removed).

23.3.8 For disabled access, the ability to specify an extended door opening time for specific users shall also be available for off-line doors.

23.3.9 Off-line doors shall support partitioning to allow specific administrators to control and assign access privileges within their own environment/facility.

23.4 The range of hardware shall include an option for an internal privacy lock which, when activated, prevents entry except for privileged users.

23.5 Hardware shall not use proprietary batteries. Batteries must be commonly available types.

23.6 Battery life shall support a minimum of 35,000 operations before replacement is required.

23.7 The escutcheon hardware shall be compatible with the lock hardware specified for this project.

23.8 Electronic escutcheon hardware shall be simple to fit to existing mechanical door lock hardware.

23.8.1 Escutcheon hardware must be compatible with the mechanical door lock hardware, noting:

(a) Spindle size; and

(b) Door handle rotation angle.

23.9 Basic maintenance (changing batteries, changing basic configuration) shall be able to be carried out by customer maintenance staff with minimal instruction.

23.10 The off-line escutcheons should be able to hold an audit trail of at minimum the last 1000 events.

23.11 The off-line escutcheons shall be able to function in a variety of modes such as but not limited to, free (unlocked), secure (locked) by schedule or as controlled by a user with privilege to change the escutcheon mode.

23.12 It shall be possible to change a door state between the free and secure states using an authorised card or facial .

23.13 It shall be possible to specify on a user by user basis what modes they can place the lock in (e.g. free or secure) and override functions the user can perform (i.e. entry allowed when privacy lock is on).

23.14 A handheld programming device shall be available for the purposes of:

(a) Diagnosing problems

(b) Performing an emergency opening of an offline escutcheon.

(c) Updating software from time to time.

(d) Provide power to the escutcheon to allow resolving a no battery voltage situation.

(e) Initialising future doors that may be added from time to time.

23.15 Multiple levels of warning for low battery indication including audible, visual and physical warnings (i.e. initially a visual signal progressing to an audible and visual indicator and then finally progressing to an audible, visual and delayed opening of the door to indicate/prompt someone to report the occurrence).

23.16 Environmental protection shall be provided for the door installation.

23.16.1 The environmental rating for the escutcheon shall be at least ip46

23.16.2 The environmental rating for the cylinders shall be at least IP66

23.17 The hardware range shall include the ability to upgrade off-line doors to wireless through a wireless gateway.

24 WIRELESS DOOR CONTROL

24.1 Where specified, doors shall be managed using an escutcheon based, wireless door locking system.

24.2 A single, seamless user interface shall be provided within the head end to ensure integrity of access decisions are maintained within the primary access control system.

24.3 The flow of information from the RFID card shall be transmitted instantaneously to the wireless card reader/lock, (escutcheon or cylinder type) which shall in turn send the card credentials to the hub and access control system.

24.4 The primary Access Control and Intruder Alarm system shall provide real-time access decisions as described elsewhere in this specification.

24.5 Assignment of access privileges for use in both wired online and wireless doors shall be available through a single interface.

24.6 Card encoding shall be carried out as a single encode operation for both wired on-line and wireless door readers

24.7 A wireless RS485 communication hub shall support up to 8 wireless escutcheons or cylinders and have reliable communication to each reader within a distance of 15 metres.

24.7.1 Wireless hubs shall be able to be wired in series with RS485 compatible cable.

24.7.2 The wireless hub shall conform to the radio standard applicable to the region of installation and conform to IEEE802.15.4 (2400 – 2483.5 MHz).

24.7.3 AES 128bit encryption shall apply for communication between the hub and each wireless reader.

24.7.4 Up to 16 (installer selectable) channels per hub shall be available to ensure each wireless escutcheon or cylinder is configured with reliable communication.

24.7.5 The hardware shall use non propriety batteries commonly available and provide for up to 40,000 operations before replacement.

24.8 The wireless doors shall be fully integrated into the Access Control and Intruder Alarm System as described below:

24.8.1 Card technology shall be contactless Mifare standard and Mifare DESFire, as required for all on-line doors.

24.8.2 Operational data shall be transferred between the integrated security system and wireless doors automatically, without the need for specific operator actions. This data shall include:

(a) Multiple levels of door low battery voltage alarms.

(b) Access activity from all doors.

(c) Disabled card information

(d) Changes to cardholder access privileges.

24.8.3 Escutcheon hardware must be compatible with the mechanical door lock hardware, noting:

(a) Spindle size; and

(b) Door handle rotation angle.

24.9 Basic maintenance (changing batteries, changing basic configuration) shall be able to be carried out by customer maintenance staff with minimal instruction.

24.10 The installer service tool shall communicate with each wireless hub and enable configuration, management and override of each door independent of the access control system.

25 SYSTEM INTEGRATION

25.1 The system shall support OPC (OLE for Process Control) Alarms and Events protocol to provide an open interface to allow integration with Building and Facilities Management, and Management Information Systems.

25.2 The OPC (Alarms and Events) interface shall allow third party OPC clients to register to receive alarms and events from the Security Management System (The System).

25.2.1 When an alarm is processed, the OPC Alarms & Events client shall send an event processed message back to the security system to process the alarm on the security system.

25.3 The system shall support OPC (OLE for Process Control) Data Access protocol to provide an open interface to allow the status of system components to be reported to an external OPC (Data Access) client.

25.4 The OPC Interface shall allow third party OPC (Data Access) clients to generate system component overrides including but not limited to alarm zone and access zone overrides.

25.5 The system shall provide an XML interface to allow for the import, export, and synchronisation of data in an on-going basis from other applications directly into the Cardholder database both an on-line real time manner or in a batch oriented approach. A developer's kit shall be readily available to allow for easy implementation.

25.6 The system shall provide an XML interface to allow for updating access control schedules from other applications directly into the system configuration database both an on-line real time manner or in a batch oriented approach. A developer's kit shall be readily available to allow for easy implementation.

25.7 The system shall provide a tool which allows configuration and synchronisation of cardholder data with 3rd party systems via a Comma Separated Variable (CSV) file.

25.7.1 Data import shall be triggered manually.

25.7.2 Data import shall be triggered on a schedule.

25.7.3 The system shall allow the import of images.

25.8 An Application Programming Interface (API) shall be available to allow 3rd party systems to be integrated into the system.

25.8.1 The API shall allow 3rd party systems to pass events to The System and for the events to appear in The System event window.

25.8.2 It shall be possible for The System to be programmed to trigger actions based upon these external events. For example, a video analytic alarm from a Video Management System is passed to The System. The System in turn will lock doors and raise and alarm.

25.8.3 It shall be possible for a 3rd party system to send a card number and site code to The System so as to act as a ‘virtual card reader’.

25.8.4 The API shall allow the 3rd party system to interact directly with the FC.

25.9 A facility shall be provided in the system to allow for the real-time export of any alarm or event information to 3rd party systems via customisable strings for the purposes of controlling the 3rd party application and/or receiving information from a third party system.

25.9.1 The system shall use Winsock

25.10 The system shall support accepting events from one or more 3rd party applications and displaying these and their status in the event and/or alarm windows.

25.11 The system shall support a Simple Network Management Protocol (SNMP) interface to allow the system to monitor network attached devices for conditions that warrant administrative attention, such as events from a UPS or network switch.

25.12 The system shall support BACnet.

25.13 Events from 3rd party systems shall be managed in the same way as inputs connected directly to the FCs.

25.14 The system shall allow a 3rd party system to create, remove and modify cardholders, including assigning access rights, via Web Services.

25.15 The system shall allow a 3rd party system to create and modify visits in the Visitor Management System, via Web Services.

25.16 Interactions with 3rd party systems shall be logged in the system.

26 ACCESS CONTROL READERS – PROXIMITY 125 KHZ TECHNOLOGY

The technology for the Access Control Readers will be specified in accompanying sections. When required, these readers shall meet the following specification:

26.1 The reader shall support Proximity 125 kHz technology.

26.2 The reader shall be capable of reading Proximity 125 kHz cards from other manufacturers.

26.3 The card only reader option shall include an audible beeper and red/green LEDs, to provide feedback to users.

26.4 The beeper shall give different beeps to indicate:

(a) Access granted

(b) Access denied.

(c) 2nd card required when dual card authorisation or escort mode is programmed.

26.5 A steady red LED shall indicate door secure.

26.6 A flashing red LED shall indicate access denied.

26.7 A steady green LED shall indicate door free access.

26.8 A flashing green LED shall indicate access granted.

26.9 Readers shall generate a heartbeat signal to enable the Intelligent Field Controller (FC) to identify lost communications and thereby generate an alarm.

26.10 The reader must accept a message from the FC to advise that the data from reader to FC has been received and to consequently stop sending the card data.

26.11 Each reader shall be identified independently at the central control by means of a unique plain language descriptor. The central control plain language descriptor shall be at least 60 characters in length.

26.12 Where a PIN pad is specified, the reader shall include:

(a) A PIN pad fully integrated with the reader.

(b) Backlit PIN pad.

(c) An backlit LCD display indicating:

i. Card required

ii. PIN required

iii. Access denied

iv. Intruder alarm set

v. Intruder alarm unset

vi. Free access

vii. 2nd card required

26.12.2 The PIN pad shall include:

(a) Standard 0 to 9 digit keys

(b) CE (clear entry)

(c) IN (enter key)

(d) Three function keys (F1, F2 and F3)

27 ACCESS CONTROL READERS – MIFARE TECHNOLOGY

How the solutionworks

Two primary aspects of biometric authentication , identification and verification

Identification

Identification is suited for customers wanting card less access to areas of their site.

Identification compares a person's fingerprint or facial to a database of stored templates, typically stored on the fingerprint or facial reader, and identities the person from this database.

This is also commonly referred to as a '1 to many' or '1 to n' comparison. An employee presents their finger or face to the reader, which checks the reader database for a matching fingerprint. Or face. If the reader finds a match, it sends through the employee's ID to the Controller for an access control decision.

Verification

Verification is suited for customers wanting the high security of multi -fact or authentication options (card + fingerprint (or face)+ pin).

Verification compares a person's fingerprint or facial against a single fingerprint or facial template, stored on the card. This is commonly referred to as a '1 to 1 ' comparison. Employees present their card to the reader, and then present their fingerprint or face.

The reader checks if the presented fingerprint or facial image matches the template stored on the card. If the reader finds a match, it sends through the employee’s ID to the Access Control Controller for an access control decision.

The technology for the Access Control Readers will be specified in accompanying sections. When required, these readers shall meet the following specification:

27.1 The reader shall support the following technologies;

27.1.1 Mifare Classic

27.1.2 Mifare Plus

27.1.3 Mifare DESFire EV1

27.1.4 Near Field Communication (NFC)

27.2 The reader shall be capable of reading the card serial number (CSN) of the Mifare card.

27.3 The readers shall support self-discovery on The Security Management System (The System).

27.3.1 Readers shall contain a unique serial number.

27.3.2 When connected to an Intelligent Field Controller (FC), the serial number of the reader shall be reported to The System.

27.3.3 Once assigned to a function within an FC, if any attempt is made to substitute readers in the field without authorisation, an alarm shall be generated.

27.4 Data communication rate between FCs and readers shall be at least 1Mbit/second.

27.5 Communication sessions between FCs and readers shall use certificate exchange protocols using keys with a minimum strength of 256 bit elliptical encryption.

27.6 Data communication between FCs and readers shall use a minimum of 128 bit AES encryption.

27.7 Readers shall generate a heartbeat signal to enable the FC to identify lost communications and thereby generate an alarm.

27.8 Readers shall be upgradeable via software downloaded from The System without any intervention at the reader.

27.9 The reader must accept a message from the FC to advise that data from reader to FC has been received and to consequently stop sending the card data.

27.10 Each reader shall be identified independently on The System by means of a unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

27.11 Where a card only reader is specified, the reader shall include:

27.11.1 Integrated reader module supporting the technologies listed above.

27.11.2 The card only reader option shall include an audible beeper and red/green LEDs to provide user feedback.

27.11.3 The beeper shall give different beeps to indicate:

(a) Access granted.

(b) Access denied.

(c) 2nd card required when dual card authorisation or escort mode is programmed.

27.11.4 A steady red LED shall indicate door secure.

27.11.5 A flashing red LED shall indicate access denied.

27.11.6 A steady green LED shall indicate door free access.

27.11.7 A flashing green LED shall indicate access granted.

27.11.8 It shall be possible to turn off the reader LED indication via The System software.

27.11.9 It shall be possible to turn off the reader beeper via The System software.

27.11.10 Readers must comply with at least IP68 environmental protection rating.

27.11.11 Readers must comply with an impact rating of at least IK07

27.11.12 A vandal resistant enclosure having an impact rating of at least IK08 rating shall be provided where.

(a) Vandal covers shall be fixed to the wall surface using tamper-resistant screws.

(b) Vandal covers shall have bevelled edges to limit the ability for persons use the reader as an aid to climbing the building.

(c) All external surfaces shall be bevelled and without protruding parts to meet anti-ligature requirements.

27.11.13 The reader must be RoHS compliant

27.11.14 The reader shall operate with a temperature range of -30ºc to +70ºc.

27.12 Where a card reader with PIN pad and display is specified, the reader shall include:

27.12.1 A minimum of a 3.5" LED colour display.

27.12.2 Backlit keys.

27.12.3 Integrated reader module supporting the technologies listed above.

27.12.4 An option with no reader module, for use as an Alarms Management Terminal.

27.12.5 Support for multiple languages which shall be selectable from The System software.

27.12.6 The reader shall display information to the user using a combination of text and graphics.

27.12.7 The reader shall display the date and time.

27.12.8 Menus shall be accessible by logging on with either a card or a PIN number.

27.12.9 The reader shall be capable of (but not limited to) carrying out the following functions:

(a) Arm alarm zones. A minimum of 50 per reader must be supported.

(b) Disarm alarm zones. A minimum of 50 per reader must be supported.

(c) View Alarms. A minimum of 100 per reader must be supported.

(d) Acknowledge alarms. A minimum of 100 per reader must be supported.

(e) View alarm history. A minimum of 100 per reader must be supported.

(f) Change the door to Free Access mode.

(g) Change the door to Secure Access mode.

(h) Change the door to operate from a user defined schedule.

(i) Turn outputs on and off. A minimum of 50 per reader must be supported.

(j) View the status of inputs. A minimum of 100 per reader must be supported.

(k) Isolate inputs. A minimum of 100 per reader must be supported.

27.12.10 User definable custom images shall be displayed on the screen when the reader is idle.

27.12.11 The reader shall support the following image formats;

(a) .PNG

(b) .JPG

(c) .JPEG

27.12.12 It shall be possible to adjust the reader beeper via The System software to the following volume levels;

(a) Off

(b) Quiet

(c) Normal

(d) Loud

27.12.13 The reader shall have the ability to display the status of alarms and system I/O via LEDs on front panel.

(a) The reader shall support at least 8 LEDs.

27.12.14 It shall be possible to turn off the reader LED indication via The System software.

27.12.15 Tamper protection shall be provided against the unit being removed from the mounting surface.

27.12.16 Readers must comply with a minimum IP66 environmental protection rating.

27.12.17 Readers must comply with an impact rating of at least IK09

27.12.18 The must be RoHS compliant

27.12.19 The reader shall operate with a temperature range of -30^{o}c to +70^{o}c.

28 ACCESS CONTROL READERS – MUTLI-TECHNOLOGY

The technology for the Access Control Readers will be specified in accompanying sections. When required, these readers shall meet the following specification:

28.1 The reader shall support the following technologies;

28.1.1 Mifare Classic

28.1.2 Mifare Plus

28.1.3 Mifare DESFire EV1

28.1.4 Near Field Communication (NFC)

28.1.5 Proximity 125 kHz

28.2 The reader shall be capable of reading the card serial number (CSN) of the Mifare card.

28.3 Where the Proximity 125 kHz is required, the reader shall be capable of reading Proximity 125 kHz cards from other manufacturers.

28.4 The readers shall support self-discovery on The Security Management System (The System).

28.4.1 Readers shall contain a unique serial number.

28.4.2 When connected to an Intelligent Field Controller (FC), the serial number of the reader shall be reported to The System.

28.4.3 Once assigned to a function within an FC, if any attempt is made to substitute readers in the field without authorisation, an alarm shall be generated.

28.5 Data communication rate between FCs and readers shall be at least 1Mbit/second.

28.6 Communication sessions between FCs and readers shall use certificate exchange protocols using keys with a minimum strength of 256 bit elliptical encryption.

28.7 Data communication between FCs and readers shall use a minimum of 128 bit AES encryption.

28.8 Readers shall generate a heartbeat signal to enable the FC to identify lost communications and thereby generate an alarm.

28.9 Readers shall be upgradeable via software downloaded from the system or IXM WEB.

28.9.1 The above must be possible without any intervention at the reader.

28.10 The reader must accept a message from the FC to advise that the data from reader to FC has been received and to consequently stop sending the card data.

28.11 Each reader shall be identified independently at the central control by means of a unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

28.12 Where a card only reader is specified, the reader shall include:

28.12.1 Integrated reader module supporting the technologies listed above.

28.12.2 The card only reader option shall include an audible beeper and red/green LEDs to provide user feedback.

28.12.3 The beeper shall give different beeps to indicate:

(a) Access granted

(b) Access denied.

(c) 2nd card required when dual card authorisation or escort mode is programmed.

28.12.4 A steady red LED shall indicate door secure.

28.12.5 A flashing red LED shall indicate access denied.

28.12.6 A steady green LED shall indicate door free access.

28.12.7 A flashing green LED shall indicate access granted.

28.12.8 It shall be possible to turn off the reader LED indication via The System software.

28.12.9 It shall be possible to turn off the reader beeper via The System software.

28.12.10 Readers must comply with at least IP68 environmental protection rating.

28.12.11 Readers must comply with an impact rating of at least IK07

28.12.12 A vandal resistant enclosure having an impact rating of at least IK08 rating shall be provided where.

(a) Vandal covers shall be fixed to the wall surface using tamper-resistant screws.

(b) Vandal covers shall have bevelled edges to limit the ability for persons use the reader as an aid to climbing the building.

(c) All external surfaces shall be bevelled and without protruding parts to meet anti-ligature requirements.

28.12.13 The reader must be RoHS compliant

28.12.14 The reader shall operate with a temperature range of -30^{o}c to +70^{o}c.

28.13 Where a card reader with PIN pad and display is specified, the reader shall include:

28.13.1 A minimum of a 3.5" LED colour display

28.13.2 Backlit keys

28.13.3 Integrated reader module supporting the technologies listed above.

28.13.4 An option with no reader module, for use as an Alarms Management Terminal.

28.13.5 Support for multiple languages which shall be selectable from The System software.

28.13.6 The reader shall display information to the user using a combination of text and graphics.

28.13.7 The reader shall display the date and time.

28.13.8 Menus shall be accessible by logging on with either a card or a PIN number.

28.13.9 The reader shall be capable of (but not limited to) carrying out the following functions;

(a) Arm alarm zones. A minimum of 50 per reader must be supported.

(b) Disarm alarm zones. A minimum of 50 per reader must be supported.

(c) View Alarms. A minimum of 100 per reader must be supported.

(d) Acknowledge alarms. A minimum of 100 per reader must be supported.

(e) View alarm history. A minimum of 100 per reader must be supported.

(f) Change the door to Free Access mode.

(g) Change the door to Secure Access mode.

(h) Change the door to operate from a user defined schedule.

(i) Turn outputs on and off. A minimum of 50 per reader must be supported.

(j) View the status of inputs. A minimum of 100 per reader must be supported.

(k) Isolate inputs. A minimum of 100 per reader must be supported.

28.13.10 User definable custom images shall be displayed on the screen when the reader is idle.

28.13.11 The reader shall support the following image formats;

(a) .PNG

(b) .JPG

(c) .JPEG

28.13.12 It shall be possible to adjust the reader beeper via The System software to the following volume levels;

(a) Off

(b) Quiet

(c) Normal

(d) Loud

28.13.13 The reader shall have the ability to display the status of alarms and system I/O via LEDs on front panel.

(a) The reader shall support at least 8 LEDs.

28.13.14 It shall be possible to turn off the reader LED indication via The System software.

28.13.15 It shall be possible to turn off the reader beeper via The System software.

28.13.16 Tamper protection shall be provided against the unit being removed from the mounting surface.

28.13.17 Readers must comply with at least IP66 environmental protection rating.

28.13.18 Readers must comply with an impact rating of at least IK09

28.13.19 The must be RoHS compliant

28.13.20 The reader shall operate with a temperature range of -30^{o}c to +70^{o}c.

29 BIOMETRIC (FACIAL) READERS

29.1 Where shown on our drawings, **biometric facial readers** are required for this project at Sentech STP.

29.2 The reader shall be designed for wall mounting, positioned to allow ease of use for the user.

29.3 Where required, visual (LED and LCD graphic display) and audible feedback shall be provided to indicate:

(a) Reposition the face for a valid read

(b) Access granted

(c) Access denied.

29.3.2 The reader shall also include a contactless hand palm reader for verification mode where the face template is stored.

29.3.3 Tamper protection shall be provided against the unit being opened and against the unit being removed from the mounting surface.

29.3.4 The sensor resolution shall be 500dpi or greater and FBI PIV-IQS certified

29.3.5 Bio template (face and/or palm) read time shall be less than one second.

29.3.6 The reader shall be able to detect and reject fake face and palm (spoofing) presented to the reader.

29.3.7 System must offer identification (1:N) and verification (1:1) modes without the need for re- enrollment or re-loading of the User database as the same respective biometric record (face/finger vein/fingerprint or hand palm) is applicable for both authentication modes.

29.3.8 Face Recognition – Reader must allow for maximum storage of 100K users and templates in 1:N mode and up to 500K in 1:1 mode. Reader must allow for the enrollment of 1 face template per user.

29.3.9 In 1:N mode, reader to provide identification matching speeds, for maximum user storage for each respective modality, in well under 1 second.

29.3.10 Reader must offers a multitude of networking capabilities which include TCP/IP, USB Auxiliary, Wi-Fi and Bluetooth.

29.3.11 The Reader must offer a embedded platform architectured and should be developed on Android Nougat or one of the latest and most advanced open sourced operating systems with the latest version of a Web-based interactive and administrative software, which must allow for remote access from any laptop, tablet or smartphone provided that there is Internet connectivity as well as authorized permission via one of the account profiles.

29.3.12 A Software Development Kit with the reader SDK must be made available, which will allow developers to integrate the reader offered, features and functions into existing or new software applications.

29.3.13 Enrollment – Creation of a Biometric record which involves the entry of User data, capturing of a live face from the camera, and hand palm, internal processing of the data to generate a User biometric record, followed by storage of the record either (a) solely in the Server database or (b) both in the Server and device databases

29.3.14 Reader must be distributed with a copy of the latest version of IXM WEB.

29.3.15 IXM WEB must provide the IT and network administrator remote access to the network of reader devices for setup, configuration and maintenance. IXM WEB shall also provide a centralized database (SQL Server Express 2008) to store the biometric records on a Server and/or locally on each device on the network.

29.3.16 **Face Recognition**

Reader must come equipped with a >5 MP camera with autofocus, LED Flash and ambient sensor for face recognition in all light conditions. Facial recognition algorithm must allow for live detection of frontal, non-frontal, and partial profiles, with the best combination of speed and accuracy. Using face tracking and video-based recognition, reader must be capable of automated demographic estimation (age, race/ethnicity, and gender) as well as automated detection of facial pose (pitch/yaw) and glasses (eyeglasses and sunglasses). These cutting-edge and sophisticated capabilities must not hinder the processing speed as the internal processor must allow for fast enrollment and matching.

29.3.17 **Certifications**

- FCC Class B
- CE certifications, along with RoHS, WEEE, IP67 and IK10 compliance

29.3.18 **Wiegand Inputs & Outputs**

Reader must have dedicated leads for Wiegand Inputs and Outputs along with Wiegand Ground via the Wired Back Cover (wiring harness). The Wiegand Inputs can be used for connectivity of a third-party proximity reader should the installation require one. The Wiegand Outputs can be used to connect directly to an access control panel.

Reader must support a Pre-defined Standard 26-bit, Pass-thru and Custom up to 512- bit Wiegand formats. The Pass-thru and Custom formats shall be configured through IXM WEB.

Reader must allow for configuration of individual Wiegand Output formats for the following events:

a. Wiegand Output – Choice of ID Type and Format for Duress
b. Identification – One format for Success, One format for Failure
c. Verification - One format for Success, One format for Failure
d. Anti-Shock – Format and Pre-defined ID Value
e. Heart-beat – Format and Pre-defined ID Value

Reader should allow for configuration of the Pass-thru format in IXM WEB based on the following specifications:

a. Total bits – The total number of bits in the Wiegand string format
b. ID Start bits – The position of the first ID bit in the Wiegand string
c. Total ID bits – The total number of bits of the ID field in the Wiegand string

Reader should allow for configuration of the Custom Wiegand format in IXM WEB based on the following specifications:

a. Even Parity
b. Odd Parity
c. Total ID bits
d. Flex Fields (ie. Facility Code, Job Code, or Company ID Code)
e. Other (ie. Access Control Panel optional fields)

29.4 Specific Purpose Inputs & Outputs

Reader can have the following dedicated leads for three Specific Purpose Inputs (SPI's) and three for Specific Purpose Outputs (SPO's) for general use.

The SPI's allow for the trigger of the following actions per each individual input line:

- None
- Release Alarm
- Restart Device

The SPO's trigger based on the following actions per each individual output line or combination of any three lines:

a. Authentication Success
b. Authentication Fail
c. Anti-Shock On

d. Door Open
e. Door Close
f. Forced Open Door
g. Door Held Open
h. Duress Finger
i. Device Boot Up

29.5 Door Access Control Mode

Readers may not be used to trigger the door magnetic lock. All door controls must be done from the controller relays in the secure side of the door

- Door strike or Dead bolt
- External Power supply for Door strike (As recommended by Door strike or Dead bolt manufacturer.
- Snubber diode for Power supply protection against inductive kickback
- Door contact
- Request-to-exit mechanism (Motion detector or Push button)

The controller will allow for configuration of the Door Access Control settings in IXM WEB for the following:

a. Unlock Time
b. Open Time
c. Request-to-Exit Time
d. Door Open Schedule (from 1 up to 1440 min)

29.6 Anti-Shock Vandal Protection (Tamper)

The reader should prefarably allows for setting of the sensitivity of an on-board accelerometer for Anti- Shock Vandal Protection. The sensitivity levels available are:

- Very High
- High
- Medium
- Low

Reader should preferably allow for an individual or a combination of actions to result based on the triggering of the Anti-Shock alarm, which are the following:

a. Delete All Users
b. Deactivate Biometrics
c. Send Wiegand
d. Audio Alert
e. LED Alert

29.7 LEDs

Reader should allow for configuration of the LEDs for 6 different colours: Red, Yellow, Green, Cyan, Blue and Magenta for the following events:

- Idle
- Device Up
- Place Finger
- Remove Credentials
- Access Granted
- Access Denied
- Processing
- Error
- Fire Alarm
- Anti-Shock Alarm
- Door Forced Open
- Door Open Too Long
- Door Open Time
- Clear Alarm
- Show Card
- Presence Detect
- Wait
- User Not Found

29.8 Fever Scanning

29.8.1 **Following the covid-19 requirement that all companies must screen all people entering their business.**

29.8.2 **Tenderers are to supply a fully integrated fever screening system linked to the new facial access control readers.**

29.8.3 **The fever readers installed on the outside of the secure areas must be able to comply to iso/tr 13154:2017**

29.8.4 **The individual being screened and the external temperature reference source (required for calibrated and thermal drift compensated cameras. Person should be in the correct position and orientation relative to the fever screener/camera for proper**

focal distance, depth of field and image capture. There should be a means of ensuring that the individual being screened is in this proper position, e.g. Marks on the floor. Consideration should be given to individuals in wheelchairs.

29.8.5 **Persons must remove eye wear**

29.8.6 **The camera should be positioned 1m in-front of the subject.**

29.8.7 **The backdrop behind the individual being screened and, when used, side screens should be thermally uniform, high emissivity (non-reflective in the ir spectrum) and light in color (visible spectrum).**

29.8.8 **The operator should be positioned with a clear visual field of the individual being screened and the display of the screening thermograph. The operator may need to intervene to correct the individual's position. The operator should also be positioned in such a way as to divert individuals to the secondary screening area when required.**

29.8.9 **If a camera is to be used the camera should measure temperature at the tear duct (inner canthus) as this location provides the closest temperature correlation to human core body temperature.**

29.8.10 **If the camera detects elevated skin temperature in a person being screened the system will stop the employee from entering into the building in the case of an visitor or contractor the security guard on duty will stop such a person to enter into sentech. Security should request that such an individual be screened using a device designed specifically for measuring body temperature, such as a clinical thermometer.**

29.8.11 **Screening must be effective or controlled outside and must be able to position the unit where direct lighting, outside light, reflective objects, or crowds of people can be seen in the field of view. Ambient temperature must be central to the controlled environment. Temperatures too warm or too cold for comfort (18°c to 24°c is optimal and iso requirement) should not affect the accuracy of the target temperature reading.**

29.8.12 **The system offered must be able to give a relay output to the access control system to control doors and turnstiles.**

29.8.13 **It is preferable to install a fever reader system that forms part of the bio-facial reader.**

29.8.14 **The fever reader unit must be ip 65 or better.**

30 ACCESS CARDS AND TOKENS

30.1 The access token technology for this project shall match the reader technology as specified separately but in association with this specification.

30.2 Access cards shall be of standard credit card size, being no larger than CR-80 and shall be direct printable using a dye-sublimation print process or be capable of accepting an adhesive label printed through such a process.

30.3 All cards shall meet ISO standards.

30.4 As well as CR80 sized cards, vehicle tokens and key-ring transponders should also be proposed as an alternative, where available.

30.4.1 The access token data shall include:

(a) Support for up to 2008-bit card numbers

(b) Where a proprietary card number format is offered, the card format shall include:

i. A unique facility (site) code not used for any other system worldwide.

ii. A unique cardholder identification number at least 7 digits long.

iii. An issue level for each card number to allow for replacing lost cards without reducing the card database size. Up to 15 levels of issue levels shall be supported.

30.4.2 The access control token shall uniquely identify the cardholder to the access control system.

30.4.3 Access control information shall be stored on or in the access token in a secure format

30.4.4 Transmission of data between the proximity access token and the proximity reader shall be in a secure format.

30.4.5 Access control encoding data shall not be displayed on the access card or token.

30.4.6 There shall be barriers employed to prevent the deciphering of access control data stored on the card using any readily available equipment.

30.4.7 There shall be barriers employed to prevent the copying or altering of access control data stored on the card using any readily available equipment. The Tenderer shall document the barriers used.

30.4.8 Cards and access tokens shall be able to be encoded by the supplier according to the client's specifications, made known at the time of order. Cards and tokens supplied with manufacturer determined card numbers will not be acceptable.

30.4.9 Allowance shall be made for the supply of encoding software and hardware to the Client to enable encoding of their own cards and/or tokens on site.

30.5 The system shall provide facility to encode cards or tokens in batches of user definable quantity.

31 MIFARE CLASSIC TECHNOLOGY

31.1 The cards shall incorporate Mifare Classic technology.

31.2 The card number must be a number specifically coded onto the card. It shall not be the card serial number (CSN).

31.3 The card data encoded shall use a secure sector authentication level of security to protect against card cloning. 128-bit AES encryption shall be used.

31.4 The encoded card data shall incorporate data consisting of:

(a) The assigned card number.

(b) A site-specific key consisting of 32 hexadecimal characters.

31.5 Card encoding shall be an integral part of card production.

31.6 It shall be possible to specify the card sector where the card number is stored.

31.7 The sector unlock key and the Mifare MAD unlock key shall be user definable.

31.8 Where multiple reader technologies are deployed, as defined in sections covering other technologies, single pass card encoding shall be used.

32 MIFARE PLUS TECHNOLOGY

32.1 The cards shall incorporate Mifare Plus technology.

32.2 The card number must be a number specifically coded onto the card. It shall not be the card serial number (CSN).

32.3 The card data encoded shall use a secure sector authentication level of security to protect against card cloning. 128-bit AES encryption shall be used.

32.4 The Mifare Plus 'S' variant shall be provided.

32.5 The encoded card data shall incorporate data consisting of:

(a) The assigned card number.

(b) A site-specific key consisting of 32 hexadecimal characters.

(c) The 32 hexadecimal key shall optionally be sourced from a customer specified key-safe.

32.6 Card encoding shall be an integral part of card production.

32.7 It shall be possible to specify the card sector where the card number is stored.

32.8 The sector unlock key and the Mifare MAD unlock key shall be user definable.

32.9 Where multiple reader technologies are deployed, as defined in sections covering other technologies, single pass card encoding shall be used.

33 BIOMETRIC AUTHENTICATION(REQUIRMENT)

33.1 The requirement for Biometric Authentication will be specified in accompanying documents.

33.2 The system shall be capable of providing biometric authentication via fingerprint or facial identification.

33.3 The biometric readers and associated technology shall be fully integrated into the system. All biometric enrolment and template management user interfaces shall be provided seamlessly in the standard central control system user interface.

33.4 The operator shall not have to access a separate biometric template database to manage biometric templates.

33.5 The identification time (time to identify a presented fingerprint from the database) shall be less than 2 seconds.

33.6 The reader shall have tamper protection against removal of the reader from the wall, and removal of the reader facia from the base.

33.7 Enrolment shall be carried out at a USB capable enrolment reader specifically provided for this purpose at reception.

33.8 The enrolled fingerprint templates shall conform to the following:

33.8.1 Each template shall be based on 3 separate finger presentations to obtain the best template or one facial presentation.

33.8.2 A second template associated with a second finger (in case the primary finger temporarily cannot be used for any reason) or a lright hand palm shall be automatically enrolled.

33.8.3 Optional duress finger templates or a left hand shall be able to be captured and stored in the reader.

(a) The duress fingerprint or hand shall be generated from a second ‘best of 3’ presented finger.

33.8.4 The enrolment user interface shall provide visual and audible guidance for correct fingerprint presentation during enrolment.

33.8.5 The enrolment user interface shall display a quality score associated with the fingerprint capture, and warn the operator if quality is low.

33.8.6 The enrolment user interface shall provide an indication of the enrolment quality of the presented fingerprints. The level of quality threshold for accepting presented fingerprints shall be adjustable by the operator.

33.9 When Identification Mode (1 to many, or 1:N) is specified:

33.9.1 The enrolment reader shall read the fingerprints or facial bio-image and store them as templates in a central database.

33.9.2 The fingerprint or facial templates defined above shall be a subset of the cardholder record.

33.9.3 During the template read process, the presentation of a fingerprint or facial a reader shall initiate a database inquiry at the reader. If the fingerprint or facial is determined to be valid, the associated access shall be granted.

33.10 When Verification Mode (1 to one, or 1:1is specified:

33.10.1 The enrolment reader shall read the fingerprints or facial template and store the template data onto the Mifare card if required.

33.10.2 The enrolment reader shall read the fingerprints or facial template and store them onto the Mifare card.

33.10.3 Fingerprints and or facial template shall also be stored in the Access Control central server database .

33.10.4 During the fingerprint read process, or the facial reading process the read shall be compared with the template data read from the Mifare card. If the template is determined to be valid, the associated access shall be granted.

33.10.5 An authorised system operator shall be able to generate and download a Mifare A key to all readers in the system.

33.10.6 The A key shall be either generated automatically as a random hexadecimal key or manually entered.

33.10.7 The Mifare start sector where the bio- template data is to be stored shall be user definable.

33.10.8 When the Mifare card is to be encoded, the user shall be prompted to enrol the fingerprints and or facial details and the card shall then be encoded with both the system identification data and the bio-template data.

34 CARDHOLDER MANAGEMENT

34.1 The cardholder database shall be structured so that the name field is the master field for each record. A background unique identifier may be used as the key field for each record but this must not be required by an operator to identify a cardholder. Use of the card number as the key field is not acceptable.

34.2 The system must allow at least 15 Issue Levels per card or token. This must deny access and raise an alarm to the operator when a wrong issue level is presented to a reader.

34.3 Cardholders must be able to be issued with more than one access token of different description and different number (i.e. access card, biometric identification and vehicle token) whilst maintaining only one cardholder record in the database.

34.4 Where biometric identification is required, the fingerprint data shall be a property of the cardholder record.

34.5 Encoding and printing cards shall be properties of the cardholder record.

34.5.1 The options for encoding and printing shall be:

(a) Print card

(b) Encode print

(c) Print and encode card

34.6 It shall be possible to prevent the duplication and/or re-printing of cards, by operator restriction.

34.7 Access Groups shall be linked to cardholders by both assigning access groups to cardholders or cardholders to Access Groups.

34.8 At least 64 user-definable ‘Personal Data Fields’ shall be provided which may be selectively reported on.

34.8.1 Personal Data Fields shall be able to be set up as either:

(a) Text User data may be entered.

(b) Text List User selects text from a pre-prepared list of text strings.

(c) Numeric User must enter numeric data.

(d) Date Calendar dates may be entered based on the workstation date format.

(e) Default Value The field has a default value assigned.

(f) Image The field may only contain an image to the field.

(g) Email/Mobile The field contains an email address or mobile number to be used for notifications.

34.8.2 Personal Data Fields shall also be able to be configured as:

(a)	Required field	Data must be entered.
(b)	Unique Values	Data must be unique from all other card records.
(c)	No default Value	Default value disabled.

34.8.3 Personal Data Fields shall support 'Regular Expression' rules to ensure data accuracy. Examples: @ in email addresses; employee codes are in the correct format.

34.9 A notes/memo field shall be available, associated with each card record.

34.9.1 The notes field shall support word-wrap, insert, delete, cut, copy and paste functions.

34.10 It shall be possible to group or filter cardholders for the purposes of editing access, generating reports and assigning operator privileges.

34.11 The following information fields shall optionally be displayed on the cardholder editing window:

(a) The date when a cardholder record was created.

(b) The date when the record was last modified.

34.11.2 For ease of programming, cardholders shall be grouped into Access Groups sharing the same access criteria and default Personal Data Fields.

34.11.3 It shall be possible to enter an automatic expiry date/time for the card.

34.11.4 It shall be possible to automatically expire cards that have not been used for a predetermined period of inactivity of up to 999 days.

34.11.5 It shall be possible to allocate start and end dates and times for an Access Groups access to a particular Access Zone.

34.11.6 Personal Data information.

34.11.7 Images which may include photos, signatures etc.

34.11.8 Allocated cards.

34.11.9 Cardholder Competency information relating to fields such as 'Security Clearance', 'Safety Induction' etc.

34.11.10 A URL link to additional information which may be located on the customer Intranet, or the Internet.

34.12 Access shall have start and end dates and time to within one minute.

34.13 The system shall be capable of importing database information, on selected cardholders, from other systems and be capable of exporting that cardholder's data, either with or without controlled alteration or amendment to other databases.

34.14 The system shall support the capability to allow bulk changes to card records. It shall be possible to carry out the following changes as a bulk change:

(a) Delete selected cardholder records.

(b) Change personal data fields

(c) Change card details.

(d) Change access options

(e) Change the system division the records are assigned to.

34.15 A bulk change shall be able to be saved and scheduled to run at a later time.

34.16 A window shall be provided to show details of created, saved, edited, pending, successful and failed bulk changes.

34.17 A personal user code (4 to 8 digits) shall be a property of the cardholder record to allow access via readers with a PIN pad and also to arm and disarm alarms

34.18 System operator management shall be a property of the cardholder record.

34.19 A change history record associated with each cardholder record shall list all changes made to a cardholder record, including details of who made the changes.

34.20 The system shall support an event trail for the cardholder which details recent card usage events for the cardholder as well as operator events which have modified the cardholder record.

34.21 The number of prior events to be shown or prior length of time to be covered shall be configurable.

34.22 The system shall allow different prior length of time / number of prior events to be displayed for different operators.

34.23 The cardholder record screen shall display a real time event trail of cardholder activity.

34.24 The system shall allow an operator to search for a cardholder by entering any part of their first and/or last name, in any order and separated by a space if using both. After three characters have been entered the system shall automatically return matching results and filter these dynamically as the operator continues to type.

34.25 The system shall allow the cardholder search fields and search results to be configurable. The system shall allow different operators to use and see different search fields and search results for the purpose of cardholder administration tasks.

34.26 The system shall allow the information returned for a cardholder and visible to the operator to be configurable and include any sub-section of the total information stored in the cardholder record (e.g. personal data, cards, access groups, competencies, biometric information etc). Different operators shall be able to view different sub-sections of the cardholder information.

34.27 It shall be possible to locate a cardholder record by presenting their card to a reading device connected directly to a Workstation.

34.28 The system shall allow design of different screen layouts for the purpose of cardholder administration, for use by different operators.

34.29 The system shall allow cardholder information to be viewed and updated in one screen.

34.30 Configuring operators shall, subject to the required privileges, be able to design single screen cardholder management viewers adapted for the specific screen resolution of the operator(s) who will use the viewer, to ensure best use of available screen real-estate.

34.31 The system shall provide tools to maximise, on screen, specific cardholder details when required. Maximising an area and returning to standard layout must both be single-click actions.

34.32 The system shall allow all cardholder administration functions to be managed solely via keyboard.

(a) Card numbers shall be enrolled against a cardholder by manually entering the card number or in the case of any of the Mifare technologies:

i. A reading device connected directly to a Workstation

35 VISITOR MANAGEMENT

35.1 The system shall allow visitors to self-register as defined in this section.

35.2 The Visitor Management Kiosk software (The Kiosk) shall support touch screen functionality.

35.3 Multiple visitor management (reception) workstations shall be supported.

35.4 The Kiosk shall operate on a workstation provided to the specification defined in 'System Requirements'.

35.5 A welcome (default) screen shall be customer configurable to allow branding and imagery to be displayed.

35.6 Visitors shall be able to search for themselves in the system and carry out the following functions:

(a) Add or update their details.

(b) Capture a photograph via a camera connected to the kiosk.

(c) A visitor search field, in addition to name search, shall be provided.

35.7 Attributes associated with the visitor(s) shall be configurable and set as mandatory or option fields. These shall include:

(a) The reception where the visitor(s) will be expected to arrive.

(b) The visitor category.

(c) The person the visitor(s) will be meeting.

(d) Visitor arrival time.

(e) Visitor departure time.

(f) Building access rights to be given to the visitor(s).

(g) Visitor photo-ID image

35.8 Visitor personal details shall be stored if required, to be reused for future visits.

35.9 Visit details shall be recorded in the system event database.

35.10 Visitor details for several visitors associated with a single visit shall be able to be pre-registered into the system.

35.11 The system shall raise an alarm should a visitor not sign out by the due time

35.12 If the visitor has been assigned an access token, then the visitor shall be able to present their card to identify the visitor.

35.13 The Kiosk shall support business card scanning via a Dymo Executive Business Card Scanner.

35.14 For pre-arranged visits, the visitor shall be able to pick the actual visit from a drop-down list.

35.15 The visitor shall be allowed to print a visitor label.

35.16 Visitors shall be able to advise their host that they have arrived via automatic email or SMS message.

35.17 Hosts shall be able to set the status of visitors to ensure current status of each visitor is always known. Host options shall include;

(a) Marking a visitor on or off site.

(b) Reprinting a badge for a visitor.

(c) Updating visitor details such as arrival and departure times.

(d) Assigning an access card to the visitor.

35.18 Tour groups shall be catered for.

35.19 Tour group members are not individually named, however the number of people in the group shall be recorded.

35.20 Groups of visitors shall be selectable as a group and their status processed as a single action

35.21 The Kiosk shall support visitor site induction.

35.22 The induction feature shall be customer configurable, incorporating the following features:

(a) Induction videos.

(b) Multi-choice questionnaire depending on induction level required.

(c) Multiple questionnaires.

(d) Induction hint feature to allow the visitor to request a hint for questions.

(e) Notify the host that the visitor requires induction assistance.

(f) A conditions of entry screen

(g) A Privacy Statement screen.

35.23 The Kiosk shall support a QR Code scanner.

35.23.1 Upon creating an appointment, the visitor shall be emailed a QR code which can be used to sign in.

35.23.2 The QR code shall also be used for signing out.

36 PHOTO ID BADGING AND IMAGE MANAGEMENT

36.1 The system shall provide a means to:

(a) Electronically capture images.

(b) Store the images in the server database.

(c) Integrate those images into a pre-designed ID card from within the system.

(d) Produce an integrated and completely finished identification card within the nominated time frame.

36.2 Images are defined as being one or more of the following:

(a) Photographic image of the cardholder.

(b) Signature of the cardholder and/or authorising person.

(c) A fingerprint of the Cardholder.

36.3 The system shall have an integrated method of card design within the system software without the requirement of having to use external software to create the card design.

36.4 The facility to import background images from other sources must be available. This must include scanned logos and other graphical imagery if desired.

36.5 The system offered shall capture images in 24-bit colour and at least 640 x 480 pixel resolution, using standard video capture hardware offering a TWAIN or Direct Draw standard interface, or a USB digital camera.

36.6 Images must be able to be cropped after capture to optimise the image size within the desirable image area. This size of the movable cropping box must be user-definable.

36.6.1 The controls must be easy to use from within the system software and once set, they must be capable of applying the same setting on subsequent image captures for future cardholder records.

36.7 Up to three images per cardholder must be capable of being captured and stored within the system.

36.8 The system shall store images in the JPEG compression format. User definable compression rates shall be easily selectable by the operator permitting, as a minimum; at least three levels of JPEG compression are required.

36.9 The system offered shall be capable of importing image files, for use in either card layout or cardholder images, from at least the following formats:

(a) JPEG

(b) Windows BMP

(c) LEAD Compression

36.10 The card design must be capable of incorporating, storing, printing and displaying bar-code information and must support the following bar-code formats:

(a) EAN 13 & 128

(b) UPC A & E

(c) Code 39 & 128

(d) Interleave 2 of 5

(e) Codabar

(f) Telepen

36.11 The system must have an integrated card design program. Systems offering a separate card design program where card designs must be created in alternate drawing programs and imported are not acceptable.

36.12 The card layout section of the system must be capable of user-selecting up to 16.7 million colours with a custom colour palette available.

36.13 Card design must be accomplished by the use of drag and drop options using a mouse.

36.14 Card design must support both sides of the card.

36.15 The system shall be capable of linking data relating to the cardholder and printing it the card. This data shall include (but not be limited to);

(a) First Name.

(b) Last Name.

(c) Card number (displayed as text and/or barcode).

(d) Card issue level.

(e) Expiry date.

(f) Visit start date/time.

(g) Visit end date/time.

(h) Person whom the visitor is meeting.

(i) Personal Data Fields as defined in the cardholder database.

36.16 The system must be capable of using all of the common word processing fonts and must also be capable of normal text manipulation including, text sizing, left and right justification, centring, bolding, underlining and italicising.

36.17 The variable cardholder image files that are selected to incorporate into the card design must be user-definable as to size. Full size being defined as 30mm x 40mm. The sizing must be fully user-configurable from 25% of full size up to 200% of full size, as a minimum, and must offer automatic aspect ratio adjustment throughout the size range.

36.18 The system shall be capable of producing hard copy output of images and data using any standard MS-Windows printer.

36.19 The system shall produce photo ID cards using a single step hard-card colour MS-Windows compatible printer. Systems offering multi-stage production, heat lamination or heat & pressure card production are not acceptable.

36.20 The system shall be capable of printing directly onto cards without damaging the card technology.

36.21 Cards must be capable of either landscape or portrait printing and Bar-codes must be capable of

37 SYSTEM OPERATOR MANAGEMENT

37.1 Operators shall be members of Operator Groups.

37.2 Operator establishment and maintenance shall be limited to assigned Senior Operators.

37.3 It must be easy to define operator privileges for a group of operators and it must be easy to add an operator to the group.

37.4 Operator access to the system is to be restricted by means of an operator identifier and individual password.

37.5 It shall be possible to apply password restrictions that consist of (but are not limited to) the following:

37.5.1 Minimum password length.

37.5.2 Mixed case characters.

37.5.3 Mixed alpha and numeric characters.

37.5.4 Change password after a defined period of up to at least 365 days.

37.5.5 Remembering and rejecting at least 99 previously used passwords.

37.6 The system shall also support a Mifare reading device connected to the workstation, allowing the operator to logon using their card.

37.7 The system shall support an Active Directory Single Sign-on feature

37.8 Each operator shall have the authority to alter his own password, but not that of other operators

37.9 Automatic logoff shall occur after a preset time of up to 60 minutes of operator inactivity.

37.10 It shall be possible to configure the system to only allow one logon per operator.

37.11 It must be possible to allow or deny Operators access to system menu functions, including viewing of Cardholder Personal Data fields, Personal Notes and Images.

37.12 It must be possible to restrict Operator access to Cardholders based on System Division.

37.13 It shall be possible to assign different access rights for each division an operator is required to access. For example, 'Advanced User' for Division 1; 'View only' for Division 2; 'no access' for Division 3 etc.

37.14 Any menu option not available to an Operator should be either greyed out or not visible.

37.15 It shall be possible for a suitably authorised operator to view all operators sessions on the system, and the following minimum information shall be displayed:

37.15.1 Workstation name.

37.15.2 Operators.

37.15.3 Session Type, i.e. Operator, Visitor Management, Mobile Application, OPC/XML connection etc.

37.15.4 Session status.

37.16 It shall be possible for a suitably authorised operator to terminate any operator session.

38 ELEVATOR CONTROL AND MANAGEMENT

38.1 The system shall provide fully integrated elevator control facilities. The elevator control access equipment must communicate with the same central control as the door card readers.

38.2 The elevator control architecture shall comprise a card reader in each elevator car, reporting to elevator control interface equipment mounted in or near the elevator motor room. Reader type shall be as specified for use on access control doors.

38.3 The elevator control system shall be capable of controlling access independently in a number of elevator shafts simultaneously.

38.4 The elevator control system shall incorporate dedicated intelligence and a local database of authorised cardholders.

38.5 Each elevator reader shall be identified independently at the central control by means of a unique plain language descriptor. The central control plain language descriptor shall be at least 60 characters in length.

38.6 Each reader head shall be capable of raising an alarm if it stops communicating with its elevator controller or is removed from the elevator.

38.7 The elevator control shall check entry based on ALL of the following criteria:

(a) Correct facility code.

(b) Authorised card in database.

(c) Correct issue number.

(d) Authorised level.

(e) Authorised time of day.

(f) Correct PIN (If PIN entry is required).

38.7.2 The access mode for each elevator shall be capable of automatically changing according to the programmed time schedules, as received from the central control. The following access criteria modes are required:

(a) Free access — Elevator level select button for that level is unlocked, no card entry required.

(b) Secure access — Elevator level is locked. A successful card attempt is required for valid entry. Elevator level re-secures after access attempt.

(c) Secure + PIN access — Elevator level is locked, a successful card and correct PIN number attempt is required for valid entry. Elevator level re-secures after access attempt.

(d) Dual Authorisation — Access is granted when two different but legitimate cards are presented within a given time frame.

(e)	Escort	A second card is required to be presented from nominated cardholder(s).
(f)	Shared PIN Number	The system Operator determines what the PIN number will be and programs this into the system. Access is allowed at the elevator level when the correct 4 digit PIN is pressed followed by the “Enter” key.

38.7.3 The elevator control system shall be capable of individually setting the access modes for each level as described above.

38.7.4 Levels must be securable on a level-by-level basis, using command instructions transmitted from the central control.

38.7.5 The central control must provide operator override facilities to enable temporary override capability on a level by level basis.

38.7.6 The elevator control system shall continue to operate without performance degradation in the event of a communications link failure with the central control.

38.8 Where a low level interface is specified:

38.8.1 The interface between the access system elevator control equipment and the actual elevator switching control equipment shall be via dry relay contacts.

38.8.2 The voltage from the elevator system connected to the relays shall not exceed 24 volts DC/AC

38.8.3 The elevator control system shall provide one relay contact per elevator shaft per level for the system. This relay contact shall be used to interface with the elevator switching control equipment.

38.8.4 An input shall be provided for each level per elevator to indicate what level the user selected. On activation of this input all relays return to secure state.

38.9 Where a high level interface is specified:

38.9.1 The interface between the access system elevator control equipment and the actual elevator switching control equipment shall be via RS-232 or TCP/IP connection depending in the elevator system requirements.

38.9.2 The elevator control equipment will provide feedback as to which level was selected by the cardholder.

39 ENERGISED PERIMETER INTRUDER DETECTION SYSTEM - PHYSICAL FENCE REQUIREMENTS (REQUIRED ON THE OUTERFENCE AREA & REMOTE SITES)

39.1 The physical fence part of the Energised Intruder Detection System shall be a multi-wire Energised Fence (EF) which consists of a horizontally spaced grid of conductive wires supported by a specially made carrier fence. This will comprise of insulated components exclusively used for a security fence and support posts retro-fitted to an existing high security solid and/or mesh type fence or wall.

39.2 The system shall be installed in accordance with the manufacturer's installation instructions and will comply to NKP requirements.

39.3 The operating voltage for the energised fence shall be a high voltage short duration pulse, managed and continually monitored to deter intrusion by giving any intruder a safe high voltage (HV) pulse should they touch any part of the grid of conductive wires whilst earthed or in contact with other conductive elements.

39.4 The system shall provide an optional reduced voltage operating mode (Low Feel) to provide full detection capability as per high voltage but with reduced deterrent.

39.5 All EF wires must deliver a safe deterrent pulse to an intruder touching a wire and earth, or attempting to penetrate between any adjacent wires.

39.6 The EF system shall contain intermediate insulating posts at a spacing not greater than 3m to minimise ability to spread the grid of conductive wires creating a viable opening in the EF.

39.7 Intermediate insulating components shall have a minimum electrical tracking distance of not less than 80mm

39.8 Intermediate insulating components shall have no area where the conductive wires can be trapped easily between insulator surfaces of the insulating components if the conductive wire is demounted from its nominal position on the insulating component.

39.9 Shielding of insulating components should be designed to direct the conductive wire to an earth contact to maximise alarm generation if the conductive wire is demounted from its nominal position.

39.10 The retention mechanism of the conductive wire on the insulating components shall be designed to 'break away' during climbing attempts where a load greater than 30kg is applied is a direction down and away from the physical fence structure.

39.11 All structural climb points must be fitted with extra alarm monitored and anti-climb protection against intrusion.

39.12 The system shall be attached to the inside of the existing inner ClearVu and access gates. The barrier security fence provides a physical separation barrier between the general public and the exposed pulsed HV conductors.

39.13 Unless otherwise specified, the conductive wires shall extend at least 0.6 metres above the top of the existing barrier security fence fabric or a minimum of 1.0 metre above a wall.

39.14 Each energised fence circuit on same fence control device must be capable of being operated independently.

39.15 Where two fence circuits are operating within the same detection zone, shorting of one conductive wire to earth or another conductive element (excluding second conductive wire) should not affect the performance and detection of the second conductive wire.

39.16 Each access gate or perimeter access door shall be fitted with a switching device that will detect and then annunciate the opening of the gate/door within 50mm. The switching device and/or attached controls shall ensure all high voltage pulses on or round the gate/door are effectively shorted to earth or disabled at the Fence Controller.

39.17 Opening of a perimeter access door or gate should annunciate an alarm condition on the system and inhibit the deterrent pulses on that gate.

39.18 Each active fence circuit shall be individually configurable for all functionality.

39.19 Zone configuration shall be interface to other systems such as the site CCTV systems.

39.20 Anti-climb configuration at strain points shall be provided, above the physical barrier. The fence circuit shall be routed around strain posts and connected to strainers such that it forms part of the continuous electrical circuit and does not constitute a parallel, redundant or dead-end path.

39.21 Re-tensioning of fence wires must be possible without the need to reposition anti-climb elements.

39.22 The anti-climb loops/links are to be supported at the back of the strain post with a separate short length of the security post.

39.23 All joints between conductive elements in a fence circuit shall be clamped and not rely solely on tension of the conductive wire to maintain the integrity of the electrical connection. This excludes the external pressure contact between gate switch halves.

39.24 Galvanised security posts embedded in concrete should be epoxy coated with contiguous paint film from the embedded end of the post to 100mm above the finished concrete level.

39.25 All metal components of the system must be protected against the environment through the use of aluminium alloy, or steel with zinc based galvanising.

(a) Copper based components are NOT permitted.

(b) Stainless steel should not to be mechanically or electrically coupled to aluminium or zinc galvanised components without measures to prevent galvanic corrosion.

39.26 Fine pitch tensioning capability shall be provided for ease of adjustment during installation and maintenance.

39.27 Re tensioning of fence wires must be possible without the need to reposition the configuring links.

39.28 Where springs are attached to the grid of conductive wires, an indication of the tension of the conductive wire must be clearly visible on the spring device.

39.29 Springs used in the tensioning of the conductive wire should be of a single continuous wire which forms part of the conductive circuit.

39.30 Any spring which form part of the conductive circuit should have a means of physically limited the length of extension of the spring.

39.31 Within each active fence circuit there shall be no parallel, redundant or dead-end paths.

39.32 Each conductive fence wire shall be capable of deterring and detecting potential intruders by means of a high voltage pulse and detecting the following types of attack:

(a) Cutting or disconnecting any wire.

(b) Shorting any wire to ground on the support fence.

(c) Shorting adjacent but different polarity wires.

(d) Shunting the wires with an electrically conductive material to reduce the pulse voltage.

39.33 Each active fence circuit shall be monitored at all times whilst operating in one or more of the following operating modes:

(a) High voltage with monitoring.

(b) High voltage disabled, **with monitoring only**. (on the Northern side of the fence boundary)

(c) Monitoring as defined above and the alarm triggering the high voltage operating mode for a pre-set period.

(d) Low Feel with monitoring.

(e) Low Feel disabled, with monitoring.

(f) Monitoring as defined above and the alarm triggering the Low Feel operating mode for a pre-set period.

(g) Low Feel Mode and the alarm triggering the high voltage operating mode for a pre-set period.

39.34 The system shall be configured in accordance with the specific contract drawings.

39.35 The system shall generate an alarm within 4 seconds if any one wire is cut or continuously short circuited to an adjacent wire or to earth.

39.36 The shorting together of any wires, or cutting of any wires shall have no impact on the deterrent or detection capability of the remaining active fence circuits and zones.

39.37 The shorting together of any wires, or cutting of any wires shall raise an alarm at the Security Management System Software.

39.38 The system shall detect all attempts by an intrusion pressure of more than 35kg on a single wire, to penetrate or scale the protected fence under any environmental conditions.

39.39 The system shall generate minimal nuisance alarms in any environmental conditions of wind, rain and temperature, nor from wildlife of less than 5 kg (birds, rabbits, foxes etc.)

39.40 The system shall have a False Alarm Rate (FAR) no greater than 1 false alarm per fence line kilometre per week.

39.41 All high voltage, and Low Feel, pulses shall be synchronised so that the pulses on adjacent fence sections do not occur at a time interval less than permitted in the reference standards.

39.42 When specified, local control at Field Cabinets shall be provided via Alarms Management Terminals.

39.43 Fully adjustable lightning diverter and protection devices shall be connected to each electric fence circuit connection. A separate ground or earthing system must be provided with a physical separation of 10m from any other earthing system.

39.44 Where the EF abuts to, attaches to or passes over any metallic structure, the structure must be grounded or earthed using a separate earthing system. The EF must have a physical separation of 2m from any other earthing system.

39.45 When specified, the energised fence must be capable of interfacing with an emergency shutdown system, which in the event of an incident will electronically deactivate and isolate the high voltage deterrent pulses on the conductive fence wire array.

39.46 The interface shall be a fail-safe interface, carried out at each of the Field Cabinets to minimise dependency on site communication systems.

39.47 The system manufacturer shall support the product for a minimum period of 10 years from the time at which the product is superseded.

39.48 The system must be formally inspected and assessed by a manufacturers approved representative, to the manufacturer’s published standard.

39.49 Full system documentation meeting the manufacturer’s compliance minimum quality and safety codes and instruction must be provided to the system end user representative.

39.50 Full system operation and maintenance training must be provided to the end user.

39.51 An annual preventative maintenance program must be provided to check and maintain the energised security fence system to an operational and safe condition.

40 ELECTRIFIED SECURITY FENCE CONTROLLER – STANDALONE (REMOTE SITES)

40.1 The Electric Security Fence Controller(ESFC) shall deliver an electric pulse through the fence wires to maximise the intruder deterrent and detection capabilities whilst meeting global safety standards.

40.2 The ESFC shall generate pulses at intervals of not less than 1.1 seconds.

40.3 The ESFC shall be available as a Single Fence Circuit (Single Zone) or Dual Fence Circuit (dual zone) option.

40.4 The ESFC shall be capable of delivering 2.3 Joules when configured as a 'live/earth' system, i.e. alternate wires have a voltage or are earthed.

40.5 An alternative ESFC shall be available with the following capabilities where the project requires:

40.5.1 When configured as a 'live/earth' system, the ESFC shall be capable of increasing the output from 2.3 Joules to 3.6 Joules per fence circuit. This is triggered when there is a drop in voltage from one high voltage pulse to the next, which has reached a pre-defined alarm threshold.

40.5.2 The system shall return to the standard output after 20 minutes.

40.6 The ESFC shall be capable of delivering 4.6 Joules when configured as a 'dual-pulse' system, i.e. alternate wires have positive or negative voltages.

40.7 An alternative ESFC shall be available with the following capabilities where the project requires:

40.7.1 When configured as a 'dual-pulse' system, the ESFC shall be capable of increasing the output from 4.6 Joules to 7.2 Joules. This is triggered when there is a drop in voltage from one high voltage pulse to the next, which has reached a pre-defined alarm threshold. Output is measured across alternate wires.

40.7.2 The system shall return to the standard output after 20 minutes.

40.8 The electric fence pulses shall be synchronised so that the pulses on adjacent fence sections occur within time intervals as permitted in the reference standards.

40.9 The ESFC shall operate within an ambient temperature range of -20ºC to +50ºC

40.10 The ESFC shall have temperature sensors to monitor the internal temperature of its enclosure and adjust performance as follows:

40.10.1 75 °C Over-temperature.

An indicator LED on the front panel shall flash and the ESFC shall reduce its pulse rate to reduce the internal temperature

40.10.2 85 °C Critical temperature. The ESFC must stop generating pulses and turn off.

40.11 The ESFC shall have indicator LEDs on the front panel to indicate the following:

(a) Over Temperature alarm.

(b) Service Alarm.

(c) Tamper.

(d) Mains Power Failure.

(e) Battery test failed, or battery missing.

(f) High Voltage Mode.

(g) Low voltage mode.

(h) Fence circuit pulsing with return voltage measurement in the form of a Bar-LED indicator.

(i) Synchronisation status:

i. Off

ii. Synchronisation conflict.

iii. Correct synchronisation.

40.12 The ESFC shall have a Service Mode to allow a service technician to easily isolate and locally control fence circuits.

40.13 This Service Mode shall be accessible at the ESFC by means of a special key.

40.14 The ESFC shall provide battery management as follows:

40.14.1 Trickle Charge Slow charge rate when battery is below 10 VDC.

40.14.2 Bulk charge Maximum charge rate for fast battery recovery.

40.14.3 Float Charge Slow charge rate to accommodate temperature variations.

40.14.4 Battery Save Reduce electric pulse rate to save battery power.

40.15 The ESFC shall support external power supplies such as additional backup batteries or solar cells to be connected.

40.16 The (ESF) Controller shall operate in a standalone mode such that it does not require any external system software for its configuration and control.

40.17 Configuration shall be via dip-switches inside the ESFC.

40.18 The Fence Circuits shall be armed and disarmed via input signals from an external switch, keypad or alarm panel.

40.19 The ESFC shall have output relays to indicate the following:

(a) System Alarm.

(b) Power Supply Failure.

(c) Fence Circuit #1 alarm.

(d) Armed status.

(e) Fence Circuit #2 alarm (for the Dual Fence Circuit ESFC)

40.20 The ESFC shall have the capability to be changed from a standalone unit to a networked unit which is connected to a Security Management System via a dip-switch, without the need to change any firmware within the ESFC.

41 ENERGISED SECURITY FENCE CONTROLLER - NETWORKED

41.1 The Energised Security Fence Controller(ESFC) shall deliver an electric pulse through the fence wires to maximise the intruder deterrent and detection capabilities whilst meeting global and SANS safety standards.

41.2 The ESFC shall operate in a networked environment and be controlled and monitored by the Security Management System software

41.3 The ESFC shall generate pulses at intervals of not less than 1.1 seconds.

41.4 The ESFC shall be available as a Single Fence Circuit (Single Zone) or Dual Fence Circuit (dual zone) option.The Dual Circuit system must be installed around the Sentech main site area with the maximum allowed energy to comply to SANS 102222-3:2016 specification

41.5 The ESFC shall be capable of delivering 2.3 Joules when configured as a 'live/earth' system, i.e. alternate wires have a voltage or are earthed.

41.6 An alternative ESFC shall be available with the following capabilities where the project requires:

41.6.1 When configured as a 'live/earth' system, the ESFC shall be capable of increasing the output from 2.3 Joules to 3.6 Joules per fence circuit. This is triggered when there is a drop in voltage from one high voltage pulse to the next, which has reached a pre-defined alarm threshold.

41.6.2 The system shall return to the standard output after 20 minutes.

41.7 The ESFC shall be capable of delivering **4.6 Joules** when configured as a 'dual-pulse' system, i.e. alternate wires have positive or negative voltages.

41.8 An alternative ESFC shall be available with the following capabilities where the project requires:

41.8.1 When configured as a 'dual-pulse' system, the ESFC shall be capable of increasing the output from 4.6 Joules to 7.2 Joules. This is triggered when there is a drop in voltage from one high voltage pulse to the next, which has reached a pre-defined alarm threshold. Output is measured across alternate wires.

41.8.2 The system shall return to the standard output after 20 minutes.

41.9 The electric fence pulses shall be synchronised so that the pulses on adjacent fence sections occur within time intervals as permitted in the reference standards.

41.10 The ESFC shall operate within an ambient temperature range of -20ºC to +50ºC

41.11 The ESFC shall have temperature sensors to monitor the internal temperature of its enclosure and adjust performance as follows:

41.11.1 60 ºC Temperature warning.

It shall be possible to activate a relay to turn on an external cooling fan.

41.11.2 75 °C Over-temperature.

An indicator LED on the front panel shall flash and the ESFC shall reduce its pulse rate to reduce the internal temperature

41.11.3 85 °C Critical temperature.

The ESFC must stop generating pulses and turn off.

41.12 The ESFC shall have indicator LEDs on the front panel to indicate the following:

(a) Over Temperature alarm.

(b) Service Alarm.

(c) Tamper.

(d) Mains Power Failure.

(e) Battery test failed or battery missing.

(f) High Voltage Mode.

(g) Low voltage mode.

(h) Fence circuit pulsing with return voltage measurement in the form of a Bar-LED indicator.

(i) Synchronisation status:

i. Off

ii. Synchronisation conflict.

iii. Correct synchronisation.

41.13 The ESFC shall have Service Mode to allow a service technician to isolate and locally control fence circuits.

41.13.1 An event shall be send to the system when the ESFC is in Service Mode.

41.13.2 The Service Mode shall be capable of being enabled from The System.

41.13.3 This Service Mode shall be accessible at the ESFC by means of a special key.

41.14 The ESFC shall provide battery management as follows:

41.14.1	Trickle Charge	Slow charge rate when battery is below 10 VDC.
41.14.2	Bulk charge	Maximum charge rate for fast battery recovery.
41.14.3	Float Charge	Slow charge rate to accommodate temperature variations.
41.14.4	Battery Save	Reduce electric pulse rate to save battery power.

41.15 The ESFC shall support external power supplies such as additional backup batteries or solar cells to be connected.

41.16 The ESFC shall support self-discovery on The System.

41.16.1 ESFC shall contain a unique serial number.

41.16.2 When connected to an Intelligent Field Controller (FC), the serial number of the ESFC shall be reported to The System.

41.16.3 Once assigned to a function within an FC, if any attempt is made to substitute ESFCs in the field without authorisation, an alarm shall be generated.

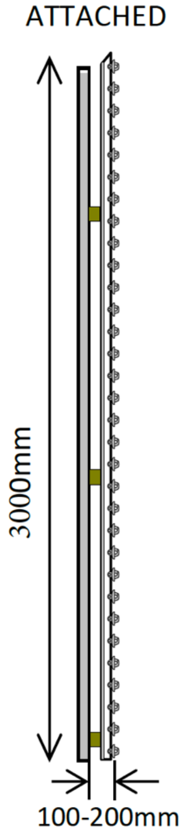
41.17 Data communication rate between FCs and the ESFC shall be at least 1Mbit/second.

41.18 Communication sessions between FCs and ESFC s shall use certificate exchange protocols using keys with a minimum strength of 256 bit elliptical encryption.

41.19 Data communication between FCs and ESFCs shall use a minimum of 128 bit AES encryption.

41.20 ESFCs shall generate a heartbeat signal to enable the FC to identify lost communications and thereby generate an alarm.

41.21 **Esfcs shall be upgradeable via software downloaded from the system without any**



Electrified fence to be installed on the inside of the existing ClearVu fence

42 INTRUDER ALARM SYSTEM

42.1 The system will incorporate a fully functional intruder alarm system.

42.2 All Inputs globally within the system must be able to be utilised as intrusion alarm inputs to allow intruder detection sensors to be connected to the system.

42.3 All outputs anywhere within the system shall be available for intruder alarm purposes such as sounding remote sirens, Smoke bombs, Pepper Spray etc.

42.4 Arming and disarming the intrusion detection system shall be either by using card readers, alarm management terminals, key-switches ,schedules or by Remote Control room.

42.5 It shall be possible for the system to cause readers to beep during entry and exit delays.

42.6 It shall be possible for the system to active outputs during entry and exit delays.

42.7 It shall be possible to configure the system to isolate faulty external devices so as not to trigger false alarms.

42.8 It shall be possible to configure the system to fail to arm if an input point is active.

42.9 It shall be possible to configure the system to fail to arm if an input point has unacknowledged alarms.

42.10 It shall be possible for the system to cause readers to beep when alarms are present in the system.

42.11 It shall be possible to set the system to a ‘Test Mode’ to allow for testing and maintenance.

42.12 The intruder alarm zone and the access zone for an area shall be treated as separate conditions.

42.13 The intruder alarm system shall provide a dependency feature where by an alarm zone does not go into the set state until the ‘dependent’ alarm zones are all in the set state.

42.13.1 If the alarm zone is set (armed) and the access door is secure:

(a) A cardholder shall require authorisation to both unset (disarm) the intruder alarm zone and to access the access zone, to be allowed access.

(b) If the card is not authorised to unset the alarm zone or not allowed to access the access zone, then access shall be denied.

42.13.2 If the alarm zone is unset (disarmed) and the access door is secure:

(a) A cardholder shall require access to the access zone only for access to be allowed.

(b) If the card is not authorised to access the access zone, then access shall be denied.

42.13.3 For normal operation, after an authorised token is presented, and access is granted, then the alarm zone shall remain unset after the door relocks.

42.13.4 As an optional function, the alarm zone must auto-set after a predetermined time period.

42.14 When specified, alarm monitoring shall use a connection with Central Alarm Monitoring stations via digital communicators using Contact ID format, connected directly to the Intelligent Field Controller (FC) panels.

42.15 Connection with Central Alarm Monitoring stations shall be via TCP/IP or cellular GPRS networks.

42.15.1 It shall be possible for alarms from one FC to be managed on a second FC where the digital communicator is installed. (Peer-to-Peer communications).

42.15.2 Digital communicators are to be able to communicate alarms from the complete system, independent of system server.

42.15.3 The system shall report and log all Digital Communicator activity and the reason for any failure to communicate.

42.15.4 The system shall provide for up to two back up diallers on different controllers to provide automatic backup capability should the designated digital communicator fail to operate on the appropriate alarm condition.

42.16 Cardholders shall be assigned to groups, to which any combination of the following intruder alarm privileges relating to the operation of the system may be assigned:

(a) Unset intruder alarm zones.

(b) Set Intruder alarms zones.

(c) Status of alarms and inputs on Alarms Management Terminals.

(d) Acknowledge Alarms.

(e) Shunt Inputs.

(f) Force-arm alarm zones.

43 ALARMS MANAGEMENT

43.1 The Security Management System (The System) shall provide entry and exit delays for the setting (arming) and unsetting (disarming) of alarms.

43.2 The entry delay shall be configurable from 0 to 999 seconds in increments of one second.

43.3 An optional audible warning must sound during the entry delay (from the time the alarm occurs to the time that the Zone state is changed). It must be possible to designate specific card readers and Alarm Management Terminals (AMTs) to sound entry delay warning beeps. Selected output relays should also be able to be operated during the entry delay period allowing suitable sounders to be connected at required locations.

43.4 The exit delay shall be configurable from 0 to 999 seconds in increments of one second.

43.5 An optional audible warning must sound during the exit delay (from the time that the alarm occurs to the time that the zone state is changed). It must be possible to designate specific card readers and AMTs to sound exit delay-warning beeps. Selected output relays should also be able to be operated during the exit delay period allowing suitable sounders to be connected at required locations. This applies to both manually and automatically changing the state of a zone in the case of automatically changing the state of a zone the exit delay and audible warning gives people working late in the building time to unset the alarms or leave the building.

43.6 The system shall include Alarm Escalation as an event. The new event shall correspond to the original alarm, but may have a different (usually higher) priority, and may require a different set of alarm relays to operate.

43.7 Escalated alarms shall be able to be displayed in a window specifically provided for this purpose.

43.8 Alarms shall be able to be escalated under the following conditions:

(a) Escalate if alarm not acknowledged for a period of time. This must be configurable from 0 to 9999 seconds in increments of one second.

(b) Escalate if the alarm remains in an active state for a period of time. This must be configurable from 0 to 999 seconds in increments of one second.

(c) Escalate if zone contains a user-defined number of alarms. This must be configurable from 0 to 99.

(d) Escalate if there are two events from same point within a user-defined period. This must be configurable from 0 to 99.

(e) Escalate if there are two events from different points in same zone within a user-definable period of time. This must be configurable from 0 to 999 seconds in increments of one second.

43.9 It shall be possible to have automatic time based setting and unsetting of alarms.

43.10 It shall be possible to configure the system such that events (such as a card badge or operation of a key switch connected to an input) can change the state of a zone.

43.11 Authorised cardholders shall be allowed to set and unset alarm zones by:

(a) Operation of the Card plus PIN reader as an alarm panel.

(b) Presenting a valid access card to a card reader associated with the alarm zone, twice within a nominated time period (double card badging).

43.12 It shall be possible to set and unset multiple alarm zones from an AMT.

43.13 All alarm occurrences shall be presented at The System within 5 seconds of their occurrence at the remote field device.

43.14 All Alarm events shall be viewable from an Alarm Stack.

43.15 It shall be possible to view all alarm events by clicking on interactive Site Plan icons that, because of their changing audible and visual states, indicate the presence of alarms.

43.16 All alarm events arriving at the central control shall be time-stamped with the time they occurred and the time they were logged at The System.

43.17 All alarm events shall have a user-definable alarm priority assigned. A minimum of 8 alarm priority levels plus non-alarm event and ignored shall be provided.

43.18 It shall be possible to assign a different audio warning sound to each alarm priority.

43.19 Incoming Alarms shall be presented in the Alarm stack according to their assigned priority with the highest level at the top. Alarms with the same priority shall be presented in time order.

43.20 The priority of Alarms in the alarm stack shall be identifiable by a user definable colour.

43.21 Identical consecutive alarms that occur within a predefined time span shall be report as a single alarm with the number of occurrences reporting as a flood alarm quantity.

43.22 The System must be able to control the actual priority assigned to any alarm activation throughout the day. This means any alarm activation may be programmed as ‘Low Priority’ during office hours and ‘High priority’ at all other times.

43.23 It shall be possible to nominate an Input (e.g. Smoke, Fire or Gas detection) as an ‘Evacuation Input’ in which case certain doors within the Site will revert immediately to Free Access.

43.24 Operators shall be required to complete two-stage alarm processing as:

43.24.1 Acknowledge Alarm.

(a) An Acknowledged alarm shall remain in the alarm stack and be easily identified as having been acknowledged but not yet processed.

(b) The central control shall record in the hard disk activity log that the operator has acknowledged the alarm. An alarm is ‘acknowledged’ by the operator selecting the ‘Acknowledge’ button in the alarm-viewing window.

(c) A second alarm from the same source as the acknowledged alarm shall be indicated as a new alarm.

43.24.2 Process Alarm.

(a) A Processed alarm shall clear from the Alarm Stack.

(b) The central control shall record in the hard disk activity log that the operator has processed the alarm. An alarm is processed by the operator selecting the ‘Process’ button which is displayed in the alarm viewing window.

43.25 The system shall allow an operator to multi-select contiguous or non-contiguous alarms in the list in order to add a note, acknowledge or process all selected alarms in one action.

43.26 The alarm list shall support mandatory fields of alarm time, alarm priority and alarm state.

43.27 The System shall allow a suitably privileged operator to configure any of the following additional fields to be visible in the alarm list and to configure their order:

(a) Full alarm message.

(b) Related cardholder name.

(c) Acknowledging operator name

(d) Alarm Zone.

(e) Alarm source.

(f) Related access zone.

(g) Event type.

(h) Event group.

(i) Division of the alarm source.

(j) Count (occurrences of alarm).

43.28 It must be possible for an operator to sort the alarm list by any of the available fields.

43.29 The system shall display a summary of alarms, by priority, which is visible to the monitoring operator at all times and updated dynamically as new alarms occur or existing alarms are actioned.

43.30 The alarm summary shall indicate if there are any unacknowledged alarms for a given priority.

43.31 The system shall allow configuration of filtered alarm lists. Alarm lists shall be filterable based on any combination of selected divisions, escalation status or alarm priority.

43.32 The system shall allow different information to be configured and displayed to a monitoring operator based on the type of alarm.

43.33 Door Open Too Long alarms must display selected and configurable information. Including, as an example, the photo and contact details for the person who left the door open, i.e. last successful access.

43.34 Cardholder related alarms shall automatically display recent events and selected information (name, photo, personal details etc) for the person causing the alarm.

43.35 An active alarm shall not be able to be finally processed and cleared from the Alarm Window until the cause of the alarm has been removed and the alarm condition has returned to the normal state.

43.36 Pre-programmed alarm instructions shall be available for the operator to provide instructions for acknowledging and processing each alarm.

43.36.1 Alarm Instructions shall have the following features:

(a) Default Alarm Instructions shall be able to be programmed and automatically applied to all events of a common type e.g. all wrong PIN events applicable to all readers.

(b) Individual Alarm Instructions shall be able to be programmed and applied to individual alarm events.

(c) A table of contact names, phone numbers or other frequently used volatile information shall be available when programming Alarm Instructions, and applied to Alarm Instructions from a pick list.

(d) When items in the pick-list are updated, the linked Alarm Instructions shall automatically update.

43.36.2 The Alarm Instruction text shall be able to be formatted using common text formatting features including but not limited to:

(a) Bold, italic and underline.

(b) Text colours.

(c) Left, centre and right justified..

(d) Bulleted text.

(e) Standard Microsoft Windows font types and sizes.

43.36.3 It shall be possible to copy and paste Alarm Instructions between alarm events.

43.37 The Alarm window shall allow the operator to enter a comment. Such comment will be date/time stamped by the system, and recorded against that alarm event in the audit trail.

43.37.1 When required, a pre-defined list of alarm responses shall be available for operators to select the appropriate response to an alarm. The alarm responses shall be user configurable to suit site requirements.

43.37.2 Keyboard function keys (F1 to F8) shall be mapped to the first 8 alarm response messages to automatically insert the associated message as required.

44 ENCRYPTED END OF LINE DEVICES

44.1 Encrypted end of line devices (ELD) shall be available to provide secure monitoring of alarms inputs such as Passive Infrared Sensors (PIRs), contacts etc.

44.2 The purpose of the ELD is to overcome the security weakness created by non-authenticated sensor inputs using a balanced resistor network.

44.3 The ELD shall conform to the AS/NZS 2201 Class 5 Intruder Alarm Standard.

44.4 The ELD shall be small enough to fit inside the housing of a PIR.

44.5 The alarm device (PIR, contact input etc) shall connect to the ELD which in turn will communicate with the FC via encrypted communications.

44.6 The ELD shall support the following I/O to the alarm device:

44.6.1 Alarm input.

44.6.2 Tamper input.

44.6.3 Anti-masking input (PIRs).

44.6.4 Walk test output (PIRs).

44.7 Events relating to the above mentioned items shall be visible at the security management system.

44.8 The ELD shall be encapsulated in a protective resin and plastic casing.

44.9 The ELD shall support self-discovery on the system.

44.10 The ELD shall contain a unique serial number.

44.11 When connected to an FC, the serial number of the ELD shall be reported to the system.

44.12 Once assigned to a function within an FC, if any attempt is made to substitute ELDs in the field without authorisation, an alarm shall be generated.

44.13 The ELD shall generate a heartbeat signal to enable the FC to identify lost communications and thereby generate an alarm.

44.14 The ELD shall be upgradeable via software downloaded from the system without any intervention at the ELD.

44.15 Each ELD shall be identified independently on the system by means of a unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

44.16 Communication sessions between FCs and ELDs shall use certificate exchange protocols using keys with a minimum strength of 256 bit elliptical encryption.

44.17 Data communication between FCs and ELDs shall use a minimum of 128 bit AES encryption.

44.18 It shall be possible to connect up to thirty (30) ELDs to an FC.

44.19 The ELD shall support a daisy chain wiring configuration to the FC.

44.20 The ELD shall operate between -10ºC to +70ºC

45 ALARMS MANAGEMENT TERMINAL – ACCESS CONTROL

45.1 Alarms Management Terminals (AMTs) shall be provided to allow keypad functionality as described in this section.

45.2 The AMTs shall support self-discovery on the Security Management System (The System).

45.2.1 AMTs shall contain a unique serial number.

45.2.2 When connected to an Intelligent Field Controller (FC), the serial number of the AMT shall be reported to The System.

45.2.3 Once assigned to a function within an FC, if any attempt is made to substitute AMTs in the field without authorisation, an alarm shall be generated.

45.3 Data communication rate between FCs and AMTs shall be at least 1Mbit/second.

45.4 Communication sessions between FCs and AMTs shall use certificate exchange protocols using keys with a minimum strength of 256 bit elliptical encryption.

45.5 Data communication between FCs and AMTs shall use a minimum of 128 bit AES encryption.

45.6 AMTs shall generate a heartbeat signal to enable the FC to identify lost communications and thereby generate an alarm.

45.7 AMTs shall be upgradeable via software downloaded from The System without any intervention at the AMT.

45.8 Each AMT shall be identified independently on The System by means of a unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

45.9 Tamper protection shall be provided against the unit being removed from the mounting surface.

45.10 AMTs must comply with a minimum of IP66 environmental protection rating.

45.11 AMTs must comply with an impact rating of at least IK09

45.12 The must be RoHS compliant

45.13 The AMT shall operate with a temperature range of -30ºc to +70ºc.

45.14 The AMT shall include:

45.14.1 A minimum of a 3.5” LED colour display.

45.14.2 Backlit keys.

45.14.3 Support for multiple languages which shall be selectable from The System software.

45.14.4 The AMT shall display information to the user using a combination of text and graphics.

45.14.5 The AMT shall display the date and time.

45.14.6 Menus shall be accessible by logging on with a PIN number between 4 and 8 digits.

45.14.7 The AMT shall be capable of (but not limited to) carrying out the following functions:

(a) Arm alarm zones. A minimum of 50 per AMT must be supported.

(b) Disarm alarm zones. A minimum of 50 per AMT must be supported.

(c) View Alarms. A minimum of 100 per AMT must be supported.

(d) Acknowledge alarms. A minimum of 100 per AMT must be supported.

(e) View alarm history. A minimum of 100 per AMT must be supported.

(f) Turn outputs on and off. A minimum of 50 per AMT must be supported.

(g) View the status of inputs. A minimum of 100 per AMT must be supported.

(h) Isolate inputs. A minimum of 100 per AMT must be supported.

45.14.8 User definable custom images shall be displayed on the screen when the AMT is idle.

45.14.9 The AMT shall support the following image formats;

(a) .PNG

(b) .JPG

(c) .JPEG

45.14.10 It shall be possible to adjust the AMT beeper via The System software to the following volume levels;

(a) Off

(b) Quiet

(c) Normal

(d) Loud

45.14.11 The AMT shall have the ability to display the status of alarms and system I/O via LEDs on front panel.

(a) The AMT shall support at least 8 LEDs.

45.15 Multiple AMTs can be used anywhere in the system to remotely manage assigned Intruder alarm zones.

46 ALARMS MANAGEMENT TERMINAL – PERIMETER

46.1 Alarms Management Terminals (AMTs) shall be provided to allow keypad functionality as described in this section.

46.2 The AMTs shall support self-discovery on the Security Management System (The System).

46.2.1 AMTs shall contain a unique serial number.

46.2.2 When connected to an Intelligent Field Controller (FC), the serial number of the AMT shall be reported to The System.

46.2.3 Once assigned to a function within an FC, if any attempt is made to substitute AMTs in the field without authorisation, an alarm shall be generated.

46.3 Data communication rate between FCs and AMTs shall be at least 1Mbit/second.

46.4 Communication sessions between FCs and AMTs shall use certificate exchange protocols using keys with a minimum strength of 256 bit elliptical encryption.

46.5 Data communication between FCs and AMTs shall use a minimum of 128 bit AES encryption.

46.6 AMTs shall generate a heartbeat signal to enable the FC to identify lost communications and thereby generate an alarm.

46.7 AMTs shall be upgradeable via software downloaded from The System without any intervention at the AMT.

46.8 Each AMT shall be identified independently on The System by means of a unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

46.9 Tamper protection shall be provided against the unit being removed from the mounting surface.

46.10 AMTs must comply with a minimum of IP66 environmental protection rating.

46.11 AMTs must comply with an impact rating of at least IK09

46.12 The must be RoHS compliant

46.13 The AMT shall operate with a temperature range of -30^{o}c to +70^{o}c.

46.14 The AMT shall include:

46.14.1 A minimum of a 3.5” LED colour display.

46.14.2 Backlit keys.

46.14.3 Support for multiple languages which shall be selectable from The System software.

46.14.4 The AMT shall display information to the user using a combination of text and graphics.

46.14.5 The AMT shall display the date and time.

46.14.6 Menus shall be accessible by logging on with a PIN number between 4 and 8 digits.

46.14.7 User definable custom images shall be displayed on the screen when the AMT is idle.

46.14.8 The AMT shall support the following image formats;

(a) .PNG

(b) .JPG

(c) .JPEG

46.14.9 It shall be possible to adjust the AMT beeper via The System software to the following volume levels;

(a) Off

(b) Quiet

(c) Normal

(d) Loud

46.14.10 The AMT shall have the ability to display the status of alarms and system I/O via LEDs on front panel.

(a) The AMT shall support at least 8 LEDs.

46.15 Multiple AMTs can be used anywhere in the system to remotely manage assigned Intruder alarm zones.

46.16 The AMT shall be capable of (but not limited to) carrying out the following perimeter security, electric fence system functions:

46.16.1 Override fence zones as follows:

(a) Arm

(b) Disarm

(c) Isolated (lock out zone(s) for maintenance)

46.16.2 Display Fence Zone status (‘Armed’, ‘Disarmed’, ‘Alarms in System’) on the front panel LEDs.

46.16.3 Display the Fence Zone status details such as High Voltage, Low Voltage and Isolated.

46.16.4 Display current fence return voltages.

46.16.5 Display fence return voltage range for the past 7 days.

46.16.6 Display backup battery status and voltage.

46.16.7 Display current ambient temperature of the Electric Fence Controller.

46.16.8 Display the temperature range for the past 7 days.

46.17 The AMT shall be capable of (but not limited to) carrying out the following Alarm and System Management functions:

(a) Arm alarm zones. A minimum of 50 per AMT must be supported.

(b) Disarm alarm zones. A minimum of 50 per AMT must be supported.

(c) View Alarms. A minimum of 100 per AMT must be supported.

(d) Acknowledge alarms. A minimum of 100 per AMT must be supported.

(e) View alarm history. A minimum of 100 per AMT must be supported.

(f) Change the door to Free Access mode.

(g) Change the door to Secure Access mode.

(h) Change the door to operate from a user defined schedule.

(i) Turn outputs on and off. A minimum of 50 per AMT must be supported.

(j) View the status of inputs. A minimum of 100 per AMT must be supported.

(k) Isolate inputs. A minimum of 100 per AMT must be supported.

47 NOTIFICATIONS

47.1 Specific event and alarm messages shall be able to be configured to be sent to nominated users via either email or SMS message.

47.2 It shall be possible for persons receiving alarm messages to be able to acknowledge the alarms via email or SMS message.

47.3 It shall be possible to send notification of imminent card or competency expiry to an individual, their manager or other nominated person.

47.4 When emailing cardholder details, it shall be possible to send an image of the cardholder from their personal data record.

47.5 A comprehensive filtering feature shall be provided to manage notification information transmission.

47.6 It shall be possible to schedule the notifications.

48 BREAKAUDIT TRAIL

48.1 The Server hard disk shall be used to record all system activity for archiving purposes. It shall not be possible to alter archived data.

48.2 Every system activity event along with all details, including but not limited to the following list, shall be time stamped with the time of occurrence at the Intelligent Field Controller (FC) and also the time the event was received by The Server, to the nearest second, and shall be recorded in the system activity log for archiving.

(a) All access attempts (allowed and disallowed).

(b) Alarm events.

(c) System events.

(d) Operator activity.

48.3 The central control shall provide an on-line facility to archive system data and event records to an archive file to free hard disk space for further activity logging.

48.4 It shall be possible to archive the data to a network device by specifying the UNC path.

48.5 The archive process shall be initiated by either manual operation or automatically by time.

48.6 It shall be possible to nominate the number of days of data that shall remain on the server subsequent to an archive process.

48.7 It shall be possible for an operator to view filtered event trails, e.g. for filtered for selected site items.

49 REPORTS

49.1 The Report Manager shall allow the Operator to select from a number of pre-defined Reports. Custom Reports can be created outside the software, and added to a Custom folder, making the Custom Reports available from within the Report Manager application.

49.2 Once a Report is selected, the default Criteria and Sorting options may be used, or custom Criteria and Sorting options may be selected.

49.2.1 Once the report is run, it may be viewed, printed, or saved in various standard file formats.

49.2.2 Standard Reports included as standard shall include:

- Customization Reports
- Component Resources;
- Customizations Report.
- Access Controller Configuration
- Controllers;
- Doors;
- Expansion Inputs;
- Expansion Relays;
- Inputs;
- Network Layout;
- Printers;
- Readers;
- Relays.
- History Logs
- Active Alarms by Date;
- Alarm Log by Date;
- Alarm Log by Date with Comments;
- All Events Log;
- External Events Log;
- Internal Events Log;
- Operator Log;
- User Activity Log.
- Person Information
- Template Status;
- Door Access by Person;
- Dossier Style by Person;
- Expired and To-Be-Expired Person Access;
- Expired Templates;
- Last Access by Person;
- Person Access by Door;
- Person Access Summary;
- Person Access Summary with Codes and Cards;
- Who Is Inside Where.

- System activity data
- Cardholder access data
- Cardholder Personal Data fields
- Cardholder Access Groups
- Site configuration and setup data.

- Electrified Perimeter Fence voltage
- Electrified Perimeter Fence Controller temperature

49.3 The report generation feature shall be easy to use and based on a 'checkbox' style of parameter selection and preparation. The report preparation process shall provide features to simplify report generation by incorporating selections such as report for 'yesterday', 'last week', 'last month' etc. This is for the purpose of quickly generating recurring, standard format, reports.

49.4 Report cover page, headers and footers, shall be configurable for individual needs.

49.5 It shall be possible to re-order columns.

49.6 It shall be possible to resize report columns.

49.7 The parameters for producing the report must be fully user definable and must be capable of searching on any cardholder or access event criteria.

49.8 It shall be possible to automatically produce the reports listed in this clause. The methods available to generate the report(s) are defined in previously.

(a)	Activity	Any site activity.
(b)	Evacuation	Last known location of all cardholders on site. With cardholder count summary.
(c)	Exception	Unprocessed alarms, un-acknowledged alarms and doors temporarily overridden from secure to free.
(d)	Cardholder	Details pertaining to cardholders, including images
(e)	Time Reports	Time and attendance based reports

49.9 Reports shall be saved for future use.

49.10 There shall be no limit imposed on the number of reports that can be saved.

49.11 It shall be possible to copy a report to be used as a template for another report.

49.12 The report shall be generated by any of the following means, as may be required by the operator:

(a) Manually

(b) Operator running a macro.

(c) An alarm event trigger.

(d) On a recurring schedule.

(e) Context sensitive, where a report option is associated with a system item, allowing a report to be generated based on the system item.

49.13 The System shall generate and format reports in the background. This means the operator must be able to process alarms, alter database parameters and perform other system changes while the report is being generated. Report generation must continue if the operator decides to perform any other task.

49.14 The System shall have a screen preview function, so that reports can be previewed during report preparation, on-screen before they are printed.

49.15 The Report Generator shall be capable of exporting reports In the following format::

(a) Adobe PDF (.PDF)

(b) Microsoft Word (.DOCX)

(c) Microsoft XPS (.XPS)

(d) Microsoft Excel (.XLSX)

(e) Selected page as Image file (.JPEG)

(f) CSV file with headers (.CSV)

(g) CSV file without header (.CSV)

49.16 It shall be possible to email reports to nominated people or groups of people using the above format.

49.17 The email capability shall be available from within The System itself. Applications that require reports to be generated, saved to a file and then emailed using an external email application will not be acceptable.

49.18 The Report Generator shall be capable of supporting wildcard searching when filtering data for reports.

49.19 It shall be possible for operators to change report parameters when generating reports.

49.20 Reports shall be able to be printed at any network-supported printers connected to the system.

49.21 The System shall be able to produce voltage reports for electrified fencing perimeter security voltage monitoring.

49.21.1 The electrified fencing perimeter security voltage reports shall be displayed in graphical form showing the fence zone voltage along with the date and time.

49.22 The System shall be able to produce temperature reports for the electrified perimeter fence controller.

49.22.1 The electrified fencing perimeter controller temperature voltage reports shall be displayed in graphical form showing the fence controller temperature along with the date and time

49.23 Operator privileges shall differentiate between:

(a) Report preparation and configuration; and

(b) Report generation only (not allowed to change the configuration).

49.24 It shall be possible to generate reports with graphical representations of data for trend analysis in the following formats:

(a) Bar graph

(b) Pie graphs

(c) Line Graphs

49.24.2 Summary report data shall be available in a table format.

50 COMMUNICATIONS & DIAGNOSTICS

50.1 The Security Management System (The System) shall automatically restart full and complete processing after a power failure.

50.2 The System shall provide a full diagnostic performance log to enable system engineers to monitor system performance in the event of a system malfunction.

50.3 The diagnostic performance log shall be stored in a separate file on hard disk from all other data files.

50.4 The diagnostic performance must be available without shutting down or ‘freezing the system’.

50.5 The central control shall provide on-line system diagnostic facilities which enable authorised operators or systems engineers to monitor and then tune the system performance (communications network performance tuning, for example).

51 MAGNETIC DOOR LOCKS

51.1 The doors controlled by the access control system shall be fitted with magnetic locks. The magnetic locks shall be of the type with a floating strike plate with a minimum pressure rating of 300kg for standard doors and 500kg for large and heavy doors like fire doors Locks shall contain circuitry for status indication.

51.2 The locks shall (door opened or closed) be continuously monitored regarding its status from the voltage across the lock. The status shall be indicated by means of a potential free change over contact to the access control system. A door kept open too long (time adjustable between 3 and 20 seconds on the "system analyst level") shall raise an intrusion alarm on the system as well as raising a audible alarm at the relevant door.

51.3 The magnetic locks shall be able to withstand more pressure than the pressure resulting in breaking the door. This includes for lock and striker plate mountings.

52 FIRE ESCAPE DOORS

The fire escape doors on each floor shall be monitored for open status (door opened) by means of recessed door monitors. The status shall be indicated by means of a potential free change over contact to the access control system. Once a door is opened a local siren will sound until door is closed. An alarm will be activated in the central control room.

Each fire escape door shall also be provided with the following equipment:

- Magnetic door lock
- Break glass unit (green)
- Door monitor

The activation of the break glass will immediately release the magnetic door lock and raise an alarm.

Both the door monitor and break glass alarms shall be relayed to the door monitor system.

The audible alarms shall be mounted flush with the ceiling on the secure side of the doors.

Emergency Release BGU's(Green unit)

53 ACCESS CONTROL DOORS

A green break glass unit shall be installed on the secure side at each access controlled door wired to directly release the door magnet and raise an alarm when the glass is broken.

53.1 POWER SUPPLY UNITS

Power supply units for the doors/door controllers shall be provided for the operation of the magnetic locks and door / biometric reader controllers and all ancillary devices and shall be equipped with an 8 hour back up battery. The unit shall be mounted in the ceiling voids above the doors. The low voltage power supply to the locking mechanism shall run in the doorframe or wall and shall not be visible. All wiring shall be on the secure side of the doors.

53.2 MICRO SWITCHES

Micro switches for door alarms shall be provided and shall be of the recessed type with N/O and N/C contacts. All wiring shall be concealed and be on the secure side of the doors.

53.3 DOOR CLOSERS & PUSH TO EXIT

53.3.1 All doors with automatic access control and monitoring shall be fitted with door closers. This is mechanical door closers to ensure that the door will not stay open.

53.3.2 The Electronic or Hydraulic automatic door closers will be installed where required and integrated with the Fire System in accordance with SANS 10400 and SANS 10139.

53.3.3 Infrared Sensor Switch No Touch Contactless Door Release Exit Button with LED Indication

- **Features :**

Featured with infrared technology, touch free.
Contactless, free from contagious disease spread.
The switch must responds agilely and quickly within one second.
IP-55 industrial protection level.
Stainless steel plate, very durable to use.
Suitable for doors, gates, or other exit automation control systems.
LED indication.

- **Specification :**

Material: stainless steel
Contact rating: 3A, AC 120V / DC 30V
Input voltage: DC 12V
Working temperature: -20 to 50 Celsius degree (-4 to 122 Fahrenheit degree)
Response range: within 10cm
LED indication: sensor standby: blue LED on, visitors approaching: red LED on

54 BIOMETRIC READERS

No capacitive type fingerprint readers will be installed. The fingerprint reader shall operate on an optical fingerprint capturing system.

54.1 Biometric Reader Type 1 – Fingerprint – PC Access Control and Take-Ons

This biometric (fingerprint) reader shall be used to authenticate users on PC's with highly sensitive information.

54.2 Biometric Reader Type 2 – Fingerprint without A Keypad & LCD : Indoor

This biometric (fingerprint) reader shall be used to authenticate users entering or leaving an area with highly sensitive information. The biometric reader shall be equipped with an alpha-numeric keypad for entering a “PIN” code as well as a LCD display for displaying user relevant information.

54.3 Biometric Reader Type 3 – Fingerprint with Keypad & LCD : Indoor

This biometric (fingerprint) reader shall be used to authenticate users entering or leaving an area with highly sensitive information. The biometric reader shall be equipped with a alpha-numeric keypad for entering a “PIN” code as well as a LCD display for displaying user relevant information.

54.4 Biometric Reader Type 4 – Fingerprint : Outdoor

This biometric (fingerprint) reader shall be used to authenticate users entering or leaving a building with highly sensitive information.

54.5 Biometric Reader Type 4 – Facial : Outdoor

54.6 This biometric (Facial) reader shall be used to authenticate users entering or leaving a building with highly sensitive information. Biometric Reader Type 5 – Facial : INDOOR/Outdoor

This biometric (Facial) reader shall be used to authenticate users entering or leaving a building with highly sensitive information.

55 IP VIDEO CCTV SURVEILLANCE SYSTEM

General

The system must be designed in line with South African Government National Key Point act,
with emphasis on implementation of International CCTV Standards.

This specification must be read in conjunction with the Bill of Quantity document attached and our marked up drawings

All cameras will be in accordance with SANS 10222-5-1-4

The Digital Video Recording & Management System shall include:

- Video Recording Server(s);
- Operator Workstation(s);
- IP Camera(s);

55.1 VIDEO RECORDING SERVER(S)

The Video Recording Server (VRS) will be able to connect to all network-connected devices. The Video Recording Server(s) shall have a large amount of disk space for online video storage and access to high capacity archiving mechanisms for the removal of stored video to off-line media.

The VRS shall comply with the following requirements:

- Receive encoded live video from IP cameras;
- Playback video to Operator Stations;
- Store live video to hard disk, for at least thirty-one (31) days or as per the SSA requirements; quality?
- Archive previously stored video to off-line storage media;
- Retrieve archived video from off-line storage media;
- Allow alarms/events in the Physical Security Information Management System (DSIM) to initiate recordings;
- Initiate recordings on the basis of video motion detection;
- Report any camera failures or recording failures to the Physical Security Information Management System (DSIM)
- Export the recordings into a format so that it can be viewed using standard tools including QuickTime and standard DVD format playable in a DVD player;
- Provide a full log of all system status (camera, streamer, server availability);
- The system must support unlimited numbers of video recording servers;

55.2 OPERATOR WORKSTATION(S)

Operator view shall be provided using many Operator Workstations. These are connected via the network. They are capable of viewing live video and recorded video from the Video Recording Server(s), controlling PTZ functionality and reception of alarms. They also provide levels of operator security.

55.3 SYSTEM SIZING

The security system or control system for the Campus requires that operators be able to view, record and replay video, as detailed in this specification, for a large number of cameras through-out the Campus.

55.4 VIDEO RECORDING SERVER

Proprietary hardware platforms are not acceptable.

55.5 MULTIPROCESSOR SUPPORT

Server shall be able to run on both multiple and single processor computers. Where a multiple processor system is used the storage server shall be able to make optimal use of that configuration.

55.6 OPERATOR WORKSTATION

The Operator Station shall as a minimum conform to the specifications for hardware requirements as shown in BOQ.

Proprietary hardware platforms are not acceptable.

The Operator Workstation will include the following system software components:

- Application software detailed in the Security Management System (SMS) and/or Physical Security Information Management (DSIM) System Specification;
- Windows 10 Professional or later Operating System.
- Application Software with functionality.
- Video Management Software
- System Functionality

The system functionality can be divided into:

- Viewing Live Video;
- Viewing Recorded Video;
- PTZ Telemetry;
- Alarms Events;
- Video Triplex.

55.7 LIVE VIDEO

The live output from cameras shall be viewed through a series of displays. These shall support:

- Single camera view;
- Multiple camera view. A view of up to fifty cameras in any configuration that suits the Operator;
- Sequence view of camera preset positions;
- Modifying settings for a camera;
- Modify recording settings for a camera;
- Adding and deleting cameras;
- Creating schedules for recordings and video motion detection;
- Modifying Video Motion Detection settings and tuning;
- Users shall be able to select a camera from a tree control listing the cameras available to the user.

The system shall also support multiple monitors in the following way:

55.8 SPOT MONITOR

When an alarm occurs in the Administration or Operator Server, the live video output of the camera associated with that alarm shall be switched directly to a Spot Monitor.

55.9 SURVEILLANCE MONITOR

Operators shall be able to send any sequence View or Single Camera View to a surveillance monitor.

55.10 SINGLE CAMERA VIEW

From this display, the user shall be able to:

- View the live output from the selected camera
- Pan, tilt, zoom and focus the camera using a keyboard attached to the Operator Workstation.
- Pan, tilt, zoom and focus the camera using the mouse attached to the Operator Workstation.
- For cameras that support continuous pan, tilt, zoom (PTZ), a mouse shall be able to be used for continuous PTZ directly the software GUI. The operator shall be able to tilt the camera up

or down, or pan the camera left or right. Zooming must also be provided using the mouse in a similar way.

- Manually record live video. Recording will continue for the configured period of time. Once recording has begun, a stop button shall be available.

- Indicate whether video motion detection is currently enabled for the selected camera.

55.11 MULTIPLE CAMERA VIEW

The DVRMS shall support multiple camera views. A multiple camera view shall consist of any number of cameras (50 cameras maximum per Operator Workstation) that the Operator wants to view simultaneously on a single display or on multiple displays.

- The multiple camera view shall be divided in any way the Operator sees fit.

- The system shall have number of different standard setups for the Operator to choose from.

- The screen can for instance be divided into a quad view with four identical views. For each quadrant the quad view shall have a camera or be blank. Within each quadrant the quad view shall be configured to cycle between any of the cameras accessible to the user on a configurable time basis.

- There shall be no limit to the number of cameras that can be assigned to a View.

- There shall also be no limit to the number of available Views.

55.12 SEQUENCE VIEW

- The DVRMS shall support sequence views.
- A sequence view consists of a single camera view, which can be cycled on a time basis. Pan-tilt-zoom cameras, which support preset positions, can have these presets cycled on a time basis.

- In this way an operator can view a variety of presets on a series of PTZ cameras.

- Fixed cameras can also be included in the sequence and cycled accordingly.

- There shall be no limit to the number of cameras that can be assigned to a single Sequence View.

- There shall also be no limit to the number of available Sequence Views.

55.13 VIDEO TRIPLEX

The system shall be capable of doing all of the following simultaneously:

- Viewing Live Video;

- Playing Back Recorded Video;

- And Backing-Up Recorded Video.

55.14 CAMERA SETTINGS

Users shall be able to change important settings for an individual camera. The details are grouped into several sections:

- Camera Details;
- Camera Connection;
- Camera PTZ Control;
- Camera Deletion.

Only users with the highest level of security are permitted to modify Camera Connection Details, Camera PTZ Control or Delete Cameras.

55.15 CAMERA DETAILS

The administrator shall be able to configure the following parameters for each Camera:

- Name;
- Location;
- Description;
- Camera Number.

55.16 SeCURITY

The following parameters shall be configurable for each Camera:

- Area : Allows the system to be configured to only allow specific users to view specified cameras. These areas shall be the defined by the Administration Client or Operator Server.
- Control Level : Determines if a user is allowed to operate the PTZ controls for a camera. Also used to allow higher-level users to take control of cameras. These Control Levels shall be defined by the Administration Server or Operator Server.

55.17 DELETE

- The “Delete” function shall allow a user with the highest-level security to delete the camera from the Video Recording Server. Deleting a camera should delete all the records relating to the camera from the database. The name of the camera will no longer appear in the list of cameras. All camera settings will be deleted.
- The user shall also be asked if they also wish to delete video clips captured for the camera. If the video clips are not deleted they will stay on the video server and archive media unless

they are later individually deleted. The camera name will also continue to appear in the list of cameras used for searching the video clip database.

- If the user chooses to delete video clips captured for the deleted camera, all video clips related to the deleted camera will be deleted. The camera name will be removed from the list of cameras used for searching the video clip database.

55.18 RECORDING

The following methods of Recording Live Video shall be supported:

- User Activated;
- Event Activated;
- Scheduled;
- Video Motion Detection.

Programmer Activated

The programmer shall be able to configure the following parameters for each Camera:

- Pre-Record Duration: The amount of pre-recorded video that will be associated with a user request for recorded video. This will allow the Video Recording Server to capture video prior to the user request, as well as after the request. Shall be selectable from a list of values ranging between 0 seconds and 15 minutes.

- Frame Rate: Video Frame Rates required for User Activated Recording. It shall be possible to have different frame rates for User and Event Activated Recordings. The Frame Rates shall be selectable from the entire range of Frame Rates supported for the Camera.

- Record Duration: User Activated Recordings shall terminate after this period of time. The Recording Duration shall be selectable from a list of values ranging between 0 seconds to 15 minutes.

- Retention Period: The default period that the Video Server shall retain User-Activated Recordings before being deleted. The Retention Period shall be selectable from a list of values ranging between one hour and forever. A First-In-First-Out (FIFO) option shall also be available that will allow the Video Recording Server(s) to over-write the oldest video clip if the storage media runs out.

55.19 EVENT ACTIVATED

There shall be at least four priorities of alarms/events from the Security System or DSIM:

- Low Priority Alarms;
- Medium Priority Alarms;
- High Priority Alarms;
- Urgent Priority Alarms.

The following settings shall be Individually Configurable for each Alarm and each Camera:

- Pre-Record Duration: The amount of pre-recorded video that will be associated with a user request for recorded video. This will allow the Video Recording Server to capture video prior to the user request, as well as after the request. Shall be selectable from a list of values ranging between 0 seconds and 15 minutes.

- Frame Rate: Video Frame Rates required for User Activated Recording. It shall be possible to have different frame rates for User and Event Activated Recordings. The Frame Rates shall be selectable from the entire range of Frame Rates supported for the Camera.

- Record Duration: User Activated Recordings shall terminate after this period of time. The Recording Duration shall be selectable from a list of values ranging between 0 seconds to 15 minutes.

- Retention Period: The default period that the Video Server shall retain User-Activated Recordings before being deleted. The Retention Period shall be selectable from a list of values ranging between one hour and forever. A First-In-First-Out (FIFO) option shall also be available that will allow the Video Recording Server(s) to over-write the oldest video clip if the storage media runs out.

- The pre-record and post-record durations in the paragraph above define the maximum allowable limits for each camera. They shall be configured on a camera-by-camera basis. However each alarm or event causing video to be recorded shall also be capable of individual configuration with pre and post alarm periods being selected from a range defined by the maximum settings for the camera.

- DVRMS systems requiring a single pre and post record event period to be defined for all alarms and events on an individual camera are not acceptable. Pre-event recording is global for each video recording server, as is retention period. In the case of multiple alarms/events relating to the same camera, a video clip shall be created for each alarm/event.

- For cameras that support Pan/Tilt/Zoom Presets, a specified preset location shall be selected automatically when the alarm/event occurs prior to the event activated recording commencing. For example, when an alarm is detected on a security door, the alarm shall trigger a PTZ camera to move to a preset position, which is pointing at the door prior to the DVRMS commencing recording.

The DVRMS shall allow Camera Output to be Recorded for the following conditions:

- Activated by Administrators, Operators, Alarms or Events;
- Manually Activated by a User viewing a Live Camera;
- Scheduled Recording;
- Video Motion Detection.

55.20 SEARCH

The DVRMS shall provide a simple search for all Video Recorded on the Video Server(s). The user selects the time indicator which shows a calendar and time line. The user selects the required search period.

Once the time criterion is entered, the “search” is selected. Video Recorded during the selected period will be returned by the search. The user shall be able to search on combinations of cameras by clicking on an “Advanced Search” icon as described in the next section.

55.21 ADVANCED SEARCH

The DVRMS shall provide an advanced search of Recorded Video. The search shall be based on recording time, camera and recording details. The User shall select from the list of cameras on the Video Server(s). It shall also include any cameras that have been deleted from the Video Server(s) but still have Video stored on the Video Server(s) or on archived media. If a camera has been deleted and all video associated with the camera has been deleted, the camera name will not appear in this list.

The time criteria shall be selected from a calendar and time line control. Days containing Recorded Video shall be shown in bold on the calendar control. Cameras shall be able to be added and removed from the search list.

The user shall be able to choose to filter the search based on the following criteria:

- Alarm or Event Type for Alarm/Event Activated Recordings;
- Recording Type (Schedule, Event, Operator, Video Motion Detection, all);
- Area
- Location Name
- Event Description
- Operator Name
- Camera Name or Number

The user shall be able to search for motion within a recording and define the motion search threshold.

55.22 SEARCH RESULTS

The DVRMS shall show the Search Results of the basic and advanced searches in a table format, such that the user is able to select columns within the list to sort the output. Functionality shall be provided to allow the user to see a list of recordings for a camera from the past 24 hours without needing to use one of the searches.

55.23 USER AUDIT TRAIL

It is a requirement that all User actions on the DVRMS Operator Workstation, Administrator Station, Video Recording Server, etc. be Recorded in a log file along with the DSIM’s actions.

User Actions include:

- Interventions such as Manual Recording and Configuration Setting Changes;
- Cameras Viewed;
- Video Replayed;
- Video Exported;
- Cameras Pan/Tilt/Zoomed and Pre-set Switching;
- This log must also contain a History of the Status of the DVRMS System Components. It shall list the Status of all Cameras, Streamers, Servers and other System Components including when they were Disabled or Failed.
- The log of actions shall be available in text format on the video recording server.

55.24 CAMERA DATABASE

The DVRMS shall support a Camera database including the following information:

- Camera Configuration Details;
- Camera Streamer Configuration Details;
- User Details.

55.25 VIDEO INTEGRATION USER TASKS

The following system tasks shall be performed from the Operator Workstation /Administration Station:

- View Live Video;
- Adjust the PTZ Position of a Camera;
- Live Video is Automatically Displayed on a Monitor when an Event Occurs;
- Search through the Stored Video Clips of a Camera;
- An Operator Records an Incident;
- Add a new Camera to the System;
- Change the Configuration Settings for a Camera/Streamer;
- Provide Alarm/Event Activated Recording from the Administration System;
- Search for Video Clips from different Cameras;
- Create a Camera Tour;
- Conduct a Camera Tour;
- Create a Camera Group;
- View a Camera Group.
- View a Camera Sequence;
- View a Multiple View Screen;
- View Live Video from a Custom Schematic;
- Add live video to a Custom Schematic;
- Configure, Schedule and Tune Video Motion Detection;

- View the Audit Log.

56 CAMERAS

The Digital Video Recording & Management System shall be capable of supporting more than 2048 cameras.

The Video Recording Server(s) will include the following system software components:

- Windows Server 2012 or later Operating System;
- Application Software with functionality

The minimum specifications of each camera type are given below:

56.1 STATIC DOME CAMERAS

Micro Dome Camera Type 3 – 1080P IP - 2.5X Varifocal Lens High Resolution Colour/Day Night STATIC Mini Dome camera

This type of camera shall be used indoors for high definition identification, recognition at short distances.

Mini Dome Camera Type 4 – 1080P IP – 10X Varifocal Lens High Resolution Colour/Day Night STATIC Mini Dome camera

This type of camera shall be used indoors for high definition identification, recognition at short distances.

Mini Dome Camera Type 5 – 5MP IP – 3X Varifocal Lens High Resolution Colour/Day Night STATIC Mini Dome camera

This type of camera shall be used indoors for high definition identification, recognition at short distances.

56.2 STATIC BULLETCAMERAS

Box Camera Type 2 – 1080P IP - High Resolution Colour/Day Night Static Box camera

This type of camera shall be used indoors for high definition identification, recognition at short distances.

Box Camera Type 3 – 5MP IP - High Resolution Colour/Day Night Static Box camera

This type of camera shall be used indoors for high definition identification, recognition at short distances.

Panoramic Camera Type 1 – 8 to 40 Megapixel 180° Panoramic IP – Very High Resolution Colour/Day Night Omni Directional Camera

The Panoramic Camera shall provide Direct Network Connection using H.264 and MJPEG compression and Bandwidth Throttling to Efficiently Manage Bandwidth and Storage Requirements while Delivering Outstanding Image Quality.

The Panoramic Camera shall be used for an all in one solution for outdoor or indoor wide area surveillance where a lot of detail is required.

57 UNINTERRUPTIBLE POWER SUPPLY (UPS)

All security equipment shall be fed from the nearest Main UPS supply where possable

58 X-RAY MACHINE

A parcel/handbag x-ray machine shall be supplied and installed at the reception in the mall.

Thex-raymachineshallbecompletewithaninandoutrollertrayand17" colour monitor.
The x-ray machine shall have the following features:

- Tunnel, min 53 x 33 cm High image resolution
- B/W or colour image representation Image Booster to increase detectability Movable zoom window
- Penetrationofupto6mmsteelwithimagebooster No risk of radiation
- No effect on food or magnetic data

X-ray Machines will be located at the following locations:

- 1 x Campus Main Security Entrance

59 DIGITAL SECURITY INFORMATION PLATFORM (DSIM)

DSIM Specification

The security system will be interfaced to a DSIM system platform to improve facility management and staff efficiencies.

The DSIM solution shall be a software product that provides a platform and applications designed to integrate multiple unconnected security applications and devices and control them through one comprehensive user interface.

The DSIM software shall be based on SOA Architecture with the ability to distribute alarm and event processing services onto multiple servers. It shall also be possible to install the software in a Windows Failover Cluster for increased availability, The DSIM solution shall support increased alarm and event handling by adding multiple servers to the solution.

The DSIM solution shall integrate a wide range of security products including Video Management Systems (VMS), Security Management Systems , Access Control, IP Intercoms (IP PBX), Fire detection(FDS) and Building Management system(BMS)

The DSIM solution shall be capable of receiving events form integrated systems and execute functions on the systems.

The DSIM solution shall incorporate means to implement business security processes through automatic workflows and visual process guidance. It shall be possible to change the workflows and process guidance without upgrading the software or restarting the solution. It shall be possible to configure the Process Guidance so that the relevant information is provided to the users, increasing the situational awareness while resolving incidents.

The DSIM solution shall include static and interactive map capability including the display of alarm locations, data layers, camera asset locations.
High resolution image files shall be supported and automatically be cached to improve the overall user experience. It shall be possible to display maps from ESRI ArcGIS and any WMS compatible map data sources.

The DSIM solution shall provide a video review interface for display of live and recorded video from connected Video Management Systems. The interface shall be unified and consistent regardless of the underlying video system and be capable of displaying video from different types of systems at the same time. It shall provide functionality for viewing live video, recorded video, saving snapshots, viewing video in full screen, pan-tilt-zoom control and pre-set functions.

The DSIM Solution shall contain a dedicated feature for exporting video. The feature shall allow the capture of all related video for an incident regardless of sub-system type or combination of sub-systems providing the video for the location where the incident occurred. The exported video shall be stored on a configured network share and it shall be possible to generate a report describing what video has been exported.

The DISM solution shall have a configurable end-user interface. It shall be possible to build new interfaces and configure interfaces to display different content depending on the situation and operator. It shall be possible to create and update user interfaces without upgrading the software or restarting the application.

The solution shall have the ability to use COTS reporting tools such as Microsoft SQL Server Reporting Services to generate reports on data collected and generated by the DSIM solution. It shall be possible to generate these reports automatically or as a result of an event. It shall be possible to preview reports in the operator user interface before generation. It shall be possible to automatically generate and email reports on a regular basis or as a result of an event.

The solution shall contain user interface components for the creation of live Dashboards. Dashboards components shall include Bar Charts and Graphs, RSS readers, Gauges, Media players, Labels and Web Browsers. It shall be possible to link the Dashboard indicators to data sources and the indicators shall update when the data changes.

The DSIM solution shall allow for granular permissions control for users and user groups and include permission inheritance. Areas that it shall be possible to restrict through permission configuration shall include: Alarm visibility, access to physical locations, and visibility of CCTV assets, video playback control, and Pan-Tilt-Zoom (PTZ) priority.

The DSIM solution shall provide functionality to connect to new and existing data sources and present this data to operators using the solution. It shall be possible to create, read update and delete data from these sources form workflows defined in the solution.

The DSIM solution shall include an easy-to-use administration interface containing functionality for managing users and groups, viewing device states, managing locations and asset locations on maps. It shall support Windows Failover clustering and be built using the latest Microsoft .Net framework.
The DSIM solution shall be designed to run on Server 2012 or later, Windows 10 and Windows 8.1 or later for workstations.
The DSIM solution shall support Federation - Using Federation, multiple independently administered same vendor DSIM systems can connect to each other and share resources. A trust relationship is configured between the DSIM Sites, ensuring that users from each system will be able to access, control and receive events from the remote systems assets.

The DSIM solution shall support a Device Driver Kit as standard, the device driver interface enables 3rd parties to write drivers which is flexible and scalable according to the need.

The DSIM solution shall support a flexible Deployment Architecture - Connection Managers can be deployed at a remote location to queue and/or filter events before being transmitted over the network (poor quality, etc.)

The DSIM solution shall support a Video Streaming Service and have the ability to stream video from any sub system in a common format such as H.264 and distribute using standard streaming techniques such as RTSP or HLS

The DSIM solution shall support a Centralised Video Export facility – with an Intuitive interface, to export incident video from multiple sources in both an industry standard format, and the native recording format
The DSIM solution shall support a Customisable User Interface, allowing trained, certified engineers to build, commission, and customise user interfaces in real-time

The DSIM solution shall include video wall tools that turn any screen into a dynamic video wall

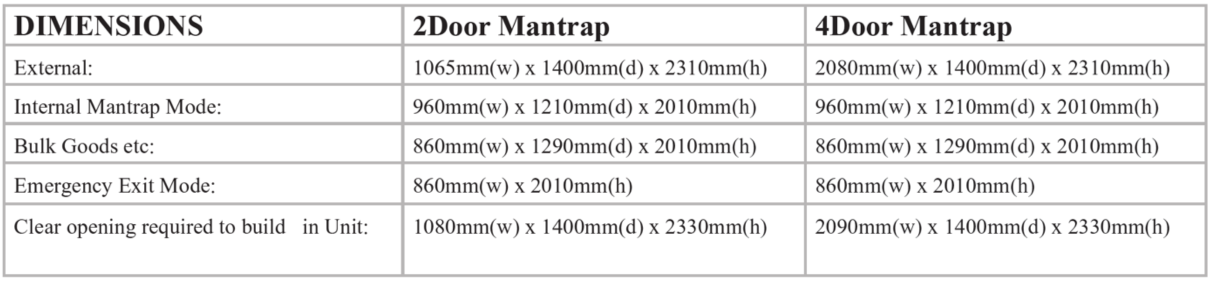
The DSIM solution shall include a Workflow Engine, which when using the response plan editor, Creating custom logic and workflows based around the customers' business process without changing the core build.

The DSIM solution shall be able to integrate any Sub-System, not just those that are traditionally related to Security.

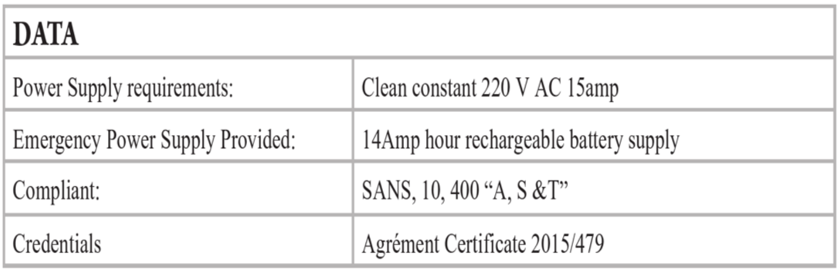
60 MANTRAPS

60.1 2 AND 4 DOOR

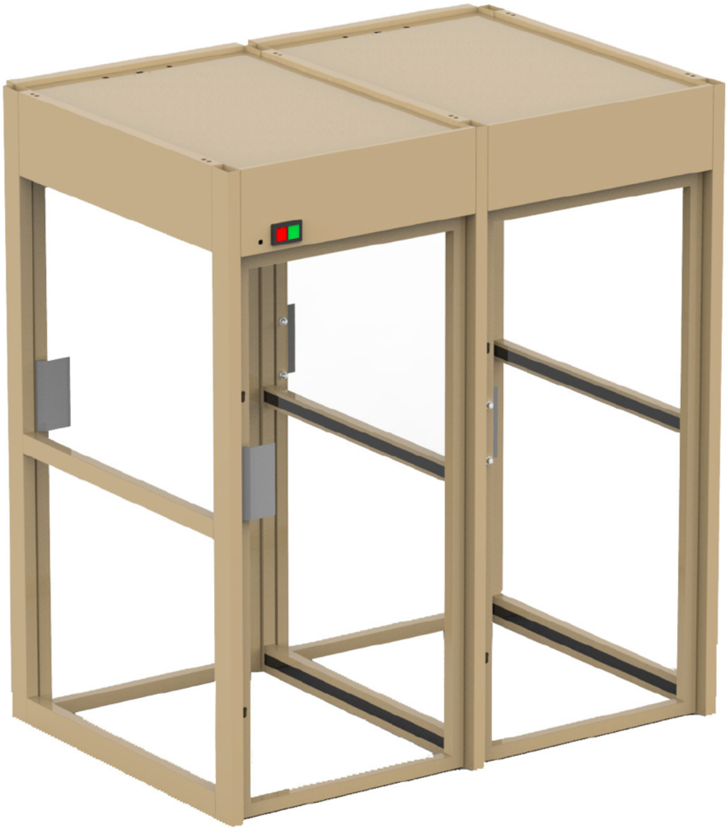
Doors must be aesthetically pleasing, user-friendly robust multiple and secure
Single person entry and exit when required door to regulate pedestrians and goods with minimum delay and inconvenience to and from secure areas, during an effective life expectancy of at least 10 years.
Build in Emergency Exit facilitiesTRUCTURE FEATURES AND CONTROLS
Standard powder coated mild steel.6.38mm sides and 8.38mm doors laminated safe glass.
Following leaves such as with conventional revolving doors which can cause injury and damage are eliminated.
Secure door position monitoring and alarm contacts.
Secure electronic key switch provided on the left eyebrow on the attack side to override the electronic system.
First unassisted automatic entry and last automatic exit through "single" access interlock.
Door open: Unassisted entry and exit.
Must be able to Interface with all reputable building management systems
Standard interface to Bio metric readers.
Remote control and monitoring of above facilities.
Facilities for Pin Lens cameras behind full length opaque lenses.
Carpet mat flooring



DIMENSIONS	2Door Mantrap	4Door Mantrap
External:	1065mm(w) x 1400mm(d) x 2310mm(h)	2080mm(w) x 1400mm(d) x 2310mm(h)
Internal Mantrap Mode:	960mm(w) x 1210mm(d) x 2010mm(h)	960mm(w) x 1210mm(d) x 2010mm(h)
Bulk Goods etc:	860mm(w) x 1290mm(d) x 2010mm(h)	860mm(w) x 1290mm(d) x 2010mm(h)
Emergency Exit Mode:	860mm(w) x 2010mm(h)	860mm(w) x 2010mm(h)
Clear opening required to build in Unit:	1080mm(w) x 1400mm(d) x 2330mm(h)	2090mm(w) x 1400mm(d) x 2330mm(h)



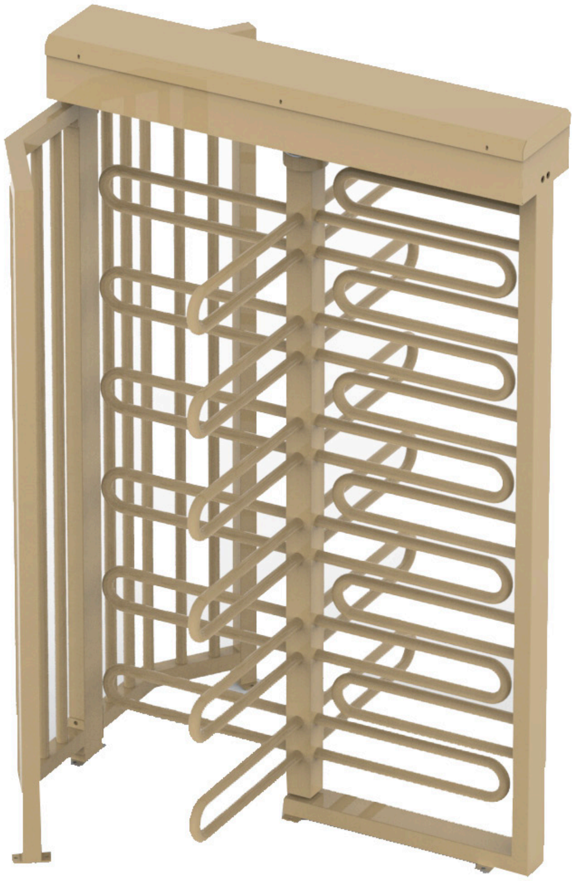
DATA	
Power Supply requirements:	Clean constant 220 V AC 15amp
Emergency Power Supply Provided:	14Amp hour rechargeable battery supply
Compliant:	SANS, 10, 400 "A, S &T"
Credentials	Agrément Certificate 2015/479

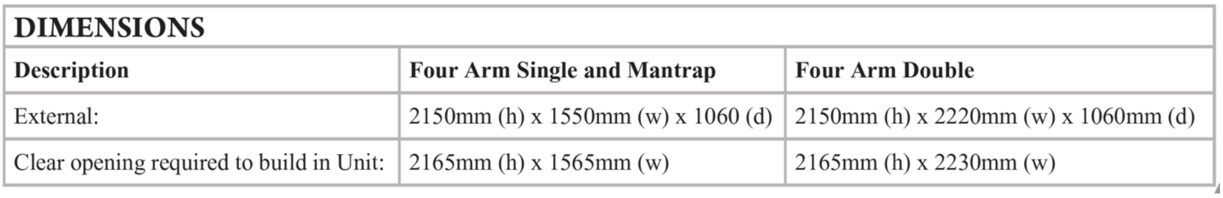


Units must be robust, secure, safe, reliable, aesthetically pleasing, user-friendly and cost effective units, using state of the art electronic and mechanical designs and components to provide physical protection and access control at high volume high risk entrances

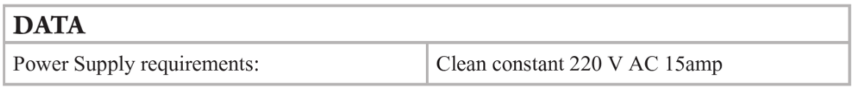
60.2 FEATURES

Spindle must be suspended on heavy duty thrust bearing at the top with up to 3000kg load bearing capacity therefore no load on bottom pivot point.
Unit must be suitable for service in harsh and hostile conditions with high traffic volumes such as in prisons, Rugby, Football etc stadiums etc.
All steel construction access control barrier with revolving spindle and automatically electro mechanical locking in four positions
Mechanical key override for emergency purposes
Resist unauthorised physically force entry.
Turnstile must be a stand-alone bolt together construction with provision for both foot and side anchoring. No welding will be allowed on site for installations.
Single entry and exit





DIMENSIONS		
Description	**Four Arm Single and Mantrap**	**Four Arm Double**
External:	2150mm (h) x 1550mm (w) x 1060 (d)	2150mm (h) x 2220mm (w) x 1060mm (d)
Clear opening required to build in Unit:	2165mm (h) x 1565mm (w)	2165mm (h) x 2230mm (w)



DATA	
Power Supply requirements:	Clean constant 220 V AC 15amp

61 FULL HEIGHT WALK THROUGH METAL DETRECTOR

Contractors to supply and install a multi-purpose multi-zone walk-through metal detector used primarily for weapons detection. Typical applications include staff screening at NKP

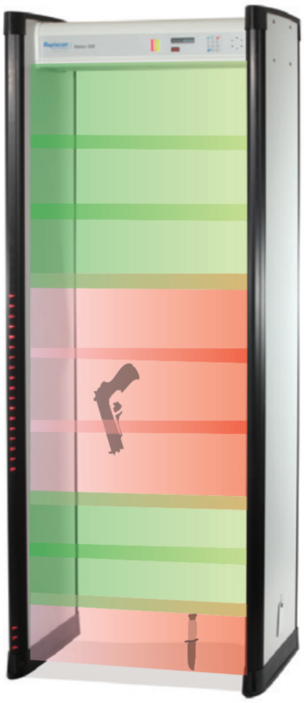
Automated sensitivity and floor sensitivity functions must make the calibration process easy to eliminate the time consuming trial and error method. Automated frequency function selects the optimum operating frequency for the installation environment or in case of side-byside use of more than one unit.

Preset Detection Programs

The unit must have multiple preset detection programs based on international standards, ready to use immediately.

Random Alarm Function

The unit must have a random alarm function that enables security personnel to randomly choose individuals for an additional security check. With the new dual random alarm feature, people who cause a normal alarm are also subject to a random alarm.
Intelligent Traffic Counters for Reliable Statistics built in with intelligent and virtually invisible traffic counters which are integrated inside the coil panels.
Counters are bi-directional with a decrease mode. Alarms, staff and alarm rates can all be counted.



- Alarm Audible/visible alarm.
- Alphanumeric display and Zone Display.
- Relay contact for remote alarm (SPDT) Sensitivity 100 sensitivity steps in each program.
- Separate horizontal zones with independently adjustable sensitivity from 0-200%.

- Calibration Automatic or manually set.
- Interference Suppression
- Digital filtering by signal processor.
- Several operating frequencies to suppress local electrical noise.
- Warranty Two (2) years, parts Network Connections
- Remote Security Monitoring System compatible (Ethernet)
- Dimensions Interior: 760 mm Width x Interior: 2050 mm Height Exterior: 900 mm Width x 2240 mm Height x 700 mm Depth

62 TOWER SECURITY SPECIFICATIONS

The client wishes to install a similar or equal security solution at two remote sites to test the connectivity between remote sites and the Sentech STC Central control room.

62.1 Access Control System

The access control system will be the same as offered for the Sentech STP Radio Kop System but of a much smaller scale.
The Access Control card will carry the Bio-Matrix details of the staff and contractor allowed them into the remote sites.
The system will record user, time and date on the site remote controller and in turn report back to the CCC access control system database.
On entering the building, the I/R Dome CCTV camera image will automatically be displayed at the CCC who in term will verify if person inside the building is legitimate or not.

The CCC operator will dispatch the **local security** response team to the site.
If it is found that the person inside the room is an intruder, the control room operator will be able to verbally (communicate)confront the intruder.
If, however the intruder does not run away the control room, the operator will activate the Pepper gas inside the building.

62.2 CCTV Surveillance system.

Contractor will be required to install one IR Dome camera (On the edge video analytics) on the inside of the building monitoring the door. Camera must be set to motion detection.
One Thermal camera will be installed on the tower looking down towards the ground (round mast)
In the case where the tower is not round two Thermal cameras will be used to do a 360-degree coverage.
Camera's must be placed in such a position that it is very difficult to be tampered with or to be stolen
Only Thermal cameras with on edge processing will be allowed.
The thermal camera must be set up with its trip wires on or just outside the perimeter fence.
The cameras will be linked to an onsite NVR and in turn be linked to the CCC in Radio Kop
Contractor will insure to offer a full solution and must add any components not in the BOQ
On the larger Platinum Sites four Thermal cameras will be installed around the perimeter fence/wall to form an overall security barrier(virtual fence) around the site

62.3 Audio Challenge

An audio challenge system must be installed at all remote tower sites to enable security in the CCC to see and speak to an intruder through the audio system. For example if an alarm was activated at any one of the sites the controller at the CCC will be able to see the

intruder and will be able to verbally warn them that they have been detected and the police have been called, minimising the amount of damage or loss.
Each Thermal camera will be equipped with a horn speaker for audio challenge

63 ELECTRIFIED FENCE

Contractor to supply a high security monitored mesh barrier fencing around the towers.
The fence will become a “monitored” fence and must provide the required notifications to ensure the necessary levels of detect, deter and delay are achieved. This in turn must result in effective local response.
The fully integrated intelligent mesh fence must be one entity and no additional fences must be required.
The Security Monitored Mesh Barrier Fencing must have a monitoring system that meets statutory requirements in RSA

63.1 FENCE HEIGHT

3 metres above ground level. (15 x Panels and 16 x line wires)

The post spacing is 3m.

63.2 POSTS

All posts are to be sunk 600mm into the ground and are set in 25mpa concrete of 600mm x 400mm x 400mm.

63.3 CORNER POSTS

Post Type:
76mm Square tubing 2mm thick.

Post Dimensions:
76mm x 76mm x 3 metres.

Post Holes:
24 x 16mm holes on two adjacent sides.

13 x 4mm holes on two adjacent sides.

63.4 STRAINING POSTS

To be planted every 50 metres)
Post Type:
76mm Square tubing 2mm thick

Post Dimensions:
76mm x 76mm x 3 metres.

Post Holes:
24 x 16mm holes on two opposite sides.

13 x 4mm holes on two opposite sides.

63.5 **END POSTS**

Post type:
76mm Square tubing 2mm thick

Post Dimensions:
76mm x 76mm x 3 metres.

Post Holes:
24 x 16mm holes on one side.

13 x 4mm holes on one side.

63.6 **INTERMEDIATE POSTS**

Post Type:
I-Post. (Rolled and shaped tube)

Post Dimensions:
70mm x 44mm x1.6mm x 3 metres.

63.7 **PANELS**

12 x individually monitored panels are installed between each pair of intermediate posts and each panel is insulated through the post.
Panels will not be stepped for incline but will follow the terrain slope.

63.8 **PANELS TYPE:**

Welded Mesh (25 x 50)
Panel Dimensions:

187mm x 2900mm with two x 300mm fly ends.

63.9 **PANEL APERTURES:**

50mm x 25mm (option 2)

63.10 **PANEL WIRE THICKNESS:**

4mm horizontal and 4mm vertical. (for option 1)

63.11 **PANELS SHAPE:**

1 x rolled bend and 1 x opposite direction V bend both with a 37mm off-set.

63.12 **PANEL FIXING METHOD**

There shall be no bolts and nuts of any description. The fly-ends (2 – off) of each panel shall be threaded through the post and affixed to the adjoining panel with pneumatically crimped clips in eight places on each fly end. (Total of 16 clips per panel)
Clip Type:

CL 23

Clip Dimensions:
18mm x 14mm overall outer.

63.13 INSULATORS

Two large insulators shall be inserted into the posts per panel. (Total 24)
One small insulator shall be inserted into the post per panel plus one above the top panel. (Total 13)

63.14 LARGE INSULATORS

Material: UV Stabilised High Density Polyethylene

Insulator Description:
Interference fit Pop-Em
Insulator Dimensions:
81mm x 28mm + 26.5mm x 26mm

63.15 SMALL INSULATORS

Material:
UV Stabilised High Density Polyethylene

63.16 INSULATOR DESCRIPTION

Interference fit Pop-Em
Insulator Dimensions:
66.3mm x 24.7mm + 18.5mm x 23.4mm

63.17 RING INSULATORS

Material:
□UV Stabilised High Density Polyethylene

63.18 INSULATOR DESCRIPTION

A threaded ring insulator which screws into the corner, strain and end posts to carry the line wires.
Insulator Dimensions:
53.5mm x 50mm x 35mm.

63.19 ADJUSTER INSULATORS

Material:
UV Stabilised High Density Polyethylene

Description
A tensioning insulator for tensioning the line wires which screws into the corner, straining and end posts.
Dimension:
72mm x 32mm

63.20 POST CAPS

All Posts shall be sealed with a Post Cap

Post Cap Type
UV Stabilised High Density Polyethylene
Post Cap Dimensions: To fit posy type

63.21 **LINE WIRES: (15-LINE WIRES ARE REQUIRED FOR A 3-METRE-HIGH FENCE.)**

Material
Stainless Steel.
Description
1.6mm Stainless steel line wire.

63.22 **ANTI-DIG SOLUTION**

300mm deep from ground level (FGL) 300 mm wide

63.23 **MONITORING**

The Unit must be a 4-zone fence monitor.
The unit must monitor up to 4 loops of fencing and unit must be able to detect tampering with the fence by cutting and climbing. An immediate alarm must be sent to the central control room.
The control unit will report an alarm on seeing a monitored loop cut (open circuit) or to ground.

Monitor via Access Control Controller

- Built-in battery charger and for optional 7aH back up battery
- Siren and Strobe switched 12V DC outputs
- 2 control inputs and 4 output relays programmable

64 BILL OF QUANTITIES

64.1 **Tenderer is to add all additional equipment under “Other” required to meet specification and to make a full workable system and should it be found that equipment is not listed in the Bill of Quantity - a complete cost break down must be attached to this document showing how cost was derived at. It is the responsibility of the tenderer to ensure that all equipment, cable and materials are priced in Bill of Quantity, This Bill of Quantity is re-measurable and quantities can be added or removed to fit the final installation as needed.**