DEPARTMENT OF PUBLIC WORKS

SECURITY
STANDARD TECHNICAL SPECIFICATION
FOR AN
INTEGRATED SECURITY SYSTEM
FOR A
CORRECTIONAL FACILITY

1 SECURITY MANAGEMENT SYSTEM (SMS)

1.1 General Description and System Overview:

The Contractor shall supply, install and commission a fully integrated multi-workstation security management system to facilitate the control and monitoring of all security sub-system components by means of a mouse activated operator workstation.

Operator Workstations shall be located within each local control room as well as the Movement and Central control rooms within the facility.

The Contractor shall provide all materials, labour and supervision required to install, commission and document the complete system as required by this specification, and as indicated on the accompanying drawings.

The SMS offered shall have demonstrated proven operation in a minimum of five (5) Correctional facilities, and a list of reference sites shall be provided as part of the tender response.

1.2 Security Sub-System Integration

The Security Management System (SMS) shall provide the integration platform for **all** Security Sub-Systems. It is a specific requirement of this tender that the SMS shall interface directly with all sub-system hardware by means of existing drivers supplied as part of the SMS software. Hardwired interface of one sub-system to another to achieve integration with the SMS shall not be accepted.

The SMS software shall perform all interlocking functions between the various subsystems i.e. the automated switching of CCTV images upon intercom selection, door alarms, fire alarms etc. The SMS software shall be capable of configuring the necessary interlock functions either by providing a configuration table or an internal scripting facility or a combination of the two. The programming of interlock functions within sub-system hardware/software as a means of achieving the required functionality shall not be accepted. The tenderer shall provide a description of the interface protocol for each sub-system hardware platform offered as part of this tender, in the clause by clause compliance statement to be returned with their submission.

The SMS software shall provide the necessary soft control functions to eliminate the need for any additional control components such as keyboards, joysticks or proprietary operator panels.

System operators shall be capable of controlling all functions of the sub-system hardware components via a single mouse driven operator workstation running on a Windows 7 or later operating platform within a single Security Management Application.

The following sub-system hardware components shall be directly integrated with the Security Management System by means of a high level interface:

1. PLC based door locking system
2. Access Control based door locking system
3. Digital Intercom & Public Address system
4. IP based CCTV system
5. IP based Video Recording system
6. Perimeter Detection system
7. Fire Detection system
8. Nurse Call system
9. Uninterruptible Power Supplies

The following devices shall be interfaced to the Security Management System via the PLC based door locking system by providing remote multi-I/O modules where required:

1. Duress Buttons
2. Non controlled door position switches (DPS)
3. Over voltage suppression devices
4. Standby Generator Sets
5. Compressor Status
6. Air Reticulation Status

1.3 Security Management functions

The Security Management System (SMS) shall provide the following software functions:

1. Graphical representation of the facility by means of multiple area maps
2. Control and Monitoring of PLC controlled Doors
3. Control and Monitoring of Access Controlled Doors
4. Control and Monitoring of Intercom and Public Address Stations
5. Manual and event based selection of IP based fixed and PTZ CCTV cameras
6. Control of Pan, Tilt, Zoom functions of CCTV Cameras
7. Event based Black Screen Management of CCTV Cameras
8. Configuration of Network Video Recording
9. Event based retrieval of recorded video footage
10. Control and Monitoring of Perimeter Detection devices
11. Control and Monitoring of Fire Detection devices
12. Control and Monitoring of Nurse Call devices
13. Monitoring of centralized UPS's
14. Monitoring of Duress Buttons
15. Monitoring of Standby Generator sets
16. Monitoring of Air Compressors
17. Monitoring of Air Reticulation statistics
18. Staff, Visitor and Inmate Enrollment
19. Staff Time and Attendance Management
20. Guard Tour
21. Visitation Management

1.4 Security Large Area Network

A high speed 1GB high speed Ethernet network shall be supplied, installed and commissioned by the contractor, which shall provide system networking for all security sub-system hardware.

It is a specific requirement that all sub-system hardware shall interface either directly or by means of IP converters within the local equipment room in each building. All communications between buildings shall be IP based.

The LAN shall be installed in a star topology with the star point being situated at the most centrally located Security Equipment room in the facility. Each local equipment room shall be equipped with a sufficient number of 24 port 10/100 Layer 3 Managed PoE Ethernet switches with a minimum of two 1GB uplink ports. Sufficient Switches shall be provided to enable the termination of all 10/100 devices provided.

The 1 GB Uplink ports shall be networked via fiber optic converters to the Central equipment room and terminated into a 24 port 10/100/1000 Layer 2 Switch.

The contractor shall supply and install all cables, enclosures, switches and any other components to make the system complete.

1.4.1 LAN Specification

Media

a.	Distance <100m:	Ethernet Category 5 – UTP
b.	Distance >100m:	Fibre Optics–1000Base-FX, 850nm Multimode
c.	Conversion Mod:	TX/FX Multi Mode/Plus-SC

1.4.2 Layer 3 Managed Switch with 2x Uplink Ports

- Port Configuration: 24x 10/100 Base-T Ports (PoE Enabled)
  2x 10/100/1000 Base-T Ports
  2x SFP Fibre Ports
  Auto-Negotiating,
  Duplex Mode
  Port Mirroring,
  Broadcast Storm Control
- Performance: 12.8 GBps Switching Capacity
  9.5 Mpps Forwarding Rate
  Minimum 8000 MAC Addresses
- Availability: Spanning Tree (IEEE 802.1D)
  Rapid Spanning Tree (IEEE 802.1w) with FLink Support
  Multiple Spanning Trees (IEEE 802.1s)

- Management: Web based Management Interface
  CLI accessible via Telnet
  SNMPv1, SNMPv2c and SNMPv3 support
  BootP/DHCP IP address management support

- Quality of Service: Layer 3 trusted mode (DSCP)
  4 Priority Queues per port
  Adjustable Weighted-Round-Robin (WRR)
  Multicasting (IGMP Snooping)

- Security: IIEEE 802.1x based edge authentication
  Switch access password protection
  Port-based MAC address alert and lock-down
  IP address filtering for management access via Telnet, HTTP, HTTPS/SSL, SH and SNMP
  RADIUS and TACACS+ remote authentication for switch management access
  SSLv3 and SSHv2 encryption

- VLAN: VLAN support for tagging and port-based as per IEEE 802.1Q
  256 VLAN support
  Dynamic VLAN with GVRP support;
  Private VLANs

1.4.3 Layer 3 Managed Switch with 24x 1GB Ports

- Port Configuration: 24x 10/1000 Base-T Auto-sensing Gigabit Ports
  2x SFP Fibre Ports
  Auto-Negotiating, Duplex Mode
  Port Mirroring, Broadcast Storm Control

- Performance: 136 GBps Switching Capacity
  95 Mpps Forwarding Rate
  Minimum 8000 MAC Addresses
  256 MB CPU SDRAM
  32 MB Flash Memory

- Availability: Spanning Tree (IEEE 802.1D)
  Rapid Spanning Tree (IEEE 802.1w) with FLink Support
  Multiple Spanning Trees (IEEE 802.1s)
  Virtual Redundant Routing Protocol Support

- Management: Web based Management Interface
  CLI accessible via Telnet
  SNMPv1, SNMPv2c and SNMPv3 support
  BootP/DHCP IP address management support

- Quality of Service: Layer 3 trusted mode (DSCP)
  Layer 4 trusted mode ((TCP/UDP)
  8 Priority Queues per port
  Adjustable Weighted-Round-Robin (WRR)
  Multicasting (IGMP Snooping)

- Security: IIEEE 802.1x based edge authentication
  Switch access password protection
  Port-based MAC address alert and lock-down
  IP address filtering for management access via Telnet, HTTP, HTTPS/SSL, SSH and SNMP
  RADIUS and TACACS+ remote authentication for switch management access
  SSLv3 and SSHv2 encryption

- VLAN: VLAN support for tagging and port-based as per IEEE 802.1Q
  256 VLAN support
  Dynamic VLAN with GVRP support;
  Private VLANs

1.5 Integration Description

1.5.1 PLC Based Door Locking Sub-System

The locking sub-system hardware shall be integrated with the SMS via a high level Interface (HLI). The full functionality of the locking sub-system hardware shall be integrated with the SMS to provide enhanced features including but not limited to:

1. Door Lock
2. Door Unlock
3. Door Inhibit
4. Door lockdown
5. Door lockdown time preset
6. Door Status monitoring

7. Door Alarm annunciation

8. Door auto-close

9. Hardware fault diagnostics.

The locking sub-system shall control and monitor all electrically and pneumatically controlled swing doors, sliding doors and gates within the facility.

The locking system control hardware (I/O points) shall be an integrated function of the door control module as described in this specification.

1.5.2 I/O Alarm Monitoring Sub-System

An Alarm monitoring sub-system shall be provided to monitor specific hardwired alarm I/O points within the facility, which shall be managed by the PLC based door locking system hardware. Such Alarms shall include but not be limited to the following:

- DPS monitored door alarms.
- Duress alarms.
- Standby generator alarms.
- Surge Voltage alarms.
- Air system alarms.

The alarm monitoring system control hardware (I/O points) shall be an integrated function of the door control module as well as the multiple I/O control modules described in this specification.

1.5.3 Access Control Sub-System

The Access Control requirement consists of two sub-components:

1. Biometric Logon of Operator Workstations

Each Security Management System Operator Workstation shall be provided with a vandal resistant fingerprint reader for logging on to the Workstation. Operator's commands and events shall be logged into the centralised database against the relevant Operators details.

2. Biometric Access Controlled Doors

Each Access Controlled door shall be equipped with a Vandal resistant IP65 rated Fingerprint Reader as detailed in the specification.

The Access Control Terminal (ACT) offered shall incorporate both Finger recognition and proximity/Contact less card recognition within a single housing. By default, 1 to Many (1:N) fingerprint matching shall be utilised for identification, and only in cases where a users fingerprint cannot be captured, shall a proximity or Contact less Mifare card be used.

The following functionality shall be provided by the Access Control System:

1. Staff Time and Attendance Management
2. Guard Tour
3. Visitation Management

1.5.4 Intercom & Public Address Sub-System

The Digital Intercom and Public Address sub-system hardware shall be integrated with the SMS via a high level Interface (HLI). The full functionality of the system shall be integrated with the SMS to provide enhanced features including but not limited to:

- Station Call-In
- Station Fault Analysis
- Call In Divert
- Call Answer
- Call Cancel
- Call-In Queuing
- Tamper Alarm monitoring
- Threshold Monitoring (Disturbance detection)
- Individual station Speaker and Microphone sensitivity adjustment

The Intercom and Public Address system shall enable the selection of any individual or group of intercom stations by any operator workstation within the facility.

1.5.5 IP Based CCTV Sub-System

A fully IP based CCTV System shall be integrated with the SMS via a high level Interface (HLI) at each workstation or server. The full functionality of the system shall be integrated with the SMS to provide enhanced features including but not limited to:

- Camera to Monitor commands
- Sequence to Monitor commands
- Sequence programming commands
- Pan, Tilt, Zoom commands
- PTZ preset select commands
- PTZ preset save commands
- Monitor Blanking commands
- Black screen technology

Camera Types that are not available as direct IP cameras shall be converted to IP via a single channel H264 IP Video Encoder mounted directly at the camera position.

1.5.6 IP Based Network Video Recording Sub-System

A fully IP based Video Recording System shall be integrated with the SMS whereby all images are stored on Digital Video Recording Servers installed within the various security equipment rooms in the facility. NVR's shall be connected directly to the appropriate 24 Port managed switches within the local equipment cabinets.

The managed Ethernet switches shall be configured to limit the Video traffic onto the incoming 1Gb uplink ports on the switches, by restricting outgoing streams to those required for live video feeds based on Operator selection, and recorded video footage being reviewed by Central Operator Workstations or the Operations room.

In order to minimize traffic on the 1 GB uplink ports, the allocated recording stream on each of the Direct IP cameras or IP Video Servers shall be assigned to the IP address of the Network Video Recorders within the local subnet.
The tenderer is required to submit a lump sum rate in the Bill of Quantities for a complete Network Video Recording system based on the total number of cameras indicated in the Bill of Quantities.

The full functionality of the NVR system shall be integrated with the SMS to provide enhanced features including but not limited to:

- Individual Channel Record and Stop commands based on other sub-system conditions such as Intercom, CCTV and Locking.
- Channel Playback select
- Play
- Stop
- Pause
- Back
- Left Jump
- Right Jump
- Left Shift
- Right Shift
- Plus
- Minus
- Log
- Search

The search and playback facility shall be an integrated function of the SMS, and shall not require any third party software platform to perform these functions.

Upon operator request the SMS system shall be capable of instructing the NVR system to playback video images to allow proper investigation of the visual event. The SMS management workstation shall be capable of recalling associated historical Video and Audio data based upon events logged to the event recording database on the severs.

System supervisors with the correct user level shall be able to query the event database as described in this specification and by double-clicking on a specific event shall be presented with the associated Video and Audio footage automatically.

1.5.7 Perimeter Security Fence Sub-System

The Perimeter Fence system shall be fully integrated with the Security Management System by means of a TCP/IP socket interface (High Level Interface), in order to carry out logical connections with other security sub-systems such as the CCTV and Digital Video recording systems.

The operator shall be able to select a graphical layout of the entire facility, which shall also be automatically activated upon an alarm event from the perimeter fence system.

The Security management system shall be capable of, but not limited to the following monitoring and control functions relating to Perimeter Detection:

- Individual Taut Wire alarm status
- Individual Taut Wire maintenance status
- Individual Taut Wire healthy status
- Non-Lethal shock energizer loop open circuit status
- Non-Lethal shock energizer loop short circuit status
- Non-Lethal shock energizer loop normal status
- Digital expansion Input status
- Field Node communication status
- Field cabinet tamper status
- Field Node logic monitoring status (Light on status)
- Field Node battery charger voltage
- Individual Taut Wire sensor deflection
- Sensor alarm Acknowledge
- Loop alarm Acknowledge
- Sensor alarm Reset
- Loop alarm Reset
- Inhibit Taut Wire Sensor alarm
- Inhibit Taut Wire Loop alarm
- Inhibit Digital Expansion Input alarm
- Inhibit Field cabinet Tamper alarm
- Individual Sensor sensitivity setting
- Loop sensitivity setting

1.5.8 Centralized UPS System

The Dual redundant centralized UPS's shall be fully integrated with the Security Management System by means of a High Level Interface (HLI), to provide operators and technicians with detailed status and alarm conditions regarding the UPS systems.

Due to the Centralized configuration, the following detailed diagnostic information is required, and shall be presented to the operator via a drop down menu option within the SMS:

1. UPS Data:

    - Manufacturer
    - Type
    - Serial Number
    - Software Version

2. Battery Data:

    - Battery Status
    - Time Remaining in minutes
    - Remaining Charge in %
    - Battery Voltage
    - Battery Current
    - Battery Temperature in Deg C

3. AC Input Data:

    - Frequency per phase
    - Voltage per phase
    - Current per phase
    - Power per phase

4. AC Output Data:

    - Frequency per phase
    - Voltage per phase
    - Current per phase
    - Power per phase
    - Load % per phase

5. UPS Alarm Conditions:

    - Battery Failure
    - On Battery Power
    - Low Battery
    - Depleted Battery
    - Over Temperature
    - Input Supply Out of Limits
    - Output Out of Limits
    - Output Overload
    - Bypass Active
    - Bypass Inhibited

- Charger Failure
- Fan Failure
- Fuse Failure
- Diagnostic Test Failure
- Communications Failure
- Shutdown Pending
- Shutdown Imminent

All alarm conditions shall be presented to the operator within the Fault queue as described in the specification.

1.5.9 Fire Detection System

The Main Fire Detection Panel shall be fully integrated with the SMS via a high level Interface (HLI) at the redundant SMS server workstations. The full functionality of the system shall be integrated with the SMS to provide enhanced features including but not limited to:

- Detector Healthy status
- Detector Alarm status
- Detector Fault/Maintenance status
- Detector Inhibit status

- Detector Inhibit Command
- Detector Un-inhibit Command

- Alarm Silence Command
- Alarm Reset Command
- Synchronize Clock Command
- Communication Failure Alarm

The position and status of each Detector, Sounder and Break-glass unit within the facility shall be indicated on the appropriate area map of the SMS.

A Fire Detection layer On/Off option shall be available through the menu structure, which shall toggle the display of the smoke detector icons on and off as required. This function is required to minimize congestion of icons on the area maps, due to the location of other sub-system equipment icons.

Upon an alarm condition regardless of Fire Layer status, the affected detector icon shall be displayed, and the alarm condition shall be presented to the operator within the Fault queue as described in the specification.

1.5.10 Nurse Call System

The Nurse Call system shall be fully integrated with the SMS via a high level Interface (HLI) at the nearest operator workstation to the hospital wards. The system shall be integrated with the SMS to provide the following information and functions:

- Nurse Call station active status
- Nurse Call station in-active status

- Nurse Call station inhibit command
- Nurse Call un-inhibit command
- Nurse Call station inhibit period set-point adjustment

The position and status of Nurse Call station within the facility shall be indicated on the appropriate area map of the SMS.

A Nurse Call layer On/Off option shall be available through the menu structure, which shall toggle the display of the Nurse Call station icons on and off as required. This function is required to minimize congestion of icons on the area maps, due to the location of other sub-system equipment icons.

Upon a Nurse Call request regardless of Layer status, the affected nurse call icon shall be displayed, and the call-in condition shall be presented to the operator within the Fault queue as described in the specification.

A dedicated Nurse Call workstation with a common version of the SMS shall be provided at the Nurse Duty desk within the hospital section, and shall contain only the necessary area maps with the nurse call icons. The use of hard-wired mimics for the annunciation of nurse call-ins shall not be considered.

1.6 System Configuration:

The Interactive Security Management System (SMS) shall consist of multiple Operator Workstations, situated in the local, movement and central control rooms, and shall be networked by means of a Fibre Optic Large Area Network (LAN). This network shall be a dedicated security network for use by the SMS only.

The network interface between control rooms shall be by means of a Fibre Optic medium, and shall form a star configuration from the Central Control room to each local control room to ensure local system autonomy.

The Operator workstations shall serve as the graphic based operator interfaces between the corrections officers and the facility's locking controls system and other security subsystems as specified herein.

All operator functions shall be controlled by means of a mouse, and shall require the minimum movement and actions in order to complete a required task.

The operator VDU shall be recessed into the control console to ensure that operator visibility is maintained.

The audio sub-system components within each control room shall form an integral part of the control console, and shall not require the use of external control equipment such as PTT buttons, Operator Keyboards etc.

All security sub-system control functions shall be interlocked to ensure that functional procedures are adhered to.

The following Interlock functions shall be programmed as an integrated function of the Security Management System:

- The selection of Cameras prior to Door opening
- The selection of Intercom communications prior to Door opening
- Automatic Camera select upon door opening
- Sally port door interlocking
- Monitored door interlocking
- Automatic Camera selection upon Intercom activation
- Automatic Video recording on camera image activity
- Automatic event recording on individual operator activity
- Automatic Control console “LOG-OFF” on control room door
- Interlock capability according to operator log-in level

Alarm processing, alarm logging, alarm response data entry, graphical and text based user interface, data entry, and other system management functions shall be performed by the SMS operator workstations connected to the SMS network. The operator workstations shall be located in the Central Control Room and other nominated locations.

All Distributed control modules as other than door control modules mounted in door headers are to be suitably mounted within secure enclosures to the approval of the Engineer and located in the respective buildings' security and communications equipment cupboard, or other secure area as approved by the Engineer.

The SMS shall utilize a single global database and shall be fully distributed to Distributed control modules connected to the SMS security network. All system operators shall have limited access to this information/data from the operator workstations. The level of access shall be controlled by use of the Biometric logon facility available at each operator workstation.

The system shall be designed such that failure of any control module or operator workstation shall not functionally affect the operation of any other module, network, building or Operator workstation connected to the SMS network.

Similarly, should any area lose power or suffer a loss in communications due to a break in the communications cabling, all Distributed control modules installed in that area shall continue to operate with no loss of functionality.

The SMS shall be fully programmable to allow:

- Response instructions to be displayed for all alarms types.
- Use dynamic (real time) graphics to display device status.
- Initiate operator commands via system tailored icons.
- Display building layouts in a graphical representation.
- Easy to follow menus with single key select options, to assist in the daily routine operations of each facility.
- Allocate alarm priorities.
- Set Alarm response properties.
- Set lock/unlock and access/secure operating schedules.
- Generate User defined reports.

The contractor shall allow adequate time to liaise with the Engineer in order to detail any user specific requirements necessary for the operation of each building, system, alarm type, and alarm response configuration within the system. This shall include the configuration of maps, report formats, access schedules, alarm response instructions and the like, to suit each operator workstation.

The system shall be modular in design to allow for future system expansion (i.e. in excess 200 % of specified capacity) with minimum cost and disruption to the existing operational system.

Tenderers are to specify the systems total capacity for future expansions.

Such upgrades shall not render a redundancy in field hardware, the Central Processing Units or any major component of software, firmware or operating systems.

1.7 System Performance:

1.7.1 Central & Movement Operator Workstations

The interaction delay between activating a control icon on any given operator workstation and the controlled point activation, (i.e., the lock), shall be no greater than one second (1 sec).

The interaction delay between controlled point activation and any given operator workstation response either by activation of an audible alarm and/or the associate icon changing state (color) shall be no greater than one second (1 sec).

The interaction delay between recalling any floor plan at any given operator workstation shall be no greater than one quarter of one second (0.25) second.

1.7.2 Local Operator Workstations

The interaction delay between activating a control icon on any given operator workstation and the controlled point activation, (i.e., the lock), shall be no greater than one half of one second (0.5 sec).

The interaction delay between controlled point activation and any given operator workstation response either by activation of an audible alarm and/or the associate icon changing state (color) shall be no greater than one half of one second (0.5 sec).

1.8 Minimum Hardware Requirements:

1.8.1 Operator Workstations

Operator Workstations shall comply with the following minimum specification:

- Chassis: Mini-Tower
- Processor: Dual Core Intel® Xeon® W3503 2.40GHz, 4M L3, 4.8GT
- OS: Windows 7 or later
- Memory: 2GB, 1066MHz, DDR3 SDRAM, ECC (2 DIMMS)
- Hard Drive: 250GB SATA 3.0Gb/s, NCQ and 16MB Cache
- HD Controller: Integrated Intel chipset SATA 3.0Gb/s

- Optical Drive: 16X DVD-ROM with Cyberlink Power Dvd
- HD Configuration: All SATA drives, No RAID
- Graphics Card: 1.5GB NVIDIA® Quadro® FX 4800, DUAL MON, 2DP & 1DVI
- Network Adapter: Intel, 1Gbps, PCI Express with SNTP and DMI2 support
- Monitor: 22”LCD HAS Wide Monitor, VGA/ DVI Inputs, Res 1680 x 1050 pixels.

Logon Reader: Vandal resistant Finger Print verification reader for automatic operator identification and logon.

1.8.2 Management Workstation

A single Management Workstation shall be provided, and shall comply with the following minimum specification:

- Chassis: Mini-Tower
- Processor: Dual Core Intel® Xeon® W3503 2.40GHz, 4M L3, 4.8GT
- OS: Windows 7 or later
- Memory: 2GB, 1066MHz, DDR3 SDRAM, ECC (2 DIMMS)
- Hard Drive: 750GB SATA 3.0Gb/s, NCQ and 16MB Cache
- HD Controller: Integrated Intel chipset SATA 3.0Gb/s
- Optical Drive: 16X DVD-ROM with Cyberlink Power Dvd
- HD Configuration: All SATA drives, No RAID
- Graphics Card: 1.5GB NVIDIA® Quadro® FX 4800, DUAL MON, 2DP & 1DVI
- Network Adapter: Intel, 1Gbps, PCI Express with SNTP and DMI2 support
- Monitor: 22”LCD HAS Wide Monitor, VGA/ DVI Inputs, Res 1680 x 1050 pixels.

Logon Reader: Vandal resistant Finger Print verification reader for automatic operator identification and logon.

1.8.3 Server Workstation

A redundant server configuration shall be provided, and shall and shall comply with the following minimum specification:

- Chassis: 2U Industrial Mount Chassis with 2 Cabled HDs and Quad-Pack LED Diagnostics
- Processor: Intel® Xeon® X3430, 2.4Ghz, 8MB Cache, Turbo
- OS Win Server 2008
- Memory: 4GB Memory, DDR3, 1066MHz (4x1GB Single Ranked UDIMM)
- Raid Connectivity: C3 MST R1 with PERC S100 (Embedded SATA Software RAID)
- RAID Controller: PERC S300 Internal Software Controller, 3Gb/s
- Hard Drives: 2x 500GB, SATA, 3.5-inch, 7.2K RPM Hard Drives
- Optical Drives: 16X DVD-ROM Drive SATA
- Network Adapter: Dual Intel, 1Gbps, PCI Express with SNTP and DMI2 support
- Monitor: 22”LCD HAS Wide Monitor, VGA/ DVI Inputs
- Licenses: Windows Server 2008, 5 CALs

1.9 Minimum Software Requirements:

1. The Security Management System (SMS) software shall be design specifically for Prison Security Management Applications, shall have a proven track record in the security industry, and shall be an Off-the-shelf package available through a distributor network. The off-the–shelf software shall be programmed and tailored to the specified functions and features described herein and as indicated on the accompanying drawings.

2. The software shall convey and accurate floor plan of all areas that require display on the VDU. The software shall utilize the maximum resolution and colours of the SVGA monitor to enhance and simplify the displayed control and status information. Fast orientation and ergonomics will be the goal of the graphic displays.

3. The software shall provide integrated Biometric (Fingerprint) log-on security functionality with security level protection for all Mouse driven operator workstations. The Biometric (Finger print) logon facility shall be capable of providing a one too many search algorithm to confirm operator credentials, without the need for entering user details or the swiping of a personal identification card.

4. There shall be a minimum of ninety nine (99) levels of access, and shall be expandable.

5. The software shall provide a user database within the Management workstation. The database shall support a minimum of two thousand (2000) users.

6. The software shall provide on-line utilities accessed through the Management workstation menu structure. These utilities shall provided the system supervisor with the ability to edit and update required data bases, system operating variable, report configuration and generation, alarm tags and point descriptions, etc. These utilities shall be protected by security levels and Biometric Access.

7. All software licenses shall be transferred to the Owner at completion of the project. This shall include but not be limited to all original installation disks, software manuals, equipment manuals, etc. All project specific applications software shall be transferred at the end of warranty period.

1.10 Spares Holding:

The tenderer should allow for the following minimum spares holding:

a. One (1) SVGA 22" LCD monitor as specified under hardware section of the specification. Packed in its original packaging. This shall include, power cords and interconnecting cables.

b. One (1) fully equipped Workstation compliant with Clause 1.81 of the specification shall be provided, which shall be capable of replacing any workstation in the facility with the exception of the servers. This shall include; power cords and all required interconnecting cables.

This also includes all the software packages required to operate the facility. When one of the workstations fails, an exchange of computers must ensure that the system is immediately on line and active.

c. The equipment supplied under this section shall be fully supported and maintained locally.

1.11 Operator Visual Display Units

1.11.1 General

The SMS system offered shall be capable of providing a multiple operator workstation environment, which may be configured for full or selective operational & functional monitoring and control of select areas and functions.

Operator workstations shall be located as indicated in the tender drawings issued.

The operator workstations shall operate in both text and graphics based display. Any operator workstation enabled via the Biometric logon system shall be capable of controlling any area within the facility providing the respective operator is authorized to do so.

The operator workstation shall also be capable of implementing changes to the system configuration and parameters, provided the operator has the necessary administration rights.

Entries, deletions or modifications to the configuration shall be possible via the operator workstation VDU/Keyboard without loss of, or degradation to, any other system functionality.

The following workstation functions shall be possible:

- Displaying point status information.
- Manually initiating control commands.
- Displaying system events and alarms.
- Displaying staff, visitor and inmate photographs for positive identification.
- Enrolling and verifying staff, visitor and inmate fingerprints. (Visitation Management module)
- Assigning operator access levels.
- Altering time schedules and creating new time schedules.
- Assigning or modifying time schedules for automatic operation of monitored doors/gates and redirection of duress alarms and indicators appropriate to the user's building/department/etc.
- Overriding time controlled functions, momentarily, to allow operator control of doors/gates/and the like.
- Altering existing or assigning new descriptions or actions.
- Displaying status of all alarm sectors within the user's areas.
- Remotely operate doors/gates within their restricted areas.
- Displaying all appropriate building activities.
- Performing on-line backup copies of complete system without any degradation in the overall system performance.
- Displaying building alarms including fire alarms, gas/vapour sensor alarms, duress push buttons, etc.
- Enable the viewing of Sub-system status icons to be enabled or disabled through a built in menu structure.

All of the above shall be restricted by user level based on the finger print access to the operator workstation.

1.11.2 Monitors

All operator workstations shall be of robust construction, ergonomically designed to minimize operator fatigue and conform to the following minimum requirements:

- Screen: An effective viewing screen size of 22".
- Character set: ASCII with near letter quality fonts with crisp, fully formed characters.
- Contrast: Sufficient brightness and contrast to be easily readable by an operator with average vision, but not to cause burn-in of fixed display on screen. Screen saver functionality shall be provided to prevent burn-in.
- Mounting: Semi-sunken mounting at 45º in an industrial frame complete with cooling fan and intercom console.
- Power: 230 VAC 50 Hz.

1.11.3 Keyboards

Keyboards shall be supplied with all workstations, however shall only be used for commissioning and maintenance purposes. All operator functions shall be performed by means of an optical mouse, with system screens being designed so as to require the minimum operator action. Functions such as audio system Push to talk, volume up and down control etc shall be possible by means of function keys on the SMS workstation.

1.11.4 Printer

A high quality Inkjet printer shall be supplied, installed and commissioned as part of this contract, for use with the management workstation in order to generate user defined management reports.

The following shall be included:

- Paper feed: Page feed capable of accepting paper at least up to 242 mm (A4) wide. Single page paper shall be used to allow users to print out historical events and system activity.

- Character set: ASCII & Graphics.
- Print speed: Minimum of 150 characters per second at 10 cpi.
- Print type: Ink jet type using continuous A4 fan fold paper handling.
- Ink Storage: Ink cartridge, including 2 spare cartridges/printer.
- Print direction: Bi-directional in text mode.
- Pitch: User selectable (i.e. 10, 12 or 15).
- Print colour: Black on white paper.

The printer shall incorporate a visible control panel with LED indication for power on, paper out and ready.

The printer shall be installed and configured into the Management workstation to be installed within the Central Control Room.

The printer shall be supplied with both power and data cables of suitable length to suit the location. In addition, the printer shall be set up complete with one full box of paper and two spare ink cartridges each.

1.11.5 Mouse

All mouse devices shall be optical of robust construction and suitably secured by an interconnecting cable.

1.11.6 Networking

Each SMS workstation installed on the security LAN shall be capable of monitoring and reporting the current status of all workstations on the network.

Should communications between workstations or control equipment be disrupted, an alarm shall be generated at the Central Control Room Operator workstations to alert the operators of the failure within the communications network.

Alarms generated shall be displayed at the operator stations, while updating the system database with the Time, Date and relevant workstation detail.

Failure of any operator workstation shall not prevent communication between any other workstation or Distributed control modules and their associated devices.

1.12 Software

1.12.1 General

Software shall be fully proven prior to being supplied, installed, tested and commissioned.

A list of reference sites at which the system software has been installed and operational at the date of the closing of this tender shall be provided.

The operator interface software shall incorporate English language descriptions and messages using both text based menus and graphical/icon displays. All configurations (e.g. entering of alarm response properties, adjusting time schedules, user data, etc) shall be performed on-line without effecting the operation of the overall system.

Selective access to different operator functions shall be configured based on an operator's user level. User levels shall be determined from the Biometric verification each time an operator logs on to a workstation.

After any predefined period, if no operator activity has occurred at the operator workstations, that station shall automatically request Biometric verification failing which the station shall log off.

The time period before automatic logging off of workstations shall be user configurable, and shall be determined during commissioning of the system, in liaison with the Engineer.

1.12.2 Operating System

The operating system shall be a recognized and widely accepted standard operating system that shall suit the requirements of the system to be installed. The operating system shall be a real time multi-user/multi-tasking system such as Windows 7.

The operating system shall have proven and demonstrated reliable operation in the security environment.

Facilities shall be provided to store all programs on site and include all equipment necessary to backup and reload all system programs, including the operating system with all user specific system parameters.

1.12.3 System Access

Operators shall be required to "log on" to operator workstations using the finger print reader provided at each operator station before being able to access the system or user information, reset alarms or access any other system functions.

Access to all workstations shall be limited through allocation of access levels.

A minimum of 2000 users and 99 User levels shall be available. Only users allocated with a user level of 99 shall be capable of the assignment and changing of passwords to all levels.

Each operator shall be allowed to access different operator commands and functions, and view certain individually assigned events, menus and functions based on their assigned user level.

1.12.4 Scheduling

The SMS system shall have the ability to configure schedules which do not restrict the user to pre-determined times, dates or access levels. Access to and editing of these schedules shall be possible via the Management workstation.

The following schedules shall be configurable:

1. Automated Public Address Announcements.
2. Operator station Access times.
3. Designated Alarm priority changes.
4. Automated door locking/unlocking.
5. Cell and Passage lighting control.

1.13 Archiving Historical Data

1.13.1 General

Archiving of historical data shall take place automatically according to a configurable time frame, which shall be set via the Management workstation. The archived files shall be stored on the Raid 1 servers situated in the Central Control Room equipment rack. The system shall be capable of storing archived history files for a minimum period of 12 months.

Archived history files shall be read directly from the current or archived databases, without terminating or suspending the logging of current events.

1.13.2 Overwriting

The SMS software shall display an alarm to system operators warning of the imminent loss of archived data once the available disk space becomes full. The alarm shall occur with sufficient margin to allow the systems operator to execute a manual history file dump to the removable storage medium, if required (normally 80%). The percentage alarm set point shall be variable by the highest user level.

1.13.3 System Logging

The server workstations shall be capable of logging the following data:

Event related data:

Item	Database Fields
1	Time and Date Stamp
2	Equipment Type
3	Control Area
4	Equipment Designation
5	Equipment Location
6	Alarm/Event Type
7	Alarm/Event Status
8	Responsible Operator
9	Operator Workstation Name
10	Control Area
11	Alarm/Event Priority

Logged Events/Alarms:

Item	Intercom Events/Alarms
1.1	Intercom Station Call in
1.2	Intercom Station Activated
1.3	Intercom Station I/O Failure
1.4	Intercom Station Tamper Alarm
1.5	Intercom Station Threshold Alarm
1.6	Intercom Station Fault
1.7	Intercom Call-in Transferred
1.8	Intercom Call-in Unanswered
1.9	Intercom Station Isolated
1.10	Intercom Station Isolated warning
1.11	Intercom System Hardware Failure
1.12	Intercom System Communication Failure

1.13	Intercom Alarm/Failure Acknowledged
1.14	Intercom System Call Central Command
1.15	Intercom System Call Movement Command
Item	CCTV Events/Alarms
2.1	CCTV Camera Activated
2.2	CCTV PTZ Preset Edited
2.3	CCTV Sequence Selected
2.4	CCTV Sequence Edited
2.5	CCTV System Hardware Failure
2.6	CCTV System Communication Failure
2.7	CCTV Alarm/Failure Acknowledged

Item	DVR Events/Alarms
3.1	DVR Channel Record Command
3.2	DVR Channel Halt Record Command
3.3	DVR System Hardware Failure
3.4	DVR System Communication Failure
3.5	DVR Alarm/Failure Acknowledged

Item	Door Events/Alarms
2.1	Door Open Command
2.2	Door Closed Command
2.3	Door Fault on Closing
2.4	Door Fault on Opening
2.5	Door Forced Open Manually
2.6	Door Open outside of limits
2.7	Door Open for extended period
2.8	Door Control module Communication Failure
2.9	Door DPS Opened
2.10	Door DPS Closed
2.11	Door Interlock Override Command

2.12	Door Group Activated
2.13	Door Group Edited
2.14	Door Emergency Release Activated
2.15	Door Control System Hardware Failure
2.16	Door Control System Communication Failure
2.17	Door Alarm/Failure Acknowledged

Item	Gate Events/Alarms
5.1	Gate Open Command
5.2	Gate Stop Command
5.3	Gate Close Command
5.4	Gate Fault on Closing
5.5	Gate Fault on Opening
5.6	Gate Forced Open Manually
5.7	Gate Open outside of limits
5.8	Gate Open for extended period
5.9	Gate Control module Communication Failure
5.10	Gate Alarm/Failure Acknowledged

Item	Lighting Events/Alarms
6.1	Lighting Zone Activated
6.2	Lighting Zone De-activated
6.3	Lighting Zone Scheduled Reset

Item	Public Address Events/Alarms
7.1	Public Address Zone Manual Activation
7.2	Public Address Zone Scheduled Activation

Item	Intrusion Events/Alarms
8.1	Intrusion Zone Activated

8.2	Intrusion Zone Alarm Acknowledged

Item	Panic Button Events/Alarms
9.1	Panic Button Activated
9.2	Panic Button Activation Acknowledged

Item	UPS Events/Alarms
10.1	UPS Mains Failure Alarm
10.2	UPS Load on Bypass
10.3	UPS Battery Low
10.4	UPS Battery Failure
10.5	UPS Load not protected
10.6	UPS Surge Arrestor Failure
10.7	UPS Communication Failure
10.8	UPS Alarm/Failure Acknowledged

Item	Air System Events/Alarms
11.1	AIR System Compressor Off
11.2	AIR System Maintenance Request
11.3	Air System Zone Pressure Test Failure
11.4	Air System Zone Low Pressure Alarm
11.5	Air System Dryer Off
11.6	Air System Dryer Failure
11.7	Air System Compressor On Load
11.8	Air System UPS Alarm/Failure Acknowledged

Item	Emergency Air System Events/Alarms
12.1	Emergency Air System Zone Low Pressure Alarm
12.2	Emergency Air System Zone Low Pressure Alarm Acknowledged

Item	SMS Events/Alarms
13.1	New Operator Enrollment Successful
13.2	New Operator Enrollment Failed
13.3	Operator Details Edited
13.4	Operator Details Deleted
13.5	Workstation Logon Successful
13.6	Workstation Logon Failed
13.7	Workstation Unauthorized Access Attempted
13.8	Workstation Manual Logoff
13.9	Workstation Automatic Logoff
13.10	Workstation Inhibited
13.11	Workstation Re-instated
13.14	Workstation Online
13.15	Workstation Offline
13.16	Workstation Communication Failure
13.17	Workstation Alarm/Failure Acknowledge

1.13.4 System Reporting

The SMS shall be capable of performing SQL queries to the current or archived databases on the server workstations, format the data into customized reports which shall allow for the following:

- Display of all relevant information on any individual alarm point including alarm point identification by device number and alarm point status.
- Display all alarm points in the system in alarm or normal condition, as a single log.
- Display all emergency procedures applicable to any alarm type with corresponding alarm response actions and locations, per alarm device.

Reporting details shall include:

- Alarm point status
- Alarm count per device.
- Alarm activity over a time period, selected by time and date.

- Display of selected alarm transactions based on alarm type and a calendar / time period.
- Display system operators login/out history
- Display all operator commands entered by any or all operators based on time/calendar interval.

1.14 System Status

The SMS shall provide a menu option which, when selected, allows the system to display or print a list of current alarms, faults and conditions including the current fault conditions relating to SMS workstations, Distributes control modules, sub-system equipment hardware and associated devices.

In graphical display mode the system shall display maps of each building complete with all internal levels and shall indicate all systems equipment status (i.e. locked/unlocked; open/closed; secure/access; isolated/active; alarm; tamper etc).

1.15 Current Alarm Window

The system shall provide an efficient and reliable alarm handling procedure and shall include both audio and visual annunciation, logging to the database and recording of the history file the device description, point description, location, time and date the alarm occurred.

The system software shall have the ability to route only selected alarms to specific operator workstations, allowing different locations or applications to be segregated on a building or system basis.

All systems activity shall be presented to ensure proper actions have been taken and that no alarm is left unattended for any lengthy period. Alarms, which have been acknowledged, and not cleared/reset shall be clearly distinguishable.

Upon occurrence of an alarm(s) a user configurable audible tone shall sound at the operator workstation(s) and display an indication of the incoming alarm together with its priority.

If there are additional alarms to acknowledge the operator's station shall continue to sound the appropriate alarm tone, display the number of alarms waiting and identify the highest priority alarm.

The first alarm displayed shall be the highest priority alarm followed by the next highest priority alarm, etc.

All alarms are required to be separately acknowledged by the operator, by means of the mouse provided to acknowledge and reset each alarm separately.

Each time new alarms are created the system shall restack the alarms so the operator sees them in order of priority.

The system shall also have an alarm/event status display available to the operator at all times on the operator's station.

The display shall be a real-time dynamic display of alarms in the active state, or system component failures.

An audit trail shall be used to log the actions taken by all system operators in response to an alarm. The audit trail shall note:

- When the alarm was activated.
- When the alarm was acknowledged.
- Who acknowledged the alarm.
- When the alarm was restored.

The system shall record every user command, acknowledgment and log every operator login.

These transactions shall be routed to the history database.

Any alarm point which has been suppressed/inhibited by the operator shall on expiry of the time zone, or when unsuppressed by the operator, generate an alarm if the alarm point is in the "active" state. The report to the operator terminal shall be the same as described above.

Each alarm point shall have the facility for a description of the alarm occurring. A

Comprehensive outline for operator instructions, detailing all response actions shall be provided for all alarms.

1.16 Graphical Display

The SMS shall support a minimum of 150 colour maps for the purpose of displaying the location and real time status of any SMS input or output.

Graphical maps to be included within the initial configuration are to show in detail the following areas:

- Site plan showing all buildings and locations of all alarm points and operator workstations.
- A plan of each accommodation unit and building.
- All buildings devices/status/alarms and the like.
- All building tamper, communications, power and the like devices/status/alarms and the like.
- Other maps as required to clearly display all alarm input within buildings, or an external equipment cubicle locations.

Each site map shall be provided with a site plan key, which shall be common to all maps and situated in the same position. The key shall provide a means for the operator to quickly navigate through the entire facility without the need to use standard navigation buttons or the main site map.

All device location and statuses shall be detailed on each map and coloured accordingly for ease of recognition of both the device type and real time status.

Text messaging identifying the device type, designation and alarm status shall be available in a “mouse over” or “windows hint” structure to minimize text on individual maps.

All text descriptors shall be approved by the Engineer prior to final acceptance. Liaise with the Engineer when programming these maps and other alarm/response descriptions.

Function key descriptions shall also be displayed as mouse over or windows hints.

Graphical map displays shall be of high resolution to enable accurate images to be represented. The configuration software shall provide a complete graphical design environment in order to design/edit building and site maps. A standard icon library shall be available to the designer in a window environment to enable efficient editing of existing maps by means of dragging and dropping equipment icons onto maps.

The system shall allow maps to be linked by means of navigation buttons to allow operators to "zoom" in or out to display either additional detail or an overall map.

Point status and locations shall be clearly displayed using colour-coded icons. All icons shall display real time status of each point with continuous updates being provided to any dynamic screen display.

Updates shall occur every 1 second or less. Icons shall be easily duplicated from a library of standard symbols at the configuration stage of developing the graphics.

1.17 Security Management Functions

1.17.1 Configuration

The SMS shall consist of a multiple screen representation of the entire facility, which shall contain all of the necessary icons to control all security sub system equipment and devices situated throughout the prison. All icons shall be activated with the use of a mouse. All icons and status indicators shall be a minimum of 5mm in diameter. All symbols shall provide status by color and/or associated text.

1.17.2 Global Function Operations:

Global function icons shall be located at the bottom of each graphic screen in the form of a footer window, which shall be common to all area maps. These icons, if active, shall control the global functions for the entire facility.

1.17.2.1 System Control

Activating this icon shall cause the system to switch to the system control screen. The System Control screen shall provide a complete system diagnostic window for all sub-system components and communication systems within the entire facility.

The diagnostic information shall include but not be limited to the following:

1. Compressor Status:
    a. Low Oil Pressure
    b. Compressor Tripped
    c. Air Dryer Failure
2. Air Reticulation System:
    a. Air Reticulation integrity per zone
    b. Operating Air pressure in KPa
    c. Normal Air pressure status per zone
    d. Emergency Air pressure status per zone
3. UPS System (Per Zone):
    a. Load on Bypass
    b. Load not protected
    c. Mains Failure
    d. Battery Fault
    e. Battery Low
    f. Surge Arrestor Failure
4. Control Hardware Status (Per Zone):
    a. TCP/IP communication Failure
    b. Control Network communication Failure
    c. Device Network communication Failure
    d. I/O Device Failure

e. Communication Redundancy Integrity

f. CCTV Matrix communication Alarm

5. Perimeter Protection System (Per Zone):

    a. Taut Wire Alarm

    b. Video Motion Detection Alarm

6. Door position switch violation alarm per DPS
7. Controlled door security violation alarm per door
8. Fire door security violation alarm per door
9. Panic Button activated alarm per Panic Button
10. Intercom Call In Failure per Intercom
11. Operator Log On Violation

Where applicable all alarm conditions shall allow for operator acknowledgement and automatic selection of the alarmed zone layout screen.

1.17.2.2 Site Plan

The site plan shall consist of an interactive miniature layout of the entire facility, and shall be situated on the bottom Right hand side of each operator screen.

The site plan shall provide the operator with a quick method to access an individual area to monitor and / or control.

The site plan shall also indicate critical operational information to the operator, which shall include but not be limited to the following:

1. Fire Doors Unsecured
2. Sally port Doors Unsecured
3. Local Control Room Logon Status
4. Local Control Room Call In
5. Local Control Room Communication Alarm

1.17.2.3 Volume Up

Activating and maintaining this icon shall result in an increase in the operator console speaker volume. The icon shall change status to RED to indicate activation of this function.

1.17.2.4 Volume Down

Activating and maintaining this icon shall result in a decrease in the operator console speaker volume. The icon shall change status to RED to indicate activation of this function.

1.17.2.5 Select

Activating this icon shall result in either the first audio call-in or the currently selected audio call-in in the Audio Call-in Queue to be answered. Upon answering the call, the call shall be removed from the Audio Call In queue on all workstations.

1.17.2.6 Reset

Activating this icon shall result in either the first audio call in or the currently selected audio call-in in the Audio Call-in Queue to be reset. Upon resetting the call, the call shall be removed from the Audio Call In queue on all workstations.

1.17.2.7 Push To Talk

Activating and maintaining this icon shall results in the PTT function being activated within the audio control hardware. Releasing the icon resets the PTT function.

1.17.2.8 All Page

Activating the ALL PAGE icon on the footer window shall activate all Public Address station within the immediate area of control, and in the case of a Central Operator shall activate all stations within the facility. The PTT function shall be enabled and remain enabled until the ALL PAGE icon is selected again in which case the stations are de-activated and the PTT released.

The ALL PAGE icon shall change colour when active to clearly indicate the current status.

1.17.2.9 Call Central/Movement

Each local operator workstation's footer window shall contain a "Call Central" and a "Call Movement" icon. When selected the SMS shall generate

a high priority call-in at the Central or Movement Control operator workstations. Central and Movement control room operators shall respond to these call-ins in the same manner as with a normal intercom station call request.

Movement Control workstations shall be equipped with "Call Central" functionality only.

1.17.2.10 Audio Call In Queue

The SMS footer window shall contain an Audio Call-in queue facility into which audio call requests are entered on a first in first out (FIFO) basis.

Upon receipt of an audio call-in from any intercom station in the facility, the call-in detail listing the control area, equipment designation and the specific location of the calling intercom station shall be entered into a FIFO queue.

The call-in priority of each Intercom station within the facility shall be individually configurable within the SMS, and station priority shall take preference over the FIFO queue. Intercom station call requests of higher priority e.g. Control room call-in requests shall be entered into the top of the queue.

The following methods of answering calls-ins shall be possible:

1. Highlighting the desired call-in in the Audio queue and clicking on the "Select" icon in the footer window.

2. Clicking repeatedly on the "Select" icon in the footer window, which shall automatically answer the oldest entry in the Audio queue.

3. Double clicking on any entry in the Audio queue.

Any of the above-mentioned methods of answering a call-in shall reset the currently selected intercom station and enable the selected station as well as simultaneously removing the entry from the Audio queue on all workstations.

When the local operator workstations are logged on, call-ins from the relevant local area shall be directed to the local workstation. In the event that the call is not answered within thirty seconds, the call shall be forwarded to the Central Control room workstations. Call-ins from local areas in which a local operator is not logged in, shall be forwarded immediately to the Central Control room operators.

1.17.2.11 Fault Queue

The SMS footer window shall contain a Fault queue facility into which all security sub-system or control system faults are entered in order of priority.

Upon receipt of any security sub-system or control system fault, the relevant fault detail including the control area, equipment designation and the specific location of the fault shall be entered into the Fault queue.

The Fault queue is intended to provide a quick reference to the system operator of current alarms, and is intended to replace functionality of the Current Alarm window described in the specification.

Faults may be dealt with in the following ways:

a. By right clicking on a specific fault in the queue, the operator shall be presented with an "Acknowledge" option. Clicking on the Acknowledge option shall enter the acknowledgement into the event recording system and remove the fault from the queue.

b. By double clicking on a specific fault in the queue, the appropriate area map shall be displayed with the faulty equipment control icon clearly visible. The equipment icon shall display the fault detail in a mouse-over or "hint" fashion. Right clicking on relevant equipment icon shall present the operator with an "Acknowledge" option. Clicking on the Acknowledge option shall enter the acknowledgement into the event recording system and remove the fault from the queue.

Local operator workstations shall display alarms and faults related to the immediate area of control only. Central operator workstations shall display all current alarms within the entire facility.

1.17.2.12 Synchronized Clock System

All operator workstations footer windows shall contain a synchronized digital clock, which indicates the Date and Time in 24 Hour mode. The accuracy of the synchronized digital clock system shall be within +- one (1) minute within a thirty (30) day period, and shall be synchronized with the management workstation within the central control room each hour on the hour.

1.17.2.13 Operator Logon Details

The SMS footer window shall contain the detail of the currently logged on operator including full name and authorized user level.

1.17.3 Locking Operations:

1.17.3.1 Door Position status (Monitored Only):

There shall be a status icon for each monitored door to indicate the position of the door. The status icon shall illuminate red when the door is unsecured and shall be green when the door is secure.

Each DPS icon shall provide mouse over or “hint” fashion detail of fault conditions relating to the equipment element as well as indicating the equipment designation.

A right mouse click over any icon shall provide the operator with an option to acknowledge an alarm condition as well as to view the engineering properties of the element provided the necessary user level is active.

1.17.3.2 Unlock Icon (Swing Door):

There shall be a single control icon with visual status indication for each controlled swing door lock. Activating the UNLOCK command shall apply power to the lock and activate the UNLOCK control cycle. The associated status icon shall indicate red when the incorporated lock status switch indicates an unsecured state and green when the lock is secured. Each door icon shall provide mouse over or “hint” fashion detail of fault conditions relating to the door.

A right mouse click over any icon shall provide the operator with an options to acknowledge an alarm condition, to inhibit a door open command, or to view the engineering properties of the element provided the necessary user level is active. Inhibiting a door open command shall change the icon colour to blue.

1.17.3.3 Unlock / Lock Icon (Sliding & Fire Doors):

There shall be a single control icon with visual status indication for each controlled sliding door control mechanism. Activating the UNLOCK/LOCK icon shall either activate the UNLOCK cycle or the LOCK CYCLE of the mechanism in a toggle fashion. The associated status icon shall illuminate red when the door is unsecured and green when the lock is secured. Activation of this icon whilst the associated door is in travel shall cause the door to instantly change its direction of travel. Each door icon shall provide mouse over or “hint” fashion detail of fault conditions relating to the door.

A right mouse click over any icon shall provide the operator with an options to acknowledge an alarm condition, to inhibit a door open command, or to view the engineering properties of the element provided the necessary user level is active. Inhibiting a door open command shall change the icon colour to blue.

1.17.3.4 Open / Close / Stop Icons (Sliding gates):

There shall be three individual control icons with visual status indication for each controlled sliding gate. Activating the OPEN icon shall activate the OPEN cycle of the controlled device Activating the CLOSE icon shall activate the CLOSE cycle of the controlled device. Activating the STOP icon while the device is in the OPEN cycle or CLOSE cycle shall STOP the device. The associated status icon shall illuminate red when the locking device is unsecured and shall be green when the locking device is secured.

Each gate icon shall provide mouse over or “hint” fashion detail of fault conditions relating to the door.

A right mouse click over any icon shall provide the operator with an option to acknowledge an alarm condition or to view the engineering properties of the element provided the necessary user level is active.

1.17.3.5 Emergency release:

An Emergency release icon shall be provided for each housing unit day room area, which shall be used to initiate an automated opening sequence for Cell and Exercise yard doors. The opening sequence shall be configurable within the SMS in order to provide the most efficient opening sequence.
Activating this icon shall cause a pop-up window to appear on top of the graphically displayed area. Located within this window shall be text explaining to the operator that the activation of this function shall result in all controlled doors in the corresponding area to be released under an emergency procedure. Also located within this window there shall be three icons namely “Open”, “Close” and “Cancel”. Activating the icon with the text “Open” text will activate the emergency open routine. Activating the icon with the text “Close” text will activate result in the same doors to simultaneously close. Activating the icon with the text “Cancel” shall remove the pop-up window and resume normal operation.

Once an emergency release routine has been activated the doors in the controlled area shall open and indicate an emergency condition by flashing the affected door icons in RED. The activation of the emergency close routine shall return the icon status to normal.

1.17.3.6 Interlock Group Status

Activating a door lock icon that is part of an interlocked group of doors of which one or more doors are currently open, shall cause a pop-up window to appear on top of the graphically displayed area to indicate to the operator that an interlocked door is currently open and that the “Interlock Override” function should be activated to open the door.

Right clicking on the door icon shall provide the operator with an interlock lock group option, which when selected shall indicate each door contained in the relevant interlock group.

1.17.3.7 Interlock Override

Activating this icon shall enable the operator to override an interlocked door. The override function shall only remain active for 10 seconds. Activating a door control icon while override is active shall cause the associated door to unlock or open. When the override timeout limit is reached, the system shall return to normal operation.

During the active 10s period the Icon shall Flash RED to indicate activity.

1.17.3.8 Group Assign Icon

Activating this icon shall result in the door status icons of all doors in the corresponding Cell area to turn White. By toggling the door control icon whilst in the "Group Assign" mode shall toggle the door icon colour from White to Grey. A White icon shall indicate that the door is included in the controlled group, whilst a Grey icon indicates that it is not included in the group.

Upon activating the Group Assign icon for a second time the system shall return to a normal state and set the controlled door group into memory. Re-activation of the Group Assign icon shall cause the door control icons to indicate there current group assign status from memory.

1.17.3.9 Group Release:

Activating this icon shall cause a pop-up window to appear on top of the graphically displayed area. Located within this window shall be three icons namely "Open", "Close" and "Cancel". Activating the icon with the text "Open" text will result in the doors included in the Group Assign memory to Open. Activating the icon with the text "Close" text will result in the doors included in the Group Assign memory to Close. Activating the icon with the text "Cancel" shall remove the pop-up window and resume normal operation.

1.17.4 Intercom Operations

1.17.4.1 Audio Control – Staff/Cell Intercom Icon:

The SMS shall provide a control icon with visual status indication for each intercom station within the entire facility.

The icons shall be used to initiate or terminate an audio channel between the relevant control room operator's audio console and the selected intercom station.

Each Intercom station icon shall provide mouse over or "hint" fashion detail of fault conditions relating to the station as well as indicating the equipment designation.

The alarm detail displayed by the "hint" function shall include:

- Intercom station Tamper alarm
- Intercom station Threshold alarm
- Intercom station I/O alarm
- Intercom station Communications alarm

All alarm conditions shall be presented to the operator within the Fault queue as described in the specification.

A right mouse click over any icon shall provide the operator with an option to acknowledge an alarm condition, to inhibit an intercom station, or to view the engineering properties of the element provided the necessary user level is active. Inhibiting an intercom station shall change the icon colour to blue.

a. Intercom Station Call Up:

Activating a staff or inmate station icon shall open a talk path between the operator and the associated intercom station. The associated status icon shall illuminate yellow to indicate an active channel.

Activating the staff station icon a second time shall close the talk path and the status icon shall extinguish.

b. Staff Station Call-In:

Upon activation of a Staff or Cell station call-in button located on the intercom station faceplate, the associated status icon shall illuminate and flash between yellow and gray with an audible tone. Activating the associated intercom station icon shall open a talk path between the operator and the staff station. The status icon shall illuminate yellow and the audible tone shall silence. Once complete, activating of the staff station icon a second time shall close the talk path and the associated status icon shall extinguish.

c. Automatic termination of an audio channel:

Should multiple audio call in's be received by the local operator, the operator shall only be required to select each audio icon once. The second icon selected shall initiate an audio channel to the appropriate intercom station and initiate an automatic de-select command to the previous channel.

d. Delayed Call-In:

Upon activation of a Staff or Cell station call-in button on an intercom station which falls under the control of a local control workstation, provided the particular operator is logged in, the call shall at first be routed to the local operator. If the local operator fails to respond to a call in within 60 seconds, the call is automatically routed to central control. This event is to be logged to the event recording system.

d. Audio Queue:

An Audio Call-in queue facility shall be provided as an integrated function of the SMS system.

1.17.5 Closed Circuit Television (C.C.T.V.) Operation:

1.17.5.1 C.C.T.V. Fixed Camera Select

The SMS shall provide a single control icon with visual status indication for each CCTV Fixed Camera within the entire facility.

Activating a camera icon shall cause the associated camera to be switched to the relevant operator's spot monitor via the IP Interface to the CCTV Virtual Matrix. By selecting another camera icon the spot monitor image shall change accordingly.

Camera to Monitor commands shall be configured within the SMS to determine the allocation of spot monitors to operator workstations.

Currently selected camera icons shall illuminate RED, whilst un-selected icons shall illuminate GREEN.

Each Camera icon shall provide mouse over or "hint" fashion detail of the camera designation.

A right mouse click over any icon shall provide the operator with an option to view the engineering properties of the element provided the necessary user level is active.

1.17.5.2 C.C.T.V. PTZ Camera Select

The SMS shall provide a single control icon with visual status indication for each CCTV PTZ Camera within the entire facility.

Activating a PTZ camera icon shall cause the associated camera to be switched to the relevant operator's spot monitor via the High Level Interface to the CCTV Matrix. By selecting any other camera icon the spot monitor image shall change accordingly.

Camera to Monitor commands shall be configured within the SMS to determine the allocation of spot monitors to operator workstations.

Currently selected PTZ camera icons shall illuminate RED, whilst un-selected icons shall illuminate PURPLE.

Each PTZ Camera icon shall provide mouse over or "hint" fashion detail of the camera designation.

A right mouse click over any icon shall provide the operator with an option to view the engineering properties of the element provided the necessary user level is active.

1.17.5.3 C.C.T.V. PTZ Control

Once a PTZ camera icon has been selected by the operator, the SMS shall provide a pop-up control window, which shall allow the following PTZ control functions:

- Pan Left
- Pan Right
- Tilt Up
- Tilt Down
- Simultaneous Pan Left, Tilt Up
- Simultaneous Pan Right, Tilt Up
- Simultaneous Pan Left, Tilt Down
- Simultaneous Pan Right, Tilt Down
- Zoom In
- Zoom Out
- Continuous rotate Left
- Continuous rotate Right
- Rotate Stop
- Preset Position Select
- Guard tour initiate

1.17.5.4 C.C.T.V. PTZ Preset Save

The SMS shall provide the operator with a menu option which shall initiate a pop-up control window, which shall allow the following PTZ control functions:

- PTZ Camera Select (1-n)
- PTZ Preset Select (1-99)
- Pan Left
- Pan Right
- Tilt Up
- Tilt Down
- Simultaneous Pan Left, Tilt Up
- Simultaneous Pan Right, Tilt Up
- Simultaneous Pan Left, Tilt Down
- Simultaneous Pan Right, Tilt Down
- Zoom In
- Zoom Out
- PTZ Preset Store Command
- PTZ Preset Load Command

The SMS shall be able to assign a specific PTZ Preset position to a standard fixed camera icon. The operator shall be able to click on a fixed camera icon, which shall load a PTZ preset position onto the appropriate spot monitor.

1.17.5.5 Sequence to Monitor Select

The SMS shall provide a single control icon with visual status indication for each Monitor within the individual control rooms.

A control room layout map shall be configured within the SMS, indicating the physical layout of the control desk and the CCTV monitors for the relevant SMS workstation.

The Monitor icon shall illuminate RED if a CCTV sequence has not been assigned to a specific monitor, and GREEN when a logical sequence has been assigned. The sequence number and description shall be displayed within the Monitor icon when a logical sequence has been assigned.

The operator shall be able to select the desired camera sequence by means of a Right mouse key function on the monitor icon.

Camera sequences may be assigned to any Monitor in the facility including the spot monitors if required, however the manual selection of a camera image shall automatically override the sequence allocation.

1.17.5.6 Perimeter Detection - Black Screen Technology

The SMS shall provide integrated Black screen technology, which shall enable the automatic selection of relevant Perimeter Cameras to be allocated to Video Wall Monitors in the case of a Perimeter Detection alarm.

The SMS through its high level interface to the Perimeter Detection, CCTV and DVR sub-system hardware shall make logical selections of camera images to the dedicated video wall monitors situated in the Central Control room.

Once a Perimeter alarm is triggered, the relevant zone fixed camera image shall be switched to the dedicated monitor along with the zone cameras on each side of the alarm zone.

The technology is required to ensure that all Perimeter alarm conditions are brought to the attention of the Central Control room operators immediately, and to present them with the necessary information to respond to the event.

The monitors to the left and right of the ALARM ZONE monitor ensure that an offender shall be visible should he/she move to the left or right of the immediate alarm zone. The PTZ preset position allows the operator to immediately view the alarm zone, and to follow the offender via the PTZ control functions.

1.17.6 Lighting and small power operations:

1.17.6.1 Cell Light Control Icon:

The SMS shall provide a control icon with visual status indication for each Cell light within the entire facility.

The icons shall be used to toggle the state of the Cell light. The status icon shall illuminate yellow when the light is on and shall be gray when the light off.

Each Cell light icon shall provide mouse over or “hint” fashion detail of light status as indicating the equipment designation.

A right mouse click over any icon shall provide the operator with an option to view the engineering properties of the element provided the necessary user level is active.

There shall be a single control icon with visual status indication within each cell on the graphical layout. The icon shall be used to toggle the cell light between the ON and OFF state. Central control operators shall be able to control any cell or day room lighting in the entire facility.

1.17.6.2 Day Room Bay Light Control Icon:

The SMS shall provide a control icon with visual status indication for the Day room high-bay lights for each housing units

The icons shall be used to toggle the state of the Day room lights. The status icon shall illuminate yellow when the lights are on and shall be gray when the lights are off.

1.18 Visitation Management Module

The Access Control hardware provided shall support the Visitation Management System, which shall be provided as a fully integrated module of the Security Management System provided under this contract.

The Visitation Management System Module (VMS), shall provide for a fully integrated Biometric based Visitor, Staff and Inmate identification System providing the following components as a minimum:

1. Visit Booking
2. Visitor, Staff and Inmate Enrolment
3. Visitor, Staff and Inmate Verification
4. Visitor, Staff and Inmate location tracking
5. Visitation Management

6. Staff Management (Time & Attendance)

7. Integration to Security Management System

1.18.1 System Components

The base system shall consist of the following components, however shall be indefinitely expandable to provide additional Visitation points, Inmate and staff tracking points, as may be required.

1. Electrically actuated Turnstiles (Dual Direction), with an access control terminal mounted on each side (General or Visitors entrance gate).

2. Visitor Enrolment stations (General or Visitors entrance gate).

3. Visitor Verification stations (Contact and Non-Contact Visitation areas*).

4. Management Administration station (Administration building).

5. Admissions Enrolment/Admissions/Release Stations (Admissions building)

* The tenderer shall refer to the Bill of Quantities to determine the actual number of stations required, and shall provide all necessary hardware, software and accessories required for a fully functional system.

1.18.2 Component Description

1.18.2.1 Electrically Actuated Turnstiles (Full Height)

Full height bi-directional electrically activated turnstiles with a parallel 850mm bypass gate shall be mounted in passageways for the monitoring and control of Staff and Inmates in strategic areas of the Prison. The turnstiles shall be equipped with a combination card reader and fingerprint reader on both sides of the turnstile. The turnstiles shall be electrically released either by swiping an authorized card and confirming with a valid fingerprint, or manually activated by the relevant Operator Station.

1.18.2.2 Visitor Enrollment Station

The Visitor Enrollment Station shall consist of a dedicated PC workstation situated at the general or visitor's entrance. The station shall consist of a PC, fingerprint reader, Camera, adhesive label printer and a storage tray for temporary visitation cards.

The station shall be used to enroll visitor information into the system, and to print and issue a temporary visitation identification card to each visitor, which shall contain the visitor details with a bar code for database indexing.

1.18.2.3 Visitor Verification Station

Visitor Verification stations shall be installed in each visitation area e.g. Contact and Non-Contact visitation, and shall consist of a PC workstation and a fingerprint reader.

The station shall be used to verify a visitor's identity both upon entering and leaving the visitation area.

1.18.2.4 Management Administration Station

The Management station shall be installed within the Administration building, and shall consist of a PC workstation, fingerprint reader, Camera, LaserJet reporting printer and a Desktop Colour PVC identification card Printer.

The station shall be used to enroll staff members onto the system.

Staff members shall have their picture and fingerprints captured and shall be issued with a permanent staff access card, which shall be required to enter and leave the facility via the entrance turnstile.

1.18.3 System Description

In summary the objective of the system is to provide the following managerial functions within the facility:

a.) The management and tracking of staff.
b.) The management and verification of Visitors and the recording of visits to inmates.
c.) The management and verification of Inmates.

1.18.4 Typical Station Allocation

Station Nº	Station Type	Building Allocation	Primary Function
1	File Server	Administration	Central file server (RAID 5 configuration).
2	Enrolment	Entrance/Gatehouse	Enrolment of Visitors Issuing of photo passes Adding to visitor count Search and display red list for banned visitors Login of Visitors to facility

			Logout Visitors from facility
3	Verification	Contact Visitation	Positive identification of visitors in and out of Contact visitation and search prisoner list.
4	Verification	Non-Contact Visitation	Positive identification of visitors in and out of Non-Contact visitation and search prisoner list.
5	Administration/ Management	Administration	System Management System Support Maintenance of Red list Report Generation System enquiries Pre-booking of domestic, legal and official visitors. Enrolment of Staff
6	Admissions/ Enrolment	Admissions	Enrolment of Inmate

1.18.5 Installation Specifications

a.) Cameras to be wall mounted approx 1.8m from subject and above head height.

b.) If possible, natural daylight from behind camera provides the best illumination

c.) Plain or light coloured background (recommended –blue or light grey)

d.) Photographic strip lighting (white light illumination) to replace fluorescent strip lighting to eliminate yellow tones.

1.18.6 Environmental Conditions

The following environmental issues shall be taken into consideration:

Temperature

To avoid overheating of the PC's, each station shall be supplied with a ventilated under-counter cabinet, which shall be lockable to prevent tampering. The cabinet shall be mounted in such a way as to ensure adequate airflow, and not directly up against walls etc.

Humidity

The contractor shall ensure that the humidity shall be maintained within the manufacturer's specification, and controlled via the internal air conditioning.

The tenderer shall ensure the adequacy of the current air conditioning system, and make allowances to replace under rated units.

Anti-Static

Adequate measures shall be taken to discharge any possible static at installation points. An installation specific survey with a list of recommended protection measures shall be required from the contractor.

Power Supply

The system shall make use of a 240V AC source. The tenderer shall allow for a suitable uninterruptible power supply for each station capable of providing 35min of backup power.

1.18.7 Training

A comprehensive operator-training programme shall be provided, and shall cover all aspects of the Management system so as to provide first line local support to prison staff members both operational and managerial.

The training shall include the following topics as a minimum:

1.18.7.1 Software

- System overview
- Pre-booking Visits Procedure
- Visits Orders
- Logging onto the System
- Enrolment procedure, and the understanding of fingerprint technology
- Verification Points and Procedures (In and Out)
- Red List Notification
- Visits Notification Prisoner / Visitor
- Prisoner Enrolment
- Visitor Pass & ID Card Design
- System Maintenance
- Reporting and Enquiries

1.18.7.2 Hardware

- PC System
- Components and field replacements
- Access Control Terminals
- Printers & Print heads

1.18.7.3 Support

- Trouble Shooting Problems / Queries
- The Support Program and Support Procedures
- Support Communications
- Environmental Issues

2 DISTRIBUTED CONTROL SYSTEM

2.1 General

All Distributed control modules and associated hardware required to provide the alarm inputs, control outputs, access control, device monitoring and the like described in this document shall be included as part of this Contract.

The modules shall be designed to continually monitor all devices connected and supervise all general inputs (i.e. or alarm points) and cabling to control outputs.

As a minimum requirement, all inputs shall be "end of line resistor" monitored and provide indication of normal, alarm and tamper (open or short) conditions.

All inputs shall be continuously supervised for high or low impedance (using end of line resistors). Upon a change of this impedance an appropriate alarm shall be annunciated to the various devices (including operator's terminal, printer and history file).

All alarms generated in the field shall be received by the Distributed control modules, and shall generate an interrupt to signify to the system that an alarm has occurred, and report its status, which shall be annunciated to any or all devices such as operator stations, printers and the history file.

Various Distributed control modules shall be used dependant on the application, and as detailed below.

Any input throughout the system shall be able to be interlocked with any other input or output through software assignment of conditional logic.

It shall be possible to disable individual or groups of alarm inputs and control any output via any operator station.

During suppressed/inhibited mode, the alarm point wiring shall be monitored to detect any unauthorized tampering (i.e. tamper alarms shall be monitored 24 hours a day, every day).

The Distributed Control System shall consist of autonomous control systems located within each local control area. Each local control system shall be capable of utilizing multiple processing units to perform the application specific logic functions, as well as to provide system redundancy.

The failure or loss of any single door or I/O control device shall not hamper the operation of any other control device or processing unit, and shall not degrade the overall system response time as indicated in the System Performance Guidelines.

Each control system shall be capable of communicating in a peer-to-peer configuration over a communication network utilizing a non-proprietary, commercially available technology and open protocol.

The communication network shall be IP based directly to the point of installation, and shall not employ any non-standard or proprietary hardware or software. All door control modules in a local control zone (i.e. housing pod) shall be terminated at the relevant Ethernet Switch within the local area equipment cabinet, and run in either a point to point or bus Ethernet configuration.

The use of discreet multi-core cabling to each door to control door functions shall not be accepted as an alternative to a bus or point to point Ethernet topology.

2.2 System Components

a. All system modules shall share the same control language and programming structure, where applicable.

b. All system modules shall have built-in comprehensive self-test and self-diagnostic capabilities.

c. All system modules shall have built in status indication of power supply voltages and module processor healthy indication to show proper operation.

d. All 24 VDC system modules shall have on board voltage regulation for logic power supply.

e. All system modules shall have on board, auto-resetting over – current protection devices for the logic supply and field input circuits.

f. The system modules shall provide all necessary logic functions, timing functions, input points, output points memory, communication capabilities and software for the operating functions and features shown in the contract documents.

g. All system modules shall be general non-location specific in their construction. They shall be made location specific and operationally customized by software configuration of network variables during the installation process.

2.2.1 Programmable Logic Controllers

The Distributed Control System shall be hosted by Industrial Programmable Logic Controllers (PLC), installed within each local area equipment cabinet.

Each PLC shall host a dedicated area such as a housing block, or group of areas. Autonomy and isolation of areas shall be achieved by installing standard Layer 2 Ethernet Switches. Dual port Ethernet compatible Door modules shall be installed in a bus configuration with the bus cabling originating at the local area switch, and shall terminate at the last door on the appropriate door run.

The PLC hardware offered shall be capable of hosting a minimum of 64 controlled cell or passage security doors plus associated I/O and peripheral devices such as Duress buttons, monitored door position switches etc.

2.2.1.1 Technical Specification

- Processor: Intel® Atom™ Z510, 1.1 GHz or equivalent
- Flash memory: 64 MB
- Main memory: 512 MB RAM
- Interfaces: 2 x RJ 45, 10/100/1000 Mbit/s, DVI-D, 2 x USB 2.0
- Diagnostics LED: 1 x power, 1 x TC status, 2 x bus status
- Clock: Internal battery-backed
- Operating system: Embedded Linux, Windows CE or Windows Embedded Standard
- Power supply: 15-30 V DC
- Dielectric strength: 500 V (supply/internal electronics)
- I/O Current: 1 A
- Operating Temp: -15 to +60 °C
- Relative humidity: 95 %, no condensation

2.2.2 Door Control Modules

The programmable door control modules shall provide the necessary I/O points to cater for the monitoring and control requirements of sliding and swing doors, and shall be installed in a recessed housing or door header located above the door or lock.

The module shall provide 2x 10/100Mb Ethernet ports to enable the devices to be run in a bus configuration between consecutive cell and/or passage doors.

The module shall provide a minimum of four (4) high current (500ma), solid-state outputs for the control of pneumatic components, locking devices and Cell Lights.

The module shall also have a minimum of eight (8) optically isolated inputs for the monitoring of door position switches and / or reset call switches.

The module shall also be used as an interface to other security and miscellaneous monitored and controlled devices.

The door module with the following minimum requirements, shall allow for the direct termination of all field signals, light relays etc, as well as the connection of the data and power services, without the need for external switching relays or communication devices:

Output Requirements

The module shall allow for the direct termination of the following Output points:

1x Sliding / Swing Door Open solenoid valve

1x Sliding Door Close solenoid valve

1x Lock Bar Up solenoid valve

1x Cell Light Control Relay

Input Requirements

The module shall allow for the direct termination of the following Input points:

- 1x Sliding Door Closed/ Swing Door Secure
- 1x Sliding Door Open/ Swing Door DPS
- 1x Lock Bar Up
- 1x Lock Bar Down
- 1x Sliding Door Obstruction Detection
- 1x Bell Push buttons (Cell Guard Tour function)
- 1x Cell Phone Detection Alarm Input
- 1x Warder Duress Alarm Input

2.2.2.1 Technical Specification

- Interfaces: 2 x RJ 45 Ethernet, 10/100 Mbit/s (Autosensing)
- Diagnostics LED: 1 x Power, 1 x TC status, 2 x Bus Status

- Operating system: Embedded Linux, Windows CE or Windows Embedded Standard
- Power supply: 15-30 V DC
- Dielectric strength: 500 V (supply/internal electronics)
- I/O Current: 500 ma
- Operating Temp: -15 to +60 °C
- Relative humidity: 95 %, no condensation
- Digital Inputs: 8
- Digital Outputs: 4

2.2.3 Control Modules

The control panel modules shall be designed to be installed within each local control room cabinet. The module shall provide for the control of 16 Output points and 16 input points. Connection to the control panel will be via front mounting Pluggable screw cage terminations.

2.2.3.1 Technical Specification

- Interfaces: 2 x RJ 45 Ethernet, 10/100 Mbit/s (Autosensing)
- Diagnostics LED: 1 x power, 1 x TC status, 2 x bus status
- Operating system: Embedded Linux, Windows CE or Windows Embedded Standard
- Power supply: 15-30 V DC
- Dielectric strength: 500 V (supply/internal electronics)
- I/O Current: 500 ma
- Operating Temp: -15 to +60 °C
- Relative humidity: 95 %, no condensation
- Digital Inputs: 16
- Digital Outputs: 16

16 way input modules compatible with the control system shall be used to receive status information of panic buttons, DPS devices etc.

16 way output modules compatible with the control system shall be used to control status indicators cell and dayroom lighting etc.

2.3 Communication Network

The communication network shall be based upon industry standard Ethernet 10/100/1000 Mb/sec utilizing standard of the shelf non proprietary hardware.

2.4 Duress buttons

Duress buttons shall consist of a latching industrial type red mushroom head button **without** key release.

The device shall be flush mounted in a standard 100mm by 100mm socket outlet connection box.

These duress buttons are required in all offices where contact between inmates and staff may occur as indicated on the drawings accompanying the tender document.

2.4.1 Activation

Activation of any duress button shall sound an audible tone in the associated control room and cause the associated icon on the operator control console to flash.

The audible tone may be silenced from the control console causing the icon to remain steady with a red colour. The emergency condition of the icon shall only be reset once the alarm has been acknowledged by the operator.

All duress alarms shall be logged together with the appropriate time and date stamp within the management workstation together with the current operator detail.

2.4.2 Hardware Platform

All Inputs required for the Duress System shall be provided by the Distributed Control System (DCS) as detailed in the specification.

The rate provided shall be inclusive of the Duress button hardware including the necessary Input points on the DCS. No claims shall be entertained for additional Input points required for the system.

2.5 Maintenance and Spare equipment

The contractor shall provide 10% spares of all system modules, control modules, door modules including peripheral equipment, with a minimum of one modules of each type.

The contractor shall provide the Using Agency with the following:

1. One printed copy of all application source code that is specific to this project, including comments; I/O lists, binding lists and a complete instruction document detailing the replacement of each module type.

2. One copy of all application source code that is specific to this project in digital format (CD Rom or DVD). The files contained shall include both compiled and un-compiled source code.

3. The contractor shall demonstrate that the un-compiled source code contained on the digital media is the current version of the code contained in the system modules.

4. One system-programming device to facilitate control module replacement and/or expansion.

3 CLOSED CIRCUIT TELEVISION SYSTEM (CCTV)

3.1 Introduction

The Contractor shall provide a fully IP based CCTV Solution as part of the project scope of works, consisting of a combination of Analogue Cameras, Direct IP enabled cameras, H264 IP Video Encoders, H264 Video Decoders, Network Video Recording Servers and Video Wall Servers, all of which shall be seamlessly integrated to the Security Management System servers and operator workstations.

Leading brand IP Video Management hardware shall be provided, and the tenderer is required to submit the make and model of proposed CCTV system components as part of the Clause by Clause compliance document provided with this tender (Information to be rendered by tenderer), which shall be completed and submitted as part of their tender submission.

Camera Types that are not available as direct IP cameras shall be converted to IP via a single channel H264 IP Video Encoder mounted directly at the camera position. The use of multiple channel IP Encoders located at centralized positions shall not be considered as will the use of RG59 cable or RG59/CAT5 converters.

The CCTV components selected shall be suitable for installation in a maximum-security facility, and shall require the prior approval of the Engineer.

3.2 General

The contractor shall provide a complete closed circuit television system to comply with the requirements as detailed in the specification and accompanying drawings.

As far as is possible, and dependant on the individual camera specifications, all cameras shall be Direct IP enabled cameras. In cases where a specialized camera is specified, which is not available as a direct IP camera, a compliant analogue camera shall be provided complete with a standalone single channel H264 IP Video Encoder. Tenderers shall include the cost of a compliant single channel IP Video Encoder in the price of the Analogue camera in such cases. No additional claims for conversion of Analogue cameras to the IP network shall be entertained.

The IP based video solution shall be networked via a 1GB High Speed Security Ethernet network as detailed in the specification.

The Video management functionality described within this section of the specification shall be an integrated function of the Security Management System software provided, and shall not require third party or hardware brand specific software to provide operator and event based selection and management of images. The selection of encoded video images either by event or manually to video decoders, the selection and replaying of historical video footage from the appropriate NVR servers, etc shall be configurable parameters of the Security Management System.

The intended function of the Security Management System and the level of integration required with the IP Video system are detailed in the specification.

3.3 CCTV Cameras

3.3.1 Camera Type 1 (Direct IP Enabled Vandal Proof Fixed Dome Camera)

This type of camera shall be the standard camera to be installed within the various buildings, passage ways and Sally ports, and shall include the necessary Surge protection, power supply and any additional hardware that may be required to make the installation complete.

3.3.1.1 Technical Specification

- Supply voltage: 12 – 28 VAC
- Signal-to-noise ratio: >50dB
- Backlight compensation: Automatic and manual
- White Balance: Automatic tracking (2500 to 10000 K), AWB hold
- Stream resolution: 4CIF/D1 @ 25 IPS
- Compression: H264 & JPEG
- TV System: PAL
- Output 1: Ethernet 10/100 Base T, Auto Sensing, RJ45, 2x DVD quality H264 streams and 1 JPEG stream, configurable from 10 Kbps to 6 Mbps per channel
- Output 2: BNC – Composite Video at 1.0 VP-P 750
- Optical Resolution: 540 TV Lines

- Colour Sensitivity: 50IRE with frame integration off and shall not be more than 1lx unless otherwise noted.
- Min Illumination: Colour,1.3Lux (0.12fc), Night Mode, 0.5 Lux(0.048fc)
- Image Sensor: 1/3" Day/Night CCD
- Lens options: 2.6 – 6mm, 3.7 – 12mm
- Power over Ethernet: IEEE 802.3af Compliant
- Housing: Cast aluminum housing, Vandal Proof clear polycarbonate dome with UV blocking properties.
- IP Rating: IP 54
- ISCSI support
- Automatic Lens detection
- On screen display (OSD)

3.3.1.2 Minimum Camera Features

1. The camera specified shall be a true hybrid, 1/3-inch format, Day/Night camera that provides an Ethernet connection for direct connection to a network and a composite video BNC connection to enable the pre-commissioning of camera positions prior to network availability.

2. The camera shall incorporate a network video server capable of encoding two individual H264 quality video streams and one JPEG stream simultaneously, to allow the configuration of bandwidth and image quality for live video and recorded video individually.

3. The camera shall produce 30 images per second (NTSC) or 25 images per second (PAL) of DVD-quality, 4CIF H264 video over IP. The camera shall also support 2CIF, ½ D1, CIF and QCIF resolution.

4. The camera shall support power over the Ethernet (PoE) using UTP Category 5 cable with RJ45 connectors when an IEEE802.3af compliant switch is utilized. The camera shall also be capable of accepting an individual 24 VAC or 12 VDC Class 2 power source.

5. The camera shall support both unicast and multicast modes.

6. Access to the camera configuration via the network shall be restricted by a minimum of three user levels of protection where each level has its own password and authorizations.

7. The camera shall have video authentication capability whereby all images transmitted are marked with a visual indication of whether the image is the original or has been manipulated.

8. The camera shall support a snapshot mode that saves individual images from the video sequence, currently being displayed on the live view page, as JPEG format, 4CIF resolution images to the Operator Workstation hard drive.

9. The camera shall provide a standalone recording function to save video sequences to the computer's hard drive. These saved images may then be viewed from the computer hard drive using an H264 viewer provided by the manufacturer.

10. The camera shall provide a web browser interface to enable remote individual camera configuration by authorised users. Settings shall be stored in the camera memory and preserved during power interruption.

11. The camera shall provide a system status log and an event log which shall display detail such as alarm trigger events and time and date stamp detail. It shall be possible to automatically store such system and event messages to file on the Operator Workstation if required.

12. The camera shall provide an automatic Time/Date synchronisation function whereby all cameras are synchronised with the Security Management System time server.

13. The camera shall provide automatic IR filter switching to enhanced night viewing. The camera shall also allow the IR filter to be switched manually via the alarm input, by pre-programming the feature in the camera mode profile, or remotely via the web browser.

14. The camera design shall provide 15-bit DSP image processing technology for enhanced sensitivity.

15. The camera shall provide an on-screen display to simplify the camera/lens back focus and network configuration settings.

16. The camera shall provide video motion detection with four programmable areas with individual thresholds. The motion detector function shall incorporate a global scene change detector to minimize false alarms caused by sudden changes in lighting conditions.

3.3.1.3 Alarm Handling

1. The camera shall provide an alarm input that may be triggered by either a normally open or normally closed contact.

2. The camera shall be capable of displaying a 30 character, programmable alarm message on alarm.

3. Upon alarm the camera shall be capable of establishing a connection to any one of five pre-defined IP addresses. IP addresses shall be sequenced until a connection is established. The camera shall be capable automatically re-establishing connection to one of the previously specified IP addresses upon restart after a loss of connection or network failure.

4. The camera shall provide a relay output that may be selected for normally open or normally closed operation. The relay may be activated from an external alarm input to the camera, manual activation from the Security Management System, upon video motion detection, or video loss.

3.3.2 Camera Type 2 (Direct IP Enabled Vandal Proof Fixed Dome Camera With Dynamic Range)

This type of camera shall be installed in areas with variable lighting conditions and in areas where simultaneous low light and highlight areas exist within the scene, and shall include the necessary Surge protection, power supply and any additional hardware that may be required to make the installation complete.

3.3.2.1 Technical Specification

1. As per Camera Type 1

2. Dynamic Range: 15-bit digital XF Dynamic range

3.3.2.2 Minimum Camera Features

1. As per Camera Type 1

2. The camera shall provide XF-Dynamic technology to extend the dynamic range of the camera to provide a sharper image, simultaneously, in both the high-light and low-light areas of the scene.

3.3.2.3 Alarm Handling

1. As per Camera Type 1

3.3.3 Camera Type 3 (Direct IP Enabled Camera with Dynamic Range)

This type of camera shall be installed in external waiting areas and for general external surveillance including the perimeter fence, and shall include the necessary Fiber Optic conversion hardware for both ends of the fiber, Surge protection, power supply and any additional hardware that may be required to

make the installation complete. The camera shall be housed in a standard IP66 cable managed external housing with heater.

3.3.3.1 Technical Specification

- Supply voltage: 12 – 28 VAC
- Signal-to-noise ratio: >46dB
- Backlight compensation: Automatic and manual
- White Balance: Automatic tracking
- Stream resolution: 4CIF/D1 @ 25 IPS
- Compression: H264 & JPEG
- TV System: PAL
- Output 1: Ethernet 10/100 Base T, Auto Sensing, RJ45, 2x DVD quality H264 streams and 1 JPEG stream, configurable from 10 Kbps to 6 Mbps per channel
- Output 2: BNC – Composite Video at 1.0 VP-P 750
- Optical Resolution: 540 TV Lines
- Colour Sensitivity: 50IRE with frame integration off and shall not be more than 1lx unless otherwise noted.
- Min Illumination: Colour - 0.24 Lux (0.024 fc), Night Mode – 0.038 Lux (0.038 fc)
- Image Sensor: 1/3” Day/Night CCD unless otherwise noted.
- Lens fitting: CS or C Type
- Power over Ethernet: IEEE 802.3af Compliant
- Housing: External IP65 rated cable managed housing.
- ISCSI support
- Automatic Lens detection
- On screen display (OSD)

3.3.3.2 Minimum Camera Features

1. As per Camera Type 1

2. The camera shall provide XF-Dynamic technology to extend the dynamic range of the camera to provide a sharper image, simultaneously, in both the high-light and low-light areas of the scene.

3.3.3.3 Alarm Handling

1. As per Camera Type 1

3.3.4 Camera Type 4 (Vandal and Weather proof Colour Dome Camera)

This type of camera shall be installed in external areas where cameras cannot be mounted out of reach, and where vandalism may occur, and shall include the necessary Fibre Optic conversion hardware for both ends of the fibre, Single Channel IP Video Server, Surge protection, power supply and any additional hardware that may be required to make the installation complete.

3.3.4.1 Technical Specification

- Supply voltage: 12 – 28 VDC or 24VAC
- Backlight compensation: Automatic
- Lens: 3-8mm Vari-Focal
- Electronic Shutter: 1/50 – 1/100,00 Sec
- Iris: Automatic
- TV System: PAL (CCIR)
- Output: BNC – Composite Video at 1.0 VP-P 750
- Optical Resolution: 470 TV Lines
- Min Illumination: 1.5 Lux (1.2 fc)
- Image Sensor: 1/3” CCD unless otherwise noted.
- Housing: Weather proof, IP66 Die-Cast Aluminum housing with Vandal proof polycarbonate cover.

3.3.5 Camera Type 5 (Outdoor Direct IP Pan, Tilt, Zoom Camera)

This type of camera shall be installed outdoors on the Perimeter Fence and at key locations indicated in the accompanying drawings, and shall include the necessary Fibre Optic conversion hardware for both ends of the fibre, Surge protection, power supply and any additional hardware that may be required to make the installation complete.

3.3.5.1 Technical Specification

- Supply voltage: 12 – 28 VDC or 24VAC
- Backlight compensation: Automatic
- Zoom: 26x Optical, 10x Digital @ Max 1.65 Sec
- Scan Scale: 360º Horizontal, 90 Vertical
- Scan precision: 0.225º +- 0.003º
- Rotation: Continuous 360º Pan, Auto turn over at 180º
- Rotation Speed: 0.3º/Sec - 240º/Sec
- Preset Positions: 64
- Preset found time: <3 Sec
- Electronic Shutter: 1/50 – 1/100,00 Sec
- Iris: Automatic
- Focusing: Auto-Sensing, Manual, Infinity, Interval AF, Zoom Trigger AF
- Stream resolution: 4CIF/D1 @ 25 IPS
- Compression: H264 & JPEG
- TV System: PAL
- Output 1: Ethernet 10/100 Base T, Auto Sensing, RJ45, 2x DVD quality H264 streams and 1 JPEG stream, configurable from 10 Kbps to 6 Mbps per channel
- Output 2: BNC – Composite Video at 1.0 VP-P 750
- Optical Resolution: 470 TV Lines

- Colour Sensitivity: 50IRE with frame integration off and shall not be more than 1lx unless otherwise noted.
- Min Illumination: Colour – 1.3 Lux (0.12 fc), Night Mode – 0.5 Lux (0.048 fc)
- Image Sensor: 1/3” Day/Night CCD
- Lens options: 2.6 – 6mm, 3.7 – 12mm
- Power over Ethernet: IEEE 802.3af Compliant
- Image Sensor: 1/4” Colour CCD
- Housing: Indoor ceiling, Outdoor Weather proof housing
- Camera Control: On Screen Display (OSD)
- Protection: Auto protection on power failure
- Auto Cruise: Auto Cruise between two presets

3.3.6 Camera Type 6 (Indoor IR Colour Dome Camera)

This type of camera shall be installed indoors in areas of low light, and shall include the necessary , Single Channel IP Video Server, Surge protection, power supply and any additional hardware that may be required to make the installation complete.

3.3.6.1 Technical Specification

- Supply voltage: 12 – 28 VDC or 24VAC
- Backlight compensation: Automatic
- Lens: 3-8mm Vari-Focal
- Electronic Shutter: 1/50 – 1/100,00 Sec
- Iris: Automatic
- TV System: PAL (CCIR)
- Output: BNC – Composite Video at 1.0 Vp-p 750
- Optical Resolution: 370 TV Lines
- Min Illumination: IR On - 0 Lux @ 10m, IR Off – 1.0 Lux (F2.0)
- Image Sensor: 1/4” CCD

- Housing: Weather proof, IP66 Die-Cast Aluminum housing

3.3.7 Camera Type 7 (Covert PIR Camera with Audio)

This type of camera shall be installed in areas that require the monitoring of staff and visitor activity, and shall include the necessary Single Channel IP Video Server, Surge protection, power supply and any additional hardware that may be required to make the installation complete.

3.3.7.1 Technical Specification

- Supply voltage: 12 – 28 VDC or 24VAC
- Backlight compensation: Automatic
- Lens: 3-8mm Vari-Focal
- Electronic Shutter: 1/50 – 1/100,00 Sec
- Iris: Automatic
- TV System: PAL (CCIR)
- Video Output: BNC – Composite Video at 1.0 VP-P 750
- Audio Output: Terminal - 1.0 Vp-p 470Ω
- Optical Resolution: 370 TV Lines
- Min Illumination: 1.0 Lux (F1.6)
- Image Sensor: 1/4" CCD unless otherwise noted.
- Signal to Noise Ratio: 48dB
- Housing: Weather proof, IP66 Die-Cast Aluminum housing with Vandal proof polycarbonate cover.

3.4 CCTV Camera Housings

3.4.1 Camera Housing Type 1 (Cable Managed IP66 External Housing)

This housing type shall be installed on all external mount camera positions including the perimeter fence 50m zones and other external pole or wall mount applications, and shall include the necessary pole/wall mount brackets, heater elements and any additional hardware that may be required to make the installation complete.

All external mount cameras shall be converted to Fibre optic transmission to eliminate damage as a result of surge voltages, and to overcome the maximum transmission range of Ethernet (100m). The 10/100 Base T Ethernet to fibre optic conversion hardware is to be priced with each camera according to the specification. Tenderers shall ensure that the proposed housing is adequately sized to accommodate the conversion hardware.

3.4.1.1 Technical Specification

- Internal Cabling: Cable Managed
- Sunshield: Stand-off sunshield to reduce solar loading
- Tamper: Tamper resistant
- Access: Flip top access
- IP Rating: IP66
- Construction: Die-Cast Aluminum
- Finish: Pre-treated, Polyester coated
- Window: 6mm strengthened glass
- Fastenings and Hinges: Stainless Steel
- Usable Internal Dimensions: 220mm (L) x 130mm (W) x 95mm (H)
- Colour: White or Grey

3.5 IP Video Encoder/Decoders

All CCTV Images shall be transmitted via the High Speed 1Gb Ethernet Network installed for the exclusive use of the Security sub-system hardware. The Network shall consist of a fibre optic backbone installed in a star topology with the Central equipment room as the hub point to provide area autonomy.

Each buildings equipment room shall be equipped with a sufficient number of 24 Port, 2 Layer managed Ethernet switches as detailed in the specification.

Each local Security Management Operator Workstation shall be equipped 3x 20" LCD Monitors, one fed by the Operator Workstation to provide the Graphical User Interface and the remaining two for the display of live and historical video images. Each of the video monitors shall be fed by a single channel IP Video Decoder.

Detail of the Security Management Workstations functional requirements with regard to video processing, are described in the specification.

Each IP Camera, IP Video Encoder and IP Video Decoder shall be assigned a unique port on the 24 port switches.

3.5.1 IP Video Encoders

IP Video Encoders shall only be installed in applications where the camera specification required cannot be met by a Direct IP enabled camera, and in such cases the Video Encoder shall be installed at the point of origin in a suitable IP65 rated enclosure or directly within the Camera Housing.

The tenderer shall ensure that all necessary media converters, power supplies, terminations etc, required for such an installation are provided for within the tendered camera rate. Where power over Ethernet (POE) cannot be used, 240VAC power shall be supplied to such camera positions under the Electrical sub-contract.

3.5.1.1 Technical Specification

- No of Channels: 1
- Compression: H264, JPEG
- Per Channel Bit Rate: Configurable 9.6 Kbit - 6 MBit
- Maximum overall IP delay: 120ms (H264)
- Network Protocols: RTP, Telnet, UDP, TCP, IP, HTTP, IGMP V3, ICMP, ARP, SNMP
- Images per second: 25 IPS on each channel @ 4CIF/Full D1
- Resolution: H264 @ 4CIF / Full D1
- No. of streams per channel: 2x H264, 1x JPEG (Dual Stream)
- Internal video storage: 10Mb
- Ethernet: 10/100 Base-T, auto-sensing, half/full duplex, RJ-45
- Alarm Inputs: 4x solid state inputs (12-24VDC)
- Alarm Outputs: 2x potential free
- Multicasting: Dual Simultaneous streaming
- Data port: Serial data port + USB
- Power over Ethernet: IEEE 802.3af Compliant

3.5.2 IP Video Decoders

Individual Single Channel IP Video Decoders shall be installed to feed each video display monitor as described in the specification. The virtual matrix switching and configuration commands shall be a fully integrated function of the Security Management System offered, and shall not require the use of third party brand specific software to relay the switching commands to the Encoders and Decoders.

The tender shall describe the software integration methodology used in the development of the required drivers.

3.5.2.1 Technical Specification

- No of Channels: 1
- Decompression: H264, JPEG to Composite Video
- Per Channel Bit Rate: Configurable 9.6 Kbit - 6 MBit
- Maximum overall IP delay: 100ms (H264)
- Network Protocols: RTP, Telnet, UDP, TCP, IP, HTTP, IGMP V3, ICMP, ARP, SNMP
- Images per second: 25 IPS on each channel @ 4CIF/Full D1
- Resolution: H264 @ 4CIF / Full D1
- Ethernet: 10/100 Base-T, auto-sensing, half/full duplex, RJ-45
- Alarm Inputs: 2x solid state inputs (12-24VDC)
- Alarm Outputs: 1x potential free
- Data port: Serial data port + USB
- Power over Ethernet: IEEE 802.3af Compliant

3.6 Intelligent Video Motion Detection

In addition to the in-built motion detection function specified for all Direct IP cameras and IP video encoders, cameras mounted externally including those monitoring the perimeter fence, shall be equipped with intelligent video motion detection “IVMD” hardware/software, in order to eliminate false motion alarms as a result of changing environmental conditions such as changing lighting, wind, rain, hail and leaves blowing in the wind.

The functionality can be provided either by dedicated hardware or as an in-built software function of the video Encoder offered. As all images are to be converted to IP at the point of origin, the IVMD processing is required to take place prior to IP conversion.

The IVMD system shall provide advanced video content analysis, and shall reliably detect moving objects, while suppressing unwanted alarms from spurious sources in the image. The algorithm shall adapt to changing lighting and environmental conditions.

Individual IVMD channels shall be configurable to enable the selection of the required sensitive areas within the image, the minimum object size and the motion direction that should trigger an alarm, so that only the objects of interest are detected.

A configuration application shall be provided in order to configure the individual camera images within a 3D Grid. A graphical display shall allow the sensitive area, size, speed and perspective for objects, and movement direction to be superimposed on the image.

Once movement has been detected, the object shall be highlighted on the display and motion shall be tracked on the monitor. If an object and its motion match the conditions defined for one of the 16 detector fields, it shall create an alarm condition within the applicable Security Management Operator Workstation. Alarms generated by the IVMD shall be fully integrated into the Security Management System, enabling automated response to an alarm via other Security sub-system hardware, such as the selection of the alarm image to the required Operator monitor, automated messages being read over the Public Address System, SMS and Email generation etc.

IVMD alarms shall be logged within the Security Management Systems central database, along with the appropriate video footage time, date and channel reference. The time, date and channel reference shall be used to replay applicable video footage via the Management System.

3.6.1 Minimum IVMD Features

- Robust motion detection
- Background self-learning algorithm
- 16 independent detector fields for alarm generation
- Differentiation between objects entering, leaving or loitering within an area
- Ability to define detection rules based on object size, speed and direction
- Tamper monitoring to detect camera hooding/ masking, blinding, defocusing and repositioning

3.6.2 IVMD Configuration

- Configurable via a graphical user interface (GUI)
- Selection of sensitive areas
- Single or multiple detector fields
- Perspective correction via a 3D grid set up
- Size and speed filter

3.7 3.7 Network Video Recorders (NVR's)

The Contractor shall provide a fully IP based Video Recording System whereby all images are stored on Digital Video Recording Servers installed within the various security equipment rooms in the facility. NVR's shall be connected directly to the appropriate 24 Port managed switches within the local equipment cabinets.

The managed Ethernet switches shall be configured to limit the Video traffic onto the incoming 1Gb uplink ports on the switches, by restricting outgoing streams to those required for live video feeds based on Operator selection, and recorded video footage being reviewed by Central Operator Workstations or the Operations room.

In order to minimize traffic on the 1 GB uplink ports, the allocated recording stream on each of the Direct IP cameras or IP Video Servers shall be assigned to the IP address of the Network Video Recorders within the local subnet.

The tenderer is required to submit a lump sum rate in the Bill of Quantities for a complete Network Video Recording system based on the total number of cameras indicated in the Bill of Quantities.

The tendered rate is deemed to be fully inclusive of all software, licenses, hardware and accessories required to make the system complete.

The tenderer shall clearly indicate the number of NVR's offered, the calculation used to determine the number of NVR's required, the additional costs or savings generated as a result of adding or omitting 1, 4, 8, 16, and 32 cameras. The calculations shall be provided as part of the clause by clause compliance document to be returned with the tender documents.

The tenderer shall provide rates for the above camera increments, which shall be used to calculate the additional cost or savings as a result of such addition or omission of cameras.

The number of NVR's required shall be determined by the following criteria:

1. A minimum of 120 GB of hard disk space shall be provided per camera.

2. Hard disk expansion by means of external raid storage is acceptable to a maximum 6Tb.

3. Licensing shall be provided on a once off basis. Systems requiring periodic re-licensing fees shall not be accepted.

3.7.1 Technical Specification

- Minimum internal storage: 1.5TB
- Maximum RAID-5 expansion: 6Tb
- No. of Gigabit Ethernet ports: 2 x TCP/IP
- Archiving: Internal DVD Writer
- Mounting: 19” 2U Rack – Horizontal mount
- Simultaneous Recording Streams: Continuous 64 Video Streams at 6Mbs per stream
- Processor: Dual Core Intel Xeon 5140 (2.33 GHz) with 1333 MHz front side bus support
- RAM: 1 GB PC2-5300 DDR2 buffered DIMMs
- Cache: 4 MB L2 Cache
- DVD: 1x 8/24X Slim line
- SCSI Host Bus Adapter: Single Channel U320 adapter for external storage connectivity
- NVR OS: A suitable OS and NVR software shall be installed that will allow multi channel remote live viewing, playback, export and archiving.
- Ethernet Adapter: PCI Gigabit Adapter
- Power Supply: Output rated steady state supply 1000W

3.7.2 Minimum NVR Requirements

1. The proposed NVR shall consist of standard components, and shall be guaranteed to be in production for a minimum of five years from date of delivery.

2. The proposed NVR shall have a proven track record in high security applications. Reference list shall be provided as part of the Clause by Clause compliance statement.

3. The proposed NVR shall display the CE, FCC and UL certified markings.

4. The NVR manufacturer shall provide a written 2 year support warranty. To be provided with tender documents.

5. The NVR hardware shall be manufactured by a reputable internationally recognised supplier such as HP, DELL, COMPAQ or equivalent.

6. All NVR software upgrades shall issued free of charge for the warranty period.

7. All NVR firmware upgrades shall be issued free of charge for the warranty period.

3.8 Digital Video Storage Raid 5 Array

The expansion of the NVR's storage capacity to meet the required 120 GB per camera shall be provided by means of external 19" Rack mount Raid 5 Arrays supplied by the same manufacturer of the NVR.

The product supplied shall have a proven track record in bulk Video Storage applications, and shall be equipped with removable drive trays, power supply units and cooling modules, which shall be hot-swappable within a cableless modular chassis.

Dual-stack connectors shall allow for daisy-chaining of disk arrays for large capacity storage. In the event of failure, the Video Storage Array shall sound an audible alarm, and notify the Security Management System of the hardware failure.

To cater for upgrades to the storage capacity, it shall be possible to route a minimum of 16 SATA drives channels through the backplane which shall feed lockable drive accessible from the front of the array.

Each Array shall be equipped with a battery backup unit (BBU) installed to prevent data loss during a power failure.

3.8.1 Technical Specification

- Power Supply: Dual Hot swappable 240V AC Supplies
- Connectivity: 2 x Ultra SCSI-320 Host Ports
- Serial Communications: RS-232 (Serial) Port DB-9 Male
- No of Hard Disk Bays: 16
- Minimum Sequential Arrays: 3
- Expansion Capability: 7.5 Tb
- Network: RJ45, Ethernet 10/100 Base-T compatible
- Mounting 19" 3U Rack – Horizontal mount
- Redundancy: Hot swappable 3 GBps SATA hard disks

- Operating Temperature: 0 °C to 40 °C
- Compliancy: CE, UL, CB and IEC

3.9 CCTV Monitors

The Contractor shall provide two monitor types within the scope of the Security Contract as follows:

1. High Resolution 22" LCD Monitor

Each Operator shall be equipped with 2x 22"LCD Monitors in compliance with Clause 3.8.1 below. The monitors shall be driven by the Small Video Wall Server detailed in Clause 3.10 below.

2. High Resolution 40" LCD Monitor

The Central Control Room shall be equipped with 9x 40" LCD Monitors in compliance with Clause 3.8.2 below. The nine monitors shall be driven by the Large Video Wall Server detailed in Clause 3.10 below.

3.9.1 22" LCD Monitor Technical Specification

- Viewing Image Size: 22" LCD HAS Wide Screen
- Input: Analogue (Composite) + Digital (SVGA)
- Contrast Ratio: 800:1
- Minimum Resolution: 1680 x 1050
- Pixel pitch: 0.255mm
- Minimum Viewing Angle: 160º/160º
- Scanning Frequency: 30-81kHz
- Brightness: 300 cd/m2
- Response Time: 5ms

3.9.2 40" LCD Monitor Technical Specification

- Viewing Image Size: 40" LCD TFT (Active Matrix)
- Input: Analogue (Composite) + Digital (SVGA)
- Contrast Ratio: 800:1
- Minimum Resolution: 1366 x 768
- Pixel pitch: 0.650mm

- Minimum Viewing Angle: 170º/170º
- Scanning Frequency: 30-70kHz Horizontal, 50-85 Vertical
- Brightness: 500 cd/m2
- Response Time: 8ms

3.10 Video Wall Servers

The Contractor shall provide two video wall types within the scope of the Security Contract as follows:

1. Small Video Wall Server (Local and Movement Control Rooms)

Each Local Security Control Room shall be capable of displaying its Graphical User Interface, Live, Sequenced and Recorded Video images over a minimum of three (3) high resolution 22" LCD Monitors.

The Centre Monitor shall be driven by the Operator Workstation running the Security Management Systems Graphical User Interface.

The remaining two monitors to the left and right hand side of the Operator Workstation shall be driven by a single small video wall server compliant with clause 3.10.1 below, as follows:

Left Monitor: Up to twenty (20) Individual Live, Sequenced and recorded video images displayed as required by the operator. The image layout shall be configurable with the ability to select various tiled modes including 1,4,6,8,9,10 and 16 tiles. Operators shall be able to drag any camera icon from the Graphical User Interface onto the Left monitor as required.

Right Monitor: Up to four (4) Individual Live or recorded images displayed as required by the Operator. The image layout shall be configurable to display either a single image in full screen mode or four images in quad mode. Operators shall be able to drag any camera icon from the graphical User Interface onto the right hand monitor or into any one of the quad positions. In the default Mode the monitor shall be configured as a spot monitor whereby the operator is able to left mouse key on any camera icon on the GUI, and the images shall appear in full screen mode on the monitor.

2. Large Video Wall Server (Central Control Room)

The Central Equipment Room shall be equipped with 2x Operator Workstations configured in the default 3x 20" LCD Monitor layout as described under the Small Video Server requirement. In addition to this a 3 x 3 x 40" Monitor Video Wall (9 x Monitors) shall be provided and mounted on the rear wall of the Central Equipment Room in front of the two Operator consoles at a distance of 3 meters.

The nine monitors shall be driven by 5x independent Large Video Wall servers compliant with clause 3.10.2 below, the images upon which shall be freely configurable with the ability for a System Supervisor to drag video images onto any of the nine monitors at will.

The Video Wall shall enable the simultaneous display of up to 50 Live and recorded Video Images.

3.10.1 Small Video Wall Server Technical Specification

- Processor: Single Intel Xeon W3505, 2.53 GHz, 4MB, 1066MHz
- Memory: 2048MB, 1066MHz DDR3, Non ECC
- Hard Drive: 500GB, 7200 Rpm, Serial ATA II (Excl recording)
- Optical Drive: 16X DVD+/-RW Drive
- Graphics Adapter: Dual Port 768 MB Quadro FX1800 Display Card
- Max Monitors/Server: Two (2)
- Max Images/Server: Twenty Five (25)
- Max CPU Usage: 50% with 25 simultaneous Images

3.10.2 Large Video Wall Server Technical Specification

- Processor: Dual Intel Xeon E5410 Quad Core, 2.33GHz, 12MB, 1333MHz
- Memory: 4096MB, 667MHz DDR2 Quad Channel FBD
- Hard Drive: 500GB, 7200 Rpm, Serial ATA II (Excl recording)
- Optical Drive: 16X DVD+/-RW Drive
- Graphics Adapter: Dual Port SLI 768MB Quadro FX4600 Display Card
- Max Monitors/Server: Two (2)
- Max Images/Server: Fifty (50)
- Max CPU Usage: 50% with 50 simultaneous Images

3.11 Video Management Software Module

The following software functions are required as a fully integrated software module of the Security Management System provided as part of this tender.

The functions described are to be built in functions of the Security Management Operator Workstation software, and it an explicit requirement of this tender that these functions are not performed by the either manufacturer specific software or third party software via a windows based interface such as DLL's, Active-X components etc.

Due to the complex nature of the sub-system integration required by the system it is imperative that the Supplier of the Security Management System provides a direct interface (driver) to the sub-system hardware offered in this tender, and that the functions described below are in-built functions of the software.

3.11.1 Minimum Video Management Module Features

1. The VMM shall be an integrated function of the Security Management System.

2. The VMM will offer a complete video surveillance solution that will be scalable from one to hundreds of cameras that can be added on a unit-by-unit basis

3. The VMM shall include the following components:

    - Scan network
    - System tree
    - Map editor
    - Alarm management
    - Workspace and site maps
    - Multi-screens windows
    - Device configuration tool
    - Current Alarm Window

4. The VMM shall allow the following primary functions:

    - Set up and dismantling of connections between cameras and monitors via drag and drop functions (virtual matrix)
    - Several simultaneous live picture connections to cameras in network
    - Configuration of monitoring areas (site maps and workspace)
    - Programming of alarm-triggered automatic events
    - Integration of Camera alarms and events with other security sub-system hardware.
    - Logging and Management of CCTV Hardware alarms and events

5. The VMM shall be capable of displaying MPEG-4,MPEG-2 and H264 live and recorded video streams in real time simultaneously at bandwidth ranging from 10 Kbits/sec to 4 Mbits/sec in MPEG-4 and from 1.5 Mbits/se to 6 MBits/sec in MPEG-2, frame rates ranging from 1fps to 30fps and resolution ranging from ¼ CIF to 4CIF.

6. The VMM shall be capable of setting individual camera bit rate, frame rate and resolution. Configuration if individual settings shall not affect the recording and display settings of other cameras

7. The VMM shall require no proprietary recording hardware, no hardware multiplexer or time-division technology for video or audio recording and monitoring.

8. The VMM shall allow:

    - Live display of camera images
    - Live display of camera sequences
    - Control of PTZ cameras
    - Playback of archived video
    - Instant Replay of live video
    - Selection of Camera Icons via area maps
    - The VMM shall support any form of IP network connectivity, including: LAN, WAN, VPN, and Internet technologies
    - The VMM shall be able to use multiple CCTV keyboards to operate any camera within the system, regardless of brand, make or model, including their PTZ functionalities (i.e. Pelco keyboard controls Panasonic dome or vice-versa)
    - The VMM shall allow for a CCTV keyboard to be attachable directly to a encoder/decoder via its serial port or directly to the PC

3.11.2 Minimum Video Management Module Functions

The Video Management Module shall enable the following minimum functions within the Security Management System.

1. The icons on a site map shall be interactive and allow:

    - Drag and drop of a camera on a monitor
    - Camera connection with on click on the camera
    - Start of an alarm scenario
    - Hyperlink to another site map
    - Activation of a camera relay output

2. An instant replay function shall be available from the site map, to allow the user direct access to the last minutes of recording available on the Network Video Recorders (NVR's)

3. The VMM shall display the current status of all NVR's on the Security LAN.

4. The VMM shall detect video loss, and display the loss of camera signal as an alarm on the appropriate operator workstation

5. The VMM shall receive all incoming events (motion detection and triggered digital input and relay output) in the system and take appropriate actions based on user defined event/action relationships within the Security Management System.

6. The VMM shall log all CCTV related events to the common Security Management System MS SQL database. It shall be possible to search for events and alarms based on various filters including time, date, event type, camera number etc.

7. The VMM shall disable or enable configuration rights based on an Operators user level which is determined by the Fingerprint logon function of the Security Management System.

8. The VMM shall allow operators to view an instant replay of the video for any archiving camera. The operator will be able to define the amount of time he wishes to go back (unlimited). As well as be able to control the playback with play, pause, forward, back, and speed buttons

9. The VMM shall treat the network as a digital matrix system by allowing cameras to be connected to monitors using a drag and drop function.

10. The VMM shall display several simultaneous live picture connections from cameras in the network.

11. Remote video servers equipped with a relay output function shall be controllable from the VMM.

12. The VMM shall have an instant replay function that allows video recorded on network devices equipped with local disk storage to be reviewed, and, if desired, backed up to network video recorders (NVR).

13. The VMM shall provide for snapshots to be saved as .JPG format images to the hard drive of the Operator Workstation.

3.11.3 Video Display Functions

The Security Management System shall provide the following two methods of displaying Live and Historical Video footage:

1. Picture in Picture Display

    a. Live Video shall be displayed in a static picture in picture video window on the operators GUI, and shall be activated by the selection of the appropriate camera icon

    b. It shall be possible to display multiple video windows, which may be dragged and sized as required within either the multi-monitor Operator station or onto the Central Control Room Video Wall Display. It shall be possible to limit the number of simultaneous video windows based on the workstation performance specifications.

    c. It shall be possible to automatically activate video windows based on either CCTV related alarms and events or any other sub-systems alarms and events. E.g. In the event of a fire zone alarm, a video window shall be activated with the appropriate video image.

2. CCTV Monitor Control

    a. The Security Management System (SMS) shall be capable of issuing control commands directly to the IP Cameras, Video Encoders, Video Decoders and the NVR's (Virtual Matrix), to select live or recorded video images onto any external Video Monitor as required.

    b. The SMS shall provide a floating virtual monitor window on the operator's workstation, which shall enable the operator to drag camera icons onto any monitor as required.

    c. The SMS shall provide a sequence video window, into which multiple camera images may be dragged, with the ability to configure the dwell time.

Virtual monitor windows shall be configurable to display in various display patterns ranging from 4 tiles to 16 tile patterns.

4 DIGITAL INTERCOM AND PUBLIC ADDRESS SYSTEM

4.1 General

The system shall consist of a VOIP (Voice Over Internet Protocol) based Full Duplex intercommunication system to provide digital voice communication, public address, voice recording and event logging facilities.

The IP (Internet Protocol) based Intercom & Public Address System shall be networked via a 1GB High Speed Security Ethernet network.

The following functional features shall be provided by the proposed system:

1. Noise immunity

   The system shall provide clear undistorted speech and music transmission.

   The audio signal shall be digitally transmitted to each intercom station to provide immunity against electrical and earthing interference typically associated with analogue systems.

2. Bus structured and Star Cabling

   Intercom stations shall allow both a Star and Bus type configuration architecture in order to reduce system cabling and conduit requirements, and shall not require an independent pair of wires per station.

3. Multiple Audio Channels

   The system shall be capable of transmitting multiple digitized audio channels simultaneously, which shall enable intercom stations to independently select either a music channel, an education channel or to call and communicate with the system operator. The channel selection and current operation of one station shall have no effect on the channel selection and operation of any other station.

4. Interface to Telephone network

   The system shall have the capability of interfacing to the prison telephone system (PABX), which will enable existing telephones situated in offices to Page intercom or Public Address Stations.

5. Tamper detection

   Each intercom station shall provide tamper detection, which shall automatically notify the system operator of an intercom station which has been opened or tampered with in any way.

6. Integration with Security Management System

All software functions are required as a fully integrated software module of the Security Management System provided as part of this works. The functions described are to be built in (integrated) functions of the Security Management Operator Workstation software – it is not to be a standalone system of a third party vendor.

7. Event Recording and Reporting

   The system shall be capable of recording and reporting the following events with an accompanying time and date stamp:

   - Intercom station call requests with station identification.
   - Operator response with operator/station identification and call duration.
   - Intercom station unanswered call requests with station identification.
   - Intercom Tamper
   - Intercom Voice Threshold Alarm
   - Intercom Communication Failure
   - Intercom Equipment Failure (Call Button failure, etc)

8. Voice recording

   Selected calls shall be recorded onto a dedicated Audio Recording System. Operators shall be able to replay the call via a Recording System, which shall indicate the associated intercom station and time and date of the call. The system shall have the ability to configure which channels are to be recorded. A portable application will be provided to export and play the recorded media on a third party computer not connected to the Security Network.

9. Full Duplex Communication

   The system operators shall be provided with handsets, which shall enable full duplex conversations with any selected intercom station.

10. Volume level Adjustment

    The system shall enable operators to independently set the speaker volume and microphone sensitivity levels for each intercom station in order to optimize the acoustic settings for each building or room.

11. VoIP Compatibility (Ethernet telephones)

    The system shall be compatible with standard Voice over IP telephone systems using the Session Initiation Protocol, which will enable the expansion or replacement of equipment with products from a variety of competitors.

4.2 System Description

Analogue/digital hybrid systems making use of separate data and audio bus cabling shall not be accepted, and the tenderer shall provide sufficient

technical literature to fully evaluate the data/audio protocol utilized by the system.

The system shall be compatible with standard voice over IP products (IP Telephony), which employ such protocols as SIP, and be capable of communicating both data and audio signals over standard TCP/IP and UDP Protocols. The system shall make use of the High Speed 1GB Security Large Area Networks for the transmission of Control and Audio data.

The overall design of the system software and cabling shall be such that as far as practical, failure of one part (building) of the system does not affect normal operation of any other part of the system.

The system shall employ full duplex digital audio technology and provide clear undistorted speech communications, free from background noise and/or external interference.

Amplification shall be provided at each intercom or PA station in order to provide the option of piping music to groups or individual stations as required.

The system shall be capable of transmitting at least 40 simultaneous full duplex conversations via the Ethernet network running between control areas and to the local intercom stations.

The system shall be configured such that if any one system fails to operate, the other systems shall continue to operate without any detrimental effect. All Bus type connections shall have a built in failover mechanism in order for individual device failures not to effect downstream communication.

4.2.1 Cell and Passage Door Intercom Stations

The contractor shall supply, install and commission a networked Cell and Passage door Intercom System to nominated locations. Interface to the Security Management System shall be provided at each local control room and the Central Control room.

Calls originated from cell and passage door intercom stations shall be routed to the respective local control room Security Management System Operator Workstation.

A Call diversion facility in the event of unanswered or unattended mode shall be provided, and shall be configured to the engineer's specification. The Call diversion facility should have comprehensive features taking into account (a) Multiple endpoints (b) Unoccupied endpoints and (c) Automatic route detection.

All calls between Control stations and intercom stations shall be able to be digitally recorded on the intercom digital recording system.

The Digital Recording System shall be expandable to cater for future system expansion.

4.3 General System Overview

The systems major components shall be located as follows:

4.3.1 Central Control Room

- 19" rack mount Digital Intercom VOIP Exchange located within an equipment rack in the Central Equipment Room with clustering ability.
- Security Management Operator Workstation Interfaces.
- Operator communications handsets.
- Digital Voice Recording System located within the Central equipment rack.

4.3.2 Local Control Locations

- 19" rack mount Digital Intercom VOIP Exchange located within an equipment rack in the Local Equipment Room.
- Security Management Operator Workstation Interface.
- Operator communications handset.
- Digital Voice Recording System located within the Local equipment rack. (Optional)

4.3.3 Field Equipment (Ethernet based)

- Amplified Intercom Endpoints
- SIP (Session Initiation Protocol) enabled Node hardware

4.4 System of Operation

4.4.1 General

Within each nominated building, the contractor shall supply and install an integrated intercom system. The system shall be complete with cell and passage digital intercom stations and 19" rack mountable VOIP exchanges to provide voice communications to the local control room and/or the Central Control Room.

The system shall provide the following minimum system functions:

4.4.1.1 Normal calls

Calls initiated from Cell/Staff Intercom stations to system operators or vice versa

4.4.1.2 Alarm calls

Emergency calls initiated by officers or automatically triggered by system events such as audio level alarms (Threshold monitoring).

4.4.1.3 Tamper calls

Tamper calls initiated when an attempt is made to gain unauthorized access to intercom station electronics

4.4.1.4 System error messages and event logging

System errors and disturbances shall be displayed on appropriately configured operator workstations according to the type and location of the error or event. Disturbances such as raised voice levels in cells shall automatically generate alarms, which shall be logged within the Security Management System.

System functionality shall not be influenced in the event of failure of any one part of the system or operator station. Each operator workstation shall be configured as an autonomous system. In the event of an operator system failure, the functionality of that station shall be transferred to another operator workstation on the system according to a pre-configured set of rules.

4.4.1.5 Data Integrity

In the event of power failure, the actual status information in the system at the time of the failure shall not be lost. When the power is reconnected, all status information at the time of the power failure shall be retrievable and will be displayed on the relevant screens.

4.4.1.6 Listen-in

A “Listen-in” function shall be provided, and configured in accordance with the engineer’s specification, to provide either overt or covert operation or to be disabled altogether. Overhearing (listening-in) from one cell to another via the cell station shall not be possible.

4.4.1.7 Public Address system

It shall be possible to annunciate messages in two ways:

- By initiating a group call to a selected group or all intercom stations.
- By initiating a group, or all PA stations which have been configured on the system.

Any operator workstation on the system shall be capable of being configured with PA functionality as required.

4.4.1.8 Call Monitor

A Call Monitor facility shall be provided, which shall provide the operator with station identification. The call monitor shall display the calls and events from individual cell intercom stations in a priority based text listing.

The Call Monitor function shall be capable of displaying the following information.

Normal calls, Tamper calls, Alarm calls, general Input/Output state, Intercom Station Error and Intercom Station Failure.

It shall be possible to configure the call or event priority on the Security Management System.

4.4.2 Establishing a Call

At a minimum the system shall be capable of establishing calls in the following two ways:

4.4.2.1 Respond to Normal Calls

Call-ins shall be entered into a Call-in queue on a first in – first out (FIFO) bases, and sorted by priority level. Priority levels shall be set for each intercom station on the system. On receiving a call-in the operator shall only need make a single keystroke to answer the highest priority call that has been in the queue for the longest period of time. It shall also be possible to select a specific call-in and initiate a call by making a single keystroke.

4.4.2.2 Response to Alarm Calls

The system shall be capable of automatically detecting raised audio levels at nominated intercom stations.

4.4.3 Call & Event Logging

All calls and events shall be logged to a Centralized Database. The Database shall be automatically archived when the pre-configured size limit has been reached. A standalone utility shall provide a customizable view of the current historic or archived data in HTML format suitable for standard web browsers.

4.4.4 System Maintenance

The system shall be provided with a system configuration tool whereby system parameters may be set for individual intercom stations. All system parameters shall be downloaded from a Central station, and shall not require the opening of intercom points in order to change system parameters.

The following maintenance parameters shall include but not be limited to:

1. System parameter initialization.

2. Intercom Station parameters configuration.

3. Line related parameters settings such as station type.

4. Station call number settings.

5. Group Call numbers setting for stations.

6. Emergency Call setting for stations

7. Call Restriction settings.

8. Control desk group settings.

9. Configure Digital Switch parameters

10. Print pre-defined reports

11. Testing of communication paths

12. Automatic addressing

4.4.5 Call Routing

If a call is not answered or cancelled locally within a user adjustable pre-determined time of 30-600 seconds the call shall be automatically transferred to the next level station group.

4.4.6 Multiple or Simultaneous Calls

Cell calls arriving at the local control panel or nominated Central Control Room operator's terminal shall be queued so that calls are listed and answered consecutively, in accordance with their priority and chronological arrival time.

Cell calls from Buildings, which are in attended mode and have been switched through to Central Control Room by default, shall have priority over calls from Buildings in unattended mode.

The system shall have programming capability for priority queuing so that inmates with medical or other problems can be assigned a higher queue priority.

Priority cells shall be highlighted on the Central Control Room operator's terminal.

4.4.7 Public Address

It shall be possible to initiate a public address call from any operator control station to a building or group of cells utilizing the cell intercom units within their area of responsibility.

The system shall also have the capability to provide control of general public address speakers to nominated areas.

4.4.8 Suppression of Call

An operator shall be able to suppress calls from an individual cell or group of cells. This shall be initiated in the event of nuisance calls from cells. The suppression of the call function shall only be available when enabled via a high-level password control allocated to a supervisor.

Once a cell has been isolated calls initiated from the cell shall not register at the operator stations.

4.4.9 Future Expansion

The Cell Intercom system shall be capable of being expanded for extended use within the total complex for future extensions. All upgrades to provide this service shall not affect the existing service as specified in this document or render the equipment, as specified, redundant in any form.

All system upgrades shall be configured using similar equipment and operate in the same manner in all respects. Any upgrades should cause minimal disturbance to the existing service.

4.5 Hardware Components

The System shall consist of 19" Rack mount VOIP exchanges, multiple channel distributed intercom modules and a variety of vandal-proof intercom station types including Cell Stations, Staff Stations, Visitation Stations and Public Address Stations.

Multiple channel distributed intercom modules shall be networked in a daisy chain configuration throughout the facility. The distributed intercom modules shall be housed in standard electrical junction boxes located in secure positions to avoid tampering.

Intercom stations shall be installed in suitable flush mount back boxes as detailed in the tender drawings. The tendered rate for the Intercom station shall include for the supply of the back box, which shall be installed together with the required conduits, junction boxes and wire ways.

Intercom stations shall consist of a vandal resistant, momentary action call switch, speaker and microphone mounted into a flush mounted stainless steel plate. All electronics (including the microphone and speaker) must be suitably packaged – the installation of bare electronic boards and/or part assemblies will not be allowed.

4.5.1 IP Based Intercom Exchange

The tendered rate shall include full compensation for the Supply, installation and commissioning of a 19" rack mount VOIP Intercom Exchange including all necessary accessories, configuration tools, software and applicable licensing to make the installation complete.

The Solution offered shall be modular in design with the following features as a minimum:

- Direct Ethernet connectivity
- Support for standard VoIP protocols including SIP and H323
- Support for a minimum of 1024 Intercom Stations per exchange
- Support FXO/FXS/BRI interface connectivity
- Full Duplex Communication between multiple Stations
- Support for Voice Transcoding
- Direct Integration with the Security Management System offered

4.5.2 Distributed Intercom Module – Two Channel

The tendered rate shall include full compensation for the supply and installation of a two (2) channel Intercom Module, capable of terminating up to a maximum of 2 Intercom stations. The module shall be capable of terminating Cell, Staff, or PA type stations, or a combination of types as may be required. The tendered rate shall include the necessary termination and fixing material to make the installation complete.

The Intercom module shall provide the following features as a minimum:

- Isolated Ethernet network In and Out ports with Failover Protection
- Two (2) Intercom (Full Duplex or Half Duplex Endpoint) Station termination ports
- Four (4) Digital (Optically Isolated) Inputs onboard for General use
- One (1) Tamper Input
- Optional expansion for 4 additional Digital Inputs for General use
- Optional expansion for 4 additional Digital Outputs for General use
- Ability to upgrade firmware from remote location
- SIP (Session Initiation Protocol) support

4.5.3 Distributed Public Address Module – Two Channel

The tendered rate shall include full compensation for the supply and installation of a two (2) channel 10W per channel Public Address Module, capable of terminating up to a maximum of 2 PA stations. The tendered rate shall include the necessary termination and fixing material to make the installation complete.

4.5.4 Distributed Visitation Module – Two Channel (One Set)

The tendered rate shall include full compensation for the supply and installation of a two (2) channel 1W per channel Visitation Module, capable of terminating one Visitation Intercom Set (1x Inmate plus 1x Visitor Station. The tendered rate shall include the necessary termination and fixing material to make the installation complete.

4.5.5 Cell Intercom Stations

The tendered rate shall include full compensation for the supply and installation of a cell speaker module with push-button mounted on a flush mounted vandal proof stainless steel faceplate, through wall back box and associated fixing equipment cable ferrules etc.

Cell Intercom units shall be designed/constructed/installed as follows:

- Front plate to be stainless steel 3 mm thick.
- The Speaker grille will be a grid pattern of vertical slots.
- A 2 mm thick baffle plate with a corresponding 3 mm offset grid pattern.
- Mylar speaker with a minimum 3 watt power rating.
- The microphone is to be an Electret type with a minimum 36 DB dynamic range.
- An exterior, which does not facilitate the concealment of contraband.
- A tamper alarm separate to the call alarm to notify the respective operator station of an intercom unit's removal.
- The call button is to be a robust, vandal resistant push button manufactured of stainless steel.
- The call button shall activate a micro switch and bear against a solid shoulder, which resists knock through. An internal neoprene gland seals the button to IP65.
- Build in 1-Watt amplifier with software adjustable gain.
- Cabling shall be CAT6 UTP, full duplex transmission of speech
- Adjustable microphone sensitivity

The through-hole back box shall be installed by the building contractor between the Service duct and the cell. The faceplate shall attach to the back-box on the cell side by means of welded studs on the faceplate, which shall be secured to the back-box with four nuts from the inside of the box.

The cell station shall consist of an intercom unit and vandal proof push button mounted on a rectangular, 3mm thick, brushed stainless steel plate. Threaded studs shall be welded to the rear of the grill plate to facilitate flush security from the rear.

A wall blank cavity cover plate of the same dimension as the steel plate shall be mounted with recessed Torx type security screws to the service duct side of the back-box.

The loudspeaker shall be a water resistant unit with a plastic cone. The loudspeaker installation shall be such that tampering and water damage is eliminated.

The finish of the speaker enclosure shall be of high quality, neatly finished and shall not require any paint or protective covering. The opening in the cover shall be situated in a manner that the speaker cannot be damaged from the outside by protruding obstacles through the sound cavities.

Intercom field modules shall accommodate either 1 station or 2 stations as detailed in the Bill of Quantities. A minimum of two additional inputs per intercom station shall be provided either directly by the field node or as an external module. The Digital inputs shall be utilized to monitor the "Guard

Present" switch mounted on the outer side of each cell door, which shall also be monitored and logged by the Security Management System or for other general purposes as required by the Engineer.

4.5.6 Staff Intercom Stations

The tendered rate shall include full compensation for the supply and installation of a Staff intercom station module with vandal proof push-button mounted on a flush mounted vandal proof stainless steel faceplate, one piece back-box as detailed in the tender drawings, and associated fixing equipment cable ferrules etc.

Staff Intercom units shall be designed/constructed/installed as follows:

- Front plate to be stainless steel 3 mm thick.
- The Speaker grille will be a grid pattern of vertical slots.
- A 2 mm thick baffle plate with a corresponding 3 mm offset grid pattern.
- Mylar speaker with 3 watt power rating.
- The microphone is to be an Electret type with a minimum 36 DB dynamic range.
- An exterior, which does not facilitate the concealment of contraband.
- A tamper alarm separate to the call alarm to notify the respective operator station of an intercom unit's removal.
- Calls to be activated via Staffs magnets.
- Build in 1-Watt amplifier with software adjustable gain.
- Cabling shall be CAT6 UTP, full duplex transmission of speech.
- Adjustable microphone sensitivity

The single sided rectangular back box shall be installed at the required positions as indicated on the tender drawings. The faceplate shall attach to the back-box with 4x Torx type security screws.

The Staff station shall consist of an intercom unit and vandal proof push button mounted on a rectangular, 3mm thick, brushed stainless steel plate.

The loudspeaker shall be a water resistant unit with a plastic cone. The loudspeaker installation shall be such that tampering and water damage is eliminated.

The finish of the speaker enclosure shall be of high quality, neatly finished and shall not require any paint or protective covering. The opening in the cover shall be situated in a manner that the speaker cannot be damaged from the outside by protruding obstacles through the sound cavities.

4.5.7 Visitor Speaker Stations

The tendered rate shall include full compensation for the supply and installation of a Visitor station set. The inmate side shall have a vandal proof telephone handset with built-in push button. The back-boxes shall consist of 45 deg surface mounted stainless steel boxes with associated fixing equipment cable, ferrules etc.

Visitor Intercom units shall be designed/constructed/installed as follows:

- Front plate to be stainless steel 3 mm thick.
- The Speaker grille will be a grid pattern of vertical slots.
- A 2 mm thick baffle plate with a corresponding 3 mm offset grid pattern.
- Mylar speaker with 3 watt power rating.
- The microphone is on the visitor side is to be an Electret type with a minimum 36 DB dynamic range.
- An exterior, which does not facilitate the concealment of contraband.
- A tamper alarm separate to the call alarm to notify the respective operator station of an intercom unit's removal.
- Build in 1-Watt amplifier with software adjustable gain.
- Cabling shall be CAT6 UTP, full duplex transmission of speech.
- Adjustable microphone sensitivity

4.5.8 Public Address Speaker Stations

The tendered rate shall include full compensation for the supply and installation of a Public Address station, with a built in 10W amplifier. The back-box shall consist of a 45 deg surface mounted with associated fixing equipment, cable, ferrules etc.

Public Address Intercom units shall be designed/constructed/installed as follows:

- Front plate to be stainless steel 3 mm thick.
- The Speaker grille will be a grid pattern of vertical slots.
- A 2 mm thick baffle plate with a corresponding 3 mm offset grid pattern.
- 2 x Mylar speakers each with 3 watt power rating.
- An exterior, which does not facilitate the concealment of contraband.
- A tamper alarm separate to the call alarm to notify the respective operator station of an intercom unit's removal.
- Build in 10-Watt amplifier with software adjustable gain.
- Cabling shall be CAT6 UTP, full duplex transmission of speech.

4.5.9 SIP Compatible IP Telephone

The tendered rate shall include full compensation for the supply, installation and Commissioning of a SIP Compatible IP Telephone. SIP Phones shall be installed in offices as indicated on the accompanying drawings, and shall be integrated with the Intercom system in order to make calls to individual Intercom and Public Address Stations, or groups of stations which shall be configurable within the Security Management System.

The SIP Phones shall comply with the following specification as a minimum:

- Connections: POE compliant Network: RJ45 (Ethernet)
  Power: 5 V DC (stabilized)
  Handset: RJ11Connector
  Headset: RJ11 connector

  User Interface: 1 x 24 Character display
  18 x Keys

		6 x Programmable Function Buttons
		Speaker Phone Menu Driven Interface 4 x Simultaneous Calls Keyboard Lock
•	Call Features:	Call Hold Call Transfer Call Divert Call Intrusion Music on hold support
•	Security:	VLAN (802.1pq) Transport Layer Security (TLS) SIPS
•	SIP:	UDP, TCP Support RFC3261 Compliant In and Out-of-band DTMF (RFC2833) Offer/Answer (RFC3264) Error information support

4.6 Digital Audio Recording System

A digital voice recording and playback system shall be supplied and installed as part of the Works.

The central processor and associated peripherals shall support digital recording for a minimum of 1024 channels without the requirement for additional central processors installed in each local area.

The system shall support up to 32 simultaneous channels of voice data information per processor.

Time and date stamping shall be automatically logged for all audio channels.

The voice recording system central processor shall provide immediate access to, and recording of, voice inputs via an onboard storage medium to a minimum capacity of 8760 hours of on-line data.

A CD-drive shall be installed as part of the central processor configuration for the archival of data.

The audio recording system shall provide the following alarm conditions:

- Recording medium capacity consumed by 80%
- Audio recording system non-operational due to power failure or failure of unit to record.

When the hard disk reaches full capacity the system shall automatically over write the oldest dated data file. Access to the voice recording system shall be controlled by password authorization. A minimum of three levels of access rights shall be provided.

The Intercom system supplied and installed, as part of these works shall be interfaced to the voice recording system.

All voice communications shall be automatically recorded on a digital recording medium with time and date being encoded on the same channel as each conversation.

4.7 Non-Contact Intercom Stations

Provide individual audio monitoring and recording of the non-contact visiting booths in the nominated locations.

Provide visitation intercom stations to the same specification to that of the cell and passage intercom stations, however without the call button.

All voice communications shall be automatically recorded on a digital recording medium with time and date being encoded on the same channel as each conversation.

4.8 Door Intercom Operation

The door intercom system shall be configured to provide the following functionality:

In general, when a door intercom point is activated the intercom shall be answered from the relevant GUI (Graphical User Interface) operator station or Intercom GUI via a dedicated handset.

The GUI terminal shall include a graphical display to connect and cancel intercom calls as elected.

In the event of a door intercom point not being answered within the default time period of 30 seconds or the relevant GUI operator terminal being off-line the call shall automatically divert to the Central Control Station.

4.9 Public Address System

The public address system shall be provided as an integral part of the Intercom system.

The system shall include internal public address to nominated buildings via ceiling or wall mounted speakers and externally mounted speakers for non-building areas such as exercise yards and external association areas at the locations indicated on the drawings.

PA stations shall be provided with a built-in 10W audio amplifier, and shall be capable of providing a continuous music channel if required.

4.10 Cabling

Bus Cabling between individual intercom and PA stations shall consist of the following:

1. 1 x 3 Core 1,5mm Power Cable

2. Cat6 UTP Data/Digital Audio Cable.

All intercom circuit cabling shall be terminated to the relevant Ethernet Switches situated in the local control racks.

4.11 Intercom Management Software Module

The Intercom System software functionalities are to be built in functions of the Security Management Operator Workstation software.

Due to the complex nature of the sub-system integration required by the system it is imperative that the Supplier of the Security Management System provides a direct interface (driver) to the sub-system hardware offered in this tender, and that the functions described are built in functions of the software.

4.11.1 Minimum Intercom Management Module (IMM) Features

1. The IMM shall be an integrated function of the Security Management System.

2. The IMM will offer a complete intercommunication solution that will be scalable from one to thousands of intercom stations that can be added on a unit-by-unit basis

3. The IMM shall provide as a minimum the following features:

    - Station Call-In
    - Station Fault Analysis
    - Call In Divert
    - Call Answer
    - Call Cancel
    - Call-In Queuing
    - Tamper Alarm per station
    - Individual station Speaker and Microphone sensitivity adjustment

4. The IMM shall allow the following primary functions:

    - Connection and disconnection of Intercom Stations

- Automatic termination of a previous selection and connection of a new station with a single mouse action
- Configuration of monitoring areas (site maps and workspace)
- Programming of alarm-triggered automatic events
- Integration of Intercom alarms and events with other security sub-system hardware.
- Logging and Management of Intercom Hardware alarms and events

5. All operator functions shall be controlled by means of a mouse, and shall require the minimum movement and actions in order to complete a required task.

6. Alarm processing, alarm logging, alarm response data entry, graphical and text based user interface, data entry, and other system management functions shall be performed by the GUI (Graphical User Interface) operator workstations. The operator workstations shall be located in the Central Control Room and other nominated locations.

7. The IMM shall be fully programmable to allow:

   - Response instructions to be displayed for all alarms types.
   - Use dynamic (real time) graphics to display device status.
   - Initiate operator commands via system tailored icons.
   - Display building layouts in a graphical representation.
   - Easy to follow menus with single key select options, to assist in the daily routine operations of each facility.
   - Allocate alarm priorities.
   - Set Alarm response properties.
   - Set lock/unlock and access/secure operating schedules.
   - Generate User defined reports.

8. The contractor shall allow adequate time to liaise with the Engineer in order to detail any user specific requirements necessary for the operation of each building, system, alarm type, and alarm response configuration within the system. This shall include the configuration of maps, report formats, access schedules, alarm response instructions and the like, to suit each operator workstation.

9. The system shall be modular in design to allow for future system expansion (i.e. in excess of 200 % of specified capacity) with minimum cost and disruption to the existing operational system.

10. Tenderers are to specify the systems total capacity for future expansions.

4.11.2 System Performance:

4.11.2.1 Central & Movement Operator Workstations

The interaction delay between activating a control icon on any given operator workstation and the controlled point activation, (i.e., the cell station), shall be no greater than one second (1 sec).

The interaction delay between controlled point activation and any given operator workstation response either by activation of an audible alarm and/or the associate icon changing state (color) shall be no greater than one second (1 sec).

The interaction delay between recalling any floor plan at any given operator workstation shall be no greater than one quarter of one second (0.25 sec).

4.11.2.2 Local Operator Workstations

The interaction delay between activating a control icon on any given operator workstation and the controlled point activation, (i.e., the cell station), shall be no greater than one second (1 sec).

The interaction delay between controlled point activation and any given operator workstation response either by activation of an audible alarm and/or the associate icon changing state (color) shall be no greater than one half of one second (0.5 sec).

5 ACCESS CONTROL SYSTEM

5.1 Introduction

The Access Control system offered shall consist of a Biometric based system with Fingerprint Recognition being the primary identification method, and Proximity/Contact less card detection as the secondary means of identification. The system shall provide a fast, accurate and versatile solution capable of managing a minimum of 20,000 users.

The Access Control Terminal (ACT) offered shall incorporate both Finger recognition and proximity/Contact less card recognition within a single housing. By default, 1 to Many (1:N) fingerprint matching shall be utilised for identification, and only in cases where a users fingerprint cannot be captured, shall a proximity or Contact less Mifare card be used.

The Access Control Terminals shall be Vandal Resistant in construction and shall be capable of being mounted either indoors or outdoors, and shall offer an IP65 protection rating.

The Access Control Terminals shall be able to connect directly onto an existing Ethernet network (100baseT), and shall be capable of operating in a standalone configuration, without the need for a separate field controller. The terminal shall provide the necessary on-board secure Input/ Output points necessary to control and monitor a single door.

The Access Control Terminal shall consist of an embedded real time device with on-board database management, including the ability to configure and process daily, weekly, monthly and holiday schedules.

Anti-pass back management can either be a function of the Access Control Terminal directly or via the Access Control Module of the Security Management Software provided. It shall be acceptable to provide Anti-Pass back management via a centralised server provide dual redundancy is employed on the servers.

5.2 Minimum Device Features

- Enclosure rating: Vandal resistant, Weatherproof (IP65) Enclosure
- Identification: 1:N and 1:1 Identification and Authentication
- 1:N Matching rate: < 1 second per 2500 Templates
- Template Capacity: Minimum 8000 templates on board storage

- Database Capacity: Minimum 8000 Users on board storage
- Anti-pass back Management: Local or centralised
- Card Reader: Proximity or Contactless Mifare reader
- Operating Parameters: Configurable
- Integration to SMS: Ethernet, via SDK
- Communication: 100BaseT, RSS232, RS-422, Wiegand In and Out
- Time Synchronization: To Security Management Server
- Offline transaction logging: Minimum 20000 events

5.3 Terminal Software Requirements

1. The terminal application shall run on an embedded operating system.
2. Anti-pass back by means of Peer to Peer of centralized server.
3. Configurable Operating Parameters shall enable project specific functionality.
4. Remote configuration of the terminal parameters shall be possible via Ethernet.

5.4 Terminal Hardware Requirements

5.4.1 Technical Specification

- Housing: Vandal Resistant Polycarbonate Enclosure
- Optical Scanner Resolution: Min 500 dpi (280 x 320 pixels)
- Platen Area: Min 16mm x 19mm
- Distortion: <1.0%
- Keypad: Minimum 2 Button Entry, Exit
- Status Indication: LCD or LED multi-colour display
- Beeper: On Transaction events
- Terminal Security: Tamper switch with system notification
- Authentication Time: < 1.0 second

- Identification Time: < 1 second per 2500 templates
- False Acceptance Ratio: 1 in 10,000 or better, configurable

5.4.2 Communications

1. Ethernet 100baseT
2. RS 422
3. RS 232
4. Wiegand In
5. Wiegand Out

5.4.3 Input Output Points

a.) Configurable High Impedance Inputs: Minimum of 1 (Door Status)
b.) Configurable Outputs: Minimum of 1 (Door Open command)
c.) Security Alarm: Minimum of 1 (Device Tamper)

5.4.4 Environmental Characteristics

a.)	Installation:	Outdoor/Indoor vandal resistant applications
b.)	Operating Temperature:	0 ° C to 50 ° C ambient
c.)	Storage Temperature:	-20 ° C to 50 ° C
d.)	Relative Humidity:	0%to 90%, non-condensing
e.)	Protection Rating:	IP65 (Fluid and dust ingress)

5.4.5 Power

a.)	Power Supply:	12 VDC +-5%
b.)	Load:	Maximum 2.5A
c.)	Battery:	Integral backup battery

5.4.6 Terminal Options

Internal Proximity Card Reader or Internal Contact less Mifare Reader

5.5 Mounting

A wall mounting back plate shall be provided to mount over a standard 4 x 2 electrical draw box the rear of the terminal shall protrude over the wall plate flush with the wall. The access hole in the wall for the wiring shall be completely covered by the back plate eliminating the possibility of tampering with power and data cables.

All cabling shall be rear entry and terminate onto the terminal with Molex or equivalent type connectors.

The terminal shall be mounted at a height that is comfortable to use. In general, the reader shall be mounted such that the height of the sensor (top of the device) is between 1.2m and 1.35m from the ground.

5.6 USB Enrollment Finger Print Reader

5.6.1 Technical Specification

- Housing Type: Stainless Steel Vandal Resistant
- Interface Type: USB 2.0 Compatible standalone Reader
- Sensor Type: Optical
- Min Resolution: Min 500 dpi (280 x 320 pixels)
- Min Imaging Area: 16 x 18mm
- Operating Temperature: 0 to 50ºC

5.7 Software Requirements

1. The Access Control System (ACS) shall be provided as an integrated function of the Security Management Systems in order to provide interlock functions between sub-system hardware such as CCTV Cameras, Fire System etc. The System shall not require the installation of vendor specific software for the enrollment of users, terminal configuration, template downloads etc. These shall be integrated functions of the Security Management System.

2. The ACS shall control the automatic locking and unlocking of nominated doors, grilles, roller shutters and gates as further specified and as indicated on the drawings and in the Bill of Quantities.

3. The ACS shall allow control of doors either by the finger print reader, proximity card reader/Contactless Mifare Reader, locally mounted door release push button, or overridden by the Security Management Workstations.

4. The System shall record all movements and activities at each control point.

5. The software shall support a minimum of 200 access groups where each access group contains a list of control points to which a user has authorized access. The System shall allow authorized users to enable, disable, or edit access control parameters (e.g. time zone control, holidays) of each access group.

6. The System shall allow any user to be included in one or several access groups.

7. The System shall allow individual users to be enabled or disabled by authorized users via any SMS Workstations, based on parameters such as time or zone control, time of day with contingencies for day of week, holidays and device status.

8. A minimum of 50 programmable time schedules shall be provided for full flexibility in the automatic locking and unlocking of buildings, as well as for controlling all users on combined time schedules and access groups. Time schedules shall include holiday facilities.

9. All schedules shall be defined by day, hours and minutes.

10. System programming, scheduling, proximity card validation and other system set up shall be carried out from the Security Management Workstations. Only authorized users shall have access to database information for review and or modification.

11. The system shall be designed such that any failure in this Sub-System shall not affect the operation of other Sub-Systems.

5.8 Software Features

The system software shall incorporate the following features:

1. Provide a Staff Database with at least the following fields:

    a. Employee Reference Number

    b. Users Name

    c. ID Number

    d. Sex

    e. Date of Birth

    f. Address

    g. Contact Telephone Number

    h. Enrollment Date

2. Provide a Visitor Database with at least the following fields:

    a. Visitor Reference Number

    b. Visitor Name

    c. ID Number

    d. Sex

    e. Date of Birth

    f. Contact Address

g. Contact Telephone Number

h. Enrollment Date

3. The System shall allow retrieval of User information based on Employee Reference Number, Staff Reference Number, Name or any other database field.

4. Invalid' transaction messages shall indicate the reason for denied access and also capture the location, date and time. 'Invalid' transactions shall also display the name of the User, his photograph, and generate an alarm.

5. It shall be possible to control any combination of outputs (e.g. access controlled doors, electrically operated locks, roller shutters, system outputs, etc) automatically on a preset user-definable time schedule basis or manually via the SMS Workstations.

6. System Administrators shall be able to create, modify, assign and delete Users, Users information, access level and time schedules from the SMS Workstations.

7. The System shall be able to cater for holidays, weekends, special occasions and other time zones.

8. The ACS database shall be held within the System and automatically updated to create a single global database to service all SMS Workstations and the other Sub-Systems across the network.

9. Disabling of Users shall be immediate.

10. Each Access Control Terminal shall be assigned an English text description which shall be displayed when the point/reader/card/alarm is displayed or logged by the system.

11. All system alarm inputs shall be allocated an alarm priority.

12. The System shall log all events and alarms with description, time and date stamps.

13. Emergency unlocking of a group of selected doors shall be made available for the operators. In the event of an emergency, the selected doors shall be opened and must remain opened by the authorized operators using the SMS Workstation. The authorized operators shall be able to resume normal operations (i.e. secure mode) using the SMS Workstation.

5.9 Monitoring and Control

1. The system shall be able to monitor and control all Input alarms and Output controls available on the Access Control Terminal including but not limited to the following:

    a. Finger print reader Status

    b. Proximity card reader status

    c. Electric/magnetic lock

    d. Door Position Switches

    e. Request to exit push button

    f. Break glass alarm device (where applicable)

2. The door control relay activation time shall be user configurable.

3. The door monitoring input alarm shall be suppressed during a valid entry or exit, and shall provide an immediate alarm indication when a door is forced open. This shall be displayed on the SMS Workstations as a 'door opened manually' alarm.

4. If the door is opened during a valid entry or exit and held open for longer than a pre-determined user-definable time, a 'door open duration' alarm shall be generated. The period for which the door may be held open prior to initiating an alarm shall be user configurable for every individual door.

5. The Access Control Terminals shall utilize the following to determine whether access shall be granted:

    a. User Group

    b. Time Schedules

    c. Holiday Schedules

    d. Anti-pass back status

6. It shall be possible to assign a user to any combination of Access Control Terminals during designated time schedules.

7. When communication between any Access Control Terminal and the SMS servers are disrupted, the Terminal shall continue to work off-line, with all valid Users still being screened for authorized entry and initiating status control and alarm messages. After re-establishment of communication, the Terminal shall update all events to the SMS servers automatically.

8. The Security NSC shall provide power supplies and batteries required to support a minimum of 2 hours operation in the event of a mains power failure. Note: The device internal battery will last +/- 45 minutes.

5.10 Inmate Roll Call Function

System Operation

1. A roll call function shall be provided as an integrated function of the SMS, using the access control terminals provided as part of this tender. The software function shall be configurable to either enable or disable the function as required.

2. The roll call function shall be initiated or cancelled by a central control room operator configured at an appropriate user level (Supervisor or Manager), by selecting function button/s on the Security Management System Menu. A function confirmation window shall be provided requiring the operator to confirm the initiation of the function by selecting "Yes" or "No".

3. The Security Management System shall be capable of configuring the access control terminals used as roll call Stations. The initiation of the roll call function from the central control room shall automatically switch the appropriate access control terminals into "Roll Call Mode".

4. The roll call procedure shall require all inmates within a designated area of the facility to form a line and one after the other to place their fingers on the access control terminal's fingerprint reader to record their presence. The access control terminal shall provide a clear audible and visual confirmation of a positive read. The terminals shall be capable of processing inmates at a rate of 1 every 3 seconds. The system shall be capable of storing the results of the last 30 roll calls and will provide for automated methods of comparison.

5. The roll call function shall provide the ability to initiate a roll call based upon:

    a. A default configuration, whereby a preconfigured group of access control terminals simultaneously enter roll call mode.

    b. An ad-hoc group of access control terminals by specified area.

    c. An ad-hoc group of access control terminals within the facility.

6. The system shall be capable of pre-configuring a group of access control terminals, which shall constitute the default group upon which the roll call procedure shall be run upon initiation from the central control room. By initiating the roll call function from the main menu, all access control terminals in the default group shall simultaneous switch to "Roll Call Mode".

7. It shall be possible to terminate the roll call procedure at individual roll call Stations once the staff member responsible for supervising the process has confirmed that all inmates have completed the procedure. The procedure shall be terminated by the Warder placing a pre-configured proximity card onto the appropriate access control terminal's proximity reader. The access control terminal shall resume normal operation immediately upon termination of the roll call procedure.

8. Upon initiation of the roll call function, the system shall prompt the Operator to verify the current inmate count. The current inmate count held in the inmate database shall be presented to the operator, however providing the operator with the ability to override the count should the database count differ from the manual

record. In the event of the count being overridden, the event shall be logged and flagged as an exception to the appropriate department.

9. The system shall provide two modes of verification, namely "Current Inmate" and "All Inmate" modes. "All Inmate" mode shall attempt to verify the finger prints read during the roll call procedure against all prisoners ever registered in the facility in an attempt to automatically correct the database of current inmates, where inmates may have been incorrectly recorded as having been released. "Current Inmate" mode shall only attempt to verify the readings against the current inmate database.

10. Inmate registration shall be performed on a dedicated inmate registration workstation equipped with a vandal proof Access Control Terminal (Fingerprint reader). A dedicated Workstation is specifically required in order to avoid the possibility of incorrectly recording a user's identity i.e. Inmate, Staff or Visitor.

11. The number of fingers registered against an inmate's record shall be determined during configuration of the system (1-10 fingers selectable). In cases where none of the inmate's fingers can be registered, and only in such cases, the system shall generate a printed proximity card containing the inmate's name, image and DCS number. Such cards shall remain in the possession of the supervising Warder who shall place the card against the proximity reader during the roll call procedure, once an inmate's identity has been manually verified against the details on the card. The system shall record the unique proximity card identification number, which shall constitute a valid inmate count.

12. The centralized database server provided as part of this tender shall poll the access control terminals in the various locations immediately upon completion of the roll call procedure and retrieve, synchronize and perform a 1:N search against either the current database or the entire database dependant on the mode selected.

13. Integration with the Security Management System shall enable each access control terminal in the facility to be graphically represented by means of a suitable icon on the operators graphical user interface. The Icon representing Terminals that are currently in roll call mode shall be clearly distinguishable from those that are not, by either a static border of an alternate colour or a flashing border.

14. The access control terminals in the field that are currently in roll call mode shall be clearly identified by a fast flashing LED or a suitable alternative approved by the Engineer.

15. Access control terminals in roll call mode shall operate in a continuous registration mode requiring no other interaction with the terminal other than presenting the inmates fingerprints one after the other. Failure by the supervising Warder to present the "end of roll call" proximity card, shall result in the unit defaulting to normal operation after a configurable period of time.

16. The system shall be capable of storing and comparing historic roll call reports.

17. The system shall allow for "incremental adding" in case of a particular Roll Call Reader procedure being accidently terminated. In such a case it shall be possible to restart the roll call procedure in the affected area and only the remaining inmates being able to register. Incremental counts shall be reset daily.

System Reports

18. The system shall have the ability to provide reports in HTML format.

19. The system shall be capable of generating the following reports as a minimum:

    a. Roll Call Summary Report (by area)

        i. Number of inmates identified

        ii. Number of inmates identified with Proximity cards

        iii. Number of fingerprints read but not identified

        iv. Number of inmates not identified

    b. Detailed Roll Call Report

        i. List of inmates identified (Name, DCS Number, Identification method, Area)

        ii. Number of inmates identified per area

        iii. List of inmates not identified (Name, DCS Number, Area)

20. Acceptance of the "Inmates Identified" report shall automatically update the Area field in the inmate's database to the location according to the last roll call.

Discrepancy Reporting and Response

21. The following discrepancies shall be logged and reported:

    a. An inmate is not registered

    b. An identified inmate is currently recorded as having been released

    c. An inmate identified in an alternative location

5.11 Guard Tour Function

1. A Guard Tour function shall be provided as an integrated function of the SMS, using the access control terminals provided as part of this tender. The software function shall be configurable to either enable or disable the function as required.

2. The system shall consist of a Centralized Server with Client Operating stations. The Server shall be responsible for the logging of data; the generation of automated archives, system health checks and the enforcement of Guard Tour system rules. The client Workstation will be utilized for the day to day user administration of the Guard tour function. The software will provide for the following essential functions:

    a. View of current historical and archived summary and detail reports

b. Daily allocations of pre-configured Guard Tour profiles to relevant staff members

c. Issuing of staff schedule summaries

d. Live Management overview of the system in operation, including the ability to "Cancel" a particular schedule due to an abnormal condition (like a Guard having to attend to an injury and thus not able to fulfill a scheduled deadline)

3. The system shall specifically provide for "automated adjustments" and configurability so as to minimize incorrect and false reports. These include the following:

    a. Ability to handle more than a thousand Guard Tour system points being a combination of hard input (presence button) or Biometric in nature

    b. Ability to provide for a configurable window in which a particular point must be reached

    c. Provision for a flexible start time

    d. Provision to easily adjust the amount of Guard Tour rounds with configurable dead time

    e. Ability to adjust the "fault tolerance" within an associated Guard Tour group in order to allow for possibility of equipment malfunction (for example a particular presence button not working) or an accidental "miss" by the Guard on route.

4. The system shall specifically provide for "automated methods" and configurability in order to minimize day to day user impact on system operation. These include the following:

    a. Provision for the editing and saving of Guard Tour profiles

    b. Provision for automated archiving of data

    c. "One button" click to allocate a particular user to a particular Guard Tour route (a daily Management function)

    d. Automatic expiry of allocated Guard Tour schedules

5. Schedules shall be flexible and shall allow for combinations of overlap, no overlap, dead time and fixed time within blocks and associated Guard Tour functions within the Facility.

6. User-level security controls will be in place for restricting unauthorised setup and operations.

7. The system shall have the ability to assign multiple tours to guard.

8. The system shall have the ability to change tour sequences and the quantity of rounds for each guard. The operator must also be able to cancel a whole tour or part of a tour.

9. Guard tour allocations will be assigned to each guard prior to the tour starting. The administration, setup and assignment process should take no longer than 5 minutes per guard.

10. The system should allow for a management view to show all currently active tours in either a detailed or summary format.

11. Biometric Terminals at block entrances shall have synchronized clock displays. Time will be synchronized with the Guard Tour system time and an audit trail of this system will be provided.

12. All operator initiated administrative changes affecting the guard tour system must be logged.

13. The system shall provide for reports in HTML format.

14. Reporting will be available for both live tours and archived tours.

15. Reporting will have an option for all daily tasks in either a summary or detailed format for each guard on duty.

16. Reporting will have an option for exceptions, along with filters to report only required exceptions. These filters will include period by date, activations in scheduled time, outside of scheduled time and non-activations in scheduled time.

17. It shall be possible to demonstrate the suitability of the system for the particular environment and to provide a reference of the particular system in use in such an environment.

5.12 Attendance Function

1. Nominated locations shall be supplied and installed with Access Control Terminals to provide a time IN and time OUT function via dedicated terminals.

   This attendance function shall be logged and recorded by the System. The Security NSC shall provide labelling to identify the respective dedicated IN and OUT terminals at each location.

2. This function shall operate on a 24 hour per day 7 days a week basis.

3. An alarm shall be provided to the respective SMS Workstations if a finger print or proximity card is presented outside of the programmed times allocated.

4. It shall be possible to demonstrate the suitability of the system for the particular environment and to provide a reference of the particular system in use in such an environment.

5. Detailed configurable Time and Attendance reporting shall be generated for each individual Staff member.

5.13 Thermal Printer & Access Cards

A Thermal Printer shall be provided as part of this tender, and shall be installed within the Central Administration Block together with the Management Workstation. The printer shall be used to print Access Control Cards for the following purposes:

1. Staff Members whose finger print/s cannot be registered at the Enrollment Station.

2. Temporary Visitor Cards

3. The Access Control Cards to be provided as part of this tender shall be printable PVC Cards with incorporated proximity or Mifare technology.

5.14 Thermal Printer Specification

- Print Method: Dye-Sublimation / Resin Thermal Transfer
- Resolution: Min 300 dpi (11.8 dots/mm)
- Colours: 16.7 million / 256 shades per pixel
- Print Speed: 30 Seconds/Card (YMCKO), 5 Seconds/Card (Black)
- Card Size: 85.6mm x 54mm
- Print Area: CR-80 edge to edge
- Card Types: PVC or Polyester with polished PVC finish
- Input Hopper: 100 Cards
- Supply Voltage: 240 VAC

5.15 Printable PVC Proximity Card Specification

- Transducer: 40 bit R/O, EM4001,TEMIC e550, eq
- Read Range: Up to 30mm
- Dimensions: 86 x 54 x 0.08mm
- Material: PVC with a printable gloss surface
- Frequency: 125 KHz excitation / 62.5 kHz return
- Temperature: -40º C to +70º C
- Humidity: 0-100% Non-condensing

- Colour: White

5.16 Turnstiles

Full height turnstiles shall be provided as part of this tender, and shall be installed in positions as indicated on the accompanying drawings. All turnstiles shall be equipped with Vandal Resistant, weather proof Access Control Terminals each side of the turnstile, which shall be linked with the Access Control Software Module within the Security Management System offered.

5.16.1 Turnstile Specification

- Number of Arms: 4
- Traffic Volume: High Traffic
- Security Rating: High Security
- Minimum Entrance Width: 500mm
- Maximum Height: 2200mm
- Maximum Width: 1500mm
- Base Bearing: Corrosion resistant, Self lubricating, Zero Maintenance
- Lock Mechanism: Corrosion resistant, Zinc plated
- Single Rotation Safety: Anti-trap System
- Rotation Options: Free Rotation, Mechanical & Electrical Override
- Finish: UV Resistant exterior powder coating, Black
- Rotor Mounting: Suspended with shock absorption
- Power: 240V AC
- Reader Brackets: Both sides, Size as per reader requirements
- Integration: Potential Free I/O Interface

5.17 Boom Gates / Spike Barrier Combination

Boom Gates incorporating a flush mount spike barrier shall be provided as part of this tender, and shall be installed in positions as indicated on the

accompanying drawings. All Boom Gates shall be equipped with Vandal Resistant, weather proof Access Control Terminals on the incoming side of the Boom Gate, which shall be linked with the Access Control Software Module within the Security Management System offered.

5.17.1 Boom Gate Specification

- Boom Arm Length: 4.5m with Jack Knife Kit and anti pedestrian curtain
- Boom Height: 900mm above road level
- Boom Arm Construction: Extruded aluminium, Epoxy coated white with red reflective tape
- Duty Cycle: 100% (High Traffic)
- Locking: Open and Closed positions
- Motor: 240V AC, 50Hz, 60W, 100% Duty Cycle with instant reverse capability
- Cycle Time: <5 seconds per open or close cycle.
- Cabinet: IP54 Enclosure, 1.6mm Stainless Steel 3CR12, Epoxy coated white with red top section
- Power Failure Position: Default to 85% of full Open position
- Reader Pedestal: Incoming Side, Stainless Steel Goose Neck
- Integration: Potential Free I/O Interface

5.17.2 Spike Barrier Specification

- Spike Barrier Length: 4.5m
- Spike Height: 90mm above road level with dual direction protection
- Spike Construction: Galvanized Mild Steel Construction
- Mounting: Flush with road level
- Weight Capacity: Minimum of 100 Ton rating
- Duty Cycle: 100% (High Traffic)
- Motor: 240V AC, 50Hz, 60W, 100% Duty Cycle with instant reverse capability

- Cycle Time: <2 seconds per open or close cycle.
- Safety: Interlocked with Barrier to avoid lifting of barrier prior to lowering of Spikes.
- Power Failure Position: Spikes down
- Emergency Trigger: Potential free Input

5.18 Remote Panic Detection System

5.18.1 General Characteristics

The following functional features shall be provided by the proposed system:

1. Be able to detect a standard security remote (pre-programmed) at 433MHz, where the panic remote could be a DIP switch or a non-DIP switch type.
2. The Panic remote enclosure shall have a slot to enable it to be tied to a warder's belt.
3. The unit connection to external hardware shall be via a potentially free contact.
4. Be able to detect RSSI (signal strength) and the particular panic button RF pattern in order to eliminate the risk of false alarms.
5. Where an activated panic remote is detected by more than one receiver, the system shall have the ability to detect which of the receivers is closer to the panic remote in question.
6. Detection range shall be a minimum of 40m line of sight.
7. Unit shall be IP65 rated, suitable for outdoor installation.
8. The system shall be capable of detecting a cable fault, the disconnection of the unit or the unit not being operational.

5.18.2 Software Operation

The Graphical User Interface shall interface with the Distributed Remote Panic Detection System. The location of the alarm shall be clearly represented both graphically and in text format. Various configurable options shall exist for the alarm handling such as "Force to Acknowledge", "Popup Window", "Automatic Camera Selection", "Jump to correct screen", etc All alarms and associated Operator Acknowledgements shall be logged in the

Events History Database with an automatic archiving facility. The software shall display the current health status of the Remote Panic Detection System.

6 COMPRESSED AIR SYSTEM, LOCKS AND LOCKING DEVICES

This section includes the pneumatic locking and operating devices, under electrical control, for individual swing and sliding prison doors.

6.1 System components:

1. Air compressors and storage tanks
2. Filtering and drying equipment
3. Air lines and associated fittings
4. Pneumatic swing door locks
5. Pneumatic sliding door locking devices

6.2 Compressed Air System and Components:

The tenderer in accordance with the component manufacturer's product requirements shall adequately size specific system components. The system shall be designed to provide a spare capacity of 100% of the normal operating load.

6.2.1 Air Compressors

The proposed Air Compressor shall be manufactured in accordance with ISO 9001 standards, and shall be certified in accordance with the following:

CEE 89/392 machinery Directive

- CEE 87/404 simple pressure vessel Directive
- CEE 73/23 low voltage Directive
- Output measured in accordance with ISO 1217

A dual Screw driven air compressor system shall be provided with the individual compressors being mounted on CEE 87/404 approved air receivers.

The compressors shall be self-contained units incorporating all of the necessary filtering and air-drying components. The units shall comply with the following technical specifications:

- Air-End — VT Rotary single stage air-end
Lubrication by means of oil injection
Drive male rotor RM with a five lobe, offset profile

	Drive female rotor RF with a six flute, offset profile.
• Motor	7.5 kW - 10HP IP55 three phase 2 pole enclosed rated speed - 3000rpm @ 50HZ; 3600rpm @ 60Hz insulation class F, service class S1.
• Fan	Two pole, three phase, protection rating IP45, insulation class B, Direct coaxial.
• Drives	Motor and compressor: Removable taper bushing pulleys and toothed v-belts.
• Air dryer	Thermostat controlled cooling cycle, direct expansion, with Freon R134a gas. Pressure due point temperature 3 deg C.
•	Clean air filtering degree 0.01um.
• Capacity	145 psi / 1000 kpa – 1 .15 m3/h (1150 Litre/Min) based upon ambient air temperature of 20 degrees and atmospheric pressure of 100 kpa.
• Working pressure	145 psi / 1000 kpa.
• Noise level	64 dB (A) Measured in accordance with ISO 3744 +/- 3dB (A).
• Max Dimensions	1170(W) x 650(D) x 1660(H).
• Max Weight	335 kg.
• Air receiver	275 or 500 litre
• Maximum installation altitude	1000m
• Minimum ambient temperature	+5 deg C
• Maximum ambient temperature	+40 deg C

The compressors and pneumatic storage vessels shall be sized such that each compressor has the ability to meet the total air requirements under normal operation and not exceed a maximum 40 % duty cycle. The compressors shall be sized in order to provide sufficient air. The minimum size of pneumatic line between the remote pneumatic storage tanks and the doors that shall be 10mm, unless otherwise specified.

The following operational requirements shall be considered in order to size the compressor units:

1. **Cell and Stair Devices**: 8 operations per 24 hour period with a maximum of 4 operations in one hour

2. **Medium Use Corridor Device**: 150 operations per 24-hour period with a maximum of 15 operations per hour. (90% of all corridor doors may be considered medium use)

3. **High Use Corridor Device**: 320 operations per 24-hour period with a maximum of 40 operations per hour. (At a minimum, 10% of all corridor doors may be considered high use).

    a. The compressor recovery time shall be no more than fifteen (15) minutes.

    b. The Compressor shall incorporate the necessary starters, solenoid unloaders pressure switches, control gear, overload protection, circuit breakers and all other miscellaneous items electrical and other wise to make this installation complete and in accordance with all the relevant S.A.B.S. regulations.

    c. The exhaust silencers/muffler shall possess a 60db rating or less

6.2.2 Alternating Compressor Controller:

Provide an automatic compressor controller system for the facility

1. Under normal conditions, the compressors shall alternate. If one compressor is out of service or if the one compressor fails to start, the second compressor shall take over the duties of the first. If one compressor starts but cannot fulfill the demand, both compressors shall deliver air until the demand is met. The two compressors are to be installed in separate locations, and are to provide a redundant supply line.

2. The compressor controller shall consist of, but not be limited to, across the line starters, motor circuit protectors, timers, counters, relays, pressure sensing switches and transformers with all necessary interconnection wiring.

6.2.3 Compressed Air Dryer:

1. The air dryer for each air compressor system furnished shall be an integral component of the Air Compressor, and shall not require external control equipment.

6.2.4 Compressed Air Receiver/Storage Tanks:

1. Receivers and compressed air storage tanks shall be sized to provide sufficient air storage to limit compressors to a maximum of six (6)

starts per hour and permit each swing lock and sliding door locking device to operate two (2) times without input from the compressors.

2. Storage tanks shall be required both at the compressor units as well as at remote locations for each control room area unless otherwise specified.

3. The tenderer shall be responsible for the complete pneumatic reticulation design, and will ensure that no control room shall be taken out of service if a pneumatic line elsewhere in the pneumatic installation is damaged.

4. Provide high pressure relief valves, air pressure gauges and pressure switches on all receivers and storage tanks

5. Pressure regulators shall be provided to reduce line pressure to a maximum of 900ka PA.

6. Automatic drains are to be provided, and shall be piped to the nearest floor drain

6.2.5 Air Quality

Air supplied to the devices shall have been processed through filtering, cooling and drying equipment and as a minimum, shall meet the following;

1. Solid particulate matter shall be filtered to 5.0 micron of less

2. Solid oil particles shall be filtered to 0.3 micron or less

3. Oil aerosols to be less than 0.1 P.P.M @ 30 degrees C.

4. The air must be free of water vapor to a pressure dew point of 3 degrees Celsius.

6.2.6 Air System Integrity

The air reticulation system shall incorporate a line pressure monitoring system, which shall be capable of detecting abnormal pressure drops of 0.01 bar.

The system shall be capable of detecting and isolating air leaks on both the main feed and control room supply lines. In the event of excessive air loss, the effected supply line shall be automatically terminated and the supply re-routed to the affected area.

The system shall be capable of generating an air supply status report on a 24-hour basis, and shall highlight potential problem areas where air loss exceeds pre-defined set points.

The status report shall form part of the overall system management application, which shall run on the management workstation.

6.3 Pneumatic operated security locks

Pneumatic swing door locks are to be installed in all corridor doors, where sliding devices cannot be installed due to a restriction in the corridor width, and shall be provided complete with the necessary pneumatic components and be fully integrated with the Security Management System.

6.3.1 Function

1. Normal Operation

    a. When electrical power is applied to the solenoid valve, the latch-bolt shall retract. The bolt shall remain retracted as long as power is applied.

    b. When power is removed, the latch-bolt shall extend, locking the door if closed, and allowing the door to be slam – locked if open.

2. Manual Operation

    a. Each lock shall have a local manual key override lock/unlock feature, generally keyed on two sides.

    b. Rotating the key shall mechanically retract the latch-bolt. Removing the key shall extend the bolt, locking the door if closed, and allowing the door to be slam-locked if open.

6.3.2 Components

1. Mechanical

    a. The lock shall operate when supplied with air at a pressure between 275kPa and 860kPa.

    b. The lock shall operate as a fail-secure slam-lock. The lock will unlock when energized.

    c. At least the lock body shall be made of hot dipped galvanized steel or stainless steel, but all moving and non moving parts shall be of a high quality material which is maintenance free.

    d. The lock shall be factory plumbed with a quick connect air fitting or fittings.

    e. The lock shall be a high security lock and shall conform to ANSI or an equivalent international body.

f. Cylinder extensions shall be provided for locks keyed on two sides or keyed stop side where applicable.

2. Electrical

   a. The solenoid valve shall be a low wattage, 12 or 24 VDC, continuous rated valve

   b. The lock shall be provided with a lock status switch to provide interlocking capabilities

   c. All switches shall be of the snap acting mechanical type or proximity type and shall have a 5-amp rating.

   d. Locks shall be factory wired to a plug disconnect.

   e. Lock status switches shall provide the following indications:

      i. Locked/deadlocked indication

      ii. Unsecured indication.

      iii. Door position indication.

All medium and maximum security remote controlled pneumatic operated locks for individual swinging doors will be a mortised slam-locks, with automatic deadlocking for a prison door frame installation. The lock shall be supplied complete with all its integral electronic and pneumatic components. The lock and doorframe shall be deemed part of this tender.

6.3.3 Physical Characteristics

1. The lock shall automatically deadlock when the door is slam-locked in the manual mode, even in the event of total loss or air and/or electric power

2. The lock shall have a mechanical deadlock actuator, and shall automatically deadlock when the door is closed.

3. Lock shall be designed to accept a mortise key cylinder. The key cylinder shall conform to ANSI.

6.4 Pneumatic sliding devices for cell, sally-port and corridor doors

6.4.1 Components

1. Mechanical

   a. Door rollers shall be self-lubricating, incorporating sealed lifetime lubricated bearings. Rollers shall provide smooth and

quiet operation. Full details of what is offered by the tenderer shall be included with the tender documentation.

b. The mechanism shall be guaranteed for a minimum life cycle of 1 million operations.

c. The door control mechanism shall have a proven history of installation in similar applications and the tenderer shall provide documented proof of a successful 1 Million-cycle test.

d. The door shall lock at the top and bottom in both the open and close positions.

e. The locking mechanism shall include an automatic mechanical deadlock feature.

f. The vertical lock bar shall be mechanically connected to the lock mechanism or to an emergency release latch above the door to ensure manual override.

g. Top and bottom door guides must be designed such that side motion of the door shall be limited to +- 1mm or less to significantly reduce rattle induced noise.

h. The doorframe shall fit tightly over the door opening and all gaps shall be sealed with vandal proof material.

2. Electrical:

a. All Pneumatic, electric and control equipment required for the control of a single sliding door shall be pre-assembled as a single control tray in order to simplify installation and maintenance requirements.

b. Any external status devices shall be factory wired to a multi-pin connector located on the door control module within the control tray, which is to be situated above each door.

c. All switches (mechanical or proximity) necessary for the functioning of the door, and for the required door status indication, shall be rated in accordance with the door control module requirements.

d. Individually isolated 24VDC power supplies are required for CPU and I/O requirements.

e. All solenoid valves shall be a low wattage, 24 VDC, and be continuously rated.

f. The door control module shall be supplied with status switches to provide indication and interlocking capabilities

g. The status switches shall provide the following indications:

i. Door fully closed.

ii. Door fully open.

iii. Lock bar fully down.

iv. Lock bar fully up.

3. Housing

   a. Housing covers to be constructed of 2mm (minimum) cold galvanized steel plate and shall be secured with security screws to the sliding door housing.

   b. Housing covers shall be hinged, and allow easy access to all working parts during maintenance.

   c. The door hanger slot shall be securely baffled in both the door open and door closed position.

   d. To reduce the possibility of hidden contraband, there shall be **no exposed flat surfaces** on the housing or in the door hanger slot.

      All security sliding doors installed in front of cell openings shall have an emergency release mechanism installed inside the pneumatic housing compartment, with an access point on the housing compartment for emergency release.

      All other security sliding doors shall have a hip high key release on both sides of the door unless otherwise specified.

      The key release feature shall provide for electric control under normal conditions and mechanical control in the case of failure.

      The release mechanism shall be located approximately 1300 mm above the finished floor level.

4. Normal Operation

   a. When the door is locked in the closed position, initiation of the open command shall cause the lock mechanism to release and the door to move to the fully open position and automatically deadlock.

   b. When the door is locked in the open position, initiation of the closed command shall cause the lock mechanism to release and the door to move to the fully closed position and automatically deadlock.

   c. Locking devices shall be capable of being controlled individually and in groups

   d. The door shall be capable of opening or closing at a speed of plus minus 0.3 m/s Door speed shall be independently

adjustable in each direction, and at each door within the maximum operating pressure of 5 bar.

e. The door shall decelerate as it reaches the fully open and fully closed positions by means of a mechanical cushion. The rate of deceleration shall be adjustable to ensure that the door opens and closes quietly.

f. The control mechanism shall allow for freewheeling of door in the event of total loss of air supply and /or electric power.

g. If an obstruction is placed in the path of the door, the door shall stall for a period of two seconds after which the door shall resume movement in the selected direction. The mechanism must be capable of being stalled indefinitely without harming the device or pedestrians. Once the obstruction is removed, the door should resume movement from any point in the door travel, without stalling.

h. The maximum pressure exerted on an obstruction placed in the path of the door should not exceed 100 Newton, in order to protect both pedestrian traffic and the mechanical components within the device.

i. The mechanism should not rely on differential pressure as a means of detecting an obstruction to the normal movement of the door.

j. The operator shall be capable of 'instantly' reversing the direction of door travel at any point and immediately resuming the preset travel speed of the door. The change of direction should not affect the normal operation of the door or the detection of an obstruction.

k. A key release cylinder fitted at 1300mm above finished floor level shall electrically activate the door, duplicating the open/close functions of the security control system.

5. Manual Operation

a. In the event of total loss of air supply and /or electric power, individual doors may be released manually at the door. With the lock mechanism released, moving the door manually to the open or full closed position shall cause the door to automatically deadlock.

b. Manual operation of any door shall not interfere with the normal operation of other doors.

6.5 Emergency Release System

As specified by the hardware schedule the following emergency release functions shall be provided for sliding cell door locking devices.

6.5.1 Emergency Air Release System

1. The contractor shall provide compressed air emergency release tank(s) and valve assembly in order to unlock all cell doors simultaneously in the case of an emergency. The system shall be defined in groups, which shall be activated by operating a manual air valve in the case of a total loss of air and/or electric power.

2. The emergency release tank(s) and valve assembly shall be installed in a lockable cabinet as per the architectural layout. The cabinet shall be clearly labeled “Emergency release system”

3. The emergency release system shall be totally manual in operation. Once the system has been activated, the doors shall unlock and remain unlocked until the system is deactivated. Once unlocked, doors may then be manually moved to the open position.

4. Non return valves shall be installed into the supply line of each tank to prevent a loss of emergency air pressure when the compressor is not loading the tank.

5. The air lines supplying each group of doors in the emergency release system shall be run in the same raceway/conduit as the normal air supply lines.

6. Air tubing for the emergency release system shall be a minimum of 6mm outside diameter, and shall be colour coded.

6.5.2 Manual Door Release System

1. Each cell door within the facility shall be equipped with a mechanical door release mechanism situated within each door header. In the case of a failure in the normal and emergency air supplies, the doors shall be opened manual by means of this system.

6.5.3 Manual Door Release System {Control I/O}

1. All Inputs and Output points required for the Air reticulation and detection system shall be provided by the Distributed Control System (DCS) as detailed in the specification.

6.6 Distribution Manifold Rates

The rates provided for distribution manifolds shall be inclusive of the necessary Input/Output cards required by the Air Reticulation System. No claims shall be entertained for additional Input points required for the system.

7 SECURITY HOLLOW METAL DOORS AND FRAMES

7.1 Clearance and Tolerances

7.1.1 Edge clearance shall be as follows:

1. Between doors and frames at head and jambs: 3.5mm
2. At door sills where no threshold is used: 10mm max (A.F.F.)
3. At door sills where threshold is used: 20mm max (A.F.F.)
4. Between edges of pairs of doors: 3.5mm

7.1.2 Manufacturing tolerances shall be maintained within the following limits:

1. Frames for single door or pair of doors width, measured between rabbets at the head: Nominal opening width +1.6mm – 0.8mm; height (total length of jamb rabbet): Nominal opening height +1.2mm
2. Cross section profile dimensions:
    a. Face: +1mm
    b. Stop: +1mm
    c. Rabbet: 0.5mm
    d. Depth: 1mm
    e. Throat: 1.6mm
3. Frames overlapping walls are to have a throat dimension of 3.2mm greater than dimensioned wall thickness to accommodate irregularities in wall construction section.
4. Hardware cutout dimensions:
    a. Template dimensions +0.5mm
    b. Hardware location: +1mm
5. Doors:
    a. Width: +1.25mm
    b. Height: 1.25mm

c. Thickness: 1.16mm

d. Hardware cutout dimensions: Templates dimensions +0.4mm

e. Hardware location: +0.8mm

7.2 Requirements for Security Hollow Metal Frames

7.2.1 Materials:

Frames shall be constructed of commercial quality steel, which complies with the SATM A366 standard. The steel shall be free of scale, pitting, coil breaks or other surface defects. Metal thickness shall be not less than 2mm.

7.2.2 Fabrication

All frames shall be custom-made welded units of the sizes and types shown on approve shop drawings and in compliance with ASTM F1450 and the SABS equivalent standard. All frames shall be manufactured to ANSI/ NAAMM HMMA 863-90(8d).

1. All finished work shall be strong and rigid, neat in appearance, square, and free of defects, warps or buckles. Pressed steel members shall be straight and of uniform profile throughout their lengths.

2. Jamb, header, and sill profiles shall be as scheduled by the architect and the door and frame details as shown on the approved shop drawings.

3. Corner joints shall have all contact edges closed tight with faces and stops either butted or mitered. Corner joints shall be continuously welded. The uses of gussets of splice plates will be unacceptable.

4. Minimum depth of stops in doorframe openings shall be 16mm and in glass or panel openings shall be 32 mm.

5. Frames will call switches will be provided with factory cut hole and enclosed in an enlarged lock pocket per manufacturers recommendations.

6. Frames having jamb mounted remote operated locks, door position switches, staff stations and/or other electronic hardware will be provided with factory installed back boxes and conduit with compression fitting which shall be grout tight.

7. Frames for multiple openings shall have mullion members which, after fabrication, are closed tubular shapes conforming to profile shown on approved shop drawings, hand having no visible seams or joints.

8. All joints between faces or abutted members shall be welded and finished smooth. All joints between stops of abutted members shall

be welded along the depth of the stop and shall be left neat and uniform in appearance.

9. A Styrofoam filler pad shall be permanently placed underneath each hinge reinforcement.

10. Glass stops to be match drilled and held in place by two (2) Phillips head screws. Mortar guards will be provided at each hole. The screw holes in the removable stops will be 3.2mm larger than the diameter of the screw to allow for adjustment. Screw head will be of sufficient size to conceal the hole in the removal stop.

11. All glass stop screws to be Torx self tapping

12. All frames with either stripping shall have a continuous mortar guard at the point of installation. Screw holes to be filed located by installer.

7.2.3 Hardware Reinforcements and Preparation:

Frames shall be mortised, reinforced, drilled and tapped for all tem plated hardware including surface mounted hardware in accordance with the final approved hardware schedule and tem plated provided by the hardware supplier.

Minimum thickness of hardware reinforcing plates shall be as follows;

1. Hinge and pivot reinforcements: 6mm x full width of hinge x 250mm in length.

2. Strike reinforcements; 3.5mm

3. Flush bolt reinforcements: 3.5mm

4. Closer reinforcements: 3.5mm

5. Reinforcements for surface applied hardware: 3.5mm

7.2.4 Frames & Fittings

In cases where electrically operated hardware is required and where shown on approved shop drawings, hardware enclosures and junction boxes shall be provided and shall be interconnected using galvanized steel 20mm conduit, elbows and connectors. Also, where shown on submittals drawings, junction boxes with access plates shall be provided to facilitate the proper installation of wiring. Access plates shall be the same size as the frame and fastened with a minimum of four tamper proof machines screws, but not to exceed 150mm o.c. Where frames are to be grouted in places, the conduit shall be connected to lock pockets and boxes with compression type fittings and grout tight. Frames with lock pockets and/or electrically operated hardware, which do not allow access for control conduit installation (by others), shall be provided with the conduit installed to the perimeter of the frame by the hollow metal manufacturer.

7.2.5 Floor Anchors:

Floor anchors with two holes for fasteners shall be fastened inside jambs with at least four (4) spot welds per anchor.

1. Where no scheduled, adjustable floor anchors, providing no less than 50mm height adjustment, shall be fastened in place with at least four (4) spot-welds per anchor.

2. Plate thickness of floor anchors shall be the same as frame.

7.2.6 Jamb Anchors:

1. Frames for installation in masonry walls shall be provided with adjustable jamb anchors of the yoke a strap type made from the same gauge steel as frame. The number of anchors provided on each jamb shall be as follows;

    a. Frames up to 2.25m height: 4

    b. Frames 2.25m to 2.5m height: 5

    c. Frames over 2.5m height: 1 anchor for each 450mm or fraction thereof.

    d. Frames for installation in pre-finished concrete openings shall be purchased and countersunk for expansion bolt anchors and provided with hat shaped reinforcements, same thickness as frame, secured in place with at least four (4) spot welds each. The number and spacing of anchors provided shall be as specified above.

    e. Frames to be installed in pre-finished concrete, or masonry openings, but not to be anchored using expansion bots, shall be constructed and proved with anchoring systems of suitable design as shown on the approved shop drawings.

2. Mortar/plaster guards made from no less than 0.5mm steel shall be welded in place at all hardware preparations on frames to be set to masonry or concrete openings. Preparations are to be totally sealed to prevent any mortar, grout or plaster from entering the protected area.

3. All frames shall be provided with two (2) temporary steel spreaders welded to the feet of the jambs to serve as bracing during shipping, handling and installation.

7.2.7 Removable Glazing Stops:

Removable glazing stops shall be pressed steel angles 32mm x 32mm minimum, not less than 2.5mm or 32mm x 32 m steel tubes, not less than 2mm. Stops shall be tight fitting at the corner joints and secured in place with hardened tamper proof button head torx self-tapping machine screws spaced

230mm maximum. Stops shall be installed on the most secure (non-prisoner) side of the frame. The frame underneath the glazing stops and the inside of the glazing stop shall be treated for maximum paint adhesion and painted with rust inhibitive primer prior to installation in the frame.

7.3 Requirements for Security Hollow Metal Doors:

7.3.1 Materials:

Doors shall be constructed in compliance with all the SABS standards for security doors, and shall be manufactured to the requirements as detailed in ANSI/NAAMM HMMA 863-90(8d) using commercial quality steel, which complies with the correct SABS standard. The steel used shall be free from scale, pitting, coil, breaks or other surface imperfections. The steel shall also be free of buckles, waves or any other defect caused by the use of improperly leveled sheets. Face sheets shall not be less than 2mm.

7.3.2 Fabrication:

All doors shall be custom made of the types and sizes shown on the approved shop drawings, and shall be prepared for hardware per the final approved hardware schedule.

1. Door edge seams shall be welded and finished smooth.

2. Door thickness shall be as specified by the architectural drawings and requirements. All doors shall be rigid, heat in appearance, and free from warp or buckle. Edge bends shall be true and straight and of minimum radius for the gauge metal used.

3. Face sheets shall be stiffened by continuous vertically formed steel sections spanning the full thickness of the interior space between door faces. These stiffeners shall be 1mm minimum, spaced so that the vertical interior webs shall be no more than 100 mm o.c., unless supported by test data, and securely fastened to both face sheets by welding. Spaces between stiffeners shall be filled with fiberglass or mineral rock wool batt-type material.

4. A continuous steel channel shall reinforce the vertical edges, not less than 2mm, extending the full length of the door. The top and bottom edges shall be closed with a continuous channel also not less than 2mm, welded to both face sheets not more than 75mm o.c. unless supported by test data. The 2mm closing end channel shall be continuously welded to vertical reinforcing channel at all four corners producing a fully welded perimeter reinforcing channel.

5. The top end channel shall be fitted with a flush closing channel of not less than 1.3mm. The flush closing channel shall be welded in place at the corners and at the center. Installation of closer channel using screws, security or otherwise shall be deemed unacceptable. The end

channel and flush closer channel shall be installed such that they are permanent and non-removable.

6. The security contractor shall allow for one door to be picked at random on site after installation of the door, to be cut opened to check for compliance. One security swing door and one security sliding door will be selected for this purpose.

7.3.3 Hardware Reinforcements:

Doors shall be mortise, reinforced, drilled and tapped at the factory for all template hardware including surface mounted hardware, in accordance with the final approved hardware schedule and templates provided by the hardware supplier.

1. Minimum sizes for hardware reinforcements shall be as follows;

    a. Full mortised hinges and pivots: 4mm

    b. Surface applied maximum security hinges; 6mm plate

    c. Reinforcements for lock mountings, conceals holders, or surface mounted closer: 2mm

    d. Internal reinforcements for all other source applied hardware: 2mm

    e. Lock bolt keeper closer: 2mm

7.3.4 Glass Moldings and Stops:

Where specified, doors shall be provided with steel moldings to secure glazing included in this contract in accordance with glass sizes and thickness shown on approved shop drawings or detailed else where in this document. If not specified on either of the above the tendered shall allow for 175mm x 700 mm x 6mm high impact glass for all swing and sliding doors equipped with view panels. The following door types will be equipped with view panels unless specified differently else where:

1. Control Room doors

2. Cell doors

3. Hospital ward doors

    a. Fixed glass melding shall be no less than 2mm and shall be welded to both face-sheets at 125mm o.c maximum

    b. Removable glass stops shall be pressed steel angels 32mm x 32mm minimum, not less than 2mm. Stops shall be tight fitting at the corner joints, and secured with button head, self-tapping torx screws located 230mm o.c maximum.

c. Where glass thickness dictates, 2mm offset surface mounted glass stop shall be used. The corners shall be tight fitting and the glass stop shall be secured to the face of the door using button head, self-tapping torx screws spaced 230mm o.c maximum.

7.4 Finish

All hollow metal doors and frames shall be thoroughly cleaned and coated inside and out with a fine grade corrosion resistant iron oxide-zinc chromate primer. After fabrication, all tools marks and surface imperfections shall be dressed clean by grinding, filling and sanding as necessary to make all faces and vertical edges smooth, level and free of all irregularities. Doors shall be treated to insure maximum paint adhesion and coated on all exposed surfaces with a rust inhibitive primer whish shall be fully cured before shipment.

7.5 ASTM Compliance

1. All hollow metal doors and frames provided shall comply with the following ASTM standards:

- ASTM F1643-05 Horizontal impact test – Hollow metal sliding detention doors
- ASTM F1450-05 Edge crush test – Hollow metal sliding detention doors
- ASTM F1450-05 Racking test – Hollow metal sliding detention doors
- ASTM F1450-05 Static load test – Hollow metal sliding detention doors
- ASTM F1450-05 Horizontal impact test – Hollow metal swinging detention doors
- ASTM F1643-05 Tool manipulation attack test – Hollow metal sliding detention doors
- ASTM F1643-05 Remote unlocking force test – Hollow metal sliding detention doors

2. A copy of the relevant manufacturers ASTM certification shall be submitted together with the tender documents.

7.6 MISCELLANEOUS HARDWARE FOR SECURITY DOORS

7.6.1 Product Description:

7.6.1.1 Hinges:

1. Full Mortise Detention Hinges shall be 115mm x 115mm x 6mm, investment cast stainless steel prime painted, with hospital tips and integral studs on both leaves.

2. Pins shall be hardened stainless steel, concealed and non-removable. Each hinge shall be supplied with eight (8) flat head torx machine screws.

3. Surface Mounted access floor hinges shall be 75mm x 100mm x 6mm, fabricated from bonderized steel and prime painted. Hinge barrels shall be solid with no visible pin line. Pin shall be fully welded. Each hinge lead shall be countersunk and be supplied with four (4) flat head torx screws.

7.6.1.2 Pulls

1. Grip Type Door Pulls shall be cast of brass or bronze with satin finish unless specified otherwise in hardware schedule. Overall length, 225mm hand hold, 135mm grip clearance, 40mm attachment holes, 200mm o.c. Provide tow (2) oval head torx screws. Provide clear lacquer finished baked for 15 mm at 175 degrees Celsius and allow to cool before packaging. A Push plate of the same dimensions shall be supplied for the opposite side of the door.

2. Knob Type Door Pulls shall be cast of bronze with stain finish unless specified otherwise in hardware schedule. Diameter, 80mm projection, 55mm. Provide three (3) oval head torx crews. Provide clear lacquer finish, baked for 15 min at 175 degrees Celsius and allow to cool before packaging.

3. Flush type door pulls, or equal and approved shall be cast of brass or bronze with satin finish unless specified otherwise in hardware schedule. Size, 100mm x 125mm x 4mm x pocket grip 25mm deep. Provide four (4) oval head torx screws. Provide clear lacquer finish, baked for 15 min (at 175 degrees) Celsius and allow cooling before packaging.

7.6.1.3 Magnetic Door Position Switches

Recessed magnetic door position switches shall be a magnet mortised type assembly used for remotely monitoring the door status / position. The device shall be moisture resistant and fit within hollow metal doorjamb. The device shall be field adjustable on 2 axis and supplied with a 1m vinyl jacketed lead wire and a 4 pin Molex connector. The device shall e all steel construction. The switch and magnet shall be encased in epoxy resin. The overall dimension shall be 30mm x 125mm x 25mm.

7.6.1.4 High Security Door Closer

High Security Closer/door position switches shall be controlled by overhead concealed or closers, which have been tested to ten million (10,000,000.00) opening-closing cycles. Closers shall have full hydraulic rack and pinion action with high strength cast iron cylinder. Spring power shall be adjustable from size ii through to size V.

Hydraulic fluid shall be a the region no seasonal adjustment for temperature ranging from 50 degrees C to –0 degrees C. Separate tamper-proof screw valves shall provide independent regularization of latch speed, general speed and hydraulic back check. Regulating screws shall be accessible through a heavy duty mounting plate when finish plates are removed.

Closer shall have an integral electro-mechanical device rates not less than 24 VAC @ 10 amperes to detect and signal rotation of the closer pinion. This device shall be field adjustable to allow setting for each door and fitting with a protective shield. Installation of the finish plate shall fully conceal all adjustment mechanisms.

Closer shall have an extra heavy-duty forged steel concealed arm. The low friction track roller shall be attached to the arm by a threaded mounting. Closers shall have a metal track designed to prevent jamming and to eject foreign objects placed in the track mortised into the top of the door. The exposed fasteners shall be torx drive with a security pin.

7.6.1.5 Floor Mount Door Stops

Wall or Floor Mounted Door Stops shall be a tamper resistant device that is embedded into the wall or floor with an epoxy resin adhesive. Bumper shall be the frame size in diameter x 90mm long and made from a non-hazardous silicone elastomer, 80 durometer. The threaded and grooved steel mounting shank shall be 16mm diameter and embedded into the bumper at least half the length of the bumper. Mounting shank shall extend 65mm beyond the bumper bottom for embedding into the wall of floor.

8 CONTROL PANEL SHEETMETAL WORK

8.1 General:

All control cabinets shall be adequately sized with an additional 25% spare capacity, and shall house the necessary control equipment, which shall include but not be limited to the following:

- Control system racks, modules and processors
- CPU and I/O 24VDC power supplies
- Camera 24VAC transformers
- Lighting Interface Relays
- Small power protection equipment
- Field terminations
- Intercom Pre-amplifier
- Public Address Power amplifier
- Audio switching circuitry
- CCTV Matrix
- CCTV Multiplexers
- Local Operator 19" Workstation
- Fibre Optic conversion equipment
- LAN services

Control Cabinets shall be sized so as to be installed in the locations as indicated in the contract drawings.

8.2 Panel Construction:

Metal cabinets shall be constructed of materials in size, thickness and type that are suitable for the final installation environment and normal operating conditions. All cabinets shall be IP28 rated.

1. Panels are to be manufactured with a suitable means of anchoring and/or affixing to permanent plant structures. Panels should be modular in nature to facilitate ease of installation and must have a suitable method for anchoring to adjacent panels.

2. Panels and structural members shall be cleanly welded, and shall be free of gaps in corners. All joins shall be free of protruding and/or sharp edges that may cause injury. Panel work shall be inspected prior to installation to ensure that an acceptable level of workmanship has been applied during the manufacturing process.

   The use of standard 19" modular cabinets is preferred to the manufacture of purpose made panel work. Drawings of all-purpose build panels shall be submitted for approval prior to manufacture.

3. All cabinets shall be supplied as floor mount units with bottom entry cable access. The cabinets shall be supplied with a plinth recessed from the front of the cabinet by a minimum of 50mm.

4. Louvered openings shall be supplied on all panels requiring excessive heat dissipation.

5. All panels housing equipment that requires routine maintenance shall be supplied with hinged and lockable doors, with handles to allow easy but controlled access to the equipment. Doors shall be manufactured consistent with the panels supplied. All panels shall make use of a common keying system. Screw type access panels shall only be accepted in areas where structural conditions prohibit the use of hinged doors.

6. All panels shall be painted as per the architect's detail.

7. All wire ways, laminated counter tops and counter supports shall be, and do not form part of security contract explicitly noted otherwise on the contract drawings.

8. It remains the contractor's responsibility to ensure that adequate notice has been taken of the architectural requirements prior to finalization of cabinet detail.

8.3 Manufacture and Supply

The panels shall be supplied complete with all necessary floor channels and securing bolts, inter-panel wiring, bus wiring, trough wiring, accessories and all necessary equipment to provide a complete assembly.

8.4 Layout

The layout of the panels in the control room/s is shown on the accompanying drawing/s, and all dimensions shall be adhered to. The layout of control equipment in the panels shall be the responsibility of the contractor. Attention should be paid to the effects of Electromagnetic coupling, and the overall responsibility for providing an acceptable control system shall remain with the contractor.

Panels shall be of the single-row (simplex) type comprising one or more modules mounted adjacent to each other, or of the double-row (duplex) type consisting of two, four or more modules mounted back-to-back.

Dust proof seals shall be provided on all doors. Rubber seals will not be acceptable.

All holes through which wiring must pass shall have chamfered edges or grommets to prevent damage to insulation.

8.4.1 Simplex Panel

This panel shall comprise one, two or more modules mounted side-by-side, each module being of the unit construction, free standing cubicle design to

enable a complete panel to be removed from the end or the middle of a suite of panels without affecting the operation of adjacent panel.

It must be possible to remove the rear portion with associated wiring and fittings, leaving only the channel base and bus-toughing with bus-wires and trough-wires undisturbed. Also, it must be possible to remove the bus-toughing without disconnecting any through-running wires.

Each simplex module shall have a cover fitted over the slot in the rear of the bus-toughing. Each suite of panels shall have slot cover plates on the extreme ends of the bus-toughing. Cover plates shall also be provided to blank-off holes in the sides of the end panels of a suite.

Vertical wiring troughs shall be provided on each side of the rear portion. Each trough shall have a maximum depth of 50mm and shall be fitted with insulated covers divided into three sections

The panel must be complete with fuses and links, terminals wiring and associated vertical and horizontal "wash lines", blank gland plates, earthing bars together with all remaining accessories, swing frames or full length doors, if specified, labels and cubicle lights.

8.4.2 Duplex Panel

This shall consist of two, four or more modules mounted back-to-back and connected by a horizontal trough which constitutes the roof of the corridor formed by the two modules or rows of modules. This trough secures the modules and shall be used for inter-panel, bus- or trough- wiring. The corridor formed by the two rows shall be provided with a dust proof door at each end.

8.5 Panel Finish

After fabrication is complete the metal surfaces shall be thoroughly degreased and cleaned of all mill scale and rust by means of shot- or sand –blasting or by pickling.

After cleaning the equipment shall be given one coat of an approved primer followed by two coats of an approved finishing paint of colour as specified. In the case of cold-rolled sheets the preparation may be waived providing an etching primer or other approved means is used.

The panels and toughing shall be finished light grey, No. 631 to BS. 381C with a semi-gloss (egg shell) finish.

The front and rear mounting channels shall receive an undercoat and two coats of bright black paint. Interior surfaces of the panels and the fuse and link mounting brackets shall have a gloss white finish.

Paint work damaged during transport or erection shall be made good by the Contractor, and one litre of un-thinned paint of each colour shall be provided on handover of the project.

8.6 Accessories

8.6.1 Fuses

The domestic type of cartridge fuse is preferred which has the cover plate and fuse carrier coloured as follows:-

- 5 amp White
- 15 amp Green (for d.c. Control Circuits)
- 15 amp Blue (for a.c circuits V.T.)
- 30 amp Red
- links Black (rated for 30 amps continuous).

All direct current circuits shall have a fuse in each phase leads.

Labels shall be affixed alongside each fuse group designating the purpose and size of the fuses.

Fuses are to be mounted as near to top and rear of panel as practicable so as to provide maximum access to their terminals and to equipment mounted at the top of the faceplate. Fuses shall not project beyond rear of panel.

8.6.2 Terminals

All terminals for connection to field wiring shall be to approval.

Not more than two conductors shall be connected to any side of a terminal.

Panel wiring shall be connected to the side of the terminal strip, which is nearest the front of the panel whilst cable tails and trough wiring shall be connected to the side nearest to the panel rear.

These terminal strips shall be mounted on the sides of each panel in such a manner as to permit easy access to all equipment after the terminals have been wired. Separate terminal studs shall be provided for incoming leads and for the corresponding internal wiring leads.

Each terminal strip shall be complete with 5% spare terminals. The terminals shall be provided with labels.

8.7 General

8.7.1 Wiring Identification

Wiring leads shall be marked at both ends with an approved type of marking device, permanently marked with black letters impressed on a white background.

Interlocking type ferrules are preferred and shall match the size of wire onto which they will be fitted. The "slip-on" type is preferred but for the smaller sizes of wire the "clip-on" type is acceptable.

For all wire without lug terminations, the ferrule must not fall off when disconnecting the wire and in this regard, the use of one strand of wire to retain the ferrule is acceptable providing that this is used in a very neat manner.

Ferrules should be handed so as to read the right way up on the cable terminal strips and to read from insulation to crimped lug in the case of relay and instrument connections, etc.

8.7.2 Cable Gland Plates

Removable blank gland plates shall be provided. They shall be fixed to the panel by hexagon headed screws. All drilling of gland plates, cabling, making-off and connection of cable tails shall be the responsibility of the contractor.

8.7.3 Earthing

A tinned copper earth bar shall be provided per panel and shall be fitted to the bottom rear at a position such that it can be connected to the earth bar of the adjacent panel by the use of a copper-connecting strap.

The Contractor shall ensure that all metal non-current carrying parts are effectively connected to this earth bar either by means of their mounting arrangement on the panel or by means of a special earthing conductor.

8.7.4 Labels

Labels shall be provided on the front of each panel, also in the interior for fuses and terminal strips.

Labels shall have a minimum thickness of 1mm and shall not discolour or distort in service. Labels made from white/black/white sandwich board, engraved through one white layer to give black letter on a white background, are preferred although labels made from white opal Perspex having black-

filled lettering are acceptable provided that the medium used for filling is black brushing cellulose lacquer.

Filling waxes are not acceptable.

For labels manufactured from sandwich board, the depth and angle of engraving cut shall be such that the black lettering shall be clearly visible and legible when viewed at an angle of 45 degrees. Width of cut is to be taken as width of exposed "Black".

The label edges shall be chamfered to give an overall neat finished appearance.

8.7.5 Panel Lighting

Each panel shall be provided with an internal lamp suitable for a 220-volt a.c. supply. A switch shall be provided in each panel.

8.8 Inspection and Tests

The user reserves the right to inspect the panels in the manufacturer's works at any stage of their manufacture. The Contractor shall advise the user in writing within 7 days of commencement of assembly /wiring etc.

Tests shall include insulation resistance, earth continuity and wiring accuracy tests in the manufacturer's works.

The Commission reserves the right to test the panels in the manufacturer's works before dispatch. Testing can be carried out "piecemeal", i.e. on individual panels or circuits as they become completed, as it is unnecessary to wait for all panels to be completed before testing is arranged.

The Contractor shall give the user at least 3 days notice of the date on which panels will be ready for final inspection and testing.

8.9 Lightning / Surge Suppression

8.9.1 General

The contractor shall provide and install all the necessary Transient Voltage Surge Suppression (TVSS) devices, for the protection of the electrical/ electronic control equipment, communication and data lines. TVSS devices shall protect all AC and DC circuits from the effect of lightning induced over voltages, internally generated transients and utility switching transients.

8.9.2 TVSS Technology – AC Power Applications

1. The primary suppression path shall be pure silicon avalanche diodes

2. Silicon avalanche diodes must be bi-polar, of grade A, +- 5 % tolerance

3. Surge suppression devices shall provide 'power on' and 'failure' indication. An optional remote status capability for indication of primary suppression path failure shall be available.

4. All AC TVSS devices shall be UL listed and bear the UL label on each component. All AC TVSS devices shall be tested in accordance with the ANSI/IEEE testing standard.

5. Gas tubes, Selenium plates, MOV or Hybrid type suppressors will not be accepted

6. AC power protection units shall be in accordance with the specifications and regulations as proposed by the IEC.

7. AC protection components shall be installed on the supply side of the local control room UPS.

8.9.3 TVSS Technology – DC Applications

1. The primary suppression path shall be pure silicon avalanche diodes

2. Silicon avalanche diodes must be bi-polar, A grade, +- 5% tolerance.

3. Surge suppression devices shall operate in parallel to the protected circuit shall not employing switching components and has no series resistance.

4. Surge suppression devices shall provide a minimum of 5 joules or silicon avalanche diode per line, not per device.

5. Initial clamping voltage shall not exceed the signal line voltage by more than 25% unless recommended by the security equipment manufacturer.

6. Gas tubes, selenium plates, MOV or hybrid type suppressors will not be accepted

7. Coaxial transient suppressor: TCS-CP 1 or approved equal.

8.9.4 Application

1. Install TVSS devices on all AC supply lines and communication lines to protect against surges induced on all control lines, sensors, data lines and cables, which enter and exit buildings.

2. Communication protection devices shall be mounted in IP54 enclosures with all wiring in the enclosure to be kept in plastic wiring troughs.

The incoming cables shall be separated from outgoing cables. There shall be an earth bar in the lower corner of each enclosure and shall be sized to accept a 16mm square BCW. The Bare Copper Wire shall be terminated to the nearest earth mat.

3. AC protection devices can be located in the equipment cabinet and must be installed prior to any distribution (i.e. multi-outlets).

   The contractor shall ensure that lightning surges of 10Ka @ 8/2 can be safely accommodated by the TVSS devices installed without damaging the surge suppression equipment permanently.

8.10 Drawings

As soon as they become available, duplicate copies of the panel, shall be handed to the user.

The contractor's panel and wiring diagrams shall be submitted for approval within three months of placing the order. These wiring diagrams will be approved by the user in principle only, as the user regards these diagrams as an intermediate step used by the Contractor to assist in the manufacture of control/relay panels.

The user may on occasion supply their own panel wiring diagrams and these may be used by the contractor to assist in manufacture. The user reserves the right to correct any manufacturing errors that may be found and to charge the contractor with appropriate costs.

9 UNINTERRUPTIBLE POWER SUPPLY SYSTEM

9.1 General:

The contractor shall supply, install and commission an adequately sized dual redundant hot standby centralized uninterruptible power supply system for all security related equipment including but not limited to Closed Circuit Television equipment, Control hardware, Operator workstations, Audio control equipment, Alarm monitoring systems and Sliding/Swing door locking devices.

The UPS system shall be centralized and consist of two hot swappable dual redundant units each capable of supplying the total load requirement of the security installation.

The units shall receive their power supply directly from the main / emergency power supply of the facility, within the Central equipment room provided. The **Electrical** contractor shall be responsible for the complete UPS power reticulation system including the supply of the Incoming and outgoing distribution cabinet, appropriately sized supply cables to each local control area and all necessary surge protection equipment.

The UPS system shall enable the entire security system to operate independently of the general facility power supply, and shall be capable of providing 35 minutes of uninterrupted power in the case of failure of the facility supply.

In the event of a failure of the facility and emergency (standby generator) power sources, the UPS system shall provide visual and audible fault indication and report the appropriate condition to the local and central operator workstations.

The interface to the Security Management System shall be via a high level interface (HLI) to the SMS server situated in the Central equipment room control cabinet. Interface. Interface via dry contact shall not be acceptable.

9.2 9.2 Construction:

The uninterruptible power supply shall have an output voltage of 230 VAC and a full load current capable of supplying all systems indicated herein.

The units shall operate with an input voltage of 380 VAC, single phase, 50 Hz.

The output frequency stability when operating without an input (inverter mode) shall be not less than +- 0.25 %. Static voltage regulation shall not exceed +- 3% with a dynamic regulation of at least +-10% for any load change not exceed 20% of full load rating. The contractor is responsible for sizing UPS systems to meet the correct requirements.

1. The unit shall operate normally with a +- 12% input voltage with an 0.85 power factor, from 0 degree to 40 degree C n a humidity of 0 % to 95 % and shall deliver 150% of rated power for 10 seconds and 125% for 10 minutes**.**

2. All units shall feed power on line and in the event of a loss AC input power, the unit shall continue to provide power to the equipment.

Output power shall remain constant during transfer to/from input AC line power of DC source inverter power.

In the event of an inverter malfunction the unit will indicate and sound an inverter malfunction alarm and the inverter will shut down. The inverter shall shut down and drive an alarm when the input voltage drops below 190 volts DC.

9.3 Batteries

The batteries shall be sealed lead acid/gel/cell maintenance free type. The batteries shall have heavy duty, radial grids for mechanical strength with low grid corrosion rate and PCV plastic separators for low internal resistance.

Batteries shall be sized as recommended by the manufacturer to supply the necessary DC power to the UPS system for the extended run time required.

The batteries shall be protected with a circuit breaker and the charger shall give a fault indication and shut down if an over voltage condition exists.

The charger shall receive source power from the same AC line circuits as the UPS AC inputs.

Sufficient batteries shall be provided in order to supply 230 volts to the load for a period of time as required above. The complete system (batteries and UPS) shall be furnished and guaranteed by the same manufacturer.

The batteries shall be sealed lead acid/gel/cell maintenance free type. The batteries shall have heavy duty, radial

9.4 Status Indication

1. The unit shall have an indicator panel with the following condition indicators:

    a. UPS Overload

    b. Electronics Fault

    c. Battery Fault

    d. Ambient Temperature warning

    e. Percentage load

    f. Lamp Test

    g. Operation on Manual Bypass

    h. Operation in Online Mode

    i. Operation on Battery

9.5 Integration with the Security Management System

The Dual redundant centralized UPS's shall be fully integrated with the Security Management System by means of a High Level Interface (HLI), to provide operators and technicians with detailed status and alarm conditions regarding the UPS systems.
Due to the Centralized configuration, the following detailed diagnostic information is required, and shall be presented to the operator via a drop down menu option within the SMS:

UPS Data:

- Manufacturer
- Type
- Serial Number
- Software Version

Battery Data:

- Battery Status
- Time Remaining in minutes
- Remaining Charge in %
- Battery Voltage
- Battery Current
- Battery Temperature in Deg C

AC Input Data:

- Frequency per phase
- Voltage per phase
- Current per phase
- Power per phase

AC Output Data:

- Frequency per phase
- Voltage per phase
- Current per phase
- Power per phase
- Load % per phase

UPS Alarm Conditions:

- Battery Failure
- On Battery Power
- Low Battery
- Depleted Battery
- Over Temperature
- Input Supply Out of Limits
- Output Out of Limits
- Output Overload
- Bypass Active
- Bypass Inhibited
- Charger Failure
- Fan Failure
- Fuse Failure
- Diagnostic Test Failure
- Communications Failure
- Shutdown Pending
- Shutdown Imminent

All alarm conditions shall be presented to the operator within the Fault queue as described in the specification.

10 ANCILLIARY EQUIPMENT

10.1 X-Ray Machines

The contractor shall supply, install and commission compliant Dual Energy Imaging X-Ray machines in accordance with the following Specification:

10.1.1 Technical Specification

- Detection System: Dual Energy (Multi Energy Imaging)

- Monitor: Colour Monitor with remote operation
- Conveyor Belt: <2100mm
- Screening: Full profile of inspection tunnel
- Discharge Roller: Entrance & Exit
- Power Supply: 240V AC 50Hz, 5A Maximum
- High Voltage Generator rating: 160kV
- Operating Temperature: 0-40°C
- Relative Humidity: 95% Non-condensating
- Min Object Height: 400mm
- Min Object Width: 600mm
- Min Object Length: Unlimited
- Max Unit Height: 1400mm from floor level

10.1.2 Construction Detail

1. The unit shall incorporate a facility to be controlled either from the right or the left-hand side.

2. The operating keyboard and monitor shall be operable remotely, at a minimum of 5m from the unit.

3. Control elements (pushbuttons, switches, etc.) are to be of sturdy design, selected for severe operating conditions.

4. Discharge rollers shall be included with the unit. The discharge roller platform shall be long enough to prevent articles being X-rayed from falling off.

5. The conveyor belt shall be designed for 24 hour, heavy-duty operation.

6. The unit shall not be more than 800mm wide and 2600mm in overall length, including the conveyor belt platform.

10.1.3 Image Processing

1. Monitor display shall cover not less than 500mm of the object length.
2. Full scan volume shall be visible on the screen, without any corner cut-off.
3. Imaging scale of all objects should be constant with the minimum distortion.
4. Nine (9), independent zoom sectors. The selected sector shall be identified by light frame before zoom is activated.
5. A colour monitor (non-interlaced), screen size of at least 34cm shall be provided. Parallel operation of additional monitors, without modification to the unit, must be available.
6. The image on the monitor screen must be flicker free.
7. Control of brightness and of contrast shall be provided on the front panel of the monitor.
8. Ability to switch between "POSITIVE" and "NEGATIVE" images.
9. Dual (Multi) energy colour system with a four (4) colour (Industry Standard) is a firm requirement.
10. Organic/Inorganic colour stripping.
11. High and low penetration.
12. Variable colour stripping and variable gamma edge enhancement.
13. Automatic density (variable) threat alert.
14. Automatic organic material threat alert.
15. Operator log-in identification facility.
16. Video output capabilities for recording of images shall be included
17. Voltage stabilizer must be included.

10.1.4 Resolution & Penetration

1. Monitor display shall cover not less than 500mm of the object length.
2. The image quality on the monitor shall be uniform, without distortion in the centre or the edges.
3. Penetration of 25mm steel minimum must be guaranteed.
4. A pre-selectable density threat level shall be a feature of the equipment, with a visual and/or audible alarm if any item being screened exceeds that pre-selected density.

10.2 Walk through Metal Detectors

The contractor shall supply, install and commission compliant Walk through Metal Detectors in accordance with the following Specification:

10.2.1 Technical Specification

- Detection System: Multi Zone
- Power Supply: 240V AC 50Hz, 2A Maximum
- Battery Backup: 45 min
- Operating Temperature: 0-40°C
- Relative Humidity: 80% Non-condensating
- Min Walk through Height: 2000mm
- Min Walk through Width: 720mm
- Throughput: 50 persons per minute

10.2.2 Minimum Features

1. The metal detector shall consist of a free standing walk-through frame with an integral control unit, and shall be suitable to detect metallic objects on a person by means of the magnetic field principle.
2. The metal detector shall be suitable to detect ferrous and non-ferrous metals.
3. The metal detector shall be equipped to eliminate false alarms.
4. The metal detector shall scan the entire area of the walk through area and detect metal objects on a person passing through to the levels as specified.
5. The metal detector shall incorporate self test button to confirm that the system is operating correctly.
6. The metal detector shall be completely tamper proof.
7. The programme and sensitivity push buttons shall be so arranged to eliminate tampering.
8. The metal detector shall not be adversely affected by stationary metal bars or structures in the vicinity of the unit or moving metal near the archway.

9. The metal detector shall be capable of operating adjacent to an X-Ray inspection unit.

10. The metal detector shall have multi-zone vertical detection zones for the full height of a person. Each zone shall have a display bar with proportional indication on the vertical sides of the metal detector.

10.2.3 Construction

1. The metal detector shall comprise a free standing walk-through frame containing the detector coils and the control unit, complete with a 5m length of flexible cable and 16A 3-pin plug top. The cord and plug top shall comply with the relevant SABS specifications.

2. The frame and the control unit shall be of robust construction and the base of the frame shall be designed to ensure rigidity.

3. The unit shall be able to execute a full body scan and detect metal objects down to the lower feet level within the settings specified.

4. The finish shall be durable and maintenance free.

5. All material consisting of metal shall be treated against corrosion.

10.2.4 Control System

1. The system shall operate by means of automatic level control adjustable to environmental changes

2. The control unit shall be equipped with an On-Off Switch and Mains On Indicator

3. The sensitivity settings shall be consistent at average walking speed.

4. Visual indication in the form of vertical display bars shall give an indication of the volume of metal on a person in accordance with the sensitivity settings. When the "ALARM" zone is activated it shall simultaneously activate an audible alarm having a continuous tone and adjustable volume. The alarm system shall automatically reset after the metal has passed through the frame.

5. The system shall be modular to facilitate maintenance and repairs.

11 HIGH SECURITY FENCES

11.1 Scope

The contractor shall furnish labour, equipment and materials for the following systems in this Section of the specification

1. 4.5m Outer Bowed Welded mesh security Fence
2. 2.7m Inner Taut Wire Detection Fence
3. Taut Wire Detection System
4. Kinematic Detection System
5. Gate Area Detection System

11.2 Integration

The Systems listed above shall be fully integrated with the Security Management System provided in accordance with Sections 1 and 11 of the specification.

11.3 Outer 4.5m Bowed Perimeter Fence

The contractor shall furnish labour, equipment and materials for the following systems in this Section of the specification

1. 4.5m Bowed Welded mesh security outer fence
2. Preparation of strip upon which the fence will be installed
3. The perimeter security fence shall be based on the following systems
4. 4.5m bowed outer security fencing
5. Delay fencing integrity detection
6. Gate area detection solution

The delay fence distribution detection system shall be based on kinematics principles detecting any cut or removal of components of the delay fence as is detailed hereunder in this specification. The detection system shall be installed on the outer perimeter fence as indicated in the fence layout drawing.

The physical perimeter shall consist of an inner fence and an outer fence of 4.5m in height.

Furthermore the outer fence detection system shall be installed on the outer perimeter fence attached to the outer fence structure as per the specifications of the technology manufacturer.

Due to the various gate area designs found on various facilities a gate area security and detection solution has to be designed on an application to application basis and has to be approved by the Engineer prior to implementation.

It is a requirement that all sub-systems must be integrated with the security management system on a site. Contractors shall ensure that the control system offered comply with this requirement.

The perimeter security fence must not to be closer than 20m from the building except in cases where the site is an existing site and site limitations are experienced. The perimeter fence shall enclose all the holding units and all the support buildings accessible to prisoners or supporting inmate activities. The minimum distance allowed between the inner detection and the bowed outer perimeter fence shall be 6m.

If fences are to be coated other than with Galfan Class A the coating will be specified in the Bills of Quantities

11.3.1 Standard Profile Corner and Intermediate Posts with Cover Plate

The standard profile intermediate and corner posts shall comply with the following specifications:

- Post Dimension: 101.6mm (Dia) x 4.5mm (Wall) x 6900mm (Len)
- Bowed Height: 4500mm (From ground level)
- Cover Plate Dimension: 50mm (Width) x 5mm (Wall)
- Fixing Holes: Pre-drilled 11mm holes for fixing Panels to Posts
- Post Coating: Hot dipped galvanized (ISO 1461)
- Coating Thickness: Min 55μm galvanising
- Posts Spacing: 3.0m
- Mounting Sleeve: 1500mm (Len) x 103mm (ID) PVC Sleeve

11.3.1.1 Erection of fence posts

After excavation of the fencing post holes, a 1500mm x 103mm (ID) PVC sleeve with positioning bolt shall be set vertically in the concrete foundation with 1300mm below finished plinth level and 200mm above.

A Minimum of 5 days setting time shall be allowed before positioning posts within sleeves.

After setting of concrete, the top 200mm PVC sleeve to be cut off flush with finished plinth height before the erection of posts. The PVC sleeves shall protrude through the 100mm concrete plinth.

Care shall be taken to ensure all posts are aligned (vertically and at post top), plump, perpendicular and in the correct position on the route of the fencing.

PVC sleeves shall be encased in a 25/19 concrete footing of adequate size. The contractor shall note that all galvanizing shall be done after manufacturing of the posts.

Prior to erection of the fence poles permission shall be obtained from both the Clients representative as well as Civil consultant of the Department to ensure that all conditions have been met.

11.3.2 Foundations

The foundations shall comply with the following specifications:

- Level Mounting: 550 mm x 550 mm x 900 mm (Deep)
- Slope Mounting: 550 mm x 550 mm x 1000 mm (Deep)
- Concrete Strength: Minimum 15 MPa with 19 mm stone.

11.3.3 Top Rail

The Top Rail shall comply with the following specifications:

- Angle Iron Dimension: 50 mm x 50 mm x 5mm
- Mounting Detail: Predrilled holes for fixing rails to the posts and for fixing the top section of the mesh to the rail.
- Coatings: Class-A hot-dipped Galvanized in accordance with ISO 1461.
  Minimum thickness of the Galvanizing: 70µm.
  Polyester Coating:
  This coating to be applied on top of the galvanizing.
  An Adhesion Coating is to be applied

before Polyester Coating is applied. Minimum thickness of the Polyester Coating: 60 µm.

11.3.4 Fixing Accessories

The fixing of the cover plate and mesh to the posts shall be achieved with the following accessories:

1. M8 x 150mm Galvanized Cup square bolts;
2. M8 x 25mm x 2mm Galvanized Fendour Washers;
3. M8 Galvanized Shear nuts.

The fixing of the top section of mesh to the Top Rail shall be done with the following accessories:

1. M8 x 40mm Galvanized Cup square bolts;
2. M8 x 25mm x 2mm Galvanized Fendour Washers;
3. M8 Galvanized Shear nuts.

The fixing of the top section of mesh to the Top Rail shall be done with the following accessories:

1. M8 x 40mm Galvanized Cup square bolts;
2. M8 x 25mm x 2mm Galvanized Fendour Washers;
3. M8 Galvanized Shear nuts

11.3.5 Mesh Panel Specification

The following information concerning the Mesh Panels shall be specified in the Bill of Quantities for the project.

1. Type of Mesh;
2. Panel Height;
3. Panel Width;
4. Coating (if other than galvanized is required).

11.3.5.1 Mesh Panel Type 1: 4mm Single Skin with Double Vertical Wires

The 4mm Single Skin Welded Mesh Panels shall comply with the following specifications:

- Internal Aperture Size: 72.2 mm x 8.7 mm
- Centre to Centre: 76.2 mm x 12.7 mm
- Minimum Wire Diameter: 4 mm (horizontal and vertical wire)
- Welding: Vertical wire shall be welded on either side of the horizontal wires
- Tensile Strength: Minimum 600 – 900 N/mm²
- Weld Strength: 60 – 80% of the original steel strength
- Maximum Weight: 10kg/m²
- Approximate Solidity: 35%;
- Standard Panel Width: 3.050m
- Standard Panel Height: 5.2m
- Coatings : Galfan Class A Coated to SANS10224-2:2003 specification;
  Minimum Thickness of the Galfan Coating on the Mesh: 70 µm.
  Polyester Coating:
  This coating is to be applied on top of the galvanizing;
  An Adhesion Coating is to be applied before Polyester Coating is applied;
  Minimum Thickness of the Polyester Coating: 60 µm.

11.3.6 BTC Extension

The fence shall be 4.5m high with and extension of 610 mm of Barbed Tape Concertina on top to bring the total height to 5.11 m.

The BTC extension shall comply with the following specifications:

1. 610 mm Diameter Razor Wire Coil :
    a. Minimum Wire Diameter : 2.5 mm;
    b. Tensile Strength of Wire : 600 – 900 N/mm²;
    c. Razors: 0.5 mm Z200 Zincalu strips.
2. Coating :
    a. Galfan Class A Coated to SANS10224-2:2003 specification;
    b. Minimum Thickness of the Galfan Coating on the BTC Coil: 70 µm.

3. Maximum Stretch: 10 m.

11.3.7 Gates

Swing or sliding gates shall be supplied and installed in accordance with the Bill of Quantities.

Sliding gates shall be controlled electrically by means of industrial type gate motors. Beams shall be provided to prevent closing of the gate while vehicle is driving through.

Refer to detail drawings.

The gate frame shall be constructed of 60 x 40 x 2mm rectangular steel tubing and Hot dipped galvanized to ISO 1461 (Min thickness 45 micron). Each gate must consist of two leaves of the same size.

Each section of the gate must be secured to the gate post be means of 3 approved hinges. Proposed hinges shall be submitted for approval before fitting.

The gate shall be installed in such a way that the leaves can open in both directions.

Each gate shall be clad with the same mesh as that of the fence using similar cover plate & bolting systems.

The gap between the bottom of the gate and the road surface shall not exceed 50 mm. The contractor shall ensure that the correct gate for the 4.5 m bowed fence is installed.

For detail of the construction of the gate area closing frame and side panels refer to the detail drawings.

11.3.8 Concrete Plinth

A 25/19mm concrete plinth shall be cast in situ along the inside of the external fence.

The plinth dimensions shall be 1000mm x 100mm or as otherwise specified in the Bill of Quantities, on top of prepared ground level. The wire mesh panels of the fence shall be cast into the concrete slab. An expansion gap of 50mm wide must be provided at 3000mm intervals, to provide drainage and expansion.

The section of mesh cast into concrete plinth and into the ground shall be bitumen coated up to 100mm above ground level.

Civil works shall include route preparation, and casting of the 1000mm wide concrete slab with welded mesh steel reinforcing to a nominal thickness of 100mm and a minimum compressive strength of 20Mpa.

All existing electrical services as well as the cables required for this installation shall be installed in 2x 50mm PVC sleeves within in the concrete slab to ensure that these services can be maintained after completion of the contract.

The area underneath the concrete plinth shall be cleared of all vegetation prior to casting and treated with a suitable sterilization herbicide to prevent any vegetation growth.

The contractor shall allow and install a 250 micron PVC sheet underneath the concrete slab, to prevent any vegetation growth.

11.3.9 Fence Line Preparation

The fence line and the eight meter sterile zone between the inner and outer fences shall be thoroughly cleared prior to commencement of the works. The area shall be prepared in such a way that each zone length runs as close as possible to the same gradient. Marginal gradient changes will only be allowed on zone ends. Approval for gradient changes in soil preparation shall only be undertaken once written approval from the Engineer has been obtained.

The eight meter sterile zone between the inner and the outer fence shall be cleared off all vegetation, treated with a suitable sterilization herbicide, preventing any vegetation growth. The area shall be covered by a layer of 19 mm single sized stone on a geo-textile similar to Bidum U34 as part of this contract.

The contractor shall include in his offer the cost to maintain this area for the full duration of the contract and shall include as part of his offer a suitable sterilization herbicide treatment once every six months for the full duration of his maintenance contract.

The contractor shall note that it shall be the responsibility of the fencing sub-contractor to liaise with the Civil Engineer regarding all civil work. All information required e.g. soil conditions, back filling etc. shall be taken into consideration during the tender period and no additional claims as a result of poor liaison shall be accepted.

11.4 Inner 2.7m Taut Wire Detection Fence

11.4.1 Scope

The contractor shall furnish all necessary labour, equipment, and materials for the following systems under this Section of the specification:

1. Security electronic equipment and cabinets.
2. Taut wire perimeter detection system.
3. Field Fibre-optic communication equipment.

4. Perimeter Controller.
5. Report printer.
6. Surge protectors.
7. Power supplies.
8. Training.
9. Spare Parts.

11.4.2 General

1. The physical perimeter shall consist of an inner fence of 2.7m in height and an outer fence of 4.5m in height.
2. The Electronic taut wire detection system shall be implemented on the 2.7m inner fence, as described in this specification.

11.4.3 Detection Fence

1. The taut wire fence and alarm system shall act as an electronic barrier to detect and alarm escape attempts.
2. The taut wire system shall be installed as a stand-alone system located on the facility side of the outer perimeter fence.
3. The electronic barrier shall consist of the following:
    a. A protective 2700 mm high barrier with 27 taut barbed wires, stretched between anchor posts, (wire tension shall be such that when a 2kg weight is applied between two slider posts the wire deflection shall be between 50mm and 75mm. All wires shall be of the same tension) and supported by a number of slider posts and detection sensors.
    b. 600mm wide side walk shall be constructed directly below the taut wire system and extend 400 mm to the facility side of the taut wire fence as shown on the layout drawings i.e. 1000mm wide in total. The sidewalk shall run the continuous length of the inner perimeter fence as indicated on the perimeter fence layout drawing.
    c. All corners shall be designed so the taut wire intersects.
4. The taut wire sensors shall be mounted on a sensor post constructed of galvanized steel. The sensors shall be spaced according to the wire spacing specification. (Bottom 18 wires 90mm, then 9 wires at 120mm spacing)
5. Movement transfer wires

a. High, tensile, double-braided barbed wire.

b. Minimum breaking strength of 439 Kg

c. Barbed 4 points.

d. Average spacing of the barbs is not to exceed 125 mm

e. Galvanised steel.

6. Tensioners

   a. Tensioners shall be galvanised, ratchet wheel type.

   b. At one end of the zone, each taut wire strand shall be attached to an individual tensioner.

7. Slider Post accessories: Slider mechanism with accessories that serve to support the wire system, converting vertical force into horizontal movement.

   All slider posts shall be manufactured and supplied in accordance with the latest fence design drawings as attached.

   All Slider post accessories shall be constructed of stainless steel.

8. Sensor Post Accessories: Sensor post shall be designed to contain the sensors.

   At a minimum, the sensor post accessories shall be constructed of galvanized steel as per detail in the drawings.

9. Sensor, anchor and slider posts: All sections shall be at least 2750 mm in height.

10. Zones: The system shall be configured as shown on the drawings.

11. All wires shall be stored on the factory shipping reel until the wire is installed on the sensors.

12. Corner Configurations: All taut wire corner configurations shall be an intersecting type installation.

11.4.4 Posts, Footers and Side Walk

1. Posts and Footers: Post and footers shall be an integral part of the side walk.

   a. All slider posts shall be equidistant, between 3.5 to 4 m separation, depending on terrain and detection system requirements. Refer to structural layout drawings for intermediate post layout.

b. All posts shall be installed in accordance with detection system manufacturer recommendations.

c. All anchor posts shall be installed in accordance with the detection system manufacturer recommendations.

d. Slider and sensor post shall be installed in accordance with the detection system manufacturer recommendations.

e. Strain posts shall allow re-tensioning of fence wires and shall withstand wire tension force as well as additional loading of a reasonable intruder without causing permanent deformation. Refer to structural layout drawings for strain post layout.

2. Sidewalk and Post Footers: A concrete sidewalk shall be installed directly below the taut wire fence and shall run the continuous length of the system.

    a. Sidewalks shall be minimum 100 mm thick and 1000mm wide as shown on the civil drawings and must include a gravel base with the appropriate wire mesh reinforcement.

    b. To prevent cracking and chipping, sidewalk expansion joints shall be installed at 3000mm intervals and as necessary.

    c. Expansion material shall be installed between the sidewalk and all posts mounted in the sidewalk barrier.

3. Concrete: All concrete shall be as specified by the Civil Engineer. At a minimum the concrete shall have a minimum compressive strength of 20MPa at 28 days.

4. Earth: Trenches and holes shall be excavated and formed as necessary to support the sidewalk and posts.

5. Rock: Holes in solid rock shall be 25 mm wider than pipe diameter, and at a minimum 300 mm deep for sensor posts, and 460 mm deep for anchor posts. Holes shall be back filled with non-shrink grout.

    a. Moisten or aerate each layer as necessary to facilitate compaction to the required density.

    b. Do not place back fill or fill materials on surfaces that are muddy, frozen, or contain frost or ice.

6. Compaction: Each layer of fill and back fill shall be 90% of the maximum density.

11.4.5 Civils

Civil construction shall include route preparations, and casting a 1000mm wide concrete slab with welded mesh steel reinforcing a nominal thickness of 100mm and a minimum compressive strength of 20Mpa.

All existing electrical services as well as the cables required for this installation shall be installed in 50mm PVC sleeves in the concrete slab to ensure that these services can be maintained after completion of the contract.

The area underneath the concrete plinth shall be cleared of all vegetation prior to casting and treated with a suitable sterilization herbicide to prevent any vegetation growth.

The contractor shall allow and install a 250 micron PVC sheet underneath the concrete slab, to prevent any vegetation growth.

11.4.6 Power and Communication Cable

All cables must comply with the manufacturer recommendations.

Exterior wire and cables shall be installed in schedule 50 PVC conduit and rated for direct burial use. The conduit shall be installed in the inner fence sidewalk.

Power distribution wire from the main equipment room to remote processors, transponders, microwave units, or other remote electronics on the site perimeter shall be minimum 2.5 mm2 copper and shall be increased in size as necessary to ensure no more than 5% (AC or DC) voltage drop from the main equipment room to the remote equipment. Power voltage drop calculations shall be submitted for all field located perimeter equipment.

Provide a two core multimode fibre optic cable, direct bury type cable between all perimeter system enclosures and the head end to create a loop around the perimeter system. Provide 1500mm of spare cable for each cable in each perimeter system enclosure.

All cables that will be directly buried shall be, rated for direct burial and approved for wet locations.

All conductors shall be rated for direct burial and approved for wet locations in accordance with SABS.

Signal and power cables shall be separate cables and not combined as part of the same cabling jacket.

11.4.7 Accessories

The system shall include all accessories required to perform the functions described in this Section.

11.4.8 Markers and Nameplates

11.4.8.1 Cable Tags:

Cable tags shall be provided in accordance with SABS.

11.4.8.2 Nameplates:

1. Precision engraved letters and numbers with uniform margins.

2. Character sizes shall be a minimum of 50 mm high.

3. Indoor : Shall be phonemic, two colour laminated stock, 2 mm thick, machine engraved to expose inn core colour (white).

4. Outdoor: Shall be Standard aluminium alloy plate stock, minimum 1 mm thick, engraved areas shall be enamel filled or background enamelled with natural aluminium engraved characters.

5. All nameplates shall be permanently attached.

11.4.8.3 Zone Identification:

1. In order for the officers inside the compound to easily identify zone locations, at the top of each sensor post, a 250mm x 200mm sign shall be installed. The sign shall face the inside compound

2. All zones shall be identified by zone number.

3. Reflective white numbers on a dark blue background shall be used.

4. All signs shall be visible from a distance of 12 meters.

5. In order for the perimeter patrol officer to easily identify zone locations, at the end of each zone a 500mm x 250mm sign shall be installed. The sign shall face the perimeter road.

    a. All zones shall be identified by zone number.

    b. Black numbers on a reflective yellow background shall be used.

    c. All signs shall be visible from a distance of 12 meters.

11.4.9 Power Supplies

Power supplies shall be furnished with characteristics as required to support the operational performance of the sensor and signal processors.

11.4.10 Enclosures

All exterior post mounted enclosures shall have the following features:

1. At least 1.6 mm stainless steel plate construction.

2. Continuously welded seams.

3. Cabinet lockable with all locks keyed alike.

4. A tamper detection device shall be provided and connected to the processor tamper circuit. The tamper switch shall detect any attempt to vandalise the enclosure including the opening of the door and the cutting or breaking of the enclosure.

11.4.11 Earthing

1. A continuous 70mm2, bare, stranded, copper earthing conductor shall be buried a minimum of 600 mm under the taut wire system's sidewalk and run the continuous length of the sidewalk.

2. At each sensor post, via cad-weld connections, the earthing conductor shall attach to the ground bus located inside the enclosure. Also, a 70mm2 earthing conductor shall bond the sensor post, processor post, and the nearest inner and outer fence post to the 70mm2 ground ring. All doors of sensor posts and field cabinets shall be earthed.

3. At a point nearest the main electronics equipment room, a 70 mm2, bare, stranded, copper conductor shall bond the buildings electrical system ground bus to the 70mm2 ground ring buried under the taut wire system's sidewalk. All direct buried ground connections shall be cad-weld type connections.

4. All systems described in this section shall be grounded in accordance with the responsible engineer’s recommendations and meet the minimum requirements of the manufacturer.

11.4.12 Surge Protection

1. All metallic data, communications, video, and sensor lines entering or leaving a building shall be protected with surge protection devices.

2. Earthing of protective devices shall be in accordance with the manufacturer's recommendations and/or as described in these specifications and drawings.

3. All signal line protective devices shall be located at the terminal point nearest the cable interface with the exterior cable plant. Devices shall be mounted to the back panel of the cabinet.

4. Where equipment is fed from a panel board not protected by a panel board protector, provide a branch circuit protector installed at the panel board.

11.4.13 Detection Measures

11.4.13.1 Taut Wire

Each sensor shall contain a dedicated microprocessor enabling a unique detection algorithm to be assigned as required.

The horizontal wires shall be attached to the sensors. The taut wire sensor shall be capable of producing an alarm when a wire is deflected by no more than 75mm. The taut wire sensor shall also respond to a cut in the wire.

The above system configuration shall have the capability to detect any attempt to penetrate the perimeter by climbing, cutting or spreading the fence wires apart.

1. The sensor detection parameters and detection performance should be accessible from the master controller on an individual sensor basis.

2. The taut wire detection performance should comply with the following minimum criteria:

    a. Nuisance alarm rate: Maximum 1 Alarm per zone per month

    b. Probability of detection: Minimum 95%.

3. The TWFDS shall annunciate an alarm condition in the event of one or combination of the following:

    a. Climbing the taut wire fence.

    b. Cutting the taut wire fence.

    c. Spreading the taut wire fence wires no further that the adjacent wire.

    d. Tampering with the processor enclosure.

    e. Attempting to remove the sensor post.

    f. Attempting to cut the power or communications of the processor to the perimeter security system.

4. Processing algorithms shall be provided as part of the TWFDS to process alarm events. Each individual wire shall be monitored for alarm conditions.

5. Subsequent attempts to climb, cut or spread the fence even after a tamper alarm condition is detected and annunciated, shall cause the processor to activate a new intrusion alarm.

6. Maximum permissible zone length is 100 meters.

7. The TWFDS shall have the ability to automatically adjust the centre of alarm detection range for gradual changes in sensor position caused by the environment, casual contact or ageing thus significantly lowering periodic maintenance.

11.4.14 System Description

11.4.14.1 Zones

The system shall be installed in specific lengths called Zones. Each zone and detection device can provide and report its own intrusion alarms, therefore providing information on the area of any intrusion attempt.

11.4.14.2 Detection units

Each zone shall be equipped with detection units, the detection unit shall include the transmitter, receiver, alarm processing unit and the required communication cable.

The parameters on the alarm processing unit must be adjustable in both the amplitude and frequency domain. The system must by commissionable to allow for maximum probability of detection (POD) and minimal nuisance alarms (NAR) and false alarms (FAR).

11.4.14.3 Installation

Measuring devices must be directly attached to the fence structure and connected via a field communication network. The network shall be connected to the main detection network via the field nodes and reflect in the main control room.

Each device with be represented in the main control user interface allow for parameter setting and diagnostics per device. The operator shall be able to identify the device that caused the alarm within a sector or zone.

The detection equipment shall be installed in accordance with the supplier specifications, the installation specifications must be presented before installation commences.

The detection units installed shall be sufficient to cover the specified area.

11.4.14.4 Maintenance

Sensor maintenance diagnostics shall be available in the control room and replacing a sensor shall be on a “plug and play” principle with no special tools required.

11.4.14.5 Detection

Detection parameters should be adjustable on an individual sensor basis for both the cutting and re-moving or moving of the fence and detection components.

The detection system shall announce at least the following alarm events:

- Fence cut

- Fence components removed

- Detection units moved

The contractor shall allow as part of this contract for the necessary tests to be effected as required by the end user.

11.4.15 Field Controller

11.4.15.1 Processor

Each zone shall be equipped with a field processor unit, performing all the functions associated with a particular zone. A field processor shall provide for / contain the following sub-systems:

- Digital inputs

- Relay outputs

- Processor

- Data communication

- Reset key switch transmitter type

Field processors shall be installed in the middle of each zone. The enclosure shall be manufactured from Stainless steel. Enclosures shall be rated IP 65 and fitted with a door lock and tamper switch.

A zone reset button (if required) shall be accessible from inside the perimeter fence and shall be of the transmitter type.

All cable entries to field units, if exposed shall be protected against vandalism by means of stainless steel covers.

11.4.15.2 Data Communication

Field processors are linked with a fiber optic serial data communication cable, in a closed ring configuration. Communication shall be fully functional with a single cut in communication cable.

11.4.15.3 Power

A single phase power feed shall supply the field processors.

(230V should be supplied to each field node.)

All equipment shall be protected against lightning surges and transient voltages to all the relevant SABS specifications and regulations

11.4.15.4 Characteristics

The unit shall have features or characteristics as follows:

1. Input voltage - 230VAC ±5%.
2. Equipped with transient suppression.
3. Supervised circuits - inputs.
4. Temperature Operating: -20 deg C to +70 deg C
5. Humidity - 20% to 95% condensing.
6. Unit shall be field addressable.
7. Shall interface with the Perimeter Controller.

11.4.16 Perimeter Controller

11.4.16.1 System operation

The system shall be installed as a zoned, automatic, supervised alarm detection system.

1. The alarm condition is transmitted from the post mounted, zone field microprocessor via redundant fibre-optic loop to the perimeter Master Controller.
2. Each detection zone shall be equipped with fibre-optic communication equipment to eliminate lightning surge problems.
3. Each independent defined intrusion event shall affect a unique signal on the perimeter controller.
4. The supervised circuit in the system causes a tamper/status alarm to signal if:
    a. Sensor circuitry is disturbed (opened or grounded).
    b. Tamper switches are activated situated in the control cubicles in the field or control room.
5. The location at any point at which an attempt is made to tamper with the system shall be identified at the perimeter controller.
6. Approved detection measures shall be incorporated into the system and used as separate zones protecting the vehicle sally port. (One zone only)

7. System status and all alarm conditions shall be reported to the central control from the field controllers to a perimeter controller.

    a. From the perimeter controller each zone shall be capable of zone access, alarm acknowledges and alarm reset. The perimeter controller shall have a distinctive audible alarm. Alarm shall annunciate both visually and audibly. The same shall be possible from security management system.

    b. The perimeter controller shall interface with an event printer located in Central Control. The event printer shall print a date and time stamped message indicating all alarms, alarm resets, and zone accesses.

    c. System status and all alarm conditions shall be reported to the system operator from the perimeter controller to a graphics display unit.

    d. All fixed components of the perimeter alarm system shall receive power from the UPS provided in central control or a main electronics equipment room.

11.4.16.2 Hardware

The perimeter controller shall be installed in the Central Control console as shown on the drawings.

The perimeter controller shall have the following characteristics:

1. Industrial grade hardware.
2. Solid state storage memory.
3. Complete with power supply.
4. Standard panel mounting for 19 inch EIA rack. Rack space requirements shall be no greater than as shown on the drawings.
5. Serial communication port
6. Ethernet port
7. Two USB ports
8. VGA port
9. Keyboard and mouse ports

The perimeter controller shall perform the following functions:

11.4.16.3 Field Communication

Communication with field controllers shall be via a redundant 2 core multimode optical fiber link. Operation of the system shall not be affected in case of a single break in the communication link.

11.4.16.4 Monitoring and Control

The controller shall contain the status map off all field detection and status devices. These devices shall include the following:

1. Taut wire sensor alarm status
2. Taut wire sensor maintenance status
3. Outer fence detection alarm
4. Outer fence detection maintenance
5. Field cabinet tamper
6. Auxiliary inputs including gate area detection devices and gate status contacts at sally port.
7. Field communication status for each field controller

11.4.16.5 Alarm and Event Printing

Alarms and selected events shall be printed on a suitable continuous paper printer via a parallel port

11.4.16.6 Alarm and Event Recording

The following shall be recorded on the alarm or event log:

1. All changes in the state of field devices. This includes alarm and maintenance conditions. These events shall be logged per zone and per device.
2. Operator master accept actions.
3. Field reset actions.

Log entries shall be date and time stamped to the nearest second.

11.4.16.7 External Interfaces

The perimeter controller shall provide the following data interfaces:

11.4.16.8 TCP/IP Socket interface

All perimeter or system devices shall be included in this interface mechanism. The external system shall initialize on selected devices and events shall be posted when any change occurs in the status of such devices. Events shall also be sent to the perimeter controller. Messages shall be in clear text.

11.4.16.9 Perimeter Controller Interface

Devices shall be mapped in a set of holding registers for access by an external SCADA system

These external data interfaces shall be used to integrate the perimeter system with a Security Management System or CCTV system.

Where a Security Management System is in operation the Perimeter system shall be fully integrated with the SMS and CCTV systems for annunciation, print recording, logging of alarms and initiation of CCTV system functions upon an alarm condition.

All perimeter alarms shall be logged, annunciated, recorded and managed by the SMS alarm terminal in Central Control. Fence Alarms, trouble and tamper conditions shall be separately annunciated by individual zone designations.

The interface definition shall be documented and delivered with the system as part of the deliverable of this project. (Proof of the operability of the interface must be given.)

11.4.16.10 Wide Area Networking

The Perimeter Controller shall be Internet Protocol (IP) enabled so as to be networked over a Wide Area Network (WAN) for the purposes of remote monitoring, control and viewing of historical information. This shall facilitate the performance assessment of both operator and equipment from anywhere on the client's network.

11.4.16.11 Diagnostic Tools

A diagnostic screen shall be included at the master indicating the following:

- On/off line status of field processors
- The alarm and maintenance status of all individual sensors
- The alarm and maintenance status of any other equipment attached to the system as required.

The diagnostic software shall include a data recording facility to record all the digital and analogue signals from any selected field processor unit and any selected detection device.

11.4.17 Performance Testing

1. The Contractor shall notify the Engineer two (2) weeks prior to the system tests so that arrangements can be made to have The DPW and DCS personnel witness the tests.

2. Each penetration of the taut wire system shall produce an alarm.

3. If an alarm is not detected on the first try of any test, the test shall be deemed a failure and all testing shall cease.

4. The Contractor shall be allowed time (not to exceed 1 hour) to make the necessary repairs before continuing the test. If additional failures are noted during the test, the test shall cease and be rescheduled for another day.

5. If the test is deemed a failure by the Engineer, DPW or DCS personnel, the Contractor shall be responsible for all cost incurred by the Government for scheduling a second test.

6. Taut Wire System: Test each system function step by step as summarized herein.

    a. The simulated intrusion attempts shall be performed by a person weighing 45 Kg or more.

    b. Safety equipment shall be provided by the Contractor and proper precautions shall be taken when performing the tests.

    c. Each attempt shall be terminated upon detection.

    d. Simulated escape attempts shall be performed at two (2) locations in each zone unless otherwise directed by the Engineer.

    e. Fast Climb: Approach and make contact with the fence and rapidly try to scale the fence.

    f. Slow/Stealth full Climb Over: Approach and make contact with the fence and slowly, deliberately, and stealth fully attempt to climb to the top of the fence.

    g. Climb Through: Spread wires apart and attempt to climb through.

    h. Tamper: Remove cover on zone processor.

    i. Trouble: In each zone, remove one side of the alarm communications wire from the processor board.

    j. Cut Test: The contractor must have the ability to simulate a "Cut Test" in any zone identified by the Contracting Officer.

7. The gate area detection system shall be tested based on the requirement that the gate area detection must be of the same standard as the perimeter detection system.

8. Delay Fence Integrity Detection System:

   A simulated breaching of the outer perimeter fence shall be performed.

   The outer fence detection system shall generate an alarm when such an attempt is made.

11.4.18 Spares

The Contractor shall provide the institution with the following spare parts upon system completion:

1. 27x Taut wire Sensors.
2. 2x Field node equipment sets.
3. 900m Taut Barbed Wire.
4. 10x Tensioners
5. 10x Delay fence detection units.
6. 1x Perimeter controller.

11.4.19 Compliance with the Specification

The Contractor shall comply with all the requirements as per this specification. Proposed deviations shall only be considered after the award of the contract. Proposed deviations shall only be accepted if it meets with all of the following criteria:

1. The proposed deviation offers a substantial improvement to the final product offered.
2. The proposed deviation has been proven in other applications.

Any deviations from the specification can only be implemented with prior approval from the various representatives from DCS and DPW. The names of the authorised representatives should be obtained from the various Head Offices of the two involved government bodies.

11.4.20 Graphical User Interface

The following software functions are required as a fully integrated software module of the Security Management System provided as part of this tender.

The functions described are to be built in functions of the Security Management Operator Workstation software.

Due to the complex nature of the sub-system integration required by the system it is imperative that the Supplier of the Security Management System provides a direct interface (driver) to the sub-system hardware offered in this tender, and that the functions described below are in-built functions of the software.

11.4.20.1 Site Perimeter Map

A graphical presentation of the site perimeter shall include the following:

1. Position of the perimeter
2. Detection zones
3. Gates
4. Other static information (buildings or roads) that may be required to assist the operator to identify the location of an occurrence.
5. The following Icons representing the alarm / maintenance status of field detection devices shall be included:
6. Alarm status of taut wire detection for each zone.
7. Alarm status of Delay Fence Integrity Detection for each zone.
8. Tamper status of each field enclosure.
9. The status of detection devices and status monitoring in the sally port area.
10. The operational (maintenance) status of field equipment for each field controller.

Abnormal conditions shall be acknowledged by the operator by activating a single icon. This shall also stop the audible sounder.

The colour of status icons shall change in the following sequence.

1. Green - Normal condition
2. Red Flashing - New alarm condition
3. Red Solid - Condition has been accepted by the operator

Blue shall indicate a device in a permanent abnormal condition and must be addressed by a maintenance repair procedure. Step 4 shall be omitted in case of certain maintenance devices or in case of CCTV surveillance where no field reset is required.

The following requirements shall be the minimum requirements for the user interface:

11.4.20.2 Operational Information

The following are shown on the operator interface:

1. Site perimeter Layout
2. Icons representing the alarm status of detection devices
3. Indications of field node status and tamper
4. Buttons to accept and reset alarms
5. Buttons to issue a reason for alarms

11.4.20.3 Management Information

Operational Status

Parameters providing a summary of the operational status of the equipment including:

1. Percentage site online
2. Detection devices in inhibit status
3. Status of worst case field node
4. Condition of field communication network

System performance

Summary of the number alarms during a daily, weekly and monthly period. Alarms are categorized as the following types:

1. Valid Alarms
2. Nuisance Alarms
3. Unknown Alarms

Operator performance

Values representing the maximum time the current and previous operator took to accept and reset alarms. Unattended time shall also be indicated.

Open a window to view the log

11.4.20.4 Diagnostic Information

The following diagnostic status information shall be made available:

1. Real time Alarm status of all devices on the selected field node
2. Maintenance status of these devices
3. Buttons to inhibit any device
4. Analogue values of detection devices
5. Controls to adjust the operating parameters of field devices

11.4.20.5 Networking

It shall be possible to link Multiple operator workstations to the same perimeter controller.

The graphical user interface as proposed must be presented to the end-user's authorised representative for approval before commencement of work. All available system information and specified requirements must be accessible through the User Interface. The user interface shall always be fully compliant to the above requirements.

11.5 Outer Fence – Kinematic Detection System

11.5.1 General

The Taut wire Inner fence is flanked by a 4,5m bowed welded mesh fence structure as per the attached drawings.

The purpose of the Kinematic detection system on the bowed outer fence is to protect it from tampering, and to detect individuals attempting to assist an escape from the outside. The system provides reaction teams with sufficient time to react and reach the point of intrusion in the case of tampering on the fence.

The physical fence acts as a delay system once a detection alarm is received to allow sufficient time for the reaction force to reach the point of intrusion.

This delay functions of the outer fence need to be protected to ensure that it fulfils its purpose. Detection is required to detect the cutting or removing of the structure and attempts thereof.

The required detection is based on direct measurement of the causes of cutting and removing of the structure and not derivatives thereof such as short circuit detection or volumetric detection not measuring fence behaviour.

Detection shall be based on the measurement of the kinematical behaviour of the structure during intrusion attempts.

The system shall be applied in order to ensure maximum coverage in the detection area.

12 OPERATIONS AND INCIDENT MANAGEMENT SYSTEM

12.1 Scope

The contractor shall supply, install and commission a web based Operations & Incident Management system capable of integrating with the Security Management System offered with this tender. The OIM System shall be capable of extracting real time operational and maintenance related alarms and events from the Security Management Sub-system hardware, and to present this data to a dedicated OIM workstation to be installed in the Central Control Room, as well as to relay the information in real time to the Correctional Services National Control Center situated in Pretoria.

The OIM System shall provide a single dashboard overview of the various system components, to enable the user Department to determine at a glance where operational procedures are being ignored, are inadequate or require amending, as well as to determine the efficiency of Maintenance activities by Area, site or country wide.

The system shall be exception based, whereby trends are analyzed against a set of rules which can be configured per device. Only when the trend or activity for a device or sub-system deviates from the configured rules shall an Operational Incident or Maintenance Activity be generated and reported. Such Incidents shall be escalated to the appropriate levels according to a configurable escalation schedule.

12.2 Integration

The OIM System shall be able to integrate with the following Security Sub-system hardware, as well as any additional hardware detailed in the site specific specifications under this tender:

1. Perimeter Detection System
2. Door Control System

3. Access Control System
4. Intercom and Public Address System
5. CCTV System
6. Fire Detection System
7. Duress System
8. Nurse Call System
9. Compressed Air System
10. Uninterruptible Power Supplies

12.3 System Overview

The OIM System shall provide access to a Web based enterprise platform to capture and report data relative to incidents, investigations and exposure, providing a single dashboard view of any risk associated with the various hardware systems.

It shall be possible to intelligently action and query system data for risk, trending. The system shall enable the user Department to make informed decisions which optimize performance and illustrate the effectiveness of it's security operation.

The system provided shall be capable of integrating with any commercially available Security Management System and Security sub-system hardware, and to present analytical data from all subsystems to the user on a single dashboard view.

The system shall have the ability to interactively manage incidents and investigations from beginning to end, including a complete sign off and review process. Automatically generated notifications via email and SMS shall alert appropriate users to issues in real time.

The System shall be accessible by any number of users, from anywhere, at any time via thin client technology enabling the system to be accessed over the Internet, LAN or WAN through any secure connection. All data shall be SSL encrypted, providing secure data transactions, to enable users to log in remotely without compromising the system security.

The System shall enable users from multiple levels within the Department to access the same information for different reasons.

12.4 Functionality

The OIM System shall offer the following functionality as a minimum:

12.4.1 Permissions

The OIM System shall have its own database security component to administer and control access to the underlying data. All users shall be granted access to the application by username and password, to allow strict control over the various levels that users are able to access. Generic username and passwords shall limit functionality, and shall be setup to cater for specific situations, for example where many different security personnel need to access, or enter data and where such personnel have not yet been designated and which may change on a day to day basis.

The system shall be capable of various levels of access, depending on the status of the user, for example, Management shall be able to view all outstanding incidents and investigation data, whilst others may be restricted to only those cases and investigations for which they are responsible. In addition, users shall be granted access to review certain aspects of a case but not to amend any of the details. The OIM Systems own Security shall be administered by users having specific administration rights, thereby allowing for the simple administration of existing and new user profiles.

12.4.2 Reference Data

The reference data elements (i.e. locations, incident types, investigating officers etc.) shall be treated as reference data items that shall be added as and when required by authorized users. This element of the application shall be tightly controlled to ensure that the referential integrity of data remains intact (i.e. reference data items cannot not be deleted, but merely flagged as "no longer in use", and thus, not viewable from any of the drop down menus within the application).

12.4.3 Incident Management

The system shall provide for two types of Incident entry. The first shall be an automated incident entry, whereby data received from the Security Management sub-system hardware e.g. an obstruction being placed in the path of a closing security door, shall be automatically entered and an incident created. The second type shall be a manual incident entry whereby users are able to enter incidents related to assets not connected to the Security Management System, e.g. an inmate reported as being in a restricted area without an escort.

An Electronic Occurrence Book/ Electronic Incident Book shall be a key component of the application and shall be available to build up a profile of various incidents (i.e. all related incident details such as an individuals, property, witnesses, vehicles, police case details, log file etc.) shall be reviewed as an extension of the incident.

Unique incident numbers shall be automatically established by the application, and once created, shall never be deleted to ensure integrity of the audit trail process. The incident shall become the primary source of input and all subsequent investigation activity shall be recorded as part of the incident.

New incident details shall be automatically entered or manually entered via a simple capture screen. It shall be possible to add specific details of the incident by the user. The capture of these details shall be standardized by means of pre-defined search lists to facilitate structured reporting (e.g. pre-defined incident types, locations etc.). Free form text input shall be limited to providing incident notes and wherever else it is considered necessary to cater for non-standard information situations. All entries into the application shall have standard time/date/user stamps for audit trail purposes. Incident details captured shall be validated as required to ensure that a minimum required level of detail is captured.

It shall be possible to select the incident complainants and any associated suspects from an existing list, or added at the time of creating the incident. Advanced search functionality shall allow a user to search across a number of search criteria (e.g. by surname, id number, name etc.) to ascertain whether the complainant or suspect already exists in the database. Mandatory procedures shall be automatically displayed in a popup window when specific incidents occur, to enable Control Room staff to follow a strict course of action when required.

12.4.4 Investigation

Subsequent investigations of an existing incident shall be treated as adding additional data to the original incident profile. Only authorized users shall be able to add and amend investigation data. It shall be possible for management to view investigation data, and to be able to add additional comments or issues that need to be followed up.

It shall be possible to conduct an investigation into the following incident categories as a minimum:

1. Security Incidents
2. Maintenance Incidents
3. Health and Safety Incidents
4. Human Resources Incidents

System prioritized incidents shall be automatically assigned to the investigations database, however, it shall be possible for authorized users to override non-prioritized incidents and flag them for investigation if necessary. Users assigned to an "Administrator" security level shall be able to create “auto assignment rules” which shall automatically assign repetitive type investigations to relevant users without the managers input.

It shall be possible for Investigation managers to be presented with an incident summary once they log in to the system, which provides a prioritized list of investigations which have been assigned to them for review.

12.4.5 Reporting

The system shall provide a range of standard and pre-defined reports, with the ability to create user defined reports on an ad-hoc basis, where users shall be able to specify report parameters at the time the report is generated.

It shall be possible to generate the following report types as a minimum:.

1. Trending/ Graph Report
2. Statistical Report
3. Management Dashboard Report
4. Map Report

All reports shall be web based, with the ability to export to Microsoft Excel or PDF format. The Management Dashboard Reports shall be dynamically linked to the database, displaying any criteria that the user wishes to view.

12.4.6 Data Search

The system shall provide the ability to cross reference between all incidents and related occurrences. The database shall be designed in such a way that the relationships between the various elements are automatically established at the point of entry, to provide advanced web based cross referencing of reports.

12.4.7 Equipment and Asset Register

The system shall provide a National equipment and asset register, which shall enable users to capture the details of any asset or piece of equipment on any of the sites linked to the National Control Centre. It shall be possible to create or edit an entry either from the relevant site or from the National Control Centre.

It shall be possible to Categorize and sub-categorize assets to three levels as a minimum, and provide the following Main Categories as standard:

1. Security
2. Electrical
3. Plumbing
4. Building

The following Sub-Categories shall be provided as standard

1. Security
    a. Perimeter

b. Security Doors
c. Door Control
d. Access Control
e. Intercom
f. Public Address
g. CCTV
h. Fire Detection
i. Duress
j. Nurse Call
k. Compressed Air
l. Control Room Equipment
m. IT Equipment
n. Ancillary Equipment
o. Radio Equipment
p. UPS
q. Power Distribution
r. Cable and Wire-ways
s. General

2. Electrical
    a. Lighting Fittings and Fixtures
    b. Power Outlets and Switches
    c. Distribution Panels
    d. Cable and Wire-ways
    e. UPS
    f. Standby Generators
    g. High Tension Equipment
    h. General
3. Plumbing
    a. Boilers

b. Domestic Heating

c. HVAC

d. Bathrooms

e. Kitchens

f. Piping

g. Valves

h. Pumps

i. Sewers

j. Drains

k. General

4. Building

a. Roofing

b. Brickwork

c. Windows

d. Doors

e. Gates

f. Lifts

g. Gardens

h. Sports Fields

i. Sports Equipment

j. Irrigation

k. Pest Control

l. Television Sets

m. Television Distribution

n. Telephone System

o. Telephone Distribution

p. Kitchen Equipment

q. Laundry Equipment

r. Medical Equipment

s. Office Equipment

The system shall provide for the seamless integration of all Security related assets into the OIM System Asset Register, by means of an automated import tool, which shall enable the Security Management System to automatically populate the OIM Systems Asset Register database with the following fields as a minimum:

1. Category (e.g. - Security)
2. Sub Category 1 (e.g. - Security - Door Control)
3. Sub Category 2 (e.g. - Security Door Control – Swing Door)
4. Site Reference
5. Area Reference
6. ID Number (Unique per asset)
7. Bar Code Number
8. Manufacturer
9. Manufacturer's Part Number
10. Description
11. Distributor Name
12. Distributor Telephone Number

In addition to the automated import facility, it shall be possible to view and manually edit the details associated with any imported asset as well as to manually create new assets and populate the database in accordance with the above-mentioned fields.

The system shall provide a standard .csv import tool for all other categories of assets not forming part of the Security Management System. The tool shall allow the user to create their own asset register in Microsoft Excel for the Electrical, Plumbing and Building related assets, and to import these spreadsheets into the OIM System via the CSV import tool provided.

The tenderer shall allow sufficient man hours for training of a suitable competent representative of the user, to enable them to create the necessary spreadsheets in preparation for importing into the system themselves.

12.4.8 Planned Preventative Maintenance Module

The system shall provide a full Planned Preventative Maintenance module which shall enable the Departments maintenance division to configure the Planned Preventative maintenance schedules for each asset type. As an example it shall be possible to schedule a routine maintenance activity for each individual asset by configuring a single asset sub-category type.

(i.e. all Security Door Controllers are to be serviced once every six months).

Once the service intervals have been entered per asset type, the system shall automatically generate the Annual maintenance schedule for each individual asset as well as to generate the daily schedule maintenance tasks for the assigned resources.

The following fields for the planned preventative maintenance schedules shall be provided within the OIM Systems database as a minimum:

1. Category (e.g. - Security)
2. Sub Category 1 (e.g. - Security - Door Control)
3. Sub Category 2 (e.g. - Security Door Control – Swing Door)
4. Site Reference
5. Area Reference
6. ID Number (Unique per asset)
7. Bar Code Number
8. Manufacturer
9. Manufacturer's Part Number
10. Description
11. Maintenance procedure (Text field describing the maintenance procedure)
12. Assigned Resource (e.g. - Team or Individual)
13. Cycle (Annual, 6 Monthly, 3 Monthly, 2 Monthly, Monthly, Weekly, Daily)
14. Estimated service time

When changes are made to a specific asset's Planned Maintenance criteria, an option shall be generated to apply the same criteria to all assets within the same Sub Category or ID Type. (Apply to all function). As an example, if the manufacturer of a specific door controller revises their recommended service period, the user need only edit the "Cycle" field of one such device, which can then be applied to all products within the same site with a single click.

Planned Maintenance Schedule Report

The system shall automatically generate a daily Planned Maintenance schedule report for each resource to which tasks have been assigned. The following information shall be provided per daily report as a minimum:

1. Category (e.g. - Security)

2. Site Reference
3. Area Reference
4. ID Number Range (display each unique ID number to be serviced that day)
5. Asset Description
6. Maintenance procedure (Text field describing the maintenance procedure)
7. Cycle (Annual, 6 Monthly, 3 Monthly, 2 Monthly, Monthly, Weekly, Daily)
8. Scheduled Start Date
9. Scheduled Completion Date
10. Scheduled Time for completion
11. Actual Time Completed (Manual entry by resource)
12. Actual Time required (Manual entry by resource)
13. Assigned Resource (e.g. - Team or Individual with space for signature)
14. Resource Comments (Technician's description of the fault)
15. Spares utilized (Technician's description of parts used)

Upon completion of scheduled Maintenance tasks, the system shall allow for all information which had been filled in on the printed report by the Technician and Administrative assistant, to be entered into the system and recorded in order to provided statistical reports relating to the predicted and actual time required to complete a group of maintenance tasks. The system shall use such information to prompt the appropriate user to amend Estimated service time per asset type,, in order to more accurately predict resource allocation.

12.4.9 Automated Breakdown Notification Module

The system shall provide a fully configurable Breakdown notification system whereby breakdown related events can be created, edited or deleted as required. Events affecting the smooth operation of the Security Management System shall be automatically reported to the appropriate specialist sub-contractor via SMS and email in order to minimize the downtime related to the breakdown.

The following maintenance related events shall exist within the system as standard, and reported via SMS and email together with the date and time of the event and the breakdown category:

1. Security Doors (Included, but not limited to)

Item	Security Door/ Gate Events
1.1	Door Fault on Closing alarm exceeding limit
1.2	Door Fault on Opening alarm exceeding limit
1.3	Door Control Node Communication Failure (with module No. notification)
1.4	Door Control Bus Segment Failure (with Bus segment No. notification)
1.5	Door Control Area Controller Failure (with controller No. notification)
1.6	Monitored DPS Open for longer than the configured time

2. Intercom & Public Address System (Included, but not limited to)

Item	Intercom & Public Address Events
2.1	Intercom Tamper Alarm (with Area and Door notification)
2.2	Intercom Node Communication Failure (with Node No. notification)
2.3	Intercom Bus Segment Failure (with Bus segment No. notification)
2.4	Intercom Area Controller Failure (with controller No. notification)
2.5	Intercom Call Button wiring fault (with station No. notification)

2. CCTV & Digital Recording System (Included, but not limited to)

Item	CCTV & Digital Recording Events
3.1	Camera Signal/Image loss Alarm (with camera No. notification)
3.2	Camera Communications Failure Alarm (with camera No. notification)
3.3	NVR Communications Failure Alarm (with NVR No. notification)
3.4	NVR Proprietary Alarm (with NVR and Alarm No. notification)

4. Duress System (Included, but not limited to)

Item	Duress System Events

4.1	Duress I/O module communication Alarm (with module No. notification)
4.2	Duress Input wiring fault (with module and Input No. notification)

5. Nurse Call System (Included, but not limited to)

Item	Nurse Call System Events
5.1	Nurse Call I/O module communication Alarm (with module No. notification)
5.2	Nurse Call Input wiring fault (with module and Input No. notification)

6. Perimeter Detection System (Included, but not limited to)

Item	Perimeter Detection Events
6.1	Taut Wire Maintenance Alarm (with Zone and sensor No. notification)
6.2	Master Controller communications Alarm
6.3	Taut Wire Loop Alarm (with Zone No. notification)
6.4	Kinematic Maintenance Alarm (with zone and sensor No. notification)
6.5	Kinematic Loop Alarm (with node and Loop No. notification)
6.6	Field Node communication Alarm (with node No. notification)
6.7	Field Cabinet Tamper Alarm (with cabinet No. notification)
6.8	Field Node Battery Charger Alarm (with node No. notification)
6.9	Taut Wire sensor Inhibit Alarm (with zone and sensor No. notification)
6.10	Taut Wire Loop Inhibit Alarm (with zone and loop No. notification)
6.11	Kinematic sensor Inhibit Alarm (with zone and sensor No. notification)
6.12	Kinematic Loop Inhibit Alarm (with zone and loop No. notification)

7. Compressed Air System (Included, but not limited to)

Item	Compressed Air System Events
7.1	Air Compressor Mains failure (with unit No. notification)
7.2	Air Compressor Maintenance Alarm (with unit No. notification)

7.3	Air Compressor Low Pressure Alarm (with unit No. notification)
7.4	Air Compressor Dryer Failure Alarm (with unit No. notification)
7.5	Air Vessel Low Pressure Alarm (with vessel No. notification)
7.6	Emergency Air Vessel Low Pressure Alarm (with vessel No. notification)
7.7	Air Manifold Low Pressure Alarm (with cabinet No. notification)
7.8	Air Manifold Cabinet Open Alarm (with cabinet No. notification)
7.9	Compressor Room Door Open Alarm (with room No. notification)
7.10	Air I/O module communications Alarm (with module No. notification)
7.11	Air I/O Input wiring fault (with module and Input No. notification)

8. UPS System (Included, but not limited to)

Item	UPS System Events
8.1	UPS Mains failure (with unit No. notification)
8.2	UPS Maintenance Alarm (with unit No. notification)
8.3	UPS Load on Bypass (with unit No. notification)
8.4	UPS Battery Low (with unit No. notification)
8.5	UPS Battery Failure (with unit No. notification)
8.6	UPS Load not protected (with unit No. notification)
8.7	UPS Surge Arrestor Failure (with unit No. notification)
8.8	UPS Communication Failure (with unit No. notification)
8.9	UPS Room Door Open Alarm (with room No. notification)
8.10	UPS I/O module communications Alarm (with module No. notification)
8.11	UPS I/O Input wiring fault (with module and Input No. notification)

9. Equipment Cabinets (Included, but not limited to)

Item	Equipment Cabinet Events
9.1	Equipment Cabinet Open Alarm (with area and cabinet No. notification)
9.2	Equipment Surge Arrestor Failure Alarm (with cabinet No. notification)

9.3	Ethernet Switch Communication Alarm (with switch No. notification)

10. Security Management System (Included, but not limited to)

Item	Security Management System Events
10.1	Server Communication Failure (with Server ID notification)
10.2	Workstation Communication Failure (with WS ID notification)

12.4.10 Operations Monitoring Module

The system shall provide an Integrated Operations Monitoring Module, whereby the standard conditions of operation of Security Sub-System hardware can be defined, and monitored in real time, and to automatically report any deviation from the standard operating conditions. As an example, it shall be possible to create a standard operating condition (set of rules) for the operation of a Security Sliding Door, in which the user can define the period for which the door may remain unlocked (open) before an exception event is generated. In addition to the open time period, the user shall be able to define the number of such events per door, that would constitute an incident, and to automatically report the incident to a senior level within the system.

The logging and reporting of such incidents shall include all details relating to the event, for example, the Time, Date and Operator responsible for opening the door.

It is a specific requirement of this tender that the OIM System and the Security Management System (SMS) are fully integrated to enable operational incidents to be monitored and reported in real time.

The system shall allow system user's with a suitable security and experience level, to create user defined operational conditions for any security sub-system hardware component.

The system shall enable senior users to configure which alarms and events are to be escalated and to whom they should be reported. The system shall also allow for general notification whereby senior users can be notified of Alarms and events without needing to take any action.

The system shall present the appropriate users with the following information relating to each alarm or event, via their Dashboard overview:

1. Date of the incident
2. Time of incident
3. Category of Incident

4. User responsible for the incident
5. Responsible Users contact details
6. Time lapsed since the incident
7. Description of the Incident
8. Recommended Action to be taken

12.4.11 Dynamic Reports and Forms

The system shall provide a dynamic Reports and Forms tool, which shall enable users to dynamically create new pages (Tabs) and Input Fields for any additional information capture requirements. The tool set shall negate the need for Hard Coding Development and shall be carried out by a System Administrator.

13 CELL PHONE DETECTION SYSTEM

13.1 General Characteristics

The following functional features shall be provided by the proposed system:

1. Be capable of detecting GSM, 3G, 4G and HSDPA type signals.
2. Be capable of detecting the abovementioned signals for voice, sms and data transmission.
3. The unit connection to external hardware shall be via a potentially free contact.
4. The system shall be capable of detecting a cable fault, the disconnection of the unit or the unit not being operational.
5. The unit shall be IP65 rated, suitable for outdoor installation.
6. Sensitivity shall be adjustable, with at least 8 settings for detection range.
7. Detection range, for a typical installation, shall be a minimum of 7m through a re-enforced concrete wall.
8. The distributed Cell Phone Detection System shall not be influenced by permitted equipment typically found in the Correctional environment such as Warder radios and repeater networks.

13.2 Software Operation

The Graphical User Interface shall interface with the Distributed Cell Phone Detection System. The location of the alarm shall be clearly represented both graphically and in text format. Various configurable options shall exist for the alarm handling such as “Force to Acknowledge”, “Popup Window”, “Automatic Camera Selection”, ”Jump to correct screen”, etc All alarms and associated Operator Acknowledgements shall be logged in the History Database with an automatic archiving facility. The software shall display the current health status of the Cell Phone Detection System.

14 NURSE CALL SYSTEM

14.1 INTRODUCTION

The Nurse Call system(s) shall be an independent system of modular design to facilitate future expansion/alteration to the design.

14.2 SCOPE OF WORK

1. The design, preparation of, detailed drawing, supply, delivery to, off-loading at and handling on-site, installation, training of selected personnel, testing and commissioning of a Nurse Call System system/s, as detailed in the summary Bill of Quantities, and strictly in accordance with the specification and list of drawings, including the provision on site of all consumables, including welding and grinding consumables, tools, contractor's equipment, skilled and unskilled labour necessary to fulfill the successful Bidder's obligation in terms of the contract to the satisfaction of the Project Manager.

2. The Nurse Call system shall be of an open voice, selective calling type with individual selector buttons for each substation.

3. The Nurse Call system shall be a standalone system situated in the hospital at each departments reception desk and shall provide the following information and functions:

    a. Provide hands free communication between each bed station and master station

    b. Three types of call-in signals identified differently by tone and LED light:

        i. Routine

        ii. Urgent Call

        iii. Cord-Out Trouble Call

    c. Nurse Call station active/inactive status

4. The system shall contain a master control station (mimic control panel) located at a central point utilizing open voice to communicate to sub-stations situated varies points in the hospital.

5. The master station shall be desk or wall mounted. The sub-stations shall be surface or flush mountable.

14.3 SYSTEM HARDWARE

1. Intercom Master Station

    a. The master station shall be available in 50 station size, with the option to expand to 80 stations with the addition of 30 call add-on selector.

    b. A handset on the master shall provide private communication to a substation.

    c. Master station shall be Voice-actuated or press-to-talk communication through the handset, with hands free response from the called sub.

    d. Communication controls shall include a"TALK" button and an All Call" button. Transmit Receive, All Call, and Call Tone volume controls shall be provided on the back of the master station.

    e. Receive and Call Tone volumes shall also have user-adjustable controls on the side of the master station. Preset volume controls shall be on the bottom of the Master station.

    f. An incoming call shall be enunciated by an electronic ringing call tone, and the corresponding station LED shall light. Both the call tone and the LED shall remain active until the call is answered at the master or reset at the calling location.

    g. The LEDs above the selector buttons shall illuminate when the station button is pressed at the calling master.

    h. Master station automatically selects and connects to the highest priority call when multiple calls are received. Up to 5 incoming calls shall be displayed at a time.

2. Bedside Sub Station

    a. Sub stations shall be surface or flush mount styles and shall be a single or dual-call station.

    b. The communication at the sub-station is hands free.

    c. Sub stations shall be fitted with a hand-held call button

    d. When activated, the station will activate a ring tone and LED at the substation. The corridor lamp will lit steadily white.

    e. When the hand-held call button is pulled out of the jack, the station will activate a ring tone and LED at the substation. The corridor lamp will blink white.

3. Bathroom/Bedside Pull Cord Station

    a. The station shall be surface or flush mount styles.

    b. The station shall be fitted with a pull cord for easy activation.

    c. The station shall be fitted with a pull-to-lock switch

    d. When activated, the station will activate a ring tone and LED at the substation. The corridor lamp will blink red.

4. Corridor Lamp

    a. The lamp will indicate location and type of call.

    b. The lamp shall have two indication lights, red and white.

14.4 POWER

1. Under normal operating conditions the system shall operate from a standard electrical supply of 220 volts (nom.) at 50Hz. notwithstanding that the primary power to the system is 220 volts individual items of equipment such as the master station, substation, corridor lamps, etc. shall always operate from 24 volts DC by means of suitably rated power supply modules.

2. Under mains fail conditions the system shall automatically draw power the UPS. The transition from AC operation to UPS operation shall be realized on a "no-break" basis. The integrity of all system settings and paging traffic in progress shall be maintained.

15 ADDRESSABLE FIRE DETECTION

15.1 GENERAL

1. This part of the specification covers the design, supply, installation and commissioning of all equipment for the Addressable Fire Detection and Gas Suppression system. The entire installation shall function as a single integrated Fire Detection system.

2. The Fire Detection system shall be capable of being fully integrated with the SMS via a bi- directional high level interface to allow monitoring of all Fire Detection Zones by the SMS and to inform the SMS operator via the GUI of any alarm condition detected by the Fire Detection system.

3. The system shall comply with SANS 10139: 2000, "Fire Detection and Alarm Systems for Buildings".

4. The complete Fire Detection system, as approved by the consultant, shall be installed throughout the building and include but not limited to the following components:

    a. Microcomputer based fire control panels, interfacing directly with field detection and control devises

    b. Communications network between the Fire Panels and Security IP Network

    c. Addressable fire detectors

    d. Addressable manual call points

    e. Addressable zone loop isolators

    f. Addressable loop sounders

    g. Interface with air conditioning & ventilation systems (where required)

5. All control, indication and monitor equipment related to the fire detection installation shall be produced by the same manufacturer.

6. All basic equipment proposed and planned for use must be formally approved by at least two (2) international recognized testing laboratories, such as:

    a. Underwriters laboratories, USA (UL)

    b. Factory Mutual, USA (FM)

    c. Verband der Schass Versekerer, West Germany (VdS)

d. Association Francais de Normalization, France (AFNOR)

e. British Standards, great Britain (BS)

f. Fire Office Committee, Great Britain (FOC)

g. Underwriters Laboratories, Canada (ULC)

h. Loss Prevention Certification Board (LPCB)

7. The control unit and sensors shall conform to the following standards:

   a. Control Unit EN54-2 (Draft 1996)

   b. Smoke Sensors EN54-7 (1996)

   c. Heat Sensors EN54-5 (1996)

   d. Multi sensors ISO7240-15 (Draft 1996)

   e. Manual call points EN54-10 (Draft 1996)

15.2 FIRE CONTROLAND FIRE DETECTORS

15.2.1 General

1. The fire detection system shall be of the addressable analogue type and the fire control panel shall be utilized to monitor and control all addressable devices installed in the building.

2. The fire control panel shall have a capacity of 4 loops, each with a capacity of up to 127 addressable devised installed onto them. The control panel will support a total of 50 zones.

3. The fire control panel shall annunciate an alarm condition as soon as a fire, abnormal rise in temperature, rise of temperature above a set level or smoke detector is detected or activated to the central fire management system.

4. The fire control panel system shall be programmable on site so that it can be modified or adjusted to accommodate changes that could be made to the building as well as to make provision for future expansion. Changes to the system software on the site shall be maintained during a power failure.

5. The fire control panel system shall be fully modular in its design to cater for the prescribed requirements and specifications.

6. The fire control panel shall consist of a LCD display, indication LED and a control keyboard. The control panel shall communicate to the SMS system via the IP network to display alarm conditions and appropriate messages on the SMS operator station and display on the GUI floor plans any alarmed fire zones.

7. The event printer of the central fire management system shall record all alarm messages with the appropriate date, time and alarm information.

8. Photo-electric Smoke detectors shall be installed on ceiling in the all Blocks in offices, store rooms and passages.

9. Heat Detectors shall be installed in all Kitchens and Laundry Areas.

10. Early warning Flame detectors shall be installed in the Generator Room.

11. An Inert Gas Control system shall be installed in the UPS room and will be incorporated into the fire detection system.

12. Fire conditions in the all areas of the building shall be detected by means of automatic fire detectors and manual alarm call points (break glass units). All the detection zones shall be wired in a Style A (ring) system to the fire control units. The fire detectors shall be installed as indicated on the drawings with. Indication LED of detectors installed inside the ceilings shall be repeated below the ceiling.

13. On the detection of a fire condition or fault, the change of state of the equipment mentioned above shall be communicated to the fire control panel.

14. The date, time, priority, geographical location, area name and description of the alarm shall be recorded on the event printer of the fire control panel.

15. The local fire control panel shall activate the fire warning alarms. These warning alarms will be communicated to the SMS operator in the Main Security Control room and displayed on the Graphical User Interface.

16. If a positive report of a fire alarm is confirmed at the fire control panel, the panel shall automatically initiate alarm equipment and activate appropriate evacuation alarms. All air conditioning and ventilation fans shall be switched off.

15.2.2 Facilities of the fire control panel

1. The transmission medium to transmit information from fire detectors and alarm points, as well as for transmitting control information to air conditioning installations, etc. shall be through a two wire connection via the fire control panel.

2. All communication shall be controlled from the fire control unit, which shall sequentially poll each device in turn and authorize communication.

3. No device shall communicate with the fire control panel unless polled.

4. The fire control unit shall be able to read information from a device or send instructions to a device.

5. Each device on line shall have a uniquely identifiable address on the control unit. This shall be achieved by pre-setting the address of each device.

6. Removal of a detector head from its base shall report a fault condition to the control unit when polled.

7. The identification of each type of address unit and each type of sensor (i.e. multi sensor, ionization detector; heat detector, I/O switch, etc.) shall be transmitted to the panel on each polling scan.

8. The condition of each line device, including circuit, calibration and contamination, shall be transmitted to the panel on each polling scan.

9. The system shall check the calibration of each analogue line device and record changes caused by environmental contamination.

10. When maximum calibration adjustment is reached the panel must indicate a "maintenance" signal. This must be a dedicated signal, and must be separate from the "pre-alarm" signal.

11. The build-up of dirt or similar contamination on the optical surfaces will cause the output signal from the detector to gradually change. The control panel shall be capable of monitoring this slow change in signal and at a predetermined level indicate that the detector is in need of servicing.

12. It shall be possible to connect the following units or detectors to the fire control panels:

    a. Optical (photo electric) smoke detectors

    b. Heat detectors set temperature level

    c. Heat detectors rate of rise

    d. Linear Beam detectors

    e. Input / Output control units

    f. Zone isolators

    g. Loop sounders

    h. Manual call points

    i. Addressable Gas control units

    j. Remote indication panels with local alarm silence facilities

13. The units mentioned above should be monitored automatically and continually for open circuit, short circuit and earth leak conditions, as

well as for instances where detectors are removed from its base plate or if device address duplication exists.

14. Any fault detected in the lines which connect the equipment to the fire control panel shall indicate a faulty condition at the fire control panel when polled by the control panel.

15. Any change in the ambient condition of any sensor unit shall automatically update the memory of the fire control panel.

15.2.3 Monitoring of elements on an alarm line

1. The alarm threshold of every detector shall vary in accordance with each idle condition. This change shall be stored and be continued updated in the memory of the fire control panel.

2. The alarm threshold of any detector shall not be manually set.

3. Each element of an alarm line shall be continually and automatically monitored, individually. When the value of an element reaches a level at which it will no longer perform its function, a fault alarm must automatically be indicated at the fire control panel.

4. Such a fault indication shall not prevent a fire alarm condition from alarming in the line being detected and indicated.

15.2.4 Monitoring of zones

1. Each detection line shall be devise able into a maximum of fifty (50) separate zones.

2. Each zone shall be clearly defined and indicated.

3. Each zone must have the facility to be monitored for a fire alarm condition from either manual or automatic detectors.

4. Devices shall be grouped into zones as follows, unless the zones are indicated on the drawings and/or Supplementary Specification:

    a. Each building shall have separate zones.

    b. The floor area of a single zone shall not exceed 2000 m2.

    c. Every floor of a building larger than 300 m2 shall be on a separate zone.

    d. Every area enclosed by fire walls shall be on a separate zone.

    e. In analogue addressable system, each zone shall be enclosed by two (2) line isolators.

15.2.5 Alarm/Detection lines

1. Alarm/detection lines may have a capacity of detectors or elements as decided upon by the manufacturer.

2. These detectors/elements shall be freely distributable over any one of the individual alarm zones.

3. An alarm zone may only extend over a single fire zone and quick and precise identification of a fire must be possible.

4. An alarm line shall not extend beyond one floor, except in the case of staircases or lift shafts.

5. The fire control panel with its LCD and mimic panel shall be utilized to indicate the exact position of triggered detectors/elements in any line.

6. A triggered detector/element shall not cause any other detectors on the line to seize monitoring.

7. The fire control panel shall be capable of switching off air conditioning units and fans, and instruct lift controls to home in the case of a fire alarm.

8. In the specific zone where a fire has been detected, it shall be possible to control equipment plant, etc. - pertinent to that particular zone only.

9. Any detector when triggered shall be capable of causing specific control functions.

10. Every line shall have "double knock" function built-in, providing a specific control function capability whenever two detectors on the line are triggered.

11. Any individual zone or detector in an alarm line shall be capable of being isolated without effecting the operation of the remaining zones or detectors in the line and without raising a fire alarm.

12. However, during this condition, an isolation indication per zone shall be displayed on the LCD of the fire control panel.

15.2.6 Processor monitoring

1. The processor shall be continuously monitored, and at the occurrence of a failure, shall the microprocessor be automatically restarted. Should the microprocessor fail to restart, an alarm to this effect shall be activated.

2. All failures and restarts of the microprocessor shall be automatically logged to a counter for statistical purposes. During start up, diagnostic tests on all memory devices must be performed.

15.2.7 Fire control panel access levels

1. Access to the system control panel shall be protected as follows:

    a. CONTROL KEY The control key shall be used to enable or disable the key board and control keys of the panel.

    b. ACCESS CODES Access codes shall be used to prevent unauthorized entry into the programming menus of the panel. Each menu shall be able to have 2 different levels of access.

    c. DOOR LOCK The panel door lock shall be used to prevent unauthorized entry into the cabinet.

    d. NON-VOLATILE MEMORY SWITCH -The non-volatile memory switch shall prevent any unauthorized or accidental changes being made to the system configuration data.

15.3 FIRE CONTROLPANEL

15.3.1 Self-monitoring

1. The control panel shall be designed and programmed to perform extensive automatic self- monitoring. If the control panel detects a fault, it shall result in a fault indication being given by means of a common fault amber LED.

2. The following shall be continuously monitored by the control panel:

    a. 24V power supply fault (external supply)

    b. Fire brigade/evacuation short circuit

    c. Alarm bell open circuit

    d. Fire Brigade short circuit

    e. Alarm bell short circuit

    f. Power failure

    g. Watchdog time-out

    h. Low battery

    i. No battery connected

    j. Tamper switch

    k. .2.11 No printer

l. Memory lock unlocks

m. Event buffer full

n. No communication

o. Earth fault

p. Battery over-voltage

q. RAM memory check

r. EPROM memory check

15.3.2 Programming of Fire Control Panel

1. Programming shall be done from the keypad at the front of the panel or by downloading data from a PC. All programming shall be menu-driven and protected by access codes and memory lock. The programming shall allow for at least the following functions:

    a. Programming Detectors

    b. Programming Inputs/Outputs

    c. Uploading/Downloading of configuration data

2. It shall be possible to programme all the above also from a PC by downloading the information to the panel. The installer/user shall copy the complete system's programme to external storage medium.

3. One way of programming will not exclude the other.

4. It shall be possible at all times to upload the stored programme to a PC in order to maintain updates.

15.3.3 Maintenance Functions of Local Fire Control Panel

1. The control panel shall provide extensive facilities to help with the general use and maintenance of the system. As a minimum the following maintenance facilities shall be available:

    a. Automatic Monitoring

        i. Every addressable device shall be continuously monitored by the control panel for the following:

            - Removal of Device
            - Quiescent Value
            - Contamination

- Circuit Failure
- Device Type
- Communication Quality
- Short Circuit
- Open Circuit

ii. Should any of the above parameters be out of specification the panel shall give a fault indication visually and audibly.

iii. A description of the nature of the fault as well as the location of the faulty device shall also be displayed.

iv. The control panel shall also monitor all loops for earth faults which shall be reported as described above.

b. Visual Monitoring

i. It shall be possible to visually monitor, on a real time basis, the status of each device connected to the system.

ii. Furthermore graphics screens shall be available for zones and individual sensors where the following may be visually monitored:

- Actual Value
- Average Value
- Maximum and Minimum Values
- Contamination Levels
- Communication Quality

iii. Each of the above screens shall be printable on demand by means of a print screen facility.

c. Archive Facility

i. The control panel shall have an archive facility capable of storing the last 999 events. The events shall be stored on a first in, first out basis. It shall be possible to print these events selectively as follows: •

- All Events.
- Fire Events Only
- Fault Events Only

- Conditions/Maintenance Events Only
- Soak Test Results
- Actions (i.e. Reset/Sound Bells, etc)
- Last x Events from a Given Date/Time

d. Statistics

i. The system shall be able to supply the following statistics per device:

ii. Maximum and Minimum Value with Data.

iii. Average Value.

iv. Number of Alarms.

v. Communication Quality.

e. System Maintenance Reports

i. The following system maintenance reports shall be available on demand:

ii. Event Buffer Data.

iii. Soak Test Results.

iv. Test Reports.

v. Exception Reports.

f. Service/Commission Mode.

i. A service/commission mode switch shall be available to assist the installer with the commissioning and servicing of the system. In the service/commission mode all panel outputs shall be disabled in order to prevent false alarms from being raised during the servicing/commissioning of the system.

g. Zone Test Mode

i. The control panel shall be able run in a test mode which will allow a one person walk test for up to 4 zones simultaneously. When in this mode, the control panel shall not operate any relays or alarms based on the data received from the zones on test. However, the panel will log all alarms occurring in these zones in order to generate a report at the end of the test period.

ii. Should an alarm occur in any zone other than those being tested, then the panel shall respond to the alarm in the normal manner.

h. Sensor Test

i. A self-test feature shall be incorporated in all analogue sensors. The control panel shall initiate the self-test for each sensor and monitor the results obtained from each sensor. After the completion of the test the control panel shall evaluate the results and pass or fail each respective sensor. A printout of all sensors failing the test shall be provided.

i. Soak Test

i. Should problems be experienced with a particular sensor, it shall be possible to run that specific sensor into a soak test mode. The soak test feature shall provide the facility to monitor and log, at programmable intervals, all data received from the sensor under test for analysis at a later stage. In this mode the control panel shall not generate any alarms or faults based on the data received from a sensor in soak test mode.

j. Remote Maintenance

15.4 FIELD DEVICES

15.4.1 Detector bases

1. All plug-in detectors shall fit onto a common type standard base. Once a base has been installed, it shall be possible to insert, remove and exchange different types of detectors.

2. Each standard base shall be equipped with scrawls wiring terminals capable of securing wire sizes up to 2,5mm2. Only 1,0mm2 or 2,5mm2 shielded two cores fire retardant cables shall be used.

3. The standard base shall be delivered with installed sealing plates which shall prevent dirt, dust, condensation or water from the conduit connection from reaching the wiring terminals of detector contact points before detector heads are installed.

4. The standard base shall feature built-in mechanisms which shall allow mechanical locking of an installed detector head and prevent unauthorized removal or tampering. It shall be hermetically sealed to prevent the ingress of dust, dirt or humidity.

5. All circuitry shall be protected against electrical transients and electromagnetic interferences. No base shall be damaged from reverse polarity or faulty zone wiring.

6. By means of another optional plug-in module it shall be possible to convert a standard detector into an individually addressable detector

system providing each connection base with its own unique identification address.

7. The detector head shall have a built-in LED alarm indicator and it shall be repeated below the ceiling should the detector be installed inside the ceiling void. The repeat LED alarm indication below the ceiling shall be connected by means of a simple two-core wire system from the base of the detector mounted inside the ceiling. No changes in the zone wiring shall be required to operate an additional remote alarm LED indicator below the ceiling.

15.4.2 Photo-electric (Eight Scattering) Smoke Detectors (Optical)

1. Photo-electric smoke detectors shall exhibit uniform response behaviour in course of time. Smoke density in the chamber shall be measured by a symmetrical optical system. They shall automatically adjust the light source intensity to compensate for further effects of dirt and dust accumulating in the measuring chamber.

2. All electronic circuits shall be solid state devices and hermetically sealed to prevent ingress of dust, dirt or humidity.

3. All circuitry shall be protected against electrical transients and electromagnetic interferences. No detectors shall be damaged by reversed polarity or faulty zone wiring.

4. Detectors shall have no moving parts or components subject to wear and tear. The detection principle shall employ a multi-light pass coincidence circuit preventing false alarms.

5. The response sensitivity of each detector shall be field adjustable to a minimum of two predetermined (factory calibrated) levels. It shall be possible to test the sensitivity of each detector in the field.

6. The response (activation) of a detector shall be clearly visible from the outside by a red LED of sufficient brightness.

7. The smoke entry window of the detectors shall be field adjustable to adapt the detector sensitivity to local conditions. A wire mesh shall prevent the entry of insects into the measuring chamber.

8. A built-in optional integration circuit shall allow the suppression of brief deceptive phenomena.

9. The detector covers shall be of the snap-on type to enable simple and thorough cleaning. The detectors shall be installed in their bases by a simple push mechanism for easy maintenance.

15.4.3 Early Warning Multi-sensing Fire Detectors

1. Multi-sensing fire and smoke detectors shall consist of integrated high sensitivity smoke & thermal detectors.

2. All electronic circuits shall be solid state devices and hermetically sealed to prevent ingress of dust, dirt or humidity.

3. All circuitry shall be protected against electrical transients and electromagnetic interferences. No detectors shall be damaged by reversed polarity or faulty zone wiring.

4. Detectors shall have no moving parts or components subject to wear and tear. The detection principle shall employ a multi-light pass coincidence circuit preventing false alarms.

5. The detector shall have the ability to discriminate against false alarms.

6. The response (activation) of a detector shall be clearly visible from the outside by a red LED of sufficient brightness.

7. The detector covers shall be of the snap-on type to enable simple and thorough cleaning. The detectors shall be installed in their bases by a simple push mechanism for easy maintenance.

15.4.4 Heat Detectors

1. A combination of rate of rise and fixed temperature heat detector. The combination detector shall consist of two independent thermistors connected into a bridged circuit.

2. All electronic circuits shall be solid state devices and hermetically sealed to prevent the ingress of dirt, dust and humidity.

3. All circuitry shall be protected against electrical transients and electromagnetic interferences. No detectors shall be damaged by reversed polarity or faulty zone wiring.

4. The detectors shall have no moving parts or components subject to wear and tear. The sensitivity of the detectors shall conform to Class 1 of "Euronorm 54-5" (+58 deg C or 82 deg C).

5. It shall be possible to check the electrical sensitivity threshold in the field.

6. The response (activation) of the detectors shall be clearly visible from the outside by a red LED of sufficient brightness.

7. The manufacturer shall produce and provide test equipment allowing to test and change the rate of rise/fixed temperature heat detectors up to 7 metres above floor level.

8. A built-in optional integrated circuit shall allow the suppression of brief deceptive phenomena.

9. Detector covers shall be of the snap-on type to enable simple and thorough cleaning. The detectors shall be installed in their bases by a simple push mechanism for easy maintenance.

15.4.5 Manual Alarm Call Points (Break glass Units)

1. The manual call points shall be electrically compatible with a standard range of automatic detectors so that it can be connected directly into a supervised line or zone of the manufacturer's standard type.

2. The manual call points shall be of present streamline appearance and design as a flat device permitting its use as flush- and surface mounted unit.

3. The manual call points shall consist of a base plate, insert and cover. The base plate shall contain prepared passages to make it adaptable for mounting on a standard round outlet box and single junction boxes.

4. The cover shall be of the snap-on type without screws and secured against unauthorized removal. Every removal of a cover shall release an alarm.

5. The breaking of the glass shall release an alarm. All inscription texts and marks shall be on the manual call point front plates and not on the glass.

6. The glass shall be secured in a cover against falling out. The alarm contact shall be of a self-cleaning design to prevent failure after a long period of inactivity in unclean environments. The manual call points shall be designed for fail-safe operation.

7. Each call point shall have a local built-in LED automatically confirming that it has been activated. It shall be possible to test a manual call point without destroying the seal or removing the cover.

8. The call points shall have clip terminals with built-in strain limits. The call point alarm actuating mechanism shall be equipped with a strain limit. It shall be possible to reset the alarm call point with a special tool only.

9. Each manual call point shall be equipped with a self-holding device to maintain the alarm condition until it is reset by an authorized person.

10. If called for, waterproof call points shall be provided in accordance with the requirements of IP66 and shall be designed to permanently

withstand corrosion as defined by European standards, made available by the manufacturer.

15.4.6 Solar Flame Sensor

1. The solar beam detector shall respond to a low frequency of 2 to 15 Hz modulation radiation emitted from flames during the combustion stage.

2. The detector shall operate properly through layers of oil, dust and water vapour. Gas fires not visible to the naked eye shall be detected. (Hydrogen)

3. The sensor shall consist of two photo electric detectors responding to adjacent Infra red wavelengths enabling the detector to discriminate between flames and a spurious source of IR radiation.

4. The detector shall be equipped with four preset sensitivity and at least three distance range settings

5. It shall be possible to check the electrical sensitivity threshold in the field.

6. The response (activation) of the detectors shall be clearly visible from the outside by a red LED of sufficient brightness.

7. The sensor housing shall be provided in accordance with the requirements of IP66 and shall be designed to permanently withstand corrosion as defined by European standards.

15.4.7 Linear Beam Detectors

1. The linear beam smoke detectors shall be powered from the control panel power source. The unit shall consist of separate a transmitter and receiver. This unit shall operate in a range of 7m to 100m.

2. The detector shall feature a bank of four alignment LEDs on both the receiver and transmitter that are used to ensure proper alignment without the use of special tools. It shall be possible to adjust the vertical and horizontal alignment without the need to refit the detector.

3. The beam detector shall feature automatic gain control which will compensate for gradual signal deterioration from dirt accumulation on lenses. Testing shall be carried out, using calibrated test filters.

15.4.8 Air Duct Smoke Detectors

1. Air duct smoke detector shall be capable of detecting visible and invisible products of combustion.

2. The detector shall be provided with a measuring chamber and a protected reference chamber sensitive to changes in temperature and

humidity only. The measuring chamber shall be protected from damage and insects.

3. A five second delay shall be employed on these detectors to minimize alarms due to transient smoke.

4. Variations in duct air velocity between 400 and 4,000 FPM (2 and 20.3 m/sec.), shall not cause any false alarms. Radioactive parts and protect circuitry shall be safeguard against electrical transients, electromagnetic interference, and polarity reversal.

5. The detector's head shall be mounted in an IP 65 rated enclosure suitable for outdoor mounting next to the air duct.

6. An air sampling tube shall be installed from the enclosure into the duct air stream.

7. A LED Alarm Indicator and key operated alarm indicator/test switch shall be fitted onto the enclosure.

15.4.9 Line Isolators

1. The line isolator shall be designed to connect into the detector line and monitor the line for short circuit. In the event of a short circuit occurring, the line isolators on each side of the short circuit should disconnect and isolate that portion of line from the system enabling the remainder of the system to function normally.

2. Each line isolator shall be under software control of the panel, but shall not remove a line address from the system. It shall be possible to selectively open or close line isolators from the panel when in maintenance mode.

3. Line isolators shall be mounted in a moulded plastic enclosure and shall be suitable for surface or semi-flush mounting. Normally one (1) line isolator will be installed for every twenty (20) detectors.

4. A light emitting diode (LED) shall illuminate when an isolator is in an open or isolated condition. It shall be possible to repeat the LED alarm indication below the ceiling by connecting a simple two-core wire to the base. No changes in the zone wiring shall be required to operate an additional alarm indicator.

15.4.10 Input Devices

1. The input devices shall be designed to collect and transmit status information from external devices via the input bits, and operate relays as instructed by the output bits from the control information.

2. The input device shall monitor conventional/sprinkler/hydrant flow switches, and varies other input types. This unit shall be addressable and connected to the same loop as the detectors.

3. The device shall report individual input statuses and faults to the panel under a single address for any one of the inputs.

4. Each input device shall be contained in a polycarbonate or metal enclosure to meet IP42 for indoors or IP65 for outdoors requirements and provide easy cable access from several sides onto a terminal block. Terminal arrangements and wiring information shall be included for each device.

5. LED's shall be fitted to the units which are turned on when the interface are operational.

15.4.11 Output Devices

1. The output device shall be design to switch external devices by means of volt free change over contacts.

2. The output device shall switch air-conditioning, extractor fans, electro magnetic locks and varies other switch-able systems. This unit shall be addressable and connected to the same loop as the detectors.

3. The device shall report individual output statuses and faults to the panel under a single address for any one of the switching systems.

4. Each input device shall be contained in a polycarbonate or metal enclosure to meet IP42 for indoors or IP65 for outdoors requirements and provide easy cable access from several sides onto a terminal block. Terminal arrangements and wiring information shall be included for each device.

5. For relay operation the operation instruction shall be continually renewed each time the control unit addresses the device. Output relay rating shall be 5A 230V AC.

6. LED's shall be fitted to the units which are turned on when the relay is operational.

15.4.12 Fire Alert Devices (Loop Sounder)

1. The addressable sounders shall be loop powered and provide both audible and visual warning signals.

2. Separate mounting bases shall be required which enable ready removal of the devices for maintenance. The units shall be provided with a locking facility as required for the fire detectors.

3. A device circuit controller shall provide a means of monitoring a device circuit and operating the devices from any location on the system.

4. The devices shall be able to generate two tones; the second tone shall be a continuous sound for evacuation purposes. The minimum sound pressure level measured at a distance of 'I meter shall be 102dBa.

15.4.13 Power Supply and Charger Unit

1. The power supply unit shall form an integral part of the control unit and shall operate from mains power of 240V ± 10%.

2. Each power supply unit shall contain over-voltage protection to prevent any malfunction or damage due to power line surges.

3. In the event of a failure of the normal mains supply to the central panel there shall be an automatic switch-over to the standby battery supply without disturbing the sound operation of the fire detection system.

4. The standby battery shall be automatically maintained in a charged condition by the charger unit.

5. When the AC power is restored the power supply shall automatically revert to battery power, and the system shall remain fully operational.

6. The power supply and charger unit, including all fuses, shall be entirely supervised. Any malfunction or blown fuse shall result in a fault indication on the control panel.

7. Nickel-cadmium batteries shall be housed in plastic containers with the maximum and minimum electrolyte levels indelibly marked on the housing.

8. Full details concerning routine maintenance, top-up or the periodic replacement of the electrolyte in the case of nickel-cadmium batteries shall be supplied by the Contractor. The necessary criteria concerning deposits such as sodium carbonate etc, which may form in the electrolyte and which may necessitate a change of electrolyte shall be submitted by the Contractor.

15.5 INTERFACE WITH AIR CONDITIONING VENTILATION SYSTEMS AND LIFTS

1. The contractor shall supply and install relays (I/O) in a separate enclosure for each unit to be switched off and wire the contacts of the relay to terminals. The feedback status of the controlled equipment: of each unit shall be monitored.

2. The contractor shall install I/O modules at the lift control panels in the lift motor rooms. The I/O relay shall activate for any fir condition, and shall cause the lifts to home. The wiring from the lift controls to the I/O modules shall be done by the lifts contractor.

15.6 SYSTEM CABLING

15.6.1 Loop Cabling

1. Return loop wiring as per style A shall be installed in all areas of the building.

2. The cable shall be suitably screened for protection against interference in any environment.

3. The cable used in fire alarm and fire evacuation communication systems including auxiliary circuits controlling equipment, shall be fire retardant with min two (2) conductors shall comply in full with all requirements and recommendations as per SANS 10139: 2000.. The cable shall be suitably screened for protection against interference in any environment.

4. The following methods are acceptable for the wiring of detector circuits:

    a. Cable racks/wire ways and steel conduit cast into, or built into, the building structure and wired with insulated conductors of a type which complies with the requirements of this specification;

    b. Cable racks/wire ways and steel conduit and conduit accessories, surface mounted in building structures and wired with insulated conductors of a type approved by the department;

5. Separate wiring installations for detector circuits, evacuation communication wiring, audible alarms, electrical lock wiring, card reader wiring, AC and DC power circuits, remote control circuits and monitor wiring, video cables, computer cables, etc., shall all be done in separate conduit, but can be shared in cable wire ways and underground sleeves.

6. Detector wiring may share the same draw boxes or expansion joint boxes with other firefighting system wiring or security system wiring, but the boxes shall be subdivided by means of steel plates.

15.7 SERIAL COMMUNICATIONS

1. Communications between the fire control panels will be via TCP/IP, connected to the Security LAN via Cat5E: FTP data cable or dedicated multi-mode fibre optic cable.

2. Communication between mimic panels and repeater panels shall be via RS485/232 communication ports and cabling.

3. The RS485/RS422 cabling shall consist of fibre optic and/or 2 conductors, shield, insulated sheath and suitable termination.

15.8 CABLING ROUTES

1. The loop cabling installed in areas where no ceiling exist, shall be installed inside metallic conduit. These conduit and conduit boxes shall be installed by others.

2. Loop cabling installed in ceiling voids, shall run in wire ways as far as possible. Where wire ways do not exist, cabling shall be installed inside metallic conduit connected to the wire ways. Should the run be shorter than 2m, cabling can be run directly on the ceiling boards or tiles to each loop device.

15.9 COMMUNICATIONS TO THE LOCAL FIRE BRIGADE (IF REQUIRED)

1. Alarm communications to the fire brigade is a requirement for this installation. The communication shall be via radio link. The radio link installation shall be as per SANS 10139: 2000.

2. The contractor shall supply all equipment required for the fire brigade communications, including radio transmitter, fire control panel interface and required radio license.

15.10 COMMISSIONING AND HANDING OVERTESTS

1. The testing of the system shall be done in the presence and to the satisfaction of an authorized representative of the department.

2. Tests shall include simulation of fire conditions in each zone to prove the efficiency of all aspects of the system to the satisfaction of the department.

3. All equipment, material, etc., which may be necessary for these tests shall be supplied by the contractor, including a suitable smoke generator.

4. The contractor shall do his own complete commissioning tests before the actual first take-over tests are done. This is to satisfy himself that everything is working and is in accordance with the specification.

16 GAS EXTINGUISHING INSTALLATION SPECIFICATION

16.1 GENERAL

1. This part of the specification covers the design, supply, installation and commissioning of all equipment for the Clean Agent Gas Extinguishing system. The entire installation shall form part of the addressable fire detection system for the facility.

2. The Gas Fire Extinguishing System will be an engineered system utilizing a fixed cylinder with a fixed nozzle for distribution of the gas. The extinguishing system would be installed generally in accordance with the National Fire Protection association Standard 2001.

3. The complete Gas Extinguishing system, as approved by the consultant, shall be installed in the UPS room and include but not limited to the following components:

    a. Addressable Gas Control Units

    b. Addressable fire detectors

    c. Gas Cylinders (mounted against the wall containing sufficient extinguishing agent for the area required)

    d. I/O devices

    e. Fire Blankets

    f. Interface with air conditioning ventilation systems

4. All control, indication and monitor equipment related to the gas protection installation shall be produced by the same manufacturer.

5. The protection system shall be a Clean Agent Inert Gas Extinguishing System.

6. The design and installation of the clean agent fire suppression system shall be strictly in accordance with the following guidelines and regulatory authorities:

    a. BS 6268:1992 - Fire Protection for EDP Installation

    b. BS 5839: Part 1:1988 - Fire Detection and Alarm System for Buildings

    c. SAABS / ISO 14520 2000 Standard on Clean Agent Fire Extinguishing Systems

7. The contractor shall only be permitted to use clean agent fire extinguishing gas (Only Inert Gas in modular cylinders will be acceptable) that are not hazardous to personnel occupying the protected area. Any hazard created by the discharge of the extinguishing agent, the extinguishment itself, the combustion product of the fire and toxic breakdown by-products of the extinguishing gas shall not be accepted.

8. All basic equipment proposed and planned for use must be formally approved by at least two (2) international recognized testing laboratories, such as:

    a. Underwriters laboratories, USA (UL)

    b. Factory Mutual, USA (FM)

    c. Verband der Schass Versekerer, West Germany (VdS)

    d. Association Francais de Normalization, France (AFNOR)

    e. British Standards, Great Britain (BS)

    f. Fire Office Committee, Great Britain (FOC)

    g. Underwriters Laboratories, Canada (ULC)

    h. Loss Prevention Certification Board (LPCB)

9. The control unit and sensors shall comply with the Addressable Fire Detection specification of this document.

10. This installation shall be carried out in strict accordance with the drawings, specifications and applicable standards. The proposed gas protection system used shall have a system approval certificate, which should be submitted at time of tender by the Contractor. This certificate will be for the total system. Component certification shall not be acceptable.

11. The system design shall be performed on software written, verified, approved or tested by an internationally accredited approval body. Proof of software acceptance shall be submitted at time of tender. System design shall be performed by persons who are competent in the field of fire engineering. Proof of his qualifications shall be submitted at time of tender.

12. The contractor shall provide all engineering design and materials for a complete fire suppression system including, storage cylinders, nozzles and all other equipment necessary for an operational system.

13. Working documents as defined in SANS /ISO 14520 part 1, Appendix A shall be submitted for approval within 4 weeks of contract award and prior to delivery of materials to site including information, outlining the operation and maintenance procedures.

14. Design drawings shall indicate locations, installation details and operation details of all equipment associated with the gas extinguishing system. Layout drawings shall be provided showing equipment locations and other details as required. The drawings shall be scale to a scale of 1/50. Elevations, cross sections and other details shall be drawn to scale.

15. The system shall be a based on a total flooding, gaseous clean agent, fire suppression system designed to provide a uniform concentration within the protected areas. The quantity of gas required shall be to obtain a uniform (minimum) concentration for a period of ten (10) minutes. Factors such as leakage under doors unclose able openings and rundown time of air-conditioning plants shall be taken into consideration.

16. A room oxygen concentration of maximum The system design shall be based on the following criteria:

    a. Indoor temperature (anticipated design) 22°C

    b. Altitude above sea level (i.e. Tzaneen) 880m

17. The contractor shall provide all and necessary anchors. The contractor shall also provide and fix in position ready for building-in all cleats, brackets and steelwork required for the anchor points.

18. Warning signs shall be provided and displayed at the entrance doors leading to the protected areas and inside the protected areas.

19. Manual release warning signs shall be provided and displayed next to each extinguishing release unit.

20. Cylinders shall be manufactured from steel with a seamless construction in accordance with BS 56045: Part 1. Each cylinder shell has been pressure tested to a test pressure of 300 bars. Each cylinder shall be fitted with a quick action discharge valve and a removable, dial faced pressure gauge with a range from 0 to 400 bars.

21. Cylinders shall be wall mounted and securely fastened back into a purpose made racking and braced installation. Each cylinder shall be provided with a certificate provided by the company who charged the vessel with the gas mixture.

22. The Engineer shall inspect all components of the gas system in the factory prior to delivery thereof to site. The contractor shall advise the Engineer of the earliest possible date to witness test the complete system as required in ISO 14520 Appendix E. The test shall be performed by a certified individual and a test certificate shall be issued stating the minimum hold time for the room.

23. The contractor shall allow within his tender for a demonstration of the correct operation of all components of the system. The contractor shall arrange for final certification by an independent third party such as SANS. This company shall issue a certificate stating that the system as installed complies with all requirements of ISO 14520 and the specification.

24. On completion of the testing and commissioning the contractor shall issue a certificate that the system is operating correctly and shall leave the system in an operational state.

16.2 SYSTEM OPERATION

16.2.1 General

1. The services fire protection control system shall consist of a separately wired detection zone connected to the fire panel and a gas protection control unit for each area. The status of the doors, gas pressure, ventilation fans, actuating devices and fire dampers shall be monitored on the system for each protected area.

2. The fire control panel shall directly control all electrically operated systems associated with the extinguishing system. The activation of the gas release shall be based on co-incidence detection process whereby at least two detectors in separate zones have been activated by means of the "try twice" feature. All requirements regarding repeating of alarms etc. shall be as specified.

3. The control units shall be fitted at the main entrance door to each gas protected area. Status units shall be fitted at each secondary entrance door to the gas protected area.

4. Warning notices shall be provided on the doors leading into the gas protected area(s) in accordance with the specifications of the supplier.

5. A manual gas release delay switch shall be provided at each gas control unit to allow staff to delay the release of gas for a period dependent on the staff member keeping the delay switch active.

6. Separate manual system isolator switches shall be provided at the fire control panel to isolate the gas protection system for maintenance work to be carried out.

16.2.2 With The Gas Control Unit in the Automatic Mode

1. First knock: (First smoke detector detects a fire)

    a. Activate alarm bells (outside room) - alert tone.

    b. The panel buzzer will sound (continuous tone) until silenced by the "Silence Buzzer" control button.

c. The bells/siren will continue to operate until silenced by enabling the control key switch and pushing the "Silence Sounders" control button.

d. If the bells have been silenced they will become active again for any new fire alarm or if the control key switch is enabled and the "Silence Sounders" control button is pushed.

e. The common fire relay will be activated.

f. If the buzzer has been silenced, the panel buzzer will become active again for any new condition

g. The appropriate zone open collector output will be activated

h. All of the above will become inactive once the fire alarm is cleared and reset is pressed

2. Second knock: (Second smoke detector detects a fire)

a. Activate alarm bells (inside & outside room) - evacuation tone.

b. Activate evacuation signs - flashing mode.

c. Activate pre-release timer adjustable from 20 to 120 seconds set at 45 seconds.

d. Activate evacuation signs steady-on mode

e. Release gas

f. Triggering the shutdown manual call point or pressing the "PREVENT" push button before the discharge delay elapsed shall prevent the discharge output and "Do not enter. Extinguishing triggered" sign output from becoming active

g. A gas area fault shall also prevent the discharge output and "Do not enter. Extinguishing triggered" sign output from becoming active until the fault is cleared.

16.2.3 With The Gas Control Unit in the Manual Mode

1. As per above, no gas release shall take place in this mode.

2. Gas release in this mode shall only be affected by either switching to the automatic mode or by activating the break glass unit on the gas control unit.

16.2.4 Break Glass Unit Activated

1. Activation of the break glass unit located on the gas control unit shall directly start steps 2 to '10 of the extinguishing cycle.

2. Manual release of the extinguishing gas shall always be possible by operation of the break glass unit on the gas control unit, regardless of the mode selected (manual or automatic).

3. All alarms shall be reported to the main fire panel.

16.2.5 INSTRUCTION FOR USE

16.2.5.1 Instructions shall consist of:

1. Notices, certificates, diagram, etc., and all notices as required by the ISO 14520 Code of Practice, Manufacturer and Engineer;

2. Notices, certificates, diagram, etc., and all notices as required by the ISO 14520 Code of Practice, Manufacturer and Engineer;

3. Schematic layout of all systems on which all equipment, control devices and instruments are correctly indicated for that particular plant room. Diagrams shall contain information on set differential bands, throttling ranges, time delays, overload settings and other relevant data necessary for the checking and adjusting of each instrument, control and motor function;

4. Wiring diagrams;

5. Detailed instructions for working of the system / equipment during emergency and normal use,

6. Instructions shall be printed on high quality, non-deteriorating paper framed behind glass;

16.3 FIELD DEVICES

16.3.1 Analogue Addressable Gas Control Unit

1. The gas control unit shall be connected directly to the fire control panel. Each gas control unit shall control a single protected area and field wiring shall consist of two separately addressable loops for secure co-incidence connection of the gas extinguishing system.

2. The fire control panel shall provide the secure co-incidence connection of the gas extinguishing system. The control unit shall be field programmable with cross mapped inputs from various fire detector line devices or zones.

3. The following delay functions such as automatic gas release delay time, selection of delay I no delay time for manual gas release and output relay delay time controls shall be field set- able.

4. The units shall be self-contained units with a key switch for automatic or manual selection as well as a lock out function for maintenance purposes.

5. The following indications shall be displayed on the gas control unit:

    a. Auto — Dual yellow LED

    b. Manual — Dual green LED

    c. Lock out — Dual red LED

    d. Fire — Dual red LED

    e. Fault — Dual yellow LED

    f. Gas discharged — Dual red LED

    g. Power on — Single green

6. The following controls shall be available on the gas control unit:

    a. Automatic / manual

    b. Lock out / reset

    c. Fire sounder silence

    d. Gas release sounder silence

    e. Manual gas release Key switch Key switch Push button Reset key switch Built-in manual call point

7. All lire alarm sounders, gas pre-warning release display/sounder and gas release valve/detonator conditions shall be monitored continuously.

16.3.2 Extinguishant

1. The extinguishant and properties offered by the bidder to be used for this project shall be filled in below:

    a. PROPERTY — REQUIREMENT
    Purity — % by mass, minimum
    Moisture Content per gas mass, maximum)

PROPERTY	UNITS	VALUE
Molecular Mass	-	
Boiling point at 1,013 bar (absolute)	°C	
Freezing point	Ic	
Critical temperature	C	
Critical pressure	bar abs	
Critical volume	cm3/mol	
Critical density	Kg/m'	
Vapour pressure 20°C	bar abs	
Liquid density 20°C	k /m3	

Saturated vapour density 20°C	k	/m3
Specific volume of superheated vapour at 1.013 bar and 20°C	m3/kg	
Design Concentration	%	
Components		
Patented Name (if applicable)		

16.3.3 Materials

1. Only equipment and components specifically designed for the proposed use may be used. To this end, all equipment shall be either listed or approved by approved testing laboratory authority. Proof of such compliance shall be provided for each item, and in the case of the gaseous extinguishing system, the software, each component and the system as a whole.

2. All devices shall be designed for the service they will encounter and shall not readily be rendered inoperative or susceptible to accidental operation. Devices normally shall be designed to function properly from 20°C to + 50°C, or marked to indicate temperature limitations, or in accordance with manufacturers' specifications which shall be marked on the nameplate, or (where there is no name-plate) in the manufacturer's instruction manual.

16.3.4 Solenoid Valves

1. An electrical solenoid operated control head (not detonator type) shall automatically release the gas on receipt of the appropriate fire alarm signal. The control head shall be provided with an override manual control arm, pull-out pin and safety chain.

16.3.5 Cylinder

1. Container shall be designed to hold the specific extinguishant. Containers shall not be charged to a full density greater than specified in that part of ISO 14520 relating to the specific extinguishant.

2. Cylinder shall be designed to suit the working pressure of the gas offered. Design pressure shall be at least 1.5 times the working pressure.

3. Cylinder shall be securely positioned on the wall by means of a rigid bracketing assembly to securely hold the container in position during discharge.

4. Container and valve manifolds shall be tested hydraulically to the highest pressure of that specified by the manufacturer and be substantiated by a relevant test certificate. All cylinders will be supplied with a pressure relief valve as per manufacturer specification.

5. Where required, the container and valve assembly should be fitted with a pressure relief device complying with the appropriate standards.

6. Cylinder shipping shall be in accordance with the design code of the cylinders.

16.3.6 Discharge Pipe/House and Nozzle

1. Nozzles, including nozzles directly attached to containers, shall be as supplied by the certified manufacturer of the equipment, and shall be of adequate strength for use with the expected working pressures, able to resist normal mechanical damage, and constructed to withstand expected temperatures with deformation.

2. The discharge nozzle shall consist of a pre-determined orifice diameter that directly corresponds to the containers assembly selected. This pre-determined orifice ensures that proper agent distribution is achieved which meets the requirements for the system.

3. The discharge nozzle shall be located to achieve the best results and shall be selected and so positioned that the discharge will not splash flammable liquids or create dust clouds that might spread a fire, create an explosion, or otherwise adversely affect the contents of the protected space. Nozzles vary in design and discharge characteristics and shall be selected on the basis of their suitability for the use intended.

4. Pipe work and fittings shall comply with appropriate international standards, shall be non- combustible and able to withstand the expected pressures and temperatures without damage. Where the manufacturer's listing requires more stringent specifications in accordance with equipment's listing these shall be followed.

5. Movement of pipe work caused by temperature fluctuations arising from environment or the discharge of extinguishant may be considerable particularly over long lengths and should be considered in the support fixing methods.

6. All pipes shall be firmly bracketed to walls to the satisfaction of the Engineer. Any piping system shall be securely supported with due allowance for expansion and concentration and shall not be subject to possible damage.

7. Where equipment is to be fixed to concrete or brickwork surfaces, and where building or casting in is not feasible or desirable, fixing shall be by means of approved expansion type anchor bolts. Due care shall be taken to ensure adequate penetration of any expansion bol', to eliminate surface damage. Pipes penetrating walls shall be sleeved.

8. Flexible connection hoses shall consist of flexible, steel reinforced hose, with swaged-on threaded connectors on either end, and shall incorporate a check valve to prevent agent loss in case of a discharge with any cylinder disconnected from the hose for any reason. These

hoses shall have at least the same pressure handling capability as the manifolds.

17 CABLING

17.1.1 General

Supply, install, connect, and terminate all cabling necessary to complete the installation, including all power and UPS distribution, audio, data, control, fibre-optic (where applicable), communications cabling and device cabling.

All cabling shall be supplied and installed as a part of this Sub-contract.

All terminated cabling shall be neatly tied/loomed to prevent damage to terminations and interference or obstruction of other services.

Strain relief shall be provided for cables connected to rack mounted equipment.

All cables shall have stranded copper conductors and shall be PVC insulated with overall PVC sheath, unless otherwise specified.

All cabling shall be concealed and installed on metal cable tray, cable duct and conduits that are supplied under the electrical contract and co-ordination with the electrical contractor for these cables must be ensured.

Cabling shall be installed with due regard to future removal and replacement of cables.

All cables shall be new and delivered on site in unbroken reels, and with the "manufacturer's" label attached.

Due consideration shall be given to voltage drop when calculating cable sizes.

Installation and cable route shall be to the satisfaction of the Engineer.

Cables shall be installed in a manner eliminating any possibility of strain on the cable itself or on cable terminations.

No joints or connections will be permitted. Adequate loose cable shall be left behind all equipment to facilitate removal for inspection, adjustment or replacement.

Coaxial cable for CCTV cameras shall be 75 Ohm impedance with pure copper centre conductor and pure copper braided shield providing minimum 95% braid coverage.

17.1.2 Cable Damage

During the installation of cable should any kinks or abrasions to insulation, braiding, sheathing or armoring occur, the affected cable shall be withdrawn and replaced with new cable.

17.1.3 Cables in Ceiling Space

Cables shall be supported at intervals not exceeding 1000 mm utilizing catenary wires, approved trimmers, roof or ceiling support members.

Cabling in major cable routes shall be installed on cable trays.

A minimum clearance of 400 mm shall be maintained from false ceilings, luminaries, hot water pipes or other heat or electrical noise generating equipment.

Cables shall be neatly grouped together and supported using approved clips or ties.

17.1.4 Cables in Conduits

In addition to the general requirements, cables shall be installed in conduits in such a way to prevent twisting or kinking of cables or damage to cable sheaths.

Communications, data or security cables installed in underground conduits shall be complete with external nylon jacket.

17.1.5 Cables in Ducts

Where cables are installed in ducting, cables shall be grouped and taped for easy identification.

Holes in duct through which cables pass shall be grommetted.

Changes in direction of duct shall be set such that the maximum bending radius of cables enclosed in the duct will not be exceeded.

17.1.6 Cables on Trays

Cables shall be neatly loomed, securely fixed to the tray and installed parallel with the edge of the tray.

Cables shall be arranged on the tray to:

- Avoid unnecessary crossover of cables,
- Spaced to allow adequate ventilation and prevent heating of cables, and separated to provide segregation between independent services.

17.1.7 Cable Numbering

Generally all cables shall be allocated and identified with unique cable number.

All cables including patch leads shall be clearly labeled. Labels shall be affixed within 250 mm of each termination.

Cables shall be fitted with tags at the following points:

- On the cable sheath next to the gland at each end.
- In cable pits.
- At any additional point on the cable sheath (or around the core bunch) where the preceding requirements are not readily traceable from the core terminations.

Cable identification tags shall be orientated uniformly to read left to right from the logical viewing point horizontally; and from bottom to top viewed from the right where installed vertically.

Duplication of cabling and equipment identities shall be avoided.

17.1.8 Co-ordination and Separation of Services

Install services for each respective section and system and physically separate from other systems to a discipline and coordinated layout plan. Adjacent services shall run approximately parallel. Crossing services shall cross at approximate right angles.

Individual services between common points of the work shall follow similar parallel routes. Cables shall be parallel to the building major axes.

Separation distances shall not be less than the following:

- Power cables - 100mm
- ELV and Communication cables to parallel power cables - 300mm
- ELV and Communication cables to power cables crossed at 900 - 100mm
- Any trade to finish floor level - 80mm
- Any trade to structure - 20mm

17.1.9 Co-ordination and Feasibility

The drawings, schematics and specification indicate the main routes and positions for the various services installations and equipment in relation to the building and other services.

Check the details shown on the drawings and co-ordinate the detail layout with the building structure and other services. Submit full details of proposed major cable routes for approval before proceeding.

17.1.10 Special Cabling

Where equipment to be supplied and installed under this specification requires special cabling (i.e. screened cables, unshielded twisted pair, coaxial, optical fibre or other special types of cable), these cables shall be provided as part of this Sub-contract.

It shall remain the responsibility of the Sub-contractor to design the cabling system network and determine the type of cable required for interconnection of the various components, which make up the total system to be installed, to comply with the Sub-contract documents.

17.1.11 Wiring Diagrams

Deliver to the Head Contractor in accordance with the scheduled works programme:

- Details of all types of cabling to be installed as part of the Sub-contract works.

- Block schematic cable diagrams indicating all system interconnecting cables including cable routes and cable types complete with core make up and numbers.

- Detailed floor plans indicating cable routes and designated circuit identification.

- Wiring diagram detailing system interconnections and cable/core identification.

17.1.12 Coaxial Cabling

Coaxial cabling used for the purpose of Closed Circuit Television (CCTV) within buildings or other approved short haul distances shall, as a minimum be RG-59B/U with a solid copper core and 95% copper braid shield. The copper shall have less than 2.0% impurities.

17.2 Fibre Optic Cabling

17.2.1 Backbone

The backbone multi-mode fibre optic cabling and conduit system between buildings shall be installed in a star topology from the Central equipment room to each local control area. The system shall be installed in such a way that a failure of a single cable shall not affect the operation and communications to other local areas from the Central Control Room.

17.2.2 Other Security Services Fibre Optic Requirements

Fibre optic cable shall be supplied and installed in the quantities and location indicated on the drawings for other elements of the security services installation as part of these works.

These requirements are generally to remote CCTV and SMS locations and will generally require conventional tight buffered 80/125 multi-mode fibre-optic cable approved for in-ground installation in sealed in-ground conduit.

17.2.3 General

A fibre-optic cabling network shall be provided for the connection and integration of various services to all nominated buildings. The fibre optic cable for the security services installation forms part of this contract.

The dedicated security services fibre optic cables will be terminated as part of this contract at 19” equipment racks or equipment cabinet installed in the nominated buildings.

Patch fibers to extend the fibre cable from the equipment racks or cabinets at which the cable terminates to the security equipment racks shall be provided in a ST terminal array. Optical fibre fly-leads to connect security services equipment to this point shall be supplied and installed by the security services sub-contractor.

The nominated security services element of the fibre optic cable network shall be utilized solely for the distribution of all security services.

Leave an excess of three meters of fibre neatly coiled up at each termination to provide spare fibre for any re-termination work in the future.

Cables shall be broken out into an approved Fibre Optic Termination Panel (FOTP) as per the cable manufacturer's specifications.

Optical pigtails shall be terminated on the trunk side of the patch panel, using ST Bulkheads.

17.2.4 Fibre Optic Termination Panel (FOTP)

All FOTP shall be 19" rack mountable, or mounted in a suitable enclosure in the equipment racks and equipment enclosures. Security services FOTP in buildings will be supplied and installed as part of this contract.

All FOTP shall provide for fibre optic termination and any through splicing and/or patching facility.

The FOTP's shall be an industry standard type and shall consist of:

- Fibre optic patch panel capable of terminating "ST" style bulkheads.
- Number of terminations as required for cable and core numbers.
- Splice organizer cassettes shall be provided to accommodate all the splices.
- PVC gland entries shall be provided for up to six incoming optical fibre cables.
- An approved strain relief fixing shall be provided for each central strength member.
- Cable strain relief/management provision shall be provided for internal and outgoing optic patch cables.

17.2.5 Optic Fibre Transmitter Receiver

High quality optical fibre transmitters and receivers, International Fibre Systems or Fibre Options manufacture, or Engineer approved equivalent, shall be supplied and installed as part of these works.

Fibre optic transmitters/receivers shall be located within Equipment Racks and equipment cubicles.

Transmit/Receive (Tx/Rx) equipment shall:

- Be 19" rack mountable.
- Have fully enclosed printed circuit boards.
- Use duplex "ST" type fibre optic connectors.
- Use BNC coaxial connectors.
- Use RJ45 connectors for LAN connections.
- Have screw clamped power connections.
- Have “Plug & Play” operations, using modules for rack mounting.
- Data modules shall be user programmable for RS232, RS422 and RS485, as a minimum.
- Have automatically re-settable fuses to module power supplies.
- Battery back-up for power supply modules.
- Have no electronic or optical adjustments.
- Operate over a temperature range of –10°C to +50°C.

- Be fully compatible with the connected equipment (i.e. without any performance degradation).

- Include self-adjusting AGC circuitry.

- Utilize frequency modulation (FM) or 8-bit digital encoding.

Optical fibre transmitters and receivers shall be located within equipment racks, equipment cubicles, camera poles and other nominated locations.

Provide optical fibre transmitters and receivers with an optical fibre budget of 18dB, including a 2.5 dB minimum margin.

Provide non-rack mount modules, as required or directed by the Engineer, for alternative locations (e.g. inside the bases of camera poles).

17.2.6 Technical

The TX/RX equipment shall comply with the following minimum technical requirements:

- Minimum video technical specifications:

- Meet the requirements of the EIA/TIA RS-250C standard for medium-haul transmission.

- 8MHz (-3dB) bandwidth.

- Level unity gain (+/-2%) from 0Hz to 5MHz.

- 65dB Crosstalk (minimum) at 4.43MHz.

- Optical loss budget of 15dB.

- Include AGC circuit, self adjusting. The AGC circuit shall not cause short term video signal synchronization pulse, luminance or chroma crushing when the luminance levels of the video signal changes from 0% to 100% luminance and back to 0% luminance at intervals exceeding 60 seconds.

- The RX/TX unit's technical specifications (e.g. SNR, bandwidth, transmission characteristics, and the like) shall not change with the change in ambient temperature.

- The RX/TX unit's technical specifications (e.g. SNR, bandwidth, transmission characteristics, and the like) shall apply for the previously specified optical loss budget.

- No intermodulation 'noise' shall be measurable on video signals.

- No sub carrier 'noise' shall be measurable on video signals.

- The sub carrier used to transmit audio and/or data shall be a different frequency for each direction of transmission.

- The sub carrier frequencies for each RX/TX unit, at each end of the optical fibre core shall not drift to within 100kHz of each other when the differential ambient temperature variation is at the maximum specified level (i.e. one TX/RX unit is operating at an ambient temperature of –100C and the other TX/RX unit is operating in an ambient temperature of +700C).

17.3 Cable Enclosures

17.3.1 General

All cable enclosures including conduits, cable trays, cable ducts and the like required to facilitate the installation of cabling within the building shall be supplied and installed as part of the **Electrical** Sub-contract.

All cabling shall be installed in cable enclosures, unless protected from mechanical damage by existing building structures.

Cable enclosures shall be installed as follows:

- Within internal ceiling or roof spaces, wall cavities and the like rigid or flexible PVC conduit may be installed.

- On external building walls, walkways and other areas rigid or flexible steel conduit or steel cable duct must be installed. All steel conduit or cable duct must be painted to match the existing adjacent structures.

- All underground conduits shall be heavy duty PVC.

All conduit shall be concealed unless it is unavoidable that the conduits be exposed. No surface mounted conduits are to be installed without consulting the Engineer.

Supply and install all conduits necessary for the installation of cabling for the various systems specified in this document.

17.3.2 Conduits

All conduits shall comply with the minimum requirements of this specification and referenced standards. Unless otherwise specified conduit used throughout the installation shall be light duty rigid PVC.

All conduit and installation shall comply with the following:

- AS 2053 "Non Metallic Conduits and Fittings" or AS2052 "Metallic Conduits and Fittings".

- Oval conduits shall not be installed.

- Minimum size of conduit shall be 20 mm.

- All conduits shall be of an adequate size and have reserve capacity for at least one additional circuit unless the conduit size is specified.

- Power, lighting and extra low voltage systems shall be installed in separate conduits.

- Conduit saddles shall be spaced a maximum of 1200 mm apart.

- Where saddles cannot be fixed to the building structure a suitable bracket shall be supplied and installed.

- Conduits shall be a minimum of 1500 mm clear of gas and hot water pipes.

- Conduits shall not be installed parallel to gas or hot water pipes.

- Conduits installed in cavity walls shall be fixed to the face of the inner leaf and shall not touch the outer leaf.

- All PVC conduit joints shall be made solid and waterproof using an approved PVC welding solution.

- Metallic conduit exposed to the weather shall be galvanized.

- A 2.5 sq. mm. TPI draw wire shall be installed in all conduits whether containing cables or not.

- Underground conduit shall be heavy-duty (HD) underground PVC conduit, unless otherwise specified.

- Flexible conduit shall be steel PVC sheathed conduit.

- Where exposed conduits are unavoidably required, the approval of the Head Contractor shall be required prior to installation commencing.

- Conduits shall be installed far enough above ceilings and below floors to avoid accidental piercing by nails and the like or restricting removal of ceiling tiles or floor panels.

- To the maximum extent possible, conduits shall be installed 150 mm clear of underside of roof decking.

- Half saddles shall not be installed.

17.3.3 Light Duty Rigid PVC Conduits

Install PVC expansion couplings in straight conduit run every 2 lengths when under roofs and every 3 lengths in other locations irrespective of intervening conduit fittings or where conduits pass across structural expansion joints.

Install saddles so that conduits are held firmly in place yet allow for movement due to linear expansion and contraction of the conduits.

Half saddles shall not be installed.

Where conduit passes through a fire wall, sleeve with next size steel conduit extending 300 mm either side of the fire wall. Seal gap at each end of steel conduit with intumescent material.

17.3.4 Steel Conduit

Before installation, clean the threads of conduits and fittings to bright metal by the use of taps and dyes. Internally ream ends of the conduits free of sharp edges and projections.

Paint exposed threads on metal conduits installation with a zinc rich paint.

Where conduits terminate in wall boxes, specifically fabricated metal boxes, switchboards and termination boxes fix them in grip entries welded to the box or by locknuts each side of the box material.

In the case of locknuts, fit a female PVC bush after the inner locknut.

Bends shall be made with tools specifically designed for bending steel pipe, with easy sweeps and shall comply with manufacturer's recommended bending radius and shall be not less than three times the external diameter of the conduit.

Conduit bends, sweeps and installation method shall not cause mechanical stress sufficient to result in deformation. Any conduit which is deemed by the Engineer to have been stressed or steel work deformed shall be replaced.

Make joints in galvanized conduits and water pipe installations watertight by applying thread seal tape or other approved jointing material to threads.

All exposed external conduits shall be galvanized steel.

Use steel screwed conduit fittings with Class B conduit, galvanized where applicable.

17.3.5 Steel Cable Duct

Fabricated from not less than 1.2mm zinc anneal with machine folded return edges for rigidity.

Steel cable ducts shall only be installed in plant rooms, equipment rooms or roof spaces.

Minimum dimensions shall be 50mm x 50mm and cable not to exceed 60% of useable capacity.

Be equipped with clip-on removable covers fixed with screws at each end and having a maximum length of each cover section of 1200mm.

Be complete with matching couplings, tees, elbows, reducers and the like as required.

Be equipped with steel couplings between duct sections, which will maintain mechanical strength and electrical conductivity.

Be fitted with integral partitions throughout its length where it is necessary to accommodate different services within the common ducting envelope.

Be fitted with matching bends sets etc. and other accessories.

Wherever possible mount ducts with the lid uppermost. Allow adequate space above for access to the duct.

Match components one with the other and ensure the fixing system is complete with angle pieces, brackets and the like, as required. Ensure heads of bolts face inside the duct.

Where ducts are mounted with the lid downwards, provide approved fibre cable retainers at maximum 600mm intervals.

Allow for the termination of ducts in the respective items of equipment.

Co-operate with other trades prior to and during the installation of cable trays and ducts to ensure that the system is installed in an efficient manner.

Flat on Walls:

- Single ducts may be fixed direct to the wall surface. For groups of ducts use supports of P3300 galvanized mill strut (at maximum 1500mm vertical centers) fixed horizontally on the wall and spanning the total width of ducts.

Flat on Underside of Concrete Slabs:

- Single ducts may be fixed direct to the slab. Fasten multiple ducts to galvanized P3300 Unistrut spanning total width of ducts.

Down from Slab Over:

- Use supports of Unistrut galvanized P1000 with 10mm galvanized threaded rod hanger s at 1500mm centers.

Suspended off Walls and Above Ceilings:

- Use supports of Unistrut P1000 or galvanized rigid MS cantilever brackets at 1500mm centers.

- Supports shall be securely supported from walls or ceiling support system.

- - At each support bracket fix to the structure and to each duct with at least 2 fixing studs.

17.3.6 Cable Tray

Manufactured from minimum 1.2mm MS sheet.

Fabricated and shaped to provide rigidity, such that when loaded with cables plus 50kg point load at mid span, they do not deflect more than 10mm at any point.

Perforated with slotted holes over the entire tray area suitable for attachment of fittings/fixings using metal thread studs and nuts or nylon tray nuts complete with matching splice plates, tees, transitions and the like, as required and suitably radiused at changes of direction.

Use trays that have a minimum bending radius of 300mm.

In ceiling spaces install horizontal runs of cable to avoid other fittings and services and where possible within the space 150mm above the ceiling surface unless otherwise shown on drawing(s). Allow sufficient space for further removal of ceiling tiles.

In equipment room and roof spaces the position of tray runs shown are approximate only.

Install as directed on site to avoid other fittings and services.

Allow for the termination of trays at the respective items of equipment.

Co-operate with other trades prior to and during the installation of cable trays to ensure that the system is installed in a coordinated manner.

At each support bracket, fix to the structure and to each tray with at least 2 fixing studs.

17.3.7 Heavy Duty PVC Conduits

All underground conduits shall be heavy duty rigid PVC.

Heavy duty conduits are to be size nominated on drawings.

Make joints between conduits and between conduits and accessories solid and waterproof.

Junction boxes and the like in heavy duty conduit systems shall be complete with a neoprene gasket.

Protect conduits exposed to sunlight with an approved painted steel cover.

Install conduits to the manufacturer’s preferred recommended practice.

Conduit fittings such as elbows, bends, tees etc. shall not be installed in underground conduit runs. All changes in direction shall be made using large radius sets in the conduits.

17.3.8 Conduit Fittings

Use junction boxes of adequate size to allow installation of cables without damage to the cabling installation.

Conduit elbows and tees are not permitted in this installation unless specified or shown on drawings.

All conduit fittings with the exception of wall boxes shall be of a material and finish

compatible with the type of conduit system to be installed.

17.3.9 Provision for drawing in of cables

Conduit installations shall be so arranged that:

- Wiring can be readily drawn in or out without damage.
- Removal, damage or alteration to any part of the building structure is avoided.
- No disruption to the conduit installation continuity occurs.
- Draw wires are provided in all conduits.

The removal of access panels, floor traps, ceiling traps/tiles (at draw-in box positions) or electrical fittings, shall not be deemed to be damage to parts of the building structure.

17.3.10 Conduit to be concealed

Conduit shall be installed within walls, wall cavity, secure ceiling space, contained in floor slab, chased into walls to be rendered and otherwise hidden by finished building structures.

Where exposed conduits are unavoidably required, the approval of the Engineer shall be required prior to installation commencing.

17.3.11 Conduit and Conduit Fitting Installation

Unless otherwise specified, draw-in boxes shall be installed in a straight conduit installation at a maximum distance of 12m apart and in such other positions as will facilitate the ready drawing in of cables. Where conduit runs are grouped together in accessible locations, draw-in boxes shall be grouped together at definite and approved positions.

In inaccessible positions, conduit boxes shall not be used to change direction in or branch off from the conduit installation.

Not more than one bend shall be used between any draw-in positions. Where more than one bend is required, the change of direction shall be achieved by setting the conduit in a large radius bend.

Ducts, conduit and conduit fittings including conduit box lids and duct covers shall not be installed or shall be visible on the surface of any floor, wall or ceiling.

All conduits and boxes shall be plugged in an approved manner against the ingress of dirt, moisture or foreign matter. This procedure shall be carried out immediately after installation of the conduit and shall remain in place until the permanent wiring is installed.

Before the permanent wiring is drawn in, conduits shall be dried internally and freed of any foreign matter. Refer at all times to drawings and study the requirements of other services, e.g.

mechanical ventilation ducting, piping and the location of other reticulation equipment and install conduit and ducting clear of same.

Conduit fittings shall be rigidly secured to the conduit. Conduit tees will not be permitted –3 way conduit boxes shall be used instead.

High impact PVC or nylon conduit bushes shall be fitted at all conduit ends.

Conduit installation in all positions shall:

- Be installed in an orderly manner and grouped, and in one plane where practicable.

- Be installed parallel with the major axes of the structure.

- Be securely fastened to rigid supports with approved type clips or saddles. Single sided clips and saddles are not an approved fixing.

17.3.12 Support Structures

Install support structures truly vertical or horizontal and parallel with major axis of the building.

17.3.13 Conduit - Flexible

Flexible conduit shall only be installed between rigid conduit and equipment subject to movement or vibration and across seismic joints.

17.4 Underground conduits

17.4.1 General

In areas adjacent to site common services trench conduit shall be installed in this trench in accordance with Head Contractor requirements and be coordinated with other services.

Generally the installation shall comply with the requirements detailed further in this document.

Where the common services trench is not adjacent then:

- Install conduits a minimum of 400mm below finished ground.
- Install conduits to the manufacturer's preferred recommended practice
- Excavate trenches straight and true and to an adequate depth to provide the required cover for conduits
- Ensure the bottom of trenches are flat and clear of protrusions such as rocks, tree roots and the like, prior to installation of conduits and backfill.
- Provide all shoring sheet piling or support necessary to maintain safe excavation of all trenching.
- Install conduits from buildings with a slight fall to the first junction box or cable pit external to the building.
- Whether containing cables or not, underground conduits shall be provided with a 7/0.67 (2.5 sq.mm) PVC insulated draw wire.
- Make joints between conduits and accessories solid and waterproof.
- Cover conduits with 150mm depth of rubble free sand and place an identification tape, 150mm above the conduit along the entire length of the installation.
- Use orange plastic tape, approximately 150mm wide and indelibly marked 'DANGER ELECTRIC CABLE BELOW' at not more than 1 meter intervals.
- Complete backfilling of trenches clean fill and compact to match surrounding material.
- Lay a bed of clean absorbent sand 100mm deep in the bottom of trench with 200mm cover or clean fill over cables or conduit.
- Backfilling and tamping of trenching where passing under buildings, paths, car parks, and other load bearing areas shall be carried out in layers, 20mm maximum thickness.

- Where conduits pass through pits PVC unsheathed cables shall be continuously enclosed in conduit with a junction box for each conduit run installed within the pit.

17.4.2 Cable Pits

Cable pits shall conform to the following:

- Install cable pits at locations required to facilitate the installation of cabling without causing damage to the cables.
- Provide cable pits with lids.
- Ensure concrete lids are molded with the word "Electric Cables", "Earth Pit" or "Communications Cables" as required.
- Neat fitting holes shall be drilled in fibrous cement pits for conduit/pipe entries and 4 x 50 mm holes shall be drilled in the bottom of the pits for drainage purposes.
- Install all pits level and with the lids flush with finished ground level.
- Minimum size to facilitate cable installation including minimum bonding radius.
- Be minimum size indicated on drawings.
- Pits shall match the manufacture and installation of pits installed by the electrical services sub-contractor.

17.4.3 Dewatering

De-water all excavations required to facilitate the installation of all in ground services and work to the satisfaction of the Engineer. All water removed from excavations shall be effectively discharged from the site. Dewatering shall include water geneted from any source entering the excavations.

17.4.4 Excavation in Rock

The Sub-contractor shall make himself fully aware of all naturally occurring ground conditions including the extent of rock likely to be encountered in the excavations and make all necessary allowances in his tender for excavating in the ground as found. No claims for excavating in hard ground, root or any other adverse conditions will be entertained.

17.4.5 Bituminous Paved Surfaces

Where a trench is to be cut through bituminous or concrete pavement and shoulders the excavation shall be saw cut in straight alignments. The excavated material shall be back-filled in accordance with this specification to

within 150mm of the pavement level and compacted to a density at least equal to the adjoining undisturbed ground and not less than 90% modified AASHO density in the top 200mm backfill.

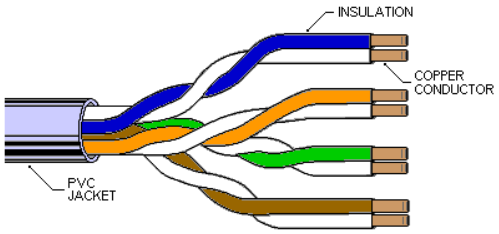
For bituminous pavements a selected base course material of equal or better quality than the existing course shall be placed and compacted to a density of not less than 95% modified AASSHO with the surface finishing flush with the existing shoulder surface and up to 25.4mm below the existing sealed pavement.

The pavement shall be sealed with a tack coat of bitumen emulsion and compacted bituminous pre-mix to finish flush with the existing seal.

17.5 Cable Specifications

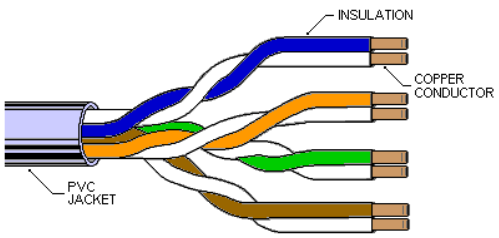
17.5.1 Cable

- Characteristic Impedance: 100 ohms +- 15% from 1 to 155MHz
- ACR: 15 at 100 MHz, 10 at 155 MHz
- Propagation Delay: 5.7 ns/m at 100 MHz, max
- Delay Skew: 48 ns at 100 m, max
- Conductor: 24 AWG solid annealed copper x 4 pair
- Primary Insulation: FEP fluorpolymer resin on each pair
- Jacket: Thermoplastic
- Compliance: ANSI / TIA / EIA 568A Category 5, ISO / IEC 11801 Class D



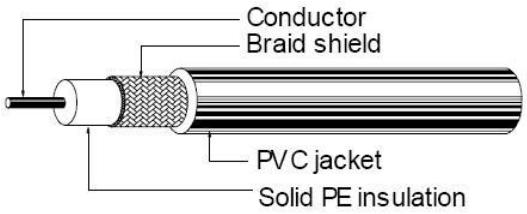
17.5.2 Cable

- Characteristic Impedance: 100 ohms +- 15% from 1 to 155MHz
- ACR: 25.4 at 100 MHz, 17.2 at 155 MHz
- Attenuation Loss: 19.9db/100m at 100 MHz, max
- Propagation Delay: 536 ns/m at 550 MHz, max
- Delay Skew: 30 ns at 100 m, max at 550MHz
- Conductor: 23 AWG solid annealed copper x 4 pair
- Primary Insulation: FEP fluorpolymer resin on each pair
- Jacket: Thermoplastic
- Compliance: ANSI / TIA / EIA 568A Category 5, ISO / IEC 11801



17.5.3 Military Spec Cable

- Conductor: 0.58mm Copper covered steel
- Insulation: 3.70mm Solid PE Insulation (SPE)
- Shield: 0.16mm Bare copper braid shield
- Jacket: 6.2mm Black PVC
- Conductor Resistance: <235Ω/KM at 20ºC
- Insulation Resistance: >500MΩ/KM at 20ºC
- Rated Temperature: 70ºC
- Rated Voltage: 30V
- Braid Coverage: >95.0%
- Capacitance: 67 +- 3pF/M
- Characteristic Impedance: 75Ω +- 3Ω
- Attenuation: 3.61 @ 10MHz, 23.8 @ 400MHz, 39.3 @ 1000MHz



17.5.4 Power Cable 3-Core 1.5mm²

- Number of Cores: 3
- Number of Strands/Core: 30
- Strand Diameter: 0.006mm
- Conductor Diameter: 1.6mm
- Average Insulation Thickness: 0.7mm
- Insulation Diameter: 3mm +- 0.05mm
- Cable Diameter: 6.5mm
- Compliance: N18155, AS/NZS3191
- Protection: Fire Retardant

17.5.5 Optic Duct Cable – 4 Core

- Number of Cores: 4
- Fibre Type: 50/125 Multi-mode
- Bandwidth: 500 MHz
- Attenuation: 2.8 dB/KM

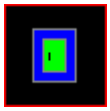
- Refraction: 1.481
- Connector Insertion Loss: 0.75 dB Maximum
- Connector Return Loss: 20 dB Minimum
- Splice Loss: 0.3 dB Maximum

17.5.6 Cable – 5 Core, Screened

- Characteristic Impedance: 2.5Ω per 300m
- Conductor: 14 AWG solid annealed copper
- Primary Insulation: Polyetherlene
- Jacket: Thermoplastic
- Compliance: Belden 8720

18 TECHNICAL SUPPORT DOCUMENTATION

18.1 SMS Workstation Icons

	DOOR SECURE		AUDIO EVESDROP ON
	DOOR UN-SECURE		CAMERA DE-SELECTED
	DOOR FAULT		CAMERA SELECTED
	DOOR INTERLOCKED		PA UN-SELECTED
	DOOR EXCLUDED FROM GROUP		PA SELECTED
	DOOR INCLUDED IN GROUP		PANIC BUTTON NON ACTIVE
	DOOR EMERGENCY RELEASED		PANIC BUTTON ACTIVE
	AUDIO CH ON		PANIC BUTTON ACK
	AUDIO CH OFF		MONITORED DOOR SECURE
	AUDIO CH CALLING		MONITORED DOOR OPEN
	AUDIO CH FAULT		AIR PRESSURE HEALTHY
	AUDIO EVESDROP OFF		AIR PRESSURE LOW

COMPRESSOR HEALTHY

COMPRESSOR FAILURE

UPS HEALTHY

UPS FAILURE

FENCE ZONE DETECTION HEALTHY

FENCE ZONE ALARM ACK

MOTION DETECTION HEALTHY

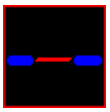
MOTION DETECTION ALARM

MOTION DETECTION ALARM ACK

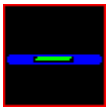
PC WORKSTATION HEALTHY

PC WORKSTATION FAILURE

ROLLER SHUTTER SECURE



ROLLER SHUTTER UN-SECURE



DPS SECURE

DPS UN-SECURE

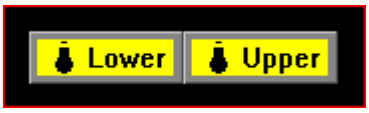
CELL LIGHT OFF

CELL LIGHT ON

DAY ROOM BAY LIGHTS OFF

DAY ROOM BAY LIGHTS ON

LIGHT GROUP NOT SELECTED



LIGHT GROUP SELECTED

GROUP PROGRAM MODE IS NOT SELECTED

GROUP PROGRAM MODE IS SELECTED

DOOR GROUP OPERATE NOT SELECTED

DOOR GROUP OPERATE SELECTED

EMERGENCY GROUP NOT SELECTED

EMERGENCY GROUP SELECTED

VECHICLE LOOP DETECTOR IN-ACTIVE

VECHICLE LOOP DETECTOR ACTIVE