SPECIFICATION FOR THE ELECTRONIC INSTALLATION FOR UMALUSI EXISTING OFFICES ADDITIONS AND ALTERATIONS: SUB CONTRACT

PROJECT SPECIFICATION

INDEX

SECTION THREE
PROJECT SPECIFICATION

1. General Description and Extent of Work

The contract consists of the supply and installation of everything necessary for the satisfactory completion of the access control system, CCTV system, smoke detection system, public address system/evacuation system as detailed in this document, drawings and bill of quantities inclusive of testing, commissioning and twelve month free maintenance and guarantee of the works.

In brief, the extent of the work is as follows.

1.1 A CCTV system for the surveillance of the various internal and external areas.

1.2 An access control system for the control of access to the building.

1.3 Smoke detection and alarm system.

1.4 IT&T system

1.5 Intercom

1.6 Audio Visual System

2. Division of Work

2.1 Principal Building Contractor (Builder)

The builder will provide all penetrations, ceiling cutouts, fire stopping etc.

The builder will be responsible for overall co-ordination and programming of the works.

2.2 Electronics Systems Sub Contractor (Contractor)

The Electronics Systems Sub Contractor is to undertake the complete installation as specified.
The Contractor will be responsible for confirming the correct installation of conduits and power supplies timeously.

2.3 IT Network and Cabling System Sub Contractor

The IT Network Sub Contractor is to undertake the complete installation as specified.

The IT Network Sub Contractor will provide the network for communication purposes.

The IT Network Sub Contractor will be responsible for system integration of all the systems on to the network as well as the software setup for the network management and facilities management systems.

The IT Network Sub Contractor will be responsible for the electronic systems interface co-ordinator’s roll for all the electronic systems implementation.

2.4 Electrical Sub-Contractor

The Electrical Sub Contractor will provide power supplies to the equipment and all wireways except for final connection of equipment and within systems room.

2.5 Gas Suppression Sub Contractor

The gas suppression Sub Contractor will provide alarm inputs at each room with gas suppression in the primary and secondary equipment rooms.

2.6 Mechanical Sub Contractor

The Mechanical Sub Contractor will provide Air Conditioning to the equipment rooms.

3. Contract Drawings

The tender drawings will become the contract drawings and will be revised, amplified and extended as necessary and in accordance with the development of the Architect's design.

The Contractor shall price for monitoring the other services drawings as issued to site, monitoring changes such as locations and swings of doors, windows, wall penetrations, etc. and for locating the terminal outlets and the installation generally to suit, as well as for informing the Engineer.

4. Cost Variations

Upon general revisions of a drawing the relevant cost implications will be calculated, using the rates included in the Bill of Quantities. Where there are no Bills of Quantities rates the calculation will be based on rates generally applicable to the industry which will become the agreed “non scheduled item” rates. Scope of work changes will be calculated using rates included in the Bills of Quantities and the agreed “non scheduled item” rates. The cost of the remeasured work and scope of work changes is to be agreed no a monthly basis. Variation Order No. 1 will be an omit of all contingency and provisional items.

Should the Contractor not agree with the rates of any non scheduled items or with the re-measurement quantities produced by the Engineer, he is required to advise the Engineer accordingly, within 2 (two) weeks of the date shown on the drawings and/or variation order, and to provide substantiation for the pricing revisions he requires, and the relevant costing details.

Where it is imperative that the Contractor takes instructions from persons other than the Engineer, and acts immediately in the interests of the Employer to avoid abortive work or fruitless expenditure, it is mandatory for him to advise the Engineer telephonically of the cost implications, preferably before proceeding with the work but, at latest, within 24 (twenty four) hours of commencing the change.

5. Testing, Setting, Commissioning and Building Tuning

The Contractor shall undertake quality control, setting equipment parameters, pre-testing, testing, pre-commissioning and commissioning on all systems in a systematic manner as individual systems as well as interfaced with other services.

On completion of the project, the Contractor shall submit a typed commissioning report demonstrating that the services were commissioned. The commissioning report shall include comprehensive records (dated and signed) of quality control, pre-testing, testing, pre-commissioning and commissioning on all systems.

The report shall include any requirements for future seasonal testing, a list of any outstanding issues, a list of changes made to the building as a result of the commissioning process, and a list of any recommended changes that should be made in the future.

The commissioning report is to be included in the O&M documentation.

Except where otherwise provided in the contract documents, the Contractor shall provide :

a) A test schedule for each section of the works, system or item of equipment/plant to be tested, giving the time, date and place of the test, detailing the method statements and test procedure, the type and number of tests to be carried out, and the type, make and serial numbers of all test instruments that will be used.

b) All labour, materials, power, fuel, accessories and properly calibrated instruments necessary for carrying out the tests.

c) Health and Safety risk assessments and method statements for the tasks to be completed.

The Contractor shall give sufficient notice, in writing, when any portion of the installation or plant is ready for testing.

In the event of the plant or installation not passing the tests, the Employer shall be at liberty to deduct from the contract price, any reasonable expenses incurred in repeating the tests.

The Contractor shall carry out preliminary tests necessary to satisfy himself that the plant, materials and equipment comply with the provisions of the contract and are in a suitable state to satisfy the requirements of the Specification. The Contractor is required to record these preliminary test results (in a manner to be agreed with the Engineer), and to submit one typed copy to the Engineer for comment, prior to the Engineer attending the acceptance tests.

If the Contractor fails to undertake the testing and commissioning within a reasonable period of time, the Employer may arrange to have the tests performed by another party. All tests so made shall be at the risk and expense of the Contractor.

Building Tuning

All Electrical and Electronic systems shall be tuned as follows.

The Contractor shall monitor on a monthly basis the systems for a period of one year after practical completion as follows.

Verify that the systems are performing to their design potential during all variations in climate and occupancy.

Optimize time schedules to best match occupant needs and system performance.

Align the systems’ operation to the attributes of the built space they serve.

Submit quarterly written reports to the Building Owner indicating the monthly monitoring outcomes to allow corrective action to be taken.

Undertake corrective actions to the system shall be performed as stipulated by recommendations of the Building Owner.

The Contractor shall fully re-commission the systems 12 months after practical completion. Results from the building tuning done in the previous 12 months shall be taken into account during the re-commissioning of the systems. The Contractor shall submit a full written Building Tuning report to the Building Owner on the outcomes of the tuning and re-commissioning process.

Corrective actions to the system shall be performed as stipulated by recommendations of the Building Owner.

6. Approvals

The drawings, documents and specification indicate the type, size and make of equipment, materials and components required.

The Contractor will be required to supply, strictly in accordance with these requirements, unless otherwise approved by the Engineer.

Approval, in all instances, shall be taken as formal approval, in writing, by the Engineer. Verbal approval will not be recognized and the Contractor will be held responsible for any subsequent costs or fruitless expenditure involved.

7. Guarantees

The Contractor shall provide a twelve-month guarantee of all labour, materials and equipment supplied in terms of this contract.

The guarantee period shall commence from the date of practical completion of the whole project in terms of the Principal Building Agreement.

During the guarantee period, the Contractor will maintain and service (to manufacturers' requirements), without charge, all equipment supplied under this contract and, notwithstanding anything to the contrary, shall replace all components that fail, free of charge.

The guarantee is deemed to cover all items of equipment and materials.

When purchasing materials and equipment from suppliers, the Contractor shall obtain formal cessions of all guarantees covering the materials and equipment, from the supplier, in favour of the Employer.

The Contractor will also be responsible for the guarantee of all components and equipment specified by name in the documents or as otherwise approved by the Engineer.

In the event of the Contractor objecting to certain types of equipment, component, manufacturer, or otherwise, this shall be stated at the time of tendering. The Contractor shall also indicate at least two alternatives that are acceptable generally and in terms of the 12 months guarantee requirement.

During the guarantee period, the Contractor will be contacted directly in regard to complaints or failures and shall in turn contact and direct the relevant supplier/manufacturer or his own staff, irrespective of whose ultimate responsibility it shall be to correct the situation.

8. Standards

The latest editions and/or amendments of the following Standards and Codes of Practice are applicable.

The latest editions and/or amendments of the following Standards and Codes of Practice are applicable :

a) The latest edition of the S.A.N.S. 10142 Code of Practice for the Wiring of Premises.

b) The Occupational Health and Safety Act, (Act 85 of 1993) as amended.

c) The application of the SANS 10400: National Building Regulations

d) The South African National Standard (S.A.N.S.) Specifications, as applicable to this contract.

e) I.E.C. Standard Specifications and Codes of Practice, where the S.A.N.S. and B.S.S. equivalents are not available.

f) The British Standard Specifications (B.S.S.) and Codes of Practice, where the S.A.N.S. and I.E.C. equivalents are not available.

g) The Municipal By-Laws and any other special requirements as deemed necessary by the Local Supply Authority;

9. Materials and Equipment

Wherever possible, material and equipment shall be of South African manufacture and of the same make and type throughout the installation.

Where materials and equipment are specified by name, make or type number, alternatives will not be considered, unless it is to the Employer's advantage.

10. Equipment Delivery

The Contractor shall place orders timeously for all materials and equipment. The responsibility for verifying delivery times of items specified rests solely with the Contractor

In this regard, the Contractor's attention is directed to long lead items
.
The Contractor must ensure that equipment is the latest available model and only delivered to site in time for installation as per the programme. Equipment delivered too early will not be paid for.

11. Drawings, Samples, and Operating Manuals

11.1 Installation and Shop Drawings & Samples

Installation and shop drawings are drawings, diagrams, illustrations, Schedules, performance charts and information brochures which are prepared by the Contractor or his suppliers, to illustrate some detailed engineering or installation aspect of the works.

Samples are physical examples, provided by the Contractor or his representative and suppliers, illustrating the intended quality and type of materials, equipment and workmanship, and to establish standards by which the works will be judged.

The relevant sections of the specifications indicate specific installation/shop drawing and sample requirements. The Contractor shall allow for the production of such additional drawings and information as may be necessary, from time to time, to illustrate compliance with the specifications, installations, method/procedure, or engineering aspects.

The Contractor shall inspect all drawings, including structural and other services, installation, shop and design drawings, pertaining to the works, and shall make the necessary allowance in the tender price for the minor extras and omissions which might occur as the result of these final detailed co-ordinated installation and shop drawings.

The Contractor shall review, stamp with his approval and submit with reasonable promptness, and in orderly sequence so as to cause no delay in the work, all drawings and samples required by the contract documents.

At the time of each submission the Contractor shall inform the Engineer, in writing, of any deviation in the installation and shop drawings or samples, from the requirements of the contract documents.

By submitting installation and shop drawings and samples, the Contractor thereby represents that he has determined and verified all field measurements, field construction criteria, materials, catalogue numbers and similar data, and that he has checked and co-ordinated each installation and shop drawing and sample, with the requirements of the works and of the contract documents.

The Engineer will review drawings and samples with reasonable promptness, but only for conformance with the design concept of the project and the contract documents.

The Contractor shall make any corrections required in terms of the Specification, and shall re-submit the required number of corrected copies of drawings or samples. The Contractor shall direct specific attention, in writing, on re- submitted installation and shop drawings, to revisions other than the corrections required by the Engineer on previous submissions.

The Contractor shall submit drawings for review, at least 6 (six) weeks in advance of the required ordering, manufacturing or installation dates.

The reviewing of drawings or samples by the engineer shall not relieve the Contractor of responsibility for any deviation from the requirement of the contract documents including compliance with program, responsibility for errors or omission in the drawings or samples, etc.

11.2 Record Drawings

Record drawings shall be maintained on a current basis as work progresses. Site inspections shall include a review of the record drawings, for the area or equipment inspected.

The Contractor shall be provided with a set of prints to be kept by him on site and dimensioned by the Contractor showing the exact locations of all electrical equipment, cast or built in conduits, sleeves etc.

The positions of all cables, sleeves, conduit, service routes, joints etc. shall be dimensioned on a triangular basis.

Prior to commissioning and handover, the Contractor shall provide a complete set of record drawings, cross-referenced to the Operating and Maintenance Manuals where necessary, and in sufficient detail to enable the employer to carry out proper maintenance, and to facilitate subsequent alterations and additions to the system.

Drawings, Legends, Schedules, Diagrams, intended for framing and wall-mounting, shall be of the fade-free, black ink on a transparency, or photographic type.

11.3 Operation/Maintenance Manuals

The operation and maintenance manuals shall contain all information required to enable the safe and efficient operation and maintenance of all systems associated with the building.

Prior to commissioning, the Contractor shall provide a draft copy of the indexed, loose-leaf manuals, containing complete operating and maintenance instructions for all systems specified under this contract.

Manuals shall be hard covered, at least A4 in size, and must be provided with transparent plastic over-covers and reinforcing ring binders, for each page.

Post commissioning and handover, the Contractor shall provide three copies of indexed, loose-leaf manuals, and electronic copy (CD/DVD) containing complete operating and maintenance instructions for all mechanical and electrical systems specified under this contract.

All manuals must lie flat when open.

Content shall be printed. Photocopies from product brochures will not be accepted. Only information relevant to this contract should be included

The scope of content should include;

System description
Modes of operation including emergency procedures and call out personnel
Equipment schedules
Software schedules and licenses
Parts identification and recommended spares
Guarantee information with work/inspection/maintenance required to ensure guarantees are not nullified
Test Certificates
Commissioning data – Refer to “Typical System Testing & Commissioning Report” and “Typical System Interface Testing Report”
Certificates of compliance
Statutory certification
Manufacturer’s technical literature.
Maintenance instructions and schedules
System training records
Record drawings
Modification information
Fault finding advice
Health and safety documentation
Advice on disposal

11.4 Logbooks

Logbooks shall be provided in each plant room, and must be at least A4 in size, typed and feint-line ruled, to provide the following columns and column headings on each page :

a) Date.

b) Description of Work.

c) Artisan's Signature.

c) Time Spent.

The logbooks shall be provided prior to commissioning and start-up of the plant, are to be kept up-to-date by the Contractor, from date of handover of the plant.

All logbooks must lie flat when open.

12. Training

Prior to handover, the Contractor shall conduct comprehensive training sessions for each installed system to minimum three client representatives to enable proper running and maintenance of the installed systems.

Proposed training times shall be submitted by the Contractor at least two weeks prior to the proposed date, and shall be agreed upon by both parties.

The training shall include, but not be limited to the following:

Systems set-up and configuration;
Modes of Operation of the System;
Systems preventive maintenance and trouble shooting.

Training sessions shall be documented and submitted with the handover documents for reference.

Separate training sessions shall be conducted and documented for each portion of works.

13. Registered Personnel

The Contractor shall have at least one SAQCC registered technician in full time employment assigned permanently to this project.

Proof of these aspects shall be submitted with the completed tender document.

The Contractor shall be registered with the PSIRA.

14. Service Conditions

14.1	Normal Service	: As scheduled.
14.2	Maximum ambient temp.	: +40°C
14.3	Minimum ambient temp.	: -5°C
14.4	Humidity	: Max. 95%
14.5	Atmosphere	: Corrosive

All equipment and materials shall be suitable for the climatic and environmental conditions pertaining to coastal conditions.

Metalwork exposed to sea water, salt water vapour and the weather shall be stainless steel or protected against corrosion to the approval of the engineer.

Contact between dissimilar metals shall be avoided. As a minimum, the following electrode potentials shall not be exceeded.

a) for connections exposed to the weather, salt water vapour or salt water, 0,25V.

b) for connections of interior parts subjected to condensation but not contaminated by salt, 0.50V.

15. Electrical Supply System

15.1 Supply Technical Data

System Voltage	400V ±10%
Rated Frequency	50Hz
Phase rotation	3 phase, RWBR (clockwise)

Design Symmetrical Short Circuit current	5kA at terminal point
Earthing Arrangement	TNS

16. Power Supplies

The Electrical Contractor will provide power supplies as required at 400/230 Volt AC. The location of the power supplies is limited to one point per panel/room/device. The Contractor is responsible for all other power supplies including all DC power supplies.

17. Earthing

The Contractor shall connect to the earthing arrangement provided by the Electrical Contractor.

Any earthing provided by the Contractor shall comply with the following;

The earthing shall be in accordance with SANS 10142. Earth conductors shall be stranded copper with green PVC insulation installed on a radial arrangement with no T-joints or interconnection of circuits.

The earthing arrangement shall be the TNS System.

All cable containment exposed metal work is to be earthed and earths are to be continuous for the length of the run and include all bends.

All circuits are to be provided with a separate earth wire as specified or as per SANS 10142 as a minimum requirement.

Common earth conductors may not be used where various circuits are installed in the same wiring channel.

18. Bonding

The Contractor shall cross bond all metallic panels etc.to bonding points provided by the electrical contractor.

19. Lightning Protection

The Contractor shall ensure that the incoming services are connected to the lightning protection system provided by the Electrical Contractor to ensure protection of equipment and personnel.

20. Surge Protection

a) Protection against lightning: Class 1 – 25 kA, (10/350 µS) impulse current waveform protection device on all phases and neutral at the power supplies source to equipment at 400/230 Volts. Connection to be suitable for TNS earthing systems.

b) Protection against surges: Class 2 – 20 kA (8/20 µS) surge current waveform protection device on all phases and neutral power supplies to equipment at 400/230 Volts in local DB. Connection to be suitable for TNS earth systems.

c) Protection against surges: Class 3 – 5 kA (8/20 µS), surge current wave and (1.2/50 µS) voltage waveform and Voltage peak of 1.5 kV on all phases and neutral power supplies to equipment at 400/230 Volt within 10 metres of equipment.

d) Internal Equipment Protection: Surge protection to electronics equipment shall be provided as required by the equipment manufacturer to be suitable for co-ordination and cascading with the above protection.

It is the responsibility of the contractor to ensure the correct surge protection Class 1 and Class 2 is provided as part of the electrical installation. If it is not provided, the Engineer is to be notified accordingly.

21. IT Network & Cabling

21.1 System Description

The IT network is made up of two networks viz Network A for commercial type services and Network B for Security and Technical services. Networks A and B are interconnected via dual firewall between primary core switches. Networks A and B access network equipment is housed in the same equipment rooms with a mechanical separation.

Network A comprises of core switches and servers interconnected with multiple 10 Gig links located in the Server Room connecting via multiple 10 Gig links to distribution switches on each floor and dual 10 Gig links (single mode fibre) which are connected to edge/access switches located in each ward IT room.

The edge/access switches (POE) are connected to the terminal devices via 1 Gig links with Cat 6a (Cu10) cabling.

The disaster recovery room is a duplication of the critical server room equipment connected via a multiples of 10 Gig links.

Network B comprises of core switches and servers interconnected with multiple 10 Gig links, located in the Server Room, connected to edge/network switches via dual 10 Gig links in each ward.

The edge/access switches are connected to the terminal devices via 1 Gig link with Cat 6 cabling.

The disaster recovery room is a duplication of the critical server room equipment connected via a multiple of 10 Gig links.

Note: Network A

This specification is to be read in conjunction with Department of Health (DOH) ICT Infrastructure Specification. The DOH ICT Infrastructure Specification takes precedence for Network A only.

21.2 Standards

All services and installations shall comply with the latest revisions and amendments of the following listed standards and specifications.

a) International open protocol standard (IEEE)

b) ICASA regulations and rulings

c) ISO/IEC 11801:2002 Ed. 2 - Generic cabling for ITC premises

d) ANSI B 286-74 (R-1985) Copper Conductors for Use in Hookup Wire for Electronic Equipment

d) The applicable SANS / SABS Specifications and Codes of Practice, or the ISO Specification where no SANS Specification exist.

e) SANS 1019/SABS 1019:2001 – Standard voltages, currents and insulation levels for electricity supply

f) ISO/IEC 11801 Information technology – Cabling systems for customer premises

g) ISO/IEC 14763-1 Information technology – Implementation and operation of customer premises Cabling – Part 1: Administration

h) ISO/IEC 14763-2 – Part 2: Planning and installation

i) IEC 60038 IEC standard voltages

j) IEC 60068-1 Environmental Testing – Part 1: General and Guidance

k) IEC 60068-2 Environmental Testing – Part 2: Tests

l) IEC 60332-1 Tests on electric cables under fire conditions – Part 1: Test on a single vertical insulated wire or cable

m) IEC 60332-2 Tests on electric cables under fire conditions – Part 2: Test for vertical flame spread of vertically-mounted bunched wires or cables

n) IEC 60529 Degree of protection provided by enclosure (IP Code)

o) IEC 60793 series Optical fibres

p) IEC 60794 series Optical fibre cables

q) IEC 60874-1 Connectors for optical fibres and cables – Part 1: Generic specification

r) IEC 60874-10 – Part 10: Sectional specification for fibre optic connector – Type BFOC/2,5

s) IEC 60874-14 – Part 14: Sectional specification for fibre optic connector – Type SC

t) IEC 60874-19 – Part 19: Sectional specification for fibre optic connector – Type SCD(duplex)

u) IEC 61156-1 Multicore and symmetrical pair/quad cables for digital communications Part 1: Generic specification

v) IEC 61156-2 Part 2: Horizontal floor wiring, Sectional specification

w) IEC 61156-3 Part 3: Work area wiring, Sectional specification

x) IEC 61300-2 Fibre optic interconnecting devices and passive components – Basic test and measurement procedures Part 2: Tests

y) IEC 61753-1-1 Fibre optic interconnecting devices and passive components performance standard – Part 1-1: General and guidance – Interconnecting devices (connectors)

z) IEC 61984 Connectors – Safety requirements and tests

Where conflict appears to exist between any of the regulations and standards listed above and this specification, the Contractor shall inform the Engineer in writing.

21.3 System Operation

21.3.1 General Information

The network shall provide the following throughput and quality.

The ITU-T Recommendation G.1010 will be used to measure the required Quality of Service (QoS), and the IETF RFC 2544 Standard will be used to verify the performance of the network.

By considering a range of applications involving the multimedia content categories such as voice, video, image and text, and the parameters that govern end-user satisfaction for these applications, a broad classification of end-user QoS categories is detailed by ITU-T Recommendation G.1010.

21.3.2 Technology Framework

The following technologies are the minimum requirements.

LAN Strategy	The LAN will be based on an Ethernet infrastructure.
WAN Strategy	WAN Services for internet and Department of Health application access will be provided by SITA/DOH VPW
Network Protocols	Support for multi-protocol routing - IP
Routing Protocols	OSPF shall be deployed in routers and switches
Quality of Service	Support for 802.1q VLANs or frame prioritisation required
Addressing and Domains	IP addresses are allocated dynamically via DHCP. DNS or WINS will be deployed to provide name-to-address translation
LAN Switching	A switched-media LAN be deployed
Remote Network Access	Configured as need to allow remote support of various application. Adequate security shall be provided
Availability and resiliency	Redundant networking and load sharing shall be provided, with redundant links to critical servers
Network management platforms	Support for a SNMP-based system, hosted on the network manager's workstation.
Network Security	SITA will provide internet firewall security. LAN based networks A&B to be repeated by dual firewalls and in blade IPS solutions.
Wireless networking	Support for a IEEE 802.11 wireless networking
Network cabling	Support for a structured cabling system, based on the ANSI/EIA/TIA 568-B.1, B.2 and B.3 standard, using copper CAT6 links, and SM fibre backbone links
PoE	802.3af Class 3 (15 W)

21.3.3 Network Performance

The network performance will be in accordance with the Internet Engineering Task Force (IETF) which has a test methodology performance verification at the Layer 2 and 3 levels. RFC 2544 - Benchmarking Methodology for Network-Interconnect Devices specifies the requirements and procedures for testing throughput (performance availability), latency (transmission delay), back-to-back frames (link burstability), and frame loss (service integrity).

Typical RFC 2544 tests, and test suites, shall be: throughput, latency, burstability, and frame loss. User-definable parameters common to all tests include frame content, frame size, layer 2 802.1p class of service priority, layer 3 IP type of service (TOS), test duration and test rate shall be selected to suite the application and service.

Tests shall be configured to test the same link multiple times with varying configurations to observe performance differences. Test multiple links from a single destination shall require using multiple EtherScope (or equivalent) remotes.

Inter-VLAN traffic must be routed. The network design needs to account for this traffic and allocate enough bandwidth to move inter-VLAN traffic from the source, through the router, to the destination. The amount of bandwidth used between switches needs to be monitored to ensure there is adequate trunk bandwidth between switches.

21.3.4 Network Equipment

The active network components shall be capable of handling the average load and peak loads. These loads will be inferred form the required services to be provided to each port.

Quick response times are required by automation controls. The relevant VLANs shall be kept free from any unnecessary traffic and dimensioned with at least a factor of ten of bandwidth reserve.

Typical response times needed are for:

- video broadcast streams: 50 ms
- video conferencing streams: 20 ms
- voice streams: 20 ms
- process control: 10 ms

21.3.5 Switch Topology

Network Topology shall be a collapsed core and distribution model using Layer 3 Distribution with Layer 3 Access.

The switches shall be configured to improve failure detection and the updating of forwarding tables so as to speed convergence.

The Access Layer, the Distribution Layer, and core layers must be configured as virtual fabrics, i.e. each layer must act as a single network switch with load sharing and Layer 3 routing/sharing (active/active).

21.3.6 Encrypted Traffic

Mission Critical network traffic shall be protected by encrypting the data transmitted.
One or more of the following methods shall be used :

IP filtering
Virtual private network
HTTPS
802.1X

IP filtering will be configure to forward select IP datagrams according to Datagram source address and Datagram destination address allowing bi-directional flow. For example, network cameras will be configured to accept commands only from the IP address of the server hosting the video management software.

VPN - virtual private network : VPN shall use IPSec (either the Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES)) to provide a secure tunnel in the network, and between networks.

HTTPS - Hyper Text Transfer Protocol Secure : Hyper Text Transfer Protocol Secure (HTTPS shall use using Secure Socket Layer (SSL) or Transport Layer Security (TLS). The system shall issue its own certificates to be used internally for closed user groups. The systems performance (frame rate) shall not be compromised by the use of HTTPS.

802.1X - Port Based Network Access Control : IEEE 802.1X shall be used to provide authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. The systems shall be provided with a RADIUS server based on an open source operating system.

21.3.7 Access Level Switches

The switch shall have performance evaluations by The Tolly Group and Miercom showing power consumption. Should these not be available, other similar performance evaluations by reputable organisations may be accepted by the Consulting Engineer.

Switches are required that offer layer 3 capability, including VLAN, OSPF routing and multicast routing protocol.

The switch shall have auto-sensing 10/100/1000 full duplex ports and support IEEE 802.3 x full duplex flow control standard.

The switch shall support the IEEE 802.3x full duplex flow-control standard

The switch shall have a non-blocking switching fabric capable of supporting wire speed layer 2 switching across all the ports, and shall allow for wire speed stacking.

The switch shall have at least 2 queues per port (CoS). QoS based on IEEE 802.1 p/Q.

Every switch stack shall have at least two uplinks which shall be 10 Gigabit with SFP + connectors as per TEA / EIA specification.

Link aggregation using lACP for automatic load balancing and high availability.

Routing shall provide for millisecond convergence.

Provided PoE - IEEE 802.3af Class 2 (15.4 W)

A stackable switch is acceptable

The switches shall allow for at least SNMPv3 management, with RMON Group 2 a preferred option

The switch must offer the option of redundant power supplies.

The access layer switches in a stack must be configured as virtual fabrics i.e. each layer must act as a single network switch with load sharing and Layer 3 routing (active/active).

21.3.8 Distribution Level Switches

The switch shall have performance evaluations by The Tolly Group and Miercom reports showing power consumption. Should these not be available, other similar performance evaluations by reputable organisations may be accepted by the Consulting Engineer.

Switches are required that offer layer 3 capability, including VLAN, OSPF routing and multicast routing protocol.

The switch shall have auto-sensing 1000/10000 full duplex ports

The switch shall support the IEEE 802.3x full duplex flow-control standard

The switch shall have a non-blocking switching fabric capable of supporting wire speed layer 2 switching across all the ports, and shall allow for wire speed stacking.

The switch shall have at least 2 queues per port (CoS) QoS based on IEEE 802.1 p/Q.

Every Distribution switch stack (2 switches) shall have at least four uplinks which shall be 10Gigabit, with SFP+ connectors as per TIA/EIA specifications.

Link aggregation using LACP for automatic load balancing and high availability.

Routing shall provide for millisecond convergence.

Stackable access switch is acceptable

The switches shall allow for at least SNMPv3 management, with RMON Group 2 a preferred option

The switch must offer the option of redundant power system.

The Distribution layer switches in a stack must be configured as virtual fabric's, i.e. each layer must act as a single network switch with load sharing and Layer 3 routing sharing (active/active).

21.3.9 Server Farm Level Switches

The switch shall have performance evaluations by The Tolly Group and Miercom reports showing power consumption. Should these not be available, other similar performance evaluations by reputable organisations may be accepted by the Consulting Engineer.

Switches are required that offer layer 3 capability, including VLAN, OSPF routing and multicast routing protocol.

The switch shall have auto-sensing fixed 1000/10000 SFP+ ports full duplex

The switch shall support the IEEE 802.3x full duplex flow-control standard

The switch shall have a non-blocking switching fabric capable of supporting wire speed layer 2 switching across all the ports, and shall allow for wire speed stacking.

The switch shall have at least 2 queues per port (CoS) QoS based on IEEE 802.1 p/Q.

Every Server Farm switch stack (2 switches) shall have at least four uplinks which shall be 10Gigabit , with SFP+ connectors as per TIA/EIA specifications.

Link aggregation using LACP for automatic load balancing and high availability.

Routing shall provide for millisecond convergence.

Stackable access switch is acceptable.

The switches shall allow for at least SNMPv3 management, with RMON Group 2 a preferred option

The switch must offer the option of redundant power system.

The Server Farm layer switches in a stack must be configured as virtual fabric's, i.e. each layer must act as a single network switch with load sharing and Layer 3 routing sharing (active/active).

21.3.10 Core / Switches

The switch shall supply have performance evaluations by The Tolly Group Group and Miercom reports showing power consumption. Should these not be available, other similar performance evaluations by reputable organisations may be accepted by the Consulting Engineer.

Switches are required that offer layer 3 capability, including inter-VLAN routing and multicast routing protocol.

Switches are required that offer layer 2 capability for non-routable protocols such as NetBIOS.

The switch shall have full-duplex 1000 BASE-LT/TX and Gigabit SFP+ ports as per schedule

The switch shall support the IEEE 802.3x full duplex flow-control standard

The switch shall have dual non-blocking switching fabrics (each switch fabric 768Gbps) capable of supporting wire speed layer 3 switching across all the ports. Backplane speed of 2.4 Tbps must support 1152 Gbps switching capacity, with dual fabrics, the core switch must deliver up to 714 Mpps throughput.

The switch shall have at least 4 queues per port (CoS) QoS based on IEEE 802.1 p/Q.

The Distribution layer switches in a stack must be configured as virtual fabric’s, i.e. each layer must act as a single network switch with load sharing and Layer 3 routing sharing (active/active).

The following in Chassis modules must be supported:

- IPS Blade
- Firewall Blade
- Wireless controller Blade

Link aggregation as per IEEE 802.1 ad or vendor specific scheme Millisecond STP convergence

A chassis-based switch is acceptable

The switches shall allow for at least SNMPv2 management, with RMON Group 1 a preferred option

The switch shall have redundant power supplies.

21.3.11 Router / Firewall

Each Wide Area Network Router must support dual LAN 1000Mbits/sec links, and be compatible with the current SITA/DOH VPN Network.

21.3.12 Management

The network shall accommodate managed and unmanaged devices.

SNMP shall be the standard method of managing devices across an internet, whether a LAN, a WAN or the Internet itself.

A SNMP-based Network Management System shall be provided. The NMS shall provide the network administrator with a graphical view of the network, together with graphical views of the individual devices, colour coded according to their operational status. The main processing of network information shall be done by NMS which will collect data from the Agents and present this information in a format specified by the network administrator. The solution must cohesively integrate fault management element configuration and network monitoring from a central vantage point with support for 3rd party devices. The NMS must be capable of management and monitoring of both virtual and physical network.

The NMS shall allow for RMON-enabled device that can either send statistics and alarms to an NMS on demand, or generate a Trap if a threshold is exceeded.

The RMON alarm and event shall be used to monitor a certain MIB object on the device, and warn the system administrator if one of those values is going out of the defined range.
The alarm shall monitor a specific object in the MIB and trigger an event when the condition (failing or rising threshold) is reached. The event is the trap or log generated when the alarm triggers it.

The NMS must be capable of the following additional functions:

- Access control list management.
- Identification and access management.
- Endpoint Admission Defense (EAD).
- Centralized reporting
- Compliance Management
- Virtual Connect support
- Mobile application: Software must include a mobile application for the iPhone and Android
- Telnet/SSH proxy
- Unified Task Management and Wizard Center
- Traffic topology
- Customized functions and third-party device

An interface or software tool shall be provided to integrate the information provided in the MIB in SNMP format into the OPC format.

21.4 WLAN Network Equipment

21.4.1 Active Components

Equipment comprising the Wireless LAN system shall consist of IEEE 802.11a/b/g multimode Access Points, radios, antennas, associated equipment, cables, and administration software, of which all must be compliant with applicable standards.

All Access Points must be capable of supporting a variety of ICASA-compliant, external omni-directional, and directional antennas.

All Access Points must meet or exceed the requirements described below and in the remainder of this specification:

21.4.2 802.11 Wireless Standards

Access Points and their integral components shall be compliant with the IEEE 802.11n standards for wireless LAN networking.
Access Points and client adapters shall be certified by the Wi-Fi Alliance organization to ensure multi-vendor interoperability.

21.4.3 Interoperability

Each access point must operate in accordance with the applicable IEEE 802.11a/b/g/n standards when interoperating with a different manufacturer’s access point.

Each access point must operate in accordance with the applicable IEEE 802.11a/b/g/n standards when interoperating with a different manufacturer’s wireless client adapter.

21.4.4 Network Connectivity

At a minimum, the Access Point shall provide a Gigabit Ethernet uplink port for connectivity to the wired network infrastructure, with data rates up to 300 Mbps when using the 802.11n standard

The Access Point shall support connecting wireless client stations over IEEE 802.11a/b/g/n networks independently or simultaneously.

The Access Point shall support IEEE 802.11e Wi-Fi Multimedia (WMM) wireless QoS standard.

21.4.5 Operational Modes

The wireless Access Point shall be IEEE 802.11h International Telecommunication Union (ITU) compliant. Dynamic Frequency Selection (DFS) to automatically select another channel and adjust transmit power to reduce interference with systems such as radar, if detected on that same channel.

The wireless Access Point shall support Auto Channel Select (ACS).

The wireless Access Point shall be based on Multiple-Input Multiple-Output (MIMO) — advanced Multiple Input Multiple Output (MIMO) technology.

21.4.6 Security

The Access Point and associated wireless client adapters shall be compliant with the IEEE 802.11a/b/g/n authentication methods and other authentication methods identified in this specification

The Access Point shall support WPA2 standards-based security—with Wi-Fi Protected Access 2 (WPA2), Advanced Encryption Standard (AES) encryption, Temporal Key Integrity Protocol (TKIP), and Wired Equivalency Protocol (WEP) for legacy clients.

The Access Point shall support location AP-based user access control.

The Access Point shall support integrated wired and wireless Endpoint Admission Defense (EAD).

The Access Point shall be IEEE 802.11h ITU compliant with Dynamic Frequency Selection (DFS) to automatically select another channel and adjust transmit power to reduce interference.

21.4.7 Encryption and Privacy

The Access Point shall provide support for static and dynamic IEEE 802.11i keys. .WPA-PSK and WEP encryption must support 128 bit key length.

VPN pass-through support - The Access Point shall allow VPN tunnels to be formed between 802.11 wireless clients and a LAN-attached VPN server.

The Access Point shall provide a capability for secured local and remote configuration management (e.g., authenticated local user console access and either remote HTTPS SSH, or secure Telnet).

The Access Point shall provide a capability for secured local and remote firmware upgrades.

The Access Point shall allow for enabling/disabling SSID broadcasts, power-save mode, system logging; automatic and manual selection of transfer rates; selecting client authentication modes, beacon intervals, DTIM intervals, RTS thresholds, and fragmentation thresholds.

21.4.8 Status and Monitoring

The Access Point shall provide diagnostic capabilities for the wireless link's connectivity status and throughput performance.

The Access Point shall provide the capability to examine radio configuration information including operating channel, transmit power, supported data rates, and regulatory settings from a remote location (via secure connection). This capability shall allow the administrator, from the central management station, to identify clients associated with the access point, run link tests, and determine signal strength and quality.

21.4.9 Wlan Controller

The Access Point shall have the ability to be securely managed from a central management console location via SNMP (v3), HTTPS, or SSH. At a minimum, a WLAN administrator should be able to perform the following activities from the central management console:

- Automatic radio power adjustment — automatic AP power adjustment features analyze user access status in real time, adapting power requirements based on environmental changes and providing high-quality user access signal coverage
- Automatic radio channel adjustment — intelligent channel switching and real-time interference detection provide the allocation of a high-quality channel to each AP, reducing adjacent channel interference
- Load balancing — intelligent load sharing analyzes the locations of wireless clients in real time, providing high-quality client throughput regardless of location or number of online sessions
- Rogue AP detection — regular scans for rogue APs help confirm that the network is secure
- Secure controller management — securely manages the controller from a single location with IMC or any other SNMP management station; controller supports SNMPv3 as well as SSH and SSL for secure CLI and Web management
- AAA server — uses an embedded authentication server or external AAA server for local users

End-to-end QoS — the WLAN controller must support not only the DiffServ standard but also the IPv6 QoS; the QoS DiffServ model includes traffic classification and traffic policing, implementing the six groups of services (EF, AF1 through AF4, and BE).

IEEE 802.1p prioritization — delivers data to devices based on the priority and type of traffic

Class of Service (CoS) — sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ

21.4.10 Site Survey Report

Prior to the WLAN installation, a WLAN Site Survey Report shall be submitted to the Electrical Engineer for review.

Prior to the WLAN installation, a WLAN Site Survey Report shall be submitted to the Electrical Engineer for review. The RF Planning tool must be able to import Building floor plan inputs — TIF, JPEG, and BMP AutoCAD files (DWG and DXF) which can be converted into these formats as well as input At a minimum, the report shall include the following information:

WLAN system configuration.

Coverage and interference areas for Access Points (including signal strengths, antenna types and locations for survey, AP model used for survey, types and strength of interference identified)

Access Point name and location

Configuration mode and detail

Antenna types to be used per Access Point

Mounting instructions for Access Points and antennas

Access Point and wireless client channel selections

Power output settings per Access Point

Connectors and cables to be used

21.4.11 Bandwidth Management

The Access Point shall provide a bandwidth management functionality (bandwidth allocation per SSID) to optimize wireless LAN bandwidth for client associations, resulting in a better network performance through load distribution.

21.4.12 Features

Hot Standby – This functionality must be built into the wireless access point controller.

QoS over Wireless - The Access Point shall provide support for 802.11e (QoS) standard (or available via firmware upgrade at no additional cost) for traffic prioritization services over the wireless link.

21.4.13 Roaming Support

The Access Point shall provide support Layer 3 roaming and fast roaming.

21.5 Structured Cabling System

21.5.1 Standards

The following codes are applicable,

ANSI/NECA/BICSI-568	Standard for Installing Commercial Building Communications Cabling
ISO 11081	International Standard for generic cabling for customer premises

ANSI/TIA/EIA Standards as listed below	
ANSI/TIA/EIA-568-B.1	Commercial Building Communications Cabling Standard, Part 1: General Requirements
ANSI/TIA/EIA-568-B.2	Commercial Building Communications Cabling Standard, Part 2: Balanced Twisted Pair Cabling Components
ANSI/TIA/EIA-568-B.3	Optical Fibre Cabling Components Standard
ANSI/TIA/EIA-569-A	Commercial Building Standard for Communications Pathways and Spaces
ANSI/TIA/EIA-606(A)	The Administration Standard for the Communications Infrastructure of Commercial Buildings
ANSI/TIA/EIA-607(A)	Commercial Building Grounding and Bonding Requirements for Communications
ANSI/TIA/EIA-526-7	Measurement of Optical Power Loss of Installed Single-Mode Fibre Cable Plant
ANSI/TIA/EIA-526-14A	Measurement of Optical Power Loss of Installed Multimode Fibre Cable Plant
ANSI/TIA/EIA-758(A)	Customer-Owned Outside Plant Communications Cabling Standard

Install cabling in accordance with the most recent edition of BICSI® publications:

BICSI	Communications Distribution Methods Manual
BICSI	Cabling Installation Manual
BICSI	LAN Design Manual
BICSI	Customer-Owned Outside Plant Design Manual

ICASA codes, rules, regulations, and ordinances governing the work, are as fully part of the specifications as if herein repeated or hereto attached.

If the Contractor should note items in the drawings or the specifications, construction of which would be code violations, promptly call them to the attention of the Engineer in writing. Where the requirements of other sections of the specifications are more stringent than applicable codes, rules, regulations, and ordinances, the specifications shall apply.

21.5.2 Certificates of Approval

The Contractor shall supply to the Engineer certificates of inspection from the manufacturer acceptable to the Engineer and approved by the ICASA and utility companies serving the project.

21.5.3 System Description

One work area or wall outlet may consist of one or two Cat6a (Cu10) with four-pair data cable/s, installed from work area outlet to the edge switch. Terminate data cables on wall / rack mounted modular patch panels located in the appropriate edge switch.

Vertical/horizontal copper backbone cabling consists of multiple pair unshielded twisted-pair installed from the main cross-connect (MC) to the horizontal cross-connect (HC) and/or from the MC to the intermediate cross-connect (IC) to the HC.

Vertical/horizontal backbone cabling consists of 62.5/125 μm singlemode optical fibre cable installed between core, distribution and access switches.

21.5.4 Suitability

Provide products that are suitable for intended use, including, but not limited to environmental, regulatory, and electrical.

21.5.5 Communications Backbone Cable

Single 62.5/125 μm diameter tight-buffered optical fibre, with fibre counts as indicated elsewhrere with mechanical and transmission performance specifications that meet or exceed ANSI/TIA/EIA-568-B.3

Multimode 50/125 μm diameter tight-buffered optical fibre, with fibre counts as indicated elsewhere, with mechanical and transmission performance specifications that meet or exceed ANSI/TIA/EIA-568-B.3

21.5.6 Voice Communications Station Cable

Solid copper, 0.5 mm², 100 Ω balanced twisted-pair (UTP) Category 3 cables with four individually twisted-pairs, which meet or exceed the mechanical and transmission performance specifications in ANSI/TIA/EIA-568-B.2 up to 16 MHz.

Solid copper, 0.5 mm², 100 Ω balanced twisted-pair (UTP) Category 6 cables with four individually twisted-pairs, which meet or exceed the mechanical and transmission performance specifications in ANSI/TIA/EIA-568-B.2 up to 250 MHz.

21.5.7 Workstation Cable (Copper)

Multi-strand copper, 0.5 mm², 100 Ω balanced twisted-pair (UTP) Category 6 cables with four individually twisted-pairs, which meet or exceed the mechanical and transmission performance specifications in ANSI/TIA/EIA-568-B.2 up to 250 MHz.

21.5.8 Underground Communications Cable (Copper)

Solid copper, 24 AWG 100 Ω balanced twisted-pair, gel-filled duct cable, in sizes as indicated elsewhere, which meet or exceed the mechanical and transmission performance specifications listed in ANSI/TIA/EIA-568-B.2 and ANSI/TIA/EIA-758(A).

21.5.9 Underground Communications Cable (Optical Fibre)

Singlemode 62.5/125 μm diameter, armoured, gel-filled optical fibre, with number of usable fibres as shown elsewhere, which meet or exceed the mechanical and transmission performance specifications listed in ANSI/TIA/EIA-568-B.3 and ANSI/TIA/EIA-758(A).

Multimode 50/125 μm diameter, armoured, gel-filled optical fibre, with number of usable fibres as shown elsewhere, which meet or exceed the mechanical and transmission performance specifications listed in ANSI/TIA/EIA-568-B.3 and ANSI/TIA/EIA-758(A).

21.5.10 Copper Area Outlets

Single-gang mounting plate with four (4) openings containing the following devices:

a) Voice Outlet - 8-pin modular, category 6, unkeyed, ivory, pinned to T568 (A) standards.
b) Data Outlet - 8-pin modular, category 6, unkeyed, black, pinned to T568 (A) standards.

21.5.11 Wall Voice Outlets

Where specified, single-gang stainless steel faceplate with six-conductor jack and wall telephone mounting lugs

21.5.12 Data Only Work Area Outlet

Single-gang faceplate with 8-pin modular, category 6, unkeyed, black data jack, pinned to T568 (A) standards.

21.5.13 Patch Panels

19 in. rack mountable, 24-port 8-pin modular to insulation displacement connector (IDC) meeting Category 5e performance standards, and pinned to T568 (A) standards.

21.5.14 Wall Mounted Optical Fibre Patch Panels

Wall-mounted optical fibre termination panel with 12-fiber capacity, hinged door, cable strain relief, slack storage, and two 6-port SC or approved alternative connector panels with adapters and provisions for two splice trays.

21.5.15 Rack Mounted Optical Fibre Termination Panel

19 in. rack mounted 72-port rack-mounted optical fibre termination panel with cable strain relief, grounding lugs, slack storage and three 12-port duplex SC or approved alternative connector panels with adapters and provisions for six (6) splice trays.

21.5.16 Splice Trays

Sized for single-mode and multimode fibres, non-metallic with clear plastic cover, 12-fibre splice capacity, and compatible with splice enclosure and splicing method.

21.5.17 Optical Fibre Connectors

Ceramic tipped field installed 568SC connectors, which meet or exceed the performance specifications in ANSI/TIA/EIA-568-B.3.

Various alternative field installed connector designs, which meet or exceed the performance specifications in ANSI/TIA/EIA-568-B.3 (Annex A).

21.5.18 Optical Fibre Jumpers

Dual 62.5/125-µm (single-mode) optical fibre jumper cable, 1 m long with 3.0 mm Duplex 568SC optical fibre connectors on each end.

Dual 62.5/125-µm (and/or single-mode) optical fibre jumper cable, 1 m long with approved alternative duplex optical fibre connectors on each end.

Dual 50/125-µm (and/or single-mode) optical fibre jumper cable, 1 m long with 3.0 mm Duplex 568 SC optical fibre connectors on each end.

Dual 50/125-µm (and/or single-mode) optical fibre jumper cable, 1 m long with approved alternative duplex optical fibre connectors on each end.

21.5.19 Optical Fibre Pigtails

62.5/125 µm (single-mode) optical fibre pigtail 1 m long with 3.0 mm single 568 SC optical fibre connectors on one end

50/125 µm (and/or single-mode) optical fibre pigtail 1 m long with 3.0 mm single 568 SC optical fibre connectors on one end

21.5.20 19” Equipment Rack - Standard

Fixed frame, 19 in. equipment rack, 2,1 meter overall height with flange base, mounting rails drilled front and back and tapped to EIA standards, and a front-rack mountable 10 outlet multiple outlet electrical strip

Swing frame, 19 in. equipment rack, 2,1 meter overall height with flange base, mounting rails drilled front and back and tapped to EIA standards, and a front-rack mountable 10 outlet multiple outlet electrical strip

21.5.21 <u>19" Equipment Rack – Wall Mount</u>

Fixed frame, 19 in. equipment rack, overall dimensions as per spec, mounting rails drilled front and back and tapped to EIA standards, and a front-rack mountable 10 outlet multiple outlet electrical strip

Swing frame / cabinet – swings from based attached to wall, 19 in. equipment rack, overall dimensions as per spec, typically 500 deep. Mounting rails drilled front and back and tapped to EIA standards, and a front-rack mountable 10 outlet multiple outlet electrical strip

21.5.22 <u>Equipment Racks – General Requirement</u>

The 19 in. equipment rack shall have the following minimum requirements:

a) 42 U rack spaces of panel space, 600 mm wide and 1 000 mm deep
b) welded frame construction
c) Locking front and rear doors
d) Adjustable front and back equipment mounting rails drilled and tapped to EIA standards
e) 10 position electrical outlet strip
f) Removable side panels
g) Top mounted, thermostatically controlled exhaust fan
h) Split Front door, each half with own lock

Blanks, brush panels, clips and labels are to be supplied and fitted to bring the existing racks up to specification.

<u>Rack Airconditioners</u>

a) CFC-free Refrigerant
b) Tested and approved by UL for NEMA 3R Enclosures
c) Digital Temperature Display
d) Built-in Condensate Evaporator to eliminate need for draining normal condensate
e) Thermostatic Low Temperature Control to prevent over-cooling and provides energy-efficient operation
f) EMI/RFI Suppressor minimizes transient line spikes during on/off cycling
g) Heavy-duty CR12 stainless steel enclosures
h) All cold components, lines and the evaporator compartment are insulated with high-performance insulation for maximum efficiency.

21.5.23 <u>Loose Equipment and Spares</u>

Furnish the following spare equipment and parts as specified:

a) Spares - Patchpanels
b) Spares - each type of jack shall be provided
c) Spares - each type of outlet
d) Workstation cable
e) Cross-connect wire for each communications closet
f) Quantity of protector modules

21.5.24 <u>Execution</u>

.1 <u>Pre-Installation Site Survey</u>

Prior to start of systems installation, meet at the project site with the Engineer , Builder and representatives of trades performing related work to coordinate efforts. Review areas of potential interference and resolve conflicts before proceeding with the work. Facilitation with the Builder will be necessary to plan the crucial scheduled completions of the equipment room and communications closets.

Examine areas and conditions under which the system is to be installed. Do not proceed with the work until satisfactory conditions have been achieved.

.2 Handling and Protection of Equipment and Materials

Be responsible for safekeeping of Contractors own and sub-contractors' property, such as equipment and materials, on the job site. The Engineer or the Builder assumes no responsibility for protection of above named property against fire, theft, and environmental conditions (salt-laden cement dust).

3 Installation

Receive, check, unload, handle, store, and adequately protect equipment and materials to be installed as part of the contract. Store in areas as directed by the Engineer or Builder. Include delivery, unloading, setting in place, fastening to walls, floors, ceilings, or other structures where required, interconnecting wiring of system components, equipment alignment and adjustment, and other related work whether or not expressly defined herein.

Install materials and equipment in accordance with applicable standards, codes, requirements, and recommendations of national, and local authorities having jurisdiction.

Adhere to manufacturer's published specifications for pulling tension, minimum bend radii, and sidewall pressure when installing cables.

Where manufacturer does not provide bending radii information, minimum-bending radius shall be 8 times cable diameter. Arrange and mount equipment and materials in a manner acceptable to the Engineer.

Penetrations through floor and fire-rated walls shall be galvanized rigid conduit sleeves and shall be fire stopped after installation and testing, utilizing a fire stopping assembly approved for that application.

Attach cables to permanent structure with suitable attachments at intervals of 1 to 1,5 meters. Support cables to be installed above removable ceilings.

Install adequate support structures for 3 meters of service slack at each equipment room.

Support riser cables on every floor and at top of run with cable grips.

Limit number of four-pair data riser cables per grip to fifty (50)

Install cables in one continuous piece. Splices shall not be allowed except as indicated on the drawings or noted below:

Provide over voltage protection on both ends of cabling exposed to lightning or accidental contact with power conductors.

The Contractor shall plan the cabling system and routing to ensure system integrity and performance, and that it does not present problems of maintenance, access nor conflict with the operation and maintenance of other systems.

Support all cabling within the false ceiling space or under raised flooring by steel cable tray, trunking and/or duct, catenary wires, fixed by approved hangers and methods.

Group cables neatly together in bundles not exceeding 50 cables per bundle. Do not try to arrange cables in bundles in straight lines leave in a random lay, to help eliminate crosstalk between cables and bundles.

Maintain at all times a minimum of 150mm spacing from parallel runs of electrical cabling and 300mm from fluorescent lights. Where telecommunications cables cross, electrical cables this shall be at right angles with approved local regulations for separation/segregation adhered to, with a minimum of 6mm of durable insulation material 300mm long with at least 25mm of overlap.

Provide and use screwed moulded plastic bushes to protect cable, with the use of locknuts inside the trunking or tray work to ensure bush remains securely in place.

Before cable is installed and after installation ensure that trunking and tray is thoroughly clean of any extraneous material, such as cable scraps, dust, dirt and construction debris.

Co-ordinate all trunking and tray work fully with other services on site as necessary.

All cable trays and catenary wires shall be earthed to a protective earth from the electrical distribution board on the floor where such cable tray is installed.

Cables shall be secured with plastic or Velcro cable ties of suitable width on cable trays and /or catenaries.

Where cabling is installed in partitions and similar enclosures, install cables in free spaces free from protrusion of screws and similar fasteners. Remove all sharp edges and allow slack in cable runs.

Where cables are installed in partitions or false walls through studs, ensure bushing is secured in these fittings to protect cables.

Restrict any single pull to no more than two (2) 90-degree bends, in conduit and ducts.

.4 Grounding

Bond and ground equipment racks, housings, messenger cables, and cableways.

Connect cabinets, racks, and frames to single-point ground which is connected to building ground system via 16 mm² green insulated copper grounding conductor.

.5 Labelling

Labelling shall conform to ANSI/TIA/EIA-606(A) standards or equivalent ISO standard. In addition, provide the following:

Label each outlet with permanent self-adhesive label with minimum 2mm high characters.

Label each cable with permanent self-adhesive label with minimum, 3mm high characters, in the following locations:

Inside receptacle box at the work area.

Behind the communication closet patch panel or punch block.

Use labels on face of data patch panels. Provide facility assignment records in a protective cover at each communications closet location that is specific to the facilities terminated therein.

Use colour-coded labels for each termination field that conforms to ANSI/TIA/EIA-606(A) standard colour codes for termination blocks.

Mount termination blocks on colour-coded backboards.

Labels shall be machine-printed. Hand-lettered labels shall not be acceptable.

Label cables, outlets, patch panels, and punch blocks with room number in which outlet is located, followed by a single letter suffix to indicate particular outlet within room.

Mark up floor plans showing outlet locations, type, and cable marking of cables. Turn these drawings over to the Engineer two (2) weeks prior to move in to allow the Engineer's personnel to connect and test Engineer-provided equipment in a timely fashion.

.6 Testing

Testing shall conform to ANSI/TIA/EIA-568-B.1 standard. Testing shall be accomplished using level IIe or higher field testers.

Test each pair and shield of each cable for opens, shorts, grounds, and pair reversal. Correct grounded, and reversed pairs. Examine open and shorted pairs to determine if problem is caused by improper termination. If termination is proper, tag bad pairs at both ends and note on termination sheets.

If copper backbone cable contains more than one (1) percent bad pairs, remove and replace entire cable.

If copper cables contain more than the following quantity of bad pairs, or if outer sheath damage is cause of bad pairs, remove and replace the entire cable:

CABLE SIZE	**MAXIMUM BAD PAIRS**
<100	1
101 to 300	1 – 3
301 to 600	3 – 6
>601	6

If horizontal cable contains bad conductors or shield, remove and replace cable.

Initially test optical cable with a light source and power meter utilizing procedures as stated in ANSI/TIA/EIA-526-14A: OFSTP-14A Optical Power Loss Measurements of Installed Multimode Fibre Cable Plant and ANSI/TIA/EIA-526-7 Measurement of Optical Power Loss of Installed Single-mode Fibre Cable Plant. Measured results shall be plus/minus 1 dB of submitted loss budget calculations. If loss figures are outside this range, test cable with optical time domain reflectometer to determine cause of variation. Correct improper splices and replace damaged cables at no charge to the Engineer.

Cables shall be tested at 850 and 1300 nm for multimode optical fibre cables. Cables shall be tested at 1310 and 1550 nm for single-mode optical fibres.

Testing procedures shall utilize “Method B” – One jumper reference.

Bi-directional testing of optical fibres is required.

Perform optical time domain reflectometer (OTDR) testing on each fibre optic conductor. Measured results shall be plus/minus 1 dB of submitted loss budget calculations.

21.6.1 Submit printout for each cable tested.
21.6.2 Submit test results in electronic format on CD-ROM

Where any portion of system does not meet the specifications, correct deviation and repeat applicable testing at no additional cost to the Engineer.

.7 Vendor Support

The intention of the following set of requirements is to ensure an adequate level of support for any vendor’s product that may be used in the network. The network shall be based on products from vendors who meet the following requirements:

The vendor shall have an internationally recognised training scheme for network designers, network managers, and support personnel.

The training scheme shall have been established in South Africa for a period of at least two (2) years and have at least 20 trained technicians.

.8 Equipment Rooms

Equipment in these rooms shall be arranged to suit current and future requirements.

The layout of the rooms shall be supplied by the Engineer once the equipment types and dimensions are known.

The room layout will comply with ISO 11064: Ergonomic design of control centers.

Operator chairs to be high quality ergonomically designed units for 24/7 use, with backrest, armrest, and be fully adjustable to suit any body type. The chairs will have at least a five castor base that will prevent tippling.

The equipment room shall be configured to suit requirements and dimensions of equipment.

This configuration shall include:-

.8.1 Positioning of existing racks and equipment

.8.2 Marking and labeling of all cables and equipment to assist maintenance

a) positioning and routing of cables and connections
b) positioning of power supply points and cable
c) installation of racks and equipment
d) configuration of the raised floor

The Contractor will be responsible for the physical movement and positioning of the racks, equipment, floors, cable ducts, and other items that make up the rooms.

The Contractor will be assisted by other specialist parties,. These other parties will take responsibility of their equipment but the contractor shall assist these parties to carry out the required actions.

Once the equipment is positioned, the relevant parties will be called in to commission the equipment. The Contractor will be required to assist where required in terms of network connectivity.

21.6 Systems Integration

The various systems in the building will interface and integrate with each other in order to exchange data. In some instances the link will be directly between two systems, in others it will be via a 3rd party system such as middleware, SQL databases, and various gateways or protocol converters.

Of relevance is the relationships between the many systems, namely the Contracts requiring communication cabling and other services. Make allowance for a series of meetings with other parties, and the need to work with these parties to integrate the entire buildings systems.

a) Access Control System
b) CCTV System
b) Smoke Detection System
c) Lighting Control
d) Substation Monitoring
e) Audio-Visual Equipment and Systems
f) TV Distribution

g) Public Address System
h) HVAC Control
i) Lifts and Escalators
j) Smoke Extraction
k) Water Pumping Systems (domestic, sump, fire booster etc.)

21.7 System Installation Process

.1 Fastening and attachment of Equipment and Cabinets

The Contractor shall ensure that all equipment is installed true, plumb and secure.

The Contractor shall be held responsible for any damage to Builder’s work due to poor installation practice.

The Contractor shall fasten and attach all housings boxes, outlets, cable trays, brackets, supports as follows:

a) Concrete (in situ) – expanding cast-in, or gun bolted, metal screw fasteners
b) Precast concrete – only with permission of the Engineer.
c) Brickwork – expanding, or built-in metal screw fasteners.
d) Ash brick – “J bolts” or approved alternative.
e) Steelwork – drilled, or tapped and screwed metal screw fasteners;
f) Woodwork – brass woodscrews, no steel screws, no nails to be used

Hard nylon plugs of not less than 6mm diameter may be used for fixing lightweight equipment.

Suitable washers shall be provided under screw head and nuts, taking into account the corrosion requirements, and ensuring dissimilar materials are not use so as to create galvanic conditions.

The Contractor shall pay particular attention to the vendor / manufacturers install procedures and instructions when fastening and attaching material and equipment.

Stainless steel brackets, anchors, gaskets, nuts, bolts, shims and all other similar materials incidental to or needed for the complete installation of equipment shall be furnished and installed by the Contractor. All the above shall be of a uniform type, size and material and shall not be used or damaged.

The dimensions of threads and hexagons of nuts, bolts and studs shall comply with the ISO metric standards. On outdoor installations all bolts, nuts and washers shall be of 316 stainless steel. No bolts or studs shall project through a nut more than 10mm. No nuts and bolts that have been stripped or have had their heads damaged shall be used.

.2 Cable Racks

All cable racks shall be installed in the vertical plane and checked by spirit level. The racks shall be parallel with wall and roof and spaced some distance from them to allow painting.

All cable racks and cable supports located within buildings shall be made of hot dip galvanised sections.

All cable racks shall be earthed by running a 70mm² copper earth wire along the entire route and bonding this securely to the rack every 15m.

The cable runs shall be firmly secured and positioned in such a manner to cause no obstruction to walkways, stairs or other normal access routes.

.3 Single Cable Support

Where a cable leaves a cable rack to drop or rise to a connection point it shall be supported on an angle support fabricated to securely carry and protect the cable. The angle shall be fixed or supported at 1500mm intervals.

Angle supports shall be carefully selected to suit the cable size being carried.

Cable entries shall be from below unless otherwise specified, or instructed by the Engineer.

The cable rack/tray or angle runs (droppers) shall be adequately supported with a maximum of approximately 1,5m centres for horizontal runs and 2,5m for vertical runs. Standard accepted radius bends shall be used. Supports shall not be welded to any vessels, piping or structures without first consulting the Engineer, the normal method for fixing shall be by bolting.

.4 Cable Installation

All cables shall be run in single continuous lengths. Splicing shall not be allowed, unless with written permission of the Engineer. In such a case, any and all splices to be located in a suitable enclosure, and marked up on the as built drawings.

Cable splicing where specifically required and agreed by the Engineer, shall be made with Kabeldon, Pratley, 3m or with jointing kits approved by him.

All cables shall be colour coded and numbered consistently and continuously throughout the work. Painting or taping of conductors will not be acceptable under any conditions.

The spacing on indoor cable racks shall be maintained by cable ties, at least every 300mm.

No cables shall be buried directly in the ground within any building or plant area.

Where cables change route, or traverse through partitions, they shall be marked by the associated cable reference numbers. All temporary strapping shall be removed.

All cable ends shall be sealed if they are to be left for a period exceeding 1 week before termination.

When complete, all cabling and wiring when complete shall present a neat and tidy appearance.

To avoid damage to cables/tubes rising from floor or grade level, protection covers shall be securely placed to a height of 600mm above floor level.

The Contractor shall be responsible for measuring and recording the length and type of all cable installed.

Should a dispute arise over the measured lengths, the Engineer may require a sample of cable to be removed to verify the accuracy of the measurements, or he will instruct the Contractor to measure the cable runs in his presence using a suitable non-destructive measuring device, to be provided by the Contractor and at the Contractors expense. Such a measuring device will be calibrated for the type of cable before use, using various lengths of suitable cable to be supplied by the Contractor.

Adequate rollers/support shall be provided when pulling cables to ensure minimum strain and no damage to cable outer sheaths. Should any damage occur, this must be brought to the attention of the Engineer and corrected as instructed.

Cable drums shall be rolled and cables unwound in the direction indicated on the drum to prevent slackening of wound cable.

Every rack and cable installed on racking/tray shall be sufficiently supported in such a manner that there is no undue mechanical strain or sagging.

Cable glands of correct size and approved type shall be used. Plastic glands will not be permitted. Where the gland is in the field, a weatherproof shroud shall be fitted to the gland. Wire ends shall be terminated with interlocking numbered ferrules and an insulated crimped lug of the correct type and size, using the correct size and approved type of wire stripper and crimping tool. The associated cable reference number shall be fixed on the cable at each gland termination, using cable markers of an approved type.

Only one wire end will be allowed per terminal connection and crimp lug. No bare wire shall be exposed beyond crimp lug insulation. The correct style of lugs only shall be used for the applicable terminal type.

Earth terminations on field mounted devices shall be via the earth core indicated in the termination schedule. Care shall be taken to only connect earth cores where shown on the drawings.

All terminations shall be made in a neat, workmanlike manner with appropriate binding of loose wires where necessary. All spare wires shall be terminated as per the termination schedule. All cables/wire markers shall be of the same size and face the same direction (left to right or bottom to top). All terminals shall be numbered as per the connection schedules, and left to right or top to bottom. Wire colour coding shall be adhered to, the painting of wire insulation will not be allowed.

The minimum radius of bends for multicore cable/tubing shall be as recommended by the manufacturer

After completion, each installation shall be visually checked and any cable defects revealed shall be brought to the attention of the Engineer. The installation shall then be handed over as mechanically complete subject to any “Punch List” rectification.

Where unarmoured cable or single wires are specified in the field, they shall be run in suitable trunking or conduit.

All debris and foreign matter shall be removed from cable racks and trenches prior to installation of the cables, and on completion of the work the Contractor shall thoroughly check all cable racks and trenches and again remove all accumulated dirt and debris. On completion of the cable installation, the Contractor shall ensure that all covers are in place on the trenches and racks where applicable and that any site damage has been repaired and racks straightened where necessary.

During installation of the cables, extreme care shall be exercised to avoid kinking or bending which may damage the cable insulation or sheath. Cables which are accidentally damaged during installation shall be repaired or replaced at the discretion of the Engineer. In no case shall a cable on which the outer sheath has been punctured be installed in that condition.

The length of overcut of free issued cables shall be limited to 600mm longer than the length of the longest conductor required in the cable. Shortages of cable caused by excessive overcut length shall be replaced by the Contractor at his own expense.

Conductors or cables shall not be laid down until the cables are safe from damage caused by construction operations. All conductors on vertical runs of cable rack shall be supported independently of the terminal connections. Cables shall be installed in the racks in logical order such that they will lie flat and with a minimum of cross overs. Cables entering or leaving racks shall be routed to prevent possible mechanical damage due to abrasion.

The Contractor shall be responsible for the storage of all cable and shall suitably protect it from weather and damage during storage and handling, and shall be responsible for the security of such cable.

Cables entering all field mounted equipment shall enter from the bottom, unless specified otherwise by the Project Manager.

Before a cable is run, the Contractor shall establish that the dielectric is sound (by testing insulation resistance) and also that all cores are correct and continuous from end to end.

.5 Terminating and Jointing

All glands shall be IP67 rating.

All conductors shall be fitted with compression type lugs of the correct size and design for the application.

.6 Panel Wiring

Every wire shall be identified by number ferrules at each end, and wherever required shall be terminated by flanged fork locking tongue crimping type BAZ Vinyl lug connectors, using tin-plated copper barrel and tongue.

A standard colour of Yellow with Black printing shall be used for all cable markers, self-sticking or clip-on types, enabling the markers to remain in position even when the cables are turned at 90º.

All panel wiring shall be neatly loomed.

Terminals shall be of the Klippon pressure and screw type. Terminals where the grub screws bear directly on the conductors will not be allowed.

Each terminal shall have a space for numbering. The Contractor shall label each terminal in a numerical sequence as shown on drawings.

Internal connection shall be made to terminal strips on one side only, leaving the other side clear for field connections. Not more than one wire shall be connected to one side of any terminal. At least twenty percent spare terminals shall be provided on the end of each terminal rail.

All integral control wiring shall be polyvinyl chloride insulated, rated 600/1000 volt with stranded copper conductors. Minimum control wiring size shall be 2,5mm^2 unless specifically specified otherwise.

All contactor connections, terminal connections and ancillary wiring connections must be checked for tightness and be properly tightened when found loose prior to energising circuit. This exercise shall be carried out by the Contractor.

On control wiring into terminals, standard blue double grip pin type solderless crimp lugs shall be used. Plant stranded wire cores directly into terminals shall not be permitted.

.7 Field Mounted Equipment

All devices in this field are to be housed inside IP65 enclosures or fabricated 304L stainless steel panels.

All marshalling cubicles and junction boxes shall be reinforced polyester. The installed cubicle shall conform to IP65. Covers shall be hinged on the side with captive fixings.

The back plates of all marshalling cubicles shall be of 304L stainless steel.

All equipment mounted in marshalling cubicles shall be secured with stainless steel or brass fasteners.

All equipment shall be mounted in marshalling cubicles with reasonable room for maintenance of tubing and electrical connections.

All field mounted socket outlets inclusive of 3 pin 15 Amp switched socket outlets are to be housed within York enclosures.

.8 Equipment Identification

The Contractor shall provide each electrical item with suitable means of identification, as indicated in this specification and shall include the following:

Stainless Steel nameplates for all field mounted devices.

Strap-on cable markers, Cat. No. 5,0 at all cable glands.

All conductors shall be identified at all terminations by sleeve type markers.

Markers shall be Yellow with Black letters.

Name plates shall not be less than 25mm high x 75mm long and shall be fastened with epoxy glue. Letters shall be upper case, minimum 6mm high. Nameplates, tags and markers shall be affixed as work progresses. Self tapping screws will not be accepted. Surface preparation shall comply with the epoxy manufacturer's specification.

.9 Painting and Restoring

All steelwork, except 3CR12, SS304L, and SS316L, installed by the Contractor shall be treated and painted as described in the Project Paint Specification and to the project colour code.

The Contractor shall be responsible for touch-up of any paint surface damaged during installation, to project Paint Specification.

After completion, the paintwork of all panels and kiosks shall be thoroughly examined and any deteriorated or mechanically damaged surfaces of such shall be made good.

Any nuts or bolts which may have been removed during site erection, or which may be required to be removed for maintenance purposes shall be restored to their original condition. Any missing bolts or washers will be replaced by the Contractor. Any damaged bolt to nut heads will be replaced by the Contractor.

.10 Corrosion Protection of Material

The Contractor shall select materials and their finishing that have the appropriate level of corrosion resistance.

The Contractor shall take measures to reduce the effect of equipment being contaminated with salt-laden dust as found in a typical costal building site by continuous vacuuming and cleaning of the equipment room, control rooms, and equipment cabinets and racks.

.11 Safety Signs, Labels, Notices

The Contractor shall be responsible for the supply and installation of safety signs as required by occupational Health and Safety Act Regulations and as stipulated by Engineer. Each door, riser section and gate shall be fitted with danger and warning signs. Each door and gate shall in addition be fitted with voltage warning, shock and fire procedure signs.

All items of equipment, switchgear panels and components, kiosks and junction boxes, shall be clearly labelled with professionally manufactured tag numbers and descriptions. The labels shall be permanent and free from fading.

Labels for mounting outdoors shall, unless otherwise approved, be stainless steel plates. The plates shall be secured by means of brass screws with protective washers back and front to prevent damage to the paint.

21.8 Acceptance Testing and Commissioning

.1 Introduction

This procedure defines the requirements and responsibilities for the IT Network equipment acceptance and prior to the connection of terminal devices.

Three phases in the project installation, commissioning and handover process will be documented according to the IEC 62381 Standard which defines procedures and specifications for the:

a) factory acceptance test (FAT)
b) site acceptance test (SAT)
c) site integration test (SIT)

These tests are carried out to prove that the electronic system is in accordance with the specification. These tests allow for planning and execution of the different test procedures for the system, which precedes the commissioning period.

.2 Standards

Relevant standards include:

IEC/PAS 62381 Ed. 1.0 en:2004 - Activities during the factory acceptance test (FAT), site acceptance test (SAT), and site integration test (SIT) for automation systems in the process industry"

.3 Acceptance Testing

The system(s) and sub-system(s) shall be verified and tested by activities to be carried out during the factory acceptance test (fat), Site acceptance test (sat), and site integration test (sit).

.3.1 Factory acceptance test (FAT)

The Contractor shall perform the following as part of the FAT:

a) Documentation check
b) HW and SW inventory check
c) Mechanical inspection
d) Wiring and termination inspection
e) Start-up text and general system functions
f) System alarm test
g) Hardware redundancy and diagnostic check
h) Visualization/operation
i) Test of functionality against FBD, FUP, etc)
j) Complex functionality and operation modes
k) Integration of subsystems
l) The Contractor shall complete a FAT checklist as provided by the Engineer
m) The Contractor shall prepare a FAT punch (snag) list to be presented to the Engineer.

.3.2 Site acceptance test (SAT)

a) SAT checklist
b) SAT punch list
c) The Contractor shall complete a SAT checklist as provided by the Engineer.

d) The Contractor shall prepare a SAT punch (snag) list to be presented to the Engineer.

e) Point to Point Checkout: Each I/O device (both field mounted as well as those located in the equipment rooms) shall be inspected and verified for proper installation and functionality. A checkout sheet itemizing each device shall be filled out, dated and approved by the a responsible party for submission to the Engineer

f) Controller and Workstation Checkout: A field checkout of all controllers and front end equipment (gateways, interfaces, networks, converters, etc.) shall be conducted to verify proper operation of both hardware and software. A checkout sheet itemizing each device and a description of the associated tests shall be filled out, dated and approved by the a responsible party for submission to the Engineer

g) Pre-System Acceptance Testing:

i) All application software will be verified and compared against the sequences of operation. Control loops will be exercised by inducing a setpoint shift of at least 10% and observing whether the system successfully returns the process variable to setpoint.

ii) Test each alarm in the system and validate that the system generates the appropriate alarm message, that the message appears at all prescribed destinations (workstations or printers), and that any other related actions occur as defined (i.e. graphic panels are invoked, reports are generated, etc.).

iii) Perform an operational test of each unique graphic display and report to verify that the item exists, that the appearance and content are correct, and that any special features work as intended.

iv) Perform an operational test of each third party interface that has been included as part of the automation system. Verify that all points are properly polled, that alarms have been configured, and that any associated graphics and reports have been completed. If the interface involves a file transfer over Ethernet, test any logic that controls the transmission of the file, and verify the content of the specified information.

.3.3 Site integration test (SIT)

a) SIT checklist

b) SIT punch list

c) The Contractor shall complete a SIAT checklist as provided by the Engineer

d) The Contractor shall prepare a SIT punch (snag) list to be presented to the Engineer.

.3.4 Commissioning

a) System Checkout And Testing

Start-up Testing: All testing listed in this document shall be performed by the contractor and shall make up part of the necessary verification of an operating control system. This testing shall be completed before the Clients representative is notified of the system demonstration.

b) System Demonstration and Final Acceptance

i) Demonstration

Prior to acceptance, the system shall undergo a series of performance tests to verify operation and compliance with this specification. These tests shall occur after the Contractor has completed the installation, started up the system, and performed the Contractor’s and Manufacturers own tests.

The tests described in this section are to be performed in addition to the tests that the contractor performs as a necessary part of the installation, start-up, and debugging process. The Engineer will be present to observe and review these tests. The Engineer shall be notified at least 10 days in advance of the start of the testing procedures.

The demonstration process shall follow that as submitted by the Engineer from time to time. The approved checklists and forms shall be completed for all systems as part of the demonstration.

The contractor shall provide at least two persons equipped with two-way communication and shall demonstrate actual field operation of each control and sensing point for all modes of operation including day, night, occupied, unoccupied, fire/smoke alarm, seasonal changeover, and power failure modes. The purpose is to demonstrate the calibration, response, and action of every point and system. Any test equipment required to prove the proper operation shall be provided by and operated by the contractor.

As each control input and output is checked, a log shall be completed showing the date, technician's initials, and any corrective action taken or needed. The log template shall be agreed with the Engineer.

Demonstrate compliance with sequences of operation through all modes of operation.

Demonstrate complete operation of operator interface.

Additionally, the following items shall be demonstrated:

Operational logs for each system that indicate all set points, operating points, field I/O positions, mode, and equipment status shall be submitted to the Engineer. These logs shall cover three 48-hour periods and have a sample frequency of not more than 10 minutes. The logs shall be provided in both printed and CR-ROM formats.

Any tests that fail to demonstrate the operation of the system shall be repeated at a later date. The contractor shall be responsible for any necessary repairs or revisions to the hardware or software to successfully complete all tests.

ii) Acceptance

All tests described in this specification shall have been performed to the satisfaction of both the engineer and Client prior to the acceptance of the control system as meeting the requirements of completion. Any tests that cannot be performed due to circumstances beyond the control of the contractor may be exempt from the completion requirements if stated as such in writing by the Engineer. Such tests shall then be performed as part of the warranty.

The system shall not be accepted until all forms and checklists completed as part of the demonstration are submitted and approved by the Engineer.

21.9 Computer Hardware

.1 General Purpose Laptop PC – (if applicable)

Intel i7 2.8 GHz or higher processor – Intel HM65 express mobile chipset and Intel HD 3000 graphics or equivalent or AMD equivalent; 4 GB DDR3 RAM; 1 Tb hard drive; 14" LCD monitor; R/W CD- ROM drive; MS keyboard & optical mouse; integrated 100/1000 LAN wireless LAN 802.I1, 2 x USB 3.0, 2 x USB 2.0, 1 x HDMI, 1 x RJ45 Ethernet, 5 in 1 cardholder. Microsoft Windows 10 Professional 64-bit, Office 2012; Business, Acrobat X professional; Trend Antivirus or equivalent.

.2 General Purpose PC

Intel i7 2.8 GHz or higher processor – Intel HM65 express mobile chipset and Intel HD 3000 graphics or equivalent or AMD equivalent; 4 GB DDR3 RAM; 1 Tb hard drive; 14" LCD monitor; R/W CD- ROM drive; MS keyboard & optical mouse; integrated 100/1000 LAN wireless LAN 802.I1, 2 x USB 3.0, 2 x USB 2.0, 1 x HDMI, 1 x RJ45 Ethernet, 5 in 1 cardholder. Microsoft Windows 10 Professional 64-bit, Office 2012; Business, Acrobat X professional; Trend Antivirus or equivalent.

.3 Server

Processor	– Dell Power Edge R730
Cache Memory	– 30 Mb
Memory	– DDR3 / 16 slots with 12 No. SATA 2 Tb 2.5 inch hard drives
Graphics	– 64 bit HD graphics card
Power	– Power Management System – dual supply
Software	– Windows Business 2012 SLQ database

.4 A3 Colour Workgroup Laser Printer

A3 colour @ 18 ppm, 128 MB RAM, 100/1000 Base TX port, 2 off 150 sheet trays, up to 120 gsm media (network enabled)

.5 A4 Colour Desktop Laser Printer

A4 colour @ 24 ppm, duplex printing, 256 MB RAM, 100/1000 Base TX port, 2 off 500 sheet trays, up to 200 gsm media (network enabled)

.6 XGA Projector

2000 ANSI Lumen 3LCD with remote control, swappable dual lamps.

.7 A3 Colour Scanner

A3 flatbed scanner with auto document feeder, 80 sheet tray, 600 x 2400 dpi, 128 MB RAM, 100/1000 Base TX port.

22. CCTV System

22.1 System Overview

The proposed system shall comprise of the following units:-

.1 System database servers (SDS)
.2 Video recorder servers for (NVR)
.3 Video Analytics Server (VAS)
.4 Software to manage the system functions and equipment database
.5 Software to manage the video recording, playback etc.
.6 Software to manage the analytics
.7 Surveillance stations for viewing of live images or playback of recorded images complete with keyboard and joysticks
.8 Various types of cameras complete with mounting accessories
.9 System cabling and other accessories required to connect to the LAN
.10 Power supply devices and cabling.

The above equipment is interconnected by a TCP/IP Network (LAN) provided by others.

The LAN (provided by others) consists of 2 No. core switches located in the Primary and Secondary Equipment Rooms with multiple 10 Gig links to (PoE) edge switches located in each ward IT Room to accommodate the connection of CCTV equipment.

The CCTV equipment is to be connected to the LAN edge switches via 1 Gig links with Cat 6a (Cu10) cabling as part of this contract.

All the systems hardware and software to be supplied from the same manufacturer

The system should allow for secure mode of communication with open architecture, allow unlimited expansion, viewing of cameras from multiple works stations over the network.

The surveillance/monitoring stations are located at the Security Rooms, Systems Servers, and the Digital Video Recording System etc. located in the “Primary Equipment Room” with redundant back up servers located in the “Secondary Equipment Room”.

A failure of any one of the Systems Database Servers (SDS) or Video Recorder Servers (NVR) shall NOT cause the system functions and Video Recording System (VRS) system to cease operation. The cameras controlled by the NVRs will be temporarily unavailable until re-allocated to other NVRs using the VRS software. No physical changes to hardware, cabling or connections shall be required.

The system is to be fully operational from the equipment located in the Primary Equipment Room with a fall over / back up system located in the “Secondary Equipment Room”.

The system must be able to be integrated with other systems which includes the Access Control System, Building Management System, Intruder Detection, third party IP surveillance hardware etc.

The (SDS) software shall have a full database of all devices and a graphical display of equipment location.

Each surveillance / monitoring station shall be fitted with a keyboard and joystick for use to view and control cameras.

CCTV equipment shall make use of Power over Ethernet (PoE) from the LAN except for PTZ's etc. which may require additional power and PoE power injector.

All network devices shall be assigned IP addresses statically, but should it be absolutely necessary to use DHCP for IP address assignment, then the IP addresses must be within a defined range.

22.2 Standards

SANS 10222-5-1 to 10222-5-5 (latest edition)

22.3 Camera Equipment - General

The CCTV System shall comprise of a mixture of IP based digital Fixed Dome Cameras, PTZ Dome Cameras, High Speed Day/Night PTZ Cameras, Weather proof housings and other associated accessories.

All cameras shall be supplied and installed with all necessary accessories and options as part of this contract, with provisions for additional units if required for future expansion.

All cameras to be ONVIF Profile S compliant.

Cameras offered shall have a Mean Time Before Failure (MTBF) exceeding 50,000 hours for static cameras and 30,000 hours for PTZ's.

The outdoor cameras shall be protected against corrosion and enclosures rated to IP66.

Camera heating shall be included if required.

Cameras to accommodate wide-angle lens, Motorised Zoom Lens, together with Pan and Tilt to attain optimum coverage and tracking.

Automatic gain control is required on certain cameras as scheduled. Auto circuits for colour to mono switching under lowlight conditions is required..

Cameras shall be supplied with tamper proof bracketry, housings, and connections.

230V 50Hz will be provided in equipment rooms only. All other power supplies and power conditioning equipment must be provided under this contract and be included in the camera pricing.

22.4 Camera Type 1 - High Resolution Colour Fixed Indoor Dome - IP

Colour High Resolution Internal Dome Camera with the following minimum features/ capabilities.

1. Image Sensor - ⅓ inch or larger (CCD or CMOS)
2. Resolution – 2 megapixels (1920 by 1080) or higher
3. Colour - Full colour down to 0.25 lux and up to 10 000 lux
4. Monochrome – Down to 0.1 lux
5. Images per second - >25
6. Lens – Varifocal auto Iris with remote zoom and focus
7. Lens focal length - (minimum of 3 lens options) from 3 mm to 40 mm
8. Day / Night Control - automatic
9. White balance - Manual / Automatic
10. Horizontal viewing angles >90º
12. Connector - Ethernet RJ45
13. Comms speed and cable - (1000 Base – TX) Cat 6a UTP cable or better
14. Comms Protocol – TCP / IP
15. Dynamic Range - 75 dB WBR or higher

16. Backlight compensation – OFF/Automatic
17. Power – POE <35 Watts
18. Video Compression - JPEG H.264 MPEG4 (Part 2), MJPEG
19. On board storage – SD card slot with 16 GB card
20. Audio Signal to noise ratio - >50 dB
21. Set up – Remote and local
22. Analogue video output
23. Image stabilizer – Auto
24. Scene change detection – Programmable
25. Video Analytical Support – Programmable
26. Audio input and output

The camera shall have the following physical properties.

27. Housing Material - Plastic
28. Housing Protection – Tamperproof
29. Dome - Polycarbonate tinted
30. Ingress Protection Rating – IP51

The camera shall be able to accommodate the following accessories.

31. Ceiling mount recess trim
31. Surface mount trim
32. Corner mount bracket
33. Microphone and speaker

22.5 Camera Type 2 - High Resolution Colour Fixed Outdoor Dome – IP

Colour High Resolution External Dome Camera with the following minimum features/ capabilities.

1. Image Sensor - ⅓ inch or larger (CCD or CMOS)
2. Resolution – 2 megapixels (1920 by 1080) or higher
3. Colour - Full colour down to 0.25 lux and up to 10 000 lux
4. Monochrome – Down to 0.1 lux
5. Images per second - >25
6. Lens – Varifocal auto Iris with remote zoom and focus
7. Lens focal length - (minimum of 3 lens options) from 3 mm to 40 mm
8. Day / Night Control - automatic
9. White balance - Manual / Automatic
10. Horizontal viewing angles >90º
11. Connector - Ethernet RJ45
12. Comms speed and cable - (1000 Base – TX) Cat 6a UTP cable or better
13. Comms Protocol – TCP / IP
14. Dynamic Range - 75 dB WBR or higher
15. Backlight compensation – OFF/Automatic
16. Power – POE <10 Watts
17. Video Compression - JPEG H.264 MPEG4 (Part 2), MJPEG
18. On board storage – SD card slot with 16 GB card
19. Audio Signal to noise ratio - >50 dB
20. Set up – Remote and local
21. Analogue video output
22. Image stabilizer – Auto
23. Scene change detection – Programmable
24. Video Analytical Support - Programmable
25. Audio input and output

The camera shall have the following physical properties.

26. Housing Material - Plastic
27. Housing Protection - Tamperproof
28. Dome - Polycarbonate tinted

29. Ingress Protection Rating – IP66

The camera shall be able to accommodate the following accessories.

30. Ceiling mount recess trim
31. Surface mount trim
32. Pendant mount bracket
33. Microphone and Speaker

22.6 Camera Type 3 - High Resolution Colour PTZ Indoor Dome - IP

Colour High Resolution Internal Dome Camera with the following minimum feature capabilities.

1. Image Sensor - ⅓ inch or larger (CCD or CMOS)
2. Resolution – 2 megapixels (1920 by 1080) or higher
3. Colour - Full colour down to 0.25 lux and up to 10 000 lux
4. Monochrome – Down to 0.1 lux
5. Images per second - >25
6. Lens – Zoom lens with auto Iris with remote zoom and focus
7. Lens zoom – 20 times optical or greater (from 4 mm to 110 mm)
8. Day / Night Control - automatic
9. White balance - Manual / Automatic
10. Horizontal viewing angles >90º
11. Connector - Ethernet RJ45
12. Comms speed and cable - (1000 Base – TX) Cat 6a UTP cable or better
13. Comms Protocol – TCP / IP
14. Dynamic Range 75 dB WBR or higher
15. Backlight compensation – OFF/Automatic
16. Power – POE <35 Watts (Power POE injecter to be provided for power required exceeding 15 Watts)
17. Video Compression - JPEG H.264 MPEG4 (Part 2), MJPEG
18. On board storage – SD card slot with 16 GB card
19. Audio Signal to noise ratio - >50 dB
20. Set up – Remote and local
21. Analogue video output
22. Image stabilizer – Auto
23. Scene change detection – Programmable
24. Video Analytical Support - Programmable
25. Audio input and output

The camera shall have the following physical properties.

26. Housing Material - Plastic
27. Housing Protection - Tamperproof
28. Dome – Polycarbonate tinted
29. Ingress Protection Rating – IP51

The PTZ shall have the following features.

30. Pan Angle - 360°
31. Pan Speed - 180° per second
    - 0.5° per second
32. Vertical Tilt - +0° to - 90°
33. Proportional Pan / Tilt Speed – Speed to decrease in proportion to increased depth of zoom
34. Motor Rating – Continuous duty

The camera shall be able to accommodate the following accessories.

35. Ceiling mount recess trim
36. Surface mount trim

37. Corner mount bracket
38. Microphone and speaker

22.7 Camera Type 4 – High Resolution Colour PTZ Outdoor Dome - IP

1. Image Sensor - ⅓ inch or larger (CCD or CMOS)
2. Resolution – 2 megapixels (1920 by 1080) or higher
3. Colour - Full colour down to 0.25 lux and up to 10 000 lux
4. Monochrome – Down to 0.1 lux
5. Images per second - >25
6. Lens – Zoom lens with auto Iris with remote zoom and focus
7. Lens zoom – 20 times optical or greater (from 4 mm to 110 mm)
8. Day / Night Control - automatic
9. White balance - Manual / Automatic
10. Horizontal viewing angles >90º
11. Connector - Ethernet RJ45
12. Comms speed and cable - (1000 Base – TX) Cat 6a UTP cable or better
13. Comms Protocol – TCP / IP
14. Dynamic Range 75 dB WBR or higher
15. Backlight compensation – OFF/Automatic
16. Power – POE <30 Watts (Power POE injecter to be provided for power required exceeding 15 Watts)
17. Video Compression - JPEG H.264 MPEG4 (Part 2), MJPEG
18. On board storage – SD card slot with 16 GB card
19. Audio Signal to noise ratio - >50 dB
20. Set up – Remote and local
21. Analogue video output
22. Image stabilizer – Auto
23. Scene change detection – Programmable
24. Video Analytical Support - Programmable
25. Audio input and output

The camera shall have the following physical properties.

26. Housing Material - Plastic
27. Housing Protection - Tamperproof
28. Dome – Polycarbonate tinted
29. Ingress Protection Rating – IP51

The PTZ shall have the following features.

30. Pan Angle - 360°
31. Pan Speed - 180° per second
    - 0.5° per second
32. Vertical Tilt - +0° to - 90°
33. Proportional Pan / Tilt Speed – Speed to decrease in proportion to increased depth of zoom
34. Motor Rating – Continuous duty

The camera shall be able to accommodate the following accessories.

35. Ceiling mount recess trim
36. Surface mount trim
37. Corner mount bracket
38. Microphone and speaker

22.8 Camera Type 5 – High Resolution Weatherproof Bullet Fixed - IP

Colour High Resolution Weatherproof Fixed Camera with the following minimum features/ capabilities.

1. Image Sensor - ⅓ inch or larger (CCD or DMOS)
2. Resolution – 3 megapixels (2048 by 1536) or higher
3. Colour - Full colour down to 0.25 lux and up to 10 000 lux
4. Monochrome – Down to 0.1 lux
5. Images per second - >25
6. Lens – Varifocal auto Iris with remote zoom and focus
7. Lens focal length - (minimum of 3 lens options) from 3 mm to 40 mm
8. Day / Night Control - automatic
9. White balance - Manual / Automatic
10. Horizontal viewing angles >90º
11. Connector - Ethernet RJ45
12. Comms - (1000 Base – TX) Cat 6a UTP cable or better
13. Comms Protocol – TCP / IP
14. Dynamic Range - 75 dB WBR or higher
15. Backlight compensation – OFF/Automatic
16. Power – POE <15 Watts
17. Video Compression - JPEG H.264 MPEG4 (Part 2), MJPEG
18. On board storage – SD card slot with 16 GB card
19. Audio Signal to noise ratio - >50 dB
20. Set up – Remote and local
21. Analogue video output
22. Image stabilizer – Auto
23. Scene change detection – Programmable
24. Video Analytical Support - Programmable
25. Audio input and output

The camera shall have the following physical properties.

26. Housing Material – Aluminium, powder coated
27. Housing Protection - Tamperproof
28. Ingress Protection Rating – IP66

The camera shall be able to accommodate the following accessories.

29. Pole mount bracket
30. Pendant mount bracket
31. Corner mount bracket
32. Microphone and speaker

22.9 Camera Type 6 – High Resolution Weatherproof Bullet PTZ - IP

Colour High Resolution Outdoor Weatherproof PTZ Camera with the following minimum features/ capabilities.

1. Image Sensor - ⅓ inch or larger (CCD or CMOS)
2. Resolution – 3 megapixels (2048 by 1536) or higher
3. Colour - Full colour down to 0.25 lux and up to 10 000 lux
4. Monochrome – Down to 0.1 lux
5. Images per second - >25
6. Lens – Zoom lens with auto Iris with remote zoom and focus
7. Lens zoom – 30 times optical or greater (from 4 mm to 110 mm)
8. Day / Night Control - automatic
9. White balance - Manual / Automatic
10. Horizontal viewing angles >90º
11. Connector - Ethernet RJ45
12. Comms speed and cable - (1000 Base – TX) Cat 6a UTP cable or better
13. Comms Protocol – TCP / IP
14. Dynamic Range 75 dB WBR or higher
15. Backlight compensation – OFF/Automatic
16. Power – POE <35 Watts (Power POE injecter to be provided for power required exceeding 15 Watts)
17. Video Compression - JPEG H.264 MPEG4 (Part 2), MJPEG

18. On board storage – SD card slot with 16 GB card
19. Audio Signal to noise ratio - >50 dB
20. Set up – Remote and local
21. Analogue video output
22. Image stabilizer – Auto
23. Scene change detection – Programmable
24. Video Analytical Support - Programmable
25. Audio input and output

The camera shall have the following physical properties.

26. Housing Material – Aluminium, powder coated
27. Housing Protection - Tamperproof
28. Ingress Protection Rating – IP66

The PTZ shall have the following features.

29. Pan Angle - 360°
30. Pan Speed - 180° per second
    - 0.5° per second
31. Vertical Tilt - +0° to - 90°
32. Proportional Pan / Tilt Speed – Speed to decrease in proportion to increased depth of zoom
33. Motor Rating – Continuous duty

The camera shall be able to accommodate the following accessories.

34. Pole mount bracket
35. Pendant mount bracket
36. Corner mount bracket
37. Microphone and speaker

22.10 Camera Type 7 – High Speed, High Resolution Weatherproof Panoramic Fixed Dome 180° – IP

A fixed 180° continuous panoramic view the following minimum feature capabilities.

1. Image sensor - ¼ inch or larger (CCD or CMOS)
2. No. of sensors – 4 No.
3. Resolution – 2 megapixels (1920 by 1080) or higher for each server
4. Colour - Full colour down to 0.7 lux and up to 10 000 lux
5. Monochrome – Down to 0.2 lux
6. Images per second - >6
7. Lens – Fixed, auto iris with manual focus
8. Day / Night Control - automatic
9. White balance - Manual / Automatic
10. Viewing angles >180º
11. Connector - Ethernet RJ45
12. Comms speed and cable - (1000 Base – TX) Cat 6a UTP cable or better
13. Comms Protocol – TCP / IP
14. Dynamic Range 75 dB WBR or higher
15. Backlight compensation – OFF/Automatic
16. Power – POE <15 Watts
17. Video Compression - JPEG H.264 MPEG4 (Part 2), MJPEG, JPEG 2000
18. On board storage – SD card slot with 16 GB card
19. Audio Signal to noise ratio - >50 dB
20. Set up – Remote and local
21. Analogue video output
22. Image stabilizer – Auto
23. Scene change detection – Programmable
24. Video Analytical Support - Programmable
25. Audio input and output

26. The camera shall have the following physical properties.
27. Housing Material – Aluminium, powder coated
28. Housing Protection – Tamperproof
29. Dome – Polycarbonate tinted
30. Ingress Protection Rating – IP66

The camera shall be able to accommodate the following accessories.

31. Ceiling mount recess trim
32. Surface mount trim
33. Corner mount bracket
34. Pole mount bracket
35. Pendant mount bracket
36. Microphone and speaker

22.11 Camera Type 8 –High Resolution Colour Weatherproof 360º Panoramic Fixed Dome – IP

Colour High Resolution Outdoor Fixed Dome Camera with the following minimum features/ capabilities.

1. Image Sensor - ¼ inch or larger (CCD or CMOS)
2. No. of sensors – 8 No.
3. Resolution – 2 megapixels (1920 by 1080) or higher for each sensor
4. Colour - Full colour down to 0.7 lux and up to 10 000 lux
5. Monochrome – Down to 0.1 lux
6. Images per second - >6
7. Lens – Fixed auto iris with fixed manual focus
8. Day / Night Control - automatic
9. White balance - Manual / Automatic
10. Viewing angles 360º
11. Connector - Ethernet RJ45
12. Comms speed and cable - (1000 Base – TX) Cat 6a UTP cable or better
13. Comms Protocol – TCP / IP
14. Dynamic Range - 75 dB WBR or higher
15. Backlight compensation – OFF/Automatic
16. Power – POE <6 Watts
17. Video Compression - JPEG H.264 MPEG4 (Part 2), MJPEG
18. On board storage – SD card slot with 16 GB card
19. Audio Signal to noise ratio - >50 dB
20. Set up – Remote and local
21. Analogue video output
22. Image stabilizer – Auto
23. Scene change detection – Programmable
24. Video Analytical Support - Programmable
25. Audio input and output

The camera shall have the following physical properties.

26. Housing Material – Aluminium, powder coated
27. Housing Protection – Tamperproof
28. Dome - Polycarbonate tinted
29. Ingress Protection Rating – IP66

The camera shall be able to accommodate the following accessories.

30. Ceiling mount recess trim
31. Surface mount trim
32. Corner mount bracket
33. Pole mount bracket
34. Pendant mount bracket
35. Microphone and speaker

22.12 Video Recording System (VRS) Operation

The VRS shall comply with or exceed the following design and performance specifications:

The VRS shall record, store and play back of images at a rate of 25 FPS per camera or higher and support at least 2000 channels and 100 channels per network video recorder (NVR).

Each NVR must have the latest Microsoft window software, have in excess of 18 TB of disk storage configured to RAID 5 using SATA hard disk drives for the storage of images in a comparable format. Hard disk drives to be hot swappable.

The VRS shall have 4 operating modes:-

Continuous viewing, event playback, client server settings and programmed modes. All modes shall be disabled and enabled using scheduled configuration..

The VRS system shall provide IP output, with high definition resolutions (1920 x 1080).

The VRS shall have the ability to control PTZ functions from the monitoring station PC using the PC keyboard with joystick for fine control.

The VRS shall allow cameras to be viewed on a variety of multi-screen modes.

The VRS shall support simultaneous playback and record full duplex operation.

The VRS shall provide programmable motion detection. Each camera shall be customised for specific ‘motion triggered’ recording rates with up to 32 x 32 grids programmable per channel, with 100 levels of sensitivity. On motion it shall capable of being programmed to bring the camera full screen to the main monitor, link to a PTZ and call a preset, sound a buzzer and trigger a relay on the alarm output.

The VRS shall provide alarm inputs to cameras.

The VRS shall provide flexible scheduling.

The VRS shall have a built in watchdog which will automatically restart after a power failure and begins to record as per its configured settings.

The VRS shall provide the ability to manually ‘back up’ recorded data to hard disk while the unit continues to record.

The video recordings shall be watermarked and encrypted. In addition, images backed up in bitmap or JPEG format, shall be in a manner so that they can be verified for authenticity.

The VRS shall support full duplex audio, complete with video / audio synchronization, analogue to digital conversion.

The VRS shall:
Manage live video from cameras
Transmit live video to Operator Stations
Receive camera control commands from Operator Stations and then send the commands to cameras
Store live video to hard disk
Transmit previously stored video to Operator Stations
Archive previously stored video to off-line storage media
Retrieve archived video from off-line storage media

The system should support the following analytics;

a) Camera sabotage
b) Loitering detection

c) Stopped vehicle / abandoned object
d) Directional motion / adaptive
e) Object counting
f) Object tracking
g) Object removal / missing object
h) Motion detection

Export the recordings into MPEG format so that it can be viewed using standard tools including Microsoft's Video Player.

Provide the following search functions

a) Date/Time search
b) Selection of time/date on graphical time line panel
c) Search by event by channel
d) Advanced event search with still image of event trigger
e) Sequence search – still image playback through multiscreen
f) Thumbnail – Thumbnail of time interval (programmable)
g) Object – search for motion in the stored video
h) POS/ATM search for specific POS/ATM data and associated video

Schedule programming multiple settings per camera, per day for record resolution, speed and quality.

Password protected with multilevel access, individual username and passwords for every user if required.

22.13 System Database Servers and System Operation

The Database Server (SDS) shall contain a database of all network-connected equipment and their configuration such as;

System configuration
Camera configuration and settings
Recording configuration and settings
Configuration of Quad Views and Sequences
Details of recordings
Schedules
Operator security details
Configuration of Surveillance and Alarm Monitors
Configuration of Video Analytics

The SDS system shall have the following features as a minimum.

Manage communication between the Operator Stations and the Camera Servers

Allow alarms/events internal and/or external to initiate recordings

Report any camera or other equipment failures.

Provide a full audit log of all system status.

The (SDS) shall be able to be used in a redundant configuration, using two separate Database Servers. The backup Database Server shall be continuously synchronised with the master Database Server to ensure that it is always up-to-date and ready for a fail-over, when required.

The minimum requirement for the rack mounted SDS is as follows.

Microsoft Windows 2012 R2, with 3 of 5 user SBS CALs giving a total user count of 15. System to be factory pre-installed onto server hardware specified as follows. Rackmount server, 2 off Intel Dual Core Xeon 2630-V2 CPU's, 12 GB RAM, dual 2 GB SCSI drive, dual power supplies, dual Gigabit Network adaptors. DVD-ROM drive, Backup Exec 10 for Window Servers. Includes the configuration of the server's network software to allow the subsequent linking of the serve to network, and the client-side network configuration necessary for the linking (physical and virtual) of a maximum of 15 other workstations to the network.

22.14 Monitors

Monitors shall provide high images of both high quality and reliability.

Key Features of Monitor

High definition
Resolution: 1920x1080
Scanning frequency: 60Hz
Light Source: LED
Duty Cycle: 24/7
240 Vac

22.15 Control Room

The Control Room shall be equipped with workstations. Each workstation shall be capable of monitoring a maximum of 16 cameras each. The centre shall monitor on a 24/7 basis. A slave controller and PC with dedicated software shall be used to control the system.

22.16 Equipment Rooms

The equipment room will house all of the equipment required to manage/control of the system and the video recording system.

22.17 Remote Monitoring

Where required colour monitors with keyboard, similar to the main Control Room equipment shall be provided in the operational staff / management offices for general/alarm viewing purposes only.

22.18 CCTV Masts

Where necessary custom-designed masts for external P.T.Z. cameras manufactured to specification.

The Contractor shall provide all bolts, erection, painting, and assembly.

The masts are to be fabricated from hot dip galvanised mild steel, primed and painted white.

Masts to include the base, mounting brackets for cameras, cabling, fibre.

Power and earthing will be supplied by others.

22.19 Weather Proof Housing

The Housing shall be made of extruded aluminium and weather proof to IP 66. The minimum internal dimensions of the housing shall be able to house both the camera and lens. The housing shall have a built-in cooling fan to cool the camera & lens. The housing shall allow an option to mount screen wiper and screen washer and water tanks.

22.20 Video Cabling

CCTV cameras are to use, Cat 6a and UTP network cable or optical fibre shall be used to connect the camera to the LAN access switches.

22.21 General System Operation

The operation will have a system that provides a real-time view of the status of the control system such as

limit and grant operator access to live and recorded video images.
send requests to record video
provide indication of any cameras or recordings which have failed
provide indication of any other equipment faults

The live output from cameras shall be viewed at the Operator Station as follows.

Single camera view
Quad view of up to 16 cameras
Sequence view of camera preset positions
Modifying settings for a camera
Modify recording settings for a camera
Adding and deleting cameras
Creating schedules for recordings and video motion detection
Modifying Video Analytics settings

Users shall be able to select a camera from a tree control listing the cameras available to the user.

The system shall also support multiple monitors in the following way:

Alarm monitor: When an alarm occurs, the live video output of the camera associated with that alarm shall be switched directly to an alarm monitor. The user shall be able to acknowledge the alarm to clear the monitor using the numeric keypad. Cameras that are directed to alarm monitors will not be removed from the queue unless explicitly cleared by the operator. It shall be possible to create a queue of alarm monitors to manage multiple alarm views simultaneously.

Cyclic Alarm Monitors: An alarm monitor shall be available at the end of a alarm monitor queue to cycle the camera views from unacknowledged alarms if the number of cameras to view exceeds the number of alarm monitors. Once the alarm monitor queue is filled, any new alarm will be placed in the queue relative to it’s priority and time of occurrence. Existing activated alarm camera views shall reshuffle to accommodate the new alarm. In the event that all the available alarm monitors are used, the oldest active alarm camera shall be added to the cycling alarm monitor. The alarm views shall cycle on this final alarm monitor until acknowledged and cleared by an operator in the event of multiple alarms added to this monitor.

Surveillance monitor: Operators shall be able to send any Quad View, Sequence View or Single Camera View to a surveillance monitor. User shall be able to clear the monitor using the numeric keypad.

Monitors shall be able to be configured to act as both Alarm and Surveillance monitors. In this case, the monitor behaves as a Surveillance monitor until an alarm occurs, in which case it shall show the alarm video. Once the alarm is acknowledged, the video previously shown (as a surveillance monitor) is displayed again.

In each of these cases, these additional monitors shall be either connected to an Operator Station using a multi-monitor PC card or to other PCs.

Operators shall have the following options.

View the live output from the selected camera.

Pan, tilt, zoom and focus the camera using a joystick attached to the Operator Station PC

Pan, tilt, zoom and focus the camera using a pointing device or joystick.

For cameras which support continuous pan, tilt, zoom (PTZ), a mouse shall be able to be used for continuous PTZ directly in the live video window. By dragging the mouse up or down, left or right in the video window, the operator shall be able to tilt the camera up or down, or pan the camera left or right. Zooming must also be provided using the mouse in a similar way.

Have a quad view consists of up to sixteen related cameras viewed simultaneously on a single display.

Have a sequence view consists of a single camera view, which can be cycled on a time basis. Pan-tilt-zoom cameras, which support preset positions, can have these presets cycled on a time basis. In this way an operator can view a variety of presets on a series of PTZ cameras. Fixed cameras can also be included in the sequence and cycled accordingly.

There shall be no limit to the number of cameras that can be assigned to a single Sequence View. There shall also be no limit to the number of available Sequence Views.

System Administration shall have the following options;

Shall be able to change settings for an individual camera. The details are grouped into several sections:

Camera Details
Camera Connection
Camera PTZ Control
Security
Camera Deletion

The parameters listed in the sub-sections below are configurable on a per camera basis and their specific selection on a particular camera(s) will not limit the ability to freely select other options on other cameras as required. It will be easy to change any of these parameters for each camera individually as and when required. Systems that do not allow changes to each camera's parameters on an individual basis will not be acceptable.

Camera details and parameters required are as follows.

Name
Location
Description
Camera Number (for fast numeric keypad call-up)
Camera Streamer Type
Resolution: The following resolutions shall be supported (depending on the functionality of the camera and camera streamer)
Megapixel (1280 x 1024, 1280 x 960 ,1280 x 720 and 1920 x 1080)
Video Image Rate: The supported image rates will be up to 30 images per second per channel but shall be scalable if slower rates are required
Choice of five levels of video compression, equally distributed from minimum to maximum compression
Streamer IP Address
Streamer Mac address
Choice of frame rate or bandwidth limited streaming
Unicast or multicast transmission of video
Allows certain users to view specified cameras
Delete camera from the system.

The user or administrator shall be able to configure the following parameters for each camera:

The amount of pre-recorded video that will be associated with a user request for recorded video. This will allow the Camera Server to capture video prior to the user request, as well as after the request. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.

Video quality required for user activated recording. It shall be possible to have different frame rates for user and event-activated recordings. Shall be selectable from the entire range of frame rates supported for the camera. For MPEG encoding, support shall be provided to record only the Index frames, or a subset of the Index frames.

User activated recordings shall terminate after this period. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes

The retention period that the video recording shall be retained before being deleted. The retention period of individual recordings shall be able to be changed on a per-recording basis. Shall be selectable from a list of values ranging between one hour and forever.

There shall be at least four priorities of alarms/events in the Security or Control System:

Event (journal priority)
Low priority alarms
High priority alarms
Urgent priority alarms

The following settings shall be individually configurable for each alarm and each camera:

The amount of pre-recorded video that will be associated with an alarm/event. This shall allow the Camera Server to capture video prior to the alarm/event, as well as after the alarm/event. Shall be selectable from a list of values ranging between 0 seconds and 15 minutes.

Post recorded duration after an event activated recording shall terminate from a selectable list of values ranging between 0 seconds and 5 minutes.

Video quality required for event activated recording. It shall be possible to have different frame rates for alarm activated recordings.

The retention period of individual recordings shall be able to be changed as necessary. Shall be selectable from a list of values ranging between one hour and forever.

In the case of multiple alarms/events relating to the same camera, a video clip shall be created for each alarm/event.

The following scheduled recordings shall be individually configured.

The system shall have the ability to schedule recordings for each individual camera for times in the future. For each scheduled recording the user shall be able to configure the following (with descriptions as per User Activated and Event Activated recordings):

Start time
Stop time
Frame rate for the recording
Retention period before the recording will be deleted
Recurrence (if this is to be a recurring schedule)
Description (at least 255 characters)

There shall be no limit on the number of schedules that can be entered for the system. There shall be no limit to the number of schedules per camera.

The system shall have the ability to provide continuous background recording from any camera(s) managed by the system. Background recordings will be stored as a discrete series of clips and will continue to operate in the event that communication between the Camera Server and the Database Server is lost. Once communication is restored, all relevant information will be updated to the Database Server.

For each camera the user shall be able to configure the following (with descriptions as per User Activated and Event Activated recordings):

Enable / disable background recording
Duration of the recorded clip
Frame rate for the recording
Enable / disable archiving of the clip and the period after which to archive
Retention period before the recording will be deleted
Enable or disable audio recording (if available)

Systems that require the configuration of multiple time periods to manage background recordings will not be accepted.

Continuous background recordings will not be dependant on network communications between the Camera Server and the Database server. Once configured, these recordings will continue to operate in the event that this communication is lost.

<u>The following analytics shall be individually configurable.</u>

Recordings must activate automatically based on events generated by the real-time analysis of video from any camera on the system that has Video Analytics enabled.

The system must support video motion detection algorithms. The enabling of Video Motion Detection shall be either:

on a continuous basis
scheduled for particular times, dates, days, months etc.

with the following functionality:

Detect and track objects
Learn the scene
Adapt to a changing outdoor environment
Ignore environmental changes including rain, hail, wind, swaying trees and gradual light changes

The amount of pre-recorded video, allowing the Camera Server to capture video prior to the detection of motion, as well as after the detection of motion. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.

Object Tracking

The system must have the ability to acquire and track an object within a predefined field of view on selected cameras.

The system must be able to provide the following functionality:

Detect and track objects
Learn the scene
Adapt to a changing outdoor environment
Ignore environmental changes including rain, hail, wind, swaying trees and gradual light changes

The system must provide every operator with the ability to record the current frame of video. This snapshot of video shall be stored as a bitmap file. The file name shall include the camera name, date and time of the recording to millisecond.

The system shall provide a simple search function for all video recorded. The user selects the time indicator which shows a calendar and time line. The user selects the required search period.

Once the time criterion is entered, the “search” is selected. Video recorded during the selected period will be returned by the search.

The user shall be able to search on combinations of cameras by clicking on an “Advanced Search” icon as described in the next section.

The system shall provide an advanced search of recorded video. The search shall be based on recording time, camera and recording details.

The user shall select from the list of cameras. It shall also include any cameras that have been deleted from the system but still have video stored on a Camera Server or on archived media. If a camera has been deleted and all video associated with the camera has been deleted, the camera name will not appear in this list.

The time criterion shall be selected from a calendar and time line control. Days containing recorded video shall be shown in bold on the calendar control. Cameras shall be able to be added and removed from the search list.

The user shall be able to choose to filter the search based on the following criteria:

Alarm or event type for alarm/event activated recordings
Recording type (schedule, event, operator, video motion detection, all)
Area
Point name
Event description
Operator name
Camera name or number
Any comments entered by users in the comments field of recordings

Wildcards shall be accepted for the Point ID, description, area, priority and value for alarm/event activated recordings.

The system shall show the results of the basic and advanced searches in a table format, such that the user is able to select columns within the list to sort the output.

The system shall have the ability to include audio with the video. Two types of audio support shall be provided:

Single directional audio from the field locations to the VRS
Bi-directional audio between the filed locations and the VRS

The system shall provide the following single directional audio support:

Audio shall be recorded by using an attached microphone
Audio shall be streamed along with the video from the camera locations to the VRS and Operator Stations using the same network used for the video stream. This shall require no additional network cabling
Audio shall be played at the Operator Stations using speakers connected to the Operator Station computer
Live audio shall be played whenever the live video is displayed
Audio shall be recorded whenever the video is recorded.
For scheduled and continuous (background) recordings, the audio shall be optionally disabled
Audio shall be played when the recording containing audio is played. The audio shall be heard in the same synchronization it was recorded in.
Wherever the audio is played with the video, a mute button and volume control shall be provided on the video player.
Recordings containing audio shall be exported with the audio and video in the same synchronization it was recorded in.

The recorded video shall be available to all users, which have adequate security as follows

Displays shall be provided to view recordings from any Operator Station. The operator can select the recording he/she wishes to view on each display,

The following information and controls shall be provided on this display:

A navigation panel to allow the user to select the required camera

A calendar control (similar to Microsoft Outlook) to select the desired date. All days which have recordings for the chosen camera shall be displayed in bold font.

A table listing all the recordings on the chosen camera for the chosen day. The user shall be able to select the required recording from this table. Each column shall be able to be sorted by selecting the column heading. This table shall display the following information as a minimum:

The time each recording was activated

The duration of each recording

The type of recording (operator activated, alarm/event activated, video motion detected, or scheduled)

The Operator or user that activated the recording (for operator activated recordings)

The Name, Description and Value of the Control System Server which activated the recording (for alarm/event activated recordings)

An embedded video player with controls (buttons) similar to a VCR (video cassette recorder). The information displayed on the video player and the controls provided shall include:

The time and date of the frame being displayed

A slider control which is used to move backwards and forwards through the recording

Play, pause and stop buttons

Step forward and step backward buttons, to move through the recording frame by frame

Fast forward and rewind buttons, to play the recording at speeds of x2, x4, x8, x16, etc (to a minimum of x1024).

A snapshot button, to allow for the frame being displayed to be stored as a bitmap file (in a similar way to the snapshot button for live video).

Information about the chosen recording. The following information as a minimum shall be displayed with the chosen recording

The type of recording (operator activated, alarm/event activated, video motion detection or scheduled)

The Operator or user that activated the recording (for operator activated recordings)

The Name, Description and Value of the Industrial Control System which activated the recording (for alarm/event activated recordings)

The sub-priority of the recording (for alarm/event activated recordings)

The frame rate that the recording was recorded at

The resolution of the recording

The compression used

The recording start time and date (including pre-record)

The recording end time and date

The date and time that the recording will be deleted by default (which can be changed as required)

Operator comments and notes about the recording (made by the scheduled recording configuration automatically or by an operator)

When a recording is displayed, the exact frame of video when the recording was activated shall be shown. The slider shall be positioned accordingly along with the frame time. It is not appropriate to show the first frame in the recording, as the recording may have pre-record.

Buttons to allow the operator to archive, delete or export the chosen recording

A button is provided to playback the recording at the recorded resolution. This shall be done using a display that pops up containing the embedded video control with full playback functionality as described above.

User actions on the Operator Station shall be recorded in a log file along with the Control System's actions. User actions include:

Interventions such as manual recording and configuration setting changes

Cameras viewed

Video replayed

Video exported

Cameras pan/tilt/zoomed and preset switching

This log must also contain a history of the status of the system components. It shall list the status of all cameras, streamers, servers and other system components including when they were disabled or failed.

The log of user and system actions shall be available in text format and automatically included with any video recordings that are exported.

It is a requirement for all exported recordings and exported audit logs to be digitally signed. This is required to prove authentication (origin of the recording and audit log) and integrity (exported recording and audit log have not been altered or tampered with).

The system shall provide a default digital certificate for signing the exported recordings and audit logs. Customization shall also be provided to allow for the user to supply his/her own digital certificate.

A utility shall be provided to display the exported recording, view the audit log and verify the digital signatures. A visual indication shall be provided to whether the exported recording and audit log have been altered or tampered with.

Watermarking of recordings is not an acceptable method to prove authentication and integrity as it alters the recording and audit log.

The system shall hold a configurable amount of video in online storage. The amount of video stored on-line shall only be limited by the NVR disk capacity.

For each Camera Server a limit on available storage space for on-line video shall be configurable.

The system shall support RAID 0, 1, 3 or 5 for video recordings (clips).

The system shall provide a flexible means to configure storage behaviour within the system administration displays. The system will provide an automated and configurable means to delete those remaining clips closest to their deletion criteria in order to increase available system storage. The disk space configuration will be separately configurable for each drive volume on each Camera Server.

Deletions will commence once the amount of available disk space decreases to below a configurable limit. Alarms will be generated by the system to warn operators of this action. It shall be possible to configure the following parameters for this purpose:

The Camera Server and volume being configuredThreshold values for alarm generation (2 alarms: low and very low)

Enable or disable automatic deletion of clips based on available disk space
The threshold value used to initiate the automatic deletion of clips
Inclusion or exclusion of clips marked for archiving in automatic deletions
Threshofld value to stop recordings when available storage is critically low
Threshold value to restart recordings when more disk space becomes available

The system shall provide a summary showing the available disk space, total disk space and number of recordings for directories used for this purpose on camera servers.

The system shall provide the ability to automatically archive all recordings. It shall be possible to automatically archive any type of recording at a preconfigured period after the recording has completed.

The following system tasks shall be performed from the Operator Station

View live video
Live video is automatically displayed on a monitor when an event occurs

Search through the stored video clips of a camera
An operator records an incident
An operator records a snapshot of the current viewed video
Add a new camera to the system
Change the configuration settings for a camera
Provide alarm/event activated recording from the integrated Industrial Control System
Search for video clips from different cameras
Create a sequence (camera tour)
Conduct a sequence (camera tour)
Create a quad view
View a quad view
View live video from a custom schematic
Add live video to a custom schematic
Configure, schedule and tune Video Analytics (video motion detection, object tracking & recognition and non motion detection)
View the audit log

It shall be possible to perform the following tasks in the Security Control Operator Station:

Acknowledge an alarm
Reset an acknowledged alarm
Control a security or control system point
Run a report containing security information
Run a report containing process control information
Respond to a security alarm
View security and control system information on a process control schematic
Configure a security report
Configure a point control schedule
Change an access level and download it to all affected access controllers
View Access Controller details

All alarms and events shall appear and be able to be managed from the same display on the Operator Station.

23. Access Control System

23.1 System Description

The Access control system comprises a central controller (rack mounted server based) located in the Security Control Room, connected to local controllers via the LAN (LAN provided by others). Local controllers connect to door controllers via proprietary protocol.

The Access Control shall comprise of the following;

- Master Controller
- Local Controller
- Door Controller
- Door Monitoring
- Readers (various)
- Door Locks
- Vehicular Traffic Booms
- Servers
- Software

23.2 System Operation Overview

The designated doors will be fitted with a combination of following components

- Door Monitoring
- Request For Entry Device
- Request For Exit Device
- Emergency Exit Device
- Locking Mechanism

Access controlled doors shall be fitted with a magnetically operated reed switch to monitor the position of the doors. The switch shall be closed when the door is closed and position monitored in control room.

Request for entry devices shall be installed on the non-secure side of the door.

Request for Entry devices shall be connected to data collection devices / access controllers, installed in convenient locations in dedicated riser shafts and/or control rooms

The system shall be capable of supporting a combination of;

- Magnetically coded [Wiegand or similar].
- Bar coded label.
- Magnetic stripe coded.
- RF ID Proximity Cards
- Smart Contactless cards
- Biometric Devices (fingerprint, retinal scan)
- Keypad

Request for exit devices shall be installed on the non-secure side of the door.

Request for Exit devices shall be connected to data collection devices / access controllers, installed in convenient locations in dedicated riser shafts and/or control rooms

`The system shall be capable of supporting a combination of;

- Magnetically coded [Wiegand or similar].
- Bar coded label.
- Magnetic stripe coded.
- RF ID Proximity Cards
- Proximity Cards.

- Biometric devices (fingerprint, retinal scan)
- Keypad
- Push Button
- Smart Contactless card

Green break glass units shall be installed where required to enable emergency egress.

Break Glass units shall be connected in series on the power supply to the locking device and connected to the intrusion detection system as an alarm input.

Electric locks shall be fitted to the doors in the various locations as shown on the drawings and/or schedules.

The doors shall be in the locked position during normal operation and it shall only be possible to open a door in one of the following ways:

- From the outside by presenting a valid card to the corresponding card reader and thereby activating the electric strike.
- From the outside by withdrawing the bolt from the strike with a key without activating the Electric strike.
- [Escape door] with a key in break glass box, audible alarm at door and alarm at control panel in the main security room.
- From the respective control room by a pushbutton that activates the electric strike and thus allowing somebody to open the door from the outside.

The electric strikes shall be suitable for intermittent duty i.e. the doors are normally locked and released only momentarily from time to time.

Electrically operated traffic control booms shall be installed in roadways and/or vehicle entrances to control the entry and exit of vehicular traffic.

Booms shall be fitted with a manual cranking device in the event of a power failure.

The motor and gearbox shall be capable of lifting and lowering the boom within a maximum of 15 seconds. Completely waterproof snap-action type limit switches shall be provided for control of arm positions.

A decelerating action shall be incorporated into the system to alleviate unnecessary wear to the motor and gearbox when the boom returns to its closed position.

The system shall incorporate a safety device that will, should the boom during its downward movement be obstructed by any object, stop the boom instantly to avoid damage to vehicles or persons.

The system shall stop the boom being manually lifted [other than cranking device].

Inductive loops shall be provided for opening and/or closing purposes. The loops shall be cut into the finished floor and sealed with a suitable sealer as approved by the Architect.

The control system shall interface with either an access card reader or a simple push button action.

23.3 Standards

SANS 17799
ISO/IEC 27002

23.4 Access Control Hardware

23.4.1 Master Controller

The Master Controller shall be a server based system and software.

The Master Controller shall provide processing and communications control functions for all devices attached to the system.

The Master Controller shall support capacities of up to 3 000 doors, 200,000 Cards and 500 Access Levels. All Cardholder records, Access Levels, Schedules and Configuration Data shall be stored at the controller level. When the central controller/PC is offline for any reason, the system shall, without performance degradation, retain full functionality. Each Controller shall store up to 100,000 local events in the log buffer when operating independently.

The Master Controller must have web based reporting facilities.

23.4.2 Local Controller

Each Controller shall include 64-bit processing power; up to 16 MB of RAM and employ flash memory firmware. Firmware upgrades shall be downloadable from the Host PC without a firmware chip change or attending at controllers in the field. All RAM will be battery backed by a replaceable lithium battery.

Controller shall supports RS-232, RS-485 and TCP/IP protocols for communications from the Master Controller. Each Controller shall support fully supervised bi-directional high-speed LAN communications for all controlled networks. These networks shall continue to function fully with a single short or a cut on any inter-controller connection and shall report the fault condition to the Controller.

The Controller shall draw power from any Reader Controller or input/output device in the local network and shall include built-in cabinet tamper functionality. A built in watchdog circuit shall monitor controller operation and perform an automatic system reset if a device controller loses complete power or is reset from a transient voltage surge.

Controllers shall have time saving installation and maintenance features including a silkscreen terminal legend, on board diagnostic LED's and quick Phoenix type plug-in connectors.

23.4.3 Door Controllers

The reader controllers shall support a minimum of 2 readers or 2 reader and keypad units using RS 485 communications at 38400 bits per second over a fully supervised 2 channel bi-directional loop to ensure data integrity in the event of a wiring short circuit or cut cable.

Reader Controllers shall have eight outputs, four per reader. All outputs shall be individually configurable from the central control (PC) to act as Normally Energised or Normally De-energised.

Outputs may be configured to act either as dedicated Access Point outputs (default mode) or to act as general-purpose outputs. In default mode outputs for each reader shall provide these functions:

23.4.4 Lock control

Door forced open that will remain on for as long as the alarm condition exists.

Door held open that remains on until the door closes.

Alarm shunt that remains on until the door relocks or closes - whichever is later.

Reader controllers shall have eight fully supervised inputs, four per reader. All inputs shall be individually configurable from the PC.

In default mode, input 1 shall be connected to a normally open or normally closed request to exit device and input 2 shall be connected to a door contact.

Each input shall be capable of reporting four states – alarm, restore, trouble which reports a short or circuit break, and illegal which reports measured loop resistance that falls outside of discrete valid state ranges.

Reader controllers shall support seven different input circuit types:

- Normally closed with two, one, or no resistors
- Normally open with two, one, or no resistors
- Normally open and normally closed circuit with one resistor that allows
- Normally open and normally closed contacts to reside on the same circuit.

Reader controllers shall have separate built-in regulated power supplies for locking devices, readers and auxiliary devices such as motion detectors. Lock, reader, auxiliary, AC and battery power functions shall be independently fused and supervised. The system shall support battery deep discharge protection and dynamic battery load testing with PC configurable frequency and duration.

Reader controllers shall employ digital filtering to minimise interference and to verify loop state changes before reporting. Input loop resistance shall be monitored continuously by a built-in analogue to digital converter, with status viewable from the PC.

Reader controllers shall provide a silk-screened terminal legend and quick Phoenix type plug-in connectors for easy installation and maintenance. On board status LED's shall indicate the status of all inputs and outputs, communication and run operations, AC high, AC low, battery trouble, lock fuse, reader fuse and auxiliary fuse. Cabinet tamper, lightning protection and fire signal supervision functions shall be built-in.

23.4.5 Input / Output Controller

The I/O controller shall support a minimum of sixteen I/O ports, all individually configurable as a fully supervised zone input or a dry contact relay output.

The controllers shall be capable of monitoring access control, alarm, elevator control, building control and other applications using RS 485 communications at 38400 bits per second over a fully supervised two channel bi-directional loop to ensure data integrity in the event of a wiring short circuit or cut cable.

I/O controllers shall support up a minimum of eight outputs. All outputs shall be individually configurable from the PC to act as Normally Energised or Normally De-energised.

Outputs shall be configurable for fail-safe mode operation. I/O controller outputs also support event "Counter" mode operation with a trip threshold range from 0 to 65,535.

Each input shall be capable of reporting four states – alarm, restore, trouble which reports a short or circuit break, and illegal which reports measured loop resistance that falls outside of discrete valid state ranges.

I/O controllers shall support seven different input circuit types:
- Normally closed with two, one, or no resistors
- Normally open with two, one, or no resistors
- Normally open and normally closed circuit with one resistor that allows normally

open and normally closed contacts to reside on the same circuit

Software shall enable any I/O port in the system to be globally linked to any other event, or programmed string of events, without restriction. Up to 10,000 links shall be configurable to trigger based on any event or chain of events, including, but not limited to following;

- Manual Intervention by an Authorised Operator
- Time Group Schedule
- Incidence of any Input Event
- Incidence of a logical combination of Input and Output Events
- Card Reader Links (presentation of any specified Card at any specified Access Point)
- Pending Commands (scheduled commands independent of any Time Group)

I/O controllers shall have a built-in regulated power supply for auxiliary devices such as motion detectors. Auxiliary, AC and battery power functions shall be independently fused and supervised.

The system shall support battery deep discharge protection and dynamic battery load testing with PC configurable frequency and duration.

I/O controllers shall provide a silk-screened terminal legend and quick Phoenix type plug-in connectors for easy installation and maintenance. Twenty-eight on board status LED's shall indicate the status of all inputs and outputs, communication and run operations, AC high, AC low, battery trouble and auxiliary fuse. Cabinet tamper, lightning protection and fire signal supervision functions shall be built-in.

23.4.6 Proximity Readers (RFID)

Proximity readers shall have an internal micro-controller, a transmitter, a receiver and a shared transmit/receive antenna. The identity of the tag shall be transmitted to the card reader controller via two data lines in Wegand format.

The reader shall read the encoded data from the access card and transmit the data back to the host panel, giving an audible and visual indication of a properly read card.

The card reader shall have a typical read range of 10 - 14 cm.

The card reader shall be a single piece unit, suitable for mounting onto a metal doorframe or mullion.

The card reader shall have wiring connections listed on the back of the reader.

The card reader shall have flush mount plugs to conceal all mounting holes.

Outdoor readers shall be vandal proof with a min IP 66 enclosure.

The card readers shall be CE listed and be FCC part 15 compliant.

When the card stays within the reader's field, the reader shall blink RED/GREEN to indicate that the reader is functioning properly.

When the reader is transmitting data, the LED shall momentarily turn colour to indicate that data transmission took place.

On a valid card read, Reader beeps and flashes AMBER (say), then goes GREEN (say) to signify acceptance of a valid card by the access control system.

Audible indicator (piezo) function shall be accomplished via a single wire.

LED colour shall be reversible via use of a colour changer card

The card reader shall have a hold line that will buffer a card read (when logic LOW) until the panel has asserted that the information can be sent up line (logic HIGH).

The card reader shall have a re-present mode in which the card must be taken from the reader field before being read again. This feature is required to eliminate multiple reads from a single card presentation.

The card reader must NOT be bit format specific and must be capable of reading 26 to 56 bits of data, as determined by programming of the proximity cards/tags alone.

The card reader shall be fully weather proof indoor/outdoor unit, and shall be capable of operating within a temperature range of -35 to +65 degrees Celsius, and an operating humidity of 0-95% non-condensing.

The card reader cover shall be made from polycarbonate material, and potted with a UL approved compound.

The card reader shall transmit and receive at a 125 kHz frequency. The reader and tag shall use combined ASK and FSK data modulation with built-in error checking.

The cable requirements of the card reader shall be a minimum five (5) conductor, 0.5 mm² stranded cable with overall shield, pigtail style.

The reader shall be able to function normally with 160m 0.5 mm² cable from a 5 V DC power source.

The proximity reader is metal compensated and therefore be able to mount on metal surfaces with less than 15% degradation of the reader's read range.

23.5 Software

23.5.1 Group Control

It shall be possible to manage access control and monitor activity of individual cardholders as well as groups of cardholders.

Group management functionality shall include the facility to administer an entire group of employers and/or visitors as a single entity.

Authorised shall be able to specify the zones and specific doors where cardholder groups will be allowed access. Specific time periods when groups will be allowed access to specific areas must be a programmable function.

It shall be possible to enable or disable a group. When a group is disabled access rights for the entire group shall be suspended thought the network.

23.5.2 Department Control

It shall be possible to define any number of departments.

The operation shall be similar to that defined for groups.

23.5.3 Employee Data

An employer management shall include the following minimum data fields:

.1 Personal Details – Title, name, surname, employee number, ID number, gender.
.2 ID cards/PIN numbers assigned to the employee
.3 Card validity, time and attendance logging options, access levels
.4 Photographs

.5 Contact details
.6 Department to which employee is assigned
.7 Zones to which employee has access
.8 Readers at which employee is allowed access
.9 Groups to which employee belongs
.10 Schedules specifying periods during which employee access card is valid
.11 In addition to the standard fields, five other users definable fields shall be available.

23.5.4 Card Assignment – Employers

Operators shall be able to assign an ID proximity hand from within the employee management module by presentation to the take-on reader connected to the workstation and to the network.

It shall be possible to assign multiple cards to a user with the option of assigning alliances to each card.

An authorised operator shall be able to issue a temporary card to an employee. When a temporary card is issued it shall inherit access control criterion previously defined for the employee

The permanent employee card shall become invalid for the period that the temporary card is valid with this period being definable.

The system shall consolidate time and attendance data for all cards issued to an employee.

The activation and expiration times shall be unambiguously specified in terms of seconds, minutes, hours, days, months and years.

It shall be possible to specify that cards expire at the end of the day that it was issued.

23.5.5 Visitor Management

A visitor management module will include the following types of information.

.1 Personal details
.2 Date and time when card becomes valid and period of validity
.3 Photographs
.4 Contract details
.5 Department that the visitor is visiting
.6 Five additional fields shall be allowed for user definable data.

23.5.6 Card Assignment – Visitor

Assignment shall be similar to the process described for employees. The following additional features shall be available.

Operators shall be able to specify that an employee accompany visitors. (Card Parenting)

It shall be possible to assign a visitor template to a visitor record that will make visitor details available to a specific operator prior to the arrival of the visitor.

23.5.7 Card Parenting

It shall be possible to link two cards/groups and control access by only allowing access if the relevant card parent is presented.

23.5.8 Image Capture

It shall be possible to capture or import digital images and associate them with cardholder records.

The software shall provide functionality-enabling operators to crop and resize captured or imported images.

23.5.9 Card Printing

Card printing shall be accessible directly from the access control software.

23.5.10 Access Control Templates

The software shall allow operators to assign a set of access control criteria by applying a predefined template.

Each template shall define the following parameters.

- Company/departments to which the template applies
- Zone and reach permissions
- Schedules specifying the periods for which the zone and reach permission are active
- Cardholder groups

When a template is assigned to a cardholder, the cardholder will intent his or her permissions from the access control template.

23.5.11 Visitor and Employee Take-on Stations

The software vendor shall provide a cardholder take-on module that enables users with limited computing experience to view, edit and add records to the employee and visitor database, and to assign cards to visitors or employees. The personnel take-on module provides functionality that allows operators to:

.1 Enter detailed information about visitors and employees using a set of administrator - configurable data entry screens.

.2 Preview input from a video camera connected to the take-on station, capture a frame, and link it to a visitor or employee data record.

.3 Capture voice samples using a microphone connected to the take-on station, and link voice samples to specific visitor data records.

.4 Ascertain the location of any visitor or employee by displaying a list of all cardholders who have passed through access points.

.5 Capture images at any size ranging from 320x240 pixels to 800x600 pixels and any aspect ratio between 800:1 and 1:800. (Administrators shall have the capability to specify limits for both the pixel resolution and aspect ratio of captured images.)

.6 Specify that a visitor shall be accompanied by a specific employee or any member of a specific group of employees (such as a company or department).

.7 Restrict a visitor to specified areas by assigning an access control template defining permissions for that visitor (as described in the section dealing with access control templates).

.8 Specify the period for which a visitor card is valid.

.9 Define templates for visitor or employee cards and select a different template for each card.

.10 Print personalised visitor and employee cards to a suitable printer connected to any workstation on the local area network.

.11 Control precisely the placement of multiple cards on a page.

The functionality available on a personnel take-on station will depend on permissions and configuration data assigned to a user group by the system administrator. Operators shall be required to log on to personnel take-on stations by entering user names and passwords, or by presenting a valid card at an ID reader that has been designated as a take-on reader for a specific workstation

23.5.12 System Alarm Management

The software shall provide tools for the configuration, monitoring and management of system alarms

Administrators shall be able to specify the security level on any alarm as critical, normal on low, enable or disable an alarm and configure an alarm to reset automatically.

Operators shall have access to an alarm viewer displays status of alarms in real time and allows the acknowledgement or reset by an operator.

The system shall allow schedules specifying period for which the alarm remains enabled to be attached to alarms.

23.5.13 System Monitoring

The software application shall incorporate modules that allow administrators and operators to monitor the status and performance of the system in real time. Specifically, modules shall be provided for the real-time viewing of access control events, system events, video inputs, the current location of cardholders, key system statistics, and system performance.

The access control event viewer shall list the last n ("n" specified by user) access control events that have been logged in the database. Users will be able to select which properties of an event are displayed and in which order they are displayed.

The system event viewer shall list the last n ("n" specified by user) system events that have been logged in the database. Users shall be able to select which properties of an event are displayed and in which order they are displayed.

A video viewer shall enable users to monitor video signals from the CCTV system.

A personnel locations viewer shall be provided to enable operators to ascertain the current location of any cardholder. This viewer shall provide information about the last reader at which a cardholder presented their card, or the last zone that the cardholder entered.

The system performance monitor shall allow users to set up real-time 2-dimensional or 3-dimensional graphical representations of transactions at any ID reader(s) defined in the system. It shall be possible to filter the data represented in a graph by selecting a day from a graphical calendar and selecting specific one-hour periods within that day. Users shall also be able selectively to display “access allowed” events, “access denied” events and “all events” in different colours. Additionally, users shall be able to preview and print reports by clicking on an icon in the performance monitor.

23.5.14 Zone control

The Access Control Software shall provide complete support for both reader based and zone-based access control models. The software shall enable administrators to define a zone by selecting doors that lead to or from the zone, and/or selecting other zones adjoining the zone. Administrators shall be able to assign enabling schedules to a zone to specify the time period(s) during which access shall be allowed to the zone.

The software shall provide the capability to enforce zone control by allowing access to a zone ("inner zone") only to cardholders who have previously been allowed access to an adjoining zone ("outer zone").

The system shall also capable of enforcing strict anti-pass back control by denying access to a zone if an employee or visitor previously entered that zone without subsequently exiting. It shall be possible for administrators and authorised operators to override the enforcement of anti-pass back control for any individual cardholder or group of cardholders.

23.5.15 Swipe sequencing

The Access Control Software shall enable administrators to define complex access permissions by configuring the system to require a specific sequence of up to five (5) card reader transactions before allowing access at a reader. For each transaction in a swipe sequence, it shall be possible to specify that a card presented by a specific cardholder, any member of a specific group, any cardholder with a specific access level, or any valid cardholder present a card.

Swipe sequencing shall be integrated with the system's event and action control functionality, thus allowing administrators to configure different sets of actions for each transaction in a swipe sequence.

23.5.16 Reader monitoring

Operators shall be able to invoke a reader-monitoring module directly from the main menu of the Access Control software application. Users shall be able to select from a drop-down list any reader defined in the system. The reader monitoring module shall indicate the date and time of the last access control transaction at the selected reader, as well as the name and photograph of the cardholder who effected the transaction. It shall be possible to access the cardholder's record in the Access Control database by clicking on a button in the reader-monitoring window.

Duly authorised operators shall be able to view and edit all fields in the cardholder's database record (as specified elsewhere) or remove a cardholder record from the database.

23.5.17 Random search functionality

Authorised operators shall be provided with the capability to define random stop-and-search procedures at any reader. For each reader, it shall be possible to enable random search separately for employees and visitors. Administrators shall be able to specify that a percentage of all cardholders, every nth person, a specific cardholder, or all members of a specific cardholder group be searched.

The random search facility shall also allow administrators to specify that a cardholder that has been identified for searching be denied access at the reader and/or be marked for searching at other readers where random searching has been enabled.

The software shall allow administrators to assign a schedule specifying the period(s) during which random search functionality is active at a reader.

23.5.18 Time control

The Access Control Software shall allow users to configure timers and triggers schedules that control the execution of actions, as well as period schedules that specify the validity of access control permissions.

Timers

It shall be possible to define timers to control the behaviour of system objects. Users shall be able to specify the duration of a timer in milliseconds; start, stop or reset a timer in response to any event generated in the system; specify actions to be performed when a timer expires; and configure a timer to restart automatically after expiring.

23.5.19 Trigger schedules

Trigger schedules shall provide the capability to generate events that execute programmes or control the behaviour of objects defined in the system. Each trigger schedule shall comprise one or more time entities, each of which shall trigger events in one of the following ways:

.1 At a specific time on a specific day
.2 Monthly at a specific time on a specific day of the month
.3 Weekly at a specific time on a specific day of the week
.4 Daily at a specific time on one or more days of the week
.5 Hourly at a specific number of minutes after the hour

Intrusion alarm control

The Access Control Software that includes Intruder Detection shall allows users to define an unlimited number of independent intrusion alarm systems, each comprising one or more user-defined alarm zones.

It shall be possible to link any available digital input point to any alarm zone and to employ any such input point as an alarm trigger. It shall be possible to raise an intrusion alarm event in response to the status of any input point, or any valid combination of object properties.

The system shall allow any alarm zone to be specified as an entry/exit zone for an intrusion alarm system associated with that alarm zone.

The system shall allow the configuration of panic inputs, i.e. alarm points that remain active regardless of whether the intrusion alarm system is armed or disarmed.

The software shall allow administrators to enable the arming of an alarm zone in response to any valid sequence of system events, including the presentation of a specified access card or the entry of a specified keystroke sequence at a specified reader.

Administrators shall be able to configure automatic arming and disarming of an intrusion alarm system by attaching appropriate schedules to the intrusion alarm system.

When an intrusion alarm zone is in an armed state, the system shall allow access to the zone only to personnel who are authorised to activate/deactivate the alarm system.

Offline functionality

The system shall be configured in such a way that it continues to function in offline mode. This is to be accomplished through the provision of local intelligence in the form of communication and reader network controllers, which shall store all necessary transaction information locally until communication with the local computer and network is restored.

As mentioned in the section of this specification pertaining to hardware, the RS 485 reader network shall have the capability to detect a break in the line of communication to the host computer, switch automatically to offline mode, and switch back to online mode as soon as communication with the host is restored.

When communication between the host computer and a RS 485 reader network is restored, the offline access control management module shall retrieve the transaction logs maintained by the host computer or local controllers in offline mode, and upload the retrieved data to the central Access Control database.

Data administration and backup

Users shall have the ability to import employee and visitor data from a variety of standard data sources.

The system shall automatically identify duplicate data entries, alert the user to the existence of such duplicate entries, and prompt the user to select, which entries should be retained and which entries should be discarded.

The Access Control Software shall provide tools that enable users to verify and maintain the integrity of the system database. The data integrity tools shall identify invalid schedules, employees belonging to more than one group, duplicate input or output addresses, and connections to addresses on undefined readers.

The software vendor shall provide tools that allow system data to be backed up and restored automatically. If such backup and restore facilities are not provided as part of the Access Control Software, it will be incumbent upon the system installer to design and implement appropriate backup procedures.

Report Generation

The reporting module shall be able to be executed from any PC with a TCP/IP connection to the host computer on which the Access Control Software is installed. At a minimum, it shall be possible to generate the following reports:

.1 Access control events
.2 System events
.3 Basic time and attendance
.4 Locations of cardholders
.5 Employee details
.6 Employee summary
.7 Visitor details
.8 Card Parenting (no limit)
.9 Visitor Linking to Staff
.10 Visitor and Tour Group Linking
.11 Visitor summary
.12 Company details
.13 Company summary
.14 Zone details
.15 Zone summary
.16 Door details
.17 Door summary
.18 ID reader details
.19 ID reader summary
.20 Digital input details
.21 Digital input summary
.22 Digital output details
.23 Digital output summary
.24 Timer details

23.6 Access Control Standard Requirements

The following technical requirements are to be read in conjunction with the specific requirements as clause 23.1 to 23.6.

23.6.1 Data Bus Communications

General data bus parameters

The Main Control Panel shall communicate with all remote devices by Modbus RS485 (or other approved protocol). Main Control panels will communicate with each other via the TCP/IP Network.

The data bus shall be cabled in Belden 8723 or equivalent (shielded, twisted, 2 pair). The shield shall be connected to the common earthing point, but strictly at one end of the cable. When the data bus stretches across different buildings, all the DGPs with power supply should be connected to the safety earth with a separated earth cable of no less than 2.5mm² connected to ground at a common point.

The Main Control Panel shall have the capability of monitoring and reporting all POLL errors from remote devices. This error count shall be resettable and shall be able to display numerically all errors per device.

Area Control and Monitoring

Area Partitioning

The Main Control Panel shall be capable of partitioning the site into at least eight (16) user definable areas for managing the unique requirements of each building or site. Each area may be operated as an entirely separate security system, or be programmed as a separate section of a common building.

Area Operation/Control

For each area, it shall be possible to have at least the following:

Assign a name to describe each area for control purposes

1. Provide each area with individual entry and exit timers
2. Enable some areas to be armed together with other areas but to be disarmed independently (area link).
3. Enable all areas to be armed by any user/s
4. Enable all areas to disarmed by any user/s
5. Enable all areas to be controlled using Access Control events such as ‘Access Granted’, ‘Region Counting’ and different Badging techniques.
6. Any or all areas arm automatically via a time zone or other specific system event
7. Any or all areas disarm automatically via a time zone or other specific event
8. Areas to monitor the status of other areas and then follow suit
9. Prevent areas from being armed if inputs assigned to that area are open
10. Prevent areas from being disarmed if inputs assigned to that area are open
11. Arm or disarm any or all areas by any system condition
12. Report to Central Monitoring Station, if any area is disarmed outside a time zone
13. Activate an event/output if any area is disarmed
14. Activate an event/output if any input in the assigned area is open
15. Activate an event/output if any input in the assigned area is inhibited
16. Activate an event/output if any input in the assigned area is in alarm
17. Activate an event/output if the area is in exit time
18. Activate an event/output if the area is in entry time
19. Activate an event/output if any area is to automatically armed (as warning)
20. Activate an event/output if any duress input is in pre-alarm mode

System Area Reporting – Local

The status of every area shall be shown clearly on the RAS. The Main Control Panel shall be capable of displaying the status of individual areas on card readers, LED RAS units as well as third party equipment such as consoles and mimic panels etc, by using the system outputs. System area status may also be controlled and monitored by the Host PC.

System Area Reporting – Remote

The Main Control Panel shall be capable of reporting to the Host PC and/or the Central Monitoring Station a change of status of any area. Areas may individually send open/close reports or may be grouped so that when all areas within one site are armed, then a collective closing report is sent. If the Main Control Panel is connected to the Host PC via a permanent connection, then the status of each area shall be dynamically updated and monitored.

23.6.2 Area Control

The Main Control Panel shall be capable of assigning to each area a unique four (4) to six (6) digit account code for the purpose of administration at the Central Monitoring Station.

Each Main Control Panel shall support both Intelligent and Standard Access Control functions. The Main Control Panel may manage, using Single Door Controllers or Smart Card readers, up to sixteen (16) standard Doors. The Single Door Controllers retain up to twenty (20) pre-programmed Users in the event of a communications failure with the Main Control Panel. Door access is restricted based on Door Groups

Arming and disarming with a card ('three times badging')

The Main Control Panel shall enable to control alarm areas using the Card Reader Access Granted to disarm and the 'three times badging' (three consecutive card presentations within ten (10) seconds time) to arm.

1. Request to Exit

   All doors shall have Request To Exit capability.

   Intelligent Door Controllers utilize Distributed Intelligence and are used to provide up to forty eight (48) intelligent access controlled doors connected to the Main Control Panel. The door controllers are also connected to the Main Control Panel via the RS485 data bus. All Intelligent door controllers shall communicate via poll & reply messages and send all alarms and events to the Main Control Panel for processing. They shall be fully housed in approved metal enclosures with tamper monitoring to detect removal of the cover, and leverage of the unit from the wall.

2. Operating Voltage & Current

   Controllers shall contain an on-board power supply with battery charger and obtain power from a 230V 50Hz/23VAC 5A transformer, which is enclosed in a polyester controller housing.

3. Communications Loss

   The entire intelligent access control system shall operate in real time mode and use distributed intelligence architecture. In the event of a communications failure between a door controller and the Main Control Panel or the failure of the Main Control Panel itself, the door controller shall continue to function as normal with no degradation in performance or response times of card and/or PIN reading, alarm activation or logic events of devices or programs associated with each controller. Additionally, all relay and open collector outputs as well as alarm sounders shall function as normal.

   In the "Off Line" state all controllers shall retain at least one thousand (1000), time and date stamped access events, which shall be immediately uploaded to the Main Control Panel and Host PC (if connected) when communications are restored.

   In the "Off Line" state, Anti-Passback and region related functionality shall only be available locally.

4. .Inputs / Outputs

   Each door controller shall have the capacity to control a minimum of four doors and monitor sixteen (16) EOL supervised inputs in the same manner as described for the Main Control Panel. These inputs may be selectable for two or four state monitoring. The door controller shall have four "on-board" relays for controlling door locks and be capable of expanding to forty eight (48) outputs.

Inputs available on the door controller shall be available also for normal intrusion alarms (i.e. a door contact used to detect if the door has opened for access control may also act as a normal intrusion zone in case the area is armed).

5. Reader Connections

Each Door Controller shall as a minimum also be capable of connecting up to four ‘Wiegand format’ or ‘Magnetic Stripe’ card readers using the four (4) on-board interfaces and may control a total of sixteen (16) Single Door Controllers as Wiegand interfaces, Smart Card readers or RAS units on a local data bus if more units are required. This enables the use of up to twenty (20) devices on each door controller to control the four (4) doors. The maximum distance between readers and the controller on the local data bus shall be one thousand five hundred (1500) m.

6. IN and OUT Readers

The on-board interfaces act as IN readers only. For OUT reader functionality Single Door Controllers are required, connected to the local data bus.

The readers on the local data bus shall behave as IN or OUT reader based on the address setting.

7. Reader LED Options

It shall be possible to program the LED on proximity readers to reflect the status of the door and/or areas assigned to the door such as the following;

- LED 1 ON Door is locked
- LED 1 OFF Door is unlocked
- LED 1 ON Area/s assigned to the door is/are armed
- LED 1 OFF Area/s assigned to the door is/are armed Dual state LED’s
- LED 2 may indicate area armed or disarmed by different colours
- LED 2 may indicate user valid or void status
- LED 2 may be controlled by macro logic equations to reflect any condition

8. Macro Logic

Each door controller shall be capable of running up to forty eight (48) programmable logic equations for any general-purpose requirements. The equations shall be capable of activating any output/s, input/s and/or events on the respective door controller. Any system event (up to four) can be included in each equation with each capable of being programmed as -

a. AND
b. OR
c. NAND
d. NOR

The result of the equation may activate either another output or an input for any of the following conditions;

e. Non Timed (Follows the result of the equation only)
f. On Pulse (Activates for the programmed time or the active period of the equation)
g. On Timed (Activates for the programmed time irrespective of the active period of the equation)
h. On Delay (Activates after the programmed time unless equation is no longer active)
i. Off Delay (Follows the equation but remains active for a time after the equation becomes inactive)
j. Latched (Activates on any of the first three inputs in the equation and is reset by the fourth)

Standard Features

Door Controllers shall have the following features as a minimum;

- Enable full integration and control of alarm areas using Intelligent Controller's facilities such as Card Reader Access Granted, Region counting, Macro Logic and programmable card badging techniques.
- All users stored locally on all Door Controllers.
- Disable access through specific doors or locations depending on the status of the alarm area behind the door.
- Allow up to sixteen (16) reader and/or Pin devices to control the four doors on each controller.
- Monitored siren output, which may be activated by any input or system event
- Forced Door monitoring on all doors
- Door Open Too Long Monitoring on all doors
- Early warning output (to drive beeper or local device) before actual DOTL alarm activates
- Enable reader LED's to follow area status, and door lock/unlock conditions
- Monitor status of doors (open or closed)
- Monitor status of door locks (locked or unlocked)
- Enable PIN and card badging for high security applications
- Enable all doors to be interlocked with any or all doors in the same 4DC
- Define a time period when doors are open (override timezone). Optionally the doors will only open after a valid badge inside the specified time period opens the door.
- Define a period when Card & PIN access only requires Card OR pin (Low Security Timezone).
- Anti-Passback with 2 modes;
- Mode 1 – Soft: Card will open door 2nd time but will generate an alarm
- Mode 2 – Hard: Card will not open door 2nd time and alarm generated
- Enable Dual Custody, where two different cards are required to gain access
- Enable Privileged cards to override Anti-Passback and disabled readers
- Enable up to sixty five thousand five hundred thirty five (65,535) users when controller is "off line"(Using IUM modules)
- Be programmed to count the number of users entering and leaving specific regions within the complex. Region count limits may also be set.
- Door Unlock, DOTL & Shunting timers can be increased, for physically challenged users
- Report Low Battery, AC Fail, Fuse Fail, Siren Fail and tamper to the MCP
- Disable RTE and exit PIRs when area/s associated with reader is/are armed
- Termination Link that places 470 Ohms resistor across data bus for balancing impedance
- Dynamic Battery testing during scheduled periods with variable duration
- On-board LED's to display TX & RX data between Main Control Panel
- Tamper switches to be monitored without taking up an input number
- Support multiple System codes with programmable offsets
- Software shunting of door inputs for variable times
- Enable area control by card badging sequences
- Supply 12 Volts DC @ 2A for auxiliary devices
- Forty eight (48) Macro Logic equations
- Enable operation of pulse release locks
- One hundred twenty eight (128) Door Groups
- Twenty four (24) Time zones
- Sixty four (64) Holidays

a. Each door controller shall have the capability of enabling or disabling Request to Exit (RTE) functions on all doors by the following methods;

o	Time Zone	- allows RTE only during any of the 24 time zones
o	Area Armed	- Restricts RTE when area associated with door is armed

b. It shall also be possible to keep the door unlocked for the duration of the RTE button being pressed or for a pre-programmed time. RTE buttons may be assigned to shunt inputs only without door control.

Door Access

Door access shall be restricted based on door groups.

23.6.3 Readers

RF ID Card Readers

1. Range

The RF ID readers shall have a minimum read range of six (6) centimetres.

2. Physical Parameters

The readers shall be suitable for use in indoor and outdoor applications. The reader shall have an IP rating of 65.

3. Colour Options

One reader shall be available with optional snap-on covers in five (5) different colours.

4. Communications

The reader to Door Controller communications shall be selectable between a selected protocol and RS485 data bus protocol. The reader shall automatically revert to a selected communications if a RS485 data bus is not detected.

5. Communications Loss

When communicating as an RS485 data bus device a loss in communications will automatically generate a 'RAS Communications Fail' alarm on the MCP and, if attached, on the Host PC. The specific device number must also be annunciated at the MCP, Host PC and/or Central Monitoring Station.

6. Tamper

The readers shall have a built-in Infrared Tamper detection feature. This facility enables the reader to activate an output or generate an alarm if it is removed from its mounting position.

7. Indicators – Visual

The readers shall contain both a Red and Blue LED indicator light. The LED indicators may be programmed to represent several system functions including door lock status and Alarm Area status when connected to the RS485 databus. When connected using Wiegand communication, the Led's are activated through hardwired inputs.

8. Indicators – Audible

The readers shall contain an audible indicator, which gives users verification when a card is presented to the reader.

9. Security

The readers shall utilize RF ID technology. This technology will enable a four (4)-byte security code (4.2 billion combinations) to be downloaded into the cards, readers and programmers to prevent illegal card duplication from one system to another. It shall also be possible to acquire a guaranteed unique four (4)-byte code from the card reader manufacturer.

This technology shall also feature a read/write encryption protocol that changes the card data each time it is presented at a reader.

10. Programmability

The readers and cards shall be programmable from the Host PC running the Security Software.

Secured mode operation shall require the use of a configuration card to insert the security code in the reader. Configuration cards are special cards programmed with a smart card programmer.

11. Card & Reader Credit Applications

a. The same readers, cards etc. shall also be suitable for 'Credit' or 'Pay per Use' applications.
b. Using the same software as listed in the previous section and connected to the same
c. PC Management Software, the card readers may be configured to deduct specific numbers of credits from one of four banks on each card or fob. When a valid read occurs, the card reader will deduct the pre-programmed number of credits and activate its open collector output to pulse, time or latch.
d. The cards and fobs may have credits added, deducted and confirmed by using the same programmer and PC Management Software.
e. Up to sixteen (16) Access Levels and four (4) locations may also be assigned to the card & readers to add restriction capabilities on the usage.
f. When used in credit applications, the readers may operate in a totally stand-alone mode. If audit tracking of usage is required, the readers may be connected, in RS485 data bus mode, to the Main Control Panel and Host PC if attached.

23.7 Central Control Software

1. General Overview

The Main Control Panel shall support one hundred and twenty eight (128) programmable Alarm Groups, up to one hundred and twenty eight (128) Door Groups and up to sixty four (64) Floor Groups. Each user may be assigned to any or all of these group types:

- Alarm Group - For control of area/s and alarm inputs and system administration
- Door Group - For access to nominated doors
- Floor Group - For access to nominated floors

2. Alarm Groups

The Main Control Panel shall have a minimum of seventy four (74) Alarm Groups, expandable to one hundred thirty eight (138). The first ten (10) shall have fixed pre-defined options. Alarm Groups shall have any or all sixteen (16) areas of the Main Control Panel and allow for total flexibility in the method of control and system operation for any user. Alarm Groups shall be programmable via any LCD RAS on the system. Alarm Groups shall have the following features as a minimum;

Define a time period using time zones during which alarm groups shall be available.

- An alphanumeric name may be assigned to each group
- Any or all areas may be assigned to the group

- Be a non user group for system functions only
- Enable the display, or hiding of areas within the group to users at RAS units
- Allow keyboard duress at any RAS for any user
- Prevent inhibited inputs from un-inhibiting when area disarmed by user
- Enable some areas to be armed and reset only by users
- Enable some areas to be disarmed only by users
- Enable some areas to be reset only by users
- Enable open inputs to automatically inhibit when areas are armed
- Enable forced arming if areas have open inputs that shall generate an alarm when armed
- Prevent disarming areas have open inputs that shall generate an alarm when disarmed
- Enable certain areas within the group to be armed/disarmed/reset automatically
- Enable access to any or all menu functions to users
- Capable of being active only when a pre-programmed time zone is running
- Have up to two alternate groups for non active periods
- Enable “Dead-man Alarm” functions
- Enable users to stop voice reporting
- Enable users to change their own code

3. Door Groups

The Main Control Panel shall have a minimum of ten (10) Door Groups, expandable to one hundred twenty eight (128). Each group may contain any or all doors on the system and restrict access to any or all doors via time zones. Users may be assigned a door group only, or, an alarm group as well as a door group. Door Groups shall be programmable via any LCD RAS on the system.

4. Floor Groups

The Main Control Panel shall have a minimum of sixty four (64) floor groups. Each group may contain any or all floors on the system and restrict access to any or all floors via time zones. Users may be assigned a door group only, a floor group only, or an alarm group as well as a door and/or floor group. Floor Groups shall be programmable via any LCD RAS on the system.

5. Reset Capabilities

The Main Control Panel shall be capable of resetting any or all alarm events automatically and sending a report to the Host PC and/or Central Monitoring Station that a resetl has occurred.

6. Time Zones

The Main Control Panel shall be capable of supporting twenty four (24) hard time zones, one (1) Service time zone and fifteen (15) software time zones that follow the status of nominated outputs. Each hard time zone shall have four (4) sub-zones and be programmable for seven (7) days a week as well as twenty four (24) different holidays (sixty four (64) if any memory extension fitted).

7. Outputs

The Main Control Panel shall be capable of mapping any output to any event. Outputs may be dry contact relays or open collector outputs and may be enabled or disabled by any time zone as well as be inverted.

The status of outputs may be altered by programmable logic reflecting system and area status, system events as well as the status of other outputs.

8. Area Linking

The master control panel shall be capable of having areas linked for arming or disarming an area based on the status of other areas. It shall be possible to program the system so that any area/s that change state will automatically force the linked area to follow and change accordingly.

9. Input Shunting

The Main Control Panel shall be capable of supporting up to sixteen (16) shunt timers for the purpose of inhibiting alarms for a set period of time. Timers, input activation or output status may activate shunts.

All shunts shall have variable timers and be capable of activating an early warning output (shunt is about to expire) as well as general output (shunt is active).

It shall be possible to program all shunts to activate in both disarmed and/or armed modes as well as entry and exit shunting. Door open commands may also start shunt timers.

Shunting shall start when a nominated output is active (e.g. a door opened).

It shall be possible to cancel any shunt timer as soon as the allocated input is closed.

10. Card Display

The Main Control Panel shall be capable of displaying the details of the last card presented to a reader connected to the data bus. Both the system code and card number as well as user number shall be displayed on the LCD RAS unit.

11. Built-in RS232 serial port

The Main Control Panel shall feature a built-in RS232 serial port connection to a PC. The connection shall be timed to maximum four (4) hours.

12. Printer Control

The Main Control Panel shall be capable of printing to a dot matrix, bubble jet or laser printer in RS232 mode with programmable baud rates, data lengths, parity and stop bits. The Main Control Panel may print access events, alarm events or both. Printing shall be allowed on a 24-hour basis or restricted via a time zone. When the time zone is active, no printing occurs and all transactions are kept in the system buffer.

It shall be possible for an authorized user to reset the system history from a RAS.

13. Dynamic Battery Testing

The Main Control Panel shall be capable of starting a Dynamic Battery Test. This may be done manually or automatically. During the test, the Main Control Panel and all auxiliary devices are powered from the battery. The test frequency shall range from each day to once a month with a programmable start time. Duration shall range from one (1) to two hundred and fifty five (255) minutes.

It shall be possible to program the same test for each controller and DGP and display a report of any failures. Failed tests shall also report to the Host PC and/or the Central Monitoring Station. If the Main Control Panel or any other device fails, then AC power shall be restored immediately.

14. Custom Text Message

The Main Control Panel shall be capable of displaying a thirty two (32)-character message on all LCD RAS units. An alternative message may override the custom message if an input is activated or inhibited.

15. Programmable Maintenance Message

The Main Control Panel shall be capable of displaying, at programmed times, a custom message indicating maintenance is due.

16. Programmable System Event Flags

The Main Control Panel shall be capable of grouping system events into a common output.

17. Macro Logic

The Main Control Panel shall be capable of running up to twenty four (24) programmable logic equations for any general-purpose requirements. The equations shall be capable of activating any event flag/s and/or input/s.

Any outputs or event flags (up to four) can be included in each equation with each capable of being programmed as;

a. AND
b. OR
c. NAND
d. NOR

The result of the equation may activate either another event flag or an input for any of the following conditions;

a. Non Timed (Follows the result of the equation only)
b. On Pulse (Activates for the programmed time or the active period of the equation)
c. On Timed (Activates for the programmed time irrespective of the active period of the equation)
d. On Delay (Activates after the programmed time unless equation is no longer active)
e. Off Delay (Follows the equation but remains active for a time after the equation becomes inactive)
f. Latched (Activates on any of the first 3 inputs in the equation and is reset by the 4th)

23.8 Security System Management Software

Summary

This specification includes a general description as well detailed functional and technical requirements for Security System Management Software (SSMS). The SSMS shall be a multi-user, multi-tasking system based on Microsoft 2000 / 2003 Server operating system and Microsoft SQL Server 2000 database technology.

Section Includes

The SSMS described in this specification is capable of operating with the access control system and sharing a data base with the entrance control system.

Architecture

1. The SSMS software shall consist of personal computer-based software capable of integrating multiple security functions; including management, control, and monitoring of access control events, access, intrusion alarms, photo ID card production, interfacing with database subsystems.

2. The SSMS software shall be a true 32-bit multi-threading client/server application, designed Microsoft Windows 2003 Server platform; with multi-user and multi-tasking capability, developed in a high level “C” language.

3. The SSMS shall use Microsoft SQL 2000 database, certified for the Microsoft Windows 2000/XP/2003 server platform. MSDE shall be part of the SSMS software package.

4. The SSMS shall conform to the standard TCP/IP networking communications protocol between the application/database server, operator workstations, control panels, video surveillance system(s) and database subsystems; using 10/100Mb Ethernet connectivity over LAN/WAN network typologies.

5. The SSMS shall be flexible and scalable in architecture, permitting expansion of both capacity and functionality, to be implemented progressively as needed, through software licensing and/or software upgrades.

6. The SSMS shall provide a real-time display of all system status and data, at all operator workstations.

7. The SSMS shall monitor status and record activity throughout the system for access, intrusion; visually and audibly annunciate alarms upon change of status, for assessment and response at all operator workstations.

8. The SSMS shall monitor and record activity throughout the system for access control, intrusion, fire events, and operator activity to an online history/archive database for reporting. A database-reporting interface shall be accessible from all operator workstations.

9. The SSMS shall operate spanning across multiple time zones with automatic adjustment for daylight savings time. The host server, operator workstations, control panels shall be capable of residing in different time zones while processing, recording, and displaying activity occurrences in their respective local time.

10. The SSMS shall employ distributed processing technology, allowing the host to function almost entirely as an application/database server. The majority of the real time, day-to-day decisions shall be made locally by intelligent control panels. The control panels shall be the direct field interface for all access control, intrusion alarm and fire alarm sensing, and input/output-controlled devices.

11. The SSMS shall manage and automatically download in real-time. All database changes made from all operator workstations, to the control panels that require notification of the specific database changes or updates.

System Capacity

Provide total system capacity to accommodate the following:

1. A minimum of two thousand (2,000) access control badges shall be available in the SSMS , upgradeable to one hundred thirty thousand (130,000). Intrusion and Access Control panels shall hold a maximum of sixty five thousand five hundred and thirty five (65535) access control badges. Multiple access control badges assignable per badge holder, each tracked separately. Access control cards shall be unique 4 to 20-digit numbers without facility code dependency or up to 48 bits using RawData formats.

2. A minimum of hundred and twenty eight (128) readers for access control or intrusion control shall be available, upgradeable to four thousand ninety six (4,096).

3. A minimum of two hundred and fifty six (256) alarm inputs shall be available, upgradeable to sixteen thousand three hundred and eighty four (16,384).

4. A minimum of two hundred and fifty five (255) Relay or Open Collector outputs shall be available, upgradeable to sixteen thousand three hundred and twenty (16,320).

5. A minimum of one (1) Fire Alarm System up to five (5) shall be available. Each Fire Alarm System shall be equal to one networked Fire ArcNet. Each Fire Alarm System shall allow for

a minimum of thirty two thousand (32000) detectors and a minimum of fifteen (32) Fire Alarm control panels.

6. A minimum of sixty Four (64) Intrusion & Access Control Panels.

7. A minimum of five (5) concurrent workstations shall be available upgradeable to ten (10).

8. Centralized on-line storage of historical transactions shall allow for a minimum of one million (1,000,000) events. The maximum shall only depend on the physical hard disk size and the use of MSDE or a full MS SQL 2000 server edition.

9. Twenty four (24) concurrently active time zones shall be available per integrated intrusion/access control panel.

10. One hundred and thirty eight (138) concurrently active intrusion control alarm groups shall be available per integrated intrusion/access control panel.

11. A minimum of four (4) independent intrusion areas shall be available per panel up to one thousand and twenty four (1024) in total.

12. One hundred and twenty eight (128) access control door groups per integrated intrusion/access panel.

13. Intrusion Alarm control is controlled through alarm groups and provided through any keypad or reader inside one local integrated intrusion/access control panel.

Computer Requirements

The server and PC with the following minimum requirements will be provided by others for use by the contractor.

SSMS Software – Server

Server

The system server and redundant server computer with a minimum of the following minimum hardware will be provided by others:

Processor	– Dell Power Edge R740
Cache Memory	– 30 Mb
Memory	– ODR3 / 16 slots with 12 No. SATA 2 Tb 2.5 inch hard drives
Graphics	– 64 bit HD graphics card
Power	– Power Management System – dual supply
Software	– Windows Business 2012 SLQ database

SSMS User Workstation

The system shall be capable of supporting up to 40 simultaneous Operator Workstation connections using a TCP/IP Local Area Network (LAN) subject to hardware capacity on the server computer.

The Operator Workstation with the following minimum hardware shall be provided by others.

Intel i7 2.8 GHz or higher processor – Intel HM65 express mobile chipset and Intel HD 3000 graphics or equivalent or AMD equivalent; 4 GB DDR3 RAM; 1 Tb hard drive; 14” LCD monitor; R/W CD- ROM drive; MS keyboard & optical mouse; integrated 100/1000 LAN wireless LAN 802.I1, 2 x USB 3.0, 2 x USB 2.0, 1 x HDMI, 1 x RJ45 Ethernet, 5 in 1 cardholder. Microsoft Windows 10 Professional 64-bit, Office 2012; Business, Acrobat X professional; Trend Antivirus or equivalent

A 21” LED back lit LCD monitor, mouse and keyboard

Operator Interface

1. The SSMS software shall use a single Windows based client application interface for system configuration, administration, management, control and monitoring operations.

2. The SSMS shall provide a mouse-driven, Windows based, graphical user interface allowing operator(s) to open and work on multiple windows simultaneously, at host server and workstation(s) with minimal degradation to system performance.

3. The SSMS shall provide on-line context sensitive help files to facilitate operators in the configuration and operation of the SSMS. Standard Windows help commands for Contents, Search, Back, and Print shall be supported.

4. The SSMS software shall implement National Language Support (NLS) in a manner that allows simultaneous multi-lingual operation, based on individual operator language preference. The graphical user interface and on-line help shall support English and [French] [Italian] [Dutch] [Polish] [Danish] [Swedish] [German] [Russian] [Spanish] [Portuguese].

5. The SSMS shall support means to manage specific facilities by specific operators.

6. The SSMS shall support defining an unlimited number of operators. Application access via workstation(s) shall be restricted by operator login and password. Operator passwords shall be stored in the database in an encrypted manner. Operator profiles shall be configurable to include form level permissions, facility, and language preference.

7. The SSMS shall allow for control of Intrusion, Access Control through graphical floor plans.

8. The SSMS software shall allow for monitoring alarms using graphical floor plans.

9. All relevant operator events shall be stored in the historic logs.

10. Operator permissions shall be customizable.

11. Operator permissions shall be based on menu access

Person Management

The SSMS shall provide an operator interface for enrolment, modification, and deletion of personal, intrusion and access control information (doors and lifts). The SSMS shall allow enrolment of personal, intrusion and access control information in advance, without requiring assignment of badges. The personal, intrusion and access control information shall include the following data:

a. First Name
b. Middle Name
c. Last Name
d. Employee Number
e. Personnel Type (Selectable from a user defined list that shall include as a minimum; Permanent, Temporary and Contractor classifications).
f. Department (Selectable from a user defined list).
g. Facility (Selectable from a user defined list of database partitioned views).
h. Trace Activity (Enable/Disable)
i. Address 1 (User definable label)
j. Address 2 (User definable label)
k. Address 3 (User definable label)
l. Address 4 (User definable label)
m. Address 5 (User definable label)
n. Telephone number
o. 90 User Fields (User definable labels)
p. Person Profile, providing access right(s).

Access Right Management: Profiles

The SSMS provides for different types of access control:

- Access rights for intrusion alarm control (Alarm groups)
- Access rights for access through doors (Door groups)
- Access rights for access to Lifts and Floors (Floor groups)

Every person shall have a selection from each of these, one per registered integrated Intrusion/Access control panel in a Person profile. Each profile shall be available to every person. Person Profiles provide the means to assign access rights to persons using functional groups like Manager, Sales Staff or Visitors.

Badge Management

The SSMS shall provide an operator interface for enrolment, modification, and deletion of badge information in advance, without requiring assignment to a person and shall include the following data:

a. Description
b. Assigned Cardholder (Selectable from predefined list of persons)
c. Badge Group (shall connect card format to badge and to panel)
d. Badge setup shall allow for either site code with card number for known card formats, as well as card learn methods. The allowed method shall be defined by the control panel setting.
e. Card ID number (4 to 20 digit, unique access control identifier).
f. Card Site/Facility code (unique ID for a range of cards)
g. PIN Number (4 – 10 digit number for authenticating cardholder in card and keypad reader applications)
h. Raw Card Data (through manual entry or card learn option)
i. Status (Active, Void, Lost, Expired, Remake).
j. Badge Issue Date (allows automatic activation of a badge at a specified time and date)
k. Badge Return Date
l. Badge Expire Date (Required to automatically expire badges at control panel level in real-time if connected to SSMS).
m. Special Badge options:
   - Dual Custody (two valid card required for access being granted)
   - Visitor (access allowed only in combination with Guard card)
   - Guard (allows access to visitors)
   - Card Only (card only, no PIN)
   - Extended Access (use extended access times)
   - Privileged (ignore Anti-Passback)

Badge Groups

The SSMS software shall provide for means to allow setup of badges in specific integrated Intrusion/Access control panels. Badge groups shall be assigned to badges and integrated Intrusion/Access control panels enabling download from badges only to those panels that have the same badge group assigned.

Access Control Management and Control

1. The integrated intrusion/access control panels within the SSMS shall allow or deny access through doors and provide output control via access control readers (card and/or PIN), based on validation of a badge holder’s assigned access rights.

2. The SSMS shall support defining access rights in a manner that associates door(s) with and time schedule. The time schedule shall define the specific time(s) of day and day(s) of the week including holidays for which access will be granted for the associated door(s) and/or controlled output(s).

3. The SSMS shall allow badge holders to be assigned access rights.

4. The SSMS shall allow badge holders to own multiple access control cards, without requiring duplicate badge holder personnel information.

5. Any and all access control cards assigned to a badge holder, shall automatically inherit all of the access rights assigned to the badge holder.

6. The integrated intrusion/access control panels within the SSMS shall monitor all doors and process an alarm notification whenever an access controlled door is opened, unless the door is opened pursuant to a valid card read, exit request through a request to exit device, or the door has been unlocked via remote command from an authorized system operator.

7. The SSMS software shall monitor all access control events and process an alarm notification whenever an alarm event is received. Any access control event shall be available as alarm event by configuration in the SSMS software.

8. The SSMS shall support IN and OUT access for Anti-Passback and time and attendance applications using intelligent access controllers. Anti-Passback shall only operate within one integrated intrusion/access control panel. Anti-Passback shall not depend or require the SSMS software to operate.

9. Control performed on doors shall allow for optional input of a purpose by an operator. The purpose and control option selected shall be logged in the historical database.

Intrusion Alarm Management and Control

1. The integrated intrusion/access control panels within the SSMS shall monitor all intrusion inputs and process all events within the local system. If configured, events shall be reported to a Central Station and sent to the SSMS software for history logging and reporting purposes.

2. The SSMS software shall monitor all intrusion events and process an alarm notification whenever an alarm event is received. Any intrusion event shall be available as alarm event by configuration in the SSMS. Alarm events shall include input related events, arming/disarming events and system events.

3. The integrated intrusion/access control panels within the SSMS shall allow for doors to be included into normal intrusion alarm processing, including reporting to Central Stations.

4. The integrated intrusion/access control panels within the SSMS shall allow for arming and disarming (set/unset) of areas by any valid badge (card and/or PIN) at any reader that is part of the integrated intrusion/access control panel where the badge holder has proper intrusion control rights.

5. The integrated intrusion/access control panels within the SSMS shall have the option to prohibit access through doors if associated areas are armed.

6. Audible Alarm notification (sirens or bells) shall be kept local to the integrated intrusion/access control panel.

7. Alarm reporting by the SSMS integrated intrusion/access control panels shall occur through PSTN, ISDN-B, ISDN-D, GSM or IP using selectable alarm transmission protocols to Central Station receivers.

8. The SSMS software shall support control of intrusion inputs by approved operators. Control shall allow for inhibiting or uninhibiting intrusion inputs and Date Gathering panels, arming or disarming areas and activating or de-activating outputs.

9. Control performed on intrusion devices shall allow for optional input of a purpose by an operator. The purpose and control option selected shall be logged in the historical database.

Alarm Management

The SSMS software shall automatically setup appropriate alarms for any device by uploading device configurations from integrated Intrusion/Access Control panels, Fire Alarm Systems or Digital Video Multiplexer/Recorders.

1. Alarm occurring shall allow for showing an alarm notification window on top of all windows in the windows desktop. The Alarm Notification window shall enable direct access to the Alarm Monitor or to the Alarm Graphics viewer.

2. Alarms shall be able to activate an audible notification based on alarm priority..

3. Alarms originating from devices shall initiate normal alarm responses in the originating integrated intrusion/access control panels and do not depend on the SSMS software. Optional alarm reporting to remote Central Station Receivers shall not be affected by the use of an SSMS software.

4. Remote Integrated Intrusion/Access Control panels shall be able to report events through PSTN, ISDN or GSM to a modem connected to the SSMS software.

5. Alarms shall be individually configurable and controlled in the following manner:

   Configure if monitoring of the alarm is enabled or disabled.

   Configure the description of the alarm event.

   Configure if operator acknowledgement of the alarm is required before the alarm can be cleared from the alarm monitor window from any operator workstation. Acknowledging the alarm in the SSMS shall reset the alarm in the originating device, provided the alarm situation is no longer present. The alarm shall remain in the Alarm Monitor until the alarm situation is no longer present.

   Configure a priority level (0 to 9) for prioritizing the processing and display of alarms.

   Configure if the alarm shall be routed to the history/archive database and/or printed on a host/server alarm printer.

   User-definable instructions shall be assignable to each alarm, required to display in the alarm monitor window at all operator workstations for alarm assessment and response.

SSMS Software System Monitoring & Control

The SSMS software shall provide for several tools to monitor SSMS relevant devices or actions.

Graphical Editor

1. The SSMS software shall provide for a Graphical Editor allowing setup of floor plans showing the selected device’s state in the Graphical Viewer.

2. Floor plans shall be added as ready made graphical images.

3. Floor plans shall be sizeable and can be enlarged to show a section in greater detail.

4. Supported image file types shall include BMP, JPEG, GIF, TIFF, PNG, WMF and EMF.

5. Devices shall be represented on the floor plan by points showing icons. Different icons shall be used for different states a device may have. User defined icons shall be allowed and shall be available for any device and device state.

6. The Graphical Editor shall provide a list of all devices. To add devices to a floor plan, devices shall be dragged and dropped onto the floor plan. Possible devices include:

a. Intrusion zones
b. Intrusion areas
c. Intelligent Access Control Doors
d. Intrusion Arming Stations
e. Intrusion outputs
f. Intrusion Data Gathering Panels
g. CCTV cameras
h. Fire Control Panels

7. Devices shall have a default set of icons representing the possible states for that device. The default icons shall be customizable by selected operators.

8. Devices shall have a default set of events associated representing device states. The assigned list of events shall be customizable.

9. Devices shall have a default label assigned. By default the label is copied from the device description and shall be truncated to 30 characters maximum. The label shall be customizable by system administrators and shall contain up to 64 characters.

10. Devices icons shall be either normal or small size.

11. A special point type (Alarm Container) shall be available to enable combining alarms from different devices into one icon. Devices shall be dragged and dropped into the Alarm Container adding all alarms from these devices into the alarm container. From the Alarm Container it shall be possible to jump to other maps.

12. The Graphical viewer shall allow switching between floor plans. The Graphical Editor shall provide two special options to enable this

    a. Using a dedicated Jump type
    b. Using an alarm container that allows to jump to another floor plan

13. Selected operators shall be allowed to access the device specific configuration for devices on the floor plan.

Graphical Viewer

1. The SSMS software shall provide for a Graphical Viewer to support identification and easy localization for events The Graphical Viewer shall provide for a floor plan with devices represented with icons indicating the current state of the device.

2. The Graphical Viewer shall show the current state of a device in real time.

3. Devices in alarm shall be flashing red when in alarm to show alarm states.

4. Selected operators shall be allowed to control devices from maps. Performing control options shall have an option to request entry of a purpose for control.

5. Floor plans in the Graphical Viewer shall adapt the size of the Graphical Viewer window size, respecting the specified aspect ratio.

6. Access to the Alarm Graphics Viewer shall be from menu, from the alarm monitor or alarm notification.

Alarm Monitor

The SSMS software shall provide for an Alarm monitor listing all Alarms.

1. Multiple occurrences of the same alarm shall only be listed as one entry in the alarm monitor, only increasing a counter.

2. The alarm monitor shall list all events with priority, time and date stamp, current state, process state, proper identification where possible and alarm occurrence counter.

3. The Alarm Monitor shall list any instruction setup for an alarm event.

4. The Alarm Monitor shall allow for entering a response when acknowledging alarms. The responses shall be stored in history log.

5. Acknowledgement of an alarm shall also reset the alarm condition for the originating device, provided the alarm situation has been resolved. If the alarm situation is still present, the alarm shall remain listed in the alarm monitor indicating the present alarm condition. As soon as the alarm condition is resolved, the alarm shall be removed from the alarm monitor.

6. Alarms shall provide an option to view the alarm on a floor plan in the Graphical Viewer, provided a floor plan having the alarm is present

Badge Monitor

1. The SSMS software shall provide for a Badge monitor listing all Badge related events happening in the SSMS for a maximum of 24 hours or 10000 events. Events shall be listed in real time. All events shall be available through reports for later evaluation.

2. The badge monitor shall list all events with time and date stamp and where possible with proper identification of door and badge holder.

3. The Badge monitor shall allow for listed badges to retrieve badge events from the past 24 hours for a person holding the badge.

Swipe and Show

The SSMS software shall have a Swipe and Show option to enable operators to directly view information on persons badging cards at selected readers.

The Swipe and Show windows shall show person name, person profile, the region the person has moved to and an image of the person when available.

An alarm trigger associated with badge events for the selected readers shall on activation dock to the Swipe and Show window to provide maximum data available for assessing correct persons passing through doors.

The Swipe and Show window shall provide additional information for the last 24 hours for the person shown in the swipe and show window.

Controller Utility

1. The SSMS software shall provide for a Controller Utility monitor listing all registered Integrated Intrusion/Access Control panels and all Fire Alarm Systems available in the SSMS.

2. The Controller Utility shall list all devices with relevant details, including connection state.

3. The Controller Utility shall provide means to connect devices to the SSMS software.

4. The Controller Utility shall provide means to upload or download configuration data to Integrated Intrusion/Access Control panels.

5. The Controller Utility shall provide means to pause receiving events from Integrated Intrusion/Access Control panels.

Digital Video Viewer

1. The SSMS software shall have a Digital Video Viewer option to control Digital Video Recorders and play live or recorded footage from any registered Digital Video Recorder

(DVR).

2. The Digital Video Viewer shall have facilities to view recorded footage from any alarm in the historical logs, provided the footage is available on the DVR.

3. The digital Video Viewer shall allow for direct playback of live footage from any registered and online Camera while allowing for calling a preset selection of PTZ cameras.

Live History Log

1. The SSMS software shall provide for a Live History Log monitor listing all events received from any device in real time in the SSMS.

2. The SSMS software shall allow filtering on alarm categories to enable monitor of specific areas of interest.
3. The Live History Log shall contain events from the last 24 hours with a maximum of ten thousand (10,000) entries.

SSMS Software System Status & Control

1. The SSMS software shall provide for several tools to control SSMS relevant devices and request the current state.

Intrusion Zone Status and Control

1. The SSMS software shall provide for Status and Control options of Intrusion Zones to selected operators.

2. The SSMS software shall allow requesting current status of Intrusion Zones.

3. The SSMS software shall allow control of Intrusion Inputs using the following options:

   a. Inhibit – Disable the input until associated area disarms
   b. Uninhibit – Enable the input after a previous inhibit
   c. Reset – Reset an alarm present. The command needs to be issued again to reset if the input is in alarm state at the moment the command is issued.
   d. Reset Ack – Reset an alarm present. When the input is in alarm state at the moment the command is issues, the input will reset automatically when it returns to normal state.
   e. Input control shall allow for a text entry to explain the reason for control. The text entry shall be logged in the history log.

Intrusion Output Status & Control

1. The SSMS software provides for Status and Control options of Intrusion Outputs to selected operators.

2. The SSMS software shall allow requesting current status of Intrusion Outputs.

3. The SSMS software shall allow control of Intrusion Inputs using the following options:

   a. On indefinitely – Switch the output active until switched off
   b. Off – De-activate the output.
   c. Output control shall allow for a text entry to explain the reason for control. The text entry shall be logged in the history log.

Intelligent Access Control Door Status & Control

1. The SSMS software provides for Status and Control options of Intelligent Access Control Doors to selected operators.

2. The SSMS software shall allow requesting current status of Intelligent Access Controller Doors.

3. The SSMS software shall allow control of Intelligent Access Control Doors using the following options:

   a. Duration Unlock – Open the door for a to be specified time.
   b. Indefinite Unlock – Open the door until relocked by selecting Lock.
   c. Open – Open the door for the programmed door open time.
   d. Lock – Lock the door.
   e. Enable – Enable the door. The door works as normal.
   f. Disable – Disable the door. The door shall no longer respond to card badges, open or unlock commands.
   g. Door control shall allow for a text entry to explain the reason for control. The text entry shall be logged in the history log.

Intrusion Area Status & Control

1. The SSMS software provides for Status and Control options of Intrusion Areas to selected operators.

2. The SSMS software shall allow requesting current status of Intrusion Areas.

3. The SSMS software shall allow control of Intrusion Areas using the following options:

   a. Arm – Arm the area.
   b. Disarm – Disarm the area.
   c. Forced Arm – Arm the area with temporary automatic inhibit of active inputs. If the inputs remain active and the zone type is such that an alarm shall occur when the area is armed, an alarm shall occur immediately.
   d. Area Control shall allow for a text entry to explain the reason for control. The text entry shall be logged in the history log.

Intrusion Arming Station (RAS) Status & Control

1. The SSMS software provides for Status and Control options of Intrusion Arming Stations to selected operators.

2. The SSMS software shall allow requesting current status of Intrusion Arming Stations.

3. The SSMS software shall allow control of Intrusion Areas using the following options:

   a. Open – Open the door associated to the RAS for the programmed door unlock time.
   b. Inhibit – Disable the RAS from reporting system alarms (like tamper, Online/Offline) to the control panel.
   c. Uninhibit – Enable the RAS for reporting system alarms (like tamper, Online/Offline) to the control panel.
   d. RAS Control shall allow for a text entry to explain the reason for control. The text entry shall be logged in the history log.

Intrusion Data Gathering Panel (DGP) Status & Control

1. The SSMS software provides for Status and Control options of Intrusion Data Gathering Panels to selected operators.

2. The SSMS software shall allow requesting current status of Intrusion Data Gathering Panels.

3. The SSMS software shall allow control of Intrusion Data Gathering Panels using the following options:

   e. Inhibit – Disable the DGP or control panel from reporting system alarms (like tamper, online/offline) to the control panel.

f. Uninhibit – Enable DGP or control panel for reporting system alarms (like tamper, online/offline) to the control panel.
g. Battery Test – Start performing an extended battery test on the DGP or control panel. This command shall have no effect on DGPs without onboard power supply
h. DGP Control shall allow for a text entry to explain the reason for control. The text entry shall be logged in the history log.

Integrated Intrusion/Access Control Configuration

The SSMS software shall provide for full configuration of the Integrated Intrusion/Access Control panels. It shall be possible to upload and download all configuration data with the exception of users, which are managed through the SSMS software to cater for large user groups.

Reporting

The SSMS software shall provide on-line database reporting without degrading system performance. The following reporting functions and capabilities shall be supported:

1. Predefined reports with the ability to create and save user definable templates for grouping, sorting, and filtering data. A minimum number of predefined reports shall be furnished covering the following topics:

   a. Person data
   b. Badge data
   c. System administration
   d. Device configurations
   e. Access of persons to specific areas, doors or floors
   f. Door, floor and alarm group details
   g. Roll call
   h. Alarm History
   i. Badge History
   j. Operator History
   k. Time and Attendance History

2. Reports shall allow operators to perform page setup, preview report on-line, print, and export reports to multiple file formats and destinations.

   a. Export file formats supported shall include:
   b. Crystal Reports.
   c. Data Interchange Format.
   d. MS Excel and Word.
   e. HTML
   f. ODBC.

3. Export destinations supported shall include:

   a. Disk File.
   b. Exchange Folder.
   c. Microsoft Mail (MAPI).

4. The SSMS shall support direct database connectivity for facilitating report generation from external 3rd party database applications. The following applications shall be supported:

   a. Microsoft SQL Server.
   b. Microsoft Access 2002.

Photo ID Badge Production

1. The SSMS software person management interface shall incorporate capture, display, and print capabilities for producing custom photo ID badges by authorized operators from any operator workstation licensed to do so. Photos and signatures shall be available on-line for positive identification from all operator workstations. The person management interface shall

include the following:

a. Digitized Photo.
b. Digitized Signature.
c. Badge Design (Selectable from a user defined list and associated to person and badge based on badge type classification)

2. The SSMS shall provide badge design and production capabilities that shall include the following:

   a. Support industry standard image formats for capture, storage, and printing of digitized photos and signatures. Image formats shall support user selectable settings for optimizing file size, compression/quality, and colour depth.
   b. Support industry standard and commercially available live video and still image capture devices and interfaces including support for:

      1. Composite, S-Video, RGB, and digital cameras.
      2. Scanners.
      3. Signature pads.
      4. TWAIN driver interface.

   c. Support image capture of photos and signatures from file.
   d. Support image cropping and quality enhancement controls at time of capture.
   e. Support on-screen print preview of card design prior to printing.
   f. Support industry standard and commercially available printers and printer interfaces including support for:

      1. Colour Laser, Inkjet, and Bubble jet printers.

      2. Colour dye sublimation badge printers. Supported badge printer functions shall include:
         - Direct printing on standard CR-80 PVC cards.
         - Single and dual sided printing.
         - In-line magnetic stripe HiCo/LoCo encoding.
         - Clear overcoat with optical or holographic security logo.

   g. Provide a user interface for creating custom badge design templates including the following:

      1. Full compliment of drawing and editing tools.
      2. Define and edit text and graphic object properties.
      3. Link persons database fields to static text, dynamic text, and graphic objects.
      4. Use of standard and custom colour palette definitions.
      5. Support industry standard graphics formats for importing logos and backgrounds.
      6. Define and apply ANSI standard barcode formats to text objects.
      7. Define and apply magnetic stripe encoding formats to text objects.

24. Smoke Detection System

24.1 System Description

The smoke detection comprising of a central addressable fire alarm panel located in the Control Room networked to remote panels with addressable devices on loops. The HMI will be a PC which will house the relevant software for complete system monitoring, system programming, fault location etc.

The fire detection system will be zoned according to the requirements of the fire rational design. This zoning information shall be issued after the contract is awarded.

Alarms in predetermined fire zones will provide output signals to other services such as elevators to initiate grounding (homing), air handling units to shut down, smoke extract fans to start up etc. on a “double knock” system.

The control unit shall continuously monitor the analogue status of all sensing devices, and initiate action when a fire or smoke condition is present. The action shall be defined via a fire action schedule that takes zoning into account.

The alarm management shall be configurable from the control panel via a PC to enable the system to be tailored to suit the protected building, and to permit future changes. This configuration shall be maintained under power failure conditions.

The control unit will have a front panel comprising of indicating LED’s, control PC and LCD display, as described in detail later.

Four levels of access into the system menu via the keypad are to be provided.

24.2 Standards

a) The latest edition of SANS 10139 Fire Detection and Alarm System for Buildings

b) The latest edition of SANS 60331 and 60332 – 11 and 12 for Fire Rated Cabling

c) EN 54 and ISO 7240 Standards

24.3 System Operation

24.3.1 Polling System

The system shall pole each sensor individually and reads information at regular intervals to the control unit. The idle value shall be continuously updated in order to compensate for ageing and atmospheric conditions. The panel shall make decisions based upon the information obtained from each detector.

System polling time shall be less than three seconds for each complete scan of all devices attached. This time shall remain constant irrespective of the number of devices attached to the loop.

24.3.2 Communication Circuit

A 2-wire circuit is to be used for power and communication between the panel and the sensors. The cable is to be a minimum conductor cross-section of 1,5mm².

24.3.3 Device Address

Each device on line shall be uniquely identifiable by the control unit. This must be achieved by pre-setting the address of each device.

Removal of a detector head from its base must extend a fault condition to the control unit.

The identification of each type of address unit and each type of sensor (i.e. multi sensor, ionisation detector, heat detector, sprinkler switch, etc.) is transmitted to the panel on each polling scan.

The condition of each line device, including circuit, calibration and contamination shall be transmitted to the panel on each polling scan.

24.3.4 Calibration

The system will check the calibration of each analogue line device and record changes caused by environmental contamination.

When maximum calibration adjustment is reached the panel will indicate a "maintenance" signal. This must be a dedicated signal, and must be separate from the “pre-alarm” signal.

The control panel is capable of monitoring the slow change in signal due to dirt contamination and at a predetermined level indicate that the detector is in need of servicing.

24.3.5 Display And Indicators

All display and indicators shall be LCD for text, and LED for lamp indication.

24.3.6 Number Of Devices In Alarm

There is no limit to the number of devices that may be in alarm simultaneously.

When a detector is in alarm an LED in its head or base shall be switched on.

24.3.7 Line protection and monitoring

The addressable line must be monitored for short circuit or open circuit.
The occurrence of an open circuit shall cause a fault signal on the panel, but all sensors or devices shall function correctly.

The occurrence of a short circuit shall cause no more than 20 sensors or call points to cease operating, and all remaining devices shall function correctly. This implies the installation of line isolators.

24.3.7 Software Algorithms

Intelligent software algorithms to identify the presence of fire or smoke, and any possible faults present must evaluate the data from each sensor.

The system must support a number of different algorithms; each tailored to suit the profile of a different hazard or protected area. These algorithms must be specifically matched to provide the optimum protection for each type of area.

It must be possible to customise algorithms to take into account special conditions that may exist in certain specific hazards. This customisation should incorporate the features below.

Alarm sensitivity relative to each analogue detector is to be individually adjustable, device-by-device, by the control panel. Not less than four levels of sensitivity adjustment are required for each device.

24.3.8 Alarm Verification.

Every analogue detector must have the facility for verifying the validity of an alarm signal over a 20 second period, before initiating an alarm. This alarm verification function must be able to be enabled or disabled, on a device-by-device basis, from the control panel.

It must be possible to allocate selected algorithms independently to each sensor in the system. In addition, different algorithms must be able to be automatically allocated to the same sensor at different times.

24.4 Loop Operation

24.4.1 Addresses

The loop devices shall each have a unique address.

There will be no preset order for addressing the devices. The devices shall be installation addressed appropriate to site conditions. This order will be determined during system. Every device must be checked by the control panel every 2 seconds. In order to maintain system integrity, the panel must not bypass any sensors during a scan.

The control panel will have the facility of determining if more than one device has the same address on the loop. A "double address" alarm shall be given if this occurs.

24.4.4 Loop devices

It must be possible to fit a range of sensors and devices to the loop.

Sensors shall transmit data to the control panel every 2 seconds, which shall be interpreted by the algorithm allocated to the particular sensor. Response will be determined by the characteristics of the algorithm.

Manual call points shall each have their own unique address and the panel is capable of identifying and responding to the operation of a call point within three seconds, as required by BS5839.

Loop sounders shall be powered directly from the addressable loop, without requiring any additional wiring.

It is possible to fit loop isolators that shall protect against short circuits, and partial short circuits, on the loop by isolating that section of the loop where the short circuit occurred.

Fire condition LED indicators fitted to the devices and any remote indicators shall be remotely and separately operated from the control panel.

Interfacing to other systems

The loop shall be capable of receiving information from third-party systems, e.g. operation of sprinkler system, by means of standard interface units. The source of this information shall be identified by its own unique address. In addition, the interface unit shall indicate to the panel the type of alarm, egg. “sprinkler”, “security”, etc.

Device identification and location

The control panel shall be able to identify the absence of a field device.

The control panel shall identify the zone in which each sensor or device address resides, and shall give a “configuration-fault” signal if a sensor or device address is located in the incorrect zone.

Line Capacity

The capacity of the address line shall be at least 127 addressable devices.

These must be input devices, such as smoke sensors, or output devices, such as sounders or relays.

24.4.3 Fire Alarm Panel

a) General Description

The central alarm panel is to be a 24-volt analogue addressable unit, designed to communicate with the remote 4 loop fire alarm panels and remote display panels and the field devices. It shall be a has a microprocessor based unit, and shall incorporate all hardware and software to enable it to make decisions based upon information received from sensors, and operate appropriate outputs to initiate required alarms and signals. The panels are to have R5485 Ethernet TCP/IP and USB ports. Panels to be supplied complete with batteries

Signalling and Annunciation

Fire indication shall be by zone, displayed on LED indicators, and on the LCD text display.

Fault, maintenance, pre-alarm, and device/zone-disabled signals shall be indicated visually by LCD text display, and audibly, in the control unit.

The top portion of the LCD text display shall always show the first alarm received. The lower portion of the LCD text display will show the last alarm received. It must be possible to manually scroll through all alarms on the lower portion of the screen, using “up” and “down” scroll buttons.

The display shall show the total number of alarm events currently in the system.

Fire alarms shall take priority when displaying. However, it must be possible to view all events currently in the system, including, fire alarms, fault alarms, pre-alarms, maintenance alarms, disabled devices, and other events.

Outputs shall be provided for audible alarms, control functions, remote mimics and Ethernet connection for computers, printers and Internet Protocol communication.

b) Zoning

The panel shall have a minimum of fifty zones. The zones must be fully fielded programmable to permit sensors to be allocated to any zone.

A 40-character text label displaying on the LCD display must identify each zone. This shall be field programmable.

The panel must provide facilities for the operator to inspect the zoning configuration, and inhibit, or activate devices. Facilities must be provided for identifying all active and inhibited addressed, and all connected device types.

c) Panel Indicators

All visual indicators shall be LED’s and no incandescent lamps are to be used.

d) Panel Controls

The panel is to incorporate a numeric keyboard and push-buttons with the following functions:

- System reset button
- Alarm accept button / silence alarm button
- Alarm sound button
- Panel buzzer “mute” button
- Lamp test function
- “Help” button
- Control buttons as required for system operation
- Menu functions for maintenance and commissioning

24.5 Alarm outputs (Fire)

The panel must incorporate two monitored audible alarm outputs for the switching-on of bells or electronic sounders.

These outputs must be continuously monitored for open and short circuit.

Each output is rated at 0,75 A at 24 V DC.

It must be possible to independently disable either of the alarm bell output by means of a control push button.

A test facility must be provided in order to test each of the alarm bells out outputs. When the test is initiated the selected alarm bell will operate intermittently.

Both the alarm bells must have a delay facility, which is selected by controls on the front panel. Manual call points will override this delay.

24.6 Alarm Contacts (Fire)

One voltage free changeover contact is to be provided. This must operate on a "fire” condition, and is to remain "on” until the system is reset.

The contacts are to be rated at 2 A at 24 V DC.

24.7 Alarm Contacts (Fault)

One voltage-free changeover contact is to be provided. This will release on a "fault” or "maintenance” condition, and is to remain "off” until the system is reset.

24.8 Processor Monitoring

A hardware “watchdog” circuit must be provided on the central processor module. In the event of a microprocessor failure the watchdog must cause a hardware reset of the microprocessor. This reset action will continue until the processor has restarted. In the event that the processor has not restarted within 20 seconds, then the panel must give an audible and visual alarm indication.

A watchdog counter must allow the viewing of the number of times that the processor has been restarted by the watchdog, for diagnostic purposes. This information will be stored in non-volatile memory, enabling it to be viewed even if the panel has been powered-down. The counter must only be able to be reset by an authorised engineer, under a level 3 access code.

The microprocessor must perform full diagnostic tests on all memory devices on start-up.

24.9 Loop Devices

24.9.1 Device Types

Intelligent Point Sensors: General Requirements

Sensors shall have complete electromagnetic and electrostatic protection against externally generated noise and the effects of devices such as fluorescent light fixtures, variable frequency motor controllers, cellular telephones, and electrical surges from other sources

Sensors shall plug into separate mounting bases with a twist-lock action. The bases shall be fitted with corrosion resistant connector springs and terminal screws with captive clamping plates.

All bases shall incorporate a concealed security lock to prevent unauthorised removal or tampering with sensors. It will be possible to activate the security lock in areas where required. With the security lock activated, it must only be possible to remove a sensor from its base using a special tool.

There shall be a facility on the base for attaching a label indicating the address of that detector. A similar facility will be available on the detector, enabling the fitting of a label indicating its address. When the detector is fitted to its base, both the detector and base address labels shall be visible, and aligned adjacent to each other.

Smoke entry points must be protected against insect ingress by corrosion resistant mesh.

The detector must be supplied complete and fully tested and calibrated.

Sealed dipswitches shall set the unique address of the detector.

The sensors shall have a dimension not exceeding 70mm x 115mm diameter maximum including the mounting base.

The detector shall be capable of being remotely tested from the control panel by the transmission of a test instruction to the addressed detector.

Multi-sensor sensors (analogue/addressable*)*

The multi-sensor sensors shall incorporate photo-electronic optical smoke sensors, and high sensitivity thermal sensors, software interlocked to provide early warning from all types of smouldering and thermal fires.

.

Multi-sensors shall be able to be operated by the control software as combination multi-sensing devices, or as smoke sensors only, thermal sensors only.

The smoke element shall be of the light scattering type using a pulsed internal LED light source and a photocell sensor.

24.9.2 Photoelectric (Optical) Smoke Sensors (Analogue/Addressable)

Photoelectric optical smoke sensors shall comply with standard EN54-7.

The photo-electronic optical smoke sensors shall be suitable for detecting visible smoke such as is produced by slow smouldering fires.

They shall be of the light scattering type using a pulsed internal LED light source and a photocell sensor.

The detector shall be capable of operating within the following environmental limits.

a) Temperature operating range -20ºC to +60ºC

b) Humidity operating range 0% to 95% RH (without condensation)

c) Wind - not affected

The detector must be capable of protecting an area up to 100m² at a height of up to 12m. The installation and sitting of the sensors must conform to BS5839 Part 1 1980, or similar Standards.

24.9.3 Heat sensors (analogue/addressable)

Heat sensors shall comply with standard EN54-5 (1996)

The heat detector must be electronic in operation, and shall monitor ambient temperature by means of a NTC thermostat.

The detector will be capable of operating within the following environmental limits.

a) Temperature operating range -20ºC to +60ºC

b) Humidity operating range 0% to 95% RH (excluding condensation)

c) Wind - not affected

Each detector must be suitable for protecting an area up to 50 m² at a height of up to 7,5 m. The installation and setting of the sensors shall be carried out in accordance with standards BS5839 Part 1.

24.9.4 Manual call point

The call point shall be manufactured from red injection moulded plastic.

Manual call-points shall comply with standard BS5839.

The overall size of the call point is 100 mm x 100 mm x 60 mm. It must consist of an enclosure, with a captive re-settable plastic pane, and it shall incorporate an addressable communications module.

Depressing the pane will initiate an alarm; the operator shall require no secondary action.

An externally visible LED shall indicate when the device is in alarm. The LED will illuminate when the call point is activated.

The manual call point must be supplied with a transparent plastic cover that would prevent accidental activation of the unit.

The system must be configured such that detection devices require double knock operation within a zone for the action to be initiated.

24.10 Loop Wiring

The wiring shall be 2-Core fire rated PH 120 minutes, low halogen, copper conductor, low impedance with foil and drain. The wire shall have a minimum conductor cross-section of 1,5mm². The outer sheath shall be red.

The wiring will be arranged for return loop

All effort will be made to avoid joints in the cable. Joints in the wire shall only be allowed in accessible boxes and only with the permission of the Engineer.

Where joints are allowed they will be made in the following manner.

- Conductors to be heat shrink
- Shield to be soldered
- Entire joint to be overall heat shrink
- The twisting if wires and wrapping with insulation tape shall not be acceptable.
- Termination of the wire to be device will be made with lugs that have been crimped with a suitable crimping tool.

At each detector base all the wires shall be terminated by lugs. This includes the shield etc. Three terminations at each base.

24.11 Network Wiring

The network wiring shall be at least a PH 120 minutes fire rated cable. The wire shall be solid copper conductors screened twisted pair/s with low smoke and zero halogen outersheath. Conductor size to be a minimum of 1.5 mm². The outer sheath shall be red.

24.12 Device Installation

The base of the detector shall be monitored such that the detector Led faces the doorway or direction of approach.

Manual call points must be mounted at 1200 AFFL using recessed backbones that are to be made available to the Electrical Contractor when wireways are installed. Where these cannot be recessed surface mount bases shall be used.

The Control panel must be mounted at 1300 AFFL to the bottom of the panel.

All wiring shall be routed along wireways provided. No loose wiring or wiring strapped to other services shall be accepted.

Detectors must have the address label fixed to both the detector head and base. Care shall be taken when installing these labels to ensure that they are correctly aligned (straight)

24.13 Testing and Commissioning

The testing of the systems shall be done in the presence of and to the satisfaction of the Engineer.

Test shall include simulation of fire conditions in each zone to prove the efficiency of the system and the Contractor shall supply all equipment necessary for these tests.

24.14 Fire Doors and Locking Systems

All Fire Doors are to be fitted with a 500kg Magnetic Lock. All Magnetic locks must be fitted onto the protected side of the door.

Red BGU – Activate fire Alarm

Green BGU – Release Fire Door and set of Alarm and door open signal.

Recessed door Monitors – be fitted to all fire door to transmit a door open signal.

24.15 Human Machine Interface (HMI)

The HMI shall consist of a 21 inch touch screen LCD/LED PC with i5 or higher processor, ultra higher resolution graphics, 8 GB RAM and 2 Tb hard drive with Microsoft Windows 8, Professional Windows Office 2015 and Acrobat Professional.

25. Fire Telephone

25.1 System Description

The fire telephone system is a hard wired stand-alone system for fire fighters and emergency personnel to communicate with each other. The system comprises of a master control unit at main entrance, operators control unit and door stations located in fire valve chambers on each block/floor.

25.2 Standards

SANS 400
SANS 10139
SANS 60331 and
SANS 60332–11 and 12

25.3 Technical Specification

The fire telephone system is a hard wired stand-alone system for fire fighters and

25.3.1 Master Control System

The master controller is to be an intelligent programmable processor based unit and capable of connecting 60 devices and have the following features.

.1 A logging system is to log the last 500 events
.2 Large LCD display
.3 Self testing and system testing facility
.4 Allow program download from PC via USP port

25.3.2 Operator Control

The operator control unit is to be an intelligent unit, expandable in modules to accommodate at least 60 remote fire alarm telephones. The unit shall have a display/mimic indicating active lines. The unit is to be hard wired to the master control unit.

25.3.3 Door Stations

The door stations are to be the handset type that automatically links the operator on lifting of the handset. Unit is to be hardwired individually to the master and control unit.

25.3.4 Cabling

The wiring shall be fire rated for at least PH 120 minutes, low halogen, copper conductor, low impedance with foil and drain. The wire shall have a minimum conductor cross-section of 1,5mm². The outer sheath shall be red.

All effort will be made to avoid joints in the cable. Joints in the wire shall only be allowed in accessible boxes and only with the permission of the Engineer.

Where joints are allowed they will be made in the following manner.

- Conductors to be heat shrink
- Shield to be soldered
- Entire joint to be overall heat shrink
- The twisting if wires and wrapping with insulation tape shall not be acceptable.

- Termination of the wire to be device will be made with lugs that have been crimped with a suitable crimping tool.

At each piece of equipment all the wires shall be terminated by lugs. This includes the shield etc.

26. Public Address System

26.1 System Description

The PA System shall be used to deliver audible signals, intelligible messages and guiding information and evacuation notices within the building area.

In case of emergency, the system will be used as the Voice-Alarm system and their signals will override programme delivery.

The PA System shall consist mainly of:

i) Loudspeaker systems
ii) Amplifiers and their power supply
iii) Interface system for voice alarm system priority integration.
iv) Cabling and wiring for this system

The General PA System delivers a processed or live audio signal with all relevant controls for this distribution network. All status messages of the VA System can be routed to the PA system.

The VA System shall employ loudspeaker systems composed of an adequate number of loudspeakers, and shall be aimed accurately to meet or exceed the minimum performance requirements.

Loudspeaker signals shall be combined to zones according to the building structure and defined by the drawings included.

The Engineer will appoint one person with name and position and train him/her to be responsible for managing the proper operation and maintenance of the PA System, so that it shall constantly work as planned.

The System operators shall have the possibility of selecting the zones, to which programme signal shall be broadcasted.

Any errors/malfunctions of the system shall be automatically monitored at all times and displayed within 100s at latest from the occurrence of the error/malfunction in accordance with SANS 60849;

Short-circuit, disconnection or other total loss of power of any power supply feeding the System;

Failure of any critical signal path, which shall include all equipment and interconnections between any initiation point of the system and the input terminals on or within each loudspeaker enclosure;

Components and/or modules missing within a critical signal path;

Failure of any loudspeaker, including open-circuit, short-circuit or earth leakage;

Failure of any power amplifier,

Any individual error or malfunction within the System shall be automatically indicated

26.2 Standards

a) The latest edition of the S.A.N.S. 60849:2005 (I.E.C. 60849:1998) Code of Practice for Sound Systems for Emergency Purposes.

b) The system equipment to be ENS4 certified.

26.3 Performance Criteria

The loudspeaker system shall be able to deliver after equalization a minimum continuous SPL of 85dB(A) for voice messages at 80% of the maximum throw distance.

A maximum SPL for attention-drawing signals as well as for voice messages at any point in the listening area shall not exceed 95 dB(A).

The distribution of the direct SPL shall be uniform over the listening area after equalization with the variation between loudest and quietest spots essentially not exceeding 6 dB in the frequency range 400 Hz to 4 kHz.

Common Intelligibility Scale (CIS) measured in the listening area shall be higher than 0.70 within a tolerance according to SANS/IEC 60849.

Amplitude frequency response averaged over the audience area shall exhibit after equalization a fluctuation of +/- 3 dB in the range 400 Hz-
4 kHz and shall roll off at a rate of
f < 250Hz with 12 dB/oct. and for f > 2500 Hz with 3 dB/oct.

Each loudspeaker shall be capable of producing a sound pressure level of at least 10dB above the average ambient background noise level throughout the building and VIP boxes, including all back of house areas.

All loudspeakers are connected in parallel and all amplifier channels to have a minimum of 6dB headroom.

The System shall be free of ground loops, oscillations, excessive noise, buzz, hum, RF interference and distortion.

26.4 Technical Specification

Equipment installed in rooms, e.g. control room, amplifier rooms, shall perform their functions properly within the following environmental conditions;

Ambient temperature: -5°C to +40°C
Relative humidity: 25% to 90%
Pressure: 86kPa to 106kPa

All other equipment of the VA System, e.g. loudspeakers, shall perform their functions properly within the following environmental conditions;

Ambient temperature: -10°C to +50°C
Relative humidity: 25% to 100%
Pressure: 86kPa to 106kPa

a) System Design

Loudspeakers shall be positioned as shown on the attached drawings. The positioning of amplifiers and associated electronics shall be decentralized as per the system schematic

A D/A-output matrix including audio signal processing serves the amplifiers decentralized in separate amplifier rooms.

Power supply of amplifiers and control room equipment is provided by others.

Acoustical adoptions, e.g. equalization, delay, etc., shall be programmable within the digital signal distribution of the System

Play-out-devices, i.e. hard disk-player, allow the usage of pre-recorded sound and music during use

Mixed programme signal shall be A/D-converted and transferred to the signal distributing digital System using an Ethernet-based protocol.

b) Gooseneck Table Top Microphone

Table top microphone, wired, with long gooseneck microphone of compact capsule size; to be used as voice microphone

Metal base plate including on/off switch and LED indicator

Condenser microphone capsule with super cardioid directivity characteristic

Frequency response 60 – 15000 Hz

Output impedance > 150 Ohms

Open circuit sensitivity > 20mV/Pa

Equivalent output noise < 30 dBA

Power supply 12 to 48 Vdc phantom

Gooseneck length > 400 mm

c) Audio Patchbay

Compact audio signal patch-bay system for any audio interconnection or switching through a preconfigured signal path

To be used for 48 incoming and 48 outgoing signals per 19” 1 RU panel

The direct switching of a signal path shall be realized by using special plugs to be provided with in an appropriated number

Panel with labelling strip, printable and changeable

Connecting patch cables in an appropriate length and number according to panel placement are to be provided

Audio frequency range 20 – 22000 Hz

Usable signal level better than -50 dBu to +20 dBu

Channel separation > 90 Db

Insertion loss < 0.03 dB

A rack-mountable drawer 19” 2 RU as deposit for plugs and patch cables is to be supplied with the patch bay

Audio patch-bay shall be Ghielmetti CSF series or approved equivalent

d) Multi-Channel Audio Interface

Audio interface, multi-channel I/O, configurable by specific order (selection of input and output modules in steps of 4), up to 16 channels per interface

The interface module shall be used either for inputting audio signals to the audio network or prepare audio out for amplifiers individually by signal processing (delay, gain, EQ)

Audio inputs and audio outputs shall provide symmetrical (barrier strip) connectors.

The interface module shall feature an A/D and D/A conversion of 24 bits.

The control terminals shall be used as 6 binary contact inputs and outputs and shall be permanently monitored. One of these outputs shall be usable as status contact on interface failure.

Communication and control options shall be available via Ethernet protocol, USB bus and RS 232 protocol

Interface shall provide build-in supervision functions to monitor and report any failure of interface or network audio interlink within the audio signal path. It shall provide an appropriate interface to the amplifiers integrating them in the surveillance circuit according to the requirements

Enclosure rack mountable, 19”, 1U

The interface module shall be connected to the an Ethernet-based digital audio distribution system, e.g. CobraNet

Audio frequency range 20 – 20000 Hz

Nominal input level +6 dBu

Input impedance 3.5 kOhms

Nominal output level +6 dBu

Maximum output level +20 dBu

Output impedance 100 Ohms

S/N ratio >99 dB

Integrated power supply

Multi-channel audio interface shall be a BSS Audio Soundweb London BLU-80 or approved equivalent

e) Voice Alarm System

Software and hardware components with highest priority for announcements using the voice alarm system described separately, output path selector defining a free choice of calling zones, at least 4, in which announcements shall be distributed, communication path delivering all relevant status messages of the signal-path-critical PA system components.

Interface shall realize at least but not limited to:

One (1) audio signal input

Nominal input level +6 dBu

Input impedance 20 KOhms

Maximum input level +21 dBu

Five (5) general purpose binary inputs

Voltage range 0 to 10 volts dc

Logic on high/low potential selectable

Functionality as “priority call”, “PA system sector A”, “PA system sector B”, “PA system sector C”, “PA system sector D”

Four (4) general purpose binary outputs, including reference voltage source (+5V/+10V/GND) Logic on high/low potential selectable

Functionality as “priority call sending”, “VA system ok”, “VA system low priority fault”, “VA system high priority fault”

Enclosure rack mountable, 19”, 1RU, inputs and outputs on barrier strip connectors

Contractor to describe solution selected in a technical attachment to its offer.

f) Data network switch with media converter

Managed data Ethernet switch, enabling redundant turbo-ring-topology, RSTP/STP (IEEE802.1W/D)

Redundant self-healing Ethernet ring capability with recovery time < 300ms at full load

Switch shall support Qos, IGMP, snooping/GMRP, VLAN, LACP, SNMP V1/V2c/V3, RMON; user-friendly web-based configuration and management

Housing enabled to be mounted either within rack enclosure back or in 19”

16 ports 10/100Base TX RJ-45 connectors

fibre ports 100/1000BaseFX on ST connectors, single mode 62.5/125 µm

g) Fibre Patch Panel

Passive patch panel for fibre cables

Metal housing enclosure in 19” 1 RU size fitted with 2 x 12 ports fibre connectors ST type

For incoming and outgoing cable connections between central control room and amplifier rooms

With labelling strip, printable and changeable

h) Service Panel

Panel in 19” 1 RU front as service panel

Fitted with:

3 x earthed wall socket for power supply 230V

1 x Neutrik EtherCon connector for data / Ethernet applications

Panel with labelling strip, printable and changeable

i) Amplifiers

Power amplifiers shall be of two/four-channel type, and power ratings suit the loudspeakers driven by them and compatible with interface module.

Power amplifiers shall feature class I of operation and possess integrated electronic protection against thermal and electrical overload and short circuit.

Power amplifiers shall possess the following characteristics;

Amplitude response of 20 Hz–22 kHz, -1 dB;

Signal-to-noise ratio of at least 105 dB;

THD (total harmonic distortion) of less than 0.08%;

Input sensitivity of +6 dBu; impedance 20 kOhms

MTBF (mean time between failures) of at least 100.000 hours

The power amplifier shall comply with IEC 60286-3.

Amplifier shall contain signal processing to adjust at least 4 parametric filters on each channel

Amplifier shall contain remote controllable functions of all relevant system parameters including amplifier operational mode and load status.

Communication shall be realized via a protocol, e.g. Ethernet. Selectable addresses allow designing a large-scaled amplifier control system.

Amplifiers to be rack mountable

j) Loudspeakers

The loudspeaker system shall be pre-selected according to performance requirements. Samples to be submitted, for approval, to the engineer / consultant prior to ordering

Flush in-ceiling mount loudspeaker system with back box

The loudspeaker shall include a transformer having multiple selectable high impedance taps typically 10W, 5W, 2.5W and 1W

Sensitivity @ 1w/1m of 88dB or higher

frequency response 100 – 15000 Hz (+/- 3 dB)

maximum SPL 98 dB at 1m

nominal coverage of 120 degrees conical

integrated mounting hardware with grille

system enclosure colour RAL 9010 (or approved equivalent), outdoor protected version for fixed installation

Wall mounted 2 way box type full range loudspeaker system

The loudspeaker shall include a transformer having multiple selectable high impedance taps typically 10W, 5W, 2.5W and 1W

Sensitivity @ 1w/1m of 88dB or higher

frequency response 90 – 14000 Hz (+/- 3 dB)

maximum SPL 100 dB at1m

nominal coverage of 90˚ x 90˚

components: 1 x 5.25” low woofer

1 x .75” high frequency cone

integrated crossover network, self-resetting protection

integrated and adjustable mounting hardware

system enclosure colour RAL 9010 (or approved equivalent), outdoor protected version for fixed installation

Horns

Due to external use and harsh climatic conditions, the loudspeaker system must have an IP-54 rating or better.

Samples will be submitted to the appointed corrosion consultant for approval prior to ordering

The loudspeaker shall include a transformer having multiple selectable high impedance taps, typically 10W, 5W, 2.5W and 1W for lower power application and 30W,15W,10W and 5W for higher power applications

Sensitivity @ 1w/1m of 97dB or higher

frequency response 150 – 14000 Hz (+/- 3 dB)

maximum SPL 112 dB at 1m

nominal coverage of 90˚ x 90˚

components: 1 x 12cm dynamic loudspeaker, weatherised

integrated and adjustable mounting hardware

system enclosure colour RAL 9010 (or approved equivalent), outdoor protected version for fixed installation

26.5 Wire and Cable

All wire and cable shall be new and unused.

All cables shall be installed on prepared routes or equivalent constructions.

Cables shall operate properly in the temperature range of -25°C to +60°C.

Fibre optical Cables

cable type for audio/data communication services within VA System

Cable specification:

A-DQ(ZN)BH E30

fibre number 12, multi-mode G62,5/125

Retain electrical function for 30 min during fire exposition

halogen-free according to IEC 60754-2

flame-resistant according to IEC 60332-1

For ring or star topology between components and next technical room or switching cabinet with data switch

Data Cables

Cable type for data communication services within VA System

Cable specification Cat.5e, S-STP 4x2xAWG 23/1 FRNC, for class D fast Ethernet according to ISO 11801

For star topology between component and next technical room or switching cabinet with Ethernet switch

cable sheath FRNC

Audio Cables

Cable type for analogue or digital audio connection

Cable construction 2Li2Y 0,22mm²(St)DY (AWG24), cable sheath FRNC

Control Cables

Cable type for control connection, e.g. GPIO or CAN bus

Cable specification Cat.5e, S-STP 4x2xAWG 23/1 FRNC, for class D fast Ethernet according to ISO 11801

cable sheath FRNC

Loudspeaker Cables

Cable for connection between loudspeaker system and amplifier

loop resistance shall not exceed 5% of the total loudspeaker impedance as seen by the amplifier

Cable specification:

2 hour fire rated polymer insulated unshielded annealed solid copper conductor with silicon rubber insulation

low smoke halogen-free according to IEC 60754-2

flame-resistant according to IEC 60332-1

Power Cables

low smoke, halogen-free copper conductor double insulators

26.6 Equipment Racks

The equipment racks shall house all rack-mounted equipment of the system.

Electrical power distribution within the racks forms part of this contract.

The equipment racks shall be EIA compliant 19” stand-alone rack. The depth shall be 32 1/2″ OD.

Whenever more than one rack is used, all racks shall be identical.

Useable height shall be 6 rack spaces

Rack shall be constructed of the following materials:

Top and bottom shall be 14-gauge steel;

Horizontal braces shall be 16-gauge steel welded to integral structural side panels of 16-gauge steel giving an 1/8” thick structure;

All structural elements shall be phosphate pre-treated and finished in a durable black powder coat.
Rack shall come equipped with two pairs of 11-gauge steel rack rail with tapped 10-32 mounting holes in universal EIA spacing.

Top and bottom of rack shall have a vertical slotted vent pattern.

Unused spaces of the racks shall be closed with blank panels.

27. Intruder Detection System

27.1 System Description

The Intruder Detection system shall form part of the Access Control System.

Intrusion detection system will be located in all general accommodation areas and be activated when rooms are not occupied. Activation will be done via local keypads or remotely from SSMS on an individual room basis.

The following devices shall be connected to the system input/output controller for the specific area with communication in the access control network.

27.2 Standards

IEC 60839-1-4

27.3 Detectors (Type 1)

.1 Dual technology passive infra red and microwave
.2 Ceiling Mount Perimeter detector
.3 30 m range
.4 Microprocessor based - digital
.5 Shall be provided with compensation algorithm to allow reliable detection over the temperature range 0 - 50ºC
.6 360º coverage (min) of lens
.7 RF immunity from 80 MHz – 1GHz

The detector shall be capable of protecting an area up to 100m² at a height of up to 12m. The installation and sitting of the sensors must conform to BS5839 Part 1 1980, or similar Standards.

27.4 Detectors (Type 2)

.1 Passive infra red detectors with the following characteristics
.2 Ceiling / wall mounted
.3 30m range
.4 Provided with compensation algorithm to allow reliable detection over the temperature range 0 - 50ºC
.5 Microprocessor based – digital
.6 90º detection angle
.7 Supplied complete with aesthetically placing monitoring bracket for installation
from overhead horizontal surface.

27.5 Panic Buttons

.1 Push contact type
.2 Approximately 60 x 20 x 15mm

27.6 Mag switch door position monitors

.1 18mmØ recessed into the doorframe
.2 Where double door exist both door will have a door monitor fitted. These shall be series connected to allow only one input.

27.7 Cabling

The cable used for detectors will be 0,5mm^2 4 Core Mylar stranded wire.

Wire for door monitors will be 0,5m^2 2 Core twisted pair with screen and drain.

28. IP Telephone System

System Description

The System shall function primarily as an IP based Private Automatic Branch Exchange complete for the exclusive use of the Venues Management Staff with a Telephone Management System which shall permit the Management to access telephone traffic, accounting and billing information in a flexible and readily useable manner.

The system shall be located in the Server Room, with the ability to locate operator and management consoles anywhere in the building.

The System shall consist of and include the following:

.1 An IP Switch with all the specified interfaces as required to allow the following capabilities, 240 lines internal, 60 ISDN (PRI – based) external lines, 24 IP trunk channels, interface to TMS, Interface to 3rd party Least Cost Routers.

.2 PC-based switchboard operators consoles, 20inch LCD Monitor, Dual core Pentium machines with headset.

.3 Executive/Secretarial (IP) telephone instrument sets,

.4 Basic (IP) instruments

.5 ISDN digital type, 2B&D, extension instruments, with an arrangement to purchase or hire others at short notice.

.6 On commissioning, the following shall be configured:

- ISDN PRI external lines.
- 24 IP Channel via the network
- 240 internal lines, with a mix of instruments as specified by the client at a later date.

.7 Whilst a total of 240 instruments are specified, the core switch shall be capable of expansion to at least twice this number with no degradation in service by adding interface cards.

.8 A central equipment rack located in the Server Room. Where necessary additional 19” patch racks as scheduled are to be supplied, installed and connected for this purpose

.9 A modem and interface to the Exchange for remote system monitoring and fault diagnostics.

10 A quality, sealed, standby battery supply with separate battery charger/rectifier, and capacity to power all the supplied equipment for a period of 24 hours.

.11 All necessary cabling, wiring, connectors, etc., to effect operation of the System as per this Specification.

.12 A Voice Mail System and a Telephone Management System, with monitoring and accounting interfaces to other building systems, cordless/smart-card cellular phones, as per this Specification and the application needs.

.13 An interface connection to a cellular GSM set for outgoing calls.

.14 A standby battery power supply shall be provided with a charging unit as described hereunder. The supply will consist of:

- A bank of sealed, lead acid batteries of sufficient capacity to maintain the operability of the Exchange, TMS, VMS, interfaces and all options to be considered for such a System, and to the requirements of this Specification for a minimum period of ten minutes in the event of a mains supply power failure; and
- A separate charger, or rectifier/ charger integral with Exchange, which is capable of charging the battery bank from its lowest state to full capacity within two hours and whilst simultaneously supplying the Exchange, System interfaces and options with sufficient power as required.
- Power calculations as to the selection and suitability of the standby power supply for the application defined herein must be provided, that is the size and capacity of the batteries offered, ratings and tolerances of the charger, etc.

.15 A service / management terminal shall be provided to allow detailed diagnostic checks and testing. Details of the types, equipment range and limitations, features and facilities, shall be submitted with each tender. The service terminal shall be programmed to facilitate fault-finding using user-friendly naming conventions

.16 An integrated Digital Voice Announcement System (pre recorded messages) shall be provided as part of the System. It shall incorporate the following features:

.17 It shall provide up to ten digital announcement channels;

- It shall be possible to store at least forty different announcements on the system;
- The duration of each message as stored shall be at least one hundred seconds, but provision need be made to expand this time interval to at least two hundred seconds at some future date.
- It shall be possible for a system administrator to program new announcements via a standard telephone instrument with an acceptable reproduced quality of speech;
- The System shall also incorporate announcement management software to administer the installation of new/changed announcements and provide backup of old announcements; and
- The management software should run on a standard IBM PC or equivalent, ideally on the operator's console and shall be simple to use and user friendly, incorporating such features as touch-screens, voice user-interface, etc. As far as possible this PC shall be the same as that utilised for the TMS facility so as to provide an integrated facility for all PC-based features of the System.

.18 A "Music on Hold" facility shall be provided as part of the System.

- The music source shall be of a compact disc quality of sound or equivalent.
- It shall be possible to couple announcements and operational advice with background music. Tenderers are also required to provide an indication of any separate cost/levy for the South African Music Rights Organisation (SAMRO) royalties.

.19 The TMS offered shall be capable of storing as a minimum, five hundred thousand call records.

.20 The TMS shall be so designed to prevent corruption or loss of data over extended periods, as well as any due to power line fluctuations, and induced transients.

Voice Mail/Messaging System

A Voice Mail or Messaging System(VMS) shall:

- allow callers to leave messages for staff, visitors or pupils who are either engaged, where there is no reply, or if the person does not wish to be disturbed: the called party can then retrieve any messages at a convenient time;
- have a collection of software numbered mail boxes, being configurable to a location number the same as the user's extension number or a user group/section number, for example each department/class group;
- provide security codes for each member or user of service to permit personalised retrieval of messages: it will only be possible to change the message by the enrolled user (i.e. called party) from his/her mail box.
- The System shall cater for 240 voice mail boxes on commissioning but be readily configurable to one thousand voice mail boxes in units of at least a hundred, as needed.
- The VMS shall give a message waiting indication to an extension mail box holder through the Exchange which shall be identified at the correct extension by means of a soft-ring. Pupils and staff shall retrieve messages by dialling up the relevant mail box number.
- Internal and external calls diverted to the mail box via "call forwarding" or "follow-me" shall go directly into the mailbox assigned to that extension. The VMS shall ask the caller for confirmation and then allow a message to be deposited.
- After retrieving a message, it will be possible to immediately send a reply to that caller without re-keying the caller's extension number.
- The mailbox holder shall be able to receive an indication of the date and the time the message was deposited.
- During retrieval, it shall be possible to retain, delete or re-transmit messages to another mailbox. It shall also be possible to add a verbal note at the beginning of a re-transmitted message.
- It shall be possible for users to record their own messages.
- Each user shall have a total of six messages of about forty second duration.

29. Cabling and Wiring

General

The cable sizes and types shall be as specified on the cable schedules.

Cable lengths indicated on the drawings and cable schedules are to be used as guidelines only.

Prior to delivery of any cable, the Contractor shall establish that its dielectric is sound, all cores are correct and continuous from end to end and that all cables are free of any visible defects. Any cost arising due to defects on cables, including installed cables, prior to hand over will be for the Contractor's account.

The Contractor shall ensure that core colours / numbers are maintained throughout the installation to avoid confusion, and that colour coding conforms to the drawing requirements.

Cable ends shall be sealed or capped immediately after cutting. This applies for the cable to be used as well as that remaining on the drum.

Joints in cables are prohibited unless the route lengths exceed the maximum drum lengths manufactured. In this eventuality, approved proprietary types of junction boxes shall be used. Jointing will need approval from the Engineer.

All cables shall be supported as specified in relevant Governmental Regulations.

All cables and terminations shall be secured and connected as to prevent undue mechanical stress upon glands, conductors or terminals.

Cable Routes

The cable routes indicated on the drawings are indicative only and actual routes shall be determined on site by the Contractor with approval from the Engineer.

Should selected routes be found to be unsuitable because of prospective obstructions, spillage of solids or liquids, or excessive temperatures, prior approval for deviations shall be obtained from the Engineer.

All cables shall be grouped and run according to the arrangements as shown on the project drawings. No installation of cables should commence without the prior approval of the Engineer in order to prevent the unnecessary crossing of cables, and to promote carefully planned routes.

No cables shall be double-banked on racks, without the approval of the Engineer. Cables are to be installed in a neat and planned manner to enable later additions and replacements.

No cable shall be buried directly in the ground without the approval of the Engineer.

Cables shall be suitably supported on structures and routed in accordance with project drawings.

Security/CCTV signal cables and 230 VAC power cables shall be separated wherever possible.

Where security signal cables and power cables run on parallel routes for distances greater than 5 meters, they shall be separated by a minimum distance of 300mm.

Perpendicular runs shall have a segregation of at least 150mm. Any deviation from this requirement shall be approved by the Engineer in writing.

Where security signal cables and security cables run on parallel routes, they shall be separated by a minimum distance of 50mm.

Installation

Where cables rise from a trench, or pass through a floor, they shall be protected against impact damage by 2mm thick galvanised pipes or other appropriate means, which shall extend at least from 50mm below to 350mm above transition points.

Holes for cables passing through steelworks shall be made smooth or bushed to prevent damage to the cable.

Conductors shall not be carried over or bent around sharp corners or edges. All bends shall be to the cable manufacturers' specification.

Conductors passing through holes in chassis or screens shall be fully protected by correctly fitted grommets or bushes.

Conductors carried across a hinged portion of a chassis or door shall be flexible.

Sufficient slack shall be provided to obviate tension. Sufficient slack shall be left at the conductor ends to allow the attached components to be removed for inspection and servicing, and to remake the ends.

Cables shall enter an enclosure from below only, and shall be formed to relieve stress on the cable end. Sealing boots shall be fitted over cable glands where required.

Wiring shall be installed neatly, either saddled or strapped to the panel or supporting steelworks. Where this is not possible or practical, the cable loom shall be strapped together using PVC cable straps available for this purpose. Cotton insulation or thread shall not be used.

Tightening of harness saddles or straps must not result in:

Excessive pressure being exerted, which would result in a reduction of the conductor insulation diameter or wear on the insulation.

Excessive tension.

Unclamped leads shall be free of tension between points of connections.

Un-armoured cables shall be secured to racks by cable ties of Polyamide 6.6. The cable ties shall be halogen free en UV resistant constructed with buckles and designed for use in outdoor areas subject to direct sunlight. The span of strapping shall be such as to prevent sagging of cables and in any event should not exceed 100mm.

In areas not subject to direct sunlight such as electrical panels / boxes and general indoor installations, un-armoured cables shall be secured to racks by cable ties which shall be self-extinguishing, class V2 according to UL-94, constructed with buckles.

Cables running horizontally on racks mounted edgewise must be secured to the racks at 300mm intervals, to prevent sagging of cables.

Cables laid flat in racks parallel with or slightly inclined to the ground or floor surfaces need not be secured to the rack s more often than is necessary to prevent the cables from walking as a consequence of expansion, contraction or vibration.

Installation of open-ended, capped conduit will be used for secondary cable support where possible.

Solitary cables may also be secured directly to purpose made corrosion resistant angle iron brackets with Engineers approval.

Cable glands

Cables shall be made off in situ and not made off and then moved into position. At the soonest practical opportunity before the commencement of terminating, the

Contractor shall establish that the cables are sound (by testing insulation resistance and for the presence of moisture in the dielectric) and also that all cables are correct and continuous from end to end.

All cables entering junction boxes or field node panels shall be stripped to the inner sleeve only, where the end will be made off with transparent heat shrink sleeves for 20mm.

Cable glands shall be as follows:

PVC insulated cables – un armoured.

ENVIRO, fixed nipple compression gland, complete with retaining washer and neoprene compression bush.

PVC insulated cables – armoured.

ENVIRO armoured, adjustable, mechanical cable gland.

The Contractor shall also include for the drilling of any gland holes required in gland plates and the supply of transparent heat shrink, strapping or other materials necessary to complete the termination.

Special care shall be taken by the Contractor when drilling holes in the gland plates for cables to ensure maximum use of space on the area of the gland plate and not to have any unused holes, which will affect the I.P. rating of the enclosures. All unused gland holes shall be sealed off with appropriate Pratley Enviro gland stoppers, which come with all the necessary accessories, such as seals and nuts.

Cable Termination

Terminations shall be made in a professional manner, with particular attention to the cleanliness of tools, materials and working site.

Wiring inside panels or junction boxes shall be well planned and neatly arranged in the best possible manner, allowing for forming of wires so that there is no strain put on them. Where flexible wiring is used, logical groups of wiring shall be tied together by means of cable ties in a neat and orderly manner.

A proprietary type of wire stripper must always be used. The stripping tool must be checked regularly and is subject to inspection by the Engineer.

When the type of insulation is suitable, a hot wire stripper is recommended. No stranded conductors shall be fitted if any one strand has been damaged or broken.

At terminations, cables shall be secured and connected in such a manner as to prevent undue mechanical stress on glands, conductors or terminals.

Spare cable cores are to be terminated such that the stripped length of the spare cores exceeds the stripped length of the longest used core.

The Contractor shall refer to the related hook-up drawings for the stripping of the cable inner sleeves and the type, colour and size of the heat shrink to be used.

Leads shall not be twisted together unless this is desirable for a design reason, i.e. to counter inductive effects.

When stripping insulation from conductors, wires strands must not be nicked or cut.

The insulation of a conductor shall not be stripped back further than or less than necessary to affect a secure joint

Wiring shall be arranged such that not more than two conductors are connected to one side of each terminal, with the understanding that the double up of conductors into one terminal should be avoided by using appropriate manufactured links.

All conductors shall be terminated in an insulated double crimped lug of the appropriate type and size, using the proper crimping tool as recommended by the manufacturer of the termination. All crimping tools shall be of the ratchet type and shall be approved by the appropriate lug vendor.

Bare wire terminations will not be accepted. Pin lugs with attached 15mm sleeves for wire marking are to be used with terminal blocks in a strip format. Spade lugs with attached 23mm sleeves for wire marking will be used when terminating under a screw head. Where the space is limited inside any termination point, the Contractor shall provide for the same type of lugs, but without sleeves attached to the lug.

It shall be the Contractor's responsibility to ensure that lugs, tools and dies are of the correct size for the conductors. Enlarging of holes in lugs is strictly forbidden.

The Contractor shall include for the supply and fitting of appropriate lugs and glands to all devices, panels (existing and new) and associated equipment.

All security devices, panels, switchboards and junction boxes, etc., shall be wired in accordance with the project security wiring diagrams and hook-ups and shall be well planned and neatly arranged in the best possible manner. Each wire termination shall be fitted with at both ends with interlocking, engraved plastic cable ferules (black letters on yellow background), reference numbered to correspond with the related schematic or wiring diagrams. Split, clip-on ferrules or adhesive marking tapes may not be used as alternatives.

The marking for horizontal runs shall be read from left to right when facing the cable.

Vertical runs shall be read from bottom upwards.

Cable screens shall be covered with a transparent heat shrink sleeve and earthed where required by drawings. Unearthed screen wires are to be tied back and insulated with heat-shrink sleeve. Under no circumstances may they be cut back.

The stripped length of the spare cores shall exceed the stripped length of the longest used core and strapped together (inside trunks) with heat shrinking tubing, if spare terminals are not provided for the termination of spare cores.

All cables entering field node boxes, junction boxes or control panels shall be stripped to the inner sleeve only where the end will be made off with heat shrink sleeve for 20mm.

Local Termination Boxes

Where indicated in the design documentation, security equipment (new and existing) shall terminate in a locally mounted approved termination box with a short length (1 to 2 meters) of flexible conduit strapped according to an approved support method.

The termination box can be a multiple-way unit to accommodate more than one associated circuit. No top entries are to be used. A suitably sized terminal strip shall be fitted inside the box.

If access to a termination box is limited, the termination box must be mounted in such a manner so as to provide easy access. No termination box shall be fitted more than 2 meters away from the device without the prior approval of the Engineer.

The Contractor shall ensure that termination boxes for security equipment with cast in fly leads shall suit the distance between the termination box and the device.

Termination boxes are to be provided according to the relevant hook-up drawing. Where security equipment housing only provides for one gland entry, but with more than one cable or wire running to the equipment, flexible conduit must be used between the termination box and the equipment. Appropriate glands and seals must be used ensuring that the IP 65 rating is maintained.

Where connection boxes cannot be used, the flexible conduit can be glanded to the normal conduit, with a special fitting that must be made up via the project Engineer

Cable Supports

All cables linking to devices shall run in Kopex conduit to the device, to a maximum length of 1m.

No cable or bundle of cables may run unsupported for a distance exceeding 300mm.

No cable will be strapped or supported to any device or equipment. An approved secondary runner shall be provided.

Racks and conduit cable supports infrastructure shall be installed in the plant as indicated in the project drawings by the Electrical Contractor. Horizontal, flat and face up rack installations shall be limited and only allowed with the approval of the Engineer. Faces down horizontal or flat cable rack installations are prohibited.

The Contractor is required to check, prior to the commencing of installation of racks and supports that routes given in the drawings are:

Sufficient

Unobstructed

Do not obstruct other reserved spaces.

Under no circumstances shall any other equipment be fixed to any security cable rack or secondary runner.

Labeling

Each and every cable and conductor in the installation shall be labelled and identified according to the design drawings and schedules. Labels shall be of the appropriate size Grafoplast printed labels.

Cable cores shall be numbered with Grafoplast S12K range labels and Trasp 200 range cable core sleeves. The labels shall be black writing on white background.

Cables shall be neatly marked for identification as per relevant cable schedules at each end and at 10m intervals along cable runs with the S12K range labels complete with sleeve. The label shall be 10mm high, black writing on white background.

The markers at each end of cables shall be located at the cable glands and shall not be obscured in any way.

The markings for horizontal runs shall be from left to right and for vertical runs from the bottom upwards.

Where a single core cable (i.e. Powax or Coax) enters a panel the numbering shall be installed outside the panel at the gland (as normally the case), and inside the panel according to the core numbering standard.

The markers, tags, sleeves and cable ties shall be self-extinguishing, UV resistant and resistance against extreme atmospheric conditions.

In the event that wiring diagrams do not indicate the required tag number, the Contractor will be responsible to source the project-numbering standard and number the wires accordingly.

All security panels, junction box stations, termination box back plates, etc. shall be marked with ‘Traffolyte’ labels with screwed on label holders.

The labels must be approximately 70mm x 25mm in size and fitted in a suitable label holder. The labels shall be provided by the Contractor and shall be as per hook-updrawing or wiring diagrams.

The same label requirements apply for the terminal blocks inside panels, junction boxes and field nodes to the required size indicated in drawings. The label shall be black writing on white background.

Temporary marking directly on any cable is not permitted unless done with a cable marking pen or removable marking material and approved by the Engineer. The Contractor will also ensure that after installation this marking is completely removed from cables and replaced by approved cable numbering methods.

Split, clip-on ferrules, non-self extinguishing tags or adhesive marking tape are not acceptable.

30. Services Interface Testing

The requirements as outlined in this section are the minimum requirement to be completed by the contractor to demonstrate correct operation of the systems, and for inclusion in the as built manuals on completion of the project

.1 Purpose of Services Interface Testing

To ensure the satisfactory and safe operation of the building. To achieve this each service and the interface of all services must be verified to ensure correct operation under all possible conditions that may be encountered during the operation of the building. The only way to check that this will be achieved, is to initially and correctly test each system in detail and then in conjunction with each other.

.2 Test Co-Ordinator

The Principal Building Contractor(PBC) is contractually responsible for co-ordinating all site activities, and is therefore responsible to plan, organise and program the various sub trades in terms of the site program.

This document is therefore an aide to the PBC and the various sub contractors involved to ensure that the Client can be satisfied that all systems work individually and collectively under all conditions that will be encountered. Notwithstanding anything to the contrary, the ultimate responsibility for the equipment on site and for on site safety aspects remains with the PBC and/or the Contractors. Sub Contractors must therefore be present to operate the relevant plant and to ensure overloading or stressing does not occur.

.3 Test Procedure

Each services sub contractor is to provide an overview of their system, a brief description of how the service operates under the various operational conditions (refer to item 26.5).

.3.1 Individual Services Preliminary Testing

Each service consulting engineer should produce a detailed testing sequence of;

a) tests to be carried for the particular service

b) how these are to be carried out to ensure compliance with the contract documents and specified conditions

c) the testing sequence priority, the required readings and the test equipment to be employed

d) the sequence of tests to suit the system/s and the service completion program starting with the control and safety systems

e) the required final test report

The PBC in conjunction with the particular services contractor prepares a suitable testing program.

The protection, control and safety aspects of each service are to be individually tested by service contractor as per the test report completed prior to permanent power being made available for plant start up (i.e. before driven equipment is started up).

Once this is done then each service can be individually tested and commissioned into service in terms of its intended design function.

Once each service has undergone start up and the respective consultants are satisfied that the plants are operating correctly and safely with the safeties and protection in place the usual on going testing, balancing and setting can continue for each service.

.3.2 Combined Services Preliminary Testing

Each service consulting engineer should produce detailed testing procedure outlining the following;

a) Tests to be carried out with each service to be interfaced with, for their area of responsibility.

b) The testing sequence, required reading and test equipment to be employed.

c) The required final test reports

The PBC in conjunction with the particular services contractor prepares a suitable testing program.

Once this is achieved the interfacing with other systems/services can be tested and commissioned into service.

For each services interface the relevant contractors, consultants, suppliers must be present with the principal contractor or his appointed agent undertaking the overall programming control and co-ordination

.3.3 Combined Services Final Testing And Commissioning

The PBC (with the assistance of the Service Consultants) should produce details of;

a) Test to be conducted for each possible operational condition

b) Testing sequence and required results

c) Equipment required for testing, commissioning

d) Personnel to be present for each test

e) The required final test report

(Refer to item 26.7 for an example of the above requirement.)

.4 Services

The following services generally interface with or rely on another service

a) Electrical
b) Heating, Ventilation & Air-conditioning
c) Sprinkler & Fire Protection
d) Smoke Extraction
e) Lifts
f) Escalators
g) Fire Pumps
h) Domestic Water Pumps
i) Sump Pumps
j) Smoke Detection
k) Ventilation

l) Access & Security
m) Building Management System
n) Public Address

.5 Possible Building Operational Conditions

The generic operational conditions are

a) Normal Conditions
b) Mains Power Failure (Short Duration)
c) Mains Power Failure (Extended Duration)
d) Fire Condition, Mains Power Available
e) Fire Condition During Power Failure
f) Power Failure During Fire Condition

.6 Brief Overview of Tests

Tests should be carried out demonstrating the correct operation under all conditions as 26.5

.6.1 Normal Conditions

All services to be operational as they would under normal conditions.

.6.2 Mains Power Failure (Extended Duration)

All services to be operational as they would under normal conditions

Simulate mains power failure.

Ensure correct operation of all essential services.

Re-instate mains power.

Ensure all services return to normal operation.

.6.3 Mains Power Failure (Short Duration)

All services to be operational as they would under normal conditions

Simulate mains power failure and after 30 seconds re-instate mains power.

Ensure all services return to normal operation.

Simulate mains power failure and after 5 seconds re-instate mains power.

Ensure all services return to normal operation.

.6.3 Mains Power Failure (Extended Duration)

All services to be operational as they would under normal conditions

Simulate mains power failure.

Ensure correct operation of all essential services.

Re-instate mains power.

Ensure all services return to normal operation.

.6.4 Fire Condition

All services to be operational as they would under normal conditions

Simulate fire condition in single fire zone.

Ensure correct start-up / shutdown and operation of equipment as required by the fire engineer.

Reset alarm.

Ensure all services return to normal operation.

Repeat test for each fire zone.

Simulate fire condition in multiple fire zones.

Ensure correct start-up / shutdown and operation of equipment as required by the fire engineer.

Reset alarm.

Ensure all services return to normal operation.

.6.5 Fire Condition During Power Failure

All services to be operational as they would under normal conditions

Simulate mains power failure.

Ensure correct operation of all essential services.

Repeat tests as outlined in 26.6.4

.6.6 Power Failure During Fire Condition

All services to be operational as they would under normal conditions

Simulate fire condition in single fire zone.

Ensure correct start-up / shutdown and operation of equipment as required by the fire engineer.

Simulate mains power failure.

Ensure correct re-start and operation of equipment as required by the fire engineer.

Simulate fire condition in single fire zone.

Ensure correct start-up / shutdown and operation of equipment as required by the fire engineer.

Re-instating mains power

Ensure correct re-start and operation of equipment as required by the fire engineer.

Reset alarm

Ensure all services return to normal operation.

.7 Sample of Building Final Services Co-ordinated Testing And Commissioning Schedule

All recorded test, settings, timings of all devices as well as corrective action for system failure to be recorded and attached to the completed item 7.0 and in the relevant manual.

SERVICES CO-ORDINATED TESTING SCHEDULE

Project Reference	
Test Co-Ordinator	

TEST 1

TEST TO VERIFY THE CORRECT SYSTEMS OPERATION UNDER NORMAL CONDITIONS

DATE		TIME ALLOCATED	

ACTION		ATTENDANCE	VERIFIED	COMMENT
	Ensure all services are operating i.e lights, air conditioning, lifts, escalators, ventilation fans, domestic water pumps, fire alarm panel, fresh air fans, all electronic systems, parking control, staircase pressurisation fans, cooking extract fans.		× / ✓	
	Ensure diesel generators, fire pumps, smoke extract fans are set on auto		× / ✓	

SERVICES CO-ORDINATED TESTING SCHEDULE

Project Reference	
Test Co-Ordinator	

TEST 2

TEST TO VERIFY THE CORRECT SYSTEMS OPERATION UNDER LONG DURATION MAINS FAILURE CONDITIONS

DATE		TIME ALLOCATED	

ACTION		ATTENDANCE	VERIFIED	COMMENT
	Ensure all services are operating i.e lights, air conditioning, lifts, escalators, ventilation fans, domestic water pumps, fire alarm panel, fresh air fans, all electronic systems, parking control, staircase pressurisation fans, cooking extract fans.		✗ / ✓	
	Ensure diesel generators, fire pumps, smoke extract fans are set on auto		✗ / ✓	
Trip Mains Power	Generators to start up, run up to speed and send signal to Main L.V. Board/s to activate changeover			
	Emergency Lighting to remain operational		✗ / ✓	
	Change over to take places within 15 seconds of power failure.		✗ / ✓	
	Schedule of equipment to run on generators to be produced, and checked		✗ / ✓	
	The delayed start up times of the above loads to be measured and recorded.		✗ / ✓	
Re-instate Mains	The essential loads to continue running on generator supply for +/- 30 seconds		✗ / ✓	
	Change over from generator to mains at Main LV. Board/s to take place		✗ / ✓	

SERVICES CO-ORDINATED TESTING SCHEDULE

Project Reference	
Test Co-Ordinator	

TEST 3

TEST TO VERIFY THE CORRECT SYSTEMS OPERATION UNDER SHORT DURATION MAINS FAILURE CONDITIONS

DATE		TIME ALLOCATED	

ACTION		ATTENDANCE	VERIFIED	COMMENT
	Ensure all services are operating i.e lights, air conditioning, lifts, escalators, ventilation fans, domestic water pumps, fire alarm panel, fresh air fans, all electronic systems, parking control, staircase pressurisation fans, cooking extract fans.		✗ / ✓	
	Ensure diesel generators, fire pumps, smoke extract fans are set on auto		✗ / ✓	
Trip Mains Power	Generators to start up, run up to speed and send signal to Main L.V. Board/s to activate changeover			
	Emergency Lighting to remain operational		✗ / ✓	
	Change over to take places within 15 seconds of power failure.		✗ / ✓	
Re-instate Mains	The essential loads to continue running on generator supply		✗ / ✓	
Trip Mains Power After 2 seconds	The essential loads to continue running on generator supply		✗ / ✓	
Re-instate Mains	The essential loads to continue running on generator supplied for +/- 30 seconds		✗ / ✓	
Trip Mains Power During Generator Rundown Period	Generators to take load immediately		✗ / ✓	
Re-instate Mains	The essential loads to continue running on generator supply+/- 30 seconds		✗ / ✓	
	Change over from generator to mains at Main LV. Board/s to take place		✗ / ✓	

SERVICES CO-ORDINATED TESTING SCHEDULE

Project Reference	
Test Co-Ordinator	

TEST 4

TEST TO VERIFY THE CORRECT SYSTEMS OPERATION UNDER FIRE CONDITIONS

DATE		TIME ALLOCATED	

ACTION		ATTENDANCE	VERIFIED	COMMENT
	Ensure all services are operating i.e lights, air conditioning, lifts, escalators, ventilation fans, domestic water pumps, fire alarm panel, fresh air fans, all electronic systems, parking control, staircase pressurisation fans, cooking extract fans.		✗ / ✓	
	Ensure diesel generators, fire pumps, smoke extract fans are set on auto		✗ / ✓	
Activate Fire Alarm (Zone 1)	Ensure alarm is audible		✗ / ✓	
	Schedule of equipment to run on fire signal to be produced, and checked		✗ / ✓	
	Cause and Effect Schedule to be produced, and checked		✗ / ✓	
Reset Fire Alarm	Ensure audible alarm stops		✗ / ✓	
	Ensure all equipment returns to normal operation.		✗ / ✓	
Activate Fire Alarm (Zone x)	Repeat test for all zones		✗ / ✓	

SERVICES CO-ORDINATED TESTING SCHEDULE

Project Reference	
Test Co-Ordinator	

TEST 5

TEST TO VERIFY THE CORRECT SYSTEMS OPERATION UNDER FIRE CONDITIONS DURING POWER FAILURE

DATE		TIME ALLOCATED	

ACTION		ATTENDANCE	VERIFIED	COMMENT
	Ensure all services are operating i.e lights, air conditioning, lifts, escalators, ventilation fans, domestic water pumps, fire alarm panel, fresh air fans, all electronic systems, parking control, staircase pressurisation fans, cooking extract fans.		× / ✓	
	Ensure diesel generators, fire pumps, smoke extract fans are set on auto		× / ✓	
Trip Mains Power	Generators to start up, run up to speed and send signal to Main L.V. Board/s to activate changeover			
	Emergency Lighting to remain operational		× / ✓	
	Change over to take places within 15 seconds of power failure.		× / ✓	
Repeat Test 4				

SERVICES CO-ORDINATED TESTING SCHEDULE

Project Reference	
Test Co-Ordinator	

TEST 6

TEST TO VERIFY THE CORRECT SYSTEMS OPERATION OF MAINS POWER FAILURE UNDER FIRE CONDITIONS

DATE		TIME ALLOCATED	

ACTION		ATTENDANCE	VERIFIED	COMMENT
	Ensure all services are operating i.e lights, air conditioning, lifts, escalators, ventilation fans, domestic water pumps, fire alarm panel, fresh air fans, all electronic systems, parking control, staircase pressurisation fans, cooking extract fans.		✗ / ✓	
	Ensure diesel generators, fire pumps, smoke extract fans are set on auto		✗ / ✓	
Activate Fire Alarm (Zone 1)	Ensure alarm is audible		✗ / ✓	
	Schedule of equipment to run on fire signal to be produced, and checked		✗ / ✓	
	Cause and Effect Schedule to be produced, and checked		✗ / ✓	
Trip Mains Power	Generators to start up, run up to speed and send signal to Main L.V. Board/s to activate changeover			
	Emergency Lighting to remain operational		✗ / ✓	
	Change over to take places within 15 seconds of power failure.		✗ / ✓	
	Equipment to re-start in fire mode, running on generator .		✗ / ✓	
Re-instate Mains	The fire loads to continue running on generator supplied for +/- 30 seconds		✗ / ✓	
	Change over from generator to mains at Main LV. Board/s to take place		✗ / ✓	
	Equipment to re-start in fire mode		✗ / ✓	
Reset Fire Alarm	Ensure audible alarm stops		✗ / ✓	
	Ensure all equipment returns to normal operation.		✗ / ✓	

.8 Safety

Appropriate equipment to be provided to ensure the safe undertaking of the testing, including two way radios for communication between various parties, Hearing protection for persons in generator / plant rooms, torches and safety lighting.

All persons on site are to be made aware of the test schedule.

.9 Operation And Maintenance Manuals

All recorded test, settings, timings of all devices as well as corrective action for system failure to be recorded and attached to the completed item 7.0 and in the relevant manual.

On completion of the tests, the system overview, how the system operates under the various building functional conditions and the remedial action should the system fail to operate correctly for the various building operational