

Project 1 Specs

ELECTRONIC SECURITY SYSTEMS

10.01 GENERAL

10.01.1 The works to be executed under this section of the contract shall include the supply, erection, installation, connection and testing of the complete electronic security systems in accordance with this specification and details shown on drawings.

10.01.2 The electronic security systems will include the following systems:

? CCTV Surveillance

? Access Control and Addressable Door Monitoring

? Guard Patrol

? Doorphone Intercommunication

? Integration of all Systems

10.01.3 All equipment shall be thoroughly inspected and functionally tested at the manufacturer's facilities prior to shipment to the site.

10.01.4 With the tendering proposal the Contractor shall supply a full set of drawings, specifications and catalogues to describe fully the proposed system and its concept.

10.01.5 All items of this specifications not fully met by the Contractor's tendering proposal must be formally indicated and documented by the Tenderer with specific reference to the relevant paragraph of the specification.

10.01.6 Tenderers may propose their own standard in production design alternatives to achieve this specification. The tender submission shall include certificates of conformity with standards, full details of design, variations, limitations and alternative or additional features provided.

10.01.7 The electronic security systems shall be interfaced with the Building Management System (BMS) which will be provided as part of the Mechanical Installations. This interfacing will provide facilities of specific control functions and communications to the specific system in an

alarm situation. This interfacing shall use a proprietary industry-standard network of open architecture such as Lonworks or equivalent. The responsibility of the interface connections and all necessary communication gateways between electronic security systems and the BMS shall be wholly on the electronics system's provider.

10.01.8 All components of the proposed systems shall be CE marked. The manufacturer of the systems shall be approved to ISO9002 quality system standard for the design and manufacture of such systems. The basic equipment of the systems shall be approved and certified by UL.

10.01.9 All the systems shall be provided with free support from the manufacturer. Also all software upgrades shall be provided free of charge to the Employer.

10.02 CCTV SURVEILLANCE SYSTEM

10.02.1 The System

10.02.1.1 A colour closed circuit television (CCTV) surveillance system shall be provided as specified in this section. Location of the cameras and of remaining equipment shall be as shown approximately on the drawings.

10.02.1.2 The system architecture shall be a state of the art IP video security solution that provides seamless management and integration of digital video, audio and data across an IP network. The video management system shall be designed to work with third party cameras. Video from other sites may view from single or numerous stations simultaneously at any time. Cameras, recording stations and receiver stations for viewing only may be placed anywhere in the IP network.

10.02.1.3 The CCTV system shall be furnished complete with all network equipment including the required hubs, routers, 19" equipment racks as indicated on the drawings.

10.02.1.4 The system shall provide digital video storage facilities to support 4 CIF, MPEG 4, at least 12.5 fps at full resolution for 16 hours per day for at least 20 days.

During the execution of the works the manufacturer of the system will confirm in writing, for a formal approval by the Engineer, his calculation of the required capacity of the proposed discs for conformity with this specification requirement.

10.02.1.5 All equipment and materials shall be standard components that are regularly manufactured and utilised in the manufacturer's proposed system. They shall be thoroughly tested and proven in actual use. The tendering proposal shall include a reference list of similar projects already carried out by the manufacturer.

10.02.1.6 The CCTV surveillance system shall be fully integrated with the Access Control System, and Alarm Door Monitoring System into

ELECTRONIC SECURITY SYSTEMS

10.01 GENERAL

10.01.1 The works to be executed under this section of the contract shall include the supply, erection, installation, connection and testing of the complete electronic security systems in accordance with this specification and details shown on drawings.

10.01.2 The electronic security systems will include the following systems:

- ? CCTV Surveillance
- ? Access Control and Addressable Door Monitoring
- ? Guard Patrol
- ? Doorphone Intercommunication
- ? Integration of all Systems

10.01.3 All equipment shall be thoroughly inspected and functionally tested at the manufacturer's facilities prior to shipment to the site.

10.01.4 With the tendering proposal the Contractor shall supply a full set of drawings, specifications and catalogues to describe fully the proposed system and its concept.

10.01.5 All items of this specifications not fully met by the Contractor's tendering proposal must be formally indicated and documented by the

Tenderer with specific reference to the relevant paragraph of the specification.

10.01.6 Tenderers may propose their own standard in production design alternatives to achieve this specification. The tender submission shall include certificates of conformity with standards, full details of design, variations, limitations and alternative or additional features provided.

10.01.7 The electronic security systems shall be interfaced with the Building Management System (BMS) which will be provided as part of the Mechanical Installations. This interfacing will provide facilities of specific control functions and communications to the specific system in an alarm situation. This interfacing shall use a proprietary industry-standard network of open architecture such as Lonworks or equivalent. The responsibility of the interface connections and all necessary communication gateways between electronic security systems and the BMS shall be wholly on the electronics system's provider.

10.01.8 All components of the proposed systems shall be CE marked. The manufacturer of the systems shall be approved to ISO9002 quality system standard for the design and manufacture of such systems. The basic equipment of the systems shall be approved and certified by UL.

10.01.9 All the systems shall be provided with free support from the manufacturer. Also all software upgrades shall be provided free of charge to the Employer.

10.02 CCTV SURVEILLANCE SYSTEM

10.02.1 The System

10.02.1.1 A colour closed circuit television (CCTV) surveillance system shall be provided as specified in this section. Location of the cameras and of remaining equipment shall be as shown approximately on the drawings.

10.02.1.2 The system architecture shall be a state of the art IP video security solution that provides seamless management and integration of digital video, audio and data across an IP

network. The video management system shall be designed to work with third party cameras. Video from other sites may view from single or numerous stations simultaneously at any time. Cameras, recording stations and receiver stations for viewing only may be placed anywhere in the IP network.

10.02.1.3 The CCTV system shall be furnished complete with all network equipment including the required hubs, routers, 19" equipment racks as indicated on the drawings.

10.02.1.4 The system shall provide digital video storage facilities to support 4 CIF, MPEG 4, at least 12.5 fps at full resolution for 16 hours per day for at least 20 days.

During the execution of the works the manufacturer of the system will confirm in writing, for a formal approval by the Engineer, his calculation of the required capacity of the proposed discs for conformity with this specification requirement.

10.02.1.5 All equipment and materials shall be standard components that are regularly manufactured and utilised in the manufacturer's proposed system. They shall be thoroughly tested and proven in actual use. The tendering proposal shall include a reference list of similar projects already carried out by the manufacturer.

10.02.1.6 The CCTV surveillance system shall be fully integrated with the Access Control System, and Alarm Door Monitoring System into card

10.03.8 The VOS shall be a map based CCTV management software. A map edition tool shall allow the user to create easily his own Graphical User Interfaces (GUI) from a wide variety of sources for screen maps (Autocad files Bitmap etc.). A site map shall include the position of the cameras and the map of the situation. A site map shall contain a number of different editable elements such as graphical elements or pictures, text, camera icons, etc. The icons on a site map shall be interactive and allow:

- Drag and drop of a camera on a monitor.
- Camera connection with a "click" action on

the camera.

- Start of an alarm scenario.
- A hyperlink to another site map.
- Activation of a relay output.
- Instant replay function.

10.03.9 In case that a camera video signal is lost, the VOS shall have the capability to alert the system's administrator. The VOS shall receive all incoming events from the electronic security systems (access control, burglar alarm devices such as motion detectors, magnetic contacts etc.) and shall take appropriate action based on user defined programmes. The VOS shall create an audit trail of events and user activities. The log file shall be editable and searched for specific events.

10.03.10 A master real time clock shall control the timing of time-based functions in the system. Discrete events may be programmed for timer activation, including camera-monitor switching, starting of sequences, alarm inputs, enable/disable patterns etc.

10.03.11 Passcode protection of the programming screens shall be provided. All programme information shall be returned during power outages and shall automatically reload on the system upon termination of the outage.

10.03.12 The VOS shall provide facilities of archive viewing. It shall have the following minimum capabilities:

- ? Video playback of any time span.
- ? Multiple video sequences at once.
- ? Shall allow the operator to select between synchronous playback of all selected video streams, allowing the operator to view events from multiple angles or across several camera fields.
- ? Shall allow the operator to control the playback with play, pause, forward, back, next frame and speed selection buttons.
- ? Shall display a single timeline with which the operator can navigate through the video sequence by simply

clicking on any point in the time line.

? Shall support frame-by-frame playback as well as playback of video at $\frac{1}{4}$ to 4 times the normal speed.

? Shall be capable to retrieve archived pictures by means of time, date, camera and site.

? Shall support digital zoom on playback video streams.

? Shall provide still image export to JPEG with date and time on the image.

The setting of bit rate, frame rate and resolution of each camera must be independent and selectable. The alteration of these settings to one camera will not affect the settings of other cameras.

10.03.13 A menu feature shall allow the operator/administrator to select the quality (1/4 to 4 CIF), or level of compression of images recorded during normal operational (1 fps to 25 fps). At least three compression levels shall be available: super, normal and extended record.

? The video window allows live viewing of video and live audio communications with individual video encoders/decoders.

? Shall enable operators to choose from a number of possible camera display patterns ranging from 4 tile patterns to 16 tile patterns.

? Shall display all cameras attached to the system

? All cameras, sequences and analogue monitors shall be displayed in a logical tree

? The operator shall be able to drag and drop a camera from a tree of cameras into a window or an analogue monitor icon for live viewing

? Shall support Mapping functionality, where digital maps are used to represent the physical location of cameras and other devices throughout the surveillance system. The mapping functionality shall be able to import maps from any graphical software supporting BMP,

JPEG and/or GIF image formats

? The operator shall be able to drag and drop a camera from a map into a window for live viewing

? The operator shall be able to click on an icon in a map to initiate a camera

card

10.03.8 The VOS shall be a map based CCTV management software. A map edition tool shall allow the user to create easily his own Graphical User Interfaces (GUI) from a wide variety of sources for screen maps (Autocad files Bitmap etc.). A site map shall include the position of the cameras and the map of the situation. A site map shall contain a number of different editable elements such as graphical elements or pictures, text, camera icons, etc. The icons on a site map shall be interactive and allow:

- Drag and drop of a camera on a monitor.
- Camera connection with a "click" action on the camera.
- Start of an alarm scenario.
- A hyperlink to another site map.
- Activation of a relay output.
- Instant replay function.

10.03.9 In case that a camera video signal is lost, the VOS shall have the capability to alert the system's administrator. The VOS shall receive all incoming events from the electronic security systems (access control, burglar alarm devices such as motion detectors, magnetic contacts etc.) and shall take appropriate action based on user defined programmes. The VOS shall create an audit trail of events and user activities. The log file shall be editable and searched for specific events.

10.03.10 A master real time clock shall control the timing of time-based functions in the system. Discrete events may be programmed for timer activation, including camera-monitor switching, starting of sequences, alarm inputs, enable/disable patterns etc.

10.03.11 Passcode protection of the programming

screens shall be provided. All programme information shall be returned during power outages and shall automatically reload on the system upon termination of the outage.

10.03.12 The VOS shall provide facilities of archive viewing. It shall have the following minimum capabilities:

? Video playback of any time span.

? Multiple video sequences at once.

? Shall allow the operator to select between synchronous playback of all selected video streams, allowing the operator to view events from multiple angles or across several camera fields.

? Shall allow the operator to control the playback with play, pause, forward, back, next frame and speed selection buttons.

? Shall display a single timeline with which the operator can navigate through the video sequence by simply clicking on any point in the time line.

? Shall support frame-by-frame playback as well as playback of video at ¼ to 4 times the normal speed.

? Shall be capable to retrieve archived pictures by means of time, date, camera and site.

? Shall support digital zoom on playback video streams.

? Shall provide still image export to JPEG with date and time on the image.

The setting of bit rate, frame rate and resolution of each camera must be independent and selectable. The alteration of these settings to one camera will not affect the settings of other cameras.

10.03.13 A menu feature shall allow the operator/administrator to select the quality (1/4 to 4 CIF), or level of compression of images recorded during normal operational (1 fps to 25 fps). At least three compression levels shall be available: super, normal and extended record.

? The video window allows live viewing of

video and live audio communications with individual video encoders/decoders.

? Shall enable operators to choose from a number of possible camera display patterns ranging from 4 tile patterns to 16 tile patterns.

? Shall display all cameras attached to the system

? All cameras, sequences and analogue monitors shall be displayed in a logical tree

? The operator shall be able to drag and drop a camera from a tree of cameras into a window or an analogue monitor icon for live viewing

? Shall support Mapping functionality, where digital maps are used to represent the physical location of cameras and other devices throughout the surveillance system. The mapping functionality shall be able to import maps from any graphical software supporting BMP, JPEG and/or GIF image formats

? The operator shall be able to drag and drop a camera from a map into a window for live viewing

? The operator shall be able to click on an icon in a map to initiate a camera

10.03.15.4 The dome cameras shall be designed to perform over a wide range of environmental and lighting conditions and automatically adjust from daytime to nighttime operation. The cameras shall automatically switch from daylight colour operation to a higher sensitivity nighttime monochrome mode when light levels fall below an adjustable threshold level. Daytime / Nighttime operation may also be manually switched on or off from the system's keyboard.

10.03.15.5 The dome camera shall operate from Power-Over-Ethernet (POE) in accordance to IEEE 802.3 at class 4 for indoor applications.

10.03.15.6 The camera shall be equipped with an 26x optical zoom lens. A full 12x digital zoom shall then be functional once the maximum 26x

optical zoom limit has been reached. The 12x digital zoom lens shall be on/off selectable from the system's keyboard.

10.03.15.7 Digital image stabilization shall be provided using a dedicated digital signal processor that filters out vibrations caused by wind and other environmental conditions maintaining a clear image as the zoom range increases. This image stabilization function shall be on/off selectable from the system's keyboard.

10.03.15.8 The camera's 360° pan rotation shall be divided into 16 independent sectors with 16-character titles per sector. Any or all of the 16 sectors may be blanked from the operator. In addition to the blanking function, a privacy masking feature shall be provided that allows creation of up to six (6) rectangular masks that prohibit areas of the field of view from being seen even if the camera is panned, tilted, or zoomed.

10.03.15.9 A fast addressing method or setting the camera address number for control shall be remotely programmable from the system's keyboard or directly settable from the camera.

10.03.15.10 The camera shall allow the storage of up to 64 preset scenes with each preset programmable for 16 character titles. A tour function shall be available to consecutively display each of the preset scenes for a programmed dwell time. Any or all of the presets may be included or excluded from the tour.

10.03.15.11 The camera shall be capable of recording two (2) separate tours of an operator's keyboard movements consisting of, tilt, and zoom activities for a total combined duration time of 15 minutes. Recorded tours can be continuously played back.

10.03.15.12 When an operator stops manual control of the camera, and a programmed period of time is allowed to expire, the camera will execute one of the following programmable options: (a) return to preset, (b) return to the automated tour previously executed, (c) do nothing.

10.03.15.13 The camera shall ensure that any

advanced commands required to program the camera are accessed via three levels of password protection ranging from low to high security.

10.03.15.14 All outdoor cameras shall be provided with surge protection devices.

10.03.15.15 The cameras shall provide consistency of operation throughout their operational life without the need for manual adjustments. Cameras which require regular manual adjustment as normal practice shall not be accepted.

10.03.15.16 The cameras shall be fully compatible with the rest of the CCTV system and shall not cause any degradation of the performance specified. The cameras shall function normally within and ambient temperature of 0°C to 45°C 93% relative humidity.

10.03.16 Fixed Cameras

10.03.16.1 All cameras shall be of high definition (HD) resolution and is to operate on an IP network using H.264 and JPEG compression and bandwidth throttling to efficiently manage bandwidth and storage requirements while delivering outstanding image quality.

10.03.16.2 The cameras shall be day/night and utilise a 1/3" day/night CCD with progressive scan. Their resolution shall be 1280 X 720 pixels at 30 ips 16:9 image format or better. The cameras shall be directly controlled from the video management system with its software to support all camera functions.

10.03.16.3 The cameras shall operate from Power-Over-Ethernet (PoE) in accordance to IEEE 802.3 at Class 3 for indoor applications.

10.03.16.4 The cameras shall conform to the ONVIF standard and shall provide motion and video motion detection analysis system that provides basic video content analysis. They shall provide at least six distinct preprogrammed operational modes stored in the camera. The cameras shall offer intelligent video analysis as a licensable option.

10.03.16.5 The cameras shall provide at least

four independent, fully programmable privacy mask areas. Also the cameras shall provide a lens on-screen facility to allow focusing at maximum lens opening to ensure that the object of interest within the field of view remains always in focus.

10.03.16.6 The cameras shall in addition be provided with the following:

- ? Auto gain control (AGC)
- ? Smart back light compensation (BLC)
- ? A built-in test pattern generator
- ? Signal-to-Noise ratio to be 50dB or better
- ? Upto four generated independent streams simultaneously
- ? Full control and configuration over the network
- ? Local storage feature which shall be capable for automatic network replenishment of central storage
- ? Alarm input for external triggering and a relay output
- ? Capability to display on alarm a display of upto 17 character programmable alarm

message

10.03.16.7 The sensitivity of the cameras shall be such that they will produce a colour image with a minimum scene illumination of 1 lux and a monochrome image when in the night mode with a minimum scene illumination of 0.4 lux. The cameras shall provide enhanced night viewing through the increase of the IR sensitivity by automatic switching from colour to monochrome operation in low-light applications. The IR filter shall be switched manually via the alarm input or remotely over the network.

10.03.16.8 The cameras shall provide consistency of operation throughout their operational life without the need for manual adjustments. Cameras which require regular manual adjustment as normal practice shall not be accepted.

10.03.16.9 The cameras shall be fully compatible with the rest of the CCTV system and shall not cause any degradation of the performance specified. The cameras shall function normally within an ambient temperature of 0°C to 45°C

93% relative humidity.

10.03.17 Dome housings

10.03.17.1 All cameras shall be provided with dome housings which shall be fixed recessed on false ceilings, fixed surface on ceilings or on brackets indoors or outdoors as detailed on the drawings.

10.03.17.2 The housings shall be of colour to the Architects' approval. They shall be protected to an IP44 for indoor use and IP66 for outdoor use. They shall be of antivandal construction IK10 and shall have a cast aluminium housing with a polycarbonate UV resistant dome.

10.03.18 Lenses for Fixed Cameras

10.03.18.1 Unless otherwise specified 1/3" auto iris, varifocal length lenses with 3,5 – 8mm focal range at F1.4-360 iris range shall be provided, to the approval of the Engineer, to achieve adequate fields of view for all cameras at the locations shown approximately on the drawings.

10.03.18.2 At maximum working distance an object 1.8m high shall give a monitor image not less than one-sixth screen height.

10.03.19 CCTV Monitors

10.03.19.1 The CCTV monitors shall be suitable for wall mounting by means of articulated brackets for adjustment in orientation. There will be two main monitors of 50" and the remaining (the quantity of which is as detailed on the drawings) of 20"/21" respectively of viewable picture. The main monitors will be used as alarm monitors to display emergency events which the remaining monitors will be used for routine monitoring. The monitors shall be Full HD LCD type with a minimum of 1080p resolution.

10.03.19.2 The monitors shall be suitable for high resolution HD CCTV applications and shall conform to the ISO 13406-2 standard.

10.03.19.3 The main monitors shall provide a luminance of 700 cd/m² or better. Their contrast ratio shall be 3500:1 or better. The remaining monitors shall provide a luminance of 450 cd/m² or better and a contrast ratio of 4000:1 or better.

10.03.19.4 The monitors shall have performance enhancing features such as picture-in-picture, menu controls to adjust the video features. They

shall have at least the following inputs:

? 1 analogue RGB input

? 1 looping Y/C (5-video) input

? 2 looping composite video inputs

? 1 looping audio input

? 2 digital DVI inputs

? 1 digital HDMI input

? 1 trigger input

10.03.19.5 The monitors shall provide a front panel that allows the user to adjust the image quality, brightness, size, position and geometry of optimal viewing. There shall be a front panel control lockout feature so that only authorized users can adjust menu settings.

10.03.19.6 The viewing angles of the monitors shall be 160° or better. They shall be suitable for operation on 230V, 50Hz ac supply.

10.03.19.7 The monitors shall operate on PAL/NTSC signal formats. They shall in addition meet at least the following requirements:

? Pixel pitch (HXV) : 0.485x0.485mm

(Main)

0.300x0.300mm

(Others)

? Resolution : 1920x1080 pixels, 600

TVL

? Aspect ratio : 16:9

? Display colours : 1073 million (Main)

16.7 million (Others)

? Response time : 8ms

? Backlight : 60000 hours (Main)

50000 hours (Others)

10.03.20 System reliability

10.03.20.1 The MTBF of the complete system shall be at least 100.000. System reliability shall achieve an availability of 99.9%.

10.03.21 Other Ancillary Equipment

10.03.21.1 The system shall be provided with the network hub and routers as indicated on the drawings and as recommended by the system manufacturer to complete the system in all respects.

10.03.22 Mounting Accessories

10.03.22.1 All cameras shall be furnished complete with all mounting brackets, and

accessories as detailed on the drawings or specified. The mounting brackets shall be in cast aluminium and be of colour to the Engineer's approval unless otherwise indicated. The design of the brackets shall be such that to achieve optimum viewing angles.

10.04 CARD ACCESS CONTROL SYSTEM

10.04.1 The System

10.04.1.1 A card access control system shall be installed as specified in this section and shown on drawings. The system shall be able to control and monitor the access to the sensitive areas shown on drawings for preventing unauthorised entry. Authorised access to these areas is gained when a coded access card is read by the system's card reader conveniently located near the access points or manually directly from the Central Control Room.

10.04.1.2 The access control system shall be fully integrated with the CCTV Surveillance System and the Fire Alarm and the Voice Evacuation Systems into a central electronic security system.

10.04.1.3 The system shall be able to control nonmotorised doors indicated on drawings.

10.04.1.4 Each access controlled door, the emergency exit doors and other doors indicated on drawings should be fully monitored so that information is available at the central equipment that the door is in closed position.

10.04.1.5 The card access control system shall be provided with a high level of flexibility and comprehensive system management and reporting facilities. The system shall utilise both access levels and time zones to determine whether access shall be granted. Time lapse between card swipe and door release shall be less than 1.5 seconds and should be specified by the Tenderer at tender stage.

10.04.1.6 The system shall contain all necessary devices such as:

- card reader interface units (ACP's)
- card readers
- electromagnetic door locks
- emergency release buttons (secure side)
- monitoring contacts

- Time and attendance card readers

10.04.1.7 The transaction period shall start upon the issue of the "access valid" signal by the processor and shall be visually or audibly indicated at the card reader. The transaction period shall then be terminated by either the physical "change of the state" on the door status monitor or automatically by the alarm signal, if the pre-programmed transaction period has expired prior to the physical transaction by the card holder.

10.04.1.8 The system shall be based on a card access system using proximity type card readers.

10.04.2 System Capacity

10.04.2.1 The system shall be expandable to at least the capacity listed below without the need of additional hardware:

400No. card readers

1000No. card holders

16No. authorisation levels

10.04.3 System Features

10.04.3.1 The system shall include the following features:

- Entry/Exit designation
 - Antipassback
 - Dual custody
 - Personnel location
 - Alternate time zones
 - Specific features
-
- Printed reports
 - Time and Attendance
 - Addressable door monitoring and controlling

10.04.4 Entry/Exit Designation

Any or all card readers shall be capable of being programmed as either an entry or an exit terminal. Before allowing access under this arrangement, the system shall verify that the reader in question can logically be accessed from the area in which the cardholder is currently recorded.

10.04.5 Anti-Passback

Any or all card readers shall be capable of being programmed as an anti-passback reader. Use of a valid card in this reader shall then prevent the card from being re-used in any other zone reader

for a specified period of time.

10.04.6 Dual Custody

It shall be possible to program any reader within the system as a dual custody reader. Any reader so programmed shall require two different valid card entries and/or insertions of valid unique numerical codes before access is granted to the relevant area.

The valid entries shall be required from two different card/code holders and shall be entered within thirty seconds of each other before access is granted.

10.04.7 Personnel Location

A facility shall be provided whereby an operator can request the location of a card holder by name of identification number and the system will display the terminal which was last accessed by that card.

10.04.8 Alternate time zones

A facility shall be provided to allow specified categories of staff to use specified facilities at certain hours but not during business hours. It

shall be possible to generate a report printout of which personnel availed themselves of this facility during the alternate time zone period.

10.04.9 Time and Attendance (T&A)

(a) The system has a high-end Time and Attendance module

(b) Readers on the access system can double up as a T & A in or T & A out reader for the purposes of Time and Attendance

(c) The access system supports the ability to offer selected clocking data to the T & A module

(d) Full T & A functionally is supported by the T & A module including but not limited to:

? European working hours directive reporting

? Calculation of hours worked and pay patterns e.g. pay + ½ etc.

? Unlimited shift patterns

? Unlimited employees

? Unlimited working patterns

? RS485 and e Series T & A terminals

with user definable menu options

? Manager options for manual clocking
and alterations

? Reasons for leaving site whilst still at
work for pay purposes

? Holiday diary

? Sickness diary

Web browser options including clocking in at an
operative desk.

10.04.10 Printed Reports

It shall be possible to retrieve historic data from
the history files in the form of specific reports.

Reports generated shall generally be as listed:

- a. All card transactions
- b. All transactions for specified identification
numbers
- c. All transactions for specified access
levels
- d. All transactions for specified readers
- e. All transactions for a specified activity
type e.g. exceptions
- f. Programmed history
- g. Password violation
- h. Sign on/off history

- i. Patrol tours
- j. Alarm activity on the CCTV system
- k. Alarm activity on the Alarm monitoring system

Reports shall be for specified start/stop date/time periods. Termination of reports shall be possible at any time by means of a keyboard entry.

10.04.11 Card Reader Interface Unit (ACU)

Surge for substitute ACP → ACU

10.04.11.1 The unit shall be a combination of a card reader controller and a microprocessor unit.

It shall be programmable to handle access control decisions for the connected card readers, alarm reporting on card controlled areas, reporting (alarm on non-alarm) of monitoring points whether or not related to the card access controlled areas and communications with the central processing unit.

10.04.11.2 The interface unit will operate a number of doors and alarms and will be associated with its own power supply. The power supply shall be capable to operate the unit for one hour in the event of total power failure. A

nonvolatile (battery back-up) memory shall store the data base and time of day.

10.04.11.3 The interface unit, which shall be installed within the secure area. The interface unit shall be housed in a key locked cabinet fitted with anti-tamper protection.

The unit shall function continuously as an alarm monitor and access control unit and/or output control unit. It shall be continuously polled by the central equipment. When all card data is valid, the unit shall grant access to the card holder.

Invalid data shall cause a real time exception report to be generated at the central processor at

the central equipment. Exceptions shall not be printed out on the alarms printer unless specifically programmed to do so.

10.04.11.4 The ACP will be connected to the host computer over the Ethernet work. The controller shall have a modular design with downloadable software so that the application program can be easily updated without touching the controller itself.

10.04.11.5 The interface unit card reader combination shall be capable to work also on a standalone basis that is, it shall be capable of maintaining full security checks of correct card access parameters when communication with the central processor has been lost. The interface unit shall provide a timer adjustable from 0 to 60 seconds which shall shunt the alarm contacts on the associated door for the period of the timer whenever access is granted to that door by the reader.

A timer, adjustable from 0 to 60 seconds shall also be provided which shall maintain the electric latch or magnetic lock in a released condition for the period of the timer.

10.04.12 Card Readers

10.04.12.1 The card readers shall only read information of the coded access cards and transmit this information to the central processor unit through the card reader interface unit. The card reader shall have no moving parts and shall require no maintenance. No system compromise shall be possible from circuitry located within the

card reader. The card readers which are to be installed outdoors in the open air should be fully weatherproof.

10.04.12.2 Readers shall provide a numeric keypad in addition to all the features described in clause 10.04.12.1. It shall grant access only after all card data is validated and a numeric code associated with the card and unique to the card holder has been correctly entered in the keypad. The personal identification number (PIN) code shall consist of at least four digits. The keypad shall be suitable for recessed wall mounting and shall be combined as one unit with the card reader.

10.04.13 Access Cards

10.04.13.1 The access cards shall be of laminated plastic and highly resistive to wear or environmental deterioration. Encoded information shall include with a combination of system code and with an individual identification number. The cards shall be virtually impossible to duplicate without facilities of the type used in manufacture. The cards shall have space to accommodate the

Employer's company logo and photograph inscribed on one face of the card. The access cards shall be of proximity type. They shall be suitable for use with the specified high security card readers which incorporate a PIN code in which each of the personal codes allotted bear an encrypted relationship to the individual identification number.

10.04.14 Image Capturing and Badging

10.04.14 1 All appropriate software and hardware should be incorporated into the system to allow Access Control User (Security office in first basement) to capture pictures and signatures and print colour badges.

The system shall use an existing photo ID database for the creation of new, personalised ID badges and allow the user to create new ID badge layouts.

Further to above, the system shall be provided complete with facilities for in-house encoding the system's code and individual identification number on the cards.

10.04.15 Electromagnetic Door Locks

10.04.15.1 The electromagnetic door locks shall be of high quality and be designated for high traffic, high security, fail safe and heavy duty use. The design of the lock shall be such that ensures no residual magnetism to the lock shall provide a holding force of at least 5.5KN with no more than 200mA current consumption. Locks are to operate with 12vDC and be powered by the ACP Power supply to ensure uninterrupted operation in the event of mains power failure.

The lock shall comprise of an armature to be fitted on the top side of the doors and the corresponding electromagnet to be fitted on the door frame. The door locks shall have no moving parts and shall be suitable for rail-safe operation and for surface installation.

Relevant brackets shall be used for different type of doors (refer to construction drawings of doors). The lock shall be equipped with a built - in feature for monitoring "door locked" position of the door leaf.

The feature must not be visible or easy to tamper when the door is closed.

10.04.16 Exit Door Release Buttons

10.04.16.1 The buttons will be used to allow exit from controlled doors in an emergency situation as indicated.

10.04.16.2 The emergency exit button shall be of large diameter (at least 20mm) be coloured in green and shall have a "break-glass" front cover to avoid incidental operation. It shall be fitted with

engraved labelling "EMERGENCY EXIT BUTTON".

10.04.17 Monitoring Contacts

10.04.17.1 All access controlled doors shall be fitted with magnetic reed contact switches for monitoring the closing/operating of each leaf.

10.04.17.2 The magnetic reed contact switches shall generally be recessed mounted on doors for monitoring the closing/opening of each leaf. The exact model, method of fixing, colour as well as the location of the contact switches shall be selected for the purpose they are to be applied to the Architect's approval.

The magnetic reed contacts shall consist of a

reed switch in a sealed plastic enclosure with a fixed cable and a permanent magnet built in to a second housing of similar size and appearance.

The contacts shall be suitable for application on ferrous and non-ferrous materials and for operation at

Ambient temperature -10oC to +40oC

Contact rating 100mA, 50V dc

10.04.17.3 The switch unit shall be mounted on the fixed part of the door (frame) and the magnet unit on the moving part.

10.04.18 Guard Patrol – Checking System

10.04.18.1 The guard patrol-checking system shall be supported and provided by the Access Control System via preselected card readers, shown on drawings.

10.04.18.2 The system shall be capable, by programming of providing the following features:

- Setting of required patrol tours at different times of day and night.
- Present the time period between patrol check-points according to the tour selected.
- Process systems information and raise the

alarm through the central equipment in case any of the preset time periods is not accomplished by the guard.

- Raise the alarm manually from the patrol check-points (card readers).

10.4.19 Disabled Persons Toilet Alarm

System

10.04.19.1 The disabled persons toilet alarm system shall be designed to provide a reliable and easy method of cabling for assistance. The system shall form part and be fully integrated with the access control system. Its connection shall be made via the nearest ACP interface unit from which its low voltage 24V supply will be derived from.

10.04.19.2 The system shall contain all components necessary for a complete system including self-adhesive stainless-steel disabled WC door sign and full installation and operation instructions. When assistance is required, a ceiling pull cord located within easy reach from the toilet should be operated activating a reassurance LED light on the reset unit within the

respective WC, raising and transmitting an alarm signal to the central security control room and at the same time shall give a local audible and visual alarm on the external side above the WC door. In this case the central monitors of the control room shall display the alarm indicating at the same time the exact location of the WC in alarm. The reset function shall only be available from the respective WC.

10.04.19.3 The main components of the system will include:

A ceiling pull switch will be located above the toilet area such that it is easily accessible to the user. The pull cord shall have a 3m long, fully adjustable cord with easy to operate "G" loop. When assistance is required the loop is gently pulled to activate the alarm. The unit shall be equipped with a reassurance LED indicator to confirm that a call has been generated and transmitted and help is on the way.

? A reset unit shall be installed on inside wall of the toilet. It should allow the call unit to be reset manually at the point of

call. The unit shall be fitted with an integral LED reassurance indicator.

? An overdoor light / sounder unit shall be installed on the external side of the toilet.

The unit shall provide a visual flashing indication and audible sound local to the toilet to draw immediate attention of the neighbourhood. The unit shall have a bright red or amber colour led light diffused through a pyramid lense cover.

The unit shall have also an integral highoutput sounder.

? A local controller is necessary for the system's operation. It shall operate at 24V voltage supply.

10.04.20 Power Supply

10.04.20.1 Power supply to all the parts of the access control system, the interface units (ACP) and including the electromagnetic door locks, shall form part of this contract and therefore it shall be included.

10.05 CENTRAL EQUIPMENT OF SECURITY SYSTEMS

10.05.1 General

10.05.1.1 The central equipment shall be installed in security control room at the first basement of the building as shown on drawings.

10.05.1.2 The exact arrangement and equipment layout will be agreed with the Employer, the Architect and the Engineer during the execution of the works.

10.05.1.3 The tenderers may propose their own standard in production design alternatives to achieve this specification. The tender submission shall include full details of the design, variations, limitations and alternative or additional features, provided.

10.05.1.4 The central equipment shall provide control, monitoring and programming facilities and they shall allow interactive control on a common platform with the Access Control, the CCTV Surveillance and the Fire Alarm and Voice Evacuation systems.

Integration of systems (Access Control, CCTV, Burglar Alarm) shall be completely seamless and

shall be done through direct software link and not through mechanical contacts or inputs / outputs.

10.05.1.5 The system shall be menu driven and shall require the minimum of key strokes for any operation. The central processors of the system and operating software shall have a multilevel priority interrupt structure proven in multitask real time applications. It shall allow simultaneous monitoring and data base modification without degradation by the function. The system shall provide a graphical user interface which shall accept a wide variety of sources for screen images (Autocad, Bitmap Graphical etc). It shall use a special configuration tool to automatically configure the system. The installation drawings, the device type and location, zoom areas and zoom magnification shall be made available and imported in the system from Autocad files. The map edition tool shall allow the user to create easily his own graphical user interfaces. A site map shall include the position of the devices of the respective system and the map of the situation. A site map

shall contain a number of different editable elements such as graphical elements or pictures, text, icons etc. The icons on a site map shall be interactive and allow:

- drag and drop of an element to perform specific function.
- connection of an element with a "click" action on the element as applicable.
- start of an alarm scenario.
- a hyperlink of another site map.
- activation of a relay output.

10.05.1.6 The processors shall be equipped with power supply and malfunction monitoring and shall include automatic restart facilities.

10.05.1.7 The system shall continuously and fully monitor all the system's devices and wiring such that the current processor programme shall be interrupted and the failed device or a cable break/short circuit shall be displayed to the operator as an alarm and logged.

10.05.1.8 The system shall have the facility of being connected via a communication link to a remote manned centre for alarm monitoring and

supervising system's overall performance.

10.05.2 Systems software

10.05.2.1 This clause of the specification consists of a list of required features. The tenderer shall ensure that the system offered is fully fitted with all necessary software options to ensure compliance with the following requirements.

Features additional to those specified may be included providing that the system offered conforms generally to the concept.

10.05.2.2 The operating system shall be a multitasking highly scalable software solution capable of receiving and processing real time alarm and access control data without data loss. The operating system must be capable of supporting the type of VDU's and printer and all other system operating components. Future requirements for additional VDU's and printers, shall be accommodated by the system without significant programme change.

10.05.2.3 All entries, deletions or modifications to the data base and report generation shall be carried out via the VDU keyboard without

degradation to any function of the system and without interruption to normal operations.

Keyboard echo and system response to execute command shall be immediate to all intents and purposes. Commands involving a search of the disc storage may involve some delay before information is displayed but such delays shall not be excessive and/or result in operator frustration. All data base memory shall be read/write type capable of read/write operations via a VDU keyboard.

10.05.2.4 To ensure security of the system a password shall be necessary to gain access to the system programme and data files. It shall be fully password protected. The highest level shall be capable of the assignment and change of passwords to all levels. Operation commands shall be individually assignable to specific password levels only.

10.05.1.1 The central equipment shall be installed in security control room at the first basement of the building as shown on drawings.

10.05.1.2 The exact arrangement and equipment layout will be agreed with the Employer, the Architect and the Engineer during the execution of the works.

10.05.1.3 The tenderers may propose their own standard in production design alternatives to achieve this specification. The tender submission shall include full details of the design, variations, limitations and alternative or additional features, provided.

10.05.1.4 The central equipment shall provide control, monitoring and programming facilities and they shall allow interactive control on a common platform with the Access Control, the CCTV Surveillance and the Fire Alarm and Voice Evacuation systems.

Integration of systems (Access Control, CCTV, Burglar Alarm) shall be completely seamless and shall be done through direct software link and not through mechanical contacts or inputs / outputs.

10.05.1.5 The system shall be menu driven and shall require the minimum of key strokes for any operation. The central processors of the

system and operating software shall have a multilevel priority interrupt structure proven in multitask real time applications. It shall allow simultaneous monitoring and data base modification without degradation by the function.

The system shall provide a graphical user interface which shall accept a wide variety of sources for screen images (Autocad, Bitmap Graphical etc). It shall use a special configuration tool to automatically configure the system. The installation drawings, the device type and location, zoom areas and zoom magnification shall be made available and imported in the system from Autocad files. The map edition tool shall allow the user to create easily his own graphical user interfaces. A site map shall include the position of the devices of the respective system and the map of the situation. A site map shall contain a number of different editable elements such as graphical elements or pictures, text, icons etc. The icons on a site map shall be interactive and allow:

- drag and drop of an element to perform

specific function.

- connection of an element with a "click"

action on the element as applicable.

- start of an alarm scenario.

- a hyperlink of another site map.

- activation of a relay output.

10.05.1.6 The processors shall be equipped with power supply and malfunction monitoring and shall include automatic restart facilities.

10.05.1.7 The system shall continuously and fully monitor all the system's devices and wiring such that the current processor programme shall be interrupted and the failed device or a cable break/short circuit shall be displayed to the operator as an alarm and logged.

10.05.1.8 The system shall have the facility of being connected via a communication link to a remote manned centre for alarm monitoring and supervising system's overall performance.

10.05.2 Systems software

10.05.2.1 This clause of the specification consists of a list of required features. The tenderer shall ensure that the system offered is fully fitted with

all necessary software options to ensure compliance with the following requirements.

Features additional to those specified may be included providing that the system offered conforms generally to the concept.

10.05.2.2 The operating system shall be a multitasking highly scalable software solution capable of receiving and processing real time alarm and access control data without data loss. The operating system must be capable of supporting the type of VDU's and printer and all other system operating components. Future requirements for additional VDU's and printers, shall be accommodated by the system without significant programme change.

10.05.2.3 All entries, deletions or modifications to the data base and report generation shall be carried out via the VDU keyboard without degradation to any function of the system and without interruption to normal operations.

Keyboard echo and system response to execute command shall be immediate to all intents and purposes. Commands involving a search of the

disc storage may involve some delay before information is displayed but such delays shall not be excessive and/or result in operator frustration.

All data base memory shall be read/write type capable of read/write operations via a VDU keyboard.

10.05.2.4 To ensure security of the system a password shall be necessary to gain access to the system programme and data files. It shall be fully password protected. The highest level shall be capable of the assignment and change of passwords to all levels. Operation commands shall be individually assignable to specific password levels only.

l. The system shall distinguish between a card reader controlled door proper open and forced door alarm.

m. The elapsed time from the occurrence of a first alarm in the system and the report to the VDU, shall not exceed five seconds.

n. All guard commands and actions via the

system keyboard shall be recorded on the history file.

o. Any card reader terminal, which fails to respond when polled, shall be displayed as an alarm on the VDU. All alarm points associated with this failure to respond shall be subject to consequential suppression.

p. Sufficient space of user defined text shall be provided on each alarm display for a description of the alarm point.

Sufficient space for text shall also be provided for guard instructions relating to the alarm point.

q. An alarm queue of a minimum of 100 events shall be provided.

10.05.4 Reports

10.05.4.1 Historical data shall be retrievable as printed reports. As a minimum, reports shall be generated for the following criteria:

- a. Total activity
- b. Start date/time to stop date/time

- c. All point related activity
- d. All operator activity
- e. All activity related to specific points
- f. All data files with specified start/stop limits

10.05.5 Data-Base Built up

10.05.5.1 The Contractor shall, in liaison with Employer, build up the data base of the entire electronic security system during the commissioning period and in any case before the handing over of the contract works. The data base shall be customised to the specific needs of the project.

10.05.6 System Records

10.05.6.1 Indexed retrieval facilities shall be available for accessing stored information files such as:

- a. Records of staff details and security authorisations
- b. Systems block diagram showing all security equipment with messages to the operator. These messages shall include system status, record status as well as

indicate to the operator invalid entries
and alarm indications.

c. Alarm text and services information text.

d. Required action text.

e. Details of maintenance programs.

Information to this file shall be able to be
linked to a time-initiated program for
display/printing at regular intervals.

Access to specified files shall be available only to
specified password levels. All information files
shall be users entered and retrieved via the
terminal keyboard. System's block diagram and
required action text shall be called up
automatically on the occurrence of the relevant
alarm or event.

10.05.7 Key-Boards Operated PC's

10.05.7.1 The PC's shall conform at least with the
following:

? CPU : Intel Xeon E5 Family, 4

cores, 3.3 GHz or better

? Hard disk : 1 TB minimum capacity,

64MB cache memory

? Operating

system

: Windows Server 2008 R2

? Graphics

card

: High resolution NVIDIA

Ge force 8600 or higher

? Ethernet

Card

10/100 Base T

? Monitor : 23" Touch screen

? Sound

card

: YES

10.05.7.2 Operating System Microsoft Windows

XP Professional/Server 2003 standard enabling

communication for live or remote viewing from

local or remote networks. The system should

include software which would allow instant

retrieval of recorder images and remote software

that would allow remote viewing of live or

recorded images plus control of external devices.

10.05.8 Laser Printer

10.05.8.1 The printer shall be latest technology

capable of operating at a minimum speed of 800 characters per second. Printer cable shall be provided by the Contractor.

10.05.8.2 The printer shall be so located that an unimpeded paper feed and discharge path is provided, and receptacles shall be provided for both feed and discharged paper. The printer shall

be housed in a suitable, standalone acoustic enclosure.

10.05.9 CDRW/DVD Recorder

10.05.9.1 Removable data storage and system software updates shall be available through a compact disc rewritable CDRW/DVD recorder, using 80 minutes (700mb) rewritable CD's

10.05.10 Full functions control keyboard with joystick

10.05.10.1 Digital keyboard with full function, to be used for systems control and programming. The keyboard must include an integral variable speed pan/tilt/zoom joystick and a splash resistant design.

10.05.10.2 Functions

The functions to be connected to the network and with menu-driven system must be for new operators to program and control even the largest systems without memorizing system commands.

The keyboard must feature a quick selection menu function, providing immediate access to the most commonly used screen displays.

The keyboard must also feature a user-friendly menu tree approach for programming all advanced system and camera settings.

- Fully compatible with the whole system
- Soft keys Allow for Product-Specific Menus
- Backlit keys & Easy-to-read LCD Displays
- Simplified System Programming
- Multilingual Support
- Plug & Play with the IP system
- Optional PC Software to allow for

Customizable Keys for Use with the system

10.05.10.3 Functionality of central security control

The central security control will consist of CCTV LCD display monitors, GUI keyboard the full

function keyboard with joystick and the DVRS.

All DVR's, GUI, etc., will be programmed by the full function keyboard. Systems demanding additional keyboards will not be accepted.

The display monitors will appear several scenarios without any restriction in combination between any cameras and monitors. Any camera, connected to DVR shall be able to appear at any monitor. The display can be either sequence mode or multiplexed etc.

The two bigger monitors will be used as spot monitor and playback.

10.05.11 Graphical user interface (GUI)

10.05.11.1 The system shall support a graphics function, which shall display building layouts and representations. The system shall display the status of all points on the system (Access, CCTV, Burglar Alarm, Door Monitoring, etc.) using graphical icons which animate when in an abnormal state. The system shall allow status information to be retrieved and remote overrides to be initiated by selecting the appropriate graphical object. The system shall allow any

number of graphical maps to be linked to allow the mouse or touch-screen to be used to zoom in or out of the graphical environment. The system shall allow the graphics to be edited and created whilst the system is fully operational and without degradation in performance. The graphical images shall be capable of being retrieved ready for editing from a standard PC graphics or paint package, AutoCAD or scanner.

10.05.12 Central Power Supply

10.05.12.1 The entire electronic security system as covered by this specification will be served from a central power supply supported by the specified UPS system in Server Room and will be the responsibility of the Contractor. Also the Contractor will provide power supply as necessary to all parts of the electronic security system. The entire electronic security system shall remain operational for at least 12 hours in case of mains failure.

10.05.13 Central Building Integration System (CBIS)

10.05.13.1 The CBIS has an open architecture

design. It supports industry standards for databases, networks, credential printers, video cameras, and more, such as OPC, AutoCAD, HTML, ASPX, and MS-SQL. No customized or proprietary PC software or hardware is required to operate the system.

10.05.13.2 Depending on the configuration or occurring load, the management system runs on one or more servers operating as one system.

One of these servers is the central login server for the operating level. The central login server and optional connection server run under one of the following operating systems:

? Windows 2000 Workstation or Server,

? Windows 2003 server

? Windows XP

Any standard PC hardware should be usable.

Multi-Core, Multi-CPU and high-end redundant hardware solutions are also supported.

The system operation uses networked workstations running under the following operating systems:

? Windows 2000

? Windows XP

? Windows Vista

10.05.13.3 The CBIS must provide a web serverbased solution. Only Internet Explorer is required for a workstation to access the CBIS login server.

The CBIS server, the optional connection servers, and the workstations all connect using a standard IP network. It is also possible for wireless connection of mobile workstations (for example, laptop PCs).

Workstations can connect using Intranet or Internet networks. Location maps and video images are delivered and adapted to the transmission conditions.

Communication between the central CBIS server and the workstations must be encrypted with 128-bit data encryption or better. The system displays the operating status of all servers and workstations/operators.

10.05.13.4 All subsystems, such as fire or intrusion panels, voice evacuation systems, or video devices are connected using the OPC

interface standard. The CBIS monitors these interfaces. The monitoring signals malfunctions and operational availability of the connection to each subsystem in the CBIS user interface.

The OPC server supports the import of existing subsystem configurations for direct use inside the CBIS configuration, avoiding double input of similar data.

It is possible to use OPC servers (software drivers) running on any PC inside the corporate network. Re-installing OPC drivers on the CBIS computer shall be avoided.

The CBIS provides flexible expansion options for the hardware (interfaces, connection server). The connection of subsystems is possible on any connection server in the network. Redundant connections are available when supported by subsystems.

10.05.13.5 Client workstations are connected by standard IP network. Any computer in the corporate network is usable as a workstation. Mobile computers (notebooks) can access the system by wireless network connection (WLAN).

The system is expandable to support an unlimited number of integrated client workstations.

The CBIS user interface is browser based and provides a flexible and simple way (standard HTML format) to adapt to specific requirements, such as different operator groups. The adaptation must be possible with standard HTML editors such as Microsoft Frontpage or Sharepoint Designer.

The CBIS supports up to four monitors per client workstation by using a corresponding graphics card. The user interface is easily adaptable to the number of monitors using standard HTML editors.

The CBIS automatically adapts the screen resolution and number of client workstation monitors from where the operator logs in. It automatically provides the user interface and screen resolution assigned to that operator.

10.05.13.6 The CBIS has a modular structure that provides specific project solutions. The system can be extended at a later date. Common

extensions are the number of operator, subsystem connections, or monitored detector points.

Each module itself is also modular and extendable. The modules and their extensions, as well as all the common system features, must allow any combination, such as access control management with video or intrusion alarm management with video.

10.05.13.7 The system can perform a wide variety of security management and administrative functions as part of a total integrated package. These functions include the following:

- ? Central alarm management and monitoring
- ? Intrusion detection and security management
- ? Fire system and life safety management
- ? Video management
- ? Access control management
- ? 3rd party system support, such as automation systems

10.05.13.8 To support central alarm management and monitoring, the CBIS must provide a wide range of display and control features. The user interface should provide the same look and feel regardless of which alarm comes in.

10.05.13.9 The central alarm management and monitoring provides an alarm/event queue where all incoming events display. At a minimum, the queue must provide the following information:

- ? Alarm date/time
- ? Alarm state
- ? Current alarm state
- ? Alarm location
- ? Operator who is working on the alarm/event when it was acknowledged

Only authorized operators see the alarm. The display is controlled by the alarm/event priority.

The alarm queue provides the acknowledging, deleting, and forwarding of entries. The system must handle up to 5000 alarms/events simultaneously.

10.05.13.10 The CBIS must support the display

of location maps. A standard vector graphics format, such as AutoCAD DWF, is the preferred location map format.

The drawing format for the location maps must support a logical partitioning by defining sub

areas inside the drawing, by marking the area and giving a logical name.

The time-consuming conversion into a bitmap format and the splitting into sections should be avoided. In the case of structural changes inside the drawing (new walls, doors, and so on), no changes inside the CBIS are necessary.

The CBIS must provide a location tree to allow easy selection of locations and sub-locations, such as single floors or rooms. The location tree should have no limits in the number of levels or sub-levels. Creating the location tree and the location names automatically by scanning the drawings for logical sub-areas should be possible. A single click on the location/sublocation should show the assigned graphics or sub-areas with all detector icons visible for that

area.

The CBIS must provide a zoom and pan feature for zooming into a location and move around inside the drawing, simply by using a standard mouse. This allows operators to find a specific detector, door, or reader for fast control, such as open door manually, switch on/off lights, show camera live image, and so on.

The CBIS must support multi-layered drawings and allows layers to be shown or hidden depending on the incoming event. For example, this allows the display of escape routes and fire extinguisher locations when there is a fire alarm. A manual layer control during normal operation must also be possible.

The CBIS must provide a library of standard detector icons for fire and intrusion detectors, doors, readers, cameras, and so on. You can place these icons directly onto the drawing. All assigned control commands are provided when clicking the icon.

When a detector point sends an alarm/event message, the assigned icon animates inside the

drawing, displaying the corresponding event color. The location and the relative size of an icon are definable inside the drawing and should be done by the architect.

The CBIS must provide a means of displaying icons corresponding to the current detector status, e.g.

? Door open - closed – blocked - ...

? barrier: open - closed – blocked - ...

? camera: motion alarm – recording - ...

All icons are provided in a vector format, so that when the operator zooms in and out, the size scales automatically to the view.

Moving the mouse cursor over a detector icon provides a tool tip with detailed detector information, such as complete address, actual status, and detector type.

10.05.13.11 The CBIS must support the display of individual alarm documents/plans depending on the alarm type. Individual documents display for:

? intrusion detection alarms

? fire alarms

- ? access control alarms
- ? video alarms
- ? maintenance and service alarms, such as pollution
- ? 3rd party events

The documents should provide at least the following information:

- ? Alarm/event date and time
- ? Alarm/event state
- ? Alarm/event location
- ? Detector type and detailed address
- ? Detailed instructions/to-do-list

To minimize the number of documents, they must support macros which were dynamically substituted by the real alarm/event data when displayed.

The documents must support the integration of bitmaps, live video, form elements (checkboxes, tables, and so on) as used in Microsoft Office to create specific forms, customizable control buttons to control subsystems directly, and any combination of these items.

The documents must be assignable to locations

inside the location tree to display information when an alarm/event comes from a specific location.

The CBIS must store an unchangeable snapshot of the alarm documents in the event log during alarm/event operation, providing seamless event reporting. The document's format is based on open standards, allowing you to configure them using standard editors.

10.05.13.12 The CBIS must provide a means of basic status overview on all relevant system functions and subsystem devices. This display should be free customizable and placeable individual inside the CBIS user interface.

Possible content should be

? Operators logged in

? all doors open

? all barriers open

? all windows open (magnetic contacts, hinders arming of IDS)

? all detectors in malfunction/technical alarm

? all fire detectors in fire alarm (if fire system

connected)

? all fire detectors blocked

? all detectors in maintenance mode

The content of that status overview or parts of it should be shown only to authorized operators.

A double-click on one of the entries should provide a filtered list with all the individual detectors and devices corresponding to that status.

10.05.13.13 The CBIS must provide timer and schedule functions to support:

? time based display of information

? time based automatic controls into any subsystem

? time based access

The timer supports time frames per weekday, public holidays, and individual special days.

10.05.13.14 The CBIS must support a manual alarm trigger by an operator to allow alarm operating caused, for example, by a bomb threat phone call.

The operator clicks on the relevant location inside the location tree and enters the specific

alarm code. The alarm operating behind that trigger is identical to alarms/events from detectors, which means all assigned documents and drawings are displayed accordingly.

10.05.13.15 The CBIS analyzes all incoming events and messages. It provides a wide range of standard alarm/event states. There should be no limitation in creating additional customer specific states. For each event state, the following parameters are definable:

? State name

? Background/foreground color

? Alarm sound

? Priority

For alarm sounds, standard formats such as WAV, MP3 or WMA are supported. The priority directly controls the order how events are displayed. For example, if an operator is working on a malfunction event, and an intrusion alarm with higher priority comes in, this event is automatically placed in the foreground. The previous event is maintained in the background. The operator can toggle between all events he

has acknowledged on his workstation. Assigned location maps and documentation toggle automatically as well.

The defined colors are used when animating a detector icon which has sent an event.

The CBIS must support the definition of escalation scenarios if an operator does not react within a defined period of time. The CBIS forwards the alarm/message automatically to the next defined and authorized operator group when the time period is exceeded. There is no limitation to the escalation levels. If no operator group acknowledges the alarm, the CBIS supports a separate and automatic way of alarm notification as a final step.

The CBIS provides a feature to the operator that allows the forwarding of events to other operator groups which are also authorized to respond to such events. This allows a workflow.

10.05.13.16 The CBIS supports a multi-client capability that separates message distribution to dedicated operator or operator groups which are permitted to operate on those events. This should

allow at least:

? individual display of locations/location maps

? individual access to subsystems

? individual control into subsystems

? individual assignment of access hardware to

tenants

10.05.13.17 The CBIS must provide a real-time device overview of the entire system's status. All connected subsystems are shown on a status tree, such as intrusion detection system (IDS), fire alarm system, video systems, access control hardware, and individual detectors, as well as internal items, such as server or operator status.

A direct control into subsystems is possible by clicking on panel/detector address.

The device overview supports state filtering/sorting to search for specific states, such as all detectors in malfunction or all doors in an open state.

The states inside the device overview are shown using the same colors as on the detector icon.

10.05.14 Subsystem's Management

10.05.14.1 The CBIS shall provide the advanced

and seamless connection, monitoring and control of OPC-compliant intrusion detection systems and similar security systems, such as hold-up systems or perimeter fence control. It should support the standard detector types typically connected to those systems, such as:

? motion detectors

? glass break sensors

? seismic detectors

? hold up buttons

? magnetic contacts

? Light barriers

? RF barriers

? Input contacts (2- and 4-state mode)

? relay outputs

? and so on

The CBIS must provide the real-time overview on actual status of all connected detectors as well as the typical controls, such as reset, block, or activate single detector points. The CBIS shows all possible states coming from a single detector, such as:

? alarm states, like intrusion or motion alarm

? malfunction states, like pollution or offline

? standby mode

The states are shown with corresponding event color/text and detailed detector group/address. If the detector is assigned to an individual location inside the location tree, the full location path is shown too, immediately identifying where the alarm is coming from.

The CBIS must provide a library of detector icons, directly to be used in location maps, that support direct controlling of the detector by clicking an icon. The CBIS configuration tool provides a simple way of assigning a detector type/icon to the detector addresses inside the subsystems by drag and drop or by auto assignment.

10.05.14.2 The CBIS must allow authorized operators to arm or disarm existing areas/zones defined inside the Intrusion Detection System..

The actual status of the areas/zones are shown real-time in the device overview.

10.05.14.3 Any alarm/event coming from an

Intruder Detection System's detector, the Intruder Detection System's itself, or from a similar system must be displayed real-time to all authorized operators on their dedicated workstations with all corresponding location maps, animated icons, and assigned alarm documents. Parallel alarms/events are stored in the CBIS event log. All operator actions on such an event are also stored in the event log for seamless reporting.

10.05.14.4 The CBIS must be able to link directly to connected video systems. It displays live video from one or more dedicated cameras in the same user interface corresponding to the intrusion alarm/event. The CBIS also allows the automatic trigger of alarm archives in corresponding OPC compliant DVR systems.

Links to such alarm archives are stored in the CBIS event log, and allow direct access to the archive in later reporting.

10.05.14.5 The CBIS provides an advanced and seamless connection, monitoring and control of OPC compliant fire alarm systems. It supports

the standard detector types typically connected to those systems, such as:

- ? smoke detectors
- ? flame detectors
- ? heat detectors
- ? fire push buttons
- ? and so on

The CBIS must provide a real-time overview of the actual status of all connected detectors, as well as typical control functions, such as reset, block, or activate single detector points, or switch them into maintenance mode. The CBIS displays all possible states coming from a single detector, such as:

- ? alarm states, like pre-alarm or fire alarm
- ? malfunction states, like pollution or offline
- ? standby mode

The CBIS displays all states using corresponding event color/text and detailed detector group/address. If the detector is assigned to an individual location inside the location tree, the full location path is displayed, providing immediate information about where the alarm is coming

from.

The CBIS must provide a library of detector icons, to be used directly in location maps, and which support direct controlling of individual detectors by clicking the icon. The CBIS configuration tool provides a simple way of assigning a detector type/icon to the detector addresses inside the subsystems by drag and drop or auto assignment.

The CBIS must allow to switch individual detectors or detector groups into maintenance mode, for operational testing on the fire system and the connected detectors. Activating a fire detector by using test gas or heat causes a maintenance alarm inside the CBIS, and is handled according to the configuration.

The CBIS must allow to deactivate/block individual fire detectors. This helps prevent false alarms if, for example, welding is taking place in the vicinity of a detector or detector group.

The actual status of the fire system, down to the individual detectors, must be visualized real-time in the device overview.

Any alarm/event coming from a fire detector or the fire panel itself must be displayed real-time to all authorized operators, on their dedicated workstations, with all corresponding location maps, animated icons, and assigned alarm documents. At the same time, the CBIS must store the alarms/events in the event log. All operator actions on an event must also be stored to the event log for seamless reporting.

10.05.14.6 The CBIS must allow to link directly to a connected access control hardware or an emergency door management system to open all doors along a dedicated escape route automatically.

10.05.14.7 Seamless Integration with PA or Evacuation Management

The CBIS must allow to trigger automatically announcements in a voice evacuation and p.a. system. With the CBIS timer functions, progressive evacuation scenarios must be definable. This allows, for example, the triggering of the same announcement with a defined delay

for different floors.

10.05.14.8 The CBIS must allow to link directly to connected video systems. It can display live video from one or more dedicated cameras, in the same user interface for the surveillance of an escape route for example. At the same time, the CBIS allows the automatic trigger of alarm archives in corresponding OPC compliant DVR systems. Links to such alarm archives must be stored in the CBIS event log, and allow direct access to the archive when generating reports. The CBIS must provide a fully integrated video management module for interaction with the following video systems:

? DVR systems

? IP video web server

? analog matrix switches

? video encoder/decoder

? IP-based matrix switches based on encoders/decoders

? IP cameras

Any combination of the above systems must be possible to be able to mix existing video

equipment with new devices.

The video management module must at least allow the display of live images from all these sources. The video streaming should be IP based to allow flexible visualization on client workstations. Analog video sources must be converted by an IP-based video web<