Q&A # 2

Date: January 25, 2016
Project: St. John's Security Upgrades Project

Bidders must make sure that their bids are based on the latest version of the tender documents published and take into consideration the following amendments and information, including any information provided in amendments or Q&As previously published for this project.

Bidders that do not comply with this requirement will be discarded.

Q24. Chubb Afx is an all in one platform that will do ULC fire monitoring, Access Control and Intrusion. Please advise if Chubb Afx is and acceptable alternative. A&E spec is attached.

A24. Yes, it is an acceptable equivalent.

All other terms and conditions remain the same

Integrated Intrusion and Access Control Guide Specification

Version 4.9

About This Guideline Specification

The CHUBB AFx Guide Specification has been prepared by CHUBB EDWARDS to aid organisations in the preparation of an RFP document for one the following systems types:

- Access Management System
- Intrusion Management System
- Integrated Access Intrusion System

Whenever possible, organisations are encouraged to use this document as the core of their own security requirements specification.

The CHUBB AFx specification outlines an integrated systems management product that will provide organisations with a comprehensive access control and critical alarm monitoring management system. The system's 32/64-bit multi-user network based graphical desktop, makes this system a perfect fit in today's office networks environment.

The CHUBB AFx Director product has been designed to operate on computers that use Microsoft Windows XP Professional, Windows 2003 Server, Vista Business or Ultimate Edition, Windows 7 Professional 32 or 64 bit and Windows Server 2008 Enterprise R2 32 or 64 bit. As well, the CHUBB AFx Director application has been designed for use within multi-user server/client systems environments, making use of the organisation's Microsoft based local and wide area networks.

The CHUBB AFx specification highlights the many features that have been designed into the system to ensure that a comprehensive solution is provided to any management team needing access management and or critical point monitoring for one or hundreds of remotely managed facilities.

The design philosophy incorporated in the platform ensures that an organisation investing in a CHUBB AFx solution will be protected for years to come. And, at the same time, maintain the most stringent yet flexible access and security privileges needed to protect an organisation's assets.

"Even when those assets are in a single location, multiple locations across town, across the country or even around the world"

CHUBB EDWARDS recommends that all systems providers that are responding to an RFP provide a point by point compliance statement. This is to protect the investing parties.

To maximise your organisation's time efficiencies, the CHUBB AFx product guide specification is available in electronic format. In cases where there are optional sizes or values available, more than one numeric value has been specified. Where this occurs, the optional values have been enclosed in brackets and separated by a slash. When modifying the specification for a project, you may select the value that best suits the project.

Revision	Comments	Date	Author
V4.7	Chubb AFX Guide Specification	8/2008	ARM
V4.7.1	Chubb AFx Guide Specification	5/2012	RD
V4.9	Chubb AFx Guide Specification	6/2013	RD

TABLE OF CONTENTS

Access Management & Event Monitoring System

GENERAL REQUIREMENTS

1.1. Standards

All system components shall conform to the following standards where appropriate:

- Manufacturing: ISO 9002
- Design: MIL 275E
- Communications: IEEE RS232C and RS485
- EMI emissions: FCC part 15
- Electrostatic immunity: IEC 801.2 level 4
- AC transients: UL 864

1.2. Experience

A reliable firm shall manufacture all system components with at least 20 years experience in the development and manufacturing of access control and alarm monitoring products.

1.3. Installation

The supplier shall supply and install all system components covered by this specification.
The supplier shall provide ___complete set(s) of documentation covering installation, operation and maintenance of all system components.
On-site training for a maximum of ___operators for __ days shall be provided as a precondition to acceptance.
The purchaser will provide a dedicated AC power circuit to the point of installation for each system component requiring AC power.

1.4. Support Services

The supplier shall be capable of providing on-going training and service for all system components.

2. SYSTEM SPECIFICATIONS

2.1 Introduction

The system software shall be a Microsoft™ Windows™ 32 or 64-bit multi-user application supporting server/client functionality. The security application software shall support database management, manual and timed control functionality, alarm and transaction monitoring and selective transaction and alarm reporting for single and multiple sites. Management of the system shall be accomplished from on-site LCD keypads, a single host PC or from multiple PCs across a LAN. The system software shall be capable of operating on computers running Windows Server 2003, Windows XP Professional, Windows Vista Business or Ultimate Edition, Windows 7 Professional 32 or 64 bit, and Windows Server 2008 Enterprise 32 or 64 bit.

The general requirements shall include a user interface that:

Incorporates a simple Windows explorer software architecture for accessing the different areas of the program. The system shall also provide the functionality required of an Access Control system and an intrusion system with complete integration of both application modules using a single software product.

Utilises a building block modular approach to facilitate expansion, without expensive and redundant hardware.

The user interface shall incorporate an active graphics module, allowing operators to view doors opening and closing, points changing state, and to perform manual commands such as lock doors, unlock doors, arm areas, disarm areas and bypass points.

2.2 System Architecture

The system software shall be designed for central database management of controllers with upload/download capabilities and full bi-directional database recovery and rebuild functionality between the host software and controllers. The system software shall be used to program each controller from its database while the controllers alone perform all real-time system functions as well as report events and alarms as they occur to the host software. The system software shall have the flexibility of being configured to support a minimum of 30 controllers connected on a polled RS485 communication bus at a single site and a minimum of 30 site controllers connected on an RS485 communication bus at each remote site. The system shall also be capable of supporting ethernet communications between the controllers and software. The host software shall not be burdened with any real-time functions. All real-time control functions shall be the responsibility of each controller.

A single account can consist of up to 250 controllers connected to multiple communications ports including a mix of RS485 and ethernet. Each controller shall support a combination of 24 application modules connected to each controller using a polled RS485 communication bus. The application modules shall include at minimum:

- UL / ULC listed Alarm input/output application module
- ULC listed Access/Reader application module
- UL / ULC listed fire alarm input application module
- UL / ULC listed multilingual (English/French/Dutch/Spanish) LCD keypad application module used for programming, control, reporting, arming, disarming, access control and system maintenance.

- UL listed wireless RF application module.

2.3 Software Organisation

All security administration, control, alarm interfacing and reporting functions shall be available through the desktop, via a “Windows Explorer” menu and control buttons.

The design and organisation of all data entry, control, alarm interface and report screens shall be such that the user does not become lost as new windows are opened. The user interface is to be intuitive to use and designed with the administration of an access control and alarm system in mind. The user shall have the option of entering the database using a grid or form view and be able to switch between views at any time. The form view will display to the user one database record at a time, while the grid view will display the user multiple records at a time, much like a spreadsheet.

2.4 Host Software Specifications

The following are the key features and functions that shall be supported by the system software, as a minimum. Features that are defined as “Unlimited” in capacity shall be limited only by available processing resources including CPU speed, disk space and available RAM on the host computer.

- Graphical User Interface
- 12 languages available, assignable to specific users (English, French, Dutch, Spanish, Simplified Chinese, Traditional Chinese, Russian, Slovak, Hungarian, German, Italian, and Portuguese)
- Relational Database
- Cardholder database; up to 64,000 per controller
- Doors; up to 32 in/out doors (64 readers) per controller / up to 8000 in/out doors (16,000 readers) per site
- Input Points : Up to 256 per controller / 64,000 per site.
- Alarm Instruction/Resolution Notepad
- Powerful Report Generation selectable by Controller Configuration, System Activity, Operator Audit, Time and Attendance and Custom Report by User field
- Relational reports between Events and Database
- Dial-Up or Direct Cable communications with controllers
- Internet Protocol communications via static IP for control, configuration and status information from controllers
- Secure Internet Reporting via connection between a VPN and the Monitoring Centre.
- RS485 polled communications with controllers
- Transaction and alarm filters for the event queue. Filters selectable by each user client.
- All features supported by the controllers shall be programmed using the host software, client software and the LCD. Where there is more than one controller on the site, programming affecting system configuration shall be performed from the host software or one of the client software modules only. Refer to the controller specifications for a detailed listing of system features that shall be supported by the system.
- All programming of data using the LCD keypads shall automatically update the host software’s database.
- Where communications between the host software and the controllers have been interrupted, upon re-establishing communications, the host software shall initiate automatic synchronisation of their databases.

- If changes have been made to the same data using the host software and the LCD keypads while communications between the software and controllers have been interrupted, upon re-establishing communications the synchronisation utility shall detect the difference and present the two changes to the operator if a conflict arises. The operator shall then choose which database change will be stored in the controllers and the host software.

2.5 Controller specifications

Each of the self-contained controllers shall provide all real-time access control and intrusion functionality. Each controller shall be capable of granting access, responding to alarm conditions and shall contain the entire database for the application modules such that the host software is required only for database management, manual control, receiving alarms and reporting purposes.

All software shall reside in read only and random access memory. No moving parts such as disk drives will be acceptable.

Each controller shall utilise a floating, scalable memory grid that shall support a minimum of 1,024 history events, 1000 users and 30 authority levels: a maximum of 65,536 history events, 64,000 users (cardholders) and 1,000 authority levels per controller may be achieved with the addition of RAM (memory) to each controller .

Each controller shall support standard and daylight savings time. This will automatically shift ahead or back all time schedules that affect doors that automatically open and close, valid card access based upon time schedules and all schedules that affect areas that are required to automatically arm and disarm. Once the dates are programmed, the system shall not require editing of these dates each year.

Each controller shall support non-floating holidays, where the position of the day of the week is fixed for the month. Once the holidays are programmed, the system shall not require editing of these dates each year.

Each controller shall incorporate an RS485 communication bus for the connection of the application expansion modules. The controller shall be configured to poll the application modules at either 19K2 baud or 38K4 baud, dependent upon the application modules connected.

Each controller shall incorporate a digital dialler for direct connection to a phone line for the purpose of transmitting alarm signals to a central Monitoring centre. The same communication line will also support paging.

Each controller will support a communications port for direct connection to the host software via a direct cable connection or modem connection. For direct connection applications, the host software shall poll the controllers at 38K4.

2.6 Access Control System Functionality

The system shall incorporate an area centric methodology, where readers and alarm points belong to designated areas. In the simplest terms, a user (cardholder) that has access to an area may automatically have access to all reader-controlled doors that belong to that area. System shall support the programming option that accessing an area using a reader will automatically disarm all points that are assigned to that area and (if selected) other designated areas within the individual user's authority : additionally, a schedule may be applied to this access-based disarming to select the disarm level (STAY or OFF) appropriate to the time such a disarm occurs.

To support applications where persons should have access to an area but not to all doors within that area, the area shall have the option of being subdivided into multiple sublevels per area. Each door in any system area may be assigned a Door Group number (possible values range from 1 to 62, and can be repeated in an area): similar programming in the system Authority Levels shall allow assignment of Door Group numbers per individual area, and the designation of an 'Equal To' or 'Greater Than/Equal To' mode per area for the Authority Level. When a user's Group Mode is set as 'Equal To' in a specified area, the user will be granted access only to doors whose Group number is equal to the user's Group number for that area : a 'Greater Than / Equal To ' setting for the user in a given area shall allow access to doors whose group number is equal to or less than the user's Door Group number for that area.

Additionally, restriction to doors within an area shall be achieved by assigning a door class priority methodology independent of the Door Group profiling described above. This methodology shall grant or deny access based on authority level settings. Three such class settings shall be available, and the class of a given door shall change according to an automatic schedule if so programmed.

The system shall support access flow control. With this feature implemented, users may enter and exit through specified door access ways during the day and shall be redirected to use another specified door access way for entry and exit during the evening and on weekends.

Each controller shall support logical anti-passback. Using a single controller, up to 32 reader-controlled doors equipped with in and out readers shall makeup a logical anti-passback grid.

Each controller shall support two custom card formats including Magstripe format, Wiegand/Proximity 36-bit format and 26-bit format concurrently. Each controller connected to the same host software may support different card-formats. The controllers shall support the changing of the card formats at the customer's site without having to change the controller's firmware.

The system shall support Wiegand, magnetic stripe and proximity card technologies. The controller shall support unique cards having up to 7-digit ID numbers. The controller may be programmed to support card only mode, card plus user ID PIN mode and also card or user ID PIN mode. These modes shall be programmable

The time for which the door relay is energised or de-energised to allow authorised access through a reader controlled doorway shall be user definable. The system shall be capable of detecting both door held open and forced entry conditions, and report these events to the host system as alarms. The duration for activating an alarm relay on a door held open alarm or forced entry condition shall be user definable.

The controller shall support a physically challenged user attribute. By tagging a user as physically challenged, the reader application module shall:

- Keep the door unlocked for a longer than normal programmable time period
- Activate a door opener for a programmable time period
- Extend the door held open alarm timer by a programmable time period.

An operator using the host software or LCD keypad shall be capable of editing the physically challenged time parameters. The minimal programmable extended physically challenged time period shall be 5 minutes.

There shall be reader-to-point group relationships such that when a valid card is used at a door, a user-defined alarm input group may be shunted and/or an output point that is defined by an area shall be activated or deactivated.

The system shall be capable of providing access to an armed area in a manner that is transparent to the valid cardholder. For example, automatic arming level changes from armed to either “stay” or “off” while granting access shall automatically occur upon presentation of a valid token or PIN at the reader.

When leaving the area, a user shall be capable of arming the group of alarm points and activating or deactivating the outputs associated with the area by using an LCD keypad or an arming reader. The area may also be automatically armed via an arming time schedule, or, by a manual command from the host software, or one of the client applications residing on the network.

A request-to-exit (RTE) facility shall be available on each reader application module to allow personnel to exit through a door configured to report forced entry alarms without generating a forced entry alarm.

Manual commands shall be available for doors, floors, input points and output relays, which allow the user to override automatic or timed commands.

All manual commands shall be available for a user-definable automatic command to allow the user to set up automatic schedules for these functions.

2.7 Access Control User Requirements

In addition to the basic function of access control by cardholder ID and time zone, the system shall support the following modes of operation:

2.7.1. Anti-Passback Mode

The system shall allow the operator to define readers for both logical IN/OUT anti-passback or timed anti-passback. Should the cardholder not use an IN reader before attempting to use an OUT reader, or try to re-use the card or PIN within a user-defined period at the same entry reader, access will be denied.

Systems that only support anti-passback for a single door shall not be acceptable.

Systems that only support anti-passback across those readers that are hardwired to the same controller must support a minimum of 32 access control doors within a single anti-passback grouping. For example, a person may enter or exit any one of 32 doors of a building and still be tracked by the anti-passback mode

The system shall be capable of automatically resetting after a programmable period of as little as 10 minutes to a maximum of 12 hours.

A master user authority level that is capable of overriding the anti-passback mode shall be supported by the system.

2.7.2. Dual Custody Mode

The system shall have provision for defining doors that require two valid cards within 10 seconds before access is granted.

A master user authority level that is capable of overriding the dual custody mode shall be supported by the system.

2.7.3. Escorted Dual Custody Mode

The system shall support an enhanced dual custody mode where the first card shall be that of an authorized escort, the second a temporary user or 'visitor'. The feature will be programmable to allow the designation of Escort privileges within an authority level, or to allow permanent or temporary users to act as Escorts for users designated 'visitors'.

A master user authority level that is capable of overriding the escort mode shall be supported by the system.

2.7.4. Doors Unlock, Pending First Valid card Mode

The system shall support the automatic unlocking of all reader-controlled doors within a predefined area that have been programmed for "unlock pending". When the first valid user enters any reader controlled door or disarms the area using an LCD keypad associated with that same area, the readers that are programmed for "unlock pending" will automatically unlock. The doors shall automatically relock when the area is rearmed. The area must be within the scheduled disarm window for this function to become active.

2.7.5. Area Disarm on Access Granted

The system shall support a mode that allows users to use either an access card or a user ID PIN to gain access into the secured area. Where the area incorporates intrusion protection, there shall be a programmable option for the area being accessed by a user to disarm : if desired, this option can be extended to disarm all areas for which the user has disarming privileges at the time access is granted. A programmable option shall allow the disarm to change the area(s) states to STAY or OFF whether inside or outside of an associated schedule.

2.7.6. Card / PIN Modes

The system shall support a manual and timed command function that will change the reader controlled door from card only mode to card plus pin mode, and then back to card only mode. When the reader is in card plus PIN mode the user must present an access card and then enter an ID PIN at the reader to gain valid access and disarm the area.

2.7.7. Invalid Card Lockout

The system shall be programmable to lock out (ignore) further attempts to use an invalid card after a specified number of access attempts have been made with the card. The duration of this lockout is programmable from 2 seconds to 1 week. In addition, the system shall provide a global lockout option that occurs after a specified number of card lockout conditions have occurred. Responses to the global lockout condition shall include offsite notification to the Monitoring Centre and the optional ability to deny user access to all areas on an area-by-area basis.

2.7.8. High Value Assets/Wandering Patient/Baby Abduction Tracking

The system shall track computers and wandering patients and babies based upon specially designed tokens and readers designed specifically for each discipline.

When the system detects the token approaching a reader-controlled door, the door shall automatically lock, sound an alarm at the door, send an alarm message to the host software and LCD keypads and initiate an alarm to a central Monitoring Centre dependant upon the settings of the control panel.

When the token moves outside the door's detection field, the reader-controlled door shall return to its normal operation and the audible alarm will silence.

A computer, wandering patient or baby token that is being accompanied by an authorised token shall be able to pass through the reader-controlled door. Both tokens shall be audited by the system for reporting.

2.8. Intrusion Alarm System Functionality

Each controller shall support the following intrusion alarm functionality:
Communications test initiated from the controller. Programmable settings from once every 30 minutes to once every 7 days.

- Dial mode, (none, digital, digital back-up to High Security)
- Dial format to alarm Monitoring Centre, (SIA, Contact ID)
- Primary phone number to call upon alarm
- Secondary phone number to call upon alarm when the panel cannot make contact with the alarm Monitoring centre using the primary phone number
- Paging when an alarm occurs
- Configurable siren time on alarm, from 1 second to 2 hours
- Number of ID plus PIN digit options supported [PIN only, ID(2 digits) + PIN(4 digits), or ID (3 to 5 digits) + PIN (4 to 5 digits)]
- Communication speed between the controller and the application modules (19K2 and 38K4)
- Support a 2 line by 16 character message to be viewed on the LCD keypad
- Support duress PIN operation

Area functionality programming options to be supported to include the following:

- Arm the area to stay on fail to exit when the area has been armed
- Arm the area when a specified time period during which no activity has been detected on area doors or security sensors has elapsed (time period programmable by area) : optional ability to transmit alarm condition offsite when the ‘no-activity’ time period for an area has elapsed
- Arm the area when the number of users in the area has reached a specified minimum threshold (number of users determined via entry and exit access readers)
- Arm the area when a combination of no activity for the specified time period AND the minimum user threshold is reached
- Arm the area when a combination of no activity for the specified time period OR the minimum user threshold is reached
- Arm and disarm a pre-designated group or groups of areas simultaneously
- Arm each area based on the armed state of other areas linked by system programming. Choices include:
    - Arm / disarm area when ALL other linked areas have been armed / disarmed.
    - Arm / disarm area when ANY of the other linked areas have been armed / disarmed.
    - Arm / disarm all linked areas when ANY one of the linked areas has been armed / disarmed
- Arm multiple areas according to a designated priority value associated with each area connected to an AFx control panel such that areas with relatively higher priority values must be armed before areas with relatively lower priority values : when disarming, the areas with higher priority values cannot be disarmed before areas with relatively lower values . Possible priority values range from 1 -15.
- Deny area access when a maximum number of occupants has been reached
- Send an alarm on fail to exit when the area has been armed
- Siren squawk when area is being armed
- Option of not using PIN to access LCD function keys 1 through 5
- Auto arm the area upon door closing
- Auto disarm area upon use of a valid token or PIN

- Auto disarm an area or areas to OFF according to a specified schedule
- Entry delay time programmable from none to 2 minutes
- Exit delay time programmable from none to 3 minutes
- Garage point delay time from none to 5 minutes
- Allow a maximum of 2 hours for an area to be disarmed outside the scheduled disarm window with optional authority to extend this time
- Allow the option of having an area begin a forced arm every 30 minutes or every 2 hours while inside the scheduled open window
- Allow the option of not allowing users to keep the area open past midnight
- Option of sending fail to close signals to the alarm Monitoring centre
- Option of having an area auto arm on fail to close
- Allow the option of persons with the appropriate authority level to open the area outside the scheduled open window

2.8.1. Invalid PIN Lockout

The system shall be programmable to lock out (ignore) further attempts to use a personal identification number after a specified number of attempts have been made with the PIN. The duration of this lockout shall be programmable from 2 seconds to 1 week. In addition, the system shall provide a global lockout option that occurs after a specified number of PIN lockout conditions have occurred. Responses to the global lockout condition shall include offsite notification to the Monitoring Centre and the optional ability to deny user access to all areas on an area-by-area basis.

Each controller will support up to 12 hardwired input devices: a maximum of 256 such input points shall be supported by each controller via supervised 8 or 16 input expansion modules. Standard input point types shall include:

- Entry exit route
- Entry exit door
- Perimeter
- PIR
- PIR with false alarm protection
- Day warning
- 24 hour burglary
- Fire class A
- Fire with a 15 second delay
- Fire
- Hold-up
- Auxiliary alert
- Supervisory
- Local 24 hour
- Local stay
- Local on

Each point shall be configured for supervision according to one of four fully programmable circuit types (including custom resistance values), Configurations include N/C, N/C with EOL, N/O with EOL, Dual EOL.

Each controller shall be capable of reporting the following system status conditions:

- System trouble
- Low/No battery
- A/C failure
- No phone line detected
- Report delay
- Time lost
- Time changed
- Program edit
- Program error
- Fuse failure
- Application module trouble

- Each controller shall support 20 custom programmable alarm point input types. These input points shall incorporate a programmable pre-process delay from 1 second to 1 week to accommodate devices in applications where an alarm condition from the device must exist continuously for the programmed pre-process period before a response occurs: (i.e. defrost cycle in a freezer where temperature is monitored). Audible outputs and central station

transmission shall be programmable based on armed state of the controller. These custom points shall include:

- Area Keyswitch arming/disarming
- Guard Tour Point
- Garage Delay
- Entry/ Exit Route
- False Alarm Prevention point
- Entry/ Exit Route w/False Alarm Prevention
- Work Late Button
- Activity Monitor (input point used with Activity- Based Arming / Alarm on No Activity area programming)
- Command Point (input programmed to carry out specific system, door or area commands upon activation of the point).

- Each controller shall support up to 128 outputs. An output shall be configured to be activated based upon the following criteria:

- System wide events
- Area events
- Specific door events
- Specific input point events
- Pressing a function key on an LCD keypad

- System type events activate a pre-programmed output based upon any one of the following actions occurring across all areas, points or doors within the controller's system configuration:

- RS485 communications failure
- Ground start
- Partially on
- Fully on
- Fully off
- In alarm
- Siren on
- Digital trouble
- Was in alarm
- Point bypassed
- Fire
- Hold-up
- Auxiliary alert
- Supervisory
- Vault
- Burglary
- Trouble
- Low/No battery
- A/C failure
- No phone line detected
- Report delay
- Time lost
- Time changed
- Program edit
- Program error
- Fuse failure
- Application module trouble
- Duress PIN
- Door locked out
- Forced entry
- Door held open
- Door tamper
- Door open
- Door secure
- Door sensor trouble

- Area type events activate a pre-programmed output based upon any one of the following actions occurring within a defined area:

- Alarm
- Was in alarm
- Siren fire
- Sonalert (entry/exit tones on stay)
- Sonalert (no entry exit tones on stay)

- Garage entry tones
- Bypasses
- Fire Hold-up Auxiliary alert
- Vault
- Burglary
- Supervisory
- Pseudo
- Walk test
- No activity detected
- Activity detected
- Entry/exit
- Entry
- Exit
- Ready
- Open window
- Closing
- Door unlocked
- Door locked out
- Door forced open
- Door held open
- Door secure
- Door tamper
- Door open
- Door sensor trouble
- Maximum area occupancy
- Minimum area occupancy

- Specific door events shall activate a pre-programmed output based upon a reader controlled door's following states:

- Door unlocked
- Door locked out
- Door forced open
- Door held open
- Door secure
- Door tamper
- Door open
- Door sensor trouble

- Specific input point events shall activate a pre-programmed output based upon the input's following states:

- Normal
- Open
- Open (armed)
- Open (disarmed)
- Alarm
- Bypass
- Pre-alarm warning

- Each function key on an LCD keypad can be programmed to activate an output for a time period lasting from 1 second to 1 week.

- Any combination of system, status, area, door, input events and schedules may be used in a combination of up to 15 events joined by Boolean operators (AND, OR, etc). Programming of these Boolean operators shall only be possible via the security management software.

2.9. Guard tour

The system must be capable of running a minimum of 12 Guard tours simultaneously per site. An unlimited number of sites shall be run simultaneously.

A Guard tour station shall include readers that are already installed in the building for the purpose controlling access through doors.

Each Guard tour station shall be programmed with an arrive time variable allowing the person a minimum and a maximum time to get from one Guard tour station to the next Guard tour station. If the person arrives before the allowable time variable or after the allowable time variable, the Guard tour station will record an alarm in the transaction window.

The Guard tour shall allow a different arrival time setting for each Guard tour station.
Each Guard tour that is running shall be shown graphically at the computer where the Guard tour is initiated.

2.10. Elevator Control

Each secured elevator shall be equipped with an elevator reader. A minimum of 30 elevators shall be supported per building. An unlimited number of buildings shall be supported per system.

A minimum of 124 floors shall be supported per elevator reader. The system shall support low rise and high rise and freight elevators within the same building.

It shall be possible to segregate users by banks of elevators.

Elevator control shall be possible by individual floor and by groups of floors. Any of the AFx schedules may be used to desecure cabs or individual floors where required.

The system shall allow users to use a pre-programmed group of floors within a pre-programmed bank of elevators at a predefined time of the day.

2.11. Capacities and features supported by each Controller

- Each controller shall support the following capacities and/or functionality:

- 300 users with names, expandable to 64,000 with names by adding additional non-volatile random access memory
- 4 reader controlled doors (each with in/out capability) expandable to 32 doors (each with in/out capability)
- 16 areas
- 50 holidays
- 50 schedules, each with 6 regular time intervals and 3 holiday schedule settings, expandable to 250 schedules.
- 30 authority levels (expandable to 1000).
- 12 input points (expandable to 256 by adding application modules)
- 2 outputs (expandable to a total of 128 by adding application modules)
- 4 programmable numerical pager outputs (expandable to 12)
- 20 custom point types
- 2 programmable Wiegand/proximity and magstripe token formats supported concurrently
- 24 application modules supported via a polled RS485 communication network, or when used as a suite multiplexer, 60 condominium application modules via a polled RS485 communication network
- 1,024 history events (expandable to 65,536 by adding additional random access memory)
- Uploading / Downloading of site databases via direct wire, modem, LAN
- Logical anti-passback across all reader application modules, minimum of 32 doors supported within a single anti-passback group
- Wandering patient detection
- Panic token detection
- Programmable Guard tours
- Contact ID communication format for communication to alarm Monitoring centres
- SIA communications format for communications to alarm Monitoring centres
- Back-up phone number

2.12. System Communications

Communications between the host software and the controller(s) shall be via a polled RS485 multi-drop communications path or ethernet at a baud rate of not less than 38K4.

Communications between the controller(s) and their application modules shall be via a polled RS485 multi-drop communications path. The controller(s) shall poll 38K4 application modules and 19K4 applications modules at their respective rates automatically.
If a controller or an application module does not respond to a poll, a verification of communications failure shall be performed and the device reported as being in a state of communications failure.

2.13. Controller Event File

The controller shall maintain a time and date stamped event file of the most recent 2,048 events. The event file within the controller shall expand to 65,536 events by adding additional memory. The installation of the memory modules may be performed at any time without removing the board from the customer's premises.

2.14. Inputs/Outputs

Each controller shall support 12 programmable on-board inputs and 2 programmable on-board outputs. The input and output capacity per controller shall be expandable to 256 inputs and 128 outputs by adding input/output application modules.

User programmable software mapping/linking of inputs and outputs based upon a library of mapping options shall be supported across all input/output application modules connected to a single controller via the polled RS485 communications network. This will allow inputs that detect a change of state to activate an output on any other application module that is connected via an RS485 communications link to the same controller.

User programmable software mapping/linking of reader and card type messages and outputs based upon a library of mapping options shall be supported across all input/output application modules connected to a single controller via the polled RS485 communications network. This will allow a reader application module that detects a card or reader message to activate an output on any other application module that is connected via an RS485 communications link to the same controller.

The system shall be capable of reporting 4 states; i.e. secure, not secure, tamper, alarm. The inputs included are door contact circuit, exit circuit, and all auxiliary input circuits.

Inputs located on the same controller or application module shall be individually configurable. Systems that require all inputs located on the same controller or application module to be configured the same shall not be accepted.

Inputs shall be individually configured to support the following conditions:

- Normally closed - no EOL
- Normally closed – custom EOL value (default 2.2 k)
- Normally open - custom EOL value (default 2.2 k)
- Dual EOL- custom EOL value (default 2.2 k)

2.15. Investigate, Status & Control

The system shall support a wide range of functions that allow the user to investigate the status and manually control the functionality of each area, point and/or reader.

From the status screen an appropriately privileged operator shall be able to perform the following manual control functions:

- Lock a door
- Unlock a door

- Lock-out all users at a door
- Bypass or shunt a point
- Arm an area to stay mode (partially armed)
- Arm an area to away mode (fully armed)
- Disarm an area
- Extend an area's open window
- Silence a siren
- Activate an output point

There shall be a status toolbar at the top of the desktop. The toolbar shall be used by the operator to quickly gain access to the detailed status and control window that is associated with the alarm type that has been received by the host software.

The status toolbar will contain siren, fire, and alarm and trouble radial buttons. When the operator is working in a non-dedicated applications environment, the status toolbar can be disconnected from the security application and dragged into the non-security application. This will allow the status toolbar to be accessible by the operator while working within other windows applications. By simply clicking on the active toolbar radial button, the operator will be taken directly to the appropriate detailed status/control screen within the security system application, based upon the appropriate authority levels.

2.16. Controller Database Updates

Each time an edit has been made by the operator to the host software's database, the change will immediately be transmitted to the controller(s) when the save button is pressed.

When a single on-line controller is used, changes made to the controller's database using the LCD keypad will result in the database changes being uploaded to the host software, where the database tables will be automatically updated.

Each controller database shall be automatically synchronised by the host software each time communications is re-established.

2.17. Controller and Application Module Diagnostics

The controllers shall incorporate the following diagnostic messages:

- System trouble
- Low/No battery
- A/C failure / brownout
- No phone line detected
- Report delay
- Time lost
- Time changed
- Program edit
- Program error
- Fuse failure
- Application module trouble

High-level configuration changes by a user, regardless of their authority level, that could potentially defeat the system's ability to communicate intended alarm conditions shall result in the system automatically sending a system tamper alarm to the Monitoring centre. The alarm shall be triggered whether the changes are made via the LCD keypad application module or the host software.

2.18. Application Modules

2.18.1. Reader application module

Each controller shall support a maximum of 16 reader application modules. Each reader application module shall support 2 access control doors, each supporting an entry and an exit reader.

Any system reader can be designated as a ‘Card Enable’ station that will validate the card upon presentation to the reader : these cards must be tagged as ‘pending enrolment’ in the system and can be used to enable temporary and permanent users. The card may be programmed to remain enabled permanently or for a specific duration.

Any system reader can be designated as a ‘Card Disable’ station that will invalidate the card upon presentation to the reader : these cards must be tagged as ‘pending enrolment’ in the system and can be used to disable temporary and permanent users.

Readers designated as ‘card enable’ or ‘card disable’ stations shall also have a programmable option to unlock the door associated with the reader as well as performing the card action.

Each reader application module shall be connected to the controller over a polled RS485 multi-drop communications network at a selectable data rate of either 19K2 or 38K4.

Door attributes for each reader door shall include:

- Unlock door mode supporting the following criteria:
- None
- Auto schedule only
- Auto schedule area off
- Auto schedule pending first valid user
- When ever the area is off

- Unlock door times supporting the following criteria:
- 1 to 90 seconds
- 2 to 90 minutes
- 2 to 20 hours
- 1 day
- 1 week

- Door processing supporting the following criteria:
- None
- Door held open
- Door forced open
- Door held open and forced open

- Door held open times supporting the following criteria
- 1 to 90 seconds
  - 2 to 90 minutes
  - 2 to 20 hours
  - 1 day
  - 1 week

Auxiliary relay attributes for each reader door shall include:

- Relay output mode
- None
- Door held open / forced entry
- Door opener

- Relay output activation time

- 1 to 90 seconds
- 2 to 90 minutes
- 2 to 20 hours
- 1 day
- 1 week

- Input mode
- None
- Maglock magnetic field bond sensor trouble input
- Physically challenged request to exit input

Physically challenged user attributes shall be in addition to standard user attributes for each reader door and shall include:

- Door held open time
- 1 to 90 seconds
- 2 to 90 minutes
- 2 to 20 hours
- 1 day
- 1 week

- Door unlock time
- 1 to 90 seconds
- 2 to 90 minutes
- 2 to 20 hours
- 1 day
- 1 week

Circuit attributes for each reader door shall include:

- Reader tampers
- Normally closed
- Normally closed with end of line resistor supervision
- Normally open with end of line resistor supervision
- Form C with Dual end of line resistor supervision

- Request to exit devices
- Normally closed
- Normally closed with end of line resistor supervision
- Normally open with end of line resistor supervision
- Form C with Dual end of line resistor supervision

- Door status sensors
- Normally closed
- Normally closed with end of line resistor supervision
- Normally open with end of line resistor supervision
- Form C with Dual end of line resistor supervision

- Auxiliary inputs
- Normally closed
- Normally closed with end of line resistor supervision
- Normally open with end of line resistor supervision
- Form C with Dual end of line resistor supervision

Each reader application module shall support a magnetic lock field sensor input. This input shall be programmed to send a trouble signal to the alarm-Monitoring centre.

Each reader application module shall support an output that can be programmed to activate an automatic door opener, when a physically challenged user presents their access token to the reader.

2.18.2. Elevator Controller application modules

The elevator controller application module shall comprise of a module that resides on the RS485 communications bus to a host controller. The elevator application module shall be software linked to a reader application module.

The reader application module shall incorporate relay boards with 8 on-board Form C relays for connection to the building's elevator controller. Control for more than eight floors shall be achieved by adding additional relay boards to support a maximum of 124 floors.

In case of an emergency, a single programmable input change of state occurring on an input application module shall automatically change elevator control from secure to free access for those elevators the input is linked to in software.

In case of communication failure between the elevator controller application module and the host controller, the elevator will revert to free access and an alarm will be sent to the host software. Immediately upon restoral of communications, the elevator application module will secure all floors based upon the programmed parameters of the system.

2.18.3. Input / output expansion application modules

Inputs shall be the system's way of monitoring devices that detect smoke, motion, door/window openings etc. in each area. The input screens shall allow fine-tuning basic monitoring characteristics, identifying the area the sensor is in, and whether or not it is on the perimeter of that area. Expansion modules shall be used when the number of detection devices required on the system site exceeds the support provided by the control panel and keypad inputs/ outputs.

The input point application modules shall connect to the controller via an RS485 polled communications network at a data rate of 19K2 or 38K4.

Two types of input/output expansion shall be supported. The first shall utilize input application modules on the AFx supervised SNAPP communications bus and shall be configurable as follows:

- 8 inputs and 2 open collector outputs
- 16 inputs and 2 open collector outputs

The second type of input/output expansion modules (Vbus) shall connect to a dedicated terminal on the Chubb AFx circuit board and application modules labelled Vbus, and provide local input/output expansion support to a maximum of 16 inputs and 32 outputs per local expansion. The Vbus output modules shall provide either open collector or dry contact relay outputs depening on Vbus type.

Input points shall be capable of sensing secure, alarm, tamper and not secure conditions.

Each input circuit shall support one of four fully programmable circuit types (including custom resistance values).The following default supervision options are available:

- Normally closed - Non ULC
- Normally closed - EOL supervision (2.2 k
- Normally open - EOL supervision
- Dual EOL supervision

2.18.4. Wireless RF application modules

Both narrow-band and spread spectrum wireless application modules shall be available for the system : each technology shall support up to 32 of its respective learn-mode devices.

The wireless application modules shall connect to the controller via an RS485 polled communications network at a data rate of 19K2. All wireless transmission devices shall have the option of transmitting supervisory check-in and low battery signals : the AFx controller shall transmit event and device specific information to the Monitoring Centre in the event of a transmitter's failure to check in or its generation of a low battery signal.

2.18.5. LCD keypad application modules

Users shall enter system commands via the LCD keypad. The LCD keypad shall be used for configuring, programming, viewing event history and system status conditions, arming, disarming and manually controlling areas and reader-controlled doors, bypassing and isolating input points, according to the user's authority level.

Common features of the system keypads shall include a 32-character display screen, 3 non-dedicated software controlled keys to direct the user through the menus, 3 emergency keys, a Sonalert, an armed status LED, a system trouble LED, a power indicator LED, an escape key and 10 programmable function keys.

Four styles of keypad shall be available for the system:

- Large style LCD readout with single input and output
- LCD PLUS with four inputs and a single output
- LCD PLUS with integral GProx II reader circuit, four inputs and a single output
- LCD PLUS with Weigand data input, two inputs and a single output

The LCD keypad versions with integral GProx II reader circuit and Wiegand data input shall provide command function activation via user access tokens : separate commands may be programmed for a single pass of the badge and a sustained hold of the token in the reader circuit's range (hold time programmable from 3 to 10 seconds). Additionally, the command activations may differ inside and outside of an assigned schedule (according to system configuration). Available command functions shall include Auto-logon, arm to ON or STAY, disarm to STAY or OFF, ON/OFF toggle, ON/STAY toggle, OFF/STAY toggle, Extend exit delay and Auto Work Late. These readers shall also be capable of providing access to one of the system controlled doors via a programmed association with the relevant door controller.

The LCD keypad application modules shall connect to the controller via an RS485 polled communications network at a data rate of 19K2 or 38K4.

2.18.7. Internet Protocol Modules

Status information as well as control and configuration of the controllers via a static Internet address shall be achieved with the addition of the IP Host Module to the main controller in an AFx system. The module shall connect to an existent network via an onboard female RJ45 network connector.

2.18.8. Intelligent Power Supply Module

The intelligent power supply module shall be a fully supervised source of up to 1 amp of auxiliary power for detection and sounding devices, capable of charging backup batteries of up to 17 aH capacity. It shall be capable of operating in two modes, selectable via onboard dipswitch : in the Master mode, the supply shall be considered a SNAPP application module and support the connection of Chubb AFx VBus input and output modules as described in Section 2.18.3. In Slave mode, the supply shall connect to the Vbus terminal of a Chubb AFx application module and shall not count toward the limit of 24 application modules supported by the Chubb AFx panel.

2.19. Arming reader

The arming reader shall be available in two styles:

- A wall mount style the approximate size of a single gang light switch
- A slim line mullion mount style.

The arming reader shall be a proximity reader and incorporate an integral keypad for manual commands at the door. The reader shall incorporate a door status LED, an armed status LED and a work late LED.

- Door status LED
- Solid red if the door is locked
- Solid green if the door is unlocked
- Flashing red at disarming if there was an alarm in the area
- Armed status LED
- Solid green if the area is off
- Solid red if the area is in stay mode
- Flashing red if the area is on
- Work late LED
- Solid yellow light within 15 minutes to the scheduled closing time Off if the area is not scheduled or there is more than 15 minutes to the scheduled closing time
- Arming reader tone/siren integrated into the reader
- Entry/Exit tones upon a valid user token or PIN
- Fire siren
- Burglary siren; continuous tone
- Bad command; double short beeps
- Command accepted; single long beep
- Unauthorized to perform command at the reader; double long beep

The arming reader shall be used to access areas. The use of an authorized token or PIN shall cause the access door to unlock and the area shall become disarmed.

When leaving the area, a person shall arm the area using the same arming reader or another arming reader connected to the same controller, or, and LCD keypad.

The arming reader shall be used in the following manner:

- Unlock door and disarm the area to off or stay using card only, card + PIN, or PIN only
- Unlock the door and disarm all areas associated with the controller
- Lock and arm all doors and areas associated with the same controller
- Extend the open window for the associated area from 2 to 8 hours.
- Silence a siren in all areas associated with the same controller

2.20. Photo ID and Badging (option)

The system shall support an optional photo ID system capable of capturing the colour image of a cardholder and saving it as part of the system database, and of producing a high quality badge using that same image from the database. This system shall be a Windows-based system with the same intuitive operation required of the base system software.

This optional system shall be capable of full integration into the main system database, systems that are interfaced and require any form of updating to synchronising two databases shall not be allowed.

The badging system shall be capable of running on the same computer as the main system, or on a separate computer if required. Appropriate network support shall be an optional part of the system.

2.20.1. Card Design

The photo ID system software shall support an integrated badge design function, allowing the user to drag & drop colour bitmaps and logos, set colour background, and select the data fields to be printed on the badge.

2.20.2 Image Capture

A high quality colour image shall be produced at the capture stage. The software shall have the tools to display the image on the screen, both the live and captured image such that the image can be reviewed and re-taken if required, before it is saved to disk, and a badge is produced.

The image saved on disk shall be in a compressed form of approximately 10 Kilobytes.

2.20.3. Badge Printing

ID Badge printing shall be an integral part of the badging system, and shall be of the 3- or 4-Colour Dye Sublimation type with direct printing on graphic quality plastic cards. The printer shall also support photo ready magnetic stripe and Wiegand and proximity cards.

2.21. Photo Verification

Photo verification shall be supported within the operation of Visual Director : once digitised photos are captured and linked to the users (cardholders) database files, photo verification shall be supported in the following manner;

When a card transaction occurs at specified reader controlled doors the database photo associated with the card used shall be displayable on any PC workstations running the software. Both access granted and denied events may be selected for the display. A green border shall appear around the photo when the user has been granted access : the border shall be red when the user has been denied access. The photos may be displayed singly or in groups of four or nine, and are time and date stamped. The display may be programmed to display for a finite time period, or to stay visible at all times. The photo verification window will appear even when the main Director application is minimized.

2.22. Visual Director

The software shall support dynamic mapping and links to closed circuit video.

The software link between the security software and the video capture stations shall be through a standard network connection to an NVe DVR or designated TruVision recorders..

Video capture, pan, tilt and zoom control of cameras on the local site and remote sites using the internet shall be achieved with the use of an NVe DVR or designated TruVision recorders. Optional surveillance software applications modules shall be available to view live video, capture video, control cameras where pan/tilt hardware has been implemented and view captured video. The surveillance software may reside on the same site as one of the capture stations or communicate with the capture stations using the Internet.

A single surveillance software package shall be able to connect, view and control cameras located on multiple sites at the same time. Also, multiple surveillance software applications operating across a network and through the Internet shall be able to connect to and view the same cameras at the same time.

Surveillance software shall be able to access cameras on their computer screens in the following manners;

- Programmable thumb nails buttons across the top of the screen
- Links to other maps/camera views stored in the Director application
- As combined views composed of dynamic maps and live cameras in one of up to fifteen matrix-style configurations.

3. SOFTWARE OPERATING SPECIFICATIONS

3.1. Introduction

The primary functions of the system software shall be the central database management of local and/or remote sites, monitoring of transactions and alarms, and generate management reports. The design shall conform to the general direction of the PC Software market and project an image of a supplier who is in tune with the state-of-the-art requirements of PC users in today's market.

The software operating on the host computer shall not be required for the hardware controllers and application modules to function.

3.2. System Operation

The system shall operate in any typical Microsoft Windows environment, including use on a PC that is part of a local area network (LAN). Multi-user operation over a network shall be supported, and the system shall allow use of networked printer resources. The software shall be based upon a 32 or 64-bit multi-user, server/client architecture and run on the operating systems listed in Section 2.1

3.2.1. General operation

The system shall display a list of operator, system configuration, administration, reports, control & status and communications options that the user may choose from. The logged on operator's authority level shall determine the system functions that the operator may have access to. The list shall be accessible by the operator using a "Windows explorer tree" pick list or a user defined Tool bar.

3.2.2. Operators

There shall be a login system for operators that allows the system software to keep track of who made changes or performed operations on the system and when. Operators may log into one of up to six Director databases : they shall be assigned permission levels that determine their ability to view and/or edit aspects of the application and the system's users, authority levels and schedules. The software shall support network connection of up to fifty client workstations via TCP/IP protocol. The workstations shall be configurable to either provide operators with the permissions associated with their log-in or to obey a set of permissions specifically assigned to the workstation.

Each database edit or manual control function made by an operator will immediately be logged in the event queue.

Operators at each of the client workstations shall be able to filter events that are viewed within the event queue based upon the following criteria:

- By site
- By specific controller
- By event type
- By area
- By door
- By user
- By input alarm
- By application module

A scheduled event filter can be assigned to each operator, ensuring only system events that are important or appropriate to the operator's privilege level are displayed. The scheduled event filter may be programmed to show certain events during the assigned schedule (in window) and different ones at all other times (outside of window). If no scheduled event filter is assigned to an operator, the operator's filter settings are saved each time the event filter is edited. The ability to change or assign a scheduled event filter is controlled via the Operator Permissions screen.

3.2.3. Access to Functions

The user interface shall be designed in a manner such that access to functions is point-and-shoot. A complex, hierarchical menu system shall be avoided. A Windows explorer tree shall be available, which allows the user direct access to the individual programming and control functions without having to step through menus.

3.2.4. System Requirements

The software shall be designed to run on a minimum 2.5GHz or faster computer with a minimum of 4GB of memeory. The video monitor shall support 1024 x 768 or higher.

In all situations where disk space is being allocated to system files, there shall be resource management such that the user is warned of insufficient space. A provision shall be available in the application to archive and purge event and communications logs manually, with an additional option to automatically purge events when the database size limit is approached. There shall also be an option to import archived event and communications logs for review.

3.3. Printer Support

The Windows operating system will provide printer driver support, and the system software shall work with the Windows Print Manager facilities to generate reports and direct them to the appropriate printer.

3.4 Language Support

The system software shall have multi-lingual capabilities and shall allow the user to select

English, French, Dutch, Spanish, Simplified Chinese, Traditional Chinese, Russian, Slovak, Hungarian, German, Italian, and Portuguese

through the desktop for all system prompts and field labels.

3.5 Database

The host software shall store the complete system database, supporting cardholders and system configuration for all controllers. All data records will be contained in the host database and the system will be capable of complete programming of the remote controllers from a central location or across a LAN.

The database structure shall be created and maintained by the Microsoft Database Engine.

3.5.1. Structure

The structure of the database shall be relational to allow descriptions to be kept in one file and referenced through pointers by other files. This minimises the editing required should the user wish to change a door description. For example, card records shall have reference indexes to the files containing site name and authority group information. The database structure shall allow for user-definable fields to be attached to a record.

The system software database shall be a global database for the entire system and each controller database shall be a sub-set of that database.

3.5.2. Database Query

The system software shall support a database query function whereby a separate utility within the application (requiring a separate log-in value) will allow the manual extraction of specific user and event tables from the database for the purpose of creating custom reports.

3.5.3. Custom User Fields

The user record shall support an additional 20 custom defined fields, including a signature field. These fields shall be alphanumeric fields and used for sorting and reporting purposes. Supported field types shall be single line edit, multiple line edit and dropdown list (a list populated with multiple items allowing selection of an individual item on each user record i.e. department). Access to the custom user fields may be restricted to an operator (in groups of five fields i.e. 1-5, 6-10) via Operator Permissions to prevent viewing of user information inappropriate to the operator's privilege level.

3.5.4. Shared User Groups

The system software shall support the designation of groups of users, authority levels and holidays as 'shared' across specified accounts in the AFx database. When changes are made to shared user records, the software shall synchronize the changes made to such users on the next occasion that an interactive connection is established between the PC and the AFx account(s) selected for inclusion in the specified shared grouping. The system shall support the establishment of multiple shared groups to facilitate user management across any number of accounts. Custom fields for shared users shall be limited to the 'single line edit' type.

3.6. Communications

Communications with controllers that are located within the same facility as the host software shall use a direct wire polling connection using an RS232 or RS485 communications path. The system shall also support Ethernet connectivity to the software. The communications rate shall be selectable at 19K2 or 38K4.

Communications with remote controllers located on other sites shall be as flexible as possible. System shall support connection of a modem, for offsite communications to the Monitoring Centre and communications to Director software : the Worldwide modem card shall support 2400 baud Director communications for AFx systems running at Feature Set 7 or lower. Remote communications shall be via dial-up modem, using a standard AT command set using a communication rate of 38K4.

Alternately, the remote controller shall be connected to a PC that resides on the WAN. The PC shall be running a system client application. That application shall be used for Administration, control and alarm monitoring. The client application shall be set to monitor all transactions across the WAN, or only the transactions on that site.

3.6.1. Controller Communications Protocol

The communications protocol between the system software and the controllers shall provide for error detection and correction to ensure the integrity of all parts of the system. Communications shall be encrypted and authenticated.

3.7. Report Generator

The report generation package of the system software shall be a fully integrated part of the system and contain the reports defined in section 5, as a minimum.

Before running any report, the user shall be able to select the Site(s), time/date limits and the target device; i.e. Screen, Printer, or Disk File. Disk file output shall be in the form of delimited ASCII.

The system shall support a number of standard reports, which will be described later in this document. These reports will be used to extract information from the event file.

3.8. Card Validation/Invalidation

The system software shall support routine validation and invalidation of cards. Both temporary cards and permanent cards shall be subject to automatic validation dates, which are to be shipped down to the controllers for processing. The controllers will be responsible for the actual validation process. Temporary card records shall contain an invalidation date that shall also be processed automatically at the site controller.

3.8.1. Permanent Cards

All cards allocated to permanent shall be valid until such times as an invalidation date is entered into the database. The invalidation time is to be taken as 00:00 on the date of invalidation. If the invalidation date is earlier than the current date, the system shall immediately invalidate the card. A permanent card shall be validated at 00:00 hours on the validation date.

3.8.2. Temporary Cards

The system software shall allow the user to assign a card to an individual on a temporary basis and automatically remove the privileges assigned to that card after a certain date and time has expired.

4. SOFTWARE CONVENTIONS

4.1. Desktop

All user interactions with the system shall be handled through a desktop using a Windows explorer methodology to select the areas of the security program the operator requires access. Areas of the program that can be directly accessed through the desktop, based upon appropriate operator authority levels include :

- Operator authorities
- System configuration files
- Administration
- Reports
- Control and status
- Communications

When editing the database or performing the status or control functions, it shall be possible to view the information in a form or grid layout. In both formats it shall be possible for the user to perform edit and control functions. While in the grid (spreadsheet) view it shall be possible for the operator to sort the information presented on the screen in a chronological order based upon the header chosen. For example, user information shall be sortable by first name, last name, authority levels, card numbers, challenged users, and language and by any one of the additional 20 custom field entries.

Where the information that is presented to the user is presented through any window that is scrollable, the system shall automatically display scroll bars on the bottom and the right side, for horizontal and vertical scrolling respectively. The following sub-sections will define the use of each aspect of the desktop.

4.2. Dynamic Windows

Information presented to the user shall be done through dynamic windows. A dynamic window is defined as a window that can be dynamically updated if the data changes. For instance, a change at the LCD keypad will dynamically update data fields within the host software application module.

4.3. Graphical Objects (Icons)

Use shall be made of graphical objects that invoke functionality in the program directly, as an alternative to stepping through a menu system. These icons shall be arranged in toolbars located in convenient parts of the screen. For example, a status toolbar shall reside at the top of the desktop.

There shall be a status toolbar at the top of the desktop. The toolbar shall be used by the operator to quickly gain access to the detailed status and control window that is associated with the alarm type that has been received by the host software.

The status toolbar will contain siren, fire, and alarm and trouble buttons. When the operator is working in a non-dedicated applications environment, the status toolbar can be disconnected from the security application and dragged into the non-security application. This will allow the status toolbar to be accessible by the operator while working within other windows applications. By clicking on the active toolbar button, the operator will be taken directly to the appropriate detailed status/control screen within the security system application, based upon the appropriate authority levels.

Status toolbar buttons shall be animated where applicable and change colours where applicable and generate sounds in order to bring to the operators attention an alarm that requires action.

4.4. Buttons

A button is defined as a rectangular object used to display a control option in a dialogue box. The user may select a control option by clicking on the appropriate button.

4.5. Status Line

All screens are to show the standard Windows status line at the bottom, which will be used throughout the program to provide the user with messages and information.

4.6. On-Line Manual

Context sensitive help shall be available for all levels of system operation, and for all screens. This documentation shall be complete enough to be considered an on-line user's manual and structured in such a way that the user can quickly find the topic of choice through a standard Windows help system.

The help files shall be organized in a fashion similar to Windows help files to provide the user with that similar look and feel which shall be consistent throughout the system. As much as possible, the text shall emulate the documentation, reducing the need for the operator to refer to manuals to obtain information. Content lists and subject headings will therefore be required

When a user is in any one of the programming or control screens and then clicks on the help button, a help window will be presented to the operator that resembles the actual active application screen. Within the help screen there shall be a picture of the active screen. Below the picture of the active screen, each header that requires data entry shall be listed with examples of the required information that needs to be entered by the operator. Along with this information, additional reference topics shall be listed in blue type set with a small control button at the end of the paragraph. When the control button is pressed, the operator will be connected to the other relative information.

4.7. Colours and Screen preferences

All set-ups of colours, preferences, and items such as printer support will be the responsibility of the Windows operating system. The application software shall not attempt to override Windows control.

5. SYSTEM SOFTWARE

5.1. Introduction

This section of the specification covers the functionality required of the system software. All functions shall be governed by the conventions laid out in section 4 and shall be consistent in usage.

5.2. Communications Program

The Communications program shall contain the communications routines, and will be responsible for the continuous monitoring of ports for incoming messages from remote sites and the continuous polling of controllers on the local site. The mode of this program will be such that a system status toolbar monitoring for siren activation, fire, intrusion alarm and trouble will become active, as well as, sounding an audible alarm tone. The user may then click on the active icons within the toolbar and switch directly to the appropriate control/status window.

The communications monitor will also be responsible for receiving incoming event files being sent from the local and remote controllers via direct wire, dial-up, LAN and WAN communications.

5.2.1. Receiving an Alarm

An incoming alarm shall contain all pertinent information on its time, date and location of origin. The alarm may be custom colour coded to reflect the alarm type, and any one of twenty custom sound files may be also be associated with the event in order to require the entry of a resolution message by the operator.

5.2.2. Event Screen

The event screen shall be part of the communications management program and represented in a dedicated window. Incoming alarms and transactions shall go into a single queue. Alarms will be tagged with a (default) red banner. Alarms and any other event shall be programmable to display in a unique custom colour. Custom and priority numerical values may also be assigned to events to assist in onscreen filtering of incoming activity : four equations are available to the operator for use with the custom and priority filters (less than, greater than, equal to, between). The application's default filters shall allow immediate filtering of the display by specific areas, door, points, application modules, elevators or suites. Operator permission levels shall allow the creation of schedules for specific association with event screen filters such that the display will automatically apply different filters inside and outside of the schedule. There shall also be an option to deny individual operators the permission to change the event display defaults associated with their login.

An optional Alarm Event screen can be enabled for each individual operator : the default position for this screen shall be immediately above the standard event screen. The Alarm Event screen shall always display (and annunciate audibly, if so programmed) any unresolved alarm event activity regardless of filtering applied to the standard event screen.

The software shall provide a serial output for selected events : when so programmed, occurrence of these events shall result in the output of a text string from the specified serial port in space or tab delimited format for use by pagers and similar devices.

5.2.2.1. Processing Alarms

To process an alarm, the operator shall click the mouse on the coloured banner associated with the alarm message that is located within the transaction window. This action shall automatically open up an Instruction/resolution dialog box, where the operator shall type his or her findings. Instruction messages can be created for any system event, including activation of individual input points. A list of predefined acknowledgment messages may also be created and stored to expedite the event resolution process. In addition, one of up to 20 unique sound files (in .wav format) can be associated with any system event (the default sound for any alarm conditions is the Windows 'exclamation' sound) : when so programmed, an event shall trigger this sound file to annunciate and repeat continuously in a 2-second looping format until the operator enters a resolution message for the event : the event may also be tagged for further analysis. Once this action has been taken a check mark will be recorded in the banner. At any time an operator can click the mouse on the alarm banner containing the check mark and add an additional message. Each time an operator adds a message in the alarm dialog box, their name is automatically recorded with a time and date stamp accompanying the message.

5.3. Active Graphic Maps

The system shall support the importing of map drawings in a variety of drawing formats including jpegs, bitmaps and word metafile format. The system shall allow the operator to choose maps from its library of floor drawings and keep them displayed.

The system shall allow the insertion of icons linking to other maps or live camera feeds via static IP address. As access-controlled doors open and close and points change state the device icons on the active graphic maps shall follow the real-time status of each. When the host software receives alarms, the icons representing areas where the alarms are initiated shall begin an animated display. The system shall allow an appropriately privileged operator to arm areas, bypass points, activate outputs and lock doors and unlock doors using the graphic map.

Each map can be viewed in one of up to fifteen combination views composed of maps and live camera feeds via static IP address. As the doors open and close and points change state the device icons on the active graphic maps shall follow the real-time status. The Arm/disarm state of areas shall also be displayed

The system shall also allow an appropriately privileged operator to arm areas, bypass points, activate outputs and lock and unlock doors utilizing the icons representing them on the maps. Status of the icon shall automatically display when the cursor rests on the icon for a brief period.

5.4 Manual Control

The user shall be capable of performing manual control functions from the host software, the client software modules and from the LCD keypads and arming readers.

Manual commands available to the operator using the software and LCD keypads shall include:

- Arming and disarming an area : choices are off, stay or on
- Arming / disarming a pre-designated group or groups of areas : choices are off, stay or on
- Arming and disarming individual suite security modules : choices are off, stay or on
- Adjust an area's schedule : choices are suspend, resume, work late
- Control a door in a specific area, choices are lock, unlock, lockout, re-instate
- Bypass an input point in a specific area
- Isolate an input point in a specific area
- Silence a siren
- Activating an output point

5.4.1 User In/Out status

There shall be a section in the application's control and status screens that displays the current IN/OUT status of system area users : this feature shall include a provision to filter the display based on a text string as well as the ability to sort the display alphabetically in ascending or descending order.

5.4.2 Upload/Download of Database between the Software and Controllers with local and remote capabilities.

To establish a connection, the site lists will be displayed in a dialogue box, allowing the user to select the target site from the site list. Once connected to the site, a pulsing icon shall be displayed to the operator in the bottom right corner of the screen.

When connecting with a controller(s) the operator shall have a choice of "normal connection", "get from panel" and "send to panel". If the operator chooses normal connection, the software will connect with the panel and automatically synchronise the host software's

database with the controller's database. If the user also chooses "stay connected", the host software shall continue to stay on-line with the controller(s) until the operator manually disconnects the communications. If the operator chooses "get from panel", the controller will upload its database files to the host software. If the operator chooses "send to panel", the host software will download its database files to the controller(s).

The "get from panel" command shall be used where the computer has failed and there is no current database backup. The user shall simply reload the application software onto the new computer, connect to the controller(s), send the command "get from panel" and the entire system database shall be written to the host software application.

5.5. Status Command

This command shall allow the user to view the state and status of areas, doors and input points. The status command also shall allow the operator to view all system modules that are in trouble condition. From the status screens, an operator may perform manual commands.

The status command screen shall allow the operator to view:

- The area state (off, on, stay)
- Name of the schedule that controls the arming and disarming of the area
- Work late schedule (active, inactive)
- Area schedule (suspend, resume)
- The time the area is set to arm
- The reader controlled doors that are assigned to the area
- The alarm points that are assigned to the area
- The status of the door (open or closed or tamper)
- The alarm status of the door (ok, not ok, off-line)
- The state of the door (locked, unlocked, locked out)
- The status of the input point (ok, not ok, bypassed)
- A power status screen displaying the status of the AC supply, the charging voltage and status of the backup battery, and the total current consumption of the panel and connected devices.
- A comprehensive diagnostic report detailing the AC and backup battery status, current consumption, status and firmware of the system's application modules and the resistance present on system hardwired inputs. The act of running this report shall automatically copy a time and date stamped copy to the Report generator section of Director software.

5.6. Report generation

A complete and fully featured report generator shall be part of the security application, providing the administrator with the utilities to create reports from the database and controller's event files saved on disk.

Each report destined for the printer must contain a header that indicates the site, Page number, number of pages contained in the report, Date/Time, Report Name, and Operators Name.

5.6.1. Report Destination

Each report requested by the user shall have a selectable destination of SCREEN, PRINTER, or FILE.

If the user selects "FILE", a standard Windows "Save As" dialog box will be presented to the operator, where a file name and directory destination for the report can be chosen.

If SCREEN is selected, a full size window will appear on the screen, and the system will display transactions a screen at a time, pausing for mouse or keyboard input before continuing with the next page.

If PRINTER is selected, a standard Windows print dialog box shall open, where the operator may choose to print all pages, current page or select pages of the report. The operator may also choose to make changes to the printer set-up window before printing the report.

5.6.2. Selecting a Report

The dialogue box for selecting a report shall be common for all reports as it will allow the user to select the report type, destination and so on. A message area shall also be provided to inform the user of status. The user may cancel a report by closing the report generator with the CLOSE icon, or clicking on the CANCEL button.

5.6.3. Database Reports

This section of the report generator will allow the user to obtain reports on the controller's database. After a report has been selected, the user will be prompted for the destination device, as described in section 5.4.1.

A dialogue box shall be displayed allowing the user to choose their report from one of the following report categories. This dialogue is to also include the selection of the destination.

Each report shall include a header that shall include the time and date the report was run, the system ID of the person that ran the report, the company name and the page number and number of pages that are included within the report.

5.6.3.1. General Report

This report shall provide the user with the following information:

- Site address
- Mailing address
- Contact name
- Phone number
- Security product version number
- Comments

5.6.3.2. User authority Levels Report

This report shall provide the user with the following information:

- Authority number and name
- Detailed listing of user profiles
- Each user profile shall include the tagging of security areas, permissions and schedules that are valid for the user

5.6.3.3. User Report

This report shall provide following information:

- User ID number
- Authority level
- First last name
- Last name
- System language preferred by the user (English or French)
- Card ID number
- Validation date and time
- Invalidation date and time
- List the information within custom user fields (20 in total)
- Suite security user parameter (where implemented)
- Master override option tag

5.6.3.4 User Access Report

This report shall provide the following information:

- Users having access to an area
- Users having access to a specific door
- Users having access to a specific floor
- Cards that have expired or will expire (time range specifiable)
- Cards that have not been active (time range specifiable)
- The time and date range for the criteria above

5.6.3.5 Schedules Report

This report shall provide the user with the following information:

- Schedule number
- Schedule name
- Graphical representation of time schedule from Sunday to Saturday including all active intervals
- Holiday settings

5.6.3.6 Holidays / Daylight Saving Report

This report shall provide the user with the following information:

- Holiday ID number
- Holiday name
- The month the holiday is active
- Day of the month the holiday is active
- Holiday type settings

5.6.3.6 System General Report

This report shall provide the user with the following information:

- Siren activation time
- Number of ID + PIN digits used by a user to access an LCD keypad or an arming reader
- RS484 communication baud rate
- LCD keypad system message (13 characters)

5.6.3.7. Operator Audit Report

This report shall provide the user with the following information:

- Detailed actions performed by operators of Director software
- Reports shall be selectable by operator, account and type of activity

5.6.3.8. System Access Format Report

This report shall provide the user with the following information:

- Fall back mode
- Primary token format
- Secondary token format

5.6.3.9. System Communications Report

This report shall provide the user with the following information:

- Digital account ID
- Communications mode
- Communications format
- Phone number of alarm-monitoring centre
- Back-up phone number of alarm-monitoring centre
- Communications test format
- Pager phone number
- Pager communications format

5.6.3.10. Area Settings Report

This report shall provide the user with the following information:

- Name of the area
- Entry, exit and garage delay times for areas
- Schedule allowing users to disarm the area to the system to automatically begin arming the area
- In window and out of window time parameters for the system to automatically arm the area
- Auto command schedule settings for an area to automatically disarm and rearm
- Auto schedule settings for a door to automatically unlock and relock

5.6.3.11. Application Module Settings Report

This report shall provide the user with the following information:

- Module number
- Module name
- Module serial number
- Input range
- Output range
- Area the module is referenced to
- Module settings for tamper, tones, and delays where applicable

5.6.3.12. Input Points Report

This report shall provide the user with the following information:

- Input point number
- Input point name
- Module type the input is wired to
- Input point type
- Circuit type
- Area the input is reference to

5.6.3.13. Equipment diagnostics settings Report

This report shall provide the user with the following information:

- Equipment reference number
- Equipment reference name
- Processing delay time before initiating the alarm
- Criteria for transmitting the alarm (area is off, stay or on)
- Criteria for initiating the sonalert (area is off, stay or on)
- Criteria for initiating the siren (area is off, stay or on)

5.6.3.14. Output settings Report

This report shall provide the user with the following information:

- Output number
- Output name
- Application module the output is connected to
- Function type causing the output to activate (system, area, door, point, and function key
- Specific function causing the output to activate (pod trouble, area armed, door unlocked, function key #1 pressed, etc)
- Time delays where applicable

5.6.3.15. Custom Point Type Report

This report shall provide the user with the following information:

- Custom point number
- Custom point name
- State the active window when the point will initiate an alarm
- State the delay time before the alarm will be initiated during the active window
- State the class of alarm the custom point represents
- Criteria for transmitting the alarm (area is off, stay or on)
- Criteria for initiating the sonalert (area is off, stay or on)
- Criteria for initiating the siren (area is off, stay or on)

5.6.3.16. Reader controlled door Report

This report shall provide the user with the following information:

- Door number
- Door name
- Application module the door is connected to
- Port number on the application module
- Reader attributes (primary area, secondary area, and reader mode and reader type
- Door attributes (unlock, mode, unlock time, door processing mode and door held open time and request to exit required or not)
- Auxiliary attributes (relay output mode, relay output time and input mode)
- Physically challenged attributes (door unlock time and door held open time)
- Circuit attributes (reader tamper, door contact and exit input and auxiliary input)

5.6.4. Event Reports

There shall be the flexibility to generate reports on single or multiple sites and to provide the user with a wider range of event reports. A user selectable event period shall be available for each report run. The following minimum report types are required:

Event types selectable by:
- System
- Operator
- Access
- Alarms
- Area
- User

Search criteria selectable by:
- Area number
- Area name
- User number
- User name
- Programmable user fields
- Door number
- Door name
- Point number
- Point name
- Application module

It shall be possible for the operator to choose from multiple event types and from multiple search criteria within the same report in order to narrow the focus the result of the event report.

5.6.5. Time & Attendance Reports

This report shall provide the user with the following minimum information:

- Late arrival
- Early departure
- Number of hours worked by a user

- Absentee
- In / out status

The report shall be based upon a single user, by department, or by all users.

5.6.6. Database Views

The user shall be able to display information in two formats, a single record form which takes the form of a dialogue box with labels and fields, and a tabular grid view which is scrollable both vertically and horizontally. The tabular view will contain the field labels in its header and will display multiple records at a time in the scrollable portion of the window. The operator clicking the mouse on a column header shall accomplish sorting of data within the grid format, based upon the information listed within that column.

Editing of any particular record and/or field will be accomplished by clicking on that field (which will become light-bar highlighted) and turning on the cursor. The user will then be able to type in the changes through the keyboard. The operator in either grid or form data view format shall accomplish editing of data.

5.6.7. Access Schedules

Each controller will support a minimum of 50 access schedules. The user shall be able to build an entire access schedule on the screen and save this as one record. The system shall then build the individual command message in background and ship the access schedule to the controllers. Each access schedule shall be a weekly schedule of 7 days, and shall contain 6 intervals per schedule.

5.6.8. User Authority Groups

Whether the system is being used for the purpose of intrusion, access control or a combination of both disciplines, the same common system configuration and administration data fields shall apply. To accomplish this, the system shall be based upon an area centric product. By this philosophy, all application modules, inputs and outputs and readers shall belong to areas. All users shall belong to authority groups. The authority groups shall determine what access privileges a user shall have. By this strategy, where the system is set-up as an intrusion system, only the user's token ID numbers shall be added to the user's file in order to convert the security system to an integrated intrusion access system. The software shall also support the creation of Authority Groups, folders that contain a number of individual authority levels grouped together in a logical manner to expedite the process of associating system users with the appropriate system authority.

5.6.9. Users

The maximum number of user records supported shall be 64,000. Adding users to the system is a culmination of all of the previous configuration activities. With those database records in place, the operator shall now pick information from lists and create the user database.

Each user file shall contain a first name supporting a minimum of 15 characters and a last name supporting a minimum of 25 characters. The security application will automatically format a shortened version that shall be editable by the operator for sending down to the LCD keypad.

As part of the user file the user may choose a unique PIN. The user to log onto the LCD keypad in order to access the functionality of this application module shall use the PIN. The user may also use the PIN when the reader is set to token +PIN mode or Token or PIN mode. At anytime the user may change his or her own PIN using the LCD keypad without using a “master user” permission. Methodologies that use a fixed PIN derived from the embedded card number shall not be acceptable.

Within a user’s file a selection of language is available. The LCD keypad shall automatically display text in the language associated with the logged-in user. Where different languages are associated with individual users in a system, the LCD keypad’s primary log on screen will toggle between the applicable languages until a user logs on.

There shall be 20 user definable fields listed in the user’s file. These fields shall be used for sorting, event and custom report generation, and automatic population of fields used in the design of user photo badges. Access to the custom user fields may be restricted to an operator (in groups of five fields i.e. 1-5, 6-10) via Operator Permissions to prevent viewing of user information inappropriate to the operator’s privilege level.

A Lost Card action button on the user screen shall delete the selected user’s card number and automatically place the card number on a Lost Card screen (a separate tab under the User heading. The card number shall be unavailable for reassignment to another system user until the Card Found action button on the Lost Card screen is used, releasing the card number for reassignment.

A Void User button shall be available on the user screen, providing immediate invalidation of the user’s system privileges without deleting the associated card, PIN or user data. A message to the immediate right of the user name indicates whether the user is currently valid or invalid. For any user designated Void, a Reinstate user button shall be available for restoration of system privileges.

It shall be possible to assign a temporary authority level to users, in addition to their permanent authority level. This Authority Plus setting allows the addition of any other defined AFx authority level to the user’s permanent privileges according to a specified validation period.

A physically challenged tag may be activated in the user’s file. A physically challenged person when presenting a token to a reader controlled door will cause the following programmable actions:

- The door shall stay unlocked for a longer than normal, programmable time
- The door shall stay open for a longer than normal, programmable time before sending a door held open alarm
- An auxiliary output on the reader application module can be programmed to activate an automatic door opener

Users tagged with master override privileges shall not be affected by the rules set by the system for anti-passback, dual custody and escort mode.

When suite security has been installed as part of the integrated system solution, a single user file shall be used to set all private security privileges pertaining to his or her suite security and all access control and intrusion authorities that are required for the common areas of the facility.

The user file shall include a validation date and time and invalidation date and time. The parameters will control when the user's privileges are active.

5.6.10. Holidays

A minimum of 50 holidays shall be defined, with two being reserved as the dates to automatically switch between daylight-savings and standard time. Dates that share the same date each year or share the same day of the week each year shall not require changing by the operator each calendar year. For example, holidays that occur the 1st Monday of a given month shall not require yearly updates.

5.6.11. Password Maintenance

This activity allows the user to enter operators into the system and to assign their activity access. Operator permissions shall be configurable to allow edit or view only privileges to the application's users. Operators logging in for the first time shall be prompted to change their password. Additionally, system wide options shall be provided to allow for increased operator password security. Selectable options shall be the length of the password, the renewal time (how often operators will be prompted to change their password) and the renewal expiry (how long after the renewal time elapses before the password itself expires).

A definable lockout period shall also be configurable such that, after three failed login attempts, the application shall lockout the operator for an hour or until reset by an operator with the permission to do so. An 'Enforce Complexity' checkbox shall also be provided to require that operator passwords must include letters and numbers, will be case sensitive, cannot include three consecutive letters or numbers (i.e. abc or 123), cannot match the login name, and cannot match the present password.

The password maintenance screen shall list all of the activities in the system and provide a means of defining access for the operators.

The password maintenance screen shall allow administration to define database access restrictions such as database partitioning. During the assignment of activity levels for database access, the operator can be assigned a group of users and authority levels that shall be valid for editing. All other user groups and authority groups will be unavailable to the operator.

Operators and users passwords shall be fully encrypted and not visible to any other user or operator in the system.

3.5 GENERAL TERMS AND CONDITIONS OF THE CONTRACT

6.1. Maintenance and Repair Agreements

If awarded the contract, the Vendor agrees to enter into an ongoing agreement with the Purchaser for the maintenance and repair of the system equipment. The cost of maintenance for a period of _____ months after system installation shall be included in the tender price. Requirements for maintenance schedules, documentation and tasks are listed in an attached addendum.

If awarded the contract, the Vendor agrees that he will arrange from his supplier all software licenses as required by the supplier. The Vendor also agrees that he will purchase appropriate software maintenance agreements for full support and

maintenance of all system software as available from the supplier. The price of all software licenses and maintenance agreements shall be included in the tender.

Where the Vendor plans to sub-contract any portion of the maintenance contract, he shall indicate the items affected and the names of the sub-contractors.

The Vendor shall specify the number and location of trained service personnel available to support the system.

6.2. Guarantee

The Vendor shall warrant all equipment furnished to be new, undamaged, and free from defects and in conformity with the requirements specified within this document.

The Vendor's obligation shall include removal, repair or replacement, transportation, re-installation and testing without charge to the Purchaser, all or any parts of the system found to be defective due to faulty materials or workmanship for a period of _____ months after system installation.

6.3. Approvals

All equipment supplied shall be approved for the purpose intended by the authority having jurisdiction. Installation shall be in accordance with all standards and practices dictated by this authority.

Installation, testing and commissioning shall be done by individuals fully qualified to perform such work.

6.4. Documentation and Training

Complete documentation shall be provided which covers all aspects of the system operation. Excerpts from each available document shall be submitted with the tender as proof of its current existence and acceptability.
Documentation that covers the following topics shall be provided:

- An easy to use operation guide for non-technical and security staff.
- A system planning guide for collecting and preparing data. All planning assistance forms shall be provided.

The Vendor shall provide at least _____ days of formal, hands-on training, using the purchased and installed system. This training shall cover all aspects of system operation, management and troubleshooting. The cost of this training shall be included in the tender price.

6.5. Drawings

The Vendor shall furnish such shop drawings and diagrams as are reasonably required to clarify the details of work included in this tender.

At the conclusion of the project, the Vendor shall provide one (1) set of "as built" drawings which indicate, for example, the location of all supplied equipment in the system, all electrical box identifications, and cable identifications as installed under the terms and conditions of the final contract.

6.6. Miscellaneous Hardware

Any miscellaneous hardware items, such as connectors, cable plugs, mounting brackets, not specified in this document but which are required to make up a fully operational system shall be provided by the Vendor as part of his tender.

6.7. Supervision

The Vendor shall be responsible for the following project supervision functions:

- Supervision of sub-trades (as required).
- Attendance at site meetings.
- Attendance at project planning meetings.
- Co-ordinating his work with the Architect, Consulting Engineer, General Contractor and others.

6.8. Commissioning the System

The Vendor shall be responsible for verifying that each component of the system is fully operational and in conformity with the requirements specified within this document. He shall also be responsible for ensuring that all elements function together as a system in accordance with this document.

Commissioning shall be done in a phased manner as the installation of field equipment proceeds. It shall not be necessary for the computer to be installed and operational in order for commissioning of the system to begin. All field equipment shall be capable of being installed and programmed to operate in a stand-alone mode prior to installation of the computer.

7. INSTRUCTIONS TO BIDDERS

7.1. Vendor Qualification

The Vendor shall be fully qualified in the performance of the class of work specified within this document and shall provide a list of similar installations which have been completed and which may be inspected by the Purchaser or his representative, should the Purchaser wish to do so.

The Purchaser reserves the right to reject any tender submitted by a party whose financial standing is not considered to be such as to ensure the Vendor obtaining reasonable credit from his proposed suppliers of materials.

7.2. Response to Specification

The Vendor shall submit a point-by-point statement of compliance with Sections 1, 2 and 3. Each point shall be numbered as per the paragraphs in Sections 1, 2 and 3. Any tender submission which does not include a point-by-point statement of compliance or non-compliance with the requirements as specified in Sections 1, 2 and 3 shall be disqualified.

Where the proposed system complies fully with a requirement, such shall be indicated by placing the word "comply" opposite the paragraph number. Where the proposed system does not comply or accomplishes the stated requirement in a manner different from that specified, a full description of the deviation shall be provided opposite the paragraph number.

Where a full description of a deviation is not provided, it shall be assumed that the proposed system does not comply with the paragraph in question.

7.3. Description of Proposed Equipment

The Vendor shall provide, as part of his proposal, a complete list and detailed description of all equipment and software that are included in his tender.

Full specification sheets shall be provided for each hardware component in order to allow the Purchaser to make a comparison of the hardware proposed by all Vendors.

End of Specification