AxiomXa A&E Specification

Table of Contents

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

1. General

1.1. Purpose

1.1.1. To establish the technical, functional, jurisdictional, or regulatory and quality requirements for security and access control systems; which are required to be purchased from vendors. Approved technical specifications define the supply and installations of all security and access control systems and identify approved manufacturers and models.

1.1.2. The security system shall consist of implementing an integrated networked Access Control and Video Assessment System (ACAMVAS) that shall control personnel access, provide real time intrusion detection alarm monitoring and provide alarm driven video surveillance for the designated buildings and operations in accordance with the requirements and specifications prescribed in these documents and the approved drawings. The security system shall include the following, where applicable:

1.1.2.1. Seamless integration of a digital video management system that will allow system operators to control and maintain the security of the facilities from multiple designated client workstations.

1.1.2.2. Installation and/or replacement of door and locking hardware to enable RFID reader access at designated apertures. The apertures designated with RFID reader access shall also allow manual unlocking using the master key system.

1.1.2.3. Supply and installation of intrusion detection alarms at designated facilities.

1.1.2.4. Supply and installation of interior and exterior motion detection devices to provide alarm coverage at designated facilities.

1.1.2.5. Seamless integration of video surveillance systems that provides alarm driven assessment for the intrusion detection equipment at designated facilities.

1.1.2.6. Supply and install RFID reader access for vehicle barriers at designated facilities.

1.1.2.7. Supply and installation of all control, signal, lighting and power distribution cabling as required for the security equipment including any trenching work required for the completion of the installation.

1.1.2.8. Commissioning and testing of the systems and equipment installed as required to meet manufacturers' specifications and documented installation procedures, and to the satisfaction of the Owner.

1.1.2.9. Training of the Owner's personnel to: fully operate, and perform routine maintenance on the systems and equipment installed.

1.1.2.10. Provide all associated documentation for the security system upgrades.

1.2. Reference Standards

1.2.1. American National Standards Institute (ANSI) Standards

1.2.2. CANASA (Canadian Alarm and Security Association)

1.2.3. CE Certification (European Union Conformity)

1.2.4. CFAA (Canadian Fire Alarm Association)

1.2.5. Ontario Building Code

1.2.6. RoHS

1.2.7. Underwriters Laboratories of Canada (ULC)

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

1.3. Definitions & Acronyms

1.3.1. Aperture – a point of access such as a door, gate, elevator floor or other barrier controlled and monitored by a controller.
1.3.2. Cardholder – an individual of record issued with a valid credential, such as a token or card, and authorized access at assigned system-controlled apertures.
1.3.3. CCTV – Closed Circuit Television.
1.3.4. Controller – Access Control Unit; can refer to either a primary or subordinate unit.
1.3.5. Credential – a card, token, PIN, biometric identifier, or other device presented at a reader by a cardholder for gaining access at system-controlled apertures.
1.3.6. DVR/NVR – Digital Video Recorder/Network Video Recorder.
1.3.7. GUI – Graphical User Interface.
1.3.8. LAN/WAN – Local Area Network/Wide Area Network.
1.3.9. Operator – an individual of record with a valid user ID and password authorized with access control system administrative responsibilities.
1.3.10. RF – Radio Frequency/Radio Frequency Signalling.
1.3.11. RFID – Radio Frequency Identification (including 125kHz "proximity" and 13.56MHz "Smart Card" technologies.
1.3.12. SQL – Structured Query Language.
1.3.13. TCP/IP – Transmission Control Protocol/Internet Protocol.
1.3.14. USB – Universal Serial Bus.
1.3.15. VMS – Video Management System.

1.4. Warranty

1.4.1. Manufacturer Warranty
1.4.1.1. The Vendor shall warrant that all equipment furnished is new, undamaged, free of defects, and conforms to the specifications within this document.
1.4.2. Extended Correction Period
1.4.2.1. The Vendor's obligation shall include removal, repair or replacement, transportation, re-installation, and testing without charge to the Purchaser, for 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.

2. Products

2.1. Manufacturers

2.1.1. Specifications, functionality, system capabilities and products presented are based on RBH Controllers, related communication devices, and RBH's AxiomXa Security Management System.

2.2. Security Components

2.2.1. Listed below are the security components that shall be supplied and installed. A detailed specification of each of the security components included in this list is also included.
2.2.1.1. Security Management Software
2.2.1.2. Controllers

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.2.1.3. Communication Devices
2.2.1.4. Readers
2.2.1.5. Credentials
2.2.1.6. Locking Devices
2.2.1.7. Power Supplies
2.2.1.8. Servers/Workstations

2.3. Access Control & Alarm Monitoring System

2.3.1. General System Specifications

2.3.1.1. The access control and alarm monitoring system shall be the RBH AxiomXa Enterprise system and meets the following design and performance specifications:

2.3.1.2. The system shall be a modular, networked access control and alarm monitoring system, comprised of proven commercial off-the-shelf components, capable of handling large proprietary corporations with multiple remote sites, alarm monitoring, video imaging, badging, paging integration, CCTV integration, interactive guard tour, mapping, visitor management, email notification, third-party monitoring, BAS integration and asset management.

2.3.1.3. The system shall assure long time performance, cost effective upgrade capability and allow for easy expansion or modification of inputs, outputs and local or remote workstations.

2.3.1.4. The system control at the central server location shall be under a single software program control, shall provide full integration of all components, and shall be alterable at any time, depending upon the requirements. Reconfiguration shall be accomplished online through system programming, without hardware changes.

2.3.1.5. The Security Management System software shall utilize Microsoft SQL Server 2016/2017/2019 for data storage and be written expressly for Microsoft SQL Server 2016/2017/2019.

2.3.1.6. The system shall have the capability to be networked via a LAN/WAN connection utilizing industry standard TCP/IP communication protocol. The system shall provide encryption via the TCP/IP connection.

2.3.1.7. The system shall incorporate the use of bi-directional RS-485 communications and/or Class “A” TCP/IP redundant connections for redundancy and reliability.

2.3.1.8. The system shall incorporate “High Availability” Communications so that multiple communication paths are available to all controllers. High Availability shall be defined as, “an existing alternate controller shall take over communications in the event the main controller fails. The controller must be located in a separate location to the first.”

2.3.1.9. The system shall support both manual and automatic responses to alarms entering the system. Each alarm shall be capable of initiating a number of different actions, such as camera switching, activation of remote devices and aperture control.

2.3.1.10. The system shall provide unlimited levels of emergency codes to allow the system to operate in different security levels depending on local threat level e.g. code black = bomb threat and building locks down.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.1.11. The system shall provide both supervised and non-supervised alarm point monitoring. Upon recognition of an alarm, the system shall be capable of switching CCTV cameras and automatically creating a pop-up window for video viewing for the associated alarm.
2.3.1.12. The system shall be capable of arming or disarming alarm points both manually and automatically, by time of day, and by day of week.
2.3.1.13. Access control functions shall include validation based on time of day, day of week, holiday scheduling, site code verification, automatic or manual retrieval of cardholder photographs, and access validation based on positive verification of the credential or credential and video verification.
2.3.1.14. The system programming shall be operator friendly, and capable of being accomplished by personnel with no prior computer experience. The programming shall be menu driven and include online “Help” with the use of F1 hotkey to automatically call the proper help information to the screen. The software shall utilize drop boxes for all previously entered system required data.
2.3.1.15. After installation, the Owner shall be able to perform basic hardware configuration changes. These hardware configuration changes shall include, but not be limited to, aperture open time, aperture contact shunt time, aperture and reader names, when and where a credential is valid, and the ability to add or modify cardholder data as desired without the services of the Manufacturer or Manufacturer’s Vendor.
2.3.1.16. Equipment repair shall be able to be accomplished on site, by module replacement, utilizing spare components. All equipment shall have unpluggable connectors for easy replacement.
2.3.1.17. All control components shall include the ability to download operating parameters to any controller, thus allowing the controller to provide full operating functions independent of any other system component.
2.3.1.18. The system shall be designed in such a way that enrolment of authorized personnel is capable from a de-centralized location.
2.3.1.19. The system shall provide seamless integration to multiple manufacturers of DVRs/NVRs/VMSs at the same time.
2.3.1.20. The system shall provide seamless integration with external Building Automation Systems (BAS), personal safety systems, remote paging and email systems.
2.3.1.21. All system events, operator actions and maintenance information shall be stored in the SQL database(s) to maintain a permanent record of system activity. The system shall have the capability for manual and automatic back-up of set-up and system events to either local removable media (optical/magnetic) or remote network resource.
2.3.1.22. All workstations shall be configurable to act as an Alarm Monitoring Centre for the system. All alarms shall be configurable by schedule and workstations will have the ability to acknowledge and clear alarms as a two-step process.
2.3.1.23. All workstations shall have the ability to define alarm routing with an unlimited number of Routing levels available to the system.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.2. Interactive Mapping and Graphics

2.3.2.1. The system shall support an unlimited number of operator programmable colour graphic map displays capable of showing the floor plan, location of alarm device, and alarm instructions.

2.3.2.2. Floor plans shall be created in an approved format and shall be capable of being imported from other systems. All of the interactive graphical maps shall be displayable on workstation monitors.

2.3.2.3. Maps shall be interactive with dynamic real time status so that the operator can control all device functions from the map.

2.3.3. Information Storage

2.3.3.1. All programmed information as well as transactional history shall be automatically stored into the SQL database for later retrieval.

2.3.4. Information Backup/Retrieval

2.3.4.1. The Server shall be capable of transferring all programmed data and transactional history to a removable drive or any logical disk drive. All programmed data shall be restorable from disk in case of system hardware failure.

2.3.5. Communication Rates

2.3.5.1. The system shall have bi-directional communications and communicate up to 2.5mb/s.

2.3.6. Printers

2.3.6.1. The system shall support all system printers configured under and supported by the Windows® operating system.

2.3.7. Pointing Device

2.3.7.1. The system shall use the pointing device configured under and supported by the Windows® operating system.

2.3.8. Communication Ports

2.3.8.1. The system shall support an unlimited number of either serial or TCP/IP ports.

2.3.9. Workstations

2.3.9.1. The system shall support an unlimited number of active local or remote workstations. These workstations shall be capable of monitoring alarms and changing the database and retrieving transaction records in real time without affecting the other stations.

2.3.10. Networking

2.3.10.1. The system shall operate with the standard Windows® networking software.

2.3.11. Database

2.3.11.1. The database shall be Microsoft SQL Server 2016/2017/2019.

2.3.12. Software Capacities

2.3.12.1. The System Server shall have the following minimum requirements:

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

OS: Server 2016, 2019, Windows 10 and 11 Pro
CPU: Dual Core 3.0GHz clock speed
RAM 8GB
Primary Hard Drive: 200GB
GPU: 512MB RAM reserved
Pointing Device

2.3.12.2. System software and language development software shall be existing, industry accepted, and of a type widely used in commercial systems. The application software shall have been written in a standard, industry accepted language. All System functions shall be accessible via Windows® operating systems compliant menu accessed screens. Systems requiring command string control or complex syntax shall not be acceptable. Systems shall not be dependent upon external input other than keyboard.

2.3.12.3. The system software shall include the following features and be configured as a minimum:

Unlimited reader expansion
Unlimited cardholders in the database
Unlimited simultaneous client workstations
Unlimited time zones
365 operator-definable holidays
Unlimited Access Levels
Access Levels for each cardholder
Unlimited alarm input points
Unlimited output control points
Unlimited operator accounts with definable privilege levels
Audible alarm annunciation at the workstation
Unlimited graphical maps to be displayed on the workstation
TCP/IP or RS-232 interface capability to a CCTV system, which provides automatic, alarm actuated camera switching.
True 32/64-bit operation
Operator activation/cancellation dates
Employee activation/cancellation dates
Optional Video Imaging/Badging & barcode imprinting

2.3.13. Operators

2.3.13.1. Operators shall have the following abilities as a minimum.

2.3.13.1.1. To change any client settings from whatever workstation they are working on.

2.3.13.1.2. To establish Station Names. Station names shall be operator definable.

2.3.13.1.3. The Station Status dialog shall be available. It shall display a list of stations and their online/offline status, along with the names of the logged-on operators.

2.3.13.1.4. Report Printers: Reports as requested by the operator are sent to printer(s) that may reside anywhere on the network.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.14. Alarm Window Description

2.3.14.1. The system shall facilitate the processing of alerts by using a pop-up alarm window.

2.3.14.2. The Window shall list the system alarms and allow the operator to acknowledge and clear by right-clicking on the event.

2.3.14.3. The alarm window shall indicate the time of alarm and response time by the operator.

2.3.14.4. The alarm shall incorporate programmable instruction messages to instruct the operator what they are to do and provide the operator an action window to log an action into history for the alarm.

2.3.15. Bulk Acknowledgment of Alarms

2.3.15.1. The system shall provide a means to bulk-acknowledge alarms, so that all alarms can be acknowledged with a single operator action.

2.3.16. Station Routing

2.3.16.1. The system shall support the routing of alarms to any or all stations. Time schedules can be used to determine which station an alarm is routed during a set time. An alarm may be routed to one station or group of stations during a time schedule and re-routed to another station or group of stations during another time schedule.

2.3.17. Operator Routing

2.3.17.1. The system shall support the routing of alarms to particular operators, regardless of which station the operator is logged onto.

2.3.18. Menu Configurations

2.3.18.1. The system shall allow for the configuration and programming of controllers through the use of a simple GUI. All devices and functions shall be right click configurable for easy operation.

2.3.19. Memory

2.3.19.1. Memory within each controller shall be automatically configured by the system.

2.3.20. Database Updates

2.3.20.1. The system shall download/upload information to the controllers automatically while the controllers are in communication with the server. A data download may also be initiated manually.

2.3.21. Reporting

2.3.21.1. The system software shall have the capability to report selectable data by type and by time zone. The system software shall allow the operator to generate a report to screen, to printer or to save to a file. The reports shall be exportable to at least ten (10) different file formats. The system shall incorporate the use of an automatic report generator.

2.3.21.2. The system shall have the capability to report selectable data by type and by time zone to any combination of the workstations simultaneously.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.22. Serial Ports

2.3.22.1. All serial ports shall be configured from an easy-to-follow menu. Systems requiring in-depth knowledge of the operating system or CMOS setup for port configuration shall not be acceptable.

2.3.23. Time Zones

2.3.23.1. The system software shall have the capacity for a minimum of 255 operator-definable time zones. Each time zone shall allow for a minimum of sixteen (16) individual time intervals.

2.3.23.2. The time zones shall be assignable to:

Apertures; such as doors or elevator floors
Alarm reporting functions
Cardholders
Inputs
Outputs
Printer operations
TCP/IP and RS-232 messaging ports
Reports
Workstations

2.3.24. Holidays

2.3.24.1. The system software shall support a minimum of 365 holidays. Holidays shall be considered H1 or H2 designation so that there are three distinct holiday times. A holiday shall be capable of starting at any time/hour during a 24-hour day. Systems requiring holiday start time of midnight shall not be acceptable.

2.3.25. Aperture Descriptions

2.3.25.1. Each aperture in the system shall be identified using logical tagging format and approved by the Owner. Each aperture description shall be assigned operator-definable text of up to fifty (50) characters.

2.3.26. Access Control Modes

2.3.26.1. Each aperture may be programmed to switch automatically based on an operator defined time schedule between the following modes of operation:

“CARD/TAG ONLY”
“CARD/TAG + PIN” – Dual authentication shall be provided for access points requiring the cardholder to use their credential and enter a four or five-digit PIN.
“PIN ONLY” – Keypad/readers shall be used at apertures to grant access to individuals knowing a valid PIN.
“HIGH SECURITY”
“TWO PERSON” – To add additional security, two cardholders must be required to present a credential each in order to access a secure area.
“FREE ACCESS"

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.27. Duress

2.3.27.1. If the reader is operating in the “CARD/TAG + PIN” mode or “PIN ONLY” mode, a duress feature shall allow an alternate code to be entered into the keypad for access.

2.3.27.2. The system shall generate an alert and may be linked to control relays for notification of the alarm.

2.3.28. Alarms

2.3.28.1. Each aperture may be programmed to generate “FORCED ENTRY” and “DOOR HELD OPEN” alarms. These alarms shall have the ability to have an operator-definable time delay.

2.3.29. Alarm Annunciation

2.3.29.1. In addition to generating an alarm message, the following conditions may activate an output for annunciation:

FORCED ENTRY
DOOR HELD OPEN (DOOR AJAR)
DOOR NOT OPEN
SECURE
PATIENT
CODE TRACING
DURESS
VOID CARD/TAG
DENIED CARD/TAG
ANTI-PASSBACK VIOLATION
INPUT DOOR ALARM
TAMPER
ALARMS

2.3.30. Alarm Description

2.3.30.1. Each alarm point may be defined with a plain text description of up to fifty (50) characters.

2.3.31. Alarm Enabling

2.3.31.1. Alarm Inputs shall be enabled during operator-definable time zones and may be manually enabled/disabled from any workstation.

2.3.32. Additional Alarms

2.3.32.1. The system must also generate alarms for the following:

Enclosure tampering
Controller communication loss
Channel 1 Fail / Channel 2 Fail
Battery Failure
AC Failure
Reader Fuse
Auxiliary Fuse

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

Lock Fuse
Alarm tampering (supervised)

2.3.33. Alarm Supervision

2.3.33.1. When using supervised alarm inputs, the system must monitor for “OPEN”, “SHORT”, in addition to “NORMAL/ABNORMAL” conditions.

2.3.34. ASCII Output

2.3.34.1. Alarm Inputs shall output an ASCII message via RS-232 or TCP/IP command for integration to any other IP commandable device. This command/output shall be an optional, operator-definable and transmitted on alarm points going into abnormal state, returning to a normal state, or both.

2.3.35. Outputs

2.3.35.1. Shunt relays: Operator definable outputs may be assigned as shunt relays, allowing access apertures to be monitored by third-party alarm systems.

2.3.35.2. Relay “on” time: Outputs assigned to control apertures shall be operator-definable from 1-127 seconds or minutes.

2.3.36. Encryption

2.3.36.1. The passwords shall be encrypted in the operator database using encryption to facilitate confidentiality of individual operator passwords.

2.3.37. Operator Access Levels

2.3.37.1. The system shall provide unlimited operator access levels for the system. All operator actions will be recorded within the system database.

2.3.38. Password Security

2.3.38.1. The Operator password shall be encrypted to prevent operators from seeing passwords. Passwords shall be up to twenty (20) alphanumeric characters and be case sensitive. Operators must have the right to edit their own password for secrecy.

2.3.39. Partitioning

2.3.39.1. The System shall incorporate true database partitioning by operator. An operator shall logon anywhere on the system and have the same functionality at any workstation. Operators will be limited to view and control of the system by their operator access level.

2.3.40. Operator Roles

2.3.40.1. The system shall have the ability to define unlimited operator roles. As a minimum, the operator roles shall be:
General Administrator
Supervisor
General operator

2.3.40.2. Privilege levels shall be assignable to, but not limited to the following menu functions:

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

View
Edit
Edit of any field within the menu
Select

2.3.41. Operator Activity

2.3.41.1. All operator activity including specific changes to the database shall be stored for later retrieval and operators shall be assigned a time zone for the purpose of logging in.

2.3.42. Audit Trail of Database Changes

2.3.42.1. The system shall record changes to the database, including the date, time, operator name and description of the record changed.

2.3.42.2. The audit trail event messages shall record additions, deletions and revisions. The record shall contain a date/time stamp for the change, the logged-on operator's name, the table name, a character identifying the change, and a description based upon the Name field from the record, such as the operator ID, operator name, controller name, device name.

2.3.42.3. The system shall do a full restore or partial depending on operator selection of the data or history files during the back-up process.

2.3.42.4. The system shall allow for viewing of the audit trail.

2.3.42.5. The system shall NOT allow the Audit Trail table to be edited.

2.3.43. Employee Definitions

2.3.43.1. Cardholder data entry – Cardholder data entry shall be easy so that minimal training is required. Credential input and changes shall be allowed through direct interface with the event viewer screen.

2.3.43.2. Credentials shall have the ability to have multiple access levels or assigned special access levels.

2.3.43.3. Cards may be deactivated in the system while the data remains for reactivation at a later date.

2.3.43.4. Credential Data – The system shall allow for credential numbers up to 18 digits.

2.3.43.5. Cardholder records shall consist of a minimum of the following:

Credential Number
Issue level
Two (2) groups of access level and time zone
Operator-definable PIN code
Facility code
Anti-passback location and status
Expiration date
High Security
Lock/Unlock privilege
Code Links
Track status
Last Door accessed
22 operator definable searchable text and data fields

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

Duration use
Escort
Extended shunt (for ADA compliance)
Anti-passback override

2.3.43.6. Batch Loading – The system software shall allow groups of card/tags to be input through the use of a card/tag number range or by a batch load employee field.

2.3.44. Reports

2.3.44.1. Data Storage – All programmed and transactional history is automatically stored to the database for later retrieval.

2.3.44.2. System Function – The system software shall be capable of generating reports without affecting the real time operation of the system.

2.3.44.3. Media – Reports shall be generated from the database and exportable to at least 10 file formats including PDF, DOC, XLS and others.

2.3.44.4. Search Criteria – The database shall be structured such that the operator shall determine the search parameters based on variables available on the individual report menu. Systems requiring the operator to type complicated search strings shall not be acceptable.

2.3.44.5. Report Types:

2.3.44.5.1. Operator-definable data reports shall be available for the following information:

Cardholder data
Door Groups
Time Zones
Doors
Inputs
Relays
Links
Controllers
Operators
System hardware configuration
System settings configuration

2.3.44.5.2. Transaction Reports – Transaction reports shall be available for the following:

Credential transactions
Alarm transactions
Event transactions
Operator activity
Time and Attendance

2.3.44.5.3. Report Scheduling – The system software shall have the ability to batch reports to any of:

screen report
report to a network printer or
save a report to a file without operator initiation

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.45. System Guides

2.3.45.1. The system software shall have on line help available at any point requiring operator input.

2.3.45.2. The help screen shall be accessible by using the standard Windows® help systems.

2.3.45.3. These help screens shall contain context sensitive information that shall allow the operator to enter correct data without consulting the manual.

2.3.45.4. The help menu shall be accessible to the exact point in software by using the “F1” hotkey.

2.3.46. System Status

2.3.46.1. Real Time Status – The operator shall be able to monitor via graphical screens, the status of devices including apertures, alarm inputs, and outputs in real time.

2.3.46.2. Alarm Monitor – A screen shall be available to monitor alarms and view, at minimum, ninety-nine (99) of the most recent events. The operator shall also have the ability to view additional detail of any event through the use of a single keystroke or click of the mouse.

2.3.47. Graphics

2.3.47.1. Graphics File Format – The floor plans shall be configured in Bitmap, GIF, JPEG or PNG.

2.3.47.2. Programming – The system software shall be able to import floor plans saved as an image type file.

2.3.47.3. Operation – Upon activation of a selected input or output alarm, the map shall pop-up and display the alarmed device with an alarmed icon. The operator shall be able to click on the map and clear the alarm or control the device from the interactive map interface.

2.3.48. Video Badging

2.3.48.1. The system shall have the capability to permit Video Imaging and Badging, which shall, when used in conjunction with the system software, function as an integrated Video Imaging/Badging and access control system.

2.3.48.2. The system shall utilize a single workstation to input data for both access and video Badging. The system shall not require the operator to enter data more than once.

2.3.48.3. Badge information including name, credential number, signature, fingerprint, operator defined text, barcoding and up to five (5) data fields shall be available for each badge template.

2.3.48.4. The system shall provide for operator definable backgrounds. These backgrounds may be a "captured" image or a colour background. The system shall be capable of supporting Windows 10 or 11 Pro compliant video printers.

2.3.48.5. Badges may be created in both horizontal and vertical configurations.

2.3.48.6. In order to change a cardholder's badge, a new background may be selected from the background table. A new picture capture is not required.

2.3.48.7. The system shall allow any input or reader to be programmed such that an event at that location is captured by a remote camera and displayed while being stored

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

in the database for later viewing or printing. Events at the reader shall display in real time and store a "split screen" showing the stored cardholder image next to the "captured" image.

2.3.48.8. Camera control shall be accomplished via a supported serial or TCP/IP interface from the system to a video switcher. The programming of the camera switcher for the individual inputs and readers shall not require exiting from the access control program.

2.3.48.9. Additional Badging and/or alarm workstations may be added via LAN.

2.3.49. Video Imaging

2.3.49.1. The system shall have the capability to import images of employees and store them in the database. These images may be recalled and displayed by the operator.

2.3.49.2. The system shall have the ability to capture and save images from IP Video Cameras.

2.3.49.3. The system shall provide for the backing up and restoring of captured pictures.

2.3.50. VMS & NVR/DVR Integration

2.3.50.1. The system shall integrate seamlessly via TCP/IP to multiple manufacturers VMS, NVR, and DVR devices simultaneously.

2.3.50.2. The operator shall have the option to associate any camera with a device and through a common video window, control and operate any device with real time viewing.

2.3.50.3. Video shall be accessible from any device via a right mouse click. Video history of any event shall be accessible via a right mouse click. The video window shall automatically pop-up upon activation of the associated device's alarm.

2.3.50.4. Video shall be common to all manufacturers systems so that the operator only sees one view.

2.3.51. Interactive Guard Tour

2.3.51.1. The system shall incorporate an interactive guard tour module to provide real time status of the Guards progression. Failure to complete a tour shall activate alarms on-site and off-site for life safety operations.

2.3.52. Asset Management

2.3.52.1. The system shall incorporate an asset management module so that owners are assigned to equipment or vehicles to prevent theft. Upon alarm the system shall notify via alarm, CCTV interface, and email status the improper event.

2.3.53. System Tools

2.3.53.1. Copy Wizard – The system shall provide a copy wizard to quickly copy any device parameter to any other single or group of devices.

2.3.53.2. Back-up Scheduler – The system shall have a backup scheduler for automatic backup of data.

2.3.53.3. Custom Cardholder fields – The system shall have the ability to custom design the cardholder data by adding new fields at will.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.54. Biometric/Fingerprint Enrollment

2.3.54.1. The software shall have an integrated tab in the cardholder screen to enable the operator to enroll fingerprints/biometrics directly from the software.

2.3.55. C-NET – Controller Network

2.3.55.1. The C-NET is the communications network that links network controllers together.

2.3.55.2. Each C-NET can support up to fifteen (15) network controllers. They must be connected to each other via RS-485 connection and each panel will take address from its dipswitches.

2.3.56. D-NET Device Network

2.3.56.1. The D-NET is the communications network that links card reader controllers (RC-2/N-IRC/N-URC) and input/output controllers (IOC-16) to the network controllers in the C-NET.

2.3.56.2. Up to four (4) RC-2/N-IRC/N-URCs and sixteen (16) IOC-16s can be connected to a single network controller via RS-485 connection and each panel will take address from its dipswitches.

2.3.57. E-NET Controller Network

2.3.57.1. The E-NET is the communications network that links network controllers together.

2.3.57.2. Each E-NET can support up to fifteen (15) network controllers. They are linked together over TCP/IP and each panel will take address through the network also without the use for the Dipswitches, but they must be on the same LAN together.

2.3.58. IP Address Change

2.3.58.1. When using static IP Addresses for controllers and for any means, migrated all device IP addresses and changed them, the controllers will sense this change and will allow the IP address changing process to be done smoothly.

2.3.59. ACS/VMS Integration

2.3.60. Integration must be through TCP/IP (relay and/or RS-232 connections are not acceptable).

2.3.61. All devices within the ACS system must have a tab to associate a video camera from the VMS to the device. This association must allow the camera to be called into the ACS GUI upon the following conditions:

2.3.61.1. Any incoming event from a specified device.

2.3.61.2. Any incoming alarm from a specified device.

2.3.61.3. The camera, if PTZ must also be called to its predesignated position.

2.3.62. The ACS must be able to connect to the VMS system and display the VMS's default video window as a native VMS viewing client.

2.3.63. The ACS must have the ability to pop-up any video event designated for pop-up without operator intervention.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.64. The ACS must have the ability to manually call video by clicking on the event anywhere it appears in the ACS.
2.3.65. The ACS must have the ability to dynamically place the cameras from the VMS system on its maps and call video from the maps directly.
2.3.66. The ACS must have the ability to report all events tagged with video and play back directly from the report within the ACS GUI.

2.4. Hardware – AxiomXa Controllers

2.4.1. UNC-500 TCP/IP Controller

2.4.1.1. The controller shall be a 32-bit microprocessor controlled solid-state electronic device and shall include a real time clock/calendar on board. Circuit boards shall be made of gold-plated construction (Copper or leaded will not be accepted) and incorporate flash-ware technology.
2.4.1.2. Communication shall consist of single or dual channel TCP/IP standard LAN/WAN environment protocol.
2.4.1.3. A subset of the system database sufficient to support access and alarm functions for its designated readers and points shall be stored at the controller.
2.4.1.4. In event of communication loss, the controller shall continue to function without degradation of operation and shall provide storage of at least 30,000 events and up to a maximum of 100,000 events with extended memory capacity. These stored events shall be uploaded to the database automatically upon restoration of the communications.
2.4.1.5. The controller shall be capable of performing all system functions indefinitely without the Server.
2.4.1.6. The controller must be FCC, CE, RoHS and (c)UL listed.
2.4.1.7. The controller must have 8MB RAM available on board.
2.4.1.8. The controller must have three (3) programmable RS-485 ports.
2.4.1.9. The controller must have two (2) on board Wiegand reader ports to accept any Wiegand format and up to five (5) Wiegand formats simultaneously.
2.4.1.10. The controller must have eight (8) fully supervised inputs capable of individual configuration for EOL (single and dual EOL), N.O, N.C. operation.
2.4.1.11. The controller must have eight (8) outputs. Four (4) form 'C' relay outputs rated for 10A-30VDC and four (4) open collector outputs rated for 100mA.
2.4.1.12. The controller must have either a single or dual on-board TCP/IP LAN connections capable of configuration in LAN switch mode or dual LAN operation for Class 'A' Communication configurations.
2.4.1.13. The Controller must have separate tamper input.
2.4.1.14. Input voltage shall support 12VDC or 30W PoE+, maximum current draw 500mA.
2.4.1.15. The controller must have internal charging circuit for 12VDC gel cell standby battery. The controller shall be capable of recharging a standby battery from either PoE+ source or 12VDC local power supply.
2.4.1.16. The controller shall be configurable in the following methods. Edge device, Wall-mount or Rackmount.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.4.1.17. Edge device deployment shall be PoE+ and operate continuously even if PoE is lost. Edge controller shall operate one (1) or two (2) apertures as desired.
2.4.1.18. Rackmount configuration shall be 2 UNC-500 controllers or four (4) apertures in a standard 1U – 19In. rack configuration. LAN connections shall be front facing as standard Network configuration. All device connections shall be independent and removable from the rear of rack for quick disconnect and easy troubleshooting. All rackmount cabinets shall have optional rails for slide out configuration. All rackmount cabinets shall have top removable panel to access control panels.
2.4.1.19. The controller, when configured in switch mode shall allow LAN looping from one standard TCP/IP device to another as any standard network switch allows without the use of external switches or special LAN cabling.
2.4.1.20. The controller must accept and control up to seven (7) subordinate reader controllers and sixteen (16) I/O controllers simultaneously.
2.4.1.21. Links are defined as any action causing any reaction on the system. Each controller shall be capable of initiating 'Links' regardless of the computer status.
2.4.1.22. Readers shall have the ability to initiate '3 swipe' and/or '4 swipe' commands based on cardholder programming to initiate a different sequence of events depending on the need.
2.4.1.23. The controller shall be capable of storing and reading up to five (5) custom credential formats simultaneously. The controller shall be able to read the format of most Magnetic Stripe, Barcode, RFID or Wiegand Effect encoded credentials.
2.4.1.24. The controller shall be capable of reading credential numbers up to eighteen (18) digits.
2.4.1.25. The controller shall have the capacity to store up to 128 time zones with each time zone consisting of up to 16 intervals of time. Each interval of time shall consist of a range of days (seven days of the week, in addition to a Holiday Schedule) as well as a range of time. The controller panel shall automatically manage time zones based upon its internal clock.
2.4.1.26. The controller shall allow for the definition of up to 365 Holidays. Holidays shall be defined according to day of year and time of day. All holidays shall be automatically incorporated into Time Zone definitions.
2.4.1.27. Each credential reader and/or keypad device shall have the ability to independently operate in up to six (6) different modes:
    2.4.1.27.1. Card/tag reader only,
    2.4.1.27.2. PIN only,
    2.4.1.27.3. Common Code only,
    2.4.1.27.4. Card/tag Reader plus PIN,
    2.4.1.27.5. High Security
    2.4.1.27.6. Free Access.
    2.4.1.27.7. These modes of operation shall be programmed from the system host computer and shall automatically change by time zone assignment.
2.4.1.28. The system shall support interlock groups for Man–trap operation.
2.4.1.29. The controller panel shall allow for the support of anti-passback operation, in which cardholders must follow a proper in/out sequence.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.4.2. UNC-100 Controller

2.4.2.1. The controller shall be a 32-bit microprocessor controlled solid-state electronic device and shall include a real time clock/calendar on board. Circuit boards shall be made of gold-plated construction (Copper or leaded will not be accepted) and incorporate flash-ware technology.

2.4.2.2. Communication shall consist of a single channel TCP/IP standard LAN/WAN environment protocol.

2.4.2.3. A subset of the system database sufficient to support access and alarm functions for its designated readers and points shall be stored at the controller.

2.4.2.4. In event of communication loss, the controller shall continue to function without degradation of operation and shall provide storage of at least 30,000 events. These stored events shall be uploaded to the database automatically upon restoration of the communications.

2.4.2.5. The controller shall be capable of performing all system functions indefinitely without the Server.

2.4.2.6. The controller must be FCC, CE, RoHS and (c)UL listed.

2.4.2.7. The controller must have 2MB RAM available on board.

2.4.2.8. The controller must have one (1) programmable RS-485 port.

2.4.2.9. The controller must have two (2) on-board Wiegand reader ports to accept any Wiegand format and five (5) Wiegand formats simultaneously.

2.4.2.10. The controller must have four (4) fully supervised inputs capable of individual configuration for EOL (single and dual EOL), N.O, N.C. operation.

2.4.2.11. The controller must have four (4) outputs. Two (2) form 'C' relay outputs rated for 10A-30VDC and two (2) open collector outputs rated for 100mA.

2.4.2.12. The Controller must have separate tamper input.

2.4.2.13. Input voltage 12VDC or 30W PoE+, maximum current draw 500mA.

2.4.2.14. The controller must have internal charging circuit for 12VDC gel cell standby battery. The controller shall be capable of recharging a standby battery from either PoE source or 12VDC local power supply.

2.4.2.15. The controller shall be configurable in the following methods. Edge device, Wall-mount controller.

2.4.2.16. Edge device deployment shall be PoE+ and operate continuously even if PoE is lost. Edge controller shall operate one (1) or two (2) apertures as desired.

2.4.2.17. The controller must accept and control up to seven (7) subordinate reader controllers and sixteen (16) I/O controllers simultaneously.

2.4.3. IOC-16 Input Output Controller

2.4.3.1. Additional inputs and outputs shall be available by adding I/O controllers. Each I/O controller shall have a minimum of sixteen (16) supervised input/output terminals. The inputs shall incorporate full supervision of seven (7) circuit types and the outputs shall be form "C". Up to sixteen (16) IO controllers shall be available for each controller UNC series controller.

2.4.3.2. The I/O controller shall be independently powered and have its own back up power supply and charging circuit for a minimum of 4-hours standby operation.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.4.4. RC-2 Reader Controller

2.4.4.1. The controller should be (c)UL listed and also comply with FCC and CE regulations.

2.4.4.2. Architecture:

2.4.4.2.1. The controller shall support two (2) access control apertures.

2.4.4.2.2. The controller shall support local means of control through system and hardware links as well as reader and/or keypad input.

2.4.4.2.3. The controller shall support field interface to eight (8) variously configured alarm inputs.

2.4.4.2.4. The controller must have eight (8) outputs.

2.4.4.3. This functionality shall enable any offline controller to maintain full access control processing capability. A cardholder shall not be aware of the offline condition.

2.4.4.4. Communications:

2.4.4.4.1. The hardwired communication network shall be wired with 18AWG twisted- pair, shielded cable.

2.4.4.4.2. The hardwired network shall have maximum length of 4,000ft.

2.4.4.4.3. This network shall be wired in a linear configuration.

2.4.4.5. The controller shall be configured to report various panel communications status messages to the Server with abilities to:

2.4.4.5.1. Suppress individual message types of a specific alarm input based on a schedule.

2.4.4.5.2. Display a pre-defined message for each event type of a specific alarm Input.

2.4.4.6. The Controller shall provide event reporting of the following events: Panel online, Panel offline & Panel trouble.

2.4.4.7. Hardware Configuration:

2.4.4.7.1. Panel Addressing – The controller's address shall be set via four onboard dip-switches. Available addresses shall be one (1) through sixteen (16).

2.4.4.7.2. Communications speed settings – The controller's communications speed shall be set via two onboard dip-switches. Available rates shall be 9.6, 28.8, 38.4 and 56kbps.

2.4.4.7.3. The controller shall provide means of RS-485 network tuning, specifically: low bias, high bias & termination. The tuning shall be accomplished by adjusting onboard jumpers.

2.4.4.8. Reader Interface:

2.4.4.8.1. The controller shall support field interface to access control readers of various types.

2.4.4.8.2. The unit shall support up to five (5) different credential formats simultaneously.

2.4.4.8.3. The unit shall support all major reader technologies:

2.4.4.8.3.1. RFID

2.4.4.8.3.2. Magnetic Stripe

2.4.4.8.3.3. Wiegand

2.4.4.8.3.4. Barcode

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.4.4.8.3.5. Keypad Only
2.4.4.8.3.6. RFID with Integrated Keypad
2.4.4.8.3.7. Magnetic Stripe with Integrated Keypad
2.4.4.8.3.8. Hand Geometry
2.4.4.8.3.9. Fingerprint
2.4.4.8.4. The unit shall provide dedicated control over Red and Green LEDs for each access point.
2.4.4.8.5. The unit shall provide dedicated control over Buzzer for each access point.
2.4.4.8.6. Wiring lengths of 500ft. utilizing 20AWG and 250ft. utilizing 22AWG six (6) or eight (8) conductor shielded cables shall be required.
2.4.4.9. Alarm Inputs:
2.4.4.9.1. The unit shall provide eight fully programmable alarm inputs.
2.4.4.9.2. Each alarm input shall support all of the following circuit types:
2.4.4.9.2.1. N.O. non-supervised
2.4.4.9.2.2. N.C. non-supervised
2.4.4.9.2.3. N.O. supervised with one resistor
2.4.4.9.2.4. N.C. supervised with one resistor
2.4.4.9.2.5. N.O. supervised with two resistors
2.4.4.9.2.6. N.C. supervised with two resistors
2.4.4.9.2.7. Combination N.O. and N.C. supervised with one resistor
2.4.4.9.3. Wiring lengths of 1,000ft. utilizing 20 or 22AWG cables shall be required.
2.4.4.10. Alarm Outputs:
2.4.4.10.1. The unit shall provide eight fully configurable outputs (four form 'C' relay and four open collector).
2.4.4.10.2. Each output shall be configured as fail-safe or fail-secure.
2.4.4.10.3. Relay output shall be rated for 2A @ 30VDC.
2.4.4.10.4. Open collector outputs shall switch negative 12VDC @ 100mA.
2.4.4.11. Enclosure Dimensions:
2.4.4.11.1. The enclosure for the controller shall be of the following dimensions: 12" x 14" x 3 ½"
2.4.4.12. Environmental tolerances:
2.4.4.12.1. The unit shall function within the following environmental tolerances – Operating temperature: 35-150°F and Operating humidity: 20-80% RH (non-condensing)

2.5. RBH-ENCL2 Wall Cabinets

2.5.1. The controller enclosure shall have a hinged cover with key lock. A control panel input point shall monitor an enclosure tamper switch.
2.5.2. The cabinet shall be 22" x 18" x 4" with ½ and ¾ inch knockouts. The back of the cabinet shall have key mounts for easy mounting.
2.5.3. The cabinet shall hold any two of the following controllers UNC-100, UNC-500, RC-2 & IOC-16.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.6. Readers & Credentials

2.6.1. The system shall employ a contactless access control/identification technology that utilizes RF circuits in microchip form. The microchips are encoded and transmit the encoded information when activated.

2.6.2. The readers shall be any Wiegand output or equivalent proximity / iCLASS / MiFARE / DESFire type. It shall read the identification number of the credential when presented to the surface of the reader without requiring physical contact.

2.6.3. Single piece window/doorframe reader, which shall mount directly on a standard 1.75" (4.5cm) metal mullion/doorframe. The reader can be mounted indoors or outdoors on virtually any surface, including metal. The reader shall operate between 5-14VDC to allow for ease and flexibility in installation. Read range with a standard RFID credential shall be up to 4" (up to 10cm) when installed according to manufacturer's specifications. Maximum dimensions of the reader shall be 5.5" (14.0cm) high x 1.6" (4.1cm) wide x 0.75" (1.9cm) thick.

2.6.4. A single piece wall switch reader, which shall mount directly on a standard metal or plastic single-gang electrical box, or on a flat wall or metal surface, and shall operate indoors or outdoors. The reader shall operate between 5-14VDC to allow for ease and flexibility in installation. Read range with a standard RFID credential shall be up to 4" (10cm) when installed according to the manufacturer's specifications. Maximum dimensions of the reader shall be 4.6" (11.7cm) high x 2.9" (7.6cm) wide x 0.5" (1.3cm) thick.

2.6.5. A single piece reader, which shall mount to any surface, including metal, or can be concealed behind most building materials, except metal. Read range with a standard RFID credential shall be up to 7" (17cm) when installed according to manufacturer's specifications. Maximum dimensions of the reader shall be 4.6" (11.7cm) high x 5.5" (14cm) wide x 1.4" (3.6cm) thick.

2.6.6. A medium range reader, which shall mount to most surfaces, except directly on metal, or can be concealed behind most building materials, except metal. Read range with a standard RFID credential shall be up to 21" (42cm) when installed according to manufacturer's specifications. Maximum dimensions of the reader head shall be 8.8" (22.4cm) high x 8.8" (22.4cm) wide x 1.14" (2.9cm) thick.

2.6.7. The credential shall be read when presented in any orientation or at any angle to the surface of the reader within the proper read range.

2.6.8. The reader shall power the credential, process the encoded data, and output the data to the access system in less than 110 milliseconds.

2.6.9. There shall be no removable plate or cover, which allows access to the reader electronics.

2.6.10. A red/green LED on the front surface of the reader shall indicate to the cardholder that the credential was read (internal/reader controlled) and an access decision was made (system controlled). The LED may be configured in either single line mode or dual line mode (allowing an "off" state) as required by the host system, and the reader may be switched between modes by presenting a programming credential to the face of the reader.

2.6.11. The reader shall have an audible "beep" tone feature to indicate to the cardholder that the credential was read (internal/reader controlled) and an access decision was

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

made (system controlled). The audio tone must be independently controllable and not tied to the status or colour of the LED. The internal control of the LED and beeper may be enabled/disabled via programming credential so as not to require the setting of switches internal to the reader.

2.6.12. The reader shall have a built-in diagnostic, which indicate to the installer that upon power up the reader has performed an internal test and is functioning properly.

2.6.13. The reader shall have a built-in diagnostic feature, which allows a single technician to test the continuity of the data lines independent of the controller. The reader may be placed into the line diagnostic mode via a programming credential, and the technician can then measure the pulses at the end of the line without the need of a second technician at the reader presenting credentials.

2.6.14. Electrical connections between the reader and the controller shall be via colour coded, multiconductor; #22 AWG shielded cable. No coaxial cable or special connectors shall be required. The output shall be in the form of Wiegand data stream.

2.6.15. Wiring from the reader assembly to the controller shall be run inside metal conduit or EMT, as may be required by electrical codes. All junction boxes are to be concealed and not normally accessible to the public. Utilization of PVC conduit is not acceptable.

2.6.16. Accidental or intentional transmission of RF signals into the reader shall not compromise the system.

2.6.17. The reader shall function in the access control system's normal or anti-passback mode without changes to the reader.

2.6.18. The reader operating temperature range shall be -40° to +50°C

2.6.19. Damage or vandalism to the reader shall not damage any other part of the system.

2.6.20. Tampering with the reader shall have no effect on the aperture security.

2.6.21. The system readers shall have the capability to accept codes from any of the following RFID devices:

2.6.22. A standard molded plastic credit card sized credential having maximum dimensions of 3.41" (8.7cm) x 2.14" (5.4cm) x 0.09" (0.23cm), and a weight of not more than 0.48 oz. (13.5g). A punched slot shall be provided for a strap or clip. The credential shall be capable of having multi-colour custom graphics and permanently marked numbers printed directly onto both sides.

2.6.23. A tag having maximum dimensions of 2.2" (5.6cm) x 1.3" (3.3cm) x 0.25" (0.6cm), and weight of 0.36 oz. (9.9g). An eyelet shall be provided for attachment to a key ring.

2.6.24. A credit card sized credential made of PVC, having maximum thickness of .036", and the capability of accepting direct print video imaged graphics and photographs and able to carry a high coercivity magnetic stripe.

2.6.25. A credit card sized credential having maximum thickness of .048", and capable of accepting a photograph and graphics via a customer laminated flap.

2.6.26. The credential shall be a polycarbonate-based form that cannot be run through direct printers. The credential shall be a PVC dual technology unit that employs RFID sensor technology. It shall comply with ISO standards for thickness (30 mil).

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.6.27. The credential shall be made of robust ABS plastic to provide maximum protection for the circuitry inside and provide minimal flexing which could cause damage to the credential.
2.6.28. The presence of small metal objects, such as keys or coins near the credential shall not alter the code read by the reader, nor prevent the code from being read by the reader.
2.6.29. The credential shall be of a proprietary format to be controlled by the Owner.
2.6.30. Credentials shall be sequentially numbered. The purchaser may specify codes or numbers.
2.6.31. The credential must have the ability to have the encoded number permanently marked on the outside surface.
2.6.32. The credential shall be a passive device with no internal battery, but shall contain a semiconductor element, which is energized when brought within the operating range of the reader causing transmission of the code from the credential to the reader. Credentials requiring an internal battery or energy cell shall not be acceptable.
2.6.33. Credentials may be used interchangeably and shall be compatible with all readers in the system, regardless of the reader's physical size or style, and without any code matching or memory devices in the reader.
2.6.34. The credential operating temperature range shall be -40° to +50°C.

2.7. Alarm Keypads

2.7.1. The system shall incorporate alarm keypads that link directly to the system for advanced alarm operation. Integration to third-party alarm systems is not acceptable.
2.7.2. Operators can arm, disarm, send messages and monitor any alarm on the keypad. In addition, the keypads shall have entry exit zones and the ability to initiate commands on the system by entering a code or command.
2.7.3. The keypads will have the ability to arm or disarm any group of inputs on the system creating a seamless alarm intrusion panel.
2.7.4. Alarm Monitoring Integration:
2.7.4.1. The system shall allow for annunciation of intrusion detection alarms. Intrusion detection alarms shall report just like any other access control alarm and shall have the same annunciation and display properties as access control alarms.
2.7.4.2. Alarms from the alarm keypad shall be displayed in the alarm monitoring window and any signal can be sent out via TCP/IP or RS-232 message port.
2.7.4.3. The system shall support an Alarm Details description that shall show the ‘Alarm Description’, ‘Time/date’, ‘Controller’, ‘Device’, and ‘Area’ associated with the alarm. The information shall also display the operator.
2.7.4.4. The system shall support tracing of intrusion detection devices and areas.
2.7.4.5. The system shall be able to report status information for the intrusion detection devices.
2.7.4.6. On alarm, the system shall automatically switch to the map that displays the alarm, the icon that represents that alarm point will flash and an audible alert will

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

be generated on the workstation sound system. The operator shall have to acknowledge the alarm before processing the alarm.

2.7.4.7. In operator alarm mode processing, the system shall allow the operator to:
- 2.7.4.7.1. Clear alarm, tamper, and diagnostic alarms.
- 2.7.4.7.2. Observe CCTV camera views, individually or in groups, that are associated with an alarm (requires video switcher option).

2.7.4.8. In normal processing mode, the system shall allow an operator to:
- 2.7.4.8.1. View a list of activity information, and select and tag any event.
- 2.7.4.8.2. View site maps.
- 2.7.4.8.3. Perform a test of testable devices/sensors.
- 2.7.4.8.4. Change the state of sensors to access or secure.
- 2.7.4.8.5. Review the last 1,000 events/actions performed on the system.

2.7.4.9. In maintenance processing mode, the system shall allow the maintenance technician to:
- 2.7.4.9.1. Assign passwords and function access to individual users.
- 2.7.4.9.2. Examine the input/output point states.
- 2.7.4.9.3. Adjust the sensitivity of the sensors.
- 2.7.4.9.4. Access the operating system to diagnose system problems.
- 2.7.4.9.5. Set the calendar clock's date and time (in Windows).
- 2.7.4.9.6. Change the format of the displayed date (in Windows).
- 2.7.4.9.7. Set the communication parameters for system devices.
- 2.7.4.9.8. Shut down the system.

2.7.5. Alarm Keypad Hardware Special Features

2.7.5.1. Combining Access Control, Burglar Alarm, Keypad Arming Stations and Monitoring functionality into an unprecedented Controller and complete security solution.

2.7.5.2. Fit into any Security application that requires Access Control and Burglar Alarm functionality such as Home, Small Business, Corporate, Industrial and Condominiums.

2.7.5.3. Can be optimized to leverage building infrastructure for a fast and economical deployment in the LAN/WAN environment. This negates the requirement to install a separate dedicated RS-485 communication infrastructure saving time and money.

2.7.5.4. Expandable and flexible with up to 256 alarm zones available to each keypad and an unlimited number of keypads there is never any need to install multiple Burglary controllers in a facility even if the buildings are not on the same property.

2.7.5.5. Packed with features such as built in Access Control, PoE+, Email notification, SMS notification.

2.7.5.6. Complete with remote access via web or App.

2.7.5.7. Credential capacity: 500 for Standalone mode, or up to 50,000 in integrated mode.

2.7.5.8. Built-in 4 inputs & 2 outputs.

2.7.5.9. Support 32 Zones for standalone mode, or up to 256 zones in integrated mode.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.7.5.10. Contains 1 MB of memory for the card storage, a single RS-485 Channel, PoE+ & single Weigand reader port.

2.8. Fingerprint/Biometric Readers and Software Integration

2.8.1. The fingerprint reader shall be of the RBH-BFR series.

2.8.2. The software shall have an integrated tab in the cardholder screen to enable the operator to enroll fingerprints/biometrics directly from the software. Programs that open third-party software are unacceptable.

2.8.3. The capture template will allow the capture of a primary and secondary finger as a backup.

2.8.4. The authentication will be automatically downloaded to the reader upon successful capture of the fingerprint without intervention by the operator. The download shall be by TCP/IP communications to the fingerprint readers.

2.8.5. The fingerprint must be saved as an algorithm to protect individual privacy.

2.8.6. The fingerprint algorithm shall be saved within the normal AxiomXa database for automatic backup and restore capabilities. External backup systems for fingerprint are not acceptable.

2.8.7. The fingerprint reader shall be configurable to operate in any of the following modes. Finger only, Card only, Card & Finger, Finger & PIN code, Finger or Card.

2.8.8. The reader shall have a Wiegand output to connect to the controller.

2.9. Wireless Lockset Integration

2.9.1. The system shall support the integration of Assa Abloy Aperio, Allegion AD-400 & Engage platform and SALTO SALLIS wireless locksets with the security management system.

2.9.2. The wireless system and components shall offer as a minimum:

2.9.2.1. Wireless Radio Frequency based on IEEE 802.15.4 at 2.4 GHz.

2.9.2.2. Wireless communication shall incorporate AES 128-bit encryption.

2.9.2.3. Reading time shall be less than 150 milliseconds.

2.9.2.4. RFID technologies: Proximity, MiFARE, DESFire, HID iCLASS.

2.9.2.5. Powering by standard non-proprietary, commercially available batteries. Renewal of batteries shall only be permissible from the secure side of any door with access to the battery compartment only achievable using non-commercially available tool sets provided exclusively by the manufacturer.

2.9.2.6. All electronic locking devices must be able to be temporarily activated by an appropriate device in the event of total battery failure.

2.9.2.7. The access control system shall have a comprehensive battery management reporting system to allow for the viewing of the battery status of any locking device in the system at any time.

2.9.2.8. The locking devices themselves shall provide, upon activation by a credential or other means, a distinguishable and audible signal when any battery is reduced to its last 1,000 usable cycles.

2.9.2.9. The system shall support more than 500 wireless locksets; each UNC-100 or UNC-500 controller configuration shall be rated for the number of locksets it can support.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.9.2.10. Once a lockset is installed and registered with the controller, it appears in the security application as a traditional access point, which can be enabled and configured to work with the controller.

2.9.3. When a wireless lockset connects to the controller, it shall report its designation number.

2.9.4. All locksets connected to the system shall be treated as an online lockset and assigned the Default (Online) lockset profile.

2.9.5. Locksets can be assigned to locations.

2.9.6. Locksets can be added and managed in floor plans.

2.9.7. Locksets can be unlocked momentarily via event actions or from the system through the workstations including floor plan view, web browser client, or mobile app.

2.9.8. Activity associated with a lockset can be viewed in real time in the Activity Log.

3. Installation

3.1. The Contractor shall install all system components in accordance with the manufacturer's instructions, and shall furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified and shown. Power, control, signal and communications, and data transmission lines plus all required grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation. Mounting hardware shall be provided as required.

3.2. All products, software, programming tools, etc. shall be registered to The Owner and will be surrendered upon successful completion of the project.

3.3. All low voltage wiring outside the control console, cabinets, boxes, and similar enclosures, shall be plenum rated where required by code. Cable shall not be pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes, or similar fittings with other building wiring.

3.4. All inputs shall be protected against surges induced on device wiring. Outputs shall be protected against surges induced on control and device wiring installed outdoors. All communications equipment shall be protected against surges induced on any communications circuit. All cables and conductors, except fibre optics, which serve as communications circuits from security console to field equipment, and between field equipment, shall have surge protection circuits installed at each end.

3.5. No wiring or cabling shall be exposed; all wiring and cabling must be fully enclosed in threaded metallic conduit, which shall be installed underground, in walls or metal structures unless physically impossible. Any conduit that is exposed shall be fully enclosed within an expanded metal protective cage that is vandal resistant and is equipped with a tamper alarm. All equipment mounting is to be such that the equipment cannot be removed or tampered.

END OF SECTION

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515