Architectural and Engineering Specification for

Access Control Solution

Senstar Symphony™ AC

This document is intended to provide performance specifications and operational requirements for the Senstar Symphony Access Control (AC) software. It is written in a generic format. These specifications may be copied verbatim to form a generic procurement specification.

PART 1 GENERAL

1.1 System Summary

A. The contractor shall install an Access Control Solution (ACS) that provides access control, alarm monitoring, graphical map or floor plan overlays, and security control functions.

1.2 Intent

A. It is the intent of this specification to identify a complete ACS for facility access and egress, alarm monitoring, facility control, and interoperation with other specified products with capabilities as indicated.

B. The purpose of this specification is to identify the required ACS features, capabilities and functions. It is understood that terminology, system architecture, and application design can vary between system manufacturers. However, the design defined in this document is preferred. Any exceptions shall be viewed as non-compliant.

C. It is expected that the majority of the features requested will be provided in the manufacturer's standard product offering. Bespoke systems or those requiring extensive modifications shall be viewed as non-compliant.

1.3 References

The following acronyms and abbreviations are used in this document:

- ACS: Access Control Solution
- IP: Internet Protocol
- LAN: Local Area Network
- LED: Light Emitting Diode
- NFC: Near Field Communication
- ODBC: Open Database Connectivity
- OSDP: Open Supervised Device Protocol
- PIDS: Perimeter Intrusion Detection System
- REX: Request to Exit
- SMTP: Simple Mail Transport Protocol
- UPS: Uninterruptible Power Supply
- VMS: Video Management Software

PART 2 PRODUCTS

2.1 Access Control Solution

A. The contractor shall supply an IP-based Access Control Solution (ACS).

B. The ACS shall be used to provide scalable access control, alarm monitoring, graphical map/floor plan overlays, and security control functions.

C. The ACS shall support integration with Senstar Symphony Video Management Software (VMS), designed by Senstar Corporation.

D. Unless otherwise noted, the contractor shall provide all materials, equipment, hardware, software, modules, accessories, and other options required to deliver a complete turnkey solution.

2.2 Manufacturers

A. The Senstar Symphony Access Control software from Senstar Corporation (www.senstar.com) meets the software-specific requirements stated in this document.

2.3 System Architecture

A. The ACS shall have an Open Database Connectivity (ODBC) compliant design that facilitates the sharing of data with external databases and the integration of the HID® Aero™ Controllers

B. Operating system:

1. The ACS shall run as a native application on a current version of the Microsoft Windows operating system and support its updates, patches, and hot fixes.

2. The ACS shall be able to work in a virtual server environment such as VMWare or Microsoft Hyper-V.

C. Database:

1. The ACS shall make use Microsoft databases such as Microsoft Access, Microsoft SQL Express, or Microsoft SQL Server.

2. The database shall be ‘Open Database Connectivity’ (ODBC) compliant to facilitate the sharing of data with external databases and the integration of a wide range of security hardware.

3. The ACS shall have the ability to import and export personnel information based on time schedules, TCP commands, and file date/time modification.

4. Import capabilities shall include:

a. The ability to import access control data including personnel, hardware, and time schedules to be used for system takeovers.

b. The ability to import using an ‘Open Database Connectivity’ (ODBC), Text or CSV file.

D. Main system components:

1. Field panels shall be used to support access control, alarm monitoring and facility control (relay output control) functions within the defined facility or facilities.
2. Intelligent system controller(s) shall:
    a. Serve as a distributed database management controller linking device sub-control modules, which connect to card readers, monitor point inputs, and system outputs.
    b. Support multiple device sub-controllers on an IEEE standard RS-485 parallel network, as shown in the drawings and defined herein.
    c. Support on-board access readers and control terminations, allowing the controller and readers to be managed with local on-board operational intelligence.
3. An IP-centric intelligent controller shall be used to support access control, and facility control (relay output control) functions within the defined facility or facilities as specified. The IP-centric intelligent controller shall:
    a. Support multi-class credential technology utilizing the same footprint as a traditional reader.
    b. Provide a complete and full-featured access control hardware and software infrastructure utilizing contactless smart card capability and Mobile Access via native Bluetooth or Near Field Communication (NFC) capability.
    c. Provide a complete and fully featured hardware and firmware infrastructure for access control, with the option to communicate via TCP/IP protocol over 10/100 Mbps Ethernet or the Internet.
    d. Provide up to 500mA of power to the reader.
    e. Not require sub-controllers to provide distributed intelligence for up to two access points, including I/O portal management and supervision.
    f. Contain on-board flash memory for program updates. Updates shall be downloadable from over the network.
    g. Be a UL294-listed component.
4. ACS server and workstation computers:
    a. The ACS server and operator workstations shall use industry standard computer hardware (PC) running a physical or virtual Microsoft Windows operating system.
    b. The ACS server shall provide centralized security control, alarm and event monitoring and response, as well as database configuration and management for all intelligent controllers and associated sub-controllers within the user's facility or facilities as specified.

c. The ACS server and operator workstations shall serve as the user interface to the ACS and be used for programming, administration, and monitoring functions.

2.4 Intelligent Controller

A. An intelligent controller shall be a field panel that provides local processing and control of all access control, alarm monitoring, and auxiliary control functions. intelligent controllers shall typically be located within equipment closets throughout the user's site or sites.

B. The term "intelligent controller' shall mean the manufacturers specific combination of control equipment necessary to provide the functions and capabilities of an "intelligent controller' as specified herein. This control equipment may include, but is not limited to, processing boards, card reader boards, input boards, output boards, communication boards, power supplies and other such equipment and accessories specific to the manufacturer's hardware architecture.

C. The intelligent controller shall provide full-featured card access control processing without requiring communication with the ACS server and shall operate in a fully distributed manner. All data necessary for card processing shall be stored within its internal memory. Communication with the ACS server shall not be required to process card access requests or other assigned control functions.

D. The intelligent controller Operating System, firmware, application program, and database shall be stored in solid-state memory media. The intelligent controller shall not use any type of disk drive (hard drive, floppy drive, CD, or optical drive) to support normal operations.

E. The application firmware embedded in the intelligent controller shall be field-upgradeable to permit system enhancements to be made as they become available from the manufacturer. The firmware provided in the intelligent controller shall be the latest version released by the manufacturer at the time of installation and certified by the ACS to be compatible.

F. The ACS shall support a means to download firmware upgrades as a standard and shall not be dependent on the manufacturer or site integrator to maintain firmware for the intelligent controllers.

G. Intelligent controllers shall be equipped with an integrated real-time clock. Intelligent controllers shall be capable of processing timed control functions (such as automatic unlock) without requiring communication with the ACS server.

H. Intelligent controllers shall be capable of processing local alarm input/output events (such as operation of local audible alarm horn when a monitored point is activated) without requiring communication with the ACS server. The intelligent controllers shall be capable of communicating to the ACS using the following methods:

1. IP Server – Configured on the intelligent controller and enables the ACS to poll the controllers over the TCP/IP network. A native implementation of TCP/IP, where the intelligent controller is directly connected to the network, is preferred.

2. IP Client – Configured on the intelligent controller and enables the user to specify the primary host ACS to send/receive information.

I. Intelligent controllers shall provide the capacity to control a minimum of one door and be expandable in increments of up to 64 doors, based on the type of intelligent controller selection for specified tasks.

J. Each door defined and managed by an intelligent controller shall be configured with one card reader input (supporting up to 2 readers), one SPDT (Form C) lock output, one supervised door switch input for door position detection (forced or held-open monitoring), and one request-to-exit (REX) input.

K. The intelligent controller shall have a memory capacity of not less than 10,000 access cards, with selected processor expandable to a maximum of 1,000,000 cards.

L. The intelligent controller shall permit access of cards not in local memory upon validation of access request by ACS server and save the card information to local memory once authorized by the ACS server.

M. The intelligent controller shall rapidly process all local access control transactions. The time between presentation of a valid card at card reader until the time that door unlocks shall not exceed 1 second under worst-case conditions.

N. The intelligent controller shall link with sub-controller modules for access reader control, input monitor points and outputs and should be available in the following hardware configuration:

1. The Intelligent controllers shall be designed as a master processor with host and sub-controller communication ports, supporting IP host communication and shall perform as the central database controller for all defined sub-controller modules.

2. The Intelligent controller shall support multiple RS-485 ports for down-line sub-controller communication and allow for connection and control of a minimum of 64 sub-controllers. The sub-controllers are:

a. Dual door sub-controller with I/O and reader termination for two doors, including 7 additional supervised inputs and 4 additional supervised relay outputs

b. Keypad display terminal with reader termination input module, supporting 16 supervised, computer configurable end-of-line, input points with 2 relay controllable outputs

c. Output module supporting 12 relay controllable outputs with 2 supervised inputs

O. The intelligent controller shall utilize an industry-standard Wiegand and OSDP protocol to connect with the specified card readers, permitting the use of multiple reader technologies and other data collection devices. Intelligent controllers that rely exclusively on proprietary card reader protocols that require use of a specific manufacturer's card reader or input device shall be viewed as non-compliant.

P. The intelligent controller shall support the use of varying card/credential bit lengths from 26 to 75 bits, with the ability to support a larger number if required.

Q. Based on the reader technology selected, the intelligent controller shall allow the user to present or insert a card at a reader and the ACS, if the format of the card is stored in a System level library, shall identify the format and list specific detail allowing the user to define the card format in the Intelligent Control for site use.

R. The ACS shall display all access requests with descriptions to assist a user in defining a card format into the ACS or selecting existing formats from a pre-defined library of formats, Wiegand and mag-stripe.

S. The Intelligent controller shall allow a maximum of 8 card formats to be stored locally for user assignment.

T. The intelligent controller shall be provided with a power supply with standby battery. Battery shall be sized to provide a minimum of eight hours of full standby operation in the event of primary power failure. The intelligent controller shall report loss of primary AC power to ACS server within 10 minutes of power failure. Power supply shall be Underwriters Laboratories (UL) listed. The power supply may be part of the intelligent controller or be furnished within a separate enclosure.

U. In the event of communications failure to the ACS server, the intelligent controller shall store access control and alarm monitoring transactions in a memory buffer. The minimum size of memory buffer shall be 50,000 transactions. When communication is restored, the intelligent controller shall automatically upload the stored transactions to ACS server.

V. The intelligent controller shall be capable of operating in a temperature range of from 0 to +70 °C (32 to 158 °F) with relative, non-condensing humidity of 5% to 85%.

2.5 Interface to Intercom System

A. The ACS shall provide a software level integration to the security intercom System specified herein. As a minimum, the intercom interface shall provide the following functions:

1. Automatic selection of a specific substation upon receipt of command from Physical Security Management System.
2. Allow activation of a “virtual” monitor point when intercom sub-station call button is pressed, to allow initiation of camera call-ups and other events.
3. Provide an operator interaction as defined by the user for events / alarms generated through the intercom System. This interaction shall be the same as any alarm response structured by the user for operator response.

2.6 Software Licensing

A. The ACS shall follow a flexible, per-door strike licensing model in which additional devices can be added to the system on a per-door strike license basis, without the need to purchase a group of licenses or other type of license.

B. All licenses shall be bound to the server, not individual devices or device controllers. Replacing a door strike or other device shall not require a new license to be purchased.

C. Operator workstations shall not require a license and shall be available on an unlimited basis for licensed systems.

D. There shall be no cost for mobile devices connected to the ACS.

2.7 Software User Interface

A. General requirements:

1. The ACS shall be designed for use by non-technical personnel who have been assigned responsibility for managing the ACS. For the purposes of this document, the term “operator” shall mean any person or employee who has responsibility for managing or operating the ACS.
2. System shall allow authorized operators to define and modify system operating parameters, such as cardholder records, doors, time codes, monitor points, and alarm conditions.
3. Operator workstations shall connect to the ACS server using the TCP/IP Ethernet protocol.
4. The use of a personal computer as an operator workstation shall not prevent other application software such as word processors, spreadsheets, and email programs from being used on the same computer.
5. The ACS shall be multi-user, multi-tasking, allowing the simultaneous use of multiple operator workstations. The ACS shall allow any number of operator workstations to be in use at the same time.

B. Language support:

1. The ACS software shall support the following languages: English, French, Portuguese, Spanish, Italian, German, Arabic and Chinese.
2. A trained dealer or integrator shall be able to customize the language by editing a text-based localization file.
3. The language used in the ACS software shall be operator-specific – logging in to a workstation shall automatically display appropriate language based on user account preference.

C. Graphical features:

1. The ACS software shall provide a standard Windows-style graphical user interface that makes extensive use of graphical elements such as toolbars, icons, and pull-down list boxes. System commands and functions shall be available by using a mouse-type pointing device.
2. Text-based systems which require the entry of commands on a command line shall be viewed as non-compliant.

3. All ACS software functions shall be available using the graphical user interface. It shall not be necessary to 'shell-out' of the graphical user interface to execute any system command. It shall be possible to access the system control panel from within the application and return to the application without minimizing any active system windows.
4. The ACS software shall offer the ability to add up to 34 custom command buttons (soft buttons) allowing the operator to click on the button to execute complex pre-configured commands. Said command buttons must have the capability of being password protected. The command buttons shall have the capability of being partitioned by profile allowing only those profiles designated to view and control only those command buttons.

D. Operator restrictions:

1. Access to any ACS workstation shall require an operator username and password.
2. The ACS software shall by default allow for a minimum of 50 individual operator accounts.
3. Adding an operator shall require an elevated, administrator-level permission.
4. Operator passwords shall be stored in encrypted form and shall be hidden except from the highest-level user. The ACS shall allow use of strong passwords which includes uppercase and lowercase letters as well as numerals and special character within passwords.
5. The ACS shall include the ability to utilize either ACS software authentication or Windows Authentication with the ability to integrate to LDAP. Windows and LDAP Authentication provides the basis for Single-Sign-In.
6. System shall provide multiple system operator profiles, each allowing a different degree of privilege, as configured by the user. Adding a profile shall require elevated administrator rights. The ACS shall provide no less than 50 User IDs with the ability to assign unique passwords and operator roles as a default. The total number of operator profiles shall be user defined. An operator profile shall allow various groupings of commands and System functions to allow access to those System commands and functions as determined by their password profiles.
7. Operator Profiles shall require the following data and set of permissions that will be assigned to each operator:
    a. General:
        1. Profile name
        2. Start-up screen
        3. Language
        4. Auto alarm call up
        5. Alarm manager administration

b. Options:

1. Log-on password (password required to log-on)
2. Log-off password (password required to log-off)

8. Controller Groups: Allow an administrator to assign or deny access by an operator to any System Controller Group. The ACS shall include the ability to conceal such items as system messaging, personnel records, access levels and hardware utilizing System Controller Groups.
9. Properties: Each application module shall allow administrative selection for operator access, view, add, change, delete and commands. At a minimum the administrator shall have the ability to set operator profile conditional access for the following system functions: access control, access levels; time schedules, secured areas, point status monitoring and commands, event management, alarm management, conditional commands (triggers and macros), custom commands, graphics, system settings, system utilities; personnel information including the ability to assign field level permissions of no access, read/write, read only, and mask field.
10. All system functions shall be available at any operator workstation provided that the operator has the correct role. The ACS shall not require that system functions be segregated by workstation, that is, there should be no distinction between an administration workstation, alarm monitoring workstation or enrollment workstation once configured.

2.8 Access Control Features

A. The ACS shall provide card access control of doors, gates, elevators, and other portal control locations as defined herein.

B. All card readers shall read the credential information programmed in access cards as well as Mobile IDs through Bluetooth and NFC presented to a reader and pass verified information through an intelligent control processor for authorization. The intelligent controller shall maintain all card information locally and verify reader information received against stored System operator-specified criteria.

1. If a card's programmed information meets the stored criteria in the intelligent controller then a return signal will be sent to unlock the electrically controlled door and initiate an Access Granted condition message to the ACS for operator notice. Using local on-board reader terminations will allow programmed information to manage access with or without sub-controller modules.
2. If card information does not meet operator-specified criteria, the intelligent controller shall initiate an Access Denied alarm condition message including a descriptive event message detailing reason for the Access Denied condition to the central System for operator response. The descriptive "Access Denied" event message may include but is not limited to "Access Denied: Level", "Access Denied: Time", and "Access Denied: Card".

C. Additionally, the ACS shall support multiple different biometric readers that may or may not be used in conjunction with an access card credential. These shall include but not be limited to fingerprint, face recognition, iris identification, and voice/hand geometry. These shall be supported via either dedicated servers or via the system controllers depending on where the template(s) are stored.

D. Each access portal shall be provided with a card reader and linked to either a sub-controller module interface or directly linked to an intelligent controller module interface with on-board reader port(s). Each sub-controller module interface or intelligent controller module interface with on-board reader port(s) shall provide a contact output for each card reader used to unlock electric door locks and/or other devices. The output from a sub-controller module interface or intelligent controller module interface with on-board reader port(s) shall provide a normally-open and normally-closed contact configuration. Output time shall be operator-definable and capable of being adjusted from 1 to a minimum of 60 seconds for each access output. The combination of card reader and output shall be defined as a door or portal. The ACS software shall be designed to support up to 2,048 doors with no change to the user interfaces. Systems that require re-training when expanded or change the basic system software interface shall be viewed as non-compliant.

E. The ACS shall include door held and door forced conditions with configurable door held times up to 2048 seconds. The ACS shall be configurable to allow for masking of door forced and door held conditions. The ACS shall include the ability to configure an unlimited access grant time to be used in conjunction with Extended Grant Time Settings (American Disability Act mode). The Extended Grant Time Settings shall be configurable per portal or reader and card holder.

F. The ACS shall include the ability to configure a door de-bounce time up to 15 seconds. The ACS shall contain the ability to assign up to 8 door reader modes including: disabled, unlocked, locked (no access, allow REX), correct facility code required, card only, pin only, card and pin, card or pin for use with the intelligent controller platforms. The ACS shall contain the ability to assign up to four (4) door reader modes including: unlocked, card only, card and pin, pin only for use with HID® Aero™ platforms.

G. The ACS shall include the ability to configure the offline reader modes to include: no offline mode, locked down (no access, no REX), unlocked, no access allow REX, correct facility code required for use with the Aero™ platforms. The ACS shall allow for correct facility required as the offline reader mode for use with HID® Aero™ platforms.

H. The ACS shall allow for customizable alarm messages to annunciate on a pre-defined alarm condition. The ACS shall allow for customizable alarm multimedia files on a pre-defined alarm condition. The ACS shall allow for configurable maximum cardholders per intelligent controller and shall also allow for configurable maximum events per intelligent controller.

I. The ACS shall include the ability to view and configure all drivers, intelligent controllers, sub-controllers, devices, readers from a hierarchical tree structure with a uniquely assigned addressing schema. The ACS shall contain the ability to view

real-time status and date/time of the intelligent controller. The ACS shall contain the ability to view real-time status of inputs, outputs and reader modes. The ACS shall have a viewable loaded card count on a per controller basis. The ACS shall have the ability to control hardware devices from the hierarchical tree with unique hardware addressing down to the device level. The ACS shall have the ability to sort the hierarchical tree alphabetically or numerically, the sort order shall follow the hardware properties throughout the software.

J. The ACS shall provide the capability for an authorized operator to assign an alphanumeric description (name) to each hardware hierarchical device. Description name fields shall allow for a maximum of 50 alphanumeric characters. The Description name field shall be used on System menus, displays and reports.

K. The ACS shall support up to 500 regionalized access levels per controller group with up to 1000 controller groups. The ACS shall support the ability to assign alphanumeric characters to each access level. The Access Level name shall allow a maximum of 50 alphanumeric characters. The ACS shall allow for Access Control Reader Groups or individual readers to be added to access levels using a drag and drop method or selection by menu. The ACS shall allow for pre-defined time schedules to be associated with an individual reader or access control reader group. The ACS shall allow for a reader or access control reader group to be added to more than one access level with a different time schedule.

L. The ACS shall support 'Access Control Reader Groups', defined as a placeholder/folder to store one or more Readers. An Access Control Reader Group shall be an operator specified combination of one or more portals or doors associated to a time schedule. The ACS shall allow the assignment of portals or doors to the Access Control Reader Groups with a drag and drop function or maybe added from a menu selection. The ACS shall allow an operator to define Access Control Reader Groups as required without limiting System expansion.

M. The ACS shall support 'Elevator Assigned Floor Groups'. Elevator Assigned Floor Groups shall be an operator specified combination of one or more portals or readers associated to an access level and time schedule that have been pre-defined with an elevator assignment.

N. The ACS shall provide the capability for an operator to assign an alphanumeric name to each Access Control Reader Group. Access Group name shall allow for a maximum of 50 alphanumeric characters. The Access Group name shall be used on System menus, displays and reports.

2.9 Anti-Passback Feature

A. The ACS shall support deployments where card readers are used for both entrance and egress and shall allow each card reader to be operator-defined as either an 'entry or 'exit reader'. The ACS shall require cardholders using a card at an 'entry' reader to subsequently use the card at an 'exit' reader before the card can once again be used at an 'entry' reader, creating an Anti-Passback (or APB) condition. Cardholders attempting to use cards without first exiting the Anti-Passback area shall be denied access and shall cause a 'Passback Violation' message to be sent to

the central System for operator notice. If so configured, Passback Violations shall create an Alarm Condition causing an immediate report generated for operator alarm response.

B. The ACS shall provide a Passback 'forgive' feature that can be activated by an authorized operator. The Passback forgive feature shall reset the Passback status of any card to a neutral condition (neither 'in' or 'out' of the anti-Passback area), allowing the Passback sequence to be restarted.

C. The ACS shall allow the Anti-Passback feature to be enabled and disabled upon authorized operator command,

D. The ACS shall allow the APB mode to automatically be "reset" by a Time Code without the need to use an "exit" reader.

E. A special Anti-Passback set flag shall be provided in the access control personnel record file that allows and authorized operator to specify a cardholder as Anti-Passback exempt. If a cardholder has the Anti-Passback exempt flag set, they may enter or egress any Anti-Passback area without causing an Anti-Passback event or alarm.

F. The ACS shall allow Anti-Passback by time such that a reader may not be used again before a pre-configured window of time has elapsed. This shall be supported on Aero™ based controller hardware.

G. The ACS shall support "Nested Anti-Passback" such that readers may be used to require a user to enter and leave an area within a certain time frame. This shall be supported on Aero™ based controller hardware

2.10 Elevator Control Feature

A. The ACS shall support elevator access control based on user controller group requirements and configuration. The supported access controller for Elevator Control shall ONLY be Aero™ controllers. The configuration shall be such that a Reader can support up to 128 Floors. The actual number of cars and floor selection outputs shall be user configurable. The ACS shall provide for the following elevator access control features, elevator call and elevator floor select for individual or a group of elevator cars:

1. Elevator call shall be an operator command or a time scheduled condition that electronically bypasses the normal use of an elevator call button at secured or unsecured floors.

2. During a command or time scheduled event the normal elevator call button conditioning shall be replaced with an access reader-controlled output. If any cardholder presenting his or her card to such a reader is authorized a sub-controller output shall activate the elevator call button to that floor

3. Elevator floor select shall be an operator specific configuration of card readers and outputs designed to allow authorized cardholders to enter an elevator and access only floors they have been pre-defined to access by a System operator. Elevator floor access selection replaces the normal elevator select push

buttons inside the elevator car. To operate an access elevator car, a cardholder must present his or her access card to a card reader located inside the elevator car. The ACS shall respond to a valid access by activating outputs which temporarily enable the floor selection buttons for those floors to which the cardholder is authorized.

B. The ACS shall allow outputs from elevator car floor selection buttons to be connected as monitor point inputs to the ACS to identify which floor was selected by each cardholder. Once a floor is selected the Aero™ controller shall automatically reset all requests until another authorized cardholder selects another floor.

C. The elevator control feature shall provide a fully distributed functionality allowing managing access requests and activating floor selections, even when an intelligent controller is offline with regards to ACS server connectivity. The ACS shall not rely on the ACS server to provide elevator control functions. Systems that use a central computer for elevator control decisions shall be viewed as non-compliant.

2.11 Digital Keypad Features

A. The ACS shall provide two specific keypad control features, keypad for access control and display keypad for secure area access and management.

B. In access control application, the ACS shall permit the use of digital keypads as an alternate or supplemental access control devices. Keypads shall provide no fewer than twelve numeric keys. Operation of digital keypad shall require the entry of a valid Personal Identity Number (PIN). The PIN for each user shall be unique and definable by operator. These keypads may use fixed numeric keypads or scrambled keypads.

C. PIN Keypads shall be capable of different mode assignments with access control readers. An operator may change a PIN keypad mode by command or automatically by a pre-set time of day.

D. When in PIN Only Mode, entry of valid PIN number shall permit access. Use of an access card shall not be required in PIN Only Mode.

E. When in PIN Plus Card Mode, the entry of valid PIN number, plus use of valid access card shall be required to permit access. Use of access a card alone or use of a PIN number alone shall not permit access when in PIN Plus Card Mode.

F. When in Card Only Mode, the ACS will disable the PIN Keypad, allowing use of a valid access card alone.

G. In the alarm access applications, the ACS shall permit the use of digital keypads as an arm or disarm alarm access device as well as a user keypad command station. Alarm access Keypads shall provide no fewer than sixteen numeric and static keys with a two level 16-character LCD display for local user interaction and status. Operation of digital keypad shall require the entry of a valid Personal Identity Number (PIN) or valid commands by the user. The PIN for each user shall be definable by an authorized operator.

H. Alarm access keypads shall allow an operator to configure secured areas and allow local users to 'Open and Close' secured areas based on pre-configured conditions. Open early, Open late, Close early and Close late. Alarm access keypad use shall allow the user to integrate alarm and access into a single integrated reporting and response System.

I. Alarm access keypads shall allow an operator to configure local controls to allow authorized users to active commands as well as Open /Close management. The ACS shall allow keypad commands to control any operator specified devices and controls by command code. Conditions such as open, close, lock, unlock, mask, un-mask, activate and de-activate shall all be assignable commands to a secured keypad area. Status and arm / disarm locations shall be displayed on the keypad LCD for pre-authorized users.

2.12 Definition of Access Privileges

A. The ACS shall use a flexible, modular method of defining "who, where and when" with regards to cardholder authorization to access or egress secured locations within a defined site.

B. As a cardholder is entered into the database the ACS shall automatically build a record and allow an authorized operator to assign access privileges. 'Who' shall be defined as the ACS defined cardholder.

C. Assigning an 'Access Level' to a cardholder record defines where and at what time (or when) that cardholder is permitted access within the facility or facilities.

D. The ACS shall allow multiple Access Levels consisting of a combination of Access Control Reader Groups, Temporary Access levels and General Access levels. The ACS shall allow for Time Schedules to be assigned to Access Levels in combination with Access Control Reader group(s).

E. The ACS shall allow for an automatic Temporary Access start and stop dates to be configured.

F. Assigning a 'Time Schedule' to readers and cardholders defines 'when' a cardholder will have access within the facility or facilities.

G. A Time Schedule shall be operator-specified combinations of Time Intervals and Days of the Week used to specify times that a card may be used to gain access throughout a facility or facilities. Each Time Schedule shall allow not less than twelve individual Time Intervals for each day of week for the Aero™ hardware. Holidays shall have multiple Time Intervals scheduled as well. The ACS shall allow for Holiday Time Schedule overrides by time schedule and interval.

H. Cardholder records, Access Levels and Time Schedules shall be definable by authorized System operators. To configure a Time Schedule the user shall select days of the week and hours of the day that will make up each Time Schedule. Time Schedules shall also have 'Time Interval'. A 'Time Interval' shall be defined as a range of times that can be contained within a 24-hour day. (An example of a Time Interval would be: 00:00 - 22:00 and 22:15 – 23:59 / 12:00 AM – 10:00 PM and 10:15P M – Midnight). Time intervals shall maintain a precision of one minute (60

seconds) or less. The ACS shall allow an authorized operator to define as many Time Intervals as required by the installation with a maximum of twelve 'Time Intervals' per day for the Aero™ hardware. Time Intervals shall have the ability to be changed using a drag and drop graphic or by typing in the numeric time value.

I. A 'Holiday' shall be an operator-specified date treated by the ACS as a Holiday. A Holiday is defined as a single or multiple consecutive-day occurrence. On dates defined as a Holiday, the ACS shall use the time criteria specified for Holidays by a System operator. The ACS shall allow a System operator to specify Holidays as required by the site. The ACS shall provide for up to 8 holidays per time schedule. Systems that do not support 8 holidays per time schedule shall be viewed as Non-Compliant.

J. The ACS shall allow an authorized operator to assign an alphanumeric name to each Access Level, Time Schedule and Holiday. These names shall allow for a maximum of 50 alphanumeric characters. These names shall be used on System menus and reports.

K. The ACS shall allow an operator to establish an 'Activation Date' for each cardholder / card. The Activation Date shall be the date that access privileges associated with that cardholder / card shall take effect.

L. The ACS shall allow an unlimited number of cards to be assigned to a single cardholder/record

M. Cardholders attempting to use an access card before the Effective Date shall cause an Access Denied Time event condition message at the central System for operator response.

N. System shall allow the operator to establish a 'Deactivation Date' for each cardholder / card.

O. The Deactivation Date shall be the date that access privileges associated with that cardholder / card shall be denied upon usage of that card. Cardholders attempting to use an access card after the Expiration Date shall cause an Access Denied Time event condition message at the central System for operator response.

P. The ACS shall support vacation start and stop dates to temporarily deactivate a cardholder card while they are listed as being on vacation and away from their normal work area. Systems that do not have and automated vacation set shall be viewed as Non-Compliant.

Q. The ACS shall support a temporary access level assignment selection with automated start and stop dates. This allows an administrator or authorized operator to assign additional access rights to an individual for a specific number of day and automatically cancel the exception. Systems that do not have an automated temporary access level assignment set shall be viewed as Non-Compliant.

R. The ACS shall allow for the automatic deactivation of cardholder records if the card has not been used within the designated "Days of Non-Use before Card Deactivation" value. This value is shall be configurable by the operator. This feature shall have the ability to be disabled if the operator so decides.

S. The ACS shall support multiple world time zones such that a system that crosses time zones will report the local time based on its local server time rather than the "host".

2.13 Cardholder Records

A. The ACS shall provide a 'Cardholder Record' to store data for each cardholder in the system. The ACS shall provide capacity for as many records as required by the operator.

B. The ACS shall provide data entry screen (form) allowing the creation, editing and deleting of Cardholder Records. The Cardholder Record shall contain the following fields and functions as a minimum:

1. Lock/unlock records from/for operator editing.
2. ADD a new card record
3. COPY an existing card record.
4. Save a record or data entered.
5. Delete a record.
6. Perform group edits and allow for Card Templates to be created allowing for predefined values to be assigned automatically to any card record assigned the Card Template. The Card Templates shall have permissions assigned by profile. The Card Templates shall automatically update any records with any values modified in the Card Template.
7. Print Personnel reports
8. Download all or selected database changes to the effected Controllers.
9. Display online help on pertaining to the software

C. Each Cardholder Record shall include support for the following general access control fields:

1. Enable/Disable Flag: Shall be used to activate / suspend card access to a record by an operator without deleting the cardholder record.
2. Card Record Count: The ACS shall display a filtered and actual card record count allowing an operator to move up and down records using an ascending and descending slide in left-hand side navigation window
3. First Name: Shall show 1 to 50 alphanumeric characters, first name field.
4. Initial Field: Shall show 1 alphanumeric character, initial field.
5. Last Name: Shall show 1 to 50 alphanumeric characters, last name field.
6. Card Template: The ACS shall support pre-defined data entry forms (ie, templates) and allow for each record to be assigned to one. This feature shall allow the operator to pre-define data fields shared amongst cardholders with similar roles, thus reducing error and data entry time.

7. Card Number: 1 to 12-digit number assigned to the card. Cardholder number entry shall support an automated entry of card number thru use of an Enrollment Reader or manual number entry. The ACS shall support an unlimited number of cards assigned to each record/cardholder. The card number shall contain information on:
    a. Card number
    b. Status: Active/Lost/Returned/Deactivated/Terminated
    c. Activation Date: Shall show the date when access privileges are to begin.
    d. De-activation Date: Shall show the date when access privileges are to expire.
    e. Card Format type: Shall display a dropdown list to identify the type of card issued
    f. Facility Code: Shall display a text field to input the facility code value of the card
    g. Card Re-Issue Code: Last card issued count. The ACS shall support a card issue count for each card re-issued to a cardholder.
    h. Hot Stamp Number: Shall show 1 to 12 numbers only.
    i. PIN Number: Shall show 4 to 8 digits user defined Personal Identification Number, if used.
    j. Vehicle ID: Shall show a text field to store auxiliary information such as Vehicle ID or License Plate
    k. Last Modified: Shall be used to show last modification data and log-on operator.
    l. Access Levels window: Shall provide a simple way for operators to assign door access t based on Access Levels and Access Group Reader Groups. Show all Controller Groups, access levels and groups associated with the cardholder record.

D. Each Cardholder Record shall include support for the following employee info fields:
    a. Company: Shall provide a dropdown list of “Company” name using 1 to 48 alphanumeric characters. This field is can be customized
    b. Department: Shall provide a dropdown list of “Department” name using 1 to 48 alphanumeric characters. This field is can be customized
    c. Title: Shall provide a dropdown list of “Title” name using 1 to 48 alphanumeric characters. This field is can be customized.
    d. Social Security#: Shall provide a textbox to store Employee Social Security numbers. This field shall be customizable and renamed if required to provide another unique ID number if so desired

e. Employee#: Shall provide a textbox to store Company employee number 1 to 20 alphanumeric characters. This field is can be customized.

f. Email Address: Shall provide a textbox to store 1 to 40 alphanumeric characters. This field is can be customized.

g. Date of Birth: The ACS shall provide a right-click calendar display to select date.

h. Date of Hire: The ACS shall provide a right-click calendar display to select date.

i. Work#: 15 telephone alphanumeric characters

j. Home#: 15 telephone alphanumeric characters

k. Address-1, 2: 2 lines 50 alpha-numeric characters each for address information.

l. Last Print: Shall be used to show the last date the record was printed by an operator.

m. Notes box: Shall provide a text box to allow operators to enter notes. Quick click button will input the timestamp of the note

E. Each Cardholder Record shall include support at least 20 custom data fields, each storing up to 50 alphanumeric characters each.

F. The ACS shall allow for a date/time-stamped notes table in general data entry.

G. Each Cardholder Record shall include support for the following advanced fields:

1. Operator: Allow the cardholder record to be associated/linked to the ACS operator.

2. Card Use Limit: This shall define the number of times the card may be used for access in each time period.

3. Guard Tour Flag: Shall be used to identify the card as a guard tour card.

4. Vacation Start Date: The ACS shall provide a right-click calendar display to select date. Cardholder card shall be suspended from access on this date.

5. Vacation Stop Date: The ACS shall provide a right-click calendar display to select date. Cardholder card shall be re-activated for access on this date.

6. Temporary Access Level Start Date: The ACS shall provide a right-click calendar display to select date. Cardholder shall be assigned the temporary access level on this date.

7. Temporary Access Level Stop Date: The ACS shall provide a right-click calendar display to select date. Cardholder's temporary access shall be removed on this date.

8. Trigger Code 1: The ACS shall allow cardholder to be assigned a Trigger Code value to specifically actuate Triggers for I/O programming

9. Anti-Passback Flag: Shall be used to allow a card access or egress in an anti-passback area without activating an operator notice.
10. Anti-Passback Exempt Flag: Shall be used to allow free access or egress in any anti-passback area without activating an operator notice.
11. ADA (Uses the Extended Grant Time) Flag: Shall be used to set momentary time for ADA persons, extending door lock and held open timers.
12. PIN Exempt Flag: Shall be used to set all cardholder reader access to card only.
13. Do Not Alter Current Anti-Passback Location Flag: Shall be used to hold a current anti-passback status for a cardholder when access is granted.
14. Do Not Alter Current Use Count Flag: Shall be used to hold a current use count on a specific area when access is granted.
15. Watch Window button: Allow operator to view most recent card usage activity for a cardholder
16. Assign Last Used Reader button: Allow operator to manually assign a cardholder their last used reader
17. Personnel Access button: Shall provide operator the ability to view a list of cardholders who should have access to a selected reader

H. The ACS shall use the Cardholder Identification Number as the primary key to uniquely identify the record in the database. The ACS shall permit the use of access card numbers as a key but shall not use access card numbers as the primary key unless defined by an operator.

I. The ACS shall provide a sort list of card holders per Controller Group selected on the Personnel Manager screen. Sort keys shall allow the list to be sorted and displayed for an operator.

J. The ACS shall permit the use of access cards encoded in Wiegand formats of varying bit lengths from 26 bit to 75 bit and MiFare cards and their derivatives (HID®, Legic etc.)

K. Note: Card bit format limitations and constraints are controlled by the field hardware. It shall be the responsibility of the bidder to ensure that the field hardware proposed can meet the standards as set forth in the specification/RFQ.

L. The ACS shall allow up to 10 different access card numbers/credentials to be assigned to each cardholder record. The ACS shall not require that a separate cardholder record be created for each access card number. The ACS shall allow each access card number on the cardholder record to use a separate format. Systems that do not support a minimum of 10 cards per cardholder record shall be viewed as Non-Compliant.

M. The ACS shall permit the creation of a Cardholder Record without requiring that an access card number be assigned. This feature shall allow a Cardholder Record to be created for “PIN Only’ users who will be assigned a PIN number (1 to 8 digits) only and not require an access card.

N. The ACS shall provide a hierarchical tree showing access level assignment for each cardholder in the Cardholder Record. This tree shall permit an authorized operator to list, and select, through 'pop-up and drop-down windows', any access level or access group defined in the ACS. To view access levels and access group shall not require an operator exit from the Cardholder Record screen to perform this function.

O. The ACS shall allow the operator to identify the Access Levels, Access Groups, readers and Time Schedules associated with each cardholder without requiring the operator to exit from the Personnel Manager screen.

P. The ACS shall allow for the automatic disabling of card records based on the configured "Days of Non-Use before Deactivation" value.

Q. The ACS shall allow for the Personnel Manager heading tags to be modified to reflect headings based on the customer's request.

2.14 Automatic Adjustment for Daylight Savings Time

A. The ACS shall provide the ability to automatically adjust the system time to accommodate changes at the beginning and end of Daylight Savings Time. The ACS shall allow the dates associated with Daylight Savings Time to be set by operators in advance.

2.15 Partitioned Database Feature

A. The ACS shall provide the ability to establish multiple 'Logical Views' of the access control system and cardholder database. Each Controller Group shall permit viewing and/or modification of only certain cardholder record fields, access levels, access groups, hardware configuration, and other such data. This capability shall allow the creation of 'Controller Group', logical Sub Systems. The ACS shall allow an authorized operator to create as many Controller Groups as required for a site or multiple sites. Systems that do not support a Controller Group management set shall be viewed as Non-Compliant.

B. Each Controller Group shall have full System capabilities; and shall appear to the operator and operate as if it were an independent access control System. The typical Controller

C. Group may consist of a single building or multiple building; or a single department in multiple buildings, or a single department within a building which houses multiple departments.

D. Creation of sub-Systems shall be accomplished through System configuration and software partitioning of the database.

E. The ACS shall allow operator profiles to view, create, or edit data in only certain Controller Groups. As an example, a operator who is assigned an operator profile for access to Controller Group 1 shall only be able to view and edit database records affecting Region 1. This operator would be restricted from viewing and modifying other portions of the ACS database based on his or her operator profile. An operator profile shall allow the operator to assign one or more Regions for operator access.

F. The ACS shall allow the ability to partition the hardware down to the device level. The ACS shall allow operator profiles to view, create, or edit hardware data for only those devices designated to the Operators profile. Systems without the capability of partitioning hardware at the device level shall be viewed as Non-Compliant.

G. Operator functions, which may be restricted by profile and Controller Group, shall include, as a minimum:

1. Adding, deleting, and modifying cardholder records
2. Locking and unlocking of doors
3. Arming and disarming of secure areas
4. Masking and unmasking of alarms
5. Printing reports
6. Configuration of access levels, time schedules, access groups, and other such system parameters.
7. Establishment of automatic door lock and unlock times.
8. Monitoring of alarm conditions from user defined doors and monitor points.

H. The ACS shall allow the assignment of any door, access group, monitor point, secured area, auxiliary output contact or other system element within a Controller Group.

I. It shall be possible to assign any door, access group, monitor point, secured area, auxiliary output contact or other system element to more than one region at the same time.

J. Operator access to specific Controller Groups shall be determined by the operator's user name and password. The use of Controller Groups shall not prevent authorized system operators from making system-wide changes or generating system-wide reports.

K. As an example, it shall be possible for an authorized system operator to add/delete a cardholder from all sub-systems with a single entry. The ACS shall not require that a separate entry be made to add/delete a cardholder from each Controller Group. Systems that require data add/delete entries in multiple partitions with in the application shall be viewed as non-compliant.

2.16 Interface to External Databases

A. The ACS shall be able to import information from existing data-compliant personnel databases. The purpose of importing this information is to minimize the need to manually enter data.

B. Import capabilities shall include:

1. The ability to import information from the databases for the initial load of the cardholder database; and for major loads of new information periodically.

2. The ability to update the cardholder database based on the import reflecting changes in employee status.
3. Import on updates/changes in the source database shall allow the ACS to automatically add cardholder records, delete cardholder records, modify access privileges, and change other information contained in the cardholder database.
4. The ACS shall allow said import to be scheduled by minute, hour or daily imports.
5. The ACS shall allow the import utility to be configured as a Windows Service.
6. The ACS shall allow import of data from Open Database Connectivity (ODBC), CSV or text files.
7. The ACS shall allow for Human Resource (HR) Integration such as PeopleSoft HCM through the available API/SDK from the HR system for bidirectional updates
    a. New employee/user entered in the HR system will automatically add new record in the ACS thru the HR Integration
    b. Updates to employee/user in HR system will automatically download changes of the record in the ACS thru the HR Integration
    c. Deletion of employee/user in HR system will automatically disable/delete record in the ACS thru the HR Integration
    d. The system shall allow “pre-canned” pictures to be imported thus limiting the amount of re-work time that might otherwise be necessary for personnel data import utilities.
8. The ACS shall allow for direct Windows Active Directory integration in real-time to populate Windows AD accounts into the Symphony Personnel database. Real-time updates to the Symphony database will be triggered by information changes to the AD account on update/edits/status of the AD account

C. The ACS shall not require a System restart or ‘reboot’ in order for data imports or updates to the cardholder record database to take effect — updates shall be made automatically upon receipt of data, if so, configured by the user.

2.17 Door Control Features

A. The ACS shall be capable of unlocking and re-locking Doors and Door Groups upon command from operator workstation. A command shall be capable of being executed by an authorized operator from pull-down menus, icons on status screens, text lines on event screens and icons on Custom Map Displays.

B. The ACS shall automatically disable Door Forced conditions and ‘Door Open / Door Held’ conditions from doors that have been unlocked by an operator command.

C. The ACS shall be capable of automatically unlocking and re-locking Doors and/or groups of Doors based on Time Schedule and Intervals. The ACS shall be capable of

automatically disabling Door Forced conditions and Open-Too-Long conditions for Doors that have been unlocked by Time Schedule and Intervals.

D. The ACS shall provide the capability to selectively disable Doors upon command from designated operator workstations based on operator profile, user name and password. Disabled Doors shall deny access to all cardholders.

2.18 Auxiliary Control Features

A. The ACS shall provide 'Auxiliary Output Contacts' for auxiliary control purposes, such as the unlocking of non-card reader-controlled doors, operation of audible alarm devices, and other such functions. Auxiliary Output Contacts shall be capable of being assigned to Door Groups; and shall be capable of being operated upon command from operator workstations, automatically by Time Schedule and Interval and Triggers and Macros. The ACS shall provide a maximum capacity of 10,000 auxiliary output contacts (or relays).

B. Cardholder trigger codes in a cardholder record shall allow trigger and macro control for command activation and de-activation of auxiliary outputs based on access grant or deny activity. At a minimum; secure areas, macro conditions to lock and unlock locations, mask and un-mask access conditions, alarms, etc., shall be activated or de-activated based on a cardholder trigger code assignment.

C. The ACS shall provide the capability for an operator to assign a unique alphanumeric name to each Auxiliary Output Contact. Auxiliary Output Contact name shall be a maximum of 50 alphanumeric characters. The Auxiliary Output Contact name shall be used on System menus, displays and reports.

2.19 Door Status Monitoring

A. The ACS shall monitor the status of each access-controlled Door to determine if a door is open or closed. If an access-controlled door is opened without the presentation of a valid card, the ACS shall generate a 'Door Forced' condition.

B. The ACS shall support an ADA (American Disabilities ACT) standard whereby a different shunt time can be set for a physically impaired person, so they can access with a longer held open / shunt time than other employees.

C. Where a card reader is provided only on the entry side of a door, the ACS shall allow the disabling of Door Forced monitor from the exit side of the door. Disabling of Door Forced monitor shall be accomplished using a request-to-exit input (REX). A REX input shall be a normally open dry contact input to the ACS, allowing connection of release buttons, motion detectors and other devices.

D. If the ACS is so configured, operation of a REX input shall disable the Door Forced monitor for a operator-specified period, allowing exit without causing a Door Forced condition. If the ACS is so configured, a REX input shall also be capable of unlocking the door. One REX input shall be provided for each access-controlled Door per door controller.

E. The ACS shall provide the capability to remotely disable REX features for each Door. Each REX shall be capable of being disabled automatically by Time Schedule, Triggers and Macros and upon command from an operator workstation.

F. The ACS shall support fully supervised End-Of-Line input circuits which are software programmable by the operator.

G. The ACS shall monitor the status of each access-controlled door to determine length of time a door is open after an authorized access grant. If the door is left open longer than an operator specified time period, the ACS shall generate a 'Door Open / Door Held' condition for operator notice.

H. The Door Open / Door Held timer shall be capable of being set for an operator-selected period of time between 1 to 4000 seconds. The Door Open / Door Held time period shall be individually selectable for each Door.

I. The ACS shall provide the capability to remotely disable the Door Open / Door Held monitoring feature for each Door. Feature shall be capable of being disabled automatically by Time Schedule, Triggers and Macros and upon a command from an operator workstation.

J. Door Forced and Door Open / Door Held conditions shall be immediately processed based on parameters pre-configured by the operator. If so configured, Door Forced and Door Open / Door Held conditions shall create an Alarm Condition; causing an immediate report to be sent to a designated operator workstations through Alarm Manager for alarm acknowledgment; and causing other operator-specified System operations to occur.

K. The system shall support a minimum of three different states for any access control door/portal.

1. Door open
2. Door closed
3. Door closed, locked and secure

L. Any system that does not record the position of the door locking hardware shall be deemed non-compliant.

2.20 Alarm Monitoring Features

A. The ACS shall provide monitoring of contact inputs from door switches, motion detectors, and other sensors located at field locations. Each input shall be defined as an individual 'Monitor Point'. The ACS shall provide the capacity for a maximum of 10,000 Monitor Points.

B. Monitor Point inputs may utilize a supervised circuit requiring the use of an End-Of-Line (EOL) resistor circuit. The ACS shall allow an authorized operator to specify, through the ACS software, the EOL circuit requirements of each individual input.

C. Monitor Point inputs shall accept both normally-open and normally-closed dry contact input signals. Monitor Point inputs shall provide a minimum of three distinct

states, including ‘normal’ (input is in normal or inactive condition), ‘alarm’ (input is in alarm or active condition), and ‘trouble’ (input is in fault or tamper condition).

D. Each Monitor Point shall be identified on System displays by a unique Monitor Point number. In addition, the ACS shall provide the capability for the operator to assign an alphanumeric name to each Monitor Point. Monitor Point name shall be a maximum of 50 alphanumeric characters. The Monitor Point name shall be used on System menus, displays and reports.

E. The ACS software shall provide an ‘A Virtual Door Monitoring Feature’. The virtual door monitoring feature shall permit a REX input point to be logically associated in software with a Monitor Point and Auxiliary Output to create a ‘Virtual’ access door. This feature shall allow non-card reader doors to be monitored for both Door Forced and Door Open / Door Held conditions without requiring a card reader or card reader sub-controller.

F. Monitor Points shall be capable of being grouped for the purpose of alarm management. A Secured Area shall be an operator-specified group of Monitor Points.

G. The ACS shall provide the capability for the operator to assign an alphanumeric name to each Secured Area. Secured Area name shall be a maximum of 50 alphanumeric characters. The Secured Area name shall be used on System menus, displays and reports.

H. The ACS shall provide the capability to Arm (enable) and disarm (disable) secured areas by command from operator workstation. Time Schedule and Interval. Arm and Disarm commands shall be capable of being executed from pull-down menus, icons on status screen, through triggers and macros and icons on Custom Map Displays.

I. The ACS Operator shall be able to enable a Monitor Point allowing the Monitor Point to cause an Alarm Condition for operator notice, if point is activated or activates after enabling. The ACS Operator shall be able to disable a Monitor Point allowing the Monitor Point to activate without causing an Alarm Condition for operator notice. Monitor Points shall be capable of being armed and disarmed individually, and by Secured Area.

J. The ACS shall have a capability to automatically Arm and Disarm Monitor Points and Secured Areas by Time Schedule and Interval.

K. Triggers and Macros shall be capable of locking and unlocking any number of access-controlled Doors and Door Groups, change any number of card reader modes, enable and disable any number of Monitor Points and activate and deactivate any number of output points based upon a Monitor Point status change. Triggers and macros shall be operator configurable and shall use any Monitor Point status change, access condition change, keypad commands and/or cardholder trigger codes for conditions of change. Triggers and Macros conditions shall be stored at the controller level and function independently of the host, provided the download to the controllers is completed

L. The ACS shall allow the disassociation of hardware points for use as another device. This option shall be available with the Aero™ controllers only.

2.21 External Control of Secured Areas

A. The ACS shall allow Secured Areas to be Armed and Disarmed using card readers designated as 'Arming Readers'. Presenting a valid access card to an Arming Reader shall toggle Secured Areas from armed state to disarmed state and vice versa.

B. The ACS shall allow Secured Areas to be managed for access into such areas using a 'Keypad Display Terminal'. The ACS shall be capable of managing up to 64 secured areas from a single Keypad Display Terminal or up to 64 secured areas across multiple Keypad Display Terminals.

C. Keypad Display Terminal alarm management shall support secured area Open / Close conditioning, tracking operator defined secured area early and late open and early and late close status for each defined area.

D. The ACS shall allow Secured Areas to be Armed and Disarmed through the use of external hardwired controls (such as a key-operated shunt switch.) The ACS shall permit Monitor Points to be defined as a trigger to run a macro assigned to Arm or Disarm a Secured Area. As an example, when Monitor Point trigger / macros are activated, the Secured Area which it controls shall be disarmed. When a Monitor Point trigger / macro is normal (inactive), the Secured Area which it controls shall be armed.

E. The ACS shall allow Auxiliary Output Contacts to function as Secured Area status outputs. Two types of outputs shall be capable of being defined:

   1. Armed Status Output: Output contact operates when Secured Area is in Armed Condition (typically used for 'armed-status' indicator lights).

   2. Secure Status Output: Output contact operates when all Monitor Points assigned to Secured Area are in normal condition (typically used for 'ready-to-arm status' indicator lights).

2.22 Graphic Maps Displays

A. In addition to other means, the ACS shall be capable of displaying the status of and controlling system devices/elements through the use of Graphic Displays and configurable map levels and icons. Graphics map displays shall be in the form of image files with the ability to provide dynamic zoom levels.

B. A 'Custom Map Display' shall be a multi-color graphic display for operator viewing and interaction at workstations. Custom Map Displays shall be operator-created graphic displays that show maps, site plans, building floor plans, and other graphic representations of the user's facilities.

C. Custom Map Displays shall allow the ability to plot devices such as doors, readers, inputs, outputs using display of symbols (icons) representing Doors, Monitor Points, Auxiliary Output Contacts, Cameras and Secured Area Keypads and other such System elements to be placed on a map level adjacent to rooms, doors and other

building features. Upon change of status, a color bar associated with the symbol / icon shall change color to identify a change of state on the graphic.

D. Custom Map Displays shall allow activation of operator commands such as the locking and unlocking of Doors, arming and disarming of Monitor Points and the operation of Auxiliary Output Contacts. Commands on Custom Map Displays shall be activated by clicking on symbols / icons representing a System element (devices) and then choosing a desired command from a selection window such as (lock, unlock, etc).

E. Custom Map Displays shall be capable of being created using complex graphics shapes including lines, circles, multi-sided polygons, complex curves, filled objects, photos and the like. Custom Map Displays shall be capable of utilizing distinct colors.

F. System shall accept image files such as jpeg, wmf, bitmap and other standards created/edited by graphic software packages, such as MS Visio, Adobe and Gliffy.

G. System shall store maps as .wmf files that will allow “dynamic resizing” (zoom layers) of map displays. “Dynamic resizing” shall allow a map image to be created and stored as a vector-based file. Once created, the image shall be capable of being “zoomed” without loss of detail, allowing a single image to be viewed on screen at a zoomed scale.

H. System shall provide for up to 10 separate layers for plotting on any map. The user shall have the ability to select the layer and plot System device assigned icons as a separate layer on a map, graphic diagram. The layers can be selectable to only display such devices/objects as needed.

I. System shall provide an unlimited number unique Custom Map Displays.

J. System shall allow the ability to group graphic files into folders easier management of files and locations.

2.23 Alarm Display Features

A. Activation of Monitor Point shall be immediately processed by the ACS in accordance with parameters as established by the operator. If so configured, the activation of a Monitor Point shall create an Alarm Condition causing an immediate report to be sent to the Alarm Manager on the operator workstations. Any event/alarm shall be configurable in the Triggers and Macro module to cause other System specified operations to occur. The maximum time period from activation of Monitor Point until Alarm Condition is displayed on the operator workstation shall not exceed 5 seconds.

B. System shall be capable of displaying customizable Operator Instruction. Operator Instruction Displays shall be operator-created text messages per alarm point or based on a typical response message from file. System shall provide a message file for every alarm setup by the administrator or authorized operator.

C. Upon Alarm Condition, the ACS shall sound an audible warning configurable by the operator, display an alarm message on a graph map by the point that activated into an alarm condition on all operators logged on to the ACS with an alarm monitoring

profile. Systems requiring Operator-designated Operator workstations only shall be viewed as Non-Compliant.

D. If configured any Alarm Condition shall automatically display a specified Custom Map display at any logged on authorized operator workstation. The symbol (icon) representing the Door Monitor Point, or other device causing the Alarm Condition shall change color to identify point of alarm origination on the map display.

E. If so configured an Alarm Condition shall automatically display a specified Custom Operator Instruction with the specific Custom Map display.

F. The ACS shall provide real-time tracking of the actual status of each Armed Monitor Point, providing an indication of when Monitor Point is activated, and of when Monitor Point is cleared. A user selected Point Status Window shall be selectable by an operator to display the real-time status of all points, outputs and readers based on their regional operator profile.

G. Alarm Conditions shall require Operator acknowledgment. Administrator Operators shall have the ability to acknowledge all alarms simultaneously. In addition, the ACS shall allow Alarm Conditions to be configured as “log only” events.

H. The ACS shall provide a visual indication of all unacknowledged Alarm Conditions in the “Alarm Manager” window on any authorized operator workstation.

I. System shall provide an Alarm Manager to display the status of all active and user assigned alarm points for any logged-on and authorized operator at any client on the network. Systems that restrict alarm displays to only assigned operator workstations shall be viewed as Non-Compliant.

2.24 Activation of Output Upon Alarms

A. Through Triggers and Macros, all Alarm conditions, including Door Forced conditions and Door-Held-Open conditions, shall be capable of activating one or more Auxiliary Contact Outputs to enable operation of audible sounders, door alarm horns, and other such devices.

B. System shall permit the global relationship of Alarm Conditions to Auxiliary Outputs, where conditions occurring at one intelligent controller shall be capable of causing outputs to occur at any intelligent controller in the ACS. This will be configured/implemented through custom scripting using command/ini files.

C. The ACS shall allow operator to define how each output is to operate during each Alarm Condition. As a minimum, the ACS shall permit the following operating conditions all configured in a separate software module, Triggers and Macros. Systems that do not support fully configurable Triggers and Macros based on any System event/alarm shall be viewed as Non-Compliant.

   1. Output tracks Alarm Condition / Event / Activity: Output activates when Alarm Condition is active and deactivates when Alarm Condition clears.

   2. Output tracks acknowledgment: Output activates when Alarm Condition is active and deactivates when Alarm Condition is acknowledged by operator, even if Alarm Condition has not yet cleared.

3. Timed output: Output activates when Alarm Condition is active, and deactivates when Alarm Condition has cleared, or after a preset time period, whichever occurs first. Time shall be definable by operator for periods of between 1 and 300 seconds.
4. Access Events: Output activates or de-activates based on any access event/status change with time of day and other event conditioning.
5. Cardholder Event: Output activates base on a cardholder trigger code and access event (granted or denied).

2.25 Email or Text Message Upon Alarm Condition

A. The ACS shall provide ability to send email messages to designated recipients upon a specified alarm condition or operator selection. The ACS shall utilize standard SMTP to permit transmission to any valid email address. This capability shall enable the transmission of alarm messages to any device capable of receiving emails.

B. The ACS shall be capable of generating emails to address groups based on time code.

C. If configured, alarms can be sent via email or SMS to a mobile device.

2.26 Sound Effects Upon Alarm Condition

A. System shall provide ability to automatically play audio messages on designated operator workstations upon Alarm Condition. System shall allow attachment of separate audio and media files to each Alarm Condition. Audio files shall be standard .WAV format audio files, media files are MS standard.

2.27 Trace Feature on Cardholder Access History

A. System shall provide a special Trace feature (Watch Window) that can be set individually for each cardholder. The Trace feature shall allow special real-time tracking of operator-specified cards. Use of a card that has been set for Trace shall be automatically logged, and if so configured, shall cause a special report to be displayed at operator workstation. Trace reports are special and are in addition to any regular report as the result of card activity, such as Valid Access or Invalid Access Attempt.

B. An automatic cardholder activity report and reader access report shall be standard selection in the cardholder file. Reader access reports shall be selected from the Event Manager display, cardholder file and graphic map icons.

2.28 System Reporting and Logging Features

A. The ACS shall provide an electronic log of events, recorded on a real-time basis as they occur. Events shall be recorded with date and time.

B. When intelligent controllers are in an 'on-line (in communication with ACS server) status condition, System events shall be immediately sent to ACS server and written to the host database

C. When intelligent controllers are in an off-line status (i.e. not in communication with the ACS server), the intelligent controllers shall store (buffer) system events in controller memory. Events will be stored in memory to its capacity overwriting as needed in first-in/first-out mechanism. Each intelligent controller shall be capable of storing a minimum of 20,000 events in memory.

D. In addition to being stored, System events shall also have the capability to be immediately displayed at designated operator workstations, providing real-time reporting of all System events.

E. The ACS shall support standard network printing facilities to allow the use of any printer connected to the user's local computer or network. The use of specific printers for specific types of reports shall not be required.

F. The ACS shall allow events to be selectively reported to operator workstations and Printers. As a minimum, the ACS shall allow the selective reporting of the following events: Alarm Condition, Monitor Point activity, Forced Door, Door-Held, Invalid Access Attempt, Passback Violation, Trace, Hardware Failure, Communication Failure, Tamper, Power Fail, etc.

G. The ACS shall provide the capability to generate a current System status report upon command from operator workstation. Status reports will indicate: current status of Doors, Monitor Points, and Alarm Conditions; current status of operator imposed commands such as Disarm, Unlock, Disable and the like; current status of timed System operations, such as timed Unlock, timed Disarm and the like; and the current status of equipment, communications, and power failure conditions.

H. All card access activity shall be logged at a minimum data retention period definable by the system operator. For Valid Access, Invalid Access Attempt, and Trace conditions, the ACS shall be capable of logging the following information as a minimum: Door name and number; card number; and cardholder name (If truncated, shall be 12 characters minimum). For Invalid Access Attempts, the ACS shall display and log reason for rejection.

I. The ACS at a minimum shall log all Monitor Point and Alarm Condition activity.

J. All operator commands from operator workstation shall be logged, including Unlock, Re-lock, Arm, Disarm, Disable, Silence, Acknowledge, Reset, and other such operator commands. Log of Operator commands shall identify the operator who issued each command. The ACS shall log unauthorized attempts to gain access to the ACS, such as the use of an invalid password, including the terminal node and/or network address from which the attempt was made.

K. The ACS shall log all automatic System operations that occur by Time schedules, including Unlock, Re-lock, Arm, Disarm, and other such timed operations.

L. All System failures shall be logged including Hardware Failure, Communications Failure, Power Fail, and other such System conditions.

M. All operator configuration activity, such as modification to card/credential numbers, Time Schedules, Access Levels, Monitor Points, Cardholder Records, and other System data, shall be recorded to an Operator audit log. As a minimum, the operator audit log shall identify the type of data that was modified, old data, new data and identify the operator who modified it. The ACS shall allow the Audit report to be filtered by date and by operator.

N. System shall be capable of selectively displaying all System configuration data at an operator workstation screen, allowing the viewing of Cardholder Records, card/credential numbers, Doors, Time Intervals, Time Codes, Monitor Points, Door Groups, Secured Areas, and other configuration data. System shall provide ability for operator to selectively view specific types and numerical ranges of data all based on their user assigned operator profile.

O. System shall be capable of printing all System configuration data to printer, allowing print-out of Cardholder Records, Clearance Codes, Doors, Time Intervals, Time Codes, Monitor Points, Door Groups, Secured Areas, and other configuration data. System shall provide ability for

P. operator to selectively print specific types and numerical ranges of data all based on an operator's assigned operator profile.

2.29 Archival Data Storage and Backup Tools

A. System shall provide capability to fully backup complete System and database files, including cardholder, hardware, alarms and events databases, to the local computer or external / network storage disk/device. System shall provide a menu-driven backup and restore graphical user interface, with operator prompts, enabling backups and restore functions to be made while the ACS application program is running (when using SQL database only). The ACS shall allow the scheduling of backups and archives using configurable days for the backup to automatically occur. Archiving of data shall be configurable to allow operator to retain up to 36 months of data in the live database.

B. Backups shall be capable of being initiated from any operator workstation. Backup capability shall be available without requiring that the ACS application be closed and backups shall not interrupt System operation or require restarting of the ACS server.

C. System shall provide for archival transfer of event data from hard disk to CD. Archival transfer shall load event data to the local drive or external / network location and shall clear event data from the on-line/live System database after verifying good archive copy. System shall provide a menu-driven utility to allow archival transfer. The ACS shall allow for configurable days and times for the archive process to occur automatically.

D. The ACS shall permit archival storage and back-up to external storage devices via the Users network.

2.30 Archival Database Retrieval Feature

A. The ACS shall provide an integrated database retrieval process for archive purposes. The database retrieval process shall include search and retrieval capabilities, enabling selective reporting from a previously archived database.

B. In addition to basic search tools, the database retrieval System allows the use of Structured Query Language (SQL) to conduct more advanced searches. The SQL used shall be an industry-standard type that is in common use. SQL queries shall permit access to all data stored in System Journal and well as all data in System configuration database including Cardholder Records.

C. Database retrieval reports shall be capable of being printed to designated printers upon operator command. Retrieval of data shall not interrupt System operations.

D. The ACS shall allow database retrieval reports to be exported in industry standard data formats capable of being exported into external spreadsheets, databases, and report analysis tools.

E. The ACS shall provide a menu-driven utility that enables the retrieval of journal data from archival storage, for the purpose of generating reports. Retrieval, reporting, and viewing of data from archival storage shall not interrupt system operation or require that the current event data be cleared from hard disk.

2.31 Quick Look-Up Feature

A. The ACS shall provide a method to quickly display the cardholder record and photo image for any cardholder based on cardholder name. This feature shall be available to authorized operators at any operator workstation.

2.32 Automatic Display of Photo Image

A. The ACS shall allow for photo callup of cardholder image based on card activity on the “Event Manager” screen where an authorized operator is logged on.

B. From the “Event Manager” screen an authorized operator shall be capable of selecting, using a single mouse click a reader access display or access the cardholders file.

PART 3 EXECUTION

3.1 System Installation

A. The Access Control Solution (ACS) shall be installed in accordance with the recommended procedures defined in the relevant manufacturer's documentation for the system, individual device or component.

B. Intelligent controller and sub-controller panel installation:

1. Install each panel in equipment closet locations as indicated. Install each panel at a location and height to facilitate ease of service.
2. Identify the software and hardware address of each panel with a permanent marking label installed on the exterior of the cabinet.
3. Neatly dress and tie all wiring within panel. Do not obstruct access to terminal strips and configuration jumpers with wiring.
4. Provide terminating resistor on all unused input connections.
5. Label all inputs and outputs with a permanent marking label.
6. Ground all shielded cables in accordance with manufacturer's instructions. Trim and wrap all unused shield wires to prevent shorting or inadvertent grounding.

C. Data communications:

1. Provide interconnection of ACS server, operator workstations, and intelligent controllers using the TCP/IP Ethernet network. Coordinate connections and IP addressing with Owners designated telecommunications representative.

D. Power supply installation:

1. Install all System power supplies at intelligent controller panel backboard locations as indicated.
2. Unless otherwise noted, all System accessories, such as REX motion detectors, door alarm horns, sounders and the like shall be powered from 12 VDC auxiliary power supply located at equipment backboard.
3. Unless otherwise noted, power all electric lock hardware from 24 VDC lock power supply located at equipment backboard. Do not power lock hardware from other power supplies.
4. Connect power supply fault output to input point on intelligent controller. Provide pilot relay where needed to provide dry-contact output from power supply.

E. Card reader installation:

1. Where possible, all card readers mounted outdoors shall be installed out of direct exposure to sunlight, rain, and snow.

2. Unless otherwise noted, card readers are to be mounted at a height of 40” above the finished floor (measured from floor to centerline of card reader.) to be ADA compliant.
3. Securely mount all card readers using tamper-resistant fasteners.
4. Card readers shall completely cover any electrical back box or other electrical rough-in. Provide trim plates, adapters and back boxes at locations where required.
5. Card readers shall be installed so that they are “low-profile” and protrude from the wall only a minimum distance.
6. Completely seal all exterior openings of outdoor mounted card readers to make weather-tight.
7. Make card reader field adjustments in accordance with manufacturer's instructions.

F. Connection to electric lock hardware:

1. Provide wiring and final connection to electric strikes, electric locks, transfer hinges, electric exit devices, detention hardware, and other such devices.
2. Provide diode for transient suppression across coils of electric locks, electric strikes, and relay coils.
3. Verify operating voltage and current requirements of all lock hardware with hardware supplier. Coordinate cable requirements and connection points. Thoroughly test the operation of all electric lock hardware for proper operation.
4. Install pilot relay to control lock hardware where current requirements of the hardware exceed the relay contact rating of the intelligent controller or where electrical isolation is required.

G. General device wiring:

1. Connect card readers, inputs, and outputs to intelligent controllers as indicated on the enclosure or otherwise indicated.
2. Card reader, door switch, request-to-exit, and lock output wiring shall be “home-run” and connected to a sub-controller as indicated on the enclosure or otherwise indicated.
3. Use standard and consistent wire conductor color-coding for device wiring. Use the same colors for each function throughout the project, for example: Red and Black colored wires always used for power, Green and Yellow colored wires always used for detection circuit, etc.
4. Install end-of-line resistors at detection device. End-of-line resistors shall be connected to flexible wire leads and be protected with heat-shrink tubing or equivalent. Direct crimp or wire nut connections to resistor are not permitted.

H. Interface to fire alarm system:

1. Fire alarm output module to be provided (under Division 16) at locations adjacent to security equipment backboards. Fire alarm output module will provide a single Form C dry-contact output rated at one ampere. Contractor to provide pilot relays as needed to provide additional contacts or greater current capacity.

I. Card reader control of elevators:

1. Coordinate installation of card access System for elevator with elevator installer.
2. Coordinate requirements for conductors in elevator traveling cables with elevator installer. Verify that conductor quantities and types are suitable for use with card reader.
3. Provide card readers to elevator installer for installation in elevator. Make final connections to card reader.
4. Provide relay interface circuit between Security Management System and elevators as indicated on drawings. Route cabling in the elevator machine room to locations designated by elevator installer.
5. With cooperation and assistance of elevator installer, fully test all elevator control functions. Provide assistance to elevator installer, as required to troubleshoot any elevator control related problems.

J. Special interface requirements:

1. "Fire Exit" Stair doors: These doors to have fail-safe electric lock hardware. Provide pilot relay at each 24 VDC lock power supply. Connect lock outputs at these doors in series with pilot relay contacts so that doors automatically unlock on fire alarm condition regardless of state of ACS output.
2. Card reader doors with automatic openers: Provide pilot relay connected to inside door opener actuator buttons. Activation of buttons shall cause activation of REX input as well as operation of automatic door opener.

3.2 Programming and Configuration

A. The system shall be configured in accordance with the manufacturer's recommended procedures as defined in the documentation for the system.

B. If bundled with a hardware, software may be configured prior to delivery and installation.

C. All device firmware shall be the most recent provided by the device manufacturer, or of a version specified by the ACS manufacturer.

D. All ACS software shall be delivered and installed with the manufacturers latest release version of the software.

E. The contractor shall provide initial programming and configuration of the software to make the ACS fully operational. Initial programming of the software shall include:

1. Installing and configuring ACS server and workstation software
2. Configuring interfaces to external systems
3. Creating and configuring:
    a. Operator accounts and permissions
    b. Graphical floor plans
    c. Alarm reporting and alarm routing
    d. Doors and device groups
    e. Individual input and outputs
    f. Input and output groups
    g. Clearance codes
    h. Schedules and operating modes

F. Input of all program data shall be performed by the Contractor. The Contractor shall consult with Owners Representative and Security Consultant to determine descriptor names and system operating parameters.

G. The Owner, with the cooperation and assistance of Contractor, will input the cardholder data for each access card.

H. Contractor shall maintain a complete, up-to-date backup of the ACS configuration and cardholder database. Backups shall be maintained throughout the programming period until final acceptance by Owner.

3.3 User Documentation

A. The manufacturer shall provide user documentation that explains how to install, configure, operate and maintain the software.

B. The Contractor shall maintain hard copy worksheets which fully document system programming and configuration:

1. Worksheets shall be kept up to date daily by Contractor until final acceptance by Owner.
2. Worksheets shall be subject to inspection and approval by Owner.
3. Contractor shall provide final copies to Owner prior to project close-out.

3.4 Training

A. The manufacturer shall offer professional training services to assist the organization in meeting their training requirements.