RBH
ACCESS
TECHNOLOGIES
INC.

Integrated Access Control

And Security Management System

ARCHITECTURAL / ENGINEERING

AND BID

SPECIFICATIONS

RBH Access Technologies Inc.

The System

The Security Management System should be capable of Controlling and Monitoring Access through the doors, Monitor and control Inputs and Outputs, include an Integrated Video Badging, Integrate Elevator Control and Seamless Integration to Digital Video Recorder and control CCTV functionality. The software should be capable of recording events in such a way that they are recorded whenever an access is granted/denied or access granted during programmed schedules or holidays etc.

Pop up screens should display the video if the Access points or input points are tagged to those points in case of alarm. This should be programmable by the operator. The system should also have video verification capability where the guard could verify the person before granting access through the software and from the video. The guard should have a single screen wherein he can see the Video as well as have the card details of the person accessing the door with his photo from the file. The system should also have a High security mode wherein only privileged card holders can have access to the facility and this should be programmable to be based on events or per a programme time schedule. This should be flexible and should be easily programmed to suit any specific needs.

The system should also provide Time & Attendance information such as Name, In Reader location, Out Reader Location, IN time, OUT Time and the number of hours worked along with other system reports. The data should be exported to any payroll or HR package in various different file formats. Whenever a card holder presents the card at the reader the system should be capable of displaying the Video from the camera focused on the door plus bring in his card details from the database on a single screen for verification. It should also be possible to verify at a later date if the access has been not been misused.

The system should also be capable of recording events automatically on any compatible DVR and should be able to retrieve recordings based on events.

System Overview

1.1 General Overview

A. Functions of the Integrated Access Security Management System (ISMS) shall include:
   1. Granting or denying access to secured areas.
   2. Controlling access point features and modes.
   3. Alarm input and abnormal access point activity monitoring.
   4. Output control.
   5. System configuration and management functionality to facilitate functions listed above.
   6. Reporting of the events generated by the functions listed above.
   7. System configuration reporting.
   8. Facilities to automate event search on connected Digital Video Recorders (DVR).
   9. Integrate seamlessly with any compatible DVR and control CCTV functionality
   10. Control Elevator Access to the floors based on Access permissions. Elevator Controller allows control of up to two elevator cabs with 8 floors total. Can be expanded to control up to 32 floors. It should utilize flash firmware for easy upgrades, and employs fully distributed intelligence for off-line operations.
   11. Integrate with third party Alarm panels

12. The software should be capable of producing ID badges and printing them on any suitable card printer
13. With optional modules the system should be capable of controlling upto 4 doors per panel or 4 doors with IN/OUT capability

1.2 System Architecture

A. ISMS shall consist of the following:
   1. Server Software package, with following functions:
      a. User interface for system control and configuration.
      b. Field hardware communication functionality.
      c. Live activity and status display.
      d. System and event history reporting functionality.
      e. Server for the Client Software packages.
   2. Client Software Packages, with following functions:
      a. User interface for system control and configuration.
      b. Live activity and status display.
      c. System and event history reporting functionality.
   3. Intelligent Field Panels, supporting:
      a. 2 access points.
      b. Local means of control trough system and panel links as well as reader and reader/keypad input.
      c. Field interface to access control readers of various types.
      d. Field interface to variously configured alarm inputs.
      e. Control relay and voltage outputs.
      f. Communicate with the Server Software package, by means of:
         1) Direct RS-232 connection
         2) Direct or networked RS-485 connection.
         3) Direct modem connection (Utilizing external modem)
         4) Direct TCP/IP connection (Utilizing TCP/IP gateway).
      g. Convert RS-232 into RS-485.

1.3 Operational Features

A. Access Points:

   1. Access point shall be configured to:
      a. Auto-relock, when door is closed. Overriding unlock timer.
      b. Deduct usages from cardholder's balance.
      c. Report or not to report door forced open events.
      d. Unlock based on a schedule.
      e. Require System Operator's decision to grant or deny access to cardholder requesting access by use of a card.
      f. Conform to "first person delay" rule of the scheduled unlocking.
      g. If specified bypass door contact only without activating lock output following request to exit activation.
      h. If specified deny access to cardholders without High Security privilege.
      i. If specified operate in site code only mode.
      j. Report or not to report request to exit activations.
      k. Report or not to report failure of a cardholder to open the door following a valid card use.
      l. Report or not to report invalid card format event.

m. If specified require both card use and PIN entry based on a schedule.
n. Function in timed anti-passback mode with a specified delay if required.
o. Function in true panel or global anti-passback mode with either hard or soft enforcement if required.
p. Associate with entering and exiting pre-defined areas.
q. Initiate display of the cardholder's information and picture on Server and Client software packages, based on Access Granted and/or denied and/or requested.
r. Initiate recording on any compatible DVR based on programmed events on the Access points.
s. POP up video of the designated camera in case of alarm
t. Allow Elevator Access to designated floors.

2. Access Points shall be granting or denying access to a secured area, based on:
   a. Access Level permissions, specifying an independent access schedule for each access point.
   b. Status of the card.
   c. High security privilege.
   d. Current usage balance.
   e. Anti-passback status or privilege.
   f. Card de-activation date and time.
   g. Card and PIN match.
   h. Site code mode.
   i. Manual command based on access request.
   j. RTE input activation.

3. Access point shall lock and unlock:
   a. Manually, through system command.
   b. Manually, through double consecutive use of an authorized card.
   c. Manually or automatically, through panel or system linking.
   d. Automatically, based on schedule.
   e. Automatically, based on schedule and first valid card use.

4. Modes of the access point shall be controlled:
   a. Manually, through system command.
   b. Manually, through quadruple consecutive use of an authorized card (See High Security Mode).
   c. Manually or automatically, through panel or system linking.

5. Access point shall posses convenience features for handicapped cardholders:
   a. Extended unlock time for designated cardholders.
   b. Activation of an additional output for designated cardholders.

6. Access point shall provide reporting of the following events:
   a. Access granted, requested.
   b. Access denied with a specific reason.
   c. Door held open warning.
   d. Door held open alarm.
   e. Door locked and unlocked.
   f. Forced entry.
   g. Restore.

h. Door not open alarm, following card access granted.

7. Access point shall have capability to trigger Recording on any compatible DVR, panel and system links by:
   a. Access granted or denied events.
   b. Door held open warning.
   c. Door held open alarm.
   d. Door locked and unlocked events.
   e. Forced entry event.
   f. Restore event.
   g. Door not open event, following card access granted.

8. Access Point shall be associated with a specific camera on a specific compatible DVR (addressed by IP address and port) for automated video retrieval and display of live picture from the camera associate with it.

B. Alarm Inputs.

1. Alarm input shall be configured to report various messages to Server software package with abilities to:
   a. Specify in which state (never, armed and/or disarmed) a specific alarm input reports.
   b. Suppress individual message types of a specific alarm input based on a schedule.
   c. Display a pre-defined message for each event type of a specific alarm input.

2. Alarm input shall have the ability to be configured with a delay on alarm reporting.

3. Alarm inputs shall be armed and disarmed:
   a. Manually, through system command.
   b. Manually or automatically, through panel or system linking.
   c. Automatically, based on schedule.

4. Alarm input shall provide event reporting of the following events:
      1) Input alarm.
      2) Input restore.
      3) Input trouble.
      4) Input normal.
      5) Input abnormal.
      6) Force armed.

5. Alarm input shall trigger panel and system links by:
      1) Input alarm and restore events.
      2) Input trouble event.
      3) Input normal and abnormal events.

6. Alarm input shall be associated with a specific camera on a specific compatible DVR (addressed by IP address and port) for automated video retrieval.
7. POP up video of the designated video in case of alarm

C. Outputs.

1. Outputs shall be configured as:
   a. Fail-safe or fail-secure.
   b. Reporting or non-reporting to the Server Software package.

2. Outputs shall be activated and deactivated:
   a. Manually, through system command.
   b. Manually or automatically, through panel or system linking.
   c. Automatically, based on schedule.

3. Output shall provide event reporting of the following events:
   1) Output on.
   2) Output off.

4. Output shall trigger panel and system links by:
   1) On and off events.
5. Alarm Output shall be associated with a specific camera on a specific compatible DVR (addressed by IP address and port) for automated video retrieval

PART 2 Hardware Specifications

2.1 Intelligent Field Panel (IFP)

The panels should be UL listed and also comply with FCC and CE regulations

A. IFP Architecture:
1. IFP shall utilize a fully distributed intelligence controller architecture whereby access decisions are made locally at the controller.
2. IFP shall utilize flash firmware for easy upgrades.
3. IFP shall support two access points.
4. IFP should be capable of expanding the functionality of the two access points to two access points IN/OUT, making the IFP a 4 reader controller.
5. IFP shall support local means of control through system and panel links as well as reader and reader/keypad input.
6. IFP shall support field interface to access control readers of various types.
7. IFP shall support field interface to eight variously configured alarm inputs.
8. IFP shall control four relay and four voltage outputs.
9. The Server software package (host computer) shall download panel specific data, including up to 8,000 cardholders, to the IFP on the network. This data shall be stored within each panel and contain all pertinent information relating to the panel's functionality.
10. Host computer shall communicate global links and anti-passback messages between panels.
11. Should communication with the Server software package (host computer) be lost, up to 3,000 time-stamped events shall be stored in panel's buffer, until communication is restored. Upon restoration of communications all event data shall be automatically uploaded to the host computer including the actual time of occurrence.
12. This functionality shall enable any off-line controller to maintain full access control processing capability. A card user shall not be aware of the off line condition.

13. A system that does not buffer event information when communications are lost will not be acceptable.

B. IFP communications:
   1. Host computer shall support up to 16 networks with a maximum of 32 panels connected, upgradeable to a maximum of 64.
   2. Up to 16 Intelligent Field Panels shall be connected on a hard wired network.
   3. Following means shall be used to connect a hard wired network of panels to the host computer:
      a. Direct RS-232 (three wire)
      b. Direct RS-485, utilizing RS-232 to RS-485 converter.
      c. Dial-up, utilizing external modem connected via RS-232 (4 wire) with modem power reset capability in IFP.
      d. TCP/IP, utilizing a field configurable network gateway.
   4. The hardwired communication network shall be wired with 18AWG twisted-pair, shielded cable. The hardwired network shall have maximum length of 4,000'. This network shall be wired in a daisy chain configuration.
   5. System shall be configured to report various panel communications status messages to the Server software package with abilities to:
      a. Suppress individual message types of a specific alarm input based on a schedule.
      b. Display a pre-defined message for each event type of a specific alarm input.
   6. System shall provide event reporting of the following events:
      1) Panel online.
      2) Panel offline.
      3) Panel trouble.

C. IFP hardware configuration:
   1. Panel Addressing
      a. IFP's address shall be set via four onboard dip-switches.
      b. Available addresses shall be 1 through 16.
   2. Communications speed settings
      a. IFP's communications speed shall be set via two onboard dip-switches.
      b. Available rates shall be 9.6, 28.8, 38.4 and 56 kbps.
   3. Modem configuration
      a. IFP's modem communications shall be enabled via an onboard dip-switch.
      b. Selection between dial-up and direct network shall be available.
   4. Host or network setting
      a. IFP's location on the network (connected to the host vs. RS485 network connection) shall be enabled via an onboard jumper.
   5. RS-485 Tuning
      a. IFP shall provide means of RS-485 network tuning, specifically:
         1) Low bias.
         2) High bias.
         3) Termination.
      b. IFP tuning shall be accomplished by adjusting onboard jumpers.

D. IFP Reader Interface
   1. IFP shall provide interface to access control readers utilizing either magnetic stripe or Weigand electrical formats.
   2. IFP shall support up to 5 different card formats simultaneously.
   3. IFP shall support all major reader technologies:
      a. Proximity
      b. Magnetic Stripe
      c. Weigand
      d. Bar Code
      e. Keypad Only
      f. Proximity with Integrated Keypad
      g. Magnetic Stripe with Integrated Keypad
      h. Hand Geometry
      i. Fingerprint
   4. IFP shall provide dedicated control over Red and Green LEDs for each access point.
   5. IFP shall provide dedicated control over Buzzer for each access point.
   6. Wire lengths of 500' utilizing 20AWG and 250' utilizing 22AWG 6 or 8 conductor shielded cables shall be required.

E. IFP Alarm Inputs:
   1. IFP shall provide eight fully programmable alarm inputs.
   2. Each alarm input shall support all of the following circuit types:
      a. N.O. Non-supervised.
      b. N.C. Non-supervised.
      c. N.O. Supervised with one resistor.
      d. N.C. Supervised with one resistor.
      e. N.O. Supervised with two resistors.
      f. N.C. Supervised with two resistors.
      g. Combination N.O. and N.C. Supervised with one resistor.
   3. Wire lengths of 1,000' utilizing 20 or 22AWG cables shall be required.

F. IFP Outputs:
   1. IFP shall provide eight fully configurable outputs (four relay and four voltage ones).
   2. Each output shall be configured as fail-safe or fail-secure.
   3. Relay output shall be rated 2A @ 30VDC.
   4. Voltage outputs shall switch negative 12VDC @ 100mA.

G. IFP Enclosure:
   1. Height: 12"
   2. Width: 14"
   3. Depth: 3 ½"

H. IFP Environmental tolerances:
   1. Operating temperature: 35-150°F
   2. Operating humidity: 20-80% RH (non-condensing)

PART 3 Reports

3.1 Time and Attendance Reports

The system should also provide Time & Attendance information such as Card Holder Name, In Reader location, Out Reader Location, IN time, OUT Time and the number of hours worked and also calculate the number of hours worked for a certain time period, say a week etc. This should be in addition to a number of other reports being able to be generated from the system. The data should be exported to any payroll or HR package in various different file formats.

Whenever a card holder presents the card at the reader the system should be capable of displaying the Video from the camera focused on the door plus bring in his card details from the database on a single screen for verification. It should also be possible to verify at a later date if the access has been not been misused. All such transactions should be capable of being stored in the database as well as on any compatible DVR.