Hartmann Controls Corp.
Toll free 1-877-411-0101
Phone: (705) 719-6705
Fax: (705) 792-5632
www.hartmann-controls.com

Specifier Notes typically precede specification text; delete notes in final copy of specification. Trade/brand names with appropriate symbols typically are used in Specifier Notes; symbols are not used in specification text. Metric conversion, where used, is soft metric conversion.

SECTION 28 13 00
ACCESS CONTROL

PART 1 GENERAL

1.1 SUMMARY

A. Section Includes: Server hardware and software, client software, security access devices, access control, relay control, elevator control, credential creation and credential holder database and management, Digital Video Integration, Basic Burglary Alarm Integration

Specifier Note: Revise paragraph below to suit project requirements. Add section numbers and titles per CSI *MasterFormat* and specifier's practice.

B. Related Sections:

1. Section [08 11 00 - Metal Doors and Frames] [_____].
2. Section [08 14 00 - Wood Doors] [_____].
3. Section [08 41 13 – Aluminum Framed Entrances and Store fronts] [_____]
4. Section [08 71 00 - Door Hardware] [_____].
5. Section [14 20 00 - Elevators] [_____].
6. Section [21 09 00 – Instrumentation and Control for Fire-Suppression Systems] [_____]
7. Section [25 15 00 - Integrated Automation Software] [_____].
8. Section [26 05 00 - Common Work Results for Electrical] [_____].
9. Section [26 05 19 - Low-Voltage Electrical Power Conductors and Cables] [_____].
10. Section [27 10 00 - Structured Cabling] [_____].

Specifier Note: Article below may be omitted when specifying manufacturer's proprietary products and recommended installation. Retain Reference Article when specifying products and installation by an industry reference standard. If retained, list standard(s) referenced in this section. Indicate issuing authority name, acronym, standard designation and title. Establish policy for indicating edition date of standard referenced. Conditions of the Contract or Section 01 42 19 - Reference Standards may establish the edition date of standards. This article does not require compliance with standard, but is merely a listing of references used. Article below should list only those industry standards referenced in this section. Retain only those reference standards to be used within the text of this Section. Add and delete as required for specific project.

1.2 REFERENCES

A. Institute of Electrical and Electronics Engineers (IEEE):

11. IEEE 1100 Recommended Practice for Powering and Grounding Electronic Equipment.

B. National Fire Protection Association (NFPA):

12. NFPA 70 2005 National Electrical Code.
13. NFPA 72 National Fire Alarm Code.
14. NFPA 80 Fire Doors and Windows, 2007 Edition.
15. NFPA 101 Life Safety Code, 2009 Edition.

C. International Organization for Standardization (ISO):

16. ISO 7816 Smart Card Standard.

Specifier Note: Article below should be restricted to statements describing design or performance requirements and functional (not dimensional) tolerances of a complete system. Limit descriptions to composite and operational properties required to link components of a system together and to interface with other systems.

1.3 SYSTEM DESCRIPTION

A. Design Requirements: Provide products and systems that have been manufactured, fabricated and installed to the following criteria:

17. Comply with IEEE 1100.
18. Comply with NFPA 70.
19. Comply with NFPA 72.
20. Comply with NFPA 80.
21. Comply with NFPA 101.
22. Access Control Management System: Protector.Net Electronic Access Control System.

a. System Capabilities:

1) Fully distributed processing, field devices not dependent on on server operations once programmed.
2) Control access to unlimited doors.
3) Control elevator access up to 64 floors per Cab.
4) Manage and control access for up to 50,000-100,000 credentials per controller.
5) Unlimited remote sites.
6) Configurable alert screen and email notifications
7) Photo ID badging integration via SQL database
8) Readers, inputs and outputs expandable and/or modifiable.
9) Single software program controlled.
10) 50 Programmable Holidays per Holiday Group
11) 50 Holiday Groups configurable
12) Multi-site Management via Partitions
13) No client software needed, client accesses via HTML5 browser
14) Local anti-passback
15) Full integration and customization of all system components.
16) Online reconfiguration through system programming without hardware changes.

b. Access Control Functions:

17) Validation of Credential based on Time of day, Day of week, Holiday scheduling, mode of Door, and special event schedules.
18) Simultaneous controlled access with various reader technologies;
    a) Proximity
    b) Pin number
    c) Biometrics
    d) Mag stripe
    e) Bar code
19) Automatic or manual retrieval of cardholder photographs.
20) First person in capability.
21) Access validation based on positive verification of Credential, PIN, or Credential/PIN combination, or dual credential with one credential being a supervisor credential.
22) Differentiates between valid credential presentation only, and valid credential presentation followed by entry (when using door position switch).

c. Passwords:

23) Assignable.

24) Unlimited number of system Administrators.

25) Permissions of system Administrators are definable per Administrator.

26) Administrator actions/capabilities range from basic system monitoring to control of all system functions.

27) Administrators can be linked and managed by LDAP systems.

d. System Programming:

28) User-friendly, intuitive, and responsive HTML5 web client interface.

29) Single Page Application (SPA) architecture allows seamless browser transition between pages.

30) Ability to import large quantities of cards in a CSV file format.

e. Alert messages:

31) Ability to monitor for specific event types, run reports based on specific event types or events associated with devices or users.

32) Alert information displayed in text format on the notifications area, and highlighted based on severity of alert.

33) Video feed switching capabilities associated with alert via IP communication. (fully configurable)

34) Capability of E-Mailing alert events to administrators.

f. System integration:

1) VMS integration:
   a. ViconNet® Digital Video Management system
   b. Digital Watchdog® DW Sprectrum
   c. ExactQ® ExactVision
   d. Milestones® Xprotect
2) Microsoft Active Directory Integration via LDAP protocol.
3) CardPresso® Photo badging software integration.
4) Alarm system integration via configurable dry contact output/input.
5) ASSA ABLOY Aperio® hub integration .

B. System minimum Requirements:

Specifier Note: The computer specifications are the minimum standards for a basic system. When a system includes a large number of clients, controllers, and/or users, additional server power is strongly recommended. Central Processing Unit Computer:

23. Microsoft compatible Windows 7 or newer.
24. 2Ghz or faster 32-bit (x86) or 64-bit (x64) processor. Two or more cores.
25. 4GB RAM for 32-bit and 4GB RAM for 64-bit
26. DVI or HDMI monitor
27. 1GB hard drive space required (Additional space required for database).
28. Microsoft .Net Framework 4.5 Full.
29. Microsoft SQL Server 2008 or SQL Server 2008 Express or Higher.

Specifier Note: Article below includes submittal of relevant data to be furnished by Contractor before, during or after construction. Coordinate this article with Architect's and Contractor's duties and responsibilities in Conditions of the Contract and Section 01 33 00 - Submittal Procedures.

1.4 SUBMITTALS

A. General: Submit listed submittals in accordance with Conditions of the Contract and Section [01 33 00 - Submittal Procedures] [_____].

B. Product Data: Submit product data for specified products, ____ copies

C. Manufacturer's Instructions: Manufacturer's Technical installation guide, and Manufacturer's Software Guide, ____copies.

D. Drawings: Submit shop drawings detailing installation procedures, including layout, dimensions and support placement, ___ copies.

Specifier Note: Coordinate paragraph below with Part 3 Field Quality Requirements Article. Retain or delete as applicable.

E. Closeout Submittals: Submit the following:

30. Warranty: Warranty documents.

31. Operation and Maintenance Data: Operation and maintenance data for installed products in accordance with Section [01 78 00 - Closeout Submittals] [_____]. Include methods for maintaining installed products and precautions against cleaning materials and methods detrimental to finishes and performance.

1.5 QUALITY ASSURANCE

A. Qualifications:

32. Installer: Experienced in performing work of this section, and having specialized knowledge in installation of systems similar to that required for this project. **Installer must be a manufacturer trained and authorized Protector.Net installer, providing termination, commissioning and end-user training (technical and/or administrative) services as required.**

33. Manufacturer: Capable of providing field service representation during construction, and approving installation and application method, as well as providing termination, commissioning and end user training (technical and/or administrative) services as required.

Specifier Note: Paragraph below should list obligations for compliance with specific code requirements particular to this section. General statements to comply with a particular code are typically addressed in Conditions of the Contract and Section 01 41 00 - Regulatory Requirements. Repetitive statements should be avoided.

B. Regulatory Requirements: In accordance with Section [01 41 00 - Regulatory Requirements] [_____].

34. IEEE 1100.

35. NFPA 70.

36. NFPA 72.

37. NFPA 80.

38. NFPA 101.

C. Pre-installation Meetings: Conduct pre-installation meeting to verify project requirements, manufacturer's installation instructions and manufacturer's warranty requirements. Comply with [Section 01 31 19 - Project Meetings].

1.6 DELIVERY, STORAGE & HANDLING

A. General: Comply with Section [01 61 00 - Common Product Requirements].

B. Ordering: Comply with manufacturer's ordering instructions and lead time requirements to avoid construction delays.

C. Delivery: Deliver materials in manufacturer's original, unopened, undamaged containers with identification labels intact.

D. Storage and Protection: Store materials indoors, protected from exposure to harmful weather conditions and at a temperature between 10 and 30 degrees Celsius, and between 10% and 90% relative humidity, non-condensing. Product boxes not to be stacked more than 3 high, and are not to have anything stacked on top or directly beside the product that could possibly cause damage based on weight, moisture, corrosive content etc.

Specifier Note: Coordinate article below with Conditions of the Contract and with Division 01 Closeout Submittals (Warranty) Section.

1.7 WARRANTY

A. Project Warranty: Refer to Conditions of the Contract for project warranty provisions. Submit, for Owner's acceptance, manufacturer's standard warranty document executed by authorized company official. Manufacturer's warranty is in addition to, and not a limitation of, other rights Owner may have under Contract Documents.

B. Manufacturer's Warranty: Hartmann Controls warrants all Protector.Net Controllers manufactured by Hartmann are free from defects in material and workmanship. However this warranty **does not** cover non-manufactured peripheral products sold by Hartmann. Peripheral products are covered by the manufacturer's warranty of the particular peripheral device.

C. Warranty Period: Hartmann Controls Protector.Net Controllers carry a 2 (two) year warranty from date of substantial completion. Hartmann Controls Corp will repair or replace defective equipment upon return to its facility, if they find that the warranty was breached in any way, Hartmann Controls Corp will not warrant any damage that occurred during shipping or handling, or damage caused by a repair or an attempt to repair by any person other than those authorized by Hartmann Controls. This warranty covers normal industrial use and does not cover defects or damage to any product which, in the sole opinion of Hartmann Controls Corp has been subject to improper installation, unauthorized modification, misuse, neglect, abuse, or abnormal operating conditions, improper storage, or which has been attributable to acts of God such as lighting. Installation, which is not in accordance with the installation instructions, published by Hartmann Controls, will void the warranty. This warranty does not cover defects or damage caused by a product, which is not approved by Hartmann Controls Corp and is connected to a Protector.Net system.

The said warranty only applies to the original purchaser and is and shall be in lieu of any and all other warranties.
*** Please note this does not include shipping, which will be supplied by the customer.*

PART 2 PRODUCTS

Specifier Note: Retain article below for proprietary method specification. Add product attributes performance characteristics, material standards and descriptions as applicable. Use of such phrases as “or equal” or “or approved equal” or similar phrases may cause ambiguity in specifications. Such phrases require verification (procedural, legal and regulatory) and assignment of responsibility for determining “or equal” products.

2.1 ELECTRONIC ACCESS CONTROL MANAGEMENT SYSTEM

A. Manufacturer: HARTMANN CONTROLS CORP.

1. Contact: PHONE 877-411-0101, FAX 705-792-5632. www.hartmann-controls.com

B. System Components:

1. 1 Door Controller: ODM-M

a. Supports up to 2 readers (IN and OUT configuration)

b. Power input: IEEE 802.3af PoE standard provides up to 15.4 Watts.

c. Processor: 32-Bit Microprocessor-Based

d. Operation mode:

1) Requires server software for credential/schedule configuration.

2) Will operate stand-alone once programmed.

e. Storage:

1) Up to 100,000 users/cardholders per controller.

2) 50,000 event storage onboard

f. Terminals: Quick disconnect terminal headers.

g. Reader Communications:

1) 2 x Wiegand Data1/Data0, with optional LED and buzzer control.

2) LED Indicator: 2 x Reader active indicators.

h. Lock Power:

1) Solid State Wet Relay 12VDC @ 500mA / 24VDC @ 250 mA (with opt. Converter).

2) LED Indicator:1 X Lock Power LED

i. Relay Outputs:

1) 2 X Solid State Relay 60V (TVS circuit limits 24V), 500mA.

2) Fully configurable, no mechanical parts.

3) Dry Contact.

4) LED Indicator: 2 x output indicator.

j. Relay Output Devices: Fully configurable to work with the following devices:

1) Door strike

2) Magnetic Lock (use external relay or dry contact module)

3) Door opener

4) External buzzer

5) External alarm systems (arming/disarming)

6) Gates

7) Aux devices that will accept dry contact input.

8) Man trap devices (door open or unlocked)

k. Inputs: 4 Dry contact inputs, fully configurable including supervised or digital input setting.

l. Input Functions include:

1) Request to exit

2) Door contact

3) Door opener to enter (require card)

4) Door opener to exit

5) External motion sensor

6) Emergency alarm

7) External alarm status (check if alarm system is armed)

8) Door prevent unlock (used with mantraps)

9) Aux input:

a) Pulse selected output

b) Activate selected output

c) Deactivate selected output

d) Toggle selected output

e) Activate alarm interfaced

f) Disengage emergency alarm

g) Override doors with crisis levels

m. Auxiliary Power: 12VDC @ 450mA without readers. (Used to power motion devices, Piezo's, etc.) Current shared with two reader ports.

n. Reader power: 12VDC @ 450mA max shared across both reader port and Auxiliary 12VDC output.

o. Reader Formats: Magnetic stripe, Biometric, Bar code, and Wiegand format up to 64 bit.

p. Networking:

1) 10/100Mbps supporting Static or DHCP modes with 2 Ethernet status LED's.

2) On board HTTP interface for diagnostics and remote IP configuration. Secured by configurable password and can be disabled.

3) LED Indicator: 2 x PoE power indicator

4) 256 bit AES encryption between Panel and Server (optional)

q. Security: Hardware secured by configurable password.

r. Tamper Sensor: Photo tamper sensor (configurable) (no moving parts).

s. Display:

1) 2 Line x 16 Character LCD Display with LED back light used for on-board diagnostics and initial configuration such as IP address and communication modes.

2) Contrast adjustable.

3) Brightness adjustable.

t. Keyboard: Four user push buttons for data entry or output selection.

u. Diagnostics: Several on board diagnostics available including the following:

1) Reader Test:

a) Ability to test if the reader on port 1 or 2 is able to read a card, and shows bit

format, facility code and card number on LCD display.

2) Output Test:

a) Ability to manually trigger each of the 3 solid state relays, used to test that output devices such as door strikes are wired up correctly.

3) Input Test:

a) Ability to test each dry contact input for changes.

b) Indicator and audible alert if an input state changes.

c) Used to test input devices such as door contacts, REX, and auto opener buttons are wired correctly.

4) Ping with IP:

a) Ability to perform a basic network connectivity test by communicating with the server IP via ICMP protocol.

5) Ping with Name:

a) Ability to perform a basic network connectivity test by communicating to the server by resolving the name of the server via a Dynamic Name Service(DNS).

6) Debug mode:

a) Optional debug mode that allows extra logging of communications and panel decisions.

7) Read Only mode: Displays controller configuration and miscellaneous information

a) Panel Name

b) Area name (anti-passback)

c) Panel ID

d) IP Address

e) Panel MAC Address

f) Panel Subnet Mask

g) Panel Gateway

h) Panel DNS

i) Communication mode

j) Server IP Address/Name

k) Server Port

l) Firmware Version

m) Network Name

n) Door State

o) Door Mode

p) DHCP Bound address

q) Time (UTC and Local)

r) Connection Status

v. On-board Communication Configuration:

1) Ability to configure communication method to server (name or IP address).

2) Ability to configure name or IP address that the server can be reached.

3) Ability to configure network settings of controller, including:

a) Static IP address or DHCP

b) Controller IP Address, subnet mask, default gateway, DNS server.

w. Sound: On-board piezo buzzer (90dB at 10cm) for the following functions:

1) Sounding alarm during forced open event.

2) Sounding alarm during held open event.

3) Feedback when arming/disarming external alarm systems.

4) Configurable to play sound when door opens.

5) External buzzer can be used.

x. Motion PIR (optional):

1) PIR motion sensor mounted on bottom of unit for authorizing exit without card read.

2) Configurable to unlock the door upon motion detection.

3) Sensitivity fully configurable via software.

y. Time: Keeps up to 1 month without power connection, No battery needed. Automatic DST switch.

z. Firmware: Controller firmware is remotely upgradable from server software for added functionality, features and patches.

aa. Anti-passback: Local anti-passback, independent of software.

bb. Labels: Controller inputs/outputs are physically labeled with default usages, buttons and panel model are also labeled.

cc. Operating Temperature: 0 degrees Celsius to 50 degrees Celsius.

dd. Operating Humidity: 10% to 90% relative humidity, non-condensing.

ee. Expandable modular design.

ff. PCB Dimensions: 19.6 cm (W) X 7.4cm (H) (7.716” X 2.913”).

gg. Enclosure Dimensions: 29.9 cm (W) X 8.8 cm (H) X 5.93 cm (D) (11.7”X3.46”X2.33”).

hh. Enclosure Color: Black or White.

2. 2 Door Controller: POE-TDM

a. Supports 2 readers (1 for each door).

b. Power input: IEEE 802.3af PoE standard provides up to 15.4 Watts.

c. Processor: 32-Bit Microprocessor-Based.

d. Storage:

1) Up to 100,000 users/cardholders per controller.

2) 50,000 event storage onboard.

e. Terminals: Quick disconnect terminal headers.

f. Reader Communications:

1) 2 x Wiegand Data1/Data0, with optional LED and buzzer control.

2) LED Indicator: 2 x Reader active indicators.

g. Lock Power 1:

1) Solid State Wet Relay 12VDC @ 500mA / 24VDC @ 250 mA (with opt. Converter).

2) LED Indicator:1 X Lock Power LED.

h. Lock Power 2:

1) Solid State Relay 60V (TVS circuit limits 24V), 500mA, fully configurable, no mechanical parts. Requires external lock power for second strike or draw power from Auxiliary Power.

2) Dry contact.

3) LED Indicator: 1 x output indicator.

i. Relay Outputs:

1) 1 X Solid State Relay 60V (TVS circuit limits 24V), 500mA.

2) Fully configurable, no mechanical parts.

3) Dry Contact.

4) LED Indicator: 1 x output indicator.

j. Relay Output Devices: Fully configurable to work with the following devices:

1) Door strike

2) Magnetic Lock (use external relay or dry contact module)

3) Door opener

4) External buzzer

5) External alarm systems (arming/disarming)

6) Gates

7) Aux devices that will accept dry contact input.

8) Man trap devices (door open or unlocked)

k. Inputs: 4 Dry contact inputs, fully configurable including supervised or digital input setting.

l. Input Functions include:

1) Request to exit

2) Door contact

3) Door opener to enter (require card)

4) Door opener to exit

5) External motion sensor

6) Emergency alarm

7) External alarm status (check if alarm system is armed)

8) Door prevent unlock (used with mantraps)

m. Auxiliary Power: 12VDC @ 450mA without readers. (Used to power motion devices, Piezo's, etc.) Current shared with two reader ports, may be used to power second door strike, but may not work depending on current draw from reader ports.

n. Reader Formats: Magnetic stripe, Biometric, Bar code, and Wiegand format up to 64 bit.

o. Networking:

1) 10/100Mbps supporting Static or DHCP modes with 2 Ethernet status LED's.

2) On board HTTP interface for diagnostics and remote IP configuration. Secured by configurable password and can be disabled.

3) LED Indicator: 2 x PoE power indicator

4) 256 bit AES encryption between Panel and Server (optional)

p. Security: Hardware secured by configurable password.

q. Tamper Sensor: Photo tamper sensor (configurable) (no moving parts).

r. Display:

1) 2 Line x 16 Character LCD Display with LED back light used for on-board diagnostics and initial configuration such as IP address and communication modes.

2) Contrast adjustable.

3) Brightness adjustable.

s. Keyboard: Four user push buttons for data entry or output selection.

t. Sound: On-board piezo buzzer (90dB at 10cm) for the following functions:

1) Sounding alarm during forced open event.

2) Sounding alarm during held open event.

3) Feedback when arming/disarming external alarm systems.

4) Configurable to play sound when door opens.

5) External buzzer can be used.

u. Diagnostics: Several on board diagnostics available including the following:

1) Reader Test:

a) Ability to test if the reader on port 1 or 2 is able to read a card, and shows bit format, facility code and card number on LCD display.

2) Output Test:

a) Ability to manually trigger each of the 3 solid state relays, used to test that output devices such as door strikes are wired up correctly.

3) Input Test:

a) Ability to test each dry contact input for changes.

b) Indicator and audible alert if an input state changes.

c) Used to test input devices such as door contacts, REX, and auto opener buttons are wired correctly.

4) Ping with IP:

a) Ability to perform a basic network connectivity test by communicating with the server IP via ICMP protocol.

5) Ping with Name:

a) Ability to perform a basic network connectivity test by communicating to the server by resolving the name of the server via a Dynamic Name Service(DNS).

6) Debug mode:

a) Optional debug mode that allows extra logging of communications and panel decisions.

7) Read Only mode: Displays controller configuration and miscellaneous information

a) Panel Name

b) Area name (anti-passback)

c) Panel ID

d) IP Address

e) Panel MAC Address

f) Panel Subnet Mask

g) Panel Gateway

h) Panel DNS

i) Communication mode

j) Server IP Address/Name

k) Server Port

l) Firmware Version

m) Network Name

n) Door State

o) Door Mode

p) DHCP Bound address

q) Time (UTC and Local)

r) Connection Status

v. On-board Communication Configuration:

1) Ability to configure communication method to server (name or IP address).

2) Ability to configure name or IP address that the server can be reached.

3) Ability to configure network settings of controller, including:

a) Static IP address or DHCP

b) Controller IP Address, subnet mask, default gateway, DNS server.

w. Motion PIR (optional):

1) PIR motion sensor mounted on bottom of unit for authorizing exit without card read.

2) Configurable to unlock the door upon motion detection.

3) Sensitivity fully configurable via software.

x. Time: Keeps up to 1 month without power connection, No battery needed. Automatic DST switch.

y. Firmware: Controller firmware is remotely upgradable from server software for added functionality, features and patches.

z. Anti-passback: Local anti-passback, independent of software.

aa. Labels: Controller inputs/outputs are physically labeled with default usages, buttons and panel model are also labeled.

bb. Operating Temperature: 0 degrees Celsius to 50 degrees Celsius.

cc. Operating Humidity: 10% to 90% relative humidity, non-condensing.

dd. Expandable modular design.

ee. PCB Dimensions: 19.6 cm (W) X 7.4cm (H) (7.716” X 2.913”).

ff. Enclosure Dimensions: 29.9 cm (W) X 8.8 cm (H) X 5.93 cm (D) (11.7”X3.46”X2.33”).

gg. Enclosure Color: Black or White.

3. Elevator Master Panel: POE-ELEV-M

a. Supports 2 Readers (1 per cab)

b. Power input: IEEE 802.3af PoE(Power over Ethernet) standard(15.4W) or PoE+ power

c. Processor: Processor: 32-bit microprocessor

d. Storage:

1) Up to 50,000 users

2) 50,000 events (on board)

e. Terminals: Quick disconnect terminal headers.

f. Reader Communications:

1) 2 x Wiegand Data1/Data0, with optional LED and buzzer control.

2) LED Indicator: 2 x Reader active indicators.

g. Auxiliary Power: 12VDC @ 450mA without readers. (Used to power PRS-IO8 Board Elevator expander board) Current shared with two reader ports.

h. Reader power: 12VDC @ 450mA max shared across both reader port and Auxiliary 12VDC output.

i. Reader Formats: Magnetic stripe, Biometric, Bar code, and Wiegand format up to 64 bit.

j. Communications: On board RS485 via RS-485 module SE-X02 to up to 8 Elevator Expander Board.

k. Networking:

1) 10/100Mbps supporting Static or DHCP modes with 2 Ethernet status LED's.

2) LED Indicator: 2 x PoE power indicator

3) 256 bit AES encryption between Panel and Server (optional)

l. Security: Hardware secured by configurable password.

m. Tamper Sensor: Photo tamper sensor (configurable) (no moving parts).

n. Display:

1) 2 Line x 16 Character LCD Display with LED back light used for on-board diagnostics and initial configuration such as IP address and communication modes.

2) Contrast adjustable.

3) Brightness adjustable.

o. Keyboard: Four user push buttons for data entry or output selection.

p. Sound: On-board piezo buzzer (90dB at 10cm).

q. Diagnostics: Several on board diagnostics available including the following:

1) Reader Test:

a) Ability to test if the reader on port 1 or 2 is able to read a card, and shows bit format, facility code and card number on LCD display.

2) Ping with IP:

a) Ability to perform a basic network connectivity test by communicating with the server IP via ICMP protocol.

3) Ping with Name:

a) Ability to perform a basic network connectivity test by communicating to the server by resolving the name of the server via a Dynamic Name Service(DNS).

4) Debug mode:

a) Optional debug mode that allows extra logging of communications and panel decisions.

5) Read Only mode: Displays controller configuration and miscellaneous information

a) Panel Name

b) Panel ID

c) IP Address

d) Panel MAC Address

e) Panel Subnet Mask

f) Panel Gateway

g) Panel DNS

h) Communication mode

i) Server IP Address/Name

j) Server Port

k) Firmware Version

l) Network Name

m) DHCP Bound address

n) Time (UTC and Local)

o) Connection Status

r. On-board Communication Configuration:

1) Ability to configure communication method to server (name or IP address).

2) Ability to configure name or IP address that the server can be reached.

3) Ability to configure network settings of controller, including:

a) Static IP address or DHCP

b) Controller IP Address, subnet mask, default gateway, DNS server.

s. Time: Keeps up to 1 month without power connection, No battery needed. Automatic DST switch.

t. Firmware: Controller firmware is remotely upgradable from server software for added functionality, features and patches.

u. Elevators:

1) Ability to support up to 4 Cabs per master panel.

2) Ability to support up to to 64 Floors per master panel (with 8 Expander Boards)

3) Up to 2 readers.

4) Ability to support Button Sensing or Non-Button Sensing.

v. Elevator Time Zones:

1) User:

a) Ability to support 254 user time zones: 4 zones (9 boundaries) per day.

b) Ability to support 50 user holiday time zone groups, each has 50 holidays, each user holiday time zone: 2 zones (5 boundaries) per day

2) Floor:

a) Ability to support 64 (unlimited) floor time zones, 4 zones (9 boundaries) per day.

b) Ability to support 8 floor holiday time zone groups, each has 50 holidays, each floor holiday time zone : 2 zones (5 boundaries) per day.

c) Ability to support 64 one time run time zones (ad-hock).

w. Operating Temperature: 0 degrees Celsius to 50 degrees Celsius.

x. Expandable modular design.

y. PCB Dimensions: 19.6 cm (W) X 7.4cm (H) (7.716” X 2.913”).

z. Enclosure Dimensions: 21.6cm(W) X 26.0cm(H) x 8.30cm (8.5" x 10.25" x 3.25").

aa. Enclosure Color: Blue can

4. **IO-Master Panel: POE-IO-M**

a. Power input: IEEE 802.3af PoE(Power over Ethernet) standard(15.4W) or PoE+ power

b. Processor: Processor: 32-bit microprocessor

c. Storage:

1) 50,000 events (on board)

d. Terminals: Quick disconnect terminal headers.

e. Auxiliary Power: 12VDC @ 450mA. (Used to power PRS-IO8 Board Elevator expander board) Current shared with two reader ports.

f. Communications: On board RS485 via RS-485 module SE-X02 to up to 8 IO Expander Boards.

g. Networking:

1) 10/100Mbps supporting Static or DHCP modes with 2 Ethernet status LED's.

2) LED Indicator: 2 x PoE power indicator

3) 256 bit AES encryption between Panel and Server (optional)

h. Security: Hardware secured by configurable password.

i. Tamper Sensor: Photo tamper sensor (configurable) (no moving parts).

j. Display:

1) 2 Line x 16 Character LCD Display with LED back light used for on-board diagnostics and initial configuration such as IP address and communication modes.

2) Contrast adjustable.

3) Brightness adjustable.

k. Keyboard: Four user push buttons for data entry or output selection.

l. Sound: On-board piezo buzzer (90dB at 10cm).

m. Diagnostics: Several on board diagnostics available including the following:

1) Ping with IP:

a) Ability to perform a basic network connectivity test by communicating with the server IP via ICMP protocol.

2) Ping with Name:

a) Ability to perform a basic network connectivity test by communicating to the server by resolving the name of the server via a Dynamic Name Service(DNS).

3) Debug mode:

a) Optional debug mode that allows extra logging of communications and panel decisions.

4) Read Only mode: Displays controller configuration and miscellaneous information

a) Panel Name

b) Panel ID

c) IP Address

d) Panel MAC Address

e) Panel Subnet Mask

f) Panel Gateway

g) Panel DNS

h) Communication mode

i) Server IP Address/Name

j) Server Port

k) Firmware Version

l) Network Name

m) DHCP Bound address

n) Time (UTC and Local)

o) Connection Status

n. On-board Communication Configuration:

1) Ability to configure communication method to server (name or IP address).

2) Ability to configure name or IP address that the server can be reached.

3) Ability to configure network settings of controller, including:

a) Static IP address or DHCP

b) Controller IP Address, subnet mask, default gateway, DNS server.

o. Time: Keeps up to 1 month without power connection, No battery needed. Automatic DST switch.

p. Firmware: Controller firmware is remotely upgradable from server software for added functionality, features and patches.

q. IO-Boards:

1) Ability to support up to to 64 Inputs and Outputs per master panel (with 8 Expander Boards)

r. Input / Output Time Zones:

1) Input:

a) Ability to support 16 Input time zones: 2 zones (5 boundaries) per day.

b) Ability to support 16 holiday groups, each has 50 holidays, each Input holiday time zone: 2 zones (5 boundaries) per day

2) Output:

a) Ability to support 64 Output time zones, 5 zones (11 boundaries) per day.

b) Ability to support 8 holiday groups, each has 50 holidays, each Output holiday time zone: 2 zones (5 boundaries) per day.

s. Input / Output Functions:

1) Ability to place an Input on a schedule

2) Ability to assign an Input to a holiday group

3) Ability to place a detection time on an Input

4) Ability to assign an action to an Input

5) Input Actions:

a) Do Nothing

b) Activate Selected Output

c) Deactivate Selected Output

d) Toggle Selected Output

e) Pulse Selected Output (high)

f) Pulse Selected Output (low)

g) Pulse Selected Output (opposite)

h) Activate Multiple Outputs (up to 5)

i) Deactivate Multiple Outputs (up to 5)

j) Toggle Multiple Outputs (up to 5)

6) Ability to place a delay on any Input Actions

7) Ability to place an action duration for pulses

8) Ability to configure an Input as Normally Closed

9) Ability to place an Output on a schedule

10) Ability to assign an Output to a holiday group

11) Ability to configure an Output as Normally Closed

12) Ability to configure an Output to not generate any events

13) Ability to protect an Output from Input Actions

14) Ability to configure an Output to be initially On

t. Operating Temperature: 0 degrees Celsius to 50 degrees Celsius.

u. Expandable modular design.

v. PCB Dimensions: 19.6 cm (W) X 7.4cm (H) (7.716” X 2.913”).

w. Enclosure Dimensions: 21.6cm(W) X 26.0cm(H) x 8.30cm (8.5" x 10.25" x 3.25").

x. Enclosure Color: Blue can

5. Elevator Expander Board: PRS-IO8 Board

a. Processor: Processor: 32-bit microprocessor

b. Power Input:12VDC supplied by Elevator/IO Master Panel, no external power needed.

c. Configuration: 8 Dip switches for inputting addressing and diagnostics.

d. Communication: RS-485 (2-wire communication) Multidrop (Daisy Chain or Star) via SE-EX02 Module.

e. Inputs:

1) 8 x dry contact inputs. Fully configurable.

2) LED Indicator: 1 x Input activity indicator.

f. Outputs:

1) 8 dry contact Solid State Relays. Fully configurable.

2) Capable of switching up to 60V,500mA limit. Other relay options available.

3) LED Indicator: 8 x output status indicator.

4) Field replaceable solid state relays.

g. Tamper: Each IO panel has individual photo-tamper sensor. Fully configurable.

h. Diagnostics: Input / Output test mode, activated through DIP switch configuration.

i. Terminals: Quick disconnect terminal headers.

j. PCB Dimensions: 9.5 cm (W) X 9.5 cm (H) (3.740" X 3.740").

6. Communication Converter: RS-485 module SE-X02

a. Power Input: From ODM /TDM

b. LED Indicators: 1 Data Receive, 1 Data Send.

c. Terminals: Quick disconnect terminals, connects to expander module on ELEV-M, IO-M Master Panel or APERIO-(2 or 4 or 8).

d. PCB Dimensions: 4.5 cm (W) X 1.5 cm (H) (1.771" X 0.590").

e. Warranty: 2 year, Limited.

7. Anti-passback plug in module HC-APB-MEM:

a. Power: From ODM /TDM

b. Memory Size: 512KB

c. LED: Power indicator

d. Application: Anti Pass Back for ODM/TDM

e. PCB Dimensions: 1.8 cm (W) x 1.4 cm (H) (0.708" X 0.551")

8. Lock power 12V to 24V convertor plug in module HC-24VCB01:

a. Input: 12VDC

b. Output: 24VDC

c. Current Max: 1.2A

d. Conversion Efficiency: 90%

e. Application: ODM Lock Power conversion. 12V, 550mA to 24V, 245mA

f. PCB Dimensions: 2.1 cm (W) x 1.1 cm (H) (0.826" X 0.433")

9. Lock power to Dry Contact convertor plug in module HC-DRYMOD:

a. Input: 12VDC

b. Output: Dry Contact

c. Current Max: 2A (5A available)

d. Voltage Max: 220 VAC/VDC

e. Application: Mag locks or high voltage devices such as lighting systems

f. PCB Dimensions: 2.1 cm (W) x 1.1 cm (H) (0.826” X 0.433”)

10. Wi-FI Enabled PoE Injector Wi-Fi-ModPOE:

a. Input: 100-240VAC

b. Output: 48VDC

c. Current Max: 0.42A

d. Application: PoE injector with built in wireless router provides capability to connect a controller to an IP network via wireless and provide PoE power.

e. CPU nominal frequency: 400 MHz

f. Size of RAM: 64 MB

g. 10/100 Ethernet ports: 2

h. Wireless standards: 802.11b/g/n

i. Operating System: RouterOS

j. Antenna gain DBI: 1.2

k. Dimensions: 68mm x 68mm x 19 mm

11. Mullion Mount Proximity Access Reader HC-PROX3:

a. Dimensions: 38 mm (W) X 114 mm (H) X 19 mm (D) (1.6” X 4.5” X 0.75”).

b. Design: Indoor / Outdoor; Weatherproof (IP67 rated); external Piezo beeper.

c. Characteristics: High reliability; consistent read range characteristics; low power consumption; vandal-resistant.

d. Colors: Available in Black

e. Features: Multicolor LED indicator - Red, Green, Amber, and Off.

f. Mounting: Mullion or Single Gang via removable back plate, can be mounted directly to metal.

g. Communication format: High Security 40 bit, AWID, HID

h. Frequency: 125 kHz excitation

i. Read Range: up to 6 inches (152 mm); credential type dependent.

j. Operating Temperature: -40°F to +149°F (-40° C to +65° C)

k. Current Draw: 45mA typical, 80mA peak @ 12VDC

l. Compliance: CSA, UL, FCC, CE, C-Tick.

m. Warranty: Limited Lifetime (as per manufacturer).

12. High Security Vandal Resistant Proximity Access Reader HC-P403 Mullion:

a. Dimensions: 51 mm (W) x 133 mm (H) x 25 mm (D) (2” X 5.25” X 1.”).

b. Design: Indoor / Outdoor; Weatherproof (IP67 rated); external Piezo beeper; Vandal resistant; solid polycarbonate construction.

c. Characteristics: High reliability; consistent read range characteristics; low power consumption.

d. Colors: Black only

e. LED: Multicolor LED indicator - Red, Green, Amber, and Off.

f. Mounting: May be mounted directly to metal.

g. Communication format: High Security 40 bit, AWID, HID

h. Frequency: 125 kHz excitation

i. Read Range: up to 5 inches (126 mm); credential type dependent.

j. Operating Temperature: -40°F to +149°F (-40° C to +65° C).

k. Current Draw: 30mA typical; 75mA peak @ 12VDC

l. Compliance: FCC, CE, C-Tick, IC

m. Warranty: Limited Lifetime (as per manufacturer).

13. High Security Vandal Resistant Proximity Access Reader HC-P405 Single Gang:

a. Dimensions: 76 mm (W) x 114 mm (H) x 25 mm (D) (3.” X 4.5” X 1.”).

b. Design: Indoor / Outdoor; Weatherproof (IP67 rated); external Piezo beeper; Vandal resistant; solid polycarbonate construction.

c. Characteristics: High reliability; consistent read range characteristics; low power consumption.

d. Colors: Black only

e. LED: Multicolor LED indicator - Red, Green, Amber, and Off.

f. Mounting: May be mounted directly to metal.

g. Communication format: High Security 40 bit, AWID, HID

h. Frequency: 125 kHz excitation

i. Read Range: up to 6 inches (152 mm); credential type dependent.

j. Operating Temperature: -40°F to +149°F (-40° C to +65° C).

k. Current Draw: 30mA typical; 75mA peak @ 12VDC

l. Compliance: FCC, CE, C-Tick, IC

m. Warranty: Limited Lifetime (as per manufacturer).

14. High Security Vandal Resistant Proximity Access Reader HC-P453 Mullion:

a. Dimensions: 51 mm (W) x 133 mm (H) x 25 mm (D) (2” X 5.25” X 1”).

b. Design: Indoor / Outdoor : Weatherproof (IP67 rated); external Piezo beeper; Vandal resistant; Stainless Steel and Fiber-Tex UL752 bulletproof construction.

c. Characteristics: High reliability; consistent read range characteristics; low power consumption; vandal-resistant.

d. Colors: Stainless Steel and Fiber-tex.

e. LED: Multicolor LED indicator - Red, Green, Amber, and Off

f. Mounting: May be mounted directly to metal.

g. Communication format: High Security 40 bit, AWID, HID

h. Frequency: 125 kHz excitation

i. Read Range: up to 1 inch (25 mm); credential type dependent.

j. Operating Temperature: -40°F to +149°F (-40° C to +65° C).

k. Current Draw: 30mA typical; 75mA peak @ 12VDC.

l. Compliance: FCC, CE, C-Tick, IC

m. Warranty: Limited Lifetime (as per manufacturer).

15. High Security Vandal Resistant Proximity Access Reader HC-P455 Single Gang:

a. Dimensions: 76 mm (W) x 114 mm (H) x 25 mm (D) (3” X 4.5” X 1”).

b. Design: Indoor / Outdoor : Weatherproof (IP67 rated); external Piezo beeper; Vandal resistant; Stainless Steel and Fiber-Tex UL752 bulletproof construction.

c. Characteristics: High reliability; consistent read range characteristics; low power consumption;

vandal-resistant.

d. Colors: Stainless Steel and Fiber-tex.

e. LED: Multicolor LED indicator - Red, Green, Amber, and Off

f. Mounting: May be mounted directly to metal.

g. Communication format: High Security 40 bit, AWID, HID

h. Frequency: 125 kHz excitation

i. Read Range: up to 1 inch (25 mm); credential type dependent.

j. Operating Temperature: -40°F to +149°F (-40° C to +65° C).

k. Current Draw: 30mA typical; 75mA peak @ 12VDC.

l. Compliance: FCC, CE, C-Tick, IC

m. Warranty: Limited Lifetime (as per manufacturer).

16. Keypad & Proximity Combo Access Reader HC-640 Single Gang:

a. Dimensions: 76 mm (W) X 117 mm (H) X 19 mm (D) (3" X 4.6" X 0.75").

b. Design: Indoor / Outdoor : Weatherproof (IP67 rated); external Piezo beeper

c. Characteristics: Uses non-mechanical capacitive technology (no moving parts), blue backlit; high reliability; consistent read range characteristics; low power consumption; vandal-resistant.

d. Colors: Available with Black or Off-White snap-on cover.

e. Features: Multicolor LED indicator - Red, Green, Amber, and Off.

f. Mounting: Wall-single gang box, or may be mounted directly to metal.

g. Communication format: High Security 40 bit, AWID, HID

h. Keypad output: Wiegand or 8-Bit Burst Mode configurable

i. Frequency: 125 kHz excitation

j. Read Range: up to 7 inches (178 mm); credential type dependent.

k. Operating Temperature: -40°F to +149°F (-40° C to +65° C).

l. Current Draw: 70mA typical, 110mA peak @ 12VDC.

m. Compliance: FCC, CE, C-Tick. IC, UL294

n. Warranty: Limited Lifetime (as per manufacturer).

17. Long Range Proximity Access Reader HC-P710 Single Gang:

a. Dimensions: 152 mm (W) x 216 mm (H) x 25 mm (D) (6" X 8.5" X 1").

b. Design: Indoor / Outdoor : Weatherproof (IP67 rated); external Piezo beeper.

c. Characteristics: High reliability; consistent read range characteristics; low power consumption; vandal-resistant.

d. Colors: Black

e. Features: Multicolor LED indicator - Red, Green, Amber, and Off.

f. Mounting: Wall-single gang box, or non-metallic flat surfaces.

g. Communication format: High Security 40 bit, AWID, HID.

h. Frequency: 125 kHz excitation

i. Read Range: Up to 15 inches (381 mm); credential type dependent.

j. Operating Temperature: -40°F to +149°F (-40° C to +65° C).

k. Current Draw: 215mA typical, 350mA peak @ 12VDC.

l. 1ompliance: FCC, CE, C-Tick, IC, UL294.

m. Warranty: Limited Lifetime (as per manufacturer).

18. Long Range Single Gang Access Reader HC-P900:

a. Dimensions: 267 mm (W) X 267 mm (H) X 53 mm (D) (10.5” X 10.5” x 2”).

b. Design: Indoor / Outdoor : Weatherproof (IP67 rated); external Piezo beeper.

c. Characteristics: High reliability; consistent read range characteristics; low power consumption; vandal-resistant.

d. Colors: Black

e. Features: Multicolor LED indicator - Red, Green, Amber, and Off.

f. Mounting: US-size metal or plastic single or double gang wall box, standard parking bollard X-mounts or non-metallic flat surfaces.

g. Communication format: High Security 40 bit, AWID, HID.

h. Frequency: 125 kHz excitation

i. Read Range: Up to 20 inches (up to 504 mm); credential type dependent.

j. Operating Temperature: -40°F to +149°F (-40° C to +65° C).

k. Current Draw: 290mA typical, 500mA peak @ 12VDC.

l. Compliance: FCC, CE, C-Tick, IC, UL294

m. Warranty: Limited Lifetime (as per manufacturer).

19. Clamshell Proximity Card HC-PSC1:

a. Dimensions: 86 mm (W) X 56 mm (H) X 1.5 mm (D) (3.4” X 2.2” X 0.06”).

b. Frequency: 125 kHz excitation.

c. Operation: Passive (no battery)

d. Communication format: High Security 40 bit.

e. Read Range: up to 8 inches (203 mm)

f. Operating Temperature: -35°F to +122°F (-37° C to +50° C).

g. Humidity: 0-95% non-condensing

h. Material: ABS Clamshell

i. Color: Off-white

j. Slot Punch: Vertical

k. Compliance: CSA, UL, FCC, CE, C-Tick.

l. Warranty: Limited Lifetime warranty (as per manufacturer).

20. Proximity Key Tag HC-PSK3:

a. Dimensions: 38 mm (W) X 30 mm (H) X 3.8 mm (D) (1.5” X 1.2” X 0.15”)

b. Frequency: 125 kHz excitation.

c. Operation: Passive (no battery)

d. Communication format: High Security 40 bit.

e. Read Range: up to 3.5 inches (88 mm)

f. Operating Temperature: -35°F to +122°F (-37° C to +50° C).

g. Humidity: 0-95% non-condensing

h. Material: ABS

i. Color: Light Grey

j. Slot Punch: Std. reinforced brass eyelet

k. Compliance: CSA, UL, FCC, CE, C-Tick.

l. Warranty: Limited Lifetime warranty (as per manufacturer).

21. Image Technology Proximity Card HC-PSI4 (46 MIL):

a. Dimensions: 86 mm (W) X 53 mm (H) X 1.17 mm (D) (3.4” X 2.1” X 0.046”).

b. Printing Surface Imaging: Appropriate for direct color dye sublimation printing of images and text.

c. Frequency: 125 kHz excitation.

d. Operation: Passive (no battery)

e. Communication format: High Security 40 bit.

f. Read Range: up to 7 inches (176 mm)

g. Operating Temperature: -35°F to +122°F (-37° C to +50° C).

h. Humidity: 0-95% non-condensing.

i. Material: PVC

j. Color: Glossy white

k. Slot Punch: Vertical and horizontal indicators

l. Compliance: CSA, UL, FCC, CE, C-Tick.

m. Warranty: Limited Lifetime warranty (as per manufacturer).

22. Image Technology Proximity Card HC-PSM-2P (31 MIL):

a. Dimensions: 86 mm (W) X 53 mm (H) X 0.79 mm (D) (3.4” X 2.1” X 0.031”).

b. Printing Surface Imaging: Appropriate for direct color dye sublimation printing of images and text.

c. Frequency: 125 kHz excitation.

d. Operation: Passive (no battery)

e. Communication format: High Security 40 bit.

f. Read Range: up to 7 inches (176 mm)

g. Operating Temperature: -35°F to +122°F (-37° C to +50° C).

h. Humidity: 0-95% non-condensing..

i. Material: PVC

j. Color: Glossy white

k. Slot Punch: Vertical

l. Compliance: CSA, UL, FCC, CE, C-Tick.

m. Warranty: Limited Lifetime warranty (as per manufacturer).

23. Image Technology Multi-Tech Proximity Card HC-PSM-2S (31 MIL):

a. Dimensions: 86 mm (W) X 53 mm (H) X 0.79 mm (D) (3.4” X 2.1” X 0.031”).

b. Printing Surface Imaging: Appropriate for direct color dye sublimation printing of images and text.

c. Frequency: 125 kHz excitation.

d. Includes 2750 Oe HiCo Magnetic stripe for ABA Track II Clock and Data

e. Operation: Passive (no battery)

f. Communication format: High Security 40 bit.

g. Read Range: up to 7 inches (176 mm)

h. Operating Temperature: -35°F to +122°F (-37° C to +50° C).

i. Humidity: 0-95% non-condensing..

j. Material: PVC

k. Color: Glossy white

l. Slot Punch: Vertical

m. Compliance: CSA, UL, FCC, CE, C-Tick.

n. Warranty: Limited Lifetime warranty (as per manufacturer).

24. Proximity Disc Tag HC-PDT1:

a. Dimensions: 25.4 mm diameter x 1.6 mm thick (1” dia. x 0.0625”)

b. Frequency: 125 kHz excitation.

c. Operation: Passive (no battery)

d. Communication format: High Security 40 bit.

e. Read Range: up to 3.5 inches (88 mm)

f. Operating Temperature: -40°F to +149°F (-40° C to +65° C).

g. Humidity: 0-95% non-condensing

h. Material: PVC with strong adhesive backing

i. Color: Glossy White

j. Compliance: CSA, UL, FCC, CE, C-Tick.

k. Warranty: Limited Lifetime warranty (as per manufacturer).

25. Long Range Wireless RF Receiver HC-WRR-44:

a. Dimensions: 86 mm (W) X 160 mm (H) X 58 mm (D) (3.4” X 6.3” X 2.3”).

b. Design: Indoor / Outdoor; Weatherproof (IP65 rating)

c. Characteristics: High reliability, long read range, encrypted rolling code + encryption transmission.

d. Read Range: Up to 200 feet (61 m), installer adjustable, up to 4 Wiegand channels.

e. Colors: Off White

f. Frequency: 433 MHz

g. Features: Multicolor LED indicator - Red, Green, Amber and Off.

h. Mounting: Wall-single gang box, or non-metallic flat surfaces.

i. Operating Temperature: -40°F to +149°F (-40° C to +65° C).

j. Current Draw: 120 mA typical @ 12 VDC

k. Compliance: FCC, IC, CE, C-Tick, UL294

l. Warranty: Limited 12 months (as per manufacturer).

26. Long Range Wireless RF Receiver HC-WRR-22:

a. Dimensions: 84 mm (W) X 84 mm (H) X 48.3 mm (D) (3.3” X 3.5” X 1.9”).

b. Design: Indoor / Outdoor; Weatherproof (IP65 rating)

c. Characteristics: High reliability, long read range, encrypted rolling code + encryption transmission.

d. Read Range: Up to 100 feet (30 m), fixed range, up to 2 Wiegand channels.

e. Colors: Off White

f. Frequency: 433 MHz

g. Features: Multicolor LED indicator-Red, Green, Amber and Off.

h. Mounting: Wall-single gang box, or non-metallic flat surfaces.

i. Operating Temperature: -40°F to +149°F (-40° C to +65° C).

j. Current Draw: 80 mA typical @ 12 VDC

k. Compliance: FCC, IC, CE, C-Tick, UL294

l. Warranty: Limited 12 months (as per manufacturer).

27. Two Button Wireless RF Transmitter and integrated Proximity Credential HC-WRT2:

a. Dimensions: 37 mm (W) X 63.5 mm (H) X 14.2 mm (D) (1.45” X 2.5” X 0.56”).

b. Design: Weather-resistant (IP65 rating), 2-button

c. Characteristics: High reliability, long transmission range, rolling code + encrypted algorithm for secure transmission.

d. Communication format: High Security 40 bit.

e. Colors: Black polycarbonate with gray ABS buttons

f. Frequency: 433 MHz

g. LED: Red LED standard (activated upon button press).

h. Read Range:

1) Button press up to 200 feet (61 m) using HC-WRR44 receiver

2) Proximity presentation up to 3.5 inches (88 mm)

i. Operating Temperature: -40°F to +122°F (-40° C to +50° C).

j. Battery: Single replaceable CR2032 3.3V lithium battery

k. Compliance: FCC, IC, CE, C-Tick, UL294.

l. Warranty: Limited 1 year (as per manufacturer).

28. Four Button Wireless RF Transmitter and Integrated Proximity Credential HC-WRT4:

a. Dimensions: 37 mm (W) X 63.5 mm (H) X 14.2 mm (D) (1.45” X 2.5” X 0.56”).

b. Design: Weather-resistant (IP65 rating), 4-button.

c. Characteristics: High reliability, long read range, rolling code + encrypted algorithm for secure transmission.

d. Communication format: High Security 40 bit.

e. Colors: Black polycarbonate with gray ABS buttons

f. Frequency: 433 MHz

g. LED: Red LED standard (activated upon button press).

h. Read Range:

1) Button press up to 200 feet (61 m) with HC-WRR44 Receiver

2) Proximity presentation up to 3.5 inches (88 mm)

i. Operating Temperature: -40°F to +122°F (-40° C to +50° C).

j. Battery: Single replaceable CR2032 3.3V lithium battery

k. Compliance: FCC, IC, CE, C-Tick, UL294.

l. Warranty: Limited 1 year (as per manufacturer).

1.8 SOFTWARE FEATURES AND FUNCTIONS

Specifier Note: The access control software modules consist of many functions and they need to be specified here. These software modules are required to activate the system component functions.

A. Server Software:

39. Shall be installed on a standard PC running Microsoft Windows 7 Home or Higher (Windows 7 Starter Not Supported) or purchased via an embedded hardware server box.
40. Shall support Microsoft SQL Server 2008 or SQL Server 2008 Express or newer.
41. Shall be 100% web based and can be accessed via any web enabled device including Cell Phones, Tablets, Laptops, P.C.'s with any operating system etc. without the need for any additional plug in's, i.e. no active x controls, Flash, etc. Supported browsers include the following:
    a. Google Chrome (desktop and mobile).
    b. Microsoft Internet Explorer.
    c. Mozilla Firefox.
    d. Apple Safari (desktop and mobile)
    e. Other browsers that support HTML5 may function, but are untested.
42. Web interface and controller communications shall be possible through WAN/LAN if network allows.
43. Software design shall be of a Single Page Application (SPA) architecture allowing seamless navigation between screens.
44. Shall have a responsive web interface. Interface will automatically adjust to ensure an optimal experience based on device.
45. Ability to Partition software for multisite all hosted from one location allowing site administrators only access to their site readers and cards or multiple sites.
46. Shall have functions that will be accessed via tool bar Icons, which will include help prompts that will appear when the mouse pointer hovers over the selection button.
47. Shall be possible to install the server software in a virtualized environment.
48. Communication shall use SSL encryption with modern cryptography, utilizing TLS 1.2, and AES 128 GCM/DHE RSA as the key exchange mechanism.
49. Software shall advise when a software update is available and who to contact in order to upgrade.
50. Software shall utilize a smart installer, capable of the following functions:
    a. Analyze if installation prerequisites are met.
    b. If prerequisites are missing, installer will locate them on installation media or download from the internet.
    c. Automatically create SQL instance and database.

d. Automatically assign database permissions and setup service users.

e. Automatically add Windows Firewall exceptions for communication ports.

1) Web server, controller communication and management interface can be configured on alternate ports.

f. Installer is capable of upgrading the software.

g. Ability to configure different communication ports when installing the software.

h. Ability to configure web services to run as a different windows user.

51. Software shall have the capability to be run via command line for advanced troubleshooting.
52. Web interface shall utilize Gzip compression for reduced load times and bandwidth consumption.
53. Web interface shall utilize cache control for static files such as images, static text and cardholder images.
54. Software shall provide a unified interface for doors and elevators, including shared time schedules and access groups.

B. Administrator Control Capabilities:

55. Administrator interface shall be secured by encrypted hashed password control and SSL communication from web client to server.
56. System shall support unlimited administrator accounts.
57. Administrator can either be a system administrator or non-system administrator with customizable permissions.
58. Ability to reset administrator passwords via email.
59. Administrator actions and changes shall be logged and visible to other administrators via reporting tools.
60. Administrator Management: An Administrator’s privilege determines which functions can be accessed, and which Partitions can be accessed. The following functions are available.

a. Manage Access Privilege Groups

b. Manage Cameras and Integration

c. Manage Door Holiday Groups

d. Manage Door Holiday TimeZones

e. Manage Door TimeZones

f. Manage Doors

g. Manage Elevators

h. Manage Floor Holiday Groups

i. Manage Floor Holiday TimeZones

j. Manage Floor TimeZones

k. Manage Holidays

l. Manage OneTimeRun TimeZones

m. Manage Panels

n. Manage Sites

o. Manage User Holiday Groups

p. Manage User Holiday TimeZones

q. Manage User TimeZones

r. Manage Users

s. Reporting Alerts

t. Reporting Door Activity

u. Reporting Floor Activity

v. Reporting User Activity

w. Reporting User List

x. Override Door

y. Override Floor

z. Override Output

aa. Update Panel

bb. View Cameras

cc. View Status

61. System shall render functions that administrators do not have access to invisible and inaccessible.
62. Ability for administrators to configure personal settings the following functions:
    a. Customize which notifications are visible when viewing event monitoring
    b. Choose which events should be treated as alerts.
    c. Choose which events will prompt an email being sent to the administrator.
    d. Choose if alerts will activate a sound in the web browser.
    e. Choose which notifications will spawn in-line camera view of associated devices.
63. Ability to integrate administrator authentication with LDAP systems.

C. System Partitioning:

64. System shall support unlimited partitions (with appropriate licensing), which logically separate the system into pieces.
65. Administrators can be given permissions to manage specific aspects of a partition or multiple partitions.
66. Administrators shall only see partitions or parts of partitions they are explicitly given permission to manage.
67. Ability to assign user/cardholders to more than 1 partition, as long as the Administrator assigning access groups has permissions to manage cardholders within the desired partitions.
68. Administrators with limited permissions will not see the menus/icons for parts of the software they do not have permission to use.
69. Door and Elevator Panels shall be assigned to a single partition.
70. Holidays, schedules and Access groups shall not be shared between partitions.
71. Administrator shall not see events on devices they do not have permission to view/manage.

D. Credential/Cardholder Management:

72. Provide User/Cardholder management screen with unlimited number of users/cardholders (up to 50,000-100,000 per controller).
73. Provide simple cardholder enrollment, with all available cardholder options available on one screen.
74. Ability to assign multiple credentials to a single cardholder, including cards, pins, biometrics, ect.
75. Ability to assign a site code in the range of 1 – 65535 for a credential.
76. Ability to assign a card number in the range of 0 to 4294967295.
77. Ability to assign manually created pins numbers or allow the system to auto-generate Pin credentials.
78. Ability to assign additional user/cardholder attributes:
    a. Assign a Start date to a cardholder. Credentials assigned to the cardholder will not work before the start date.
    b. Assign a Stop date to a cardholder. Credentials assigned to the cardholder will not work after the stop date.

c. Assign a security level for crisis Level feature.

d. Assign the cardholder as a master user.

e. Assign the cardholder as a supervisor user.

f. Assign the cardholder the permission to activate First Person In schedules.

g. Assign the cardholder the ability to perform Triple Swipe Actions.

h. Assign the cardholder the ability to disarm an external alarm system.

i. Assign the cardholder the ability to open auto-openers without the use of a button.

79. Ability to view a list of all cardholders.
80. Capability of finding a specific card holder based on specified search criteria such as name or credentials.
81. Provide the ability to assign a photographic image for each Cardholder, image can be uploaded from local device or taken in the web browser with an image device. (Google Chrome only).
82. Assign up to three images to a cardholder, which appear on the notifications screen when a cardholder presents a credential.
83. Ability to assign to unlimited Access Privilege Groups.
84. Ability to assign cardholder to Access Privilege Groups across different Partitions.
85. Ability to assign cardholder directly to a Partition for later access assignment.
86. Ability to assign unlimited custom fields to a cardholder.
87. Ability to import large amounts of users/cardholders via CSV file.
88. System shall optionally disallow creation of Pin numbers that are too similar to other pin numbers automatically.

E. Access Privilege Groups:

89. Ability to create unlimited administrator definable/customizable Access Privilege Groups.
90. Ability to apply any combination of user time zones.
91. Apply to restrict/allow Cardholders movement through identified doors, at specific times, including holiday schedules.
92. Cardholders can be assigned to multiple access groups for enhanced customization.
93. Software shall have built in validation to prevent conflicts of users being given different permissions for the same doors/floors.
94. Ability to search for readers, floors and users when creating or modifying Access Privilege Groups.

F. Time Zone Management:

95. The system shall support separately definable time zones for user access (User Time Zone), door access (Door Time Zone) floor access (Floor Time Zone), Output mode (Output Time Zone), and Input monitoring (Input Time Zone).
96. The system Time Zones within the system shall support an easy to use graphical interface for creation and modification
97. The system time zones shall be color coded to the mode of the span for easy viewing and eliminating the chance of programming error.
98. Ability to provide a specific schedule name and description.
99. Ability to re-use time schedules across multiple devices.
100. Ability to replicate a schedule across multiple days via click and drag to weekdays, weekends, week.
101. Software shall create per-configured time schedules used in typical deployments.
102. Door Time Zones (door schedule):

a. Ability to support unlimited amount of Door Time Zones.

b. Ability to have 20 unlock/lock times per day.

c. Support 8 different Time Zone modes in any combination:

1) Ability to have Lockdown (no cards other than cards flagged as master will be granted access).

2) Ability to have Card Only (valid cards required to grant access).

3) Ability to have Pin Only (valid pins required to grant access).

4) Ability to have Card Or Pin (valid card or pin required for access).

5) Ability to have Card And Pin (valid card and pin required for access).

6) Ability to have Unlock (door is in public mode).

7) Ability to have “First Credential in” by card (door will not follow its public schedule until a card flagged with first card in feature is presented at the door during the public schedule).

8) Ability to have Dual Credentials (2 valid cards with an option to require the first card to have a supervisor privilege).

103. User Time Zone (user access schedule):

a. Ability to support up to 254 User Time Zone Schedules.

b. Ability to have 8 Allowed/Not Allowed time spans per day.

c. Support 2 different Time Zone modes in any combination:

1) Ability to have Allowed (user will be allowed through the door as long as the Door Time Zone is in a mode that accepts the type of credential being presented).

2) Ability to have Not Allowed (user will be denied access to the door).

104. Floor Time Zones (elevator floor schedule):

a. Ability to support unlimited Floor Time zone schedules the system will support.

b. Ability to have up to 8 time spans per day.

c. Support 3 different Time Zone modes in any combination:

1) Ability to have Card Only (valid cards required to grant access).

2) Ability to have Unlock (floor is in public mode).

3) Ability to have Lockdown (no cards other than cards flagged as master will be granted access).

105. Input Time Zones (Input schedule):

a. Ability to support unlimited Input Time zone schedules the system will support.

b. Ability to have up to 5 time spans per day.

c. Support 2 different Time Zone modes in any combination:

1) Ability to have Monitor (Input will be monitored during this span).

2) Ability to have Not Monitored (Input changes will be ignored).

106. Output Time Zones (Output schedule):

a. Ability to support unlimited Output Time zone schedules the system will support.

b. Ability to have up to 11 time spans per day.

c. Support 2 different Time Zone modes in any combination:

1) Ability to have On (Output relay will close during this span).

2) Ability to have OFF (Output relay will open during this span).

107. One Time Run Time Zones (elevator and doors):

a. Ability to create one time event schedules that can change the state and mode of a door or elevator floor for a period of time, can also span multiple days.

G. Holiday Management to Allow:

108. Ability to apply a specific schedule for groups of doors to follow when it is a holiday.
109. Ability to apply a specific user schedule for groups of users to follow during a holiday.
110. Ability to create a holiday with the following options:
    a. Date of the holidays.
    b. If the holiday is reoccurring annually.
    c. Name and description of the holiday.
    d. Which groups of doors will be affected by the holiday and what holiday time zone they will follow.
    e. Which groups of Access Privilege Groups will be affected by the holiday and what holiday time zone they will follow.
    f. Which groups of elevator floors will be affected by the holiday and what holiday time zone they will follow.
    g. Which groups of Inputs and outputs will be affected by the holiday and what holiday time zone they will follow.

H. Door Management to Allow:

111. Ability to apply a specific name and description to each door and reader.
112. Ability to apply a time zone to control when a specific door is to unlock/lock, accept cards, pins, etc.
113. Ability to apply a Holiday group to control how a specific door will behave on a Holiday.
114. Configure Door Held Open:
    a. Ability to disable Door Held Open alert.
    b. Ability to disable Held Open buzzer.
    c. Ability to configure how long a door can be held open before an alert is raised.
    d. Ability to configure if the held open alert/buzzer will stop once the door is closed.
115. Configure Forced Open:
    a. Ability to disable Door Forced Open alert.
    b. Ability to disable Forced Open buzzer.
    c. Ability to configure if the Forced Open alert/buzzer will stop once the door is closed.
116. Ability to configure an unlock delay.
117. Ability to configure how long the door will be unlocked after a valid credential presentation.
118. Configure if a motion device can unlock the door.
119. Ability to configure the controller to play a sound when the door opens.
120. Automatic Door Operator:
    a. Ability to enable/disable the use of an auto-opening device on a door.
    b. Ability to configure an unlock delay when using auto-opening device.
    c. Ability to configure the insecure side of the door to require a card read before auto-opener button will function.
    d. Ability to configure auto-opener to open with REX.
    e. Ability to configure auto-opener to open with motion.
121. Reader Configuration:
    a. Ability to apply a name and description to a reader.
    b. Ability to enable/disable keypad use on a reader.
    c. Ability to configure how many seconds between pin presses will pass before the credential becomes invalid.

d. Ability to configure back to back reader interference interval.

e. Ability to configure what area a reader is granting access to for use of tracking where users are in a building (used for muster and anti-passback).

f. Ability to configure Triple Swipe actions.

122. Local Anti-passback Configuration:

a. Ability to enable local anti-passback.

b. Ability to monitor door contact for passage through a door

c. Ability to configure soft or hard anti-passback

d. Ability to configure a timeout period for anti-passback.

e. Ability to exclude supervisor users from anti-passback limitations.

123. Video Integration:

a. Ability to create an association between a door and a camera(s).

b. Ability to view associated cameras from the doors page.

c. Ability to associate a predefined position to a camera if using PTZ camera.

124. Door Override:

a. Ability to deviate the state of the door from the normal schedule.

b. Ability to override a door until explicitly resuming the normal schedule.

c. Ability to override the state of a door and instruct the controller to resume the normal schedule once the door is scheduled to change state. The door will resume normal schedule after that.

d. Ability to resume a door to its normal schedule regardless of override method.

e. Ability to override a door through the following methods:

1) Override door from the software web interface.

2) Override door via triple swipe action at reader

3) Override door via auxiliary input action.

4) Override door via Crisis Levels feature.

f. Ability to pulse a door to unlock from any page in the software web interface.

I. Elevator management to Allow:

125. Ability to manage up to 64 floors with up to 4 elevator cabs per elevator master panel.

126. Ability to apply a specific name and description to each cab, reader and floor.

127. Ability to manage up to 4 cabs per Elevator Master Panel.

128. Ability to apply a time zone to control when a specific Floor is to unlock/lock, accept cards.

129. Ability to apply a Holiday group to control how a specific floor will behave on a Holiday.

130. Ability to configure if an individual cab is using button sensing elevator technology.

131. Ability to generate floor to output map for wiring and diagnostic purposes.

132. Ability to assign readers to 2 cabs.

133. Ability to configure up to 4 cabs on schedules without readers.

134. Floor Override:

a. Ability to deviate the state of a floor from the normal schedule.

b. Ability to override a floor until explicitly resuming the normal schedule.

c. Ability to override the state of a floor and instruct the controller to resume the normal schedule once the floor is scheduled to change state. The floor will resume normal schedule after that.

d. Ability to resume a floor to its normal schedule regardless of override method.

e. Ability to override a door through the following methods:

1) Override floor from the software web interface.

J. Panel management to Allow:

135. Ability to apply a specific name and description to each door/elevator panel.

136. Ability to assign a panel to a specific partition/site.

137. Ability to configure a password code for accessing the panel LCD interface and panel web interface.

138. Ability to configure the panel connection mode as static IP or DHCP.

139. Ability to enable/disable 256 bit AES encryption between Panel and Server.

140. Ability to configure the LCD screen on the panel, brightness and on time.

141. Ability to configure how long a forced open buzzer lasts.

142. Ability to configure the panel tamper sensor sensitivity and disable/enable.

143. Ability to configure how the integrated motion behaves, along with sensitivity options.

144. Panel Inputs and outputs are 100% configurable, all inputs/outputs can be configured as normally open or normally closed, supervised, events enabled/disabled.

145. Ability to configure Inputs as any of the following functions:

a. Request to Exit.

b. Door Contact.

c. Door Opener to exit.

d. Motion Sensor.

e. Emergency alarm.

f. External Alarm Status.

g. Door Opener to Require Card.

h. Man trap input

i. Aux Input action:

1) Toggle/Activate/Pulse selected output.

2) Toggle/Activate/Pulse alarm interface.

3) Override doors with Crisis Level.

4) Play Sound.

146. Ability to configure Outputs/Relays as any of the following functions:

a. Door Strike.

b. Door Opener.

c. External Buzzer.

d. Alarm Interface.

e. Aux Output.

f. Secondary Door Strike.

g. Door unlocked or open.

147. Ability to place panel into debug mode for diagnostics, troubleshooting and additional logging.

148. Ability to view in real time the following information:

a. Real time door contact status (open or closed).

b. Real time if the door is in an overridden state.

c. Real time mode of the door (card mode, unlocked)

149. Ability to unload an update to an individual panel.
150. Ability to request a panel show its currently known time.
151. Ability to reset anti-passback locations of users on a specific panel.
152. Ability to request a panel to disconnect from the server for a period of time.
153. Ability to manually place a panel into firmware update mode.
154. Output Override:
    a. Ability to deviate the state of an output from the normal state (open or closed)..
    b. Ability to override an output until explicitly resuming to its normal state.
    c. Ability to resume an output to its normal state regardless of override method.
    d. Ability to override an output through the following methods:
        1) Override output from the software web interface.
        2) Override output via triple swipe action.
        3) Override Output via aux input function.

K. IO-Board management to allow:

155. Inputs:
    a. Ability to apply a name to each Input.
    b. Ability to define a detection time until the input is considered active.
    c. Ability to place an Input on a schedule to only monitor during specific times.
    d. Ability to apply holiday schedules to an input for alternate schedules during holidays.
    e. Ability to assign an action to be performed when the input is activated.
    f. Actions:
        1) Do Nothing
        2) Activate Selected Output
        3) Deactivate Selected Output
        4) Toggle Selected Output
        5) Pulse Selected Output (high)
        6) Pulse Selected Output (low)
        7) Pulse Selected Output (opposite)
        8) Activate Multiple Outputs (up to 5)
        9) Deactivate Multiple Outputs (up to 5)
        10) Toggle Multiple Outputs (up to 5)
    g. Ability to place a delay on any Input Actions.
    h. Ability to place an action duration for pulses.
    i. Ability to configure an Input as Normally Closed.
156. Outputs:
    a. Ability to apply a name to each Output
    b. Ability to place an Output on a schedule
    c. Ability to apply holiday schedules to an Output for alternate schedules during holidays.
    d. Ability to configure an Output as Normally Closed.
    e. Ability to configure an Output to not generate any events.
    f. Ability to protect an Output from Input Actions.
    g. Ability to configure an Output to be initially On.

L. Site Management to allow:

157. Labeling:

a. Ability to name any created sites.

b. Ability to create a description for each site.

c. Ability to assign a Site to a Partition.

d. Ability to designate a timezone that the site will reside in, used to automatically convert devices timezone to local time zone.

158. Areas:

a. Ability to configure up to 254 areas in each site.

b. Ability to apply a name to each area.

c. Ability to assign to a reader what area the reader grants access to.

d. Ability to run muster report based on site and areas.

159. Anti-passback configuration to allow:

a. Local Timed anti-passback: Ability to control re-entry into an area, at a specific door, based on a definable time value.

b. Reset: Allow the ability to reset the anti-passback on a per panel basis.

c. Ability to configure soft or hard anti-passback.

d. Ability to configure anti-passback to ignore cardholders with the Supervisor flag.

e. Ability to configure anti-passback to ignore or take into consideration the opening of a door as a cardholder entering/exiting an area.

M. Historical Reports to allow:

160. Ability to execute various historical reports in the system and define which administrators can run which reports.

161. Ability to define a Start Time and Stop time for each report using intuitive slider bars or manually input time.

162. Ability to select a time zone (EST, UTC, ect) that the results of the report will be displayed in.

163. Ability to export any report into CSV or HTML format file for later viewing.

164. Historical information related to an elevator or door shall have a camera icon associated with the event that when clicked will bring up historical video for any cameras associated with that door/elevator at the specific time of the event if there are cameras associated with the device the event is related to.

165. Ability to execute the following historical reports:

a. Administrator Log Report:

1) Ability to select one, some or all administrators to run the report against.

2) View administrator activity for the selected administrators, including changes to users, system settings, panel updates, the time of the change along with the previous value of the field in some cases.

3) Logged administrator changes shall include the new value of the change, and the old value of the change.

b. User Activity Report:

1) Ability to select one, some or all users/cardholders to run the report against.

2) View user activity for the selected users based on date criteria. Results will include all doors/floors the user has been granted/denied access to, along with which credential that was used.

c. Door Activity Report:

1) Ability to select one, some or all doors to run the report against.

2) View door/reader activity for the selected doors based on date criteria, including the time of the event, the device that spawned the event, a user/credential if the event involved a user and the message associated with the event.

d. Floor Activity Report:

1) Ability to select one, some or all elevator floors to run the report against.

2) View Floor activity for the selected floors based on date criteria, including the time of the event, the device that spawned the event, the Cab the floor is attached to, a user/credential if the event involved a user and the message associated with the event.

e. Input Activity Report:

1) Ability to select one or more Inputs attached to any IO-Panels or Door Panels in the system that was defined as an “Aux Input”.

2) View Input activity for the selected Inputs based on date criteria, including the time of the event, the device that spawned the event, the controller the Input is attached to and the message associated with the event.

f. Output Activity Report:

1) Ability to select one or more Outputs attached to any IO-Panels or Door Panels in the system that was defined as an “Aux Output”.

2) View Output activity for the selected Outputs based on date criteria, including the time of the event, the device that spawned the event, the controller the Output is attached to and the message associated with the event.

g. Muster Report:

1) Ability to select a site and areas to run the report against.

2) View cardholders that are in the selected areas based on the date criteria.

h. Notifications Report:

1) Ability to view all historical notifications/events based on date criteria.

i. User List Report:

1) Ability to generate a list of all cardholders in the system along with their user properties, credentials and which access groups they are a member of.

j. Alert Monitoring Report:

1) Ability to have a separate screen dedicated to monitoring live notifications.

2) Ability to use global or temporary notification filtering options.

3) Ability to track which notifications the administrator has seen or missed.

4) Ability to auto select notifications as they come in

5) Ability to click on a notification and see more information about that specific notification. If a cardholder is attached to the event and has a picture; Picture will displayed as large as possible on the same screen.

k. Configuration Reports:

1) Reports that display system configuration, this includes the following:

a) Access Privilege Group - Device Configuration:

(1) Sorted by site, will display each Access Privilege group along with which readers are in that group and the associated User Time zone.

b) Door Configuration:

(1) Sorted by site, will display each door in the system along with the name of the schedule the door is following, associated holiday group, names of readers attached to the doors and the associated panel.

c) Elevator/Floor Configuration:

(1) Sorted by site and elevator, will display all elevators and floors along with the name of the schedule the floor is following, associated holiday group, name of readers attached to the cabs and the associated panel.

d) Input Configuration:

(1) Sorted by site and Panel, will display Input configuration for all IO and Door Panels. Report will display the name of each Input, the location of the input, the defined usage. Will also display IO-Panel input information such as Time Zone, Holiday Group, Action and Affected Outputs.

e) Output Configuration:

(1) Sorted by site and Panel, will display Output configuration for all IO and Door Panels. Report will display the name of each Output, the location of the Output, the defined usage. Will also display IO-Panel Output information such as Time Zone, Holiday Group and if the Output is protected from Input actions.

f) Panel Network Configuration:

(1) Sorted by site, will display network configuration of all panels along with the model of each panel, connection mode (static or DHCP), IP address, subnet mask, gateway and DNS server.

g) TimeZone – Reports:

(1) Ability to show the configuration of various time zones and schedules in the system, along with what day of the week, span lengths and modes during each day.

(2) The following time zone reports are available:

(a) Floor Time Zones

(b) Door Time Zones

(c) User Time Zones

(d) Holiday Door Time Zones

(e) Holiday Floor Time Zones

(f) Holiday User Time Zones

N. Notification and Alert Management:

166. Software web interface shall provide an in-line notification area that statically follows the screen as the administrator navigates the software.

167. Notification area shall provide near real-time events as they are happening.

168. Ability to click on specific notifications and be linked to a page in the web interface specific to the event such as:

a. Clicking an “unknown connection from panel with Mac address 4A5342343” will bring the administrator to the “Add panel” screen with the Mac address filled.

b. Clicking an “Unknown user denied access with credential 33-45545” will bring the administrator to the “Add User” screen with the credential pre-populated.

c. Clicking an “Access Denied” or “Access Granted” notification will bring the administrator to the “Edit User” page of the specific user.

169. Ability to configure which notifications show up in red (alerts).

170. Ability to configure if alerts will produce a warning sound in the web browser.

171. Ability to configure which notifications/alerts will be emailed to the administrator.

172. Ability to pause real time events.

173. Ability to clear real time events that are currently on the screen.

174. Ability to configure which notifications spawn in-line camera view with associated cameras.

175. Ability to configure which notifications will send an email with information about the event to the administrator.

O. Video Camera integration to allow:

176. Ability to integrate with 1 or more of the following Video Management Software (VMS) systems:

a. ViconNet® Digital Video Management system.

b. Digital Watchdog® DW Sprectrum

c. ExactQ® ExactVision

d. Milestones® XProtect

177. Support to integrate with multiple instances of VMS systems across different communication mediums such as LAN/WAN.

178. Ability to synchronize individual cameras or groups of cameras from the VMS software.

179. Shall support real-time video monitoring displays.

a. Up to 2 separate video streams simultaneously.

b. View up to 16 cameras in each stream (if VMS supports matrix larger than 1 x 1)

c. View in-line camera view, browser view or full window view.

180. Associate cameras with a door, elevator or both.

181. Associate a PTZ camera with a door based on a pre-set position.

182. Ability to configure specific events to spawn an inline camera view directly above the notifications/events area of the web interface.

183. Linking of video and events based on pre-set events provided by the access control software.

184. Historical events can spawn a video matrix to cameras based on the time of the event and associated cameras.

185. Administrator permissions specific to who can manage and make changes to the camera system.

P. Alert Management:

186. Ability to display alert events with date and time, source and description on the notifications screen, colour coded to the severity of the event. (Red, Blue or Green).

187. Permit event type alert messages, such as access denied, door forced open, and door held open.

188. Ability to configure specific event types to spawn camera matrix with cameras associated with the door/elevator the event is associated with.

189. Ability to configure e-mail alert messages to the administrator. Each administrator configures their own list of alerts that they are notified of via email.

Q. Microsoft Active Directory (AD) Integration via LDAP protocol:

190. Ability to obtain read only directory information from LDAP provider.

191. Ability to synchronize AD Users based on selected AD Security Groups.

192. Ability to choose which AD Security Groups AD Users will be synchronized from.

193. Ability to configure AD Security Groups as Access Privilege Groups.

194. Ability to give access to Doors/Floors based on AD Security Group membership.

195. Ability to synchronize the following AD User information:

a. First Name & Last Name

b. User Expiry Date

1) Expired Users will have access rights to Doors/Floors removed.

c. User Status (enabled/disabled)

1) Disabled Users will have access rights to Doors/Floors removed.

d. AD Group membership

196. Ability to synchronize credentials (Card/FOB/PIN) via AD User Attribute Fields.

197. Ability to synchronize credentials in the following manners:

a. Wiegand Credential from Single AD Attribute Field

b. Wiegand Credential from 2 individual fields with Fixed Site Code

c. Wiegand Credential from three Individual Fields

d. PIN from single field

198. Ability to synchronize AD User Attributes as Custom Fields.

199. Ability to configure how often Protector.Net checks the LDAP provider for changes (1 to 60 minutes).

200. Ability to automatically disable Users who have been deleted or disabled in Active Directory without panel update required.

201. Ability to filter AD groups by root OU.

R. Crisis Levels, security levels:

202. Ability to configure up to 16 Crisis levels (Code Red, Code yellow, Code Green, etc.) that can be used to quickly make global changes to the entire system in an emergency.

203. Ability to configure the name and door mode of each crisis level.

204. Ability to apply a crisis level to all doors in a particular site or a single door via web browser interface.

205. Ability to apply a crisis level to a panel via an Aux input function.

206. Ability to apply a security level to each user/cardholder. If a user/cardholder security level is equal or higher than the crisis level, the user/cardholder will be granted access based on the door mode and access privilege rules.

S. Triple Swipe Actions:

207. Ability to configure a reader and credential to activate one or more functions via swiping or presenting a credential 3 times in a row within a set span of time.

208. Ability to change the mode of a door via triple swipe action:

a. Override Lockdown Mode

b. Override Card mode

c. Override Pin mode

d. Override Card or Pin mode

e. Override Card and Pin mode

f. Override Unlock mode

g. Override First Card In mode

h. Override Lockdown with Auto-resume

i. Override Card mode with Auto-resume

j. Override Pin mode with Auto-resume

k. Override Card or Pin mode with Auto-resume

l. Override Card and Pin mode with Auto-resume

m. Override Unlock mode with Auto-resume

n. Override First Card In mode with Auto-resume

o. Cancel Override

209. Ability to toggle, activate, deactivate or pulse a relay via triple swipe action.
    a. Activate Aux Output
    b. Deactivate Aux Output
    c. Toggle Aux Output
    d. Pulse Aux Output
    e. Cancel Output Overrides
210. Ability to toggle, activate, deactivate or pulse an output connected to an external alarm system to arm or disarm an alarm.
    a. Activate Alarm Interface
    b. Deactivate Alarm Interface
    c. Toggle Alarm Interface
211. Ability to configure which users/cardholders can execute triple swipe actions, including which users can disarm the alarm system.
212. Ability to configure a single triple swipe action per reader if using regular proximity type reader.
213. Ability to configure up to 5 triple swipe actions at one reader if the reader has keypad input.
214. Ability to use any of 3 predefined triple swipe actions when using keypad input for a total of 8 actions:
    a. Override the door into card mode.
    b. Resume an overridden door.
    c. Resume any overridden outputs.

T. Data Management: System to Allow:

215. Software shall provide the ability to perform automatic database backup to a location selected by the administrator.
216. Ability to backup user profile pictures along with database backup.
217. Backup locations shall include:
    a. Shared network drive.
    b. External USB drive.
    c. Folder on local hard drive.
218. Ability to compress database backups for better space utilization.
219. Ability to encrypt a backup with a definable password.
220. Software shall provide the capability to manually back up the database to a selected location.
221. Ability to automatically remove backups older than a defined period of days in the backup directory.
222. Availability of a database restore utility that can be performed via web browser.
223. Ability to stop/start/restart the web service through management web interface.
224. Software shall include system tray application that shows status of web service, and provides control to stop/start the web service.
225. Ability to remotely change network settings on remote server hosting the web service.

U. Software Registration Management:

226. Software registration directly through dealer or the manufacturer.
227. Ability to manage and view the following licensing information from web interface:
    a. View current license package.
    b. View expiry date of license.
    c. View license features and limitations

228. Software shall provide 30 day warning prior to software license expiration.

229. Software shall provide 10 day grace period after software license expiration if no administrator has logged in since the license expired.

V. Photographic Badge Design to Include:

230. Functional integration with cardPresso photographic badge software via SQL database.

231. Ability to link card to database data and include links to any of the customizable card holder fields, including date of birth, titles, initials, first or last name, and photograph.

232. Ability to import Cardholder photographs or images from files.

W. Assa Abloy Aperio Integration:

233. Software shall provide unified management of Aperio devices.

234. Ability to communicate with up to 8 Aperio wireless locks per Aperio controller.

235. Ability to store 100,000 users, bypasses Aperio 2,000 user limitation.

236. Cabinet or door locks supported.

237. Ability to share time schedules between regular door controllers an Aperio controllers.

X. Software Navigation and Contextual Help:

238. Offer contextual help file by hovering over fields, check boxes, drop-down menus.

239. Ability to place objects into list format (such as panels, doors, user) for conducting comparisons between objects.

240. Ability to edit attributes of objects from the list view.

241. Software shall offer comprehensive documentation can be accessed through web interface, or accessed via start menu shortcut on host web server.

PRODUCT SUBSTITUTIONS

A Substitutions: No substitutions permitted.

PART 3 EXECUTION

MANUFACTURER'S INSTRUCTIONS

Specifier Note: Article below is an addition to the CSI *Section Format*; please revise to suit project requirements and specifier's practice.

Y. Compliance: Comply with manufacturer's written data, including product technical bulletins, product catalog installation instructions and product carton installation instructions.

EXAMINATION

A Site Verification of Conditions:

242. Verify that substrate conditions, which have either been previously installed under other sections, or that existing site conditions, are acceptable for product installation in accordance with manufacturer's instructions.

243. Verify that building doors, frames, walls, wire runs, related items and conditions are ready to receive work of this Section.

PROTECTION

A Other Trades: Protect installed work of other trades.

PREPARATION

A Project Planning Forms:

244. Manufacturer Forms: Obtain and complete project planning forms from manufacturer of surveillance system; customize forms to be project specific.

245. Final Setup: Review, adjust and prepare final documents to establish system software setup.

Z. Record Setup Data:

1. Record server and workstations setup data.
2. Record controller address, features and access requirements for each location.
3. Propose start and stop times for Time Zones, including holidays; match up for Door Schedule.
4. Set up Access Privilege groups, Elevator Privilege groups, list inputs and outputs for each Controller.

AA. Electrical Preparation:

246. Ensure dedicated 120 VAC power circuits, conduit, raceways, back boxes, j-boxes, fittings, hardware and earth grounds supplied as necessary to provide complete working system.

247. Ensure power supplies associated with electrified door hardware is installed.

248. Ensure conduit for cable protection within walls, back boxes, door jambs, stubbed above drop ceilings, within closed ceilings, where exposed, and penetrating walls and ceilings, have been provided.

249. Ensure back box installations in masonry have been completed.

250. Ensure patching and painting items related to conduit, raceways, j-boxes, fittings hardware and earth grounds conduit and conduit installations has been done.

251. Ensure cabling for alarm systems is installed and completed.

BB. Elevators:

Specifier Note: Installation of equipment and wiring to the elevator to be coordinated with the elevator.

252. Coordinate installation of wiring, card readers and relay's to cab(s).

253. Coordinate installation of wiring and equipment for elevator control, life safety to cab(s).

254. Coordinate testing and commissioning of elevator system after installation of equipment.

Specifier Note: Installation of equipment and wiring for information services to be coordinated with the IT personnel.

CC. Information Services:

255. Ensure that dedicated phone lines and phone equipment have been provided and completed.

256. Ensure that network drops are being installed and installation coordinated with the work of this section.

257. Ensure coordination of Server and Client software installations with IT personnel.

258. Ensure coordination of IT personnel prior to configuration and installation of Ethernet devices.

Specifier Note: Installation of equipment and wiring for the fire alarm panel to be coordinated with the fire contractor.

DD. Fire Alarm:

259. Ensure coordination of installation, including wiring and equipment for the fire alarm panel to interface with access control alarm monitoring system, is undertaken.

1INSTALLATION

A Comply with:

260. IEEE 1100.

261. NFPA 70.

262. NFPA 72.

263. NFPA 80.

264. NFPA 101.

EE. Installation:

265. Install surface mounted units to finished substrates.

266. Set units level, plumb and true to line and location.

267. Comply with positioning requirements for disabled accessibility.

268. Provide 120 VAC power circuits, conduit, raceways, back boxes, j-boxes, fittings, hardware and earth grounds as required to provide electrical requirements for access control systems.

FF. Cabling:

Specifier Note: Select the cabling system appropriate to the installation. Delete paragraphs that are not applicable.

269. Raceway and Cable Tray: Install wiring in raceway and cable tray, except:

g. Within consoles, cabinets, desks and counters.

h. In accessible ceiling spaces.

i. In gypsum board partitions where unenclosed wiring method may be used.

270. Conduit: Install wiring in conduit, except:

j. Within consoles, cabinets, desks and counters.

271. J-Hooks: Install wiring in j-hooks and associated wire hardware.

272. Conceal [Raceway and cable tray] [Conduit] [J-hooks and cables] except in unfinished spaces.

273. Use NRTL-listed plenum cable in environmental airspaces, including plenum ceilings.

274. Install cables without damaging conductors, shield or jacket.

275. Use only Manufacturer recommended wiring,

276. Basic elevation drawings available from manufacturer upon request.

277. Advanced elevation, riser and point to point diagrams available from manufacturer for an additional fee, based on the complexity of the project, and the level of integration required with other systems.

GG. Grounding:

278. Comply with IEEE 1100.

Specifier Note: To eliminate shock hazard and to minimize ground loops, common-mode returns, noise pick-up, cross-talk and other impairments, use the following.

279. Ground cable shields, drain conductors and equipment.

280. Bond shields and drain conductors to ground at only one point.

HH. System Software:

281. Develop, install and test software and databases for complete and proper operation of systems involved.

282. Register all Software within 30 days of on-site installation.

FIELD QUALITY CONTROL

Specifier Note: Use the following Articles only when manufacturer's field services are desired to verify the quality of the installed components. Establish the number and duration of periodic site visits required by Manufacturer and specify below. Consult Manufacturer for services required. Delete if field services are not required.

A Written Reports: Have manufacturer of products supplied under this Section review Work involved in handling, installation/application, protection and cleaning of its product[s], and submit written reports in acceptable format to verify compliance of Work with Contract.

II. Manufacturer's Field Services: Provide manufacturer's field services consisting of product use recommendations and periodic site visits for inspection of product installation in accordance with manufacturer's instructions.

JJ. Schedule site visits to review Work at stages listed:

283. After delivery and storage of products, and when preparatory Work on which Work of this Section depends is complete, but before installation begins.

284. Throughout progress of Work.

285. [Twice] [_____] during progress of Work at [25%] [_____] and [60%] [_____] complete.

286. Upon completion of Work, after cleaning is carried out.

KK. Obtain reports within [Five] [_____] days of review and submit.

TESTING & VERIFICATION

A Perform tests recommended and required by manufacturer to verify required performance of all products manufactured and /or supplied by Hartmann Controls Corp.

Specifier Note: Provide test descriptions in sufficient detail to fully describe the specific tests to be conducted to demonstrate conformance with the specification.

287. Complete system diagnostics and operation verification.

288. Prepare specific plan for system testing, start-up and demonstration.

289. Develop acceptance test concept and specifics.

290. Test each circuit and component of each system. System components with battery back-up to operated on battery power for not less than [10] percent of calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.

291. Operational Test: Demonstrate product capability and compliance with requirements.

292. Remove and replace malfunctioning devices and circuits and retest.

293. Complete installation and start-up checks in accordance with manufacturer's written instructions.

294. Maintain strict security during installation of equipment and software. Secure rooms housing the Server software and workstations.

DEMONSTRATION

Specifier Note: A training program is required to educate personnel with the required level of system familiarity to provide a common working knowledge concerning all aspects of the system.

A Training Program:

295. Provide training to Owner's personnel to adjust, operate and maintain access system.

296. Two week prior to the start of the program, submit proposed dates for training.

297. Develop separate training modules consisting of at least, but not limited to 1 hour per group, based on the level of knowledge required by the specific group.

298. Provide group specific operator manuals covering all areas of hardware/software required.

299. Groups:

k. Computer system administration personnel tasked with managing and maintaining databases and updating and maintaining software.

l. Operators tasked with preparing and imputing credentials to staff/users.

m. Operators tasked with configuring hardware and or software features and functions.

n. Security personnel.

.

COMPLETION & CLEANUP

A Upon completion and verification of performance of installation, remove surplus materials, excess materials, rubbish, tools and equipment.

END OF SECTION