MILLENNIUM

SECURE YOUR WORLD

Electronic Access Control System

Specifications for Architects & Engineers
28 13 00

December 31, 2020

Millennium Group Inc. ● 16 Tech Circle ● Natick, MA 01760 ● (508) 344-1340

PART 1 GENERAL

1.0 SECTION INCLUDES

A. Access Control System ("ACS") Millennium Ultra
B. Local (LAN) Server based software application deployed using Microsoft SQL and Microsoft .NET technology (Ultra Local Version)
C. Web (WAN) Server based Software application deployed on AWS cloud services (Ultra Hosted Version)
D. Local Client browser interface for either server system, including configuration, operations, management, and reporting.
E. ID Badging Module
F. Visitor Management Module
G. Parking Management Module
H. Specialized partner Interface Modules for 3rd party vendor hardware integration
I. Specialized partner API Module for 3rd party vendor database integration
J. IP based Site Controller boards (ESCU) with 485 communication interfaces for ACS devices
K. RS-485 based Door Controller boards (EDCD) with Wiegand reader interfaces
L. NetDCD-1 and -2 Combination Site Controller and One-Door or Two-Door Controller board
M. RS-485 Elevator Control Unit (ECU-2 & 3b) with 16 relays each for building floor control
N. IP based Elevator Control Unit (ECU-3c) with 16 relays each for building floor control
O. RS-485 based Elevator Cab Reader board for interface with ECU-2 or ECU-3
P. RS-485 based Relay Control board providing 8 relays for general use
Q. Other associated hardware and software components
R. ACS control cabling and power supplies

1.1 RELATED SECTIONS

A. 08 10 10 Doors and Frames
B. 08 31 13 Access Doors & Frames
C. 08 42 00 Entrances
D. 27 15 00 Communications Horizontal Cabling
E. 27 24 00 Peripheral Data Communications Equipment

1.2 REFERENCES

A. IEEE 802.3 Ethernet Standards
B. Electronic Industries Alliance (EIA) for RS232C - Interface between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange and RS485 - Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multi-Point Systems
C. UL 294 - Standard for Access Control System Units
D. FCC - Code of Federal Regulations, Title 47, Part 15, Class B
E. Federal Information Processing Standards Publication 197 – Advanced Encryption Standard
F. EMC Directive 89/336/EEC
G. International Organization for Standardization - ISO 8601 Data elements and interchange

formats – Information interchange – Representation of dates and times

H. NFPA 70: National Electric Code (NEC)
I. NFPA 101: Life Safety Code
J. NFPA 730: Guide for Premises Security
K. NFPA 731: Standard for the Installation of Electronic Premises Security

1.3 DEFINITIONS USED WITH ON-LINE ELECTRONIC ACCESS CONTROL SYSTEM

A. Access Level: A list of defined access points and the time periods that users will be allowed to access.
B. Access Point: A door, gate, elevator floor, or other point of egress into or out of a protected Site.
C. Access Reader: Converts Credential's information as a Wiegand, or other format, identifier to be matched to the ACS to allow access to an Access Point based on the assigned Access Level.
D. Alarm Monitoring: Provides a supervisory function for the status of an alarm device which is reported back to ACS.
E. Cardholder: A holder of a Credential which has been activated and assigned an Access Level.
F. Credential: A card, fob, transmitter, bracelet, biometric, bluetooth, NFC, keypad number, or other unique identifier assigned to a Cardholder to allow egress through an Access Point.
G. Distributed Architecture: Describes the operation of the ACS that allows the distributed ACS hardware and software to function with its normal routines without communication with the ACS server.
H. Door Controller: Provides the ACS with an interface between an Access Reader, an Access Point's alarm inputs and outputs, relays, and communicates via RS-485 with the Site Controller or Net Controller.
I. Elevator Controller: Provides the ACS with an interface between the Elevator Company's floor relays and the board's 16 relays in order to provide an interface for the Access Reader in the elevator cab, each floor (Access Point) the elevator cab serves, by Access Level, depending on the Credential presented.
J. Elevator Cab Interface board: Provides the interface between the Access Reader and the Elevator Controller by relaying Credential information back to the Elevator Controller.
K. Net Controller: Provides an IP interface (LAN or WAN) with the ACS server for up to 100 Access Points or Relays per Net controller, less the number of Access Points provided for on the Net Controller, with a limit of 5,000 Cardholders in the ACS allocated to any particular Net Controller.
L. Operator: A user that has been granted access to the ACS software via a user ID and password, based on the Operator Level's security granularity of rights and privileges to various areas of the ACS Software (Ultra).
M. Relay Controller: Provides control of up to 8 access related devices by time periods, supervisory function, or linking events by the ACS software through relays on the board.
N. Site Controller: Provides an IP interface (LAN or WAN) with the ACS server for up to 100 Access Points or Relays per Site controller connected via RS-485.
O. Time Period: Start and end period along with days of the week that can be used to control Cardholder Access, automatic unlocking of Access Points, alarms inputs, reports, and relay operations.

1.4 SYSTEM GENERAL DESCRIPTION

A. The Electronic Access Control System (ACS) shall be a secure, modular, scalable system designed

to control and manage the movement of Site occupants. The ACS shall include a centralized Access Management Server (Server), configured, monitored, and operated from a web browser or software client app, located on a common Local Area Network (LAN) device (Ultra Local Version), or on any internet capable device through a Wide Area Network (WAN) connection (Ultra Hosted Version).

B. The ACS Server shall be deployed on a device running a Microsoft Windows operating system or is capable of being run on a dedicated server or a virtual machine in order to support multiple simultaneous users; or the ACS Server shall be deployed on Amazon Web Services (AWS) Servers and shall be accessed via any device with a WAN connection, depending on whether Ultra Local or Hosted is utilized.

C. The ACS shall include either RS-485 or IP based communication links between system components. Inputs, outputs, and peripheral devices shall be connected to Door or Relay Controller boards capable of operating with or without connectivity to the ACS Server via the Site Controller boards. In many instances, the Door, and Net Controller boards with Door Access Points onboard, will remain in disconnected, yet operational status from the ACS Server wherever required.

1.5 SUBMITTALS

A. Shop Drawings

Prior to assembling or installing the ACS, the contractor shall provide complete shop drawings including the following:

i. Architectural floor plans indicating all system device locations.
ii. Wiring schematics for all devices including cable types, lengths, routings and termination requirements.
iii. Complete block diagram of the ACS.
iv. Detailed drawings showing mounting and fastening methods for system components
v. System commissioning requirements and report format

B. Product Data

Prior to assembling or installing the ACS, the contractor shall provide the following details for ACS system components:

i. Manufacturers technical specifications and/or data sheets for all system components and accessories, including but not limited to Server specifications, supervisory and control devices, Credentials, Access Readers, and any other equipment provided as part of the integrated Security Management System (SMS).
ii. Detailed requirements for the ACS Server, including processor, RAM, storage capacity, LAN & WAN capabilities, USB ports and speeds, graphics outputs by type and total bandwidth, and Uninterruptible Power Supply and Battery Backup requirements.

C. Product Manuals

Upon completion of the system installation, the contractor shall make available print or digital versions of the following manuals:

i. Hardware manual describing the installation, configuration, and operation of hardware

deployed as part of the ACS installation.

ii. Software manual describing the proper configuration and operation of the ACS Server.

iii. Maintenance manual describing the proper maintenance and repair of the ACS.

D. Warranty & Software Maintenance Agreements

Upon completion of the system installation, the contractor shall make available the manufacturers product warrant and software maintenance agreement.

1.6 QUALIFICATIONS

A. Manufacturer Qualifications:

The manufacturer and supplier of all hardware and software components deployed as part of the ACS shall be reputable, established vendors in the industry for not less than ten (10) years and shall have demonstrated the ability to support projects of a similar size and complexity.

B. Installer Qualifications:

1. Installers shall have a demonstrated history of successfully installing and servicing an ACS of a similar size, scope, and complexity.
2. Installers shall be capable of providing evidence that they are trained and authorized by the ACS manufacturer.
3. The installer shall retain sufficient personnel, capacity, and spare parts to support the ongoing operation of the ACS or demonstrate that such support can be provided by other local service providers that have also been trained and authorized by the ACS manufacturer.

1.7 DELIVERY, STORAGE, AND HANDLING

A. Delivery: Deliver materials to site in manufacturer's original, unopened containers and packaging, with labels clearly identifying product name and manufacturer.

B. Storage: Store materials indoors, in a clean, dry area in accordance with manufacturer's instructions.

C. Handling: Protect materials and finishes during handling and installation to prevent damage.

1.8 WARRANTY

The ACS shall be provided with a 12-month warranty from the date of system registration and shall include software updates for the duration of the warranty period.

END OF SECTION

PART 2 - PRODUCTS

2.1 MANUFACTURER

The Electronic Access Control System (ACS) shall utilize the Millennium Ultra ACS Server and the complete system shall include Site Controllers, Net Controllers, Door and Relay Controllers, and Elevator Controllers, compatible with Millennium Ultra and manufactured by Millennium Group Inc.

2.2 EQUIPMENT

A. The following equipment shall be required as the core elements of the EACS and shall be developed and manufactured by the following supplier:

Millennium Group, Inc.
16 Tech Circle
Natick, MA 01760
Phone: (866) 455-5222
Fax: (508) 651-2902
Url: www.mgiaccess.com

B. Software shall be Millennium Ultra Version 4.00 or later

C. Site Controllers shall be Millennium E-Series ESCU Site controllers or E-Series NetDCD Net Controllers depending on ACS requirements

D. Door Controllers shall be Millennium E-Series EDCD Door Controllers

E. Elevator Controllers, if required, shall be Millennium ECU-3b or ECU -3c Elevator Controllers

F. Power Supplies shall be Millennium PS-1 series power supplies

2.3 SYSTEM DESCRIPTION

A. The ACS shall be an integrated system built upon the Microsoft Operating System platform including the Microsoft Windows/Server operating system, Microsoft SQL Server, and Microsoft .NET software framework. The complete system shall include, but not be limited to the ACS Server, Site controllers, Door controllers, Access Readers, door locking and release hardware, power supplies, and sufficient Credentials for the size and scale of the system deployed

B. The ACS shall allow or deny Access Point egress to a Cardholder based upon the Access Level, Time Period, and term of the deployment through the expiration date.

C. The ACS shall prevent access by Non-Cardholders, or Cardholders who are inactive, are not egressing an Access Point that has been assigned to their Access Level, or their assigned Time Period, regardless of whether the Access Point is being currently supervised and managed by the ACS, or whether it is functioning in disconnected

distributed mode.

D. Operators of the ACS shall be capable of accessing routine functions such as adding new Cardholders, removing Cardholders, running reports, or monitoring system access events, status and alarms, from either a web browser or a client app installed on a LAN or WAN capable device.

E. The ACS system shall be expandable and scalable to support an unlimited number of controllers, access points, cardholders, credentials, and capable of supporting multiple operators.

2.4 ACCESS CONTROL SERVER SOFTWARE – MILLENNIUM ULTRA

A. On-Line Electronic Access Control System: Millennium Ultra.

1. System shall have capability to perform:

    a. Access control configuration & monitoring
    b. Activity monitoring
    c. Programmable relay control
    d. Real-time event viewing
    e. Elevator control
    f. Database backup and support functions
    g. System configuration and troubleshooting
    h. Extended functionality through optional manufacturer supplied and third-party integrations

B. ACS Server Characteristics for Ultra Local Version Implementation (MINIMUM):

1. Reliable brand PC (Dell, HP, etc.) (Min. 3-year onsite warranty)
2. Windows 10 Home, 64-bit; VMWare or MS Hyper-V
3. Processor: Intel i3 Processor
4. RAM: 8 GB
5. Storage: 2TB SATA Drive
6. Graphics: Intel onboard graphics
7. Printer: Support any Windows installed printer for reports.

C. ACS Server Characteristics for Ultra Local Version Implementation (BETTER):

1. Reliable brand PC (Dell, HP, etc.) (Min. 3-year onsite warranty)
2. Windows 10 Pro, 64-bit; VMWare or MS Hyper-V
3. Processor: Intel i5 Processor
4. RAM: 12 GB
5. Storage: 256GB SSD and 8TB SATA Drive
6. Graphics: nVidia or AMD discrete video card with at least 2GB RAM and 2 HDMI out for dual monitors
7. Printer: Support any Windows installed printer for reports.

D. ACS Server Characteristics for Large Scale Ultra Local Version Implementation (SERVER):

1. Reliable brand Server (Dell, HP, etc.) (Min. 3-year onsite warranty)
2. Windows Server 2012 R2 or 2016; VMWare or MS Hyper-V
3. Processor: Xeon E-Series Processor
4. RAM: 16 GB
5. Storage: 256GB SSD and 8TB SATA Drive or RAID Configuration
6. Graphics: Dual video out for situational awareness
7. Printer: Support any Windows installed printer for reports.

DI. Software:

1. Server: MS SQL Server, provided by Millennium and .NET Framework 4.5 or higher
2. Client: Any well-supported web browser, including Internet Explorer, Edge, Firefox, Chrome, and Safari; or Millennium Client App
3. Client requires Operator login to Millennium Ultra to operate ACS

DII. Database:

1. Supplied with full support of Microsoft SQL 2012 –2014 database server application to allow archiving of history, database repair functions, and import/ export facilities.
2. Support real-time import and export of data.
3. Supports automatic update of Operator Access Level as a result of the import process.
4. Allows for a unique industry standard ISO card number to be generated on demand as part of import process.
5. Provides an optional tenant feature; allows specific system entities in the database to be seen and manipulated only by certain "Tenants." Such entities can be cardholders, operators, sites and elevator floors. When the database is divided into spheres of control in this way, operators in a given tenant will control data such as sites, doors, cardholders for their own tenant(s) only. The database itself is complete, but views are generated such that what the operator can view, add, modify, delete or print reports, and is limited by the Tenant(s) to which they have rights to as well as by Operator Level.

DIII. Operators:

1. Limits system operation by different Operator Levels.
2. Individual Operators have unique passwords for logging in.
3. Custom configured Operator Levels. Operators may have rights to view, add, change, delete, or execute program features.
4. Provide an automatic operator logout feature.

F. Software Functions and Options:

1. Software to provide support for the following:

a. Unlimited number of Cardholders
b. Each Site Controller: 100 Access Readers, Floor Relays, or General Relays (Limit 64 Floor Relays or 80 General Relays per Site Controller; however doors alone can reach maximum of 100)
c. Up to 1,000 site controllers per Ultra instance or 100,000 Access Points
d. Number of Tenants: Unlimited
e. Number of Access Levels: Unlimited (10 per Credential)
f. Supports multiple Access Reader technologies and protocol on same Door Controller simultaneously (up to 4 formats)
g. Supports simultaneously 2 custom ABA formats and 2 Wiegand formats for Access Readers
h. Supports combination Access Readers with one Wiegand output. Support custom Wiegand outputs from 0 to 50bits, including 32 bits, 37 bits, HID Corporate 1000 program, and Motorola 27 bits
i. Supports Suprema fingerprint Access Readers
j. Supports dual authentication with a pin number along with a Credential that is enabled by a time period
k. Supports a door pin number that is enabled by a time period.
l. Able to accept any facility code of card provided (0 to 31bit facility code)
m. Supports unique Cardholder Record Number or optionally not required
n. Option to rename fields on the Cardholder page
o. Allows up to three Credentials to be programmed per Cardholder.
p. Supports “disable card” function for each Credential.
q. Supports anti-passback modes
r. Supports a door controller address and text description name in a field; maximum of 19 characters.
s. Supports 2 relays included with each door controller.
t. Supports “Autoactivating” an Access Point to automatically unlock and automatically relock an electric strike or magnetic lock according to the Time Period set.
u. Supports Autoactivating, as above t., but only after first valid Cardholder presents Credential to Access Reader.
v. Notifies when the status of a door or relay controller changes because of a communication or device problem.
w. Supports programmable reports viewed on monitor or printed.
x. Provides capability of sorting history events by time, dates, cardholders, access readers, and operators.
y. Ability to preprogram dates for Daylight Savings Time.
z. Supports relays that can be programmed to operate by a time period, alarm, or by event, linked to Access Points.
aa. Have the Owner’s name encrypted on Site Controllers and displayed on monitor.
bb. Capability to automatically archive activity and alarm data and be able to select date range being archived.

cc. Provides communication to sites using LAN or WAN.
dd. Advises and displays on computer monitor, the status of Site, Net, Door and Relay controllers, if communication or power is lost on ACS hardware.

G. Software Optional Functions

1. Supports system lockdown on programmable Threat Levels.
2. Supports system lockdown by pre-programming Access Point groups.
3. Supports linking any system alarm point or action with lockdown function.
4. Supports system Toggle function allowing first valid card to unlock and hold unlock. The next valid card will lock the door. This function can be set to follow a Time Period or Schedule.
5. Supports 3rd party integrations including:
    a. March Networks IP based video security solutions
    b. Milestone xProtect IP based video security solutions
    c. Allegion AD Lockets; LE & NDE Locksets; Control Deadbolts; Engage Gateway and PIM400 integration
    d. Assa Abloy IN120 based Wireless door solutions
    e. Assa Abloy VINGCard door management solutions
    f. DMP XR Series Intrusion systems

Specifiers note: Supported 3rd part integrations are constantly evolving. Contact the Millennium Group for the latest list of supported integrations

H. Alarm Monitoring Software:

1. Supports a minimum of 7 supervised alarm inputs per door control unit with time period disable feature, and a programmable shunt delay timer from 0 to 255 seconds.
2. Supervision of alarm points can be either two (Alarm, Reset) or four states (Alarm, Reset, Open, Shorted) determined at software configuration.
3. Provides a forced-door entry alarm and a door ajar alarm. Forced-door alarm shall have a shunt delay timer of 0 to 255 seconds. Ajar alarm shall have a programmable delay timer of 1 to 255 minutes.
4. Supports adding comments to the alarm/events.
5. Supports prioritizing of alarms to 100 levels.
6. Supports linking specific alarms to Relay Controllers.
7. Requires acknowledgment text so personnel monitoring alarms shall provide response information.
8. Includes an alarm monitor app, which shall display alarms graphically in the priority with which they were programmed. Application can be run from any Windows based computer. Allows alarm acknowledgment from any LAN connected device with synchronization between operators.
9. Provide alarm monitor with capability to display a Cardholder portrait in response to valid or invalid access attempts.

I. Scheduler; integrated software:

1. Fully configurable integrated module allowing scheduled actions for any access points of the system, overriding the normal door unlock/lock set up
2. Unlimited number of schedules supported
3. Configurable actions
4. Unlock – Lock
5. Shunt alarms

J. System Hardware:

1. System components to include Site Controllers, Net Controllers, Door Controllers, Power Supplies, optional Relay controllers, optional Elevator Controllers, and other auxiliary devices
2. System shall be able to be configured from 1 to 100 Access Readers for each Site controller
3. Controllers shall store basic parameters, including real-time clock, for a minimum of 24 hours, in case of AC power loss and battery backup is exhausted
4. System shall use a fully distributed architecture in which system alarms, access, relays, and elevator control shall continue to function in a normal mode without LAN or WAN communications
5. Site controller shall be able to communicate via LAN or WAN
6. Site controller shall have a local relay to monitor status of communications with Door, Relay, or Elevator Controllers. In case of device failure, a relay will open, providing a means of triggering an external monitoring device
7. Site, Net, Door, Relay, and Elevator controller features shall have capability to be field or factory upgraded for firmware changes via physical chip replacement or via the Ultra Configurator app, depending on type. Such firmware upgrades shall be offered as needed to registered Sites on an exchange basis
8. Door controllers shall support any Wiegand standard Access Readers in any bit format up to 50 total; bit patterns are fully programmable within Ultra ACS
9. Supported Access Reader types to include, but are not limited to: Wiegand, Mag stripe, Bar Code, Proximity, Keypad, Biometrics, combination keypad with Wiegand/Proximity/Magnetic stripe, WiFi, Bluetooth, NFC, etc.
10. Door Controllers shall be able to be programmed for custom ABA formats from the software, including ability to ignore user specified characters in format.
11. Door Controllers shall be programmable to accept either normal or inverted strobe signals from ABA format readers.
12. Door Controller shall be programmed for appropriate Access Reader technology.
13. Site Controllers shall buffer the last 2,000 events from Door Controllers when LAN or WAN communication has been lost or interrupted.
14. Each Door Controller shall buffer an additional 2,000 events when its Site Controller buffer has been filled.
15. All ACS Controllers shall have a built-in tamper alarm to detect when a cover to the controller is removed.
16. Door Controllers shall include:
    a. A Request to Exit input

b. A Single Access Reader connection
c. Function at full capacity without LAN or WAN communications, and buffer events up to a maximum of 2,000 during this period
d. Continue to function on battery backup at a minimum of 9 VDC?

17. Door and Relay Controllers shall have Form C dry contact configurations
18. Door and Relay Controllers shall have relays with a minimum current rating of 24VDC at 2A, with solid-state, automatically resettable, overcurrent protection for contacts
19. Door Controller shall have a relay that can be programmed by software for: Valid User, Auto Activate, First User Auto Activate, Any User, Rejected User, Dual Custody (2 valid token to be presented within 5 sec), or Alarm Options
20. Relay Controller shall have relays that can be configured by software for Time Period Activation, Timed Activation, Timed Released, First Event Activation, First Event Released, and Last Person Out
21. Relay on Door Controller shall have a programmable timer and settings in software for electric strike and magnetic lock operation
22. Site controller to door controller communication shall conform to EIA RS-485 with a recommended total cable length of 5,000 feet (1,524 m) when utilizing 18AWG cabling for the proper conditions
23. Power Supply:
    a. Battery backup capable of providing power for system during temporary AC power outage.
    b. Provide a supervisory output to notify system when there is a loss of AC power.

K. System Access Readers:

1. Wiegand Output Format Readers: Output of 26-bit Wiegand format or a custom bit configuration from 13 to 50 with configurable facility codes
2. Example of supported Access Reader types include, but are not limited to: Proximity, Mag Stripe, Bar Code, Wiegand, Keypad, Biometrics, combination keypad with Wiegand/Proximity/Magnetic stripe, Bluetooth, NFC, WiFi, etc.
3. ABA Format Readers: ABA, ABA inverted.

L. E-Series Door Control Device (EDCD):

1. Description:
    a. Designed to control a single Access Point
    b. Contains a real-time clock and sufficient memory to provide normal operations when in disconnected, distributed mode
    c. Transaction history shall be automatically buffered when not online with ACS Server
    d. Priority event buffer assures alarms are annunciated in a timely manner even if history buffer is full
2. Power: 9 to 14 VDC, supplied by central power supply; 80 to 110 mA, depending upon reader technology. Accessory relays require additional 20 mA each
3. Power Protection: Reverse polarity, overvoltage, and transient
4. Access Reader technologies supported: Wiegand Credential (any bit format up

to 50), ABA/ISO Track 2, proximity, keypad, combination reader/keypad, biometrics, WiFi, NFC, Bluetooth, etc.

5. Access Reader Interfaces Supported: clock/data, clock/data inverted, Wiegand
6. History Buffer: 2,000 transactions
7. Priority Event Buffer: 100 transactions
8. On-Board Memory and Clock Backup: 24 hours minimum
9. Maximum Cardholders stored in memory: either 60,000 for Site Controller or 10,000 for Net Controller
10. Alarm Input Points: 7 total, 2-wire supervised, Two or four state selectable (EOL resistor) including, built-in door contact monitoring
11. Alarm Input Monitoring Circuit: Analog to digital conversion
12. Tamper Alarm: On-board switch
13. Output Relays: 2 each with Form C contacts rated 2A, 30VDC
14. Output Relay Contact Protection: Solid-state polymeric resettable
15. Connectors: 5 mm plug-on screw terminal
16. Address Switches: Rotary, direct-reading, 00 to 99.
17. Communications: Multi-drop RS-485, proprietary protocol
18. Operating Environment:
    a. Between 14° F and 104° F (-10° C and 40° C)
    b. Less than 90 percent noncondensing humidity
19. Supports T-TAP, Daisy Chain, or Star Topology connectivity

M. E-Series Site Controller (ESCU):

1. Description:
    a. Designed to control a maximum of 100 Access Readers, Floor Relays, or General Relays (Practicable Limits: 64 Floor Relays or 80 General Relays per Site Controller; however, doors alone can reach maximum of 100)
    b. Normally used for a single site or building, contains a real-time clock and sufficient memory to supervise site up to 60,000 Cardholders.
    c. Maximum of 1,000 site controllers can be addressed in an Ultra ACS.
    d. Transaction history is automatically buffered when not online with ACS Server.
    e. Priority event buffer assures alarms are annunciated in a timely manner even if history buffer is full.
    f. On-board switches select operational modes.
2. Power: 9 to 14 VDC, supplied by central power supply; 50 mA standby, 90 mA maximum.
3. Power Protection: Reverse polarity, over voltage, transient.
4. ACS Server to Site Controller communications interface: LAN or WAN
5. Site or Net Controller to Door Controller communications interface: RS-485 multi-drop, 2-wire
6. Supervisory Relay: Rated 2A, 30VDC Form C. Opens on Site Controller fault
7. History Buffer: 2,000 transactions

8. Priority Event Buffer: 100 transactions
9. On-Board Memory and Clock Backup: 24 hours minimum
10. Alarms: Lost AC input
11. Tamper Alarm: On-board switch
12. Connectors: 5 mm screw terminals
13. Address Switches: Rotary, direct-reading, 000 to 999.
14. Operating Environment:
    a. Between 14° F and 104° F (-10° C and 40° C)
    b. Less than 90 percent noncondensing humidity
15. Supports T-TAP, Daisy Chain, or Star Topology connectivity

N. E-Series Net Controller (NetDCD-1 & NetDCD-2):

1. Description:
    a. Designed to control a maximum of 100 Access Readers, Floor Relays, or General Relays (Practicable Limits: 64 Floor Relays or 80 General Relays per Site Controller; however, doors alone can reach maximum of 100), including the one or two Access Reader connections onboard.
    b. Normally used for a single site or building, contains a real-time clock and sufficient memory to supervise site up to 10,000 Cardholders.
    c. Maximum of 1,000 Net controllers can be addressed in an Ultra ACS.
    d. Transaction history is automatically buffered when not online with ACS Server.
    e. Priority event buffer assures alarms are annunciated in a timely manner even if history buffer is full.
    f. On-board switches select operational modes.

2. Power: 9 to 14 VDC, supplied by central power supply; 50 mA standby, 90 mA maximum.
3. Power Protection: Reverse polarity, over voltage, transient.
4. ACS Server to Net Controller communications interface: LAN or WAN
5. Site or Net Controller to Door Controller communications interface: RS-485 multi-drop, 2-wire
6. Supervisory Relay: Rated 2A, 30VDC Form C. Opens on Net Controller fault
7. History Buffer: 2,000 transactions
8. Priority Event Buffer: 100 transactions
9. On-Board Memory and Clock Backup: 24 hours minimum
10. Alarms: Lost AC input
11. Tamper Alarm: On-board switch
12. Connectors: 5 mm screw terminals
13. Address Switches: Rotary, direct-reading, 000 to 999.
14. Operating Environment:
    a. Between 14° F and 104° F (-10° C and 40° C)
    b. Less than 90 percent noncondensing humidity
15. Supports T-TAP, Daisy Chain, or Star Topology connectivity

O. Relay Controller (RCD):

1. Power: 9VDC to 14VDC, supplied by central power supply; 35 mA standby current, 20 mA additional for each relay activated
2. Memory and Clock Backup: 24 hours minimum
3. Relay Outputs: 7 Form C contacts, rated 30 VDC maximum at 2A
4. Supervisory Function: Relay 0 on first board installed. Opens on system fault
5. Communications: Multi-drop RS-485, proprietary protocol
6. Tamper Alarm: On-board switch
7. Configuration Jumpers: J3, relay polarity, select all 16 relays; J5, relay override selectable
8. Address Switch: Rotary, direct-reading, 0 to 9.
9. Operating Environment:
    a. Between 14° F and 104° F (-10° C and 40° C)
    b. Less than 90 percent noncondensing humidity

P. Power Supply:

1. Power: 120VAC, 60Hz, 2A, unswitched [or 240VAC, 50Hz, 1A, unswitched (export)]
2. Fuses: 2A AC input, slow-blow, [1A AC input (export)], 8A (battery output protection)
3. Output: 13.8 VDC nominal, 5A maximum
4. Battery Backup: 2 gelled, lead-acid cells, 6VDC, 8.0Ah, supplied with power supply
5. Alarm Outputs: Cover tamper switch and AC or power supply failure (dry contacts)

Q. Elevator Controller (ECU):

1. Description:

    a. Provides 16 relays for elevator floor control
    b. Each Site Controller can support a maximum of 4 Elevator Controllers, giving a maximum of 64 Floors per Site Controller.
    c. Each group of Elevator Controllers supports a maximum of 10 Elevator Access Readers

2. Power: 120VAC, 60Hz, 2A, unswitched [or 240VAC, 50Hz, 1A, unswitched (export)]
3. Power Supply Output: 5VDC, 1A, for local circuit board only
4. Memory and Clock Backup: 24 hours minimum
5. Relay Outputs: 16 Form C
6. Contact Ratings: 5A, 30VDC; 10A, 125VAC; 6A, 277VAC.
7. Normal Mode: Energized
8. Override Input: Normally closed
9. Unit Address: 4 position dip

10. Alarm Inputs: 4 unsupervised
11. Tamper: Built-in switch with activation spring

R. Elevator Reader Interface (ECD):

1. Description:
   a. Designed to mount inside of, or on top of, elevator car
   b. Contains reader and communications circuitry to interface with Elevator Controller
   c. Maximum of 10 Elevator Reader Interfaces can be used for each Site Controller
2. Power: 9VDC to 14VDC, supplied by transformer (on cab) or from Power Supply; 80 to 110 mA depending upon reader technology
3. Power Protection: Reverse polarity, overvoltage, and transient
4. Access Reader technologies supported: Wiegand card (any bit format up to 50), ABA/ISO track 2, proximity, keypad, biometrics, Bluetooth, NFC, WiFi, etc.
5. Access Reader interfaces supported: clock/data, clock/data inverted, and Wiegand
6. Connectors: 5 mm plug-on screw terminal
7. Address Switches: Rotary, direct-reading, 0 to 9.
8. Communications: Multi-drop RS-485, proprietary protocol
9. Operating Environment:
   a. Between 14° F and 104° F (-10° C and 40° C)
   b. Less than 90 percent noncondensing humidity

END OF SECTION

PART 3 EXECUTION

3.1 EXAMINATION

Examine areas to receive ACS. Notify Architect if areas are not acceptable. Do not begin installation until unacceptable conditions have been corrected.

3.2 INSTALLATION

A. Install ACS in accordance with manufacturer's instructions
B. Install ACS at locations as indicated on the drawings
C. Install door hardware as specified in Section 08710
D. Install electrical wiring to online system components as specified in Section 16100
E. Use manufacturer’s supplied hardware
F. Replace defective or damaged components as directed by the Architect
G. Furnish to the Owner all required Credentials

3.3 FIELD QUALITY CONTROL

Test completed installation to verify each component of ACS is properly installed and operating

3.4 ADJUSTING

A. Adjust ACS as required to perform properly
B. Adjust locksets for smooth operation without binding

3.5 CLEANING

A. Clean surfaces in accordance with manufacturer's instructions
B. Use cleaners approved by manufacturer, as some cleaners may damage Access Readers
C. Do not use abrasive cleaners

3.6 DEMONSTRATION

A. Provide a maximum of 2 consecutive days of on-site service by manufacturer

    1. Demonstrate system to Owner’s personnel
    2. Train Owner’s personnel in proper operation and maintenance