Electronic Access Control System

Specifications for Architects & Engineers 28 13 00

August 1, 2024

SECTION 281300 Specifications for Architects and Engineers

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. EID 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. Other associated hardware and software components
Q. 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
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
B. UL 294 - Standard for Access Control System Units
C. FCC - Code of Federal Regulations, Title 47, Part 15, Class B
D. Federal Information Processing Standards Publication 197 – Advanced Encryption Standard

E. EMC Directive 89/336/EEC
F. International Organization for Standardization - ISO 8601 Data elements and interchange formats – Information interchange – Representation of dates and times
G. NFPA 70: National Electric Code (NEC)
H. NFPA 101: Life Safety Code
I. NFPA 730: Guide for Premises Security
J. 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.
   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.
K. 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).
L. 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.

M. 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.
N. 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 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 or Linux Server operating system platform (Ubuntu) and MS SQL or PostgreSQL database servers. The ACS is additionally 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. Software shall be Millennium Ultra Version 7.0 and up.

Supported Operating Systems:

1. Windows 10 Pro, 11 Pro
2. Windows Server 2012 R2
3. Windows Server 2016
4. Windows Server 2019
5. Windows Server 2022
6. Linux Ubuntu v. 18 and up

Required: .NET 8 Framework
Only 64-bit OS versions for Windows supported

Supported database server versions:
MS SQL 2012, 2014, 2016, 2019, 2022 with Advanced Services / Tools
PostgreSQL versions: 9.5 and up.

Client Requirements:
Web version supports any well-supported web browser, including Internet Explorer, Edge, Firefox, Chrome, and Safari; or Millennium Windows Client App

Database:

1. Supplied with full support of Microsoft SQL 2012 –2022 database server application and PostgreSQL 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 because of the import process.
4. Allows for a unique industry standard ISO card number to be generated on demand as part of the 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 each 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 the operator can view, add, modify, delete, or print reports, and is limited by the Tenant(s) to which they have rights as well as by Operator Level.

Server Requirements:

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

1. Reliable brand PC (Dell, HP, etc.) (Min. 3-year onsite warranty)
2. Windows 10 or 11 Premium, 64-bit; Linux (Ubuntu)
3. Processor: Intel i5 Processor
4. RAM: 8 Gb
5. Storage: 2TB SATA Drive
6. Graphics: Intel onboard graphics
7. Printer: Support any Windows installed printer for reports.

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

1. Reliable brand PC (Dell, HP, etc.) (Min. 3-year onsite warranty)
2. Windows 10 or 11 Pro, 64-bit or Windows Server version 2012-2022 or Linux (Ubuntu)
3. Processor: Intel i7 Processor
4. RAM: 12 GB
5. Storage: 256GB SSD and 8TB SATA Drive
6. Graphics: Intel onboard graphics and 2 HDMI out for dual monitors
7. Printer: Support any Windows installed printer for reports.

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

a. Reliable brand Server (Dell, HP, etc.) (Min. 3-year onsite warranty)
b. Windows Server 2012 R2 or 2022 or Linux (Ubuntu)
c. Processor: Xeon E-Series Processor
d. RAM: 16 GB
e. Storage: 256GB SSD and 8TB SATA Drive or RAID Configuration
f. Graphics: Dual video out for situational awareness
g. Printer: Support any Windows installed printer for reports.

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 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 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 manufacturer's 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:

i Installers shall have a demonstrated history of successfully installing and servicing an ACS of an equivalent size, scope, and complexity.

ii Installers shall be capable of providing evidence that they are trained and authorized by the ACS manufacturer.

iii 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.

PART 2 - PRODUCTS

2.0 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.
588 Boston Post Road, STE 384, Weston,
MA 02493
Phone: (866) 455-5222
Url: www.mgiaccess.com

B. The software shall be Millennium Ultra Version 7.00 or later.

C. Site Controllers shall be Millennium E-Series ESCU Site controllers, Millennium PoE Controller 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.

2.1 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, 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.
7. Door controllers shall support any Wiegand standard Access Readers in any bit format up to 255 bit total; bit patterns are fully programmable within Ultra ACS

8. 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, OSDP, etc.
9. Door Controllers will be able to be programmed for custom ABA formats from the software, including the ability to ignore user specific characters in format.
10. Door Controllers shall be programmable to accept either normal or inverted strobe signals from ABA format readers.
11. Door Controller shall be programmed for appropriate Access Reader technology.
12. Site Controllers shall buffer the last 2,000 events from Door Controllers when LAN or WAN communication has been lost or interrupted.
13. Each Door Controller shall buffer an additional 2,000 events when its Site Controller buffer has been filled.
14. All ACS Controllers shall have a built-in tamper alarm to detect when a cover to the controller is removed.
15. 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 12 VDC
16. Door and Relay Controllers shall have Form C dry contact configurations
17. 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
18. 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 Toggle Mode
19. Relay Controller shall have relays that can be configured by software for Time Period Activation, Time Activation, Time Released, First Event Activation, First Event Released, and Alarm Latch
20. Relay on Door Controller shall have a programmable timer and settings in software for electric strike and magnetic lock operation
21. 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
22. 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.

2.2 HARDWARE

(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 the history buffer is full.

2. Power: 10 to 14 VDC, supplied by PS1 central power supply; 375 - 500 mA, depending upon reader technology. Accessory relays require an additional 20 mA each.
3. Power Protection: Reverse polarity, overvoltage, and transient
4. Access Reader technologies supported: Wiegand Credential (any bit format up to 255), ABA/ISO Track 2, proximity, keypad, combination reader/keypad, biometrics, NFC, Bluetooth, etc.
5. Access Reader Interfaces Supported: clock/data, clock/data inverted, Wiegand
6. History Buffer: 2,000 transactions
7. On-Board Memory and Clock Backup: 24 hours minimum
8. Maximum Cardholders stored in memory: either 40,000 for Door Controller or 20,000 for Net Site/Door Controller
9. Alarm Input Points: 7 total, 2-wire supervised, Two or four state selectable (EOL resistor) including, built-in door contact monitoring
10. Alarm Input Monitoring Circuit: Analog to digital conversion
11. Tamper Alarm: On-board switch
12. Output Relays: 2 each with Form C contacts rated 2A, 30VDC
13. Output Relay Contact Protection: Solid-state polymeric resettable
14. Connectors: 5 mm plug-on screw terminal
15. Address Switches: Rotary, direct-reading, 00 to 99.
16. Communications: Multi-drop RS-485, proprietary protocol
17. Operating Environment:
    a. Between 14◦ F and 104◦ F (-10◦ C and 40◦ C)
    b. Less than 90 percent noncondensing humidity
18. 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: 100 Floor Relays or 100 General Relays per Site Controller; however, doors alone can reach maximum of 100)

b. Maximum of 1,000 site controllers can be addressed in an Ultra ACS.

c. Transaction history is 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.

e. On-board switches select operational modes.

2. Power: 10 to 14 VDC, supplied by central power supply; 200 mA standby, 300 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. History Buffer: 2,000 transactions
7. On-Board Memory and Clock Backup: 24 hours minimum
8. Alarms: Lost AC input
9. Tamper Alarm: On-board switch
10. Connectors: 5 mm screw terminals
11. Address Switches: Rotary, direct-reading, 000 to 999.
12. Operating Environment:
    a. Between 14◦ F and 104◦ F (-10◦ C and 40◦ C)
    b. Less than 90 percent noncondensing humidity
13. 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 sites for up to 20,000 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: 10 to 14 VDC, supplied by central power supply; 350 mA standby, 550 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. On-Board Memory and Clock Backup: 24 hours minimum
9. Alarms: Lost AC input
10. Tamper Alarm: On-board switch
11. Connectors: 5 mm screw terminals
12. Address Switches: Rotary, direct-reading, 000 to 999.
13. Operating Environment:
    a. Between 14◦ F and 104◦ F (-10◦ C and 40◦ C)
    b. Less than 90 percent noncondensing humidity
14. Supports T-TAP, Daisy Chain, or Star Topology connectivity

Relay Controller (ERCD):

1. Power: 10VDC to 14VDC, supplied by central power supply; 350 mA standby current, 20 mA additional for each relay activated
2. Memory and Clock Backup: 24 hours minimum
3. Relay Outputs: 4 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. Address Switch: Rotary, direct-reading, 0 to 9.
8. Operating Environment:
   a. Between 14◦ F and 104◦ F (-10◦ C and 40◦ C)
   b. Less than 90 percent noncondensing humidity
9. Supports T-TAP, Daisy Chain, or Star Topology connectivity

Elevator Controller (ECU3):

1. Description:
   a. Provides 16 relays for elevator floor control
   b. Each Site Controller can support a maximum of 6 Elevator Controllers, giving a maximum of 96 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. Address Switch: Rotary, direct-reading, 0 to 9.
10. Tamper: Built-in switch with activation spring.

Elevator Reader Interface (ECD3):

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: 10VDC to 14VDC, supplied by transformer (on cab) or from PS1 Power Supply; 380 to 550 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, Wi-Fi, 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

E-Series Net Controller (NEW POE BOARD):

1. Description:
    a. Designed to control a maximum of 100 Access Readers, Floor Relays, or General Relays (Practicable Limits: 96 Floor Relays or 99 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 sites for 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 history when buffer is full.
    f. On-board switches select operational modes.
2. Power: 10 to 14 VDC, supplied by central power supply; 450 mA standby, 550 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. On-Board Memory and Clock Backup: 24 hours minimum
9. Alarms: Lost AC input
10. Tamper Alarm: On-board switch
11. Connectors: 5 mm screw terminals
12. Address Switches: Rotary, direct-reading, 000 to 999.
13. Operating Environment:
    a. Between 14◦ F and 104◦ F (-10◦ C and 40◦ C)
    b. Less than 90 percent noncondensing humidity
14. Supports T-TAP, Daisy Chain, or Star Topology connectivity
15. Supports Bluetooth Connectivity for Board Configuration and Setup

Smart Locks (Wireless Handles):

1. Description:
    a. Millennium wireless locks offer an alternative to hardwired access control for residential doors or challenging installation locations. These locks seamlessly connect to the Millennium Ultra software.

b. Designed for various settings such as villas, offices, apartments, student housing, and Airbnb rooms, the stylish wireless handles empower users to manage access with precision.

2. Features:
   a. Keyless Entry
   b. Audible Alert
   c. Integration with Millennium Ultra
   d. Remote access through the Mobile App
   e. Battery Level Monitoring
   f. Holds up to 200 cardholders.

2. Power: 6V (4xAA Batteries).
3. Lock Panel Material: Aluminum Alloy
4. Mortise Material: Zinc allow
5. Battery Life: Up to 2 years – one Wi-Fi update per day
6. Application Door Thickness: 1.3” -2.1”
7. Backup Unlock Mechanism: Mechanical Key, USB emergency power interface
8. Working Temperature: -4°F to 122°F
9. Opening Direction: left inside, right inside, left outside, right outside.
10. Mortise Grade Level: C-level true plug core copper lock cylinder.
11. Working Humidity 20%-70%
12. Dimensions: 10.25” x 2.75” x .9”
13. Weight: 6.6 lbs.

2.3 ACCESS CONTROL SYSTEM (ACS) OVERVIEW

A. System Description

1. The Physical Access Control System (ACS) shall be an IT standards compliant, full featured physical access control system solution. The ACS shall be built upon an industry standard Microsoft Windows operating system or Linux operating system and relational database server infrastructure.

2. The ACS shall utilize a network-based architecture. All ACS components, including Intelligent Field Controllers and client workstations shall communicate over industry standard TCP/IP network infrastructures.

The ACS shall be configured in a traditional client server model. The ACS database server shall act as the central repository for all system configuration and activity.

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

4. All passwords required to login to the ACS shall be encrypted within the system database.

5. The ACS architecture shall enable distributed decision-making at the Intelligent Field Controllers. The ACS architecture shall enable complete ACS functionality during periods where communication is lost between an ACS and its associated Intelligent Field Controllers. During downtime, the Intelligent Field Controllers shall maintain an audit log of all ACS activity that occurred and shall upload this data to the ACS once normal communications is restored.

6. The ACS architecture shall provide scalability to support the addition of card readers and/or input/output points. Additional Intelligent Field Controllers may be added to increase ACS capacity as required.

7. The ACS shall support integration with 3rd party subsystems. Integration shall be possible with 3rd party IT and business systems. The ACS shall be able to pull information into its system database and push events out to 3rd party systems.

8. The ACS shall provide a single software-based license key that resides on each ACS server to control licensable features and/or components. Software licenses shall be upgradable through fast and efficient methods and shall be available for distribution via email or manufacturer secured web site. Individual license keys for client workstations and/or physical hardware license keys shall not be acceptable.

9. The ACS shall support seamless and efficient upgrades of the ACS application software. In addition, all systems of the same generation shall be upward compatible, allowing them to start small and grow as the user's system needs grow. Access control field hardware devices shall not have to be replaced as the system grows to larger levels.

2.4 ACCESS CONTROL SYSTEM (ACS) CAPACITIES

A. ACS Capacities

1. Card Readers: Unlimited
2. Each Site Controller: 100 Access Readers, Floor Relays, or General Relays (Limit 96 Floor Relays or 80 General Relays per Site Controller; however, doors alone can reach maximum of 100)

3. Up to 1,000 site controllers per Ultra instance or 100,000 Access Points
4. Number of Tenants: Unlimited
5. Number of Access Levels: Unlimited (10 per tenant per Credential)
6. Supports multiple Access Reader technologies and protocol on same Door Controller simultaneously (up to 4 formats)
7. Supports combination Access Readers with one Wiegand output.
8. Support custom Wiegand outputs from 0 to 255-bits, including 32-bits, 37-bits, HID Corporate 1000 program, and Motorola 27-bit.

9. Supports 3rd party integrations including:

    i Milestone xProtect IP based video security solutions

    ii Allegion AD Lockets; LE & NDE Locksets; Control Deadbolts; Engage Gateway and PIM integrations

    iii Assa Abloy IN120 based Wireless door solutions

    iv Assa Abloy VINGCard door management solutions

    v DMP XR Series Intrusion systems

    vi BOSCH G Series Panels B9512G and B8512G

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

10. Able to accept any facility code of card provided (0 to 256) facility code.
11. Supports dual authentication with a pin number along with a Credential that is enabled via Time Period.
12. Supports unique Cardholder Record Number or optionally not required.
13. Option to rename fields on the Cardholder page.
14. Allows up to three Credentials to be programmed per Cardholder.
15. Supports anti-passback modes.
16. Option to rename fields on the Cardholder page.
17. Allows up to three Credentials to be programmed per Cardholder.
18. Supports “disable card” function for each Credential.
19. Supports a door controller address and text description name in a field
20. Supports Primary and Secondary relays included with each door controller.
21. Supports “Auto Activate” for a Door to automatically unlock and automatically relock an electric strike or magnetic lock according to the Time Period set.
22. Supports First User Auto Active, as above, but only after first valid Cardholder presents Credential to Door Reader.
23. Notifies when the status of a door or relay controller changes because of a communication or device problem.
24. Supports programmable reports viewed on monitor or printed.

25. Provides capability of sorting historical events by time, dates, cardholders, access readers, and operators.
26. Ability to preprogram dates for Daylight Savings Time.
27. Supports relays that can be programmed to operate by a Time Period, alarm, or by event, linked to Access Points.
28. Have the Owner's name encrypted on Site Controllers and displayed on monitor.
29. Capability to automatically archive activity and alarm data and be able to select date range being archived.
30. Provides communication to sites using LAN or WAN.
31. Advises and displays on computer monitor, the status of Site, Door, and Relay controllers, if communication or power is lost on ACS hardware.
32. Alarm Input Points: Unlimited
33. Relay Output Points: Unlimited
34. Cardholders: Unlimited
35. Concurrent Client Connections: Unlimited
36. On-line Event History Log: 500,000,000

2.5 PHYSICAL ACCESS CONTROL SYSTEM (ACS) SOFTWARE

A. Access Control Functionality

1. Alarm Attributes - The ACS shall allow Operators to configure how each alarm annunciates in the Alarm Monitor Application. The Alarm grid shall list all alarms with their associated data.

For each alarm in the system, Operators shall have the option to:

a. Display the alarm in the Alarm Monitor Application.
b. Mask the alarm or event from displaying in the Alarm Monitor Application.
c. Display text instructions that shall guide the Operator in responding to the alarm.
d. Have the alarm display in priority order based on the priority of the alarm. A minimum of 100 priorities shall be supported.
e. Set the priority of the alarm or event, as well as its associated Return to Normal event priority.
f. Store the alarm information for later retrieval.

2. Alarm Logging - All alarms in the ACS shall log by default to the ACS internal data storage logging structure.

3. Off-Line Alarm/Event Queue - The ACS shall queue Alarms that occur while the Alarm Monitor Application is off-line with the rest of the system or when an Operator is not logged into the Alarm Monitor Application. Upon logging in and accessing the Alarm Monitor Application, all queued alarms shall report into the Alarm Monitor Application for Operator action.

4. Alarm/Event Synchronization - The ACS shall support Alarm Synchronization for alarms that report into multiple Alarm Monitor Applications. When an alarm or event is acknowledged or cleared by an Alarm Monitor Application Operator, it shall be cleared from all other Alarm Monitor Applications.

5. Alarm Reporting Based on Schedule - The ACS shall support the reporting of alarms to Alarm Monitor Applications based on time zones. Each alarm in the system shall have the ability to have its own associated schedule.

6. Alarm/Event Text Instructions - The ACS shall allow each alarm in the system to have associated text instructions defined that guides Alarm Monitor Application Operators through alarm response procedures. Text instructions shall be a minimum of 1040 characters in length.

7. Access Levels - The ACS shall allow cardholder access to secure areas based on card reader, time, and day. An Access Group shall consist of card reader and time zone combinations. Access Groups shall consist of any number of card readers in the system each assigned to a time zone. Any card reader shall have the ability to belong to any Access Group and a card reader shall have the ability to belong to multiple Access Groups. Access Groups shall support conventional names up to 50 alphanumeric characters.

8. Time Periods- The ACS shall support a minimum of 255 Time Periods per Site controller. Time Periods shall serve as templates for application to Access Groups, masking devices, and device modes, among others. Each time zone shall have the ability to be assigned to any day(s) of the week and shall be assigned to function on a holiday.

   Time Periods shall be downloaded to all related Site Controllers for local processing and decision making. Time zones shall support conventional names up to 50 alphanumeric characters.

9. Threat Levels – The system shall support 6 Threat Levels with each one being controlled though Threat Level Settings. The system shall be able to send Door / Floor Commands to define Door and Floor Groups. Threat Levels are assigned to Access Levels as well as Operators. Threat Levels can restrict Operator access to the system as well as restrict Cardholder Access.

10. Holidays - The ACS shall allow specific dates and/or date ranges to be designated as Holidays. Items such as card reader modes, a cardholder's access rights, and masking time zones may be altered when a specific day has been designated a Holiday. The ACS shall support a minimum of 255 Holidays. Each Holiday shall have the ability to span multiple days. Holidays shall support conventional names up to 50 alphanumeric characters.

11. Card Reader Options - The ACS shall allow the following options to be defined for card readers in the system:

    a. Event Triggers shall allow Operators to place the card reader in a custom mode during a pre-defined time. At the completion of the time, the card reader shall revert to its Normal operating mode.
    b. Door Forced Filter shall reduce false alarms for doors that "bounced". Opening the door within 3 seconds of the door closing shall not report a Door Forced Open alarm.
    c. Mask Alarms shall allow Door Forced Open and Door Held Open alarms to mask either permanently or during a scheduled basis. Distinct schedules shall be able to be assigned to different Alarm Types.
    d. Relay Setup shall allow Operators to define, upon a valid access, whether the door strike remains active for the entire strike time/turns off after the door has closed or to deactivate as soon as the door is open.
    e. Allow REX to Activate Relay shall determine if the door strike should not be pulsed upon a valid request to exit.
    f. Send Request to Exit Messages shall not log request to exit transactions to the database.
    g. Log all Access as Used shall be configured when there is not a door contact at the door to monitor door position. Upon a valid access grant, the ACS shall assume entry and report an event into the Alarm Monitor Application.
    h. Two Card Control shall require that two valid access requests occur prior to granting access to the door. Both requests must occur within a 10 second period. In the event a second valid access has not occurred within 10 seconds of the first valid access request, the card reader shall reset, and the first badge shall have to be presented again.
    i. Auto Activate shall allow Operators to activate outputs attached to the card reader on a scheduled basis.
    j. Shunt Delay shall define the number of seconds prior to a generated Door Ajar alarm.

12. Emergency Mode Overrides - The ACS shall support the ability for Door reader modes to be overridden from the standard mode. Based on the card reader type, custom modes shall include card only, card and PIN, card or PIN, locked, unlocked, and facility code. At the end of the scheduled override, the card reader shall return to its default standard mode.

13. Multiple Card Formats - The ACS, Intelligent Field Controller, and card readers shall all support a minimum of 4 card formats. Wiegand and Magnetic Stripe card formats shall both be supported. The ACS shall support any industry standard Wiegand card format

and any magnetic stripe card format that uses a card number, facility code, and issue code combination. The ACS shall support a reverse card read for Wiegand formats.

14. Pre-Alarm - The ACS shall support a door held open pre-alarm capability. When a door has been held open for a pre-determined amount of time after a valid access grant, an alarm and a local audible annunciation shall alert the cardholder to close the door. Failure to close the door between the pre-alarm annunciation and the configured door held open time shall generate an alarm at the Alarm Monitor

15. Custom Device Mappings / Local Alarms – Local Alarms shall give Operators the ability to assign a unique group of alarm attributes to specific device-alarm combinations to override the global settings for generic attributes. For example, Operators may assign a different set of attributes to be applied to a 'forced door' at a research lab than they would for a 'forced door' at a perimeter location.

16. Entry / Exit Delay - Operators shall have the ability to set up Shunt delays for inputs that are attached to any controller with the ability to set up Ignore Time Periods. The ACS shall support a maximum of 99 seconds for entry and exit delays.

17. Alarm Input Options - The ACS shall allow the following options to be defined for inputs on the Reader Controller:

    a. Hold Time shall be the amount of time in seconds to wait to report an input activation as restored when an input goes active and then is restored. The hold time shall be configurable from 99 seconds.
    b. Alarm Masking shall allow the input to be masked either all the time or during a defined schedule.
    c. Activate Output shall allow Operators to configure an output to activate all the time or during a defined schedule.
    d. Logging shall allow Operators to determine whether to log all change of state events or only when the event is not masked.

18. Relay Output Options - The ACS shall allow the following options to be defined for outputs on the Reader Controller:

    a. Relay Output Mode shall set the default mode of the relay output.
    b. Seconds Active shall define how long the output shall pulse when the command is given.
    c. Activation Time Period shall define the time the relay output is active.

19. Alarm External Commands - The ACS shall support Alarm Definitions with Assigned Commands whereby an input/output/event in an Intelligent Field Controller can trigger an action within the same Intelligent Field Controller. All linkage decisions shall be made at the host level.

20. Operators shall be able to Hot Commands each consisting of a sequence of single or grouped actions to be performed, such as changing card reader modes and activating outputs. Operators shall then be able to link events to the aforementioned. Hot Commands such that a particular action will trigger a Hot Command to execute.
21. To simplify the ability to trigger multiple actions as the result of a single event, the ACS shall allow Operators to create Hot Command groups that may include multiple actions associated with a single event.

22. Cardholder filters shall be available to allow activity from specific Cardholders to trigger an action.

23. Inputs shall include any Site/Door Controller level event, including but not limited to:

    a. Site Controller Events
        1). Cabinet tamper
        2). Power failure
        3). Communication failure

    b. Door Controller Events
        1). Door controller tamper
        2). Door forced open.
        3). Door held open.
        4). Power failure

Additional filters shall be applied so that an Event Input can be filtered to a specific hardware device.

Hot Command actions shall include, but not be limited to:

a. Activating an Output Control Module Output
b. Shunting/Clear Shunt for an Alarm Input
c. Setting the active mode of a card reader

An Alarm/Event Definition may trigger a Hot Command which shall have the ability to trigger a single or multiple commands.

B. Cardholder Management Functionality

1. Cardholder Management Integration - The ACS shall offer an integrated Cardholder Management and Enrollment functionality as part of the core system functionality.

2. Data Import - The ACS shall have the ability to import Cardholder records and their associated image in a standard jpeg format. Cardholder records shall be able to be preloaded prior to implementation or added at any time after deployment.

3. Cardholder Enrollment - The ACS shall allow individual enrollment of Cardholders. Each Cardholder shall allow entry of required and optional fields.

   A Card shall be created and assigned during enrollment. For each Badge, a Badge ID and, if applicable, an Embossed number and PIN code shall be assigned. The ACS shall support a minimum of 10 digits Badge ID. The ACS shall also allow an Operator to set the activation and deactivation date of the Badge.

   A Cardholder shall have the option to be added to a Badge Template during enrollment. During
   Enrollment, the Cardholder's image shall be captured or loaded in from a JPEG file format and a badge template shall be assigned.

4. Badge Re-Issuance - Should a badge need to be re-issued, the process shall be fast and efficient. The Operator shall be able to first deactivate the existing credential. The ACS shall be able to use the existing Cardholder information and photo for the new badge, thus not requiring re-enrollment of the cardholder. The re-issuance process shall automatically remove access rights from the deactivated Card and enable those same rights in the new Card, including automatically sending the appropriate changes to the intelligent controllers.

5. Cardholder Database - Each Cardholder shall have a unique record in the system database. Operators shall be able to construct their Cardholder data to meet their needs through the addition of User Defined Fields and Forms.

6. Deleting Cardholders - The ability to delete Cardholders shall be permission controlled such that only the Operator with this rights shall have this capability.

7. Assign Access Groups - The ACS shall allow Operators to assign Access Levels to Cardholders. Each may have up to 10 Access Levels assigned to their record per tenant.

   All modifications to Access Levels or assignments shall be automatically downloaded to the appropriate Site and Door Controllers without Operator intervention as soon as possible after a Cardholder record is saved.

   Additionally, and optionally, the ACS shall support the ability to import industry standard JPEG or PNG photos from digital cameras or other image capture sources.

   Images shall be associated with the Cardholder and shall be stored in the system database.

8. Badge Activation and Deactivation Dates - The ACS shall support activation and deactivation dates for all Badges created. A Badge shall have the ability to be configured to activate at a future date from time of creation. When a Badge reaches its deactivation date/time, the ACS shall automatically deactivate the access rights associated with the Card. All access rights of a Card shall be eliminated after the deactivation date. Should the Cardholder become authorized for access again, new access rights shall be applicable to the same Badge, and re-issue shall not be required.

9. Badge Issue Codes - The ACS shall support a minimum of a 1-digit issue code.

10. PIN Codes - The ACS shall support up to 8-digit PIN codes. Each cardholder in the ACS shall have the ability to choose a PIN to be associated with their record. A cardholder's PIN shall have the ability to be changed should the original PIN code be compromised.

11. Credential Options - The ACS shall support industry standard pre-encoded physical credential options including:

    a. Composite Credentials such as PVC cards
    b. Proximity Credentials including dual PVC technology that includes both proximity and magnetic stripe technology.
    c. Contact Smart Credentials
    d. Mifare Credentials
    e. DESFIRE Credentials
    f. HID iClass Credentials
    g. UMC Mobile Credentials

13. Multiple Active Badges - The ACS shall allow Cardholders to have multiple active Badges associated with their record. A maximum of 3 active Badges may be assigned to a Cardholder.

14. Badge Printing – The ACS shall allow for the printing of a badge.

15. Deactivate Badge Access - The ACS shall allow Operators to revoke access privileges from a cardholder by updating that cardholder's Badge status. A Badge with Deactivated access shall immediately stop functioning at all card readers.

16. Search Capabilities - The ACS shall have the ability to search Cardholders by First Name, Last Name or by any Cardholder or Badge field in the system. The ACS shall allow multiple field-based cardholder / badge searches.

17. Drop-Down Entries - The ACS shall include a Drop-Down Entry builder that allows Administrators to define Operator selection options that appear in Cardholder form pick lists. Each pick list shall have an unlimited number of pre-defined selections.

18. The ACS shall support the standard Cardholder and Card fields:

    a. Last name
    b. First name
    c. Middle Name
    d. ID
    e. E-mail Address
    f. Status
    g. Photo
    h. Encoded Number
    i. PIN
    j. Badge Status
    k. Issue Level
    l. Activation Date
    m. Expiration date

19. Access History - The ACS shall provide a form listing the most recent transaction activity associated with a Cardholder, without having to run a report. Information provided shall include transaction activity, time/date, and related badge.

20. User Defined Fields - The ACS shall support the ability to add additional Cardholder User Defined Fields. Unlimited number of User Defined Fields shall be able to be added. Each user defined field shall be given a Field Name.

21. Badge Layout Tool - The ACS shall support a tool to allow for the custom creation of Cardholder/Badge Layouts.

    The ACS shall support any size badge provided the printer used for badge creation supports the desired badge size.

    The ACS shall allow multiple objects to be configured for a badge layout including alphanumeric text fields, database fields, photos, cardholder photos, and graphics such as logos.

    Each text and database field added to the layout shall have the ability to employ the following properties: location of the object, background color, typeface of text, size of text, color of text, and horizontal and vertical alignment of text.

    Each Photo and Graphic field added to the layout shall have the ability to employ the following properties: location of the object, height and width, and horizontal and vertical alignment.

C. Alarm/Event Definitions

1. Alarm Acknowledgment - The ACS shall allow Operators to configure how alarms should be acknowledged into the Alarm/Event Viewer. The Alarm/Event Viewer shall be user configurable to play an audible notification at the workstation when alarms arrive in the system. Each alarm shall have the capability to be distinctly configured. Each alarm shall have the following configuration options:

    a. Display in the Alarm/Event Viewer.
    b. Be masked from displaying in the Alarm/Event Viewer.
    c. Display Text Instructions that shall guide the Operator in alarm response.

2. Alarm Management and Handling - The ACS Alarm/Event Viewer shall provide a real time count of all alarms in the Alarm/Event Viewer awaiting Operator action. The ACS shall support the following options for handling / responding to alarms upon selection:

    a. Acknowledge the alarm.
    b. Review text instructions on pre-defined alarm response.
    c. Enter unlimited Notes on reason for alarm and/or action taken in alarm response.
    d. Review the History of the alarm.
    e. For alarms or events with Video associated, automatically launch the Video Player to display a live video feed from the camera associated with the device that generated the alarm or event.
    f. Clear the alarm.

3. Bulk Alarm Management and Handling - The ACS shall support the ability to manage and handle multiple alarms. Upon selection, Operators shall have the ability to clear all selected alarms in a single action.

4. Alarm Filters – The ACS shall support Alarm filtering by Category, Location, or Device. Operators shall have the ability to filter and display a subset of alarms with a single click of the mouse.

5. Hold Queue – The ACS shall support the ability to hold incoming alarm traffic while other alarm activity is being processed. The alarm queue can be restarted at any time, and all queued up alarms shall then report into the Alarm/Event Viewer with their proper time stamps.

6. Alarm Masking - The ACS shall allow masking of specific alarms based on pre-defined Time zones or via manual overrides.

7. Alarm Sorting - The ACS shall allow alarms to be sorted in the Alarm/Event Viewer by any of the currently configured viewable columns.

8. The Operator shall not be required to exit the Alarm/Event Viewer to access this information and this functionality shall not prevent additional alarm activity from reporting to the Alarm/Event Viewer.

9. Operator Control of Field Hardware Devices - The ACS shall allow Operators to manually control the state of field hardware devices and their input/output points.

    a. Card Readers – manually control reader state (unlocked, locked, facility code, card only, PIN only, card and PIN, card or PIN), pulse the door open, mask/unmask door forced opens/door held opens, disable the door, and restore the door to its correct state based on current schedule
    b. Alarm Inputs – mask and unmask input.
    c. Outputs – turn on, turn off, and pulse outputs.

    The ACS shall utilize a last command wins methodology. For example, if an output is set to off due to a schedule and an Operator manually turns it on, then the output will remain on until it is manually turned off or until the next scheduled interval occurs.

    All manual controls shall be recorded in the Operator Audit log with the time of the change, Operator performing the function, and description of the activity performed.

10. Maps - The ACS shall support graphical maps through the import of map backgrounds from standard 'off-the-shelf' drawing packages in the formats listed below:

    a. JPEG (.jpg)
    b. Portable Network Graphics (.png)

    The ACS Operator shall have the ability to place system icons including doors, alarms, cameras, and other access control field hardware to indicate their location in the facility.

    From the Map, operators shall be able to:
    a. Send commands to devices
    b. Momentarily open a door

D. Device Map

1. Devie Map - The ACS shall support a Devie Map that shall display a list of all controllers and doors defined in the system. For each door in the system, the Door Status page shall display:

    a. Door Name
    b. Current Door Mode
    c. Door Status including forced and held states, masking states, as well as communications and tamper states.

Options shall be available to control the operational state of the reader including:

    a. Disable

b. Lock
c. Unlock
d. Momentary

2. Recent Door Transactions - The ACS shall provide a form listing the most recent transaction activity associated with a door. The information provided shall include transaction activity, time/date, and cardholder & badge related details.

E. Image Verification

1. Swipe and Show Cardholder Image Verification - The ACS shall support Swipe and Show functionality that allows the display of the cardholder's photo as they swipe their badge through a specified card reader. Swipe and show allow Operators to verify the cardholder to their photo as they enter a portal.

2. Door History – The ACS shall allow Operators to view the most recent history of all access activity for a door with a transaction in the Alarm/Event Viewer with a single click of a button.

3. Cardholder History – The ACS shall allow Operators to view the most recent history of all access activity for a cardholder with a transaction in the Alarm/Event Viewer with a single click of a button.

F. Integration with Video/CCTV

1. The ACS shall support digital video integration with Onvif and RTSP digital video cameras. The digital video cameras shall be integrated with the ACS such that alarms generated by the ACS shall link to video, both live and recorded, on the video management system (VMS). Any alarm/event in the ACS shall have the ability to be associated with a digital video clip in real time. Each alarm/event in the ACS shall trigger the VMS to store a pre-defined number of seconds of video before the event occurred and a pre-defined number of seconds of video after the event occurred.

2. The ACS shall support LAN/WAN connectivity for streaming live video of a camera or for reviewing stored recorded video of alarm or event activity.

3. Playback Control

The ACS shall provide the following playback controls for viewing recorded video:

a. Start and Stop Playback - The Operator shall be able to start and stop playback.

b. Pause and Resume - The Operator shall be able to pause and resume current playback.

c. Skip Backward - The Operator shall be able to use the Skip Backward button to rewind the playback.

d. The Operator shall have the option to switch to Live Mode from a camera at any time during the operation.

e. Any alarm / event generated shall be configurable to automatically launch the Video Player in the ACS.

f. Should a VMS Server or any associated cameras go off-line, a specific alarm shall be sent to the ACS.

G. System Configuration and Administration

1. Alarm Logging - The ACS shall track and keep a comprehensive log of all alarm activity. All alarms that occur shall be logged with the following information:

   a. Alarm Name
   b. Time and Date Stamp
   c. Where the alarm occurred
   d. Acknowledgement information
   e. All Operator actions associated with the alarm or event.

   Alarm information can be viewed through the ACS reporting engine that shall list the total number of alarms that are logged in the ACS. The number of stored alarms shall be limited only by the amount of disk space available in the ACS.

2. Permissions - All major ACS features and functions shall be permission protected through the use of Operator Level controls. Each operator account shall be assigned an Operator Level, which shall include a list of permissions assigned to that Group, as well as individual permissions outside of the Operator Level, if applicable. Operator access to ACS screens, as well as their ability to view, add, edit, or delete ACS objects shall be controlled though permissions.

3. Software Based Licensing - The ACS shall support a software-based License Enforcement model. A hardware key or dongle shall not be acceptable for controlling licensed features and functionality.

4. On-Line, Context Sensitive Help - The ACS shall support on-line, context sensitive help to assist system users in the operation of the system. Once inside the help program, users shall be able to navigate the help files, moving to other areas of the documentation while having to go back into the application software. The help files shall have a linked table of contents, index, and search capability.

5. Operator Accounts - The ACS shall support Operator Accounts. Each operator account shall require a unique username and password to access the system. Each operator account shall also be assigned a Group, which shall determine the permission level for that account, thus controlling what functions the operator can perform in the system. In addition, individual permissions can be assigned to the operator account. All modifications to an operator account shall be stored in the ACS database for audit and reporting processes. The ACS shall support as many operator accounts as configured cardholders.

6. Password Protection - Each Operator Account shall require a unique username and password to access the ACS. This password, in association with the account's permission rights, shall restrict what screens the Operator can access and what tasks

the Operator can perform. An Operator shall be able to change their ACS password at any time.

7. Operator Activity Logging - The ACS shall track and keep a comprehensive log of all operator account activity. All changes that occur in the database shall be logged including, but not limited to:

    a. Operator Account Login / Logout Activity.
    b. Adding, Deleting, or Changing Cardholder Records.
    c. Change to system configurations such as field hardware, Access Groups, or Time zones.
    d. Activity performed inside the Alarm Monitor Application, such as acknowledging alarms, opening doors, or clearing events.

    The log shall include:

    a. Operator Account.
    b. Date and time of the activity.
    c. Activity that was performed.

    The Operator Account activity information can be viewed through the ACS reporting engine that shall list the total number of operator events that are logged in the ACS. The number of stored operator account events shall be limited only by the amount of disk space available in the ACS.

8. Operator Commands and Grouped Commands – The Operator Commands shall allow Operators to schedule actions to occur on a one-time or a recurring basis. The Scheduling Utility shall provide a flexible scheduling mechanism to satisfy a wide range of scheduling needs, such as “every day on the hour”, “every Monday at 8:00 am”, etc.

    The Operator Commands and Grouped Commands shall allow the Operator to configure an action to occur one time, on a given date and time. The scheduling utility shall also allow the Operator to configure an action to be performed many times over a period or indefinitely.

9. Reports - The ACS shall support a minimum of 30 standard reports. Reports shall have the ability to be exported to a PDF, Word or Spreadsheet format and/or printed to a local or networked printer. Each report shall have the ability to be customized / filtered on relevant data for that report. Standard ACS reports shall include:

    a. Event Report – The Event History Report shall present information on all access activity including grants and denials and shall include the door that was involved in the transaction, time, and cardholder involved in the transaction.

b. Cardholder Access Report - The Cardholder Access Report shall present information on all defined ACS Access Groups, including the Time Zone(s) assigned to the group and a list of the doors assigned to the group.
c. Cardholder Access Report – The Cardholder Access Report shall present information on all cardholders that are assigned to an Access Level, including the Card Number, Expiration Date.
d. Event Report - The Event Report shall present information on each ACS event/alarm generated at the field hardware level. Each event record shall include a date/time stamp, the source of the event, event name and type, and any relevant Cardholder and Card information.

10. Schedule Reports - The ACS shall support Schedule Reports. Each of the standard reports defined in the Reports section shall have the ability to have relevant data filters applied to them, prior to running, to provide a report with more specific information than the generic report.

11. Software Updates - The ACS shall support updates via downloading from the manufacturer web site, or scheduled upgrade via Cloud Hosted.

12. System Backups - The ACS shall have the ability to backup and restore the system database. Backups shall run concurrently with the rest of the system and shall not require all Operators to log out of the ACS. Backups shall include transaction data and system configuration data. The ACS shall support backups to a Windows Shared directory. Backups shall have the ability to run automatically on a predefined daily schedule.

13. System Data Logs - The ACS shall support system data logs to assist with diagnostics and troubleshooting. Standard logs shall include field hardware communication logs, system software logs, and system transaction logs. All logs shall be viewable in a plain text format.

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.