Access Controller Specification
Manufacturer - Matrix Research Limited
Product Brand - ACX

1. Integrated Access Control System Software
    a. Architecture
        i. Windows-based application which can run on WIN 10/ Windows Server 2020 or higher version.
        ii. Server Program is a service in the PC/Server, once the PC/Server is restarted, the server program will run automatically.
        iii. Software has multi-language features. English, Traditional Chinese, and Simplify Chinese are a MUST.
        iv. Users can online change the software text content.
        v. The maximum number of concurrent user logins will be under control.
        vi. Same database for storing Facial templates, Palm Vein templates, Fingerprint templates, mobile virtual cards, and physical card numbers.
        vii. Same software interface for managing Facial, Palm Vein, Virtual Card registration, fingerprint, mobile virtual card, and access control distribution.
        viii. The access control system shall be integrated with the Virtual Card Platform.
    b. Communication
        i. Server program uses a multi-threading programming technique, which direct communication to access the control panel on an Ethernet cable, real-time response.
        ii. TCP/IP communication.
    c. Data Security
        i. User-defined 128 bits master key in Server and Panel for data encryption.
        ii. A unique 192 bits random key is generated per data transmission.
        iii. In the Data encryption method, the master key encrypts the random key, random key encrypts the exchanged data during communication.
        iv. AES128 and 3DES Algorithm mixed.
    d. Database requirement
        i. MS SQL 2019 or above
    e. Application user authority
        i. Password protection
        ii. Application’s access can be filtered by View / Add / Edit / Delete
        iii. User data access can be filtered

iv. Access panel access can be filtered
v. Event status can be filtered
vi. Event acknowledge can be filtered

f. Reporting
   i. All kinds of reports can be viewed on-screen and sent to the printer
   ii. Report can export to TEXT, EXCEL & PDF files.

g. Email Service
   i. User can receive alarm records by email
   ii. User can receive their daily access record by email
   iii. Supervisor can view group users' access reports and different kinds of time attendance reports by email

h. Access control system
   i. Real-time upload parameters to panels
   ii. Client software can read controller and reader parameters instantly.
   iii. Controller and reader parameters can be defined by global or by individual
   iv. Door Group
      - Allow 10,000 door groups set up
      - Card access per door of its time zone can be classified by different door group
      - Door group can be assigned to the department
   v. Fire Alarm Group
      - Allow 255 fire alarm groups for any combination of the door lock released when the fire alarm is triggered

i. Cardholder management
   i. Provide Import and Export data tools for 3rd party data integration
   ii. Cardholder access rights can be selected by department or door group
   iii. Software can define 1,000+ suspected cardholder groups for instant enable or disable their access rights
   iv. Cardholder access rights can be defined by door group or by department

j. Staff management
   i. Provide Import and Export data tools for 3rd party data integration
   ii. Online capture of a personal photo, palm vein, fingerprint biometric templates
   iii. Print staff badge

k. Time zone control
   i. Each time zone has 4 intervals per day, Mon to Sun & Holiday
   ii. 100 Holiday dates per door access control panel
   iii. 10,000+ door access time zone in the database, 80 door time zones per door access control panel

iv. Password time zone
v. Electric Lock release time zone
vi. Twin card operation time zone
vii. Release button time zone
viii. Door opens too long time zone
ix. Alarm time zone

l. Twin card operation
   i. Twin card operation with time zone control for high-security access control application.

m. Door access activated by the specified cardholder
   i. The door is allowed for use before the specified card authorization

n. Power Monitoring
   i. A.C. power failure monitoring
   ii. Backup failure monitoring (20% of full load)

o. Transaction and Events viewer
   i. Global viewer for card access records and events
   ii. Individual / Multi viewer for card access records to the display card holder details information, e.g., Photo, etc.
   iii. Alarm viewer displays the live camera
   iv. Card access records filter by user, control panel, date and time, and access status.
   v. Different sorting order, ascending or descending, all access record, only IN or OUT or First IN last OUT record.
   vi. Event records can be filtered by the control panel, date and time, and status.
   vii. Event records can be previewed and sent the file to the printer.
   viii. Export the file to EXCEL, text, and PDF

p. Event monitoring system
   i. Each event can be defined by different icons
   ii. Software can define the device input normal status in NC or NO
   iii. Action taken can be assigned to each device input when the alarm triggered
   iv. Action items as like as Acknowledgment requested, door open by the fire alarm, enabling surveillance integration, signal integration with third-party BMS, and playing music etc.

2. PoE+ Networked Single Door Access Panel
    a) Architecture
        i. PoE+ TCP/IP-based single door panel
        ii. The overall power consumption is 30W, max. 17W power reserves for E-Lock.
        iii. Wiring method: Cat 5 cable for the panel to PoE+ switch
    b) Communication
        i. PC to Panel, TCP/IP communication
        ii. Scramble data encryption during PC/Server to panel data exchanges through the network cable
        iii. Panel to the reader, Wiegand or scramble RS485 data encryption
        iv. Active upload for swipe card records and events
    c) Data Security
        i. Apply scramble data encryption methodology during data exchange
        ii. 128 bits user master key on PC, Panel, and Reader
        iii. 192 bits random key auto-generated per communication
        iv. Master key encrypts random key, random key encrypts data exchanges between PC and Panel, Panel and Reader
        v. AES 128 & 3 DES mixed Algorithm
    d) Reader supports
        i. 1 x IN and 1 x OUT for single door panel
        ii. Supports scramble RS485 reader
        iii. Support multi-technology reader Card reader (e.g., Facial + Palm Vein + QR + Bluetooth + 13.56MHz contactless smartcard, Facial + QR + Bluetooth + 13.56MHz contactless smartcard, Palm Vein+ QR + Bluetooth + 13.56MHz contactless smartcard, Keypad + QR + Bluetooth + 13.56MHz contactless smartcard and QR + Bluetooth + 13.56MHz contactless smartcard)
    e) Card number format
        i. Default 26 / 32/ 34 / 35 / 37 / 56 / 64 and three custom formats
        ii. Each card format can have three facility code
        iii. Support four card formats at the same time
        iv. Card number length, maximum 64 bits
    f) Memory storage
        i. Memory for cardholder
            - Single-door controller
                - Allow storage of at least 40,000 sets of card numbers
        ii. Memory for transactions
            - Single door controller: allow storage of at least 42,000 nos. of transactions

iii. Events: allow storage of at least 800 nos. of events

g) Time zone control
   i. Each time zone has 4 intervals per day, Mon to Sun & Holiday
   ii. 100 Holiday dates per door access control panel
   iii. 10,000+ Door access time zone in the database, 80 time zones per door access control panel
   iv. Password time zone
   v. Electric Lock release time zone
   vi. Twin card operation time zone
   vii. Release button time zone
   viii. Door opens too long time zone
   ix. Alarm time zone
   x. LCD reader message time zone

h) Fire Alarm
   i. Panel AUX #1 for fire alarm input
   ii. 255 fire alarm groups per panel
   iii. Firm alarm signal broadcasts through the network card, no need through the PC server

i) Twin card operation
   i. Twin card operation with time zone control for high-security access control application. E.g., Car park system, treasury application.

j) Anti-pass back
   i. Single door panel (single anti-passback)

k) Device Inputs
   i. Auto detect end-of-line resistors installed or not, if yes, enable supervised monitoring
   ii. Supervised monitoring needs end-of-line resistors, 1K ohm + 1K ohm
   iii. Door release button (Normal Open)
   iv. Door Sensor (Normal close)
   v. Panel temper box sensor (Normal Close)
   vi. 2 x AUX inputs
      - Normal mode can be defined by N.O. or N.C.
      - Fire alarm signal, broadcast release E-Lock command instantly through the network cable
      - Non-fire signal depends on COM server command configuration

l) Device Outputs
   i. Access granted output for E-Lock operation. 12VDC, 10A Relay (N.O. / N.C.)

ii. Alarm output. 12VDC, 5A Reply (N.O. / N.C.)
iii. Door Ajar. 5VDC, 10mA output

m) High-Security Key Switch
   i. Tamper proof for the E-Lock override
   ii. Tamper proof for short circuit or open circuit of the exposed key switch's wires
n) Expand RS485 port
   i. 2 x RS485 port
   ii. High-level data exchange with a third-party system
o) 2 x Auxiliary input
   i. Auxiliary input # 1 – Fire alarm trigger then auto release E-Lock
   ii. Auxiliary input # 2 – Trigger alarm relay

3. Networked Door Access Panel
    a) Architecture
        i. TCP/IP-based network control panel
        ii. Built-in two LAN ports
        iii. Wiring method: Cat 5 cable for the panel to a network switch or panel-to-panel (daisy chain)
    b) Communication
        i. PC to Panel, TCP/IP communication
        ii. Scramble data encryption during PC-to-panel data exchanges through a network cable
        iii. Panel to the reader, Wiegand or scramble RS485 data encryption
        iv. Active upload for swipe card records and events
    c) Data Security
        i. Apply scramble data encryption methodology during data exchange
        ii. 128 bits user master key on PC, Panel, and Reader
        iii. 192 bits random key auto-generated per communication
        iv. Master key encrypts random key, random key encrypts data exchanges between PC and Panel, Panel and Reader
        v. AES 128 & 3 DES mixed Algorithm
    d) Reader supports
        i. 1 x IN and 1 x OUT for single door panel
        ii. 2 x IN and 2 x OUT for two-door panel
        iii. Supports scramble RS485 reader
        iv. Support multi-technology reader Card reader (e.g., Facial + Palm Vein + QR + Bluetooth + 13.56MHz contactless smartcard, Facial + QR + Bluetooth + 13.56MHz contactless smartcard, Palm Vein+ QR + Bluetooth + 13.56MHz contactless smartcard, Keypad + QR + Bluetooth + 13.56MHz contactless smartcard and QR + Bluetooth + 13.56MHz contactless smartcard)
    e) Card number format
        i. Default 26 / 32/ 34 / 35 / 37 / 56 / 64 and three custom formats
        ii. Each card format can have three facility code
        iii. Support four card formats at the same time
        iv. Card number length, maximum 64 bits
    f) Memory storage
        i. Memory for the cardholder
            - Single-door controller
                - Allow storage of at least 40,000 sets of card numbers only
            - Two-door controller
                - Allow storage of at least 20,000 sets of card numbers only
        ii. Memory for transactions

- Single door controller: allow storage of at least 42,000 nos. of transactions
- Two-door controller: allow storage of at least 21,000 nos. of transactions

iii. Events: allow storage of at least 800 nos. of events

g) Time zone control
   i. Each time zone has 4 intervals per day, Mon to Sun & Holiday
   ii. 100 Holiday dates per door access control panel
   iii. 10,000+ Door access time zone in the database, 80 time zones per door access control panel
   iv. Password time zone
   v. Electric Lock release time zone
   vi. Twin card operation time zone
   vii. Release button time zone
   viii. Door opens too long time zone
   ix. Alarm time zone
   x. LCD reader message time zone

h) Fire Alarm
   i. Panel AUX #1 for fire alarm input
   ii. 255 fire alarm groups per panel
   iii. Firm alarm signal broadcasts through the network card, no need through the PC server

i) Twin card operation
   i. Twin card operation with time zone control for high-security access control application. E.g., Car park system, treasury application.

j) Anti-pass back
   i. Single door panel (single anti-passback)
   ii. Two-door panel (single or global anti-passback)
   iii. Global anti-passback, through the server.

k) Device Inputs
   i. Auto detect end-of-line resistors were installed or not, if yes, enable supervised monitoring
   ii. Supervised monitoring needs end-of-line resistors, 1K ohm + 1K ohm
   iii. Door release button (Normal Open)
   iv. Door Sensor (Normal close)
   v. Panel temper box sensor (Normal Close)
   vi. 2 x AUX inputs
      - Normal mode can be defined by N.O. or N.C.
      - Fire alarm signal, broadcast release E-Lock command instantly through the network cable

- Non-fire signal depends on COM server command configuration

l) Device Outputs
   i. Access granted output for E-Lock operation. 12VDC, 10A Relay (N.O. / N.C.)
   ii. Alarm output. 12VDC, 5A Reply (N.O. / N.C.)
   iii. Door Ajar. 5VDC, 10mA output

m) High-Security Key Switch
   i. Tamper proof for the E-Lock override
   ii. Tamper proof for short circuit or open circuit of the exposed key switch's wires

n) Expand RS485 port
   i. 2 x RS485 port
   ii. High-level data exchange with third-party system

o) 2 x Auxiliary input
   i. Auxiliary input # 1 – Fire alarm trigger then auto release E-Lock
   ii. Auxiliary input # 2 – Trigger alarm relay

4. Networked Lift Control Master Panel
   a. A multi-purpose device that provides an interface between field-level input, output devices, and a Lift application server
   b. True IP device, support DHCP
   c. Supports 2 sets of ACX readers.
   d. 2 x LAN Port, allow daisy chain connection.
   e. Dry contact supervised monitoring
   f. User-defined NC / NO at normal mode
   g. 2 x INPUTs for Manual key overwrite and Fire Alarm input
   h. 28 x RELAY outputs for 28 Floors access, RELAY in 3A DC output
   i. Panel installation depends on the IP address available
   j. RS485 port for 8907 Lift control expansion panel
   k. 12VDC input, 1A

5. Networked Lift Control Expansion Panel
   a. Works with Networked Lift Control Master Panel
   b. RS485 connection
   c. User-defined NC / NO at normal mode
   d. 38 x RELAY outputs for extra 38 Floors access, RELAY in 3A DC output
   e. 12VDC input, 1A

6. Network Alarm Input Panel
   a. 2 x LAN Port, allow daisy chain connection
   b. Suitable for huge sensors monitoring
   c. Dry contact supervised monitoring
   d. User-defined NC / NO at normal mode
   e. 28 Input Points, 2 RELAY 10A output per panel
   f. Panel installation depends on the IP address available
   g. Relay status triggered by 28 Inputs AND / OR program logic
   h. RS485 port for proprietary device communication
   i. 12VDC, 500mA

7. Controller Power Supply
   a. The power supply box shall have a metal casing.
   b. The power supply box shall have earth wiring.
   c. The size of the power supply box shall be not more than 340mm(H) x 290mm(W) x 80mm(D).
   d. The power supply box shall have 12VDC, 3A power supply output for ONE set of electric lock installed; and 5A power supply output for TWO sets of electric locks installed.
   e. The power supply shall have a battery charging function, and the battery charging voltage is 13.8VDC
   f. The power supply can output 0VDC or 5VDC voltage level to the controller to indicate the occurrence of the following events: -
      i. AC. power failure
      ii. DC battery installed
      iii. backup battery power was lowered by 20%
   g. A 7AH DC battery shall be included for a single E-Lock installed. In case of the AC power supply failure, assume the E-Lock power consumption is 12V 0.5ADC, the door access system can be operated for 4 hours.
   h. A 9AH DC battery shall be included for a double E-Lock installed. In case of the AC power supply failure, assume the E-Lock power consumption is 12V 0.5ADC, the door access system can be operated for 3 hours.

8. Door emergency exit device (Resettable Call Point)
   a. The resettable call point comes with a hinged front cover to prevent the unit from activating randomly.
   b. Once the “PRESS HERE” button was pressed, the fail-safe type E-Lock power is cut off, and the door is released.
   c. The call point can be reset by inserting a plastic key horizontally into the front panel of the resettable call point.
   d. The call point unit shall have an LED light to identify the operation mode. RED, GREEN, BLUE, and mixed colors shall be assigned for normal mode and emergency exit mode.
   e. The LED light of the call point is provided by the E-Lock power input, if the LED light is ON, the E-Lock power supply is normal and vice versa.
   f. For emergency exit mode, the call point shall have a beep sound notification.
   g. The LED and buzzer settings shall be operated by a DIP switch.
   h. The call point shall have two set dry contact switches, one set for E-Lock power, and another set for signal output. The current rate of the switch is 5ADC under a 12VDC power supply.
   i. The resettable call point shall have a voltage regulator to support E-Lock power in AC/DC, 12V/24V.

9. High-Security Override key switch and key switch controller
   a. The High-security override key switch works with a key controller, no matter if the key switch has been tampered, the electric lock keeps the original lock status
   b. One LED indicator on the key switch front plate: LED indicator in RED in normal operation, after key override, the LED indicator changes to GREEN. Once the key switch has been tampered with, the LED indicator goes off.
   c. If the key switch has been tampered with, no matter short-circuits or cuts the wires between the key switch and key switch controller, the electric lock status remains unchanged.
   d. Reset the button in the key switch controller which to activate the key switch function
   e. The key cylinder shall have a master operation key that can open all high-security override key switches, the master key built in a small movable pellet that cannot be physically duplicated excludes the original cylinder supplier.
   f. Minimum 3 sets of master keys shall be provided to the end customer.
   g. The Key cylinder is by ABLOY PROTEC2, 1.7 billion key combinations