**Access Controller Specification**

**Manufacturer - Matrix Research Limited**

**Product Brand - ACX**

1. Integrated Access Control System Software
2. Architecture
3. Windows-based application which can run on WIN 10/ Windows Server 2020 or higher version.
4. Server Program is a service in the PC/Server, once the PC/Server is restarted, the server program will run automatically.
5. Software has multi-language features.
6. User can online change the software text content.
7. The maximum number of concurrent user logins will be under control.
8. Same database for storing Facial template, Palm Vein template, Fingerprint template, and card number.
9. Same software interface for managing Facial, Palm Vein, Virtual Card registration, fingerprint, mobile virtual card, and access control distribution.
10. Communication
11. Server program uses multi-threading programming technique, which direct communication to access the control panel on Ethernet cable, real-time response.
12. TCP/IP communication.
13. Data Security
14. User-defined 128 bits master key in Server and Panel for data encryption.
15. A unique 192 bits random key is generated per data transmission.
16. Data encryption method, master key encrypts random key, random key encrypts the exchanged data during communication.
17. AES128 and 3DES Algorithm mixed.
18. Database requirement
19. MS SQL 2019 or above
20. Application user authority
21. Password protection
22. Application’s access can be filtered by View / Add / Edit / Delete
23. User data access can be filtered
24. Access panel access can be filtered
25. Event status can be filtered
26. Event acknowledge can be filtered
27. Reporting
28. All kinds of reports can be viewed on-screen and sent to printer
29. Report can export to TEXT, EXCEL & PDF files.
30. Email Service
31. User can receive alarm records by email
32. User can receive their daily access record by email
33. Supervisor can view group users’ access reports and different kinds of time attendance reports by email
34. Access control system
35. Real-time upload parameters to panels
36. Client software can read controller and reader parameters instantly.
37. Controller and reader parameters can be defined by global or by individual
38. 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
39. Fire Alarm Group
	* + Allow 255 fire alarm groups for any combination of the door lock released when fire alarm is triggered
40. Cardholder management
41. Provide Import and Export data tool for 3rd party data integration
42. Cardholder access rights can be selected by department or door group
43. Software can define 1,000+ suspected cardholder groups for instant enable or disable their access rights
44. Cardholder access rights can be defined by door group or by department
45. Staff management
46. Provide Import and Export data tool for 3rd party data integration
47. Online capture of a personal photo, palm vein, fingerprint biometric templates
48. Print staff badge
49. Time zone control
50. Each time zone has 4 intervals per day, Mon to Sun & Holiday
51. 100 Holiday dates per door access control panel
52. 10,000+ door access time zone in the database, 80 door time zones per door access control panel
53. Password time zone
54. Electric Lock release time zone
55. Twin card operation time zone
56. Release button time zone
57. Door opens too long time zone
58. Alarm time zone
59. Twin card operation
60. Twin card operation with time zone control for high-security access control application.
61. Door access activated by the specified card holder
62. The door is allowed for use before the specified card authorization
63. Power Monitoring
64. A.C. power failure monitoring
65. Backup failure monitoring (20% of full load)
66. Transaction and Events viewer
67. Global viewer for card access records and events
68. Individual / Multi viewer for card access records to display card holder details information, e.g., Photo etc.
69. Alarm viewer displays the live camera
70. Card access records filter by user, control panel, date and time, and access status.
71. Different sorting order, ascending or descending, all access record, only IN or OUT or First IN last OUT record.
72. Event records can be filtered by the control panel, date and time, and status.
73. Event records can be previewed and sent the file to the printer.
74. Export the file to EXCEL, text, and PDF
75. Event monitoring system
76. Each event can be defined by different icons
77. Software can define the device input normal status in NC or NO
78. Action taken can be assigned to each device input when the alarm triggered
79. Action items as like as Acknowledgment requested, door open by the fire alarm, enable surveillance integration, signal integration with third-party BMS, and play music etc.
80. PoE+ Networked Single Door Access Panel
81. Architecture
82. PoE+ TCP/IP based single door panel
83. The overall power consumption is 30W, max. 17W power reserves for E-Lock.
84. Wiring method: Cat 5 cable for the panel to PoE+ switch
85. Communication
86. PC to Panel, TCP/IP communication
87. Scramble data encryption during PC/Server to panel data exchanges through the network cable
88. Panel to the reader, Wiegand or scramble RS485 data encryption
89. Active upload for swipe card records and events
90. Data Security
91. Apply scramble data encryption methodology during data exchange
92. 128 bits’ user master key on PC, Panel, and Reader
93. 192 bits’ random key auto-generated per communication
94. Master key encrypts random key, random key encrypts data exchanges between PC and Panel, Panel and Reader
95. AES 128 & 3 DES mixed Algorithm
96. Reader supports
97. 1 x IN and 1 x OUT for single door panel
98. Supports scramble RS485 reader
99. Support multi-technology reader Card reader (e.g., 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)
100. Card number format
101. Default 26 / 32/ 34 / 35 / 37 / 56 / 64 and three custom formats
102. Each card format can have three facility code
103. Support four card formats at the same time
104. Card number length, maximum 64 bits
105. Memory storage
106. Memory for card holder
	* + Single door controller
			- Allow storage of at least 40,000 sets of card numbers
107. Memory for transactions
	* + Single door controller: allow storage of at least 42,000 nos. of transactions
108. Events: allow storage of at least 800 nos. of events
109. Time zone control
110. Each time zone has 4 intervals per day, Mon to Sun & Holiday
111. 100 Holiday dates per door access control panel
112. 10,000+ Door access time zone in the database, 80 time zones per door access control panel
113. Password time zone
114. Electric Lock release time zone
115. Twin card operation time zone
116. Release button time zone
117. Door opens too long time zone
118. Alarm time zone
119. LCD reader message time zone
120. Fire Alarm
121. Panel AUX #1 for fire alarm input
122. 255 fire alarm groups per panel
123. Firm alarm signal broadcasts through the network card, no need through the PC server
124. Twin card operation
125. Twin card operation with time zone control for high-security access control application. E.g., Car park system, treasury application.
126. Anti-pass back
127. Single door panel (single anti-passback)
128. Device Inputs
129. Auto detect end-of-line resistors were installed or not, if yes, enable supervised monitoring
130. Supervised monitoring needs end-of-line resistors, 1K ohm + 1K ohm
131. Door release button (Normal Open)
132. Door Sensor (Normal close)
133. Panel temper box sensor (Normal Close)
134. 2 x AUX inputs
	* + Normal mode can be defined by N.O. or N.C.
		+ Fire alarm signal, broadcast release E-Lock command instantly though network cable
		+ Non-fire signal depends on COM server command configuration
135. Device Outputs
136. Access granted output for E-Lock operation. 12VDC, 10A Relay (N.O. / N.C.)
137. Alarm output. 12VDC, 5A Reply (N.O. / N.C.)
138. Door Ajar. 5VDC, 10mA output
139. High-Security Key Switch
140. Tamper proof for the E-Lock override
141. Tamper proof for short circuit or open circuit of the exposed key switch’s wires
142. Expand RS485 port
143. 2 x RS485 port
144. High-level data exchange with a third-party system
145. 2 x Auxiliary input
146. Auxiliary input # 1 – Fire alarm trigger then auto release E-Lock
147. Auxiliary input # 2 – Trigger alarm relay
148. Networked Door Access Panel
	* 1. Architecture
149. TCP/IP-based network control panel
150. Built-in two LAN ports
151. Wiring method: Cat 5 cable for the panel to network switch or panel to panel (daisy chain)
152. Communication
153. PC to Panel, TCP/IP communication
154. Scramble data encryption during PC to panel data exchanges through a network cable
155. Panel to the reader, Wiegand or scramble RS485 data encryption
156. Active upload for swipe card records and events
157. Data Security
158. Apply scramble data encryption methodology during data exchange
159. 128 bits’ user master key on PC, Panel, and Reader
160. 192 bits’ random key auto-generated per communication
161. Master key encrypts random key, random key encrypts data exchanges between PC and Panel, Panel and Reader
162. AES 128 & 3 DES mixed Algorithm
163. Reader supports
164. 1 x IN and 1 x OUT for single door panel
165. 2 x IN and 2 x OUT for two-door panel
166. Supports scramble RS485 reader
167. Support multi-technology reader Card reader (e.g., 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)
168. Card number format
169. Default 26 / 32/ 34 / 35 / 37 / 56 / 64 and three custom formats
170. Each card format can have three facility code
171. Support four card formats at the same time
172. Card number length, maximum 64 bits
173. Memory storage
174. Memory for the card holder
	* + Single door controller
			- Allow storage of at least 40,000 sets of card numbers only
		+ Two-dooror controller
			- Allow storage of at least 20,000 sets of card numbers only
175. Memory for transactions
	* + Single door controller: allow storage of at least 42,000 nos. of transactions
		+ Two-dooror controller: allow storage of at least 21,000 nos. of transactions
176. Events: allow storage of at least 800 nos. of events
177. Time zone control
178. Each time zone has 4 intervals per day, Mon to Sun & Holiday
179. 100 Holiday dates per door access control panel
180. 10,000+ Door access time zone in the database, 80 time zones per door access control panel
181. Password time zone
182. Electric Lock release time zone
183. Twin card operation time zone
184. Release button time zone
185. Door opens too long time zone
186. Alarm time zone
187. LCD reader message time zone
188. Fire Alarm
189. Panel AUX #1 for fire alarm input
190. 255 fire alarm groups per panel
191. Firm alarm signal broadcasts through the network card, no need through the PC server
192. Twin card operation
193. Twin card operation with time zone control for high-security access control application. E.g., Car park system, treasury application.
194. Anti-pass back
195. Single door panel (single anti-passback)
196. Two-door panel (single or global anti-passback)
197. Global anti-passback, through the server.
198. Device Inputs
199. Auto detect end-of-line resistors were installed or not, if yes, enable supervised monitoring
200. Supervised monitoring needs end-of-line resistors, 1K ohm + 1K ohm
201. Door release button (Normal Open)
202. Door Sensor (Normal close)
203. Panel temper box sensor (Normal Close)
204. 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 network cable
		+ Non-fire signal depends on COM server command configuration
205. Device Outputs
206. Access granted output for E-Lock operation. 12VDC, 10A Relay (N.O. / N.C.)
207. Alarm output. 12VDC, 5A Reply (N.O. / N.C.)
208. Door Ajar. 5VDC, 10mA output
209. High-Security Key Switch
210. Tamper proof for the E-Lock override
211. Tamper proof for short circuit or open circuit of the exposed key switch’s wires
212. Expand RS485 port
213. 2 x RS485 port
214. High-level data exchange with third-party system
215. 2 x Auxiliary input
216. Auxiliary input # 1 – Fire alarm trigger then auto release E-Lock
217. Auxiliary input # 2 – Trigger alarm relay

1. Networked Lift Control Master Panel
2. A multi-purpose device that provides an interface between field-level input, output devices, and a Lift application server
3. True IP device, support DHCP
4. 2 x LAN Port, allow daisy chain connection
5. Dry contact supervised monitoring
6. User-defined NC / NO at normal mode
7. 2 x INPUTs for Manual key overwrite and Fire Alarm input
8. 28 x RELAY outputs for 28 Floors access, RELAY in 3A DC output
9. Panel installation depends on the IP address available
10. RS485 port for 8907 Lift control expand panel
11. 12VDC input, 1A
12. Networked Lift Control Expansion Panel
13. Works with Networked Lift Control Master Panel
14. RS485 connection
15. User-defined NC / NO at normal mode
16. 38 x RELAY outputs for extra 38 Floors access, RELAY in 3A DC output
17. 12VDC input, 1A
18. Network Alarm Panel
19. 2 x LAN Port, allow daisy chain connection
20. Suitable for huge sensors monitoring
21. Dry contact supervised monitoring
22. User-defined NC / NO at normal mode
23. 28 Input Points, 2 RELAY 10A output per panel
24. Panel installation depends on the IP address available
25. Relay status triggered by 28 Inputs AND / OR program logic
26. RS485 port for proprietary device communication
27. 12VDC, 500mA
28. Door emergency exit device (Resettable Call Point)
29. The resettable call point comes with a hinged front cover to prevent the unit from activating randomly.
30. Once the “PRESS HERE” button was pressed, the E-Lock power is cut, and the door is released.
31. The call point can be reset by inserting a plastic key horizontally into the front panel of the resettable call point.
32. 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.
33. 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.
34. For emergency exit mode, the call point shall have a beep sound notification.
35. The LED and buzzer setting shall be operated by a DIP switch.
36. 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.
37. The resettable call point shall have a voltage regulator to support E-Lock power in AC/DC, 12V/24V.
38. Power Supply Box
39. The power supply box shall have a metal casing.
40. The power supply box shall have earth wiring.
41. The size of the power supply box shall be not more than 340mm(H) x 290mm(W) x 80mm(D).
42. The power supply box shall have 12VDC, 3A power supply output for ONE set electric lock installed; and 5A power supply output for TWO sets of electric lock installed.
43. The power supply shall have a battery charging function, the battery charging voltage is 13.8VDC
44. The power supply can output 0VDC or 5VDC voltage level to the controller to indicate the occurrence of the following events: -
45. AC. power failure
46. DC battery installed
47. backup battery power was lowered by 20%
48. A 7AH DC battery shall be included. In case of the AC power supply failure, the door access system can be operated for 4 hours.

1. High-Security Override key switch and key switch controller
2. 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
3. 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.
4. 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.
5. Reset the button in the key switch controller which to activate the key switch function
6. 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.
7. Minimum 3 sets of master keys shall be provided to the end customer.
8. The Key cylinder is by ABLOY PROTEC2, 1.7 billion key combinations