Access Control
CONTENTS

1 PURPOSE AND SCOPE ........................................................................................................... 6

2 INTRODUCTION .................................................................................................................. 6

3 SYSTEM CAPACITY OVERVIEW .......................................................................................... 7
   3.1 SYSTEM-WIDE SYSTEM LIMITATIONS .................................................................... 7
   3.2 COMMUNICATIONS ................................................................................................. 7
   3.3 SYSTEM INPUTS ...................................................................................................... 7
   3.4 SYSTEM OUTPUTS ................................................................................................... 7
   3.5 SYSTEM ADMINISTRATION AND CONNECTIONS TO MAIN SYSTEM SERVER ...... 7

4 SYSTEM HARDWARE ............................................................................................................. 8
   4.1 SYSTEM ARCHITECTURE AND BASIC OPERATIONAL OVERVIEW ............... 8
   4.2 IP CONNECTED CONTROLLERS .......................................................................... 9
   4.3 FIELD NETWORK .................................................................................................. 9
   4.4 INTELLIGENT DOOR CONTROLLERS ............................................................... 9
   4.5 INPUT/OUTPUT CONTROLLERS ........................................................................ 12
   4.6 CONTROLLER SOFTWARE .................................................................................. 12
   4.7 ENCLOSURES AND POWER SUPPLIES ......................................................... 13
   4.8 READERS AND KEYPADS ............................................................................... 13
   4.9 CE COMPLIANCE ............................................................................................... 13

5 SYSTEM SOFTWARE - OVERVIEW ..................................................................................... 14
   5.1 GENERAL SYSTEM OPERATION ......................................................................... 14
   5.2 USER/SYSTEM OPERATOR ACCESS .................................................................. 15

6 SYSTEM SOFTWARE - HARDWARE CONFIGURATION ...................................................... 16
   6.1 GENERAL ............................................................................................................. 16
   6.2 PANEL/CONTROLLER CONFIGURATION ....................................................... 16
   6.3 FIELD NETWORK/PORT CONFIGURATION .................................................... 17
   6.4 DOOR CONFIGURATION .................................................................................... 17
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5</td>
<td>Reader Configuration</td>
<td>18</td>
</tr>
<tr>
<td>6.6</td>
<td>Input Configuration</td>
<td>18</td>
</tr>
<tr>
<td>6.7</td>
<td>Output Configuration</td>
<td>19</td>
</tr>
<tr>
<td>6.8</td>
<td>Lift/Elevator Control</td>
<td>19</td>
</tr>
<tr>
<td>7</td>
<td>System Software - Access Control Elements</td>
<td>19</td>
</tr>
<tr>
<td>7.1</td>
<td>Time Schedules and Patterns</td>
<td>19</td>
</tr>
<tr>
<td>7.2</td>
<td>System Modes</td>
<td>20</td>
</tr>
<tr>
<td>7.3</td>
<td>Card/Token Types</td>
<td>21</td>
</tr>
<tr>
<td>7.4</td>
<td>Card/Token Pools</td>
<td>21</td>
</tr>
<tr>
<td>7.5</td>
<td>Cards/Tokens</td>
<td>21</td>
</tr>
<tr>
<td>7.6</td>
<td>Id Card/Token Printing</td>
<td>22</td>
</tr>
<tr>
<td>7.7</td>
<td>Card/Token Penalty Points</td>
<td>22</td>
</tr>
<tr>
<td>7.8</td>
<td>Unused Card/Token</td>
<td>23</td>
</tr>
<tr>
<td>7.9</td>
<td>Duress Pin</td>
<td>23</td>
</tr>
<tr>
<td>7.10</td>
<td>Area Control</td>
<td>24</td>
</tr>
<tr>
<td>8</td>
<td>System Software - Personnel/Cardholders</td>
<td>25</td>
</tr>
<tr>
<td>8.1</td>
<td>Personnel/Cardholders</td>
<td>25</td>
</tr>
<tr>
<td>8.2</td>
<td>Personnel Card/Token Management</td>
<td>26</td>
</tr>
<tr>
<td>8.3</td>
<td>Personnel Photo/Image Management</td>
<td>26</td>
</tr>
<tr>
<td>8.4</td>
<td>Personnel Access Management</td>
<td>27</td>
</tr>
<tr>
<td>9</td>
<td>System Software - Visitor Management</td>
<td>27</td>
</tr>
<tr>
<td>9.1</td>
<td>General</td>
<td>27</td>
</tr>
<tr>
<td>9.2</td>
<td>Visitor Arrival</td>
<td>28</td>
</tr>
<tr>
<td>9.3</td>
<td>Visitor Departure</td>
<td>28</td>
</tr>
<tr>
<td>9.4</td>
<td>Visitor Monitoring</td>
<td>28</td>
</tr>
<tr>
<td>10</td>
<td>System Software - Control Centre</td>
<td>29</td>
</tr>
<tr>
<td>10.1</td>
<td>General</td>
<td>29</td>
</tr>
<tr>
<td>10.2</td>
<td>Incident/Alert Reporting</td>
<td>30</td>
</tr>
<tr>
<td>10.3</td>
<td>Device Management</td>
<td>30</td>
</tr>
<tr>
<td>10.4</td>
<td>Area Management</td>
<td>31</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td>10.5</td>
<td>WATCH LIST</td>
<td>31</td>
</tr>
<tr>
<td>10.6</td>
<td>VISUAL REPRESENTATION</td>
<td>32</td>
</tr>
<tr>
<td>10.7</td>
<td>PHOTOGRAPHIC IDENTIFICATION</td>
<td>32</td>
</tr>
<tr>
<td>11</td>
<td>SYSTEM SOFTWARE - EVENT CONFIGURATION</td>
<td>33</td>
</tr>
<tr>
<td>11.1</td>
<td>EVENT NOTIFICATION</td>
<td>33</td>
</tr>
<tr>
<td>11.2</td>
<td>TRIGGERING COMMANDS</td>
<td>33</td>
</tr>
<tr>
<td>12</td>
<td>SYSTEM SOFTWARE - SYSTEM REPORTS</td>
<td>33</td>
</tr>
<tr>
<td>12.1</td>
<td>GENERAL SYSTEM REPORTS</td>
<td>33</td>
</tr>
<tr>
<td>12.2</td>
<td>TRANSACTIONAL HISTORY REPORTS</td>
<td>34</td>
</tr>
<tr>
<td>12.3</td>
<td>PERSONNEL AND ACCESS</td>
<td>34</td>
</tr>
<tr>
<td>12.4</td>
<td>AREA MONITORING</td>
<td>34</td>
</tr>
<tr>
<td>12.5</td>
<td>SYSTEM AUDIT</td>
<td>35</td>
</tr>
<tr>
<td>12.6</td>
<td>VISITORS</td>
<td>35</td>
</tr>
<tr>
<td>12.7</td>
<td>SYSTEM SETTINGS</td>
<td>35</td>
</tr>
<tr>
<td>12.8</td>
<td>DEVICES</td>
<td>35</td>
</tr>
<tr>
<td>13</td>
<td>MANAGEMENT/SYSADMIN OPTIONS</td>
<td>35</td>
</tr>
<tr>
<td>13.1</td>
<td>USER MANAGEMENT</td>
<td>35</td>
</tr>
<tr>
<td>13.2</td>
<td>ADDITIONAL DATA FIELDS</td>
<td>36</td>
</tr>
<tr>
<td>13.3</td>
<td>RUNNING AND SCHEDULING BACKUPS</td>
<td>36</td>
</tr>
<tr>
<td>13.4</td>
<td>DIAGNOSTICS</td>
<td>36</td>
</tr>
<tr>
<td>14</td>
<td>TENANCY</td>
<td>36</td>
</tr>
<tr>
<td>14.1</td>
<td>GENERAL</td>
<td>36</td>
</tr>
<tr>
<td>14.2</td>
<td>LANDLORD ACCESS</td>
<td>36</td>
</tr>
<tr>
<td>14.3</td>
<td>TENANT ACCESS</td>
<td>37</td>
</tr>
<tr>
<td>15</td>
<td>INTEGRATION OPTIONS</td>
<td>37</td>
</tr>
<tr>
<td>15.1</td>
<td>EVENT BASED INCLUDING CCTV</td>
<td>37</td>
</tr>
<tr>
<td>15.2</td>
<td>ELEVATORS</td>
<td>37</td>
</tr>
<tr>
<td>15.3</td>
<td>FIRE PANEL</td>
<td>38</td>
</tr>
<tr>
<td>15.4</td>
<td>ALARM PANEL</td>
<td>38</td>
</tr>
<tr>
<td>15.5</td>
<td>DATABASE IMPORT</td>
<td>38</td>
</tr>
</tbody>
</table>
15.6 WIRELESS LOCKS .................................................................................. 38

16 WARRANTIES, MAINTENANCE AND SERVICE ............................................. 39
   16.1 WARRANTY ......................................................................................... 39
   16.2 MAINTENANCE AND SERVICE ............................................................ 39
   16.3 QUALITY ASSURANCE ....................................................................... 39
1 PURPOSE AND SCOPE

a) This specification is a description of the integrated access control system (ACS) and its minimum required capability. Equipment specified herein includes the ACS computer and software organisation, the ACS features and functions, and the ACS intelligent controllers and their capability.

b) It is recognised that not all of this specification will be deliverable from a basic core system and that some additional system modules may be required. Optional modules required in order to comply with this specification shall be readily available from the manufacturer's standard catalogue of products and options.

c) Equipment required for this project shall be quantified using the Tender Drawings and the Tender Bill of Quantities. It is a requirement that as the system expands throughout its lifetime that any or all of this specification shall easily be implemented without needing to change or re-install the field equipment, the field wiring, the system database, or the software application.

2 INTRODUCTION

a) The system shall include all hardware and software, including intelligent controller units, ID cards, tokens and readers, power supplies, conduits, raceways, enclosures, mounting hardware and all other equipment as indicated on the tender drawings and specified herein.

b) The ACS shall be feature-rich and scalable for small, medium and large enterprise installations and shall be specifically designed to be easy to administer by operators with limited experience of such a system.

c) It is a requirement for future scalability and system resilience, that the ACS shall consist of a webserver, a database and system service components that can be configured across multiple physical servers in a distributed computing solution. An ACS that cannot operate or grow into a distributed computing solution will not be accepted.

d) The ACS user interface shall be 100% browser compliant. ACS application software that needs to be installed on a local or 'client' PC will not be accepted.

e) The ACS whilst being highly secure shall be open architecture and utilise a MS SQL database. Only industry standard tools and practices shall be required to create customised management reports.

f) The ACS shall support a network of Intelligent Controllers which shall be responsible for managing the real-time status of fixed control points such as electrically operated doors and initiating system-wide logical actions across alarm input groups and relay output groups.

g) The Intelligent Controllers shall employ micro-controller units and memory and shall be responsible for authorising card and token presentations at readers and for storing relevant system information at the intelligent node. IP and RS485 controller nodes shall be available to suit local communication requirements and
with the exception of IP line headers where RS485 Field Networks are proposed, no other field processor or interfacing hardware shall be required to control and manage the system portals.

3 SYSTEM CAPACITY OVERVIEW

3.1 SYSTEM-WIDE SYSTEM LIMITATIONS

- Sites – No practical system limit
- Door/Reader capacity – No practical system limit
- Card/Token Holders – No practical system limit
- Access Groups – No practical system limit
- Weekly Time Zones – No practical system limit
- System Modes – No practical system limit
- User Definable data fields for Personnel records – No practical system limit
- User Definable data fields for System User records – No practical system limit
- Area Management/Anti-Passback – No practical system limit
- System Actions – No practical system limit

3.2 COMMUNICATIONS

- Concurrent Communication Engines – No practical system limit
- TCP/IP direct to Controllers for IP connected Controllers – No practical system limit
- 2-wire RS485 Field Network Controllers – No practical system limit

3.3 SYSTEM INPUTS

- No practical system limit

3.4 SYSTEM OUTPUTS

- No practical system limit

3.5 SYSTEM ADMINISTRATION AND CONNECTIONS TO MAIN SYSTEM SERVER

- No practical system limit
4 SYSTEM HARDWARE

4.1 SYSTEM ARCHITECTURE AND BASIC OPERATIONAL OVERVIEW

a) The system shall use intelligent distributed processing controller architecture with access decisions being made locally at each controller without reference to any other processor

b) The ACS main server shall connect to IP controllers and Field Networks with RS485 controllers

c) A Field Network shall support 32 Intelligent Controller nodes

d) There shall be no limit to the number of Intelligent Controllers per system

e) An Intelligent Controller node shall consist of an Intelligent Door Controller (IDC) or an Input/Output Controller (IOC)

f) Controllers shall be installed into purpose made steel enclosures and shall be powered by local mains power or POE. Every power supply, including POE shall include battery back-up and battery charging circuits

g) The ACS main server shall download controller-specific data to each Intelligent Controller node. This data shall be stored at the controller and shall be pertinent information relating to the controller’s functionality. Should communication with the ACS main server be lost, the controller shall continue to operate without degradation of security whilst transaction data including event activity and its date and time stamp shall be stored at the controller. Upon restoration of communications transaction data shall be automatically uploaded to the ACS main server for future historical reporting

h) Under normal system operation, Intelligent Controllers shall send details of events and transactions to the ACS main server to ensure that:
   - The latest data is always available in the central logs
   - Global functions such as area control and system-wide actions are maintained

i) If communications are lost to an Intelligent Controller the controller shall enter into fall-back mode. In fall-back mode an IDC shall:
   - Carry on normal access control operations using its on-board database
   - Store up to 4,000 alarms, events and transactions
   - When the event buffer is full, the oldest, non-important events shall be over-written first
   - Automatically send stored data to the ACS main server upon return of communications
4.2 IP CONNECTED CONTROLLERS

a) An IP Controller shall be able to connect directly to the ACS main server via an IP network

b) IP Controllers shall support 10/100 Mbps full duplex communications

c) IP Controllers shall support DHCP

d) It shall be possible to support multiple IP ACS systems on the same corporate network with absolute system security between the individual systems. This shall be done without having to change or modify the client’s IT settings or infrastructure

e) A software application shall be provided to allow each IP device to be easily configured on the network

f) Once the communications security features have been invoked on the IP device, it shall not be possible to modify or reconfigure the device unless carried out at the ACS main server

4.3 FIELD NETWORK

a) The system shall support multiple RS485 2-wire Field Networks

b) Each Field Network shall support a minimum of 32 nodes which may consist of any combination of Intelligent Door Controllers and Input/Output Controllers

c) Field Networks shall connect to the ACS main server via an IP Field Network Line Header. USB or RS232 direct-connect line headers will not be accepted

d) Field Networks shall be capable of extending to a minimum of 1,200m without boosters or repeaters. It shall be possible to include additional Intelligent Controller nodes without affecting the operation or set-up of any existing node

e) Field Networks of greater distance than 1,200m shall be supported with suitable line drivers

f) It shall be possible to connect at least three Field Network Line Headers to the same Field Network in order to provide superior communications resilience. In the event of a network communications failure the system shall be capable of automatically re-routing communications accordingly

4.4 INTELLIGENT DOOR CONTROLLERS

a) Intelligent Door Controllers (IDCs) shall connect to the system via an IP connection directly at the controller (IP Controllers), or a 2-wire RS485 Field Network (RS485 Controllers)

b) Field Network controllers shall support 2-wire RS485 communications and connect to the ACS via an IP line header. USB or RS232 direct-connect line headers will not be accepted
c) To aid installation, servicing and maintenance, every IDC shall include plugdisconnect for all wiring at the controller.

d) An IDC shall have its own on-board database and carry out system transactions such as card/token authorisations without reference to any other controller or processor. The standard memory allocation at each controller shall allow the on-board database to store up to 31 x Weekly Time Zones, 8 x System Modes, 65,000 card/token holders with their system-generated PINs and card/token status. In addition, there shall be sufficient memory to maintain a local log of up to 4,000 historical events and transactions if the IDC goes off line from the ACS main server.

e) In the event that the historical memory buffer becomes full at an IDC whilst off line, the oldest, non-important events shall be over-written first, thus retaining alarms and high-priority events. These events shall be synchronised with the main historical database once communications are restored.

f) The ACS shall include a system-wide option where user-defined PINs can be defined rather than using the default system-generated PINs. When this option is selected, the IDC card/token holder capacity shall be reduced from 65,000 to 55,000. All other parameters shall remain the same.

g) Whether on line or off line an IDC shall provide a door open command within 0.25 seconds of a valid access card being recognised by the reader.

h) An IDC shall support a minimum of:
   - 2 x door lock output relays suitable for switching 30V at 3A each.
   - 4 x dedicated outputs (two per door) to control reader LEDs for user information.
   - 2 x dedicated outputs to drive optional sounders for providing local alarm signals or user information.
   - 2 x dedicated inputs (N/O) for request to exit (REX) buttons.
   - 2 x dedicated supervised inputs (N/C) for door position monitoring.
   - 1 x dedicated tamper monitoring for the IDC enclosure.
   - 1 x supervised input that is not required for the normal door function but is available for general alarm monitoring such as:
     - Fire and emergency monitoring.
     - Intruder detection monitoring.
     - Plant alarm and status monitoring.
     - Monitoring of emergency door.
     - System logic input.

i) IDC supervised inputs shall be tamper monitored for open and short circuit conditions.
j) An IDC shall support a minimum of two card readers and two PIN units which may be used in a two door configuration with reader IN and egress button OUT, or a one door configuration with reader IN and reader OUT. In addition, associated monitoring, local sounders, information LEDs and lock outputs for the two complete door-sets shall also be supported. The following door configurations shall be available as a minimum:

- Keypad only
- Reader only
- Reader and keypad
- Keypad for ingress and egress
- Reader for ingress and egress
- Reader and keypad for ingress and egress
- Reader and keypad for ingress and reader only for egress
- Reader and keypad for ingress and keypad only for egress

k) Each IDC shall be capable of supporting two different reader technologies at the same time, whether the combination is on one door or two

l) Each IDC shall be capable of supporting a minimum of thirty-one different weekly time patterns

m) In the event of a power failure an IDC shall monitor the voltage at its supporting battery. In the event of the battery capacity dropping below 80% of its normal value the IDC shall remove power from the locks to prevent spurious locking/unlocking and eventual lock damage occurring

n) Each IDC shall incorporate a ‘graceful shut-down’ attribute. In the event of both power and communications failure, and eventual depletion of the battery back-up, IDCs shall retain their last known complete configuration for up to 100 hours. When power is restored the IDC shall continue to operate without having to communicate or reload data from the ACS server

o) Diagnostic LEDs shall be included on each IDC. An IP IDC shall include indicators for:

- LED indicators for Readers
- Relays
- Online – Connected to host
- CTS – Ethernet not ready
- RTS – Handshake
- RUN – CPU activity
- Eng1 and Eng2 – Engineering diagnostics
A RS485 IDC shall include indicators for:

- LED indicators for Readers
- Relays
- Communicating with host
- RUN – CPU Activity
- Eng1 and Eng2 diagnostics

4.5 INPUT/OUTPUT CONTROLLERS

a) Input/Output Controllers (IOCs) shall connect to the system via an IP connection directly at the controller (IP Controllers), or a 2-wire RS485 Field Network (RS485 Controllers)

b) Field Network controllers shall support 2-wire RS485 communications and connect to the ACS via an IP line header. USB or RS232 direct-connect line headers will not be accepted

c) To aid installation, servicing and maintenance, each IOC shall support plug-disconnect for all wiring at the controller

d) Two versions of IOCs shall be supported.
   - One shall support a minimum of 8 x supervised alarm inputs and 4 x change-over relay outputs
   - One shall support a minimum of 8 x supervised alarm inputs and 16 x change-over relay outputs

e) An additional tamper input shall be available to monitor the panel enclosure.

f) The IOC shall maintain a local log of up to 4,000 historical events and transactions if off line from the ACS main server. In the event that the memory buffer becomes full whilst off line, the oldest, non-important events shall be over-written first, thus retaining alarms and high-priority events. These events shall be synchronised with the main historical database once communications are restored

4.6 CONTROLLER SOFTWARE

a) IDC and IOC controller software shall be held in flash memory. Future software upgrades shall be downloaded from the ACS main server without the need to change the controller EPROM or other physical IC. At all times during a new download the controller shall continue to operate on the existing configuration and the changeover shall only occur once the whole of the new software has been downloaded and verified

b) The original version of flash software shall always be held in memory and available for use if required or until overwritten by a further version at a later date
4.7 ENCLOSURES AND POWER SUPPLIES

c) Intelligent Controllers shall be contained within a steel enclosure and include a
dedicated tamper circuit without having to use auxiliary input circuitry on the
controller boards

d) Intelligent Controllers shall have a mains power supply with dedicated LV
circuits or a Power over Ethernet (POE) supply. Each power supply option shall
include an integral 4-hour battery back-up and for additional resilience the POE
option may also include UPS protection

e) Each LV PSU shall be incorporated into the Intelligent Controller enclosure and
support the system electronics, two card readers and two lock outputs. The
integral PSU shall have a minimum capacity of 3A at 12Vdc. POE shall have a
minimum capacity of 25W (POE Plus)

f) HV power supply circuits shall be clearly identified and shall always conform to
the relevant electricity at work act

g) Intelligent Controllers with POE Plus shall include an integral battery for
extended power resilience and for inrush support on locking circuits

h) To avoid nuisance alarms, Intelligent Controllers shall detect and report mains
power failure only after 10 minutes duration

4.8 READERS AND KEYPADS

a) The system shall support modern-day reader types, allowing the use of ID card
and biometric technologies

b) The system shall support 2 x different reader technologies being active at the
same time on any single IDC

c) The system shall support an additional reader at each operator station to enable
new cards to be added to the system

4.9 CE COMPLIANCE

a) System hardware, including Field Network communications equipment, shall
produce low level electromagnetic emissions and exhibit a high degree of
electrical noise immunity. As a minimum the equipment shall meet the following
standards without the use of screened cables:

- IBS EN 50133-1 + A1 1997 – Emissions and immunity standard for access
  control systems
- BS EN 55022 class B 1998 – Emissions standard for information
  technology equipment
- BS EN 50133-1 + A1 1997 – Immunity standard for access control systems
- BS EN 61000-4-2 1995 – ESD requirements
5 SYSTEM SOFTWARE – OVERVIEW

5.1 GENERAL SYSTEM OPERATION

a) System software shall be installed on the ACS main server or a suitable distributed computing solution and shall be accessed via a system PC running a supported browser.

b) The ACS user interface shall be 100% browser compliant. ACS application software that needs to be installed on a local or client PC will not be accepted.

c) A single log-on page shall open all of the administrative privileges for any given user. ACS management including configuration, administration, real-time system monitoring and system reporting shall all be accessed within a single browser instance from any system PC. Systems that require a user to log-on more than once in the same session or requires a separate log-on instance for different parts of the system will not be accepted.

d) The features and options that are available within the ACS shall be controlled by licensing. The licence shall be able to switch options on and off and to control limits of the software including the number of personnel and the number of controllers supported. The software shall not operate without a licence and licence shall require security validation in order to continue working after a trial period.

e) The ACS software shall include a multi-lingual capability that is readily available within the ACS browser application. The operator shall be able to easily change to their preferred installed language, including right-to-left and Cyrillic fonts.

f) Log-on security permissions shall not be compromised or altered when changing between different languages. When right-to-left languages are selected, system work-flow, system procedures, and the entire graphical environment shall change into a right-to-left presentation.

g) New language packs shall be easily installed without needing to reinstall or update the existing ACS software.

h) The ACS shall be easily navigated via a system of menus and navigation hubs. While browsing anywhere in the system, a single click shall take the user back to a start menu where any new task may be started.
i) Every device and operating parameter within the system, for example Readers, Time Zones, Access Levels, etc. shall be described with an alphanumeric name and shall support a minimum of 256 characters per field name/description

j) System transactions and system status shall be transmitted from IP and Field Network Controllers to the main ACS server in real time. This information shall be used to generate on-screen incidents and historical reports

k) The ACS shall support pre-defined emails and/or SMS text messages upon the occurrence of nominated incidents or events

l) The system shall interface with third-party systems for example CCTV, Fire and Intruder systems.

5.2 USER/SYSTEM OPERATOR ACCESS

a) The ACS shall allow an unlimited number of system users, each with strictly controlled administrative privileges. Each user shall have a log-on username and password

b) A user shall belong to a system user group which shall determine the system functions the user is permitted to use. The system shall support an unlimited number of user groups and shall include default user groups to minimise initial configuration work. Default user group profiles shall include:

- Installer
- Security Manager
- Administrator
- Guard
- Token Administrator
- Standard Operator

It shall be possible to edit the permitted system functions and options associated with each user group.

c) It shall be possible to set up and edit system policies for the use and management of passwords. The password policy shall specify the minimum length of the password, how often the password is to be changed, the number of permitted failed attempts before the system user is locked, whether upper case and/or non-alpha characters are mandatory, and the size of the password history to keep. There shall be no limits to the number of password policies supported

d) There shall be no limits to the set-up and control of hidden, read only, read/write, and delete functions on a field-by-field level. This feature shall be available system wide

e) Allow and Deny rules shall include the ability to configure detailed data access either for User Groups or individual Users. Such rules shall include the ability to
allow or prevent access to individual types of data objects, fields within those objects and specific tasks and commands relating to the objects

f) The system shall include the facility to lock out a system user who uses an incorrect ID or password more than a certain, configurable, number of times

6  SYSTEM SOFTWARE – HARDWARE CONFIGURATION

6.1  GENERAL

a) The ACS system shall allow hardware configuration to be implemented via any system PC running a system supported browser

b) It shall be possible to configure and save any system device without previously defining its parent device

c) Orphaned devices in the software shall be clearly flagged by the system so they are not overlooked during system commissioning

d) The system shall support multiple sites, where each site is a separately managed access control location

e) It shall be possible to add additional communications software elements in order to support remote sites or to implement distributed processing

6.2  PANEL/CONTROLLER CONFIGURATION

a) There shall be no practical limit to the number of panels on the system

b) IP connected and RS485 controllers shall be supported on the same system

c) The following minimum attributes shall be specified for each panel on the system:
   • Chosen language name/description (256 characters minimum)
   • Panel Type (hardware variant)
   • IP address
   • Parent Comms Engine
   • Whether the panel is to be regularly polled by the system

d) The following connection attributes shall also be specified for each IP-connected panel:
   • IP address
   • Whether link is encrypted

e) The following minimum attributes shall also be specified for each 485-connected panel on the system:
Field network
Unique address on the field network

6.3 FIELD NETWORK/PORT CONFIGURATION

a) There shall be no practical limit to the number of field networks on the system. Up to 32 485-connected panels/controllers shall be supported on each field network.

b) The following minimum attributes shall be specified for each 485 connected panel on the system:
   - Chosen language name/description (256 characters minimum)

c) The following minimum attributes shall be specified for each port on the system:
   - Chosen language name/description (256 characters minimum)
   - IP address
   - Parent field network
   - Whether encrypted

6.4 DOOR CONFIGURATION

a) There shall be no practical limit to the number of doors on the system

b) The following minimum attributes shall be specified for each door on the system:
   - Chosen language name/description (256 characters minimum)
   - Associated panel/controller
   - Unlock period (in hours, minutes and seconds - minimum 0.1s)
   - Indicate valid reads sounder
   - Indicate invalid reads sounder
   - Max. open period before the door is deemed to be wedged open
   - Minimum open period
   - Indicate wedged option (per door)
   - Indicate forced option (per door)

c) The system software shall allow a door to be interlocked with another door on the same controller such that both doors cannot be unlocked at the same time

d) The system shall allow other events or modes to operate a door; for example emergency mode or schedule
6.5 READER CONFIGURATION

a) There shall be no practical limit to the number of car/token readers on the system

b) The following minimum attributes shall be specified for each reader on the system:
   - Chosen language name/description (256 characters minimum)
   - Reader type/technology
   - Associated panel/controller
   - Associated door
   - Reader group

c) A keypad shall be supported to enable entry to additionally be verified by PIN entry. If keypads are supported a maximum time shall be defined for keypad entry

d) It shall be possible to configure a reader as requiring an additional card/token to be read before the door will unlock. If Dual Read is required, a maximum time for the second read shall be configurable

e) It shall be possible to configure a reader as requiring an additional card/token to be read for users that require an escort

f) It shall be possible to configure a reader to permit commands to be issued by entering numbers at the associated keypad

6.6 INPUT CONFIGURATION

a) There shall be no practical limit to the number of inputs on the system

b) The following minimum attributes shall be specified for each input on the system:
   - Chosen language name/description (256 characters minimum)
   - Associated panel/controller
   - Type of input
   - Sense period
• Description that is reported when input is Activated
• Description that is reported when input is Reset
• Normally open or normally closed

c) It shall be possible to group inputs that are to be used or managed together. There shall be no restriction of the number of inputs in a group

6.7 OUTPUT CONFIGURATION

a) There shall be no practical limit to the number of outputs on the system

b) The following minimum attributes to be specified for each output on the system:
   • Chosen language name/description (256 characters minimum)
   • Associated panel/controller
   • Time that output will remain switched on when activated

c) It shall be possible to group outputs that are to be used or managed together. There shall be no restriction of the number of outputs in a group

6.8 LIFT/ELEVATOR CONTROL

a) The system shall allow access to elevators and elevator floors to be restricted according to access management rules including time, day and system mode

b) For generic lift/elevator interfacing the ACS shall be capable of operating system outputs that can be used to restrict access to specific call buttons in a lift/elevator cab. Subsequent to a successful card/token read, and subject to access groups associated with the card/token, Input/Output (IOC) relay outputs shall be operated to invoke nominated call buttons

7 SYSTEM SOFTWARE – ACCESS CONTROL ELEMENTS

7.1 TIME SCHEDULES AND PATTERNS

a) The ACS shall support the definition of time schedules that are used to define when access is permitted at certain doors, when events are reported and when actions can be set to occur

b) The system shall use time schedules for:
   • Defining when access is permitted
   • Defining times when intruder detectors and alarm inputs are active
   • Defining when system actions such as the automatic locking and unlocking of doors are in operation
   • Defining when events are reported as alerts
• Defining when reports and backups are automatically run

c) There shall be no practical limit to the number of time schedules defined on the system

d) The system shall include a number of default time schedules including All The Time and Never

e) Each time schedule shall consist of one or more time patterns, where each time period will define one or more specific periods of time

f) It shall be possible to set up recurring time patterns, such as every Monday morning

g) It shall be possible to exclude time patterns from a schedule, for example public holidays

h) It shall be possible to import time patterns held in standard calendar formats, for example representing public holidays or scheduling information

i) Relevant time zones shall be stored at the controllers and continue to operate in the event of a communications failure or failure of the ACS main server

7.2 SYSTEM MODES

a) The ACS shall permit the use of system modes that enable a straightforward way to manage multiple aspects of the access control system

b) The following minimum attributes shall be specified for each system mode name:
   • Chosen language name/description (256 characters minimum)
   • Flag indicating whether the mode is Active by Default

c) The ACS shall allow the following system functions to be altered by using system modes:
   • Access permissions
   • Automatic actions such as unlocking doors
   • The operation of outputs
   • The sending of commands to the system including third-party integrations
   • Alarm event handling and redirection

d) There shall be no practical limit to the number of modes defined on the system

e) The ACS shall allow system modes to be activated and deactivated from the ‘real time’ control centre screen
f) The control centre module shall display the modes of operation currently activated

7.3 CARD/TOKEN TYPES

a) The ACS shall support multiple card/token types. There shall be no practical limit to the number of card/token types to be defined on the system

b) It shall be possible to define tokens that use different access technologies, such as wireless locks

c) The following minimum attributes shall be specified for each card/token pool name:
   - Chosen language name/description (256 characters minimum)
   - Whether cards/tokens of this type can be returned
   - Whether cards/tokens of this type can be printed

d) It shall be possible to select one card/token type as a default, to simplify the process of issuing cards/tokens

7.4 CARD/TOKEN POOLS

a) The ACS shall support multiple card/token pools. There shall be no practical limit to the number of card/token pools to be defined on the system

b) The system shall support multiple card/token pools for example Permanent, Temporary, Contractor, and Visitor. Card/token pools shall enable batch control of access rights and greater categorisation of cards/tokens for filtering and reporting purposes

c) The following minimum attributes shall be specified for each card/token pool:
   - Chosen language name/description (256 characters minimum)
   - Whether the pool is to be used for temporary tokens
   - Whether the pool is to be used as the default pool for token assignment

7.5 CARDS/TOKENS

a) The ACS shall permit cards/tokens to be set up and issued to people. There shall be no practical limit to the number of cards/tokens to be defined on the system

b) Card/token records shall be held separately from personnel records, such that there may be a card record without a person or a personnel record without a card/token.

c) The following minimum attributes shall be specified for each card/token:
- Token card number
- Associated Token Pool
- Token Status
- Associated Token Type
- Validity Dates of the token
- PIN

d) Each card/token shall have a status. Only cards/tokens with a status of Enabled are permitted to gain access

e) The system shall support the capture of the Card number/ID by the presentation of the card/token at an attached reader

f) Each card/token shall have a start date and an end date which shall be separate from the user validity or access permission period. This shall be used to indicate that a card is Pending or Expired

g) The system shall allow users to monitor the status of a token from a summary information page

7.6  ID CARD/TOKEN PRINTING

a) The ACS shall support the printing of cards/tokens for cardholders

b) The card/token designs shall enable personal data from the ACS database to be incorporated, including photos. The designs shall also enable the inclusion of standard text and graphics such as company names and logos

c) The ACS shall allow ID cards to be linked to a department or token type

d) ID card printing shall be managed via any system PC using a supported browser interface but the ACS shall only allow card/token printing to be carried out at pre-designated ID card/token printers. To control and manage this requirement, system ID printer services shall be installed at the nominated ID card/token printer stations

e) The ACS shall include some sample token designs: additional ones can be created and modified using a separate software tool

f) The ACS shall support multiple printers for staff and visitor cards. Different printers shall be supported to allow permanent or temporary badges. Card designs shall be available in landscape and portrait

7.7  CARD/TOKEN PENALTY POINTS

a) The ACS shall include a facility to automatically suspend cards/tokens that are misused
b) A card/token shall gain penalty points for certain violations. Points shall be configurable on a system-wide basis and shall be gained by any card/token for the following:
   - Entering the wrong PIN
   - No access rights
   - Attempting access at the wrong time

c) If a card/token gains a pre-determined amount of points the card/token shall automatically be suspended and a system event created. This threshold for suspension shall be configurable on a system-wide basis

d) Points shall expire over time to forgive occasional mistakes

e) No access rights and wrong time violations shall have similar behaviours. Points shall only be gained by attempting different readers. Presenting a card/token many times to the same reader consecutively shall not gain additional points

f) A wrong PIN shall gain points for every attempt regardless of the reader used. If that card/token subsequently has a valid access at the same reader the points shall immediately be cancelled so that a genuine user is not penalised

g) Points acquired shall expire at a rate of 1 point every 6 minutes (10 points per hour)

h) A card/token automatically suspended by the system for misuse shall not affect other cards/tokens assigned to the same card/token holder

i) It shall also be possible for the ACS system administrator to suspend a card manually

j) A suspended card/token shall require a manual re-set before the card/token can be re-used

7.8 UNUSED CARD/TOKEN

a) The ACS shall include a facility to automatically suspend a card/token if the card/token has not been used for a number of days

b) This number of days of inactivity shall be configurable on a system-wide basis

7.9 DURESS PIN

a) The ACS shall provide a facility whereby a cardholder, if forced against his/her will to open a PIN controlled door under duress, will create an immediate duress alarm condition. For the cardholder’s safety, the raising of this alarm shall not have any obvious effect at the door concerned

b) A duress alarm shall be activated if the cardholder enters a known Duress PIN at the reader in place of their normal PIN
c) A duress alarm shall not be evident at the reader. The access checks normally executed by the system, for example if person is authorised for that door, at that time and that day of the week, shall still be enforced for a duress event.

### 7.10 AREA CONTROL

a) The ACS shall support the definition of secure areas.

b) There shall be no practical limit to the number of areas to be defined on the system.

c) The following minimum attributes shall be specified for each area:
   - Name/description (256 characters minimum)
   - Timeout
   - Maximum occupancy permitted
   - Minimum occupancy permitted
   - Snapshot

d) An area shall be defined with entry and exit readers and shall allow the system to monitor people in specific locations and enforce anti-passback rules.

e) When a card/token holder enters an enforced anti-passback area all of their cards/tokens shall be deemed to be in the same area. This shall prevent the card/token holder from passing back their card for use a second time into the area and shall also prevent other cards held by the card/token holder being distributed for use by others into the same area.

f) In the event of loss of communications the controllers managing area readers shall preserve soft anti-passback rules which shall maintain anti-passback rules at a single door level and shall monitor individual card/token usage rather than all cards/tokens assigned to a card/token holder. Once communications have been restored, transactions and area information shall be updated and synchronised with the ACS.

g) When people tailgate from an area and the system believes them to still be in an area, at the same time each day an optional Timeout shall clear all cards/tokens from the area and make their whereabouts on the system ‘Unknown’. The next use of these cards/tokens shall place them into the correct area. The Timeout setting for each area on the system shall be optional, user-definable and specific to the particular area.

h) The system shall support Maximum and Minimum Occupancy settings that shall cause a system event and/or incident if the settings are violated.

i) The system shall permit an area to be marked as abnormal when it only has one occupant.

j) For any given area the ACS shall optionally maintain historical snapshots of who was in an area at any particular time in the past. The frequency of updating
area snapshots shall be defined by a time period in days, hours, minutes and seconds, or by a number of events occurring between the snapshots. Snapshots shall be retained by the system for a time period set in days, hours, minutes and seconds

8 SYSTEM SOFTWARE – PERSONNEL/CARDHOLDERS

8.1 PERSONNEL/CARDHOLDERS

a) There shall be no practical limit to the number of card/token holders (personnel) on the system

b) There shall be no practical limit to the number of active cards/tokens, or combination of card/token technologies to be allocated to an individual

c) The following information shall be required as a minimum for personnel and shall be available for input and edit directly from the card/token holder record (personnel record):
   - Title
   - First name (256 characters minimum)
   - Surname/family name (256 characters minimum)
   - Employee number
   - Department name (256 characters minimum)
   - Escorted and extended unlock options for the specific card/token holder
   - Area exempt option for the specific card/token holder
   - A blanket ‘access start date’ and ‘access end date’ for the specific card/token holder
   - Card/token administration history for each card/token held by the card/token holder
   - Custom defined fields with no practical system limit to the number of fields definable
   - Token management for cards/tokens allocated to the card/token holder
   - Access management for the card/token holder
   - Card/token holder photo management
   - A comment ‘free text’ field (256 characters minimum)

d) An escort function when selected, shall require that the card/token holder is valid at a reader and is also accompanied and verified by a valid ‘host card/token’ before the door will unlock
e) To assist card/token holders that have mobility difficulties the extended unlock feature shall allow a card/token holder to have longer unlock periods at nominated doors. This feature when selected, shall only apply at pre-defined readers/doors and shall not be a global setting.

f) The area exempt function shall allow the card/token holder to be exempt from area rules. For example, enforced anti-passback violations would not restrict the card/token holder from entering an area.

8.2 PERSONNEL CARD/TOKEN MANAGEMENT

a) The ACS shall permit card/token management tasks to be directly available from the card/token holder (personnel) record. These shall include:
   - Creating and issuing cards/tokens for the card/token holder
   - Printing a card/token with a selectable design at a selectable ID card/token printer
   - Revoking individual cards/tokens from the card/token holder
   - Suspending and resetting individual cards/tokens from the card/token holder

b) The system shall support intelligent issue of temporary tokens, such that when a temporary token is assigned to a person, other tokens of that type and assigned to that person will be made unusable.

c) The system shall permit the display of token diagnostics and status enabling the user to check permissions, validity and status of tokens.

d) The system shall permit the display of history token history, enabling the user to view details of token assignment and status changes.

8.3 PERSONNEL PHOTO/IMAGE MANAGEMENT

a) The ACS shall allow personnel ID images to be associated with personnel/cardholders.

b) The system shall permit images to be captured directly from a webcam feed or imported from previously acquired .jpg or .png images.

c) The system shall allow stored images to be cropped in 16:9, 4:3, 1:1, 3:4, or 9:16 ratio.

d) The system shall also allow other documents such as passport and driving licence images to be saved with the personnel record.

e) The system shall permit multiple photos to be associated with a single person/cardholder. It shall be possible to select one photograph to be displayed by default.

f) The system shall allow photos to be exported/saved to file system.
8.4 PERSONNEL ACCESS MANAGEMENT

a) The ACS shall provide precision access capability for every card/token holder on the system

b) There shall be no practical limit to the number of Access Groups defined on the system

c) The following minimum attributes shall be specified for each Access Group name:
   - Chosen language name/description (256 characters minimum)
   - Access start/end

d) Access Groups shall be associated with personnel (card/token holders) and shall not be associated with specific tokens. Every card/token assigned to a card/token holder shall inherit the Access Groups associated with the card/token holder

e) Multiple and varied Access Permissions shall be applied under a single Access Group which shall incorporate Reader Groups, Access Permissions, and Access Groups:
   - A Reader Group shall be a group of one or more readers into a specific area for example:
     ‘Development Office’
   - An Access Permission shall be a single Reader Group associated with a single Weekly Time Zone and a single System Mode, for example:
     ‘Development Office : All the Time : Normal System Mode’
   - An Access Group shall be a selection of one or more Access Permissions and assignable to any card/token holder in a single operation for example a single Access Group may include:
     - Development Office : All the Time : Normal System Mode
     - General Office : Monday to Friday 08:00 – 18:00 : Normal System Mode
     - Warehouse : Monday to Friday 09:00 – 17:00 : Normal System Mode

f) The system shall support one or many Access Groups being assigned to any card/token holder on the system

9 SYSTEM SOFTWARE – VISITOR MANAGEMENT

9.1 GENERAL

a) The ACS system structure shall support a Visitor feature that enables visitors to be recorded and managed.
b) The system shall enable visitors to be recorded either in advance or at the point of arrival.

c) Visitor details including the ID photograph shall be stored on the system for future visits

9.2 VISITOR ARRIVAL

a) The use of a visitor wizard shall enable visitors to be recorded easily at the point of arrival.

b) The visitor arrival process shall support the linking of a visitor to a host. It shall be possible to specify that a visitor must be escorted at all times.

c) The visitor arrival process shall support webcam ID capture to allow personnel ID images to be associated with the visitor. It shall also be possible to import previously acquired .jpg or .png images

d) The visitor arrival process shall support the issue a visitor access card/token with access permissions being assigned to the card at the point of issue

e) The visitor arrival process shall support the recording of visitor car registrations/ and details of baggage left at the reception desk

f) The visitor arrival process shall enable the printing of visitor tokens/ passes/ badges to paper or plastic ID cards

9.3 VISITOR DEPARTURE

a) The end of the visit shall be recorded including the return of an issued token and the return of baggage.

b) Visitor cards shall be made void of access authorities upon being returned to reception

c) The system shall support both a temporary and a permanent departure.

9.4 VISITOR MONITORING

a) A visitors’ dashboard screen shall give an overview of expected and current visitors within a specified time period

b) The system shall enable users can view scheduled visits for a specific day, hour or week. It also supports the definition of a specific time period.

c) The system shall support the viewing/filtering of planned visits by status.
10 SYSTEM SOFTWARE – CONTROL CENTRE

10.1 GENERAL

a) The ACS shall incorporate a fully comprehensive Control Centre function that allows security staff and operators to monitor and interact with the system in real-time.

b) The ACS shall display incidents/alarms and normal events (non-alarms) in separate sections of the same Live View page. Normal (non-alarm) events shall be displayed with the most recent event at the top of the list.

c) Normal events shall be for information only and shall not have a workflow.

d) For normal (non-alarm) events the system shall support event profiles that can be configured to include or omit certain types of events. For example, a security guard that is responsible for a single building may wish to only view transactions for that particular building and a maintenance engineer may wish to only see hardware events but from across the whole system. The configuration flexibility of Event Profiles shall be unlimited with pre-defined Event Profiles being selectable at any time from within the Live View page. Consequently the event list shall immediately reflect the new reporting rules in the event list.

e) Events shown in the event list shall be selectable by the operator and shall ‘drill-down’ to show more detailed information about the selected event. For example, a card/token event at a reader shall show:
   - The status of the door associated with the reader
   - The occupancy status of an area associated with the reader
   - The card/token status including any penalty points applied to the card
   - The ID image of the card/token holder

f) In addition, depending upon the security log-on level of the operator, selected events in the event list shall invoke interactive controls that the operator may wish to command directly from the event list. For example, a card/token event at a reader shall present:
   - Door controls – Lock, Unlock, Single Unlock, Isolate Switch
   - Reader controls – Inhibit Reader, Restore Reader
   - Card/token controls – Suspend, Reset Suspension
   - Area controls – Resync, Make All Unknown from the area, Move Everyone from the area

g) The Control Centre shall include interfacing to third-party systems such as CCTV systems, Intruder Panels and Fire Panels.
10.2 INCIDENT/ALERT REPORTING

a) The ACS shall display incidents/alarms on the same Live View page as non-alert events.

b) Incidents/alarms shall be displayed with the highest priority at the top of their list and moving off the list when closed by an operator. Incidents/alarms shall append to the normal event list when they are closed and removed from the incident/alarm list.

c) Incidents/alarms shall have three states and shall require a basic workflow:
   - Open – This shall be the initial state when an incident/alarm is created
   - Acknowledged – This state shall be caused by the operator by selecting an incident and choosing to acknowledge the incident
   - Closed – This shall be the final state of an incident and shall indicate that no further action shall occur

d) The system shall allow an operator to include notes when acknowledging or closing an incident/alarm. These notes shall assist other operators with processing the incident. Additional notes may be included at any time by any operator.

10.3 DEVICE MANAGEMENT

a) The Control Centre shall include, depending upon the security log-on level of the operator, a Device list showing every device on the system. The device list shall include, but not be limited to:
   - Area
   - Panel
   - Door
   - Reader
   - Input
   - Output
   - Personnel
   - System Mode
   - Card/Token
   - Third-Party device integrated with the ACS

b) Depending upon the security log-on level of the operator, any Device on the system shall be selectable to show its status. Abnormal or insecure states shall be highlighted.
c) Appropriate interactive controls shall also become available to manage and control the Device selected.

d) Depending upon the security log-on level of the operator, System Modes shall be easily activated/deactivated from this page.

e) The Control Centre shall report on devices in an insecure or unexpected state. Depending upon the security log-on level of the operator, appropriate interactive controls shall also become available to manage and control any device that is selected.

10.4 AREA MANAGEMENT

a) The Control Centre shall include a real-time Areas control that shall list people in a selected area. A selected Area shall display:

- People in the area by full name
- The card/token number used to enter the area
- The date and time of entry into the area
- The reader used to enter the area

b) The Areas control shall also include, depending upon the security log-on level of the operator, interactive controls for the operator to:

- Move everyone from the area
- Make all unknown
- Make selected person unknown
- Make selected person out-of-area
- Resync the area
- Print a muster report for the area

10.5 WATCH LIST

a) The Control Centre shall allow a Watch List to be configured and displayed. A watch shall allow the operator to select one or more card/token holders and display all their subsequent transactions on a separate temporary Watch list.

b) The list of watched transactions shall include full details of each card/token read associated with that cardholder.

c) The watch list shall enable the selection of visitors.
10.6 VISUAL REPRESENTATION

a) The ACS Control Centre shall include the option of including a visual representation of the managed site, and the status of various elements of the access control system.

b) The system shall support the import of maps/plans in .jpg or .png format and shall support multiple maps which may provide different levels of detail. There shall be no practical limit to the number of maps/plans on the system.

c) Navigation between maps/plans shall be via definable hot-spots or from a list of system maps/plans.

d) Objects within the access control system shall be represented by icons appearing on the maps/plans. The system shall distinguish between objects in a normal state and objects in an insecure state.

e) The objects that can appear shall include, but not be limited to:

   • Doors
   • Panels
   • Readers
   • Inputs
   • Outputs
   • Areas
   • System Modes

f) Depending upon the security log-on level of the operator, doors, inputs and outputs shall be easily controlled from the map page

g) The system shall support different sets of icons

10.7 PHOTOGRAPHIC IDENTIFICATION

a) The ACS shall enable the display of user photographs in real-time, in order to check the identity of personnel as cards/tokens are read at selected readers.

b) It shall permit multiple readers to be selected for monitoring.

c) It shall enable pictures to be viewed in different sizes and with varying levels of detail about the user, card/token and access attempt.

d) It shall enable a historical list of reads on the selected reader to be displayed.

e) It shall allow the user to select the display of photographs from all reads, Valid reads only or Invalid reads only.
f) It shall permit the real-time update of photographic display to be paused and restarted.

11 SYSTEM SOFTWARE – EVENT CONFIGURATION

11.1 EVENT NOTIFICATION

a) The ACS shall support the automatic sending of messages to specific recipient when specific defined events are generated on the system.

b) It shall support the sending of messages via email or SMS

c) It shall support the identification of recipients by email address or telephone number.

d) It shall support the use of a standard template that can include formatted text and graphics.

e) It shall support the inclusion of strings that shall be substituted by appropriate information about the event at the point the message is sent. For example, the time of the event, the name of the specific object.

11.2 TRIGGERING COMMANDS

a) The ACS shall include a method of issuing commands directly to access control equipment including elements of the access control hardware (doors, reader, panels, inputs and outputs) and logical elements such as reports, areas, modes, and system services

b) It shall permit anything controlled by the ACS system itself to be commanded, including external equipment

c) It shall permit any event that can be raised within the ACS system to trigger the sending of a command

12 SYSTEM SOFTWARE – SYSTEM REPORTS

12.1 GENERAL SYSTEM REPORTS

a) The system shall offer a wide variety of management reports that shall be generated from the system database and the historical events database

b) Reports shall be selected and run within a browser environment

c) Reports shall offer options for tailoring reports by setting parameters/filters. Time/date filters will allows a report to be run relative to a specific date, such as yesterday or the last day of the month

d) The system shall allow reports to be printed to any system printer in a high quality format
e) The system shall permit reports to be exported in various formats, including, but not limited to, PDF, CSV and MS Excel formats.

f) The system shall support the saving of report definitions/filters so that the same user can run the same report again.

g) The system shall permit reports to be shared with other system users.

h) The system shall permit reports to be run on a regular schedule. It shall be possible for scheduled reports to be printed automatically, emailed or saved to a file location.

12.2 TRANSACTIONAL HISTORY REPORTS

a) Reports related to personnel/cardholders and access shall include, but not be limited to, the following:
   - List of history events occurring on the system
   - Details of personnel attendance
   - Details of acknowledged incidents
   - Actions performed by system accounts

12.3 PERSONNEL AND ACCESS

a) Reports related to personnel/cardholders and access shall include, but not be limited to, the following:
   - Details of access group membership
   - Details of cardholder and the tokens they hold
   - Access permissions by cardholder
   - Reader access by cardholder
   - Door access by cardholder
   - Details of changes to cards/tokens

12.4 AREA MONITORING

a) Reports related to areas shall include, but not be limited to, the following:
   - Current occupancy
   - Total time spent in an area
   - Muster report
   - All transactions related to an area
12.5 SYSTEM AUDIT
a) Reports related to system auditing shall include, but not be limited to, the following:
   - Audit of all changes made to system objects
   - Log of reports run

12.6 VISITORS
a) Reports related to visitors shall include, but not be limited to, the following:
   - Details of all visitors and visits recorded on the system
   - Details of all visitors currently on site

12.7 SYSTEM SETTINGS
a) Reports related to system settings shall include, but not be limited to, the following:
   - Details of all system users
   - Details of security rules that apply to system users

12.8 DEVICES
a) Reports related to hardware and devices shall include, but not be limited to, the following:
   - Details of configured doors
   - Details of configured panels
   - Details of configured readers
   - Details of configured inputs
   - Details of configured outputs

13 MANAGEMENT/SYSADMIN OPTIONS

13.1 USER MANAGEMENT
a) The ACS shall include the facility to allow a system administrator to reset a user who has been locked out following the entry of an incorrect ID or password

b) It shall include the facility to allow a system administrator to change a user’s password
13.2 ADDITIONAL DATA FIELDS

a) The ACS shall enable extra data fields to be added to any of the data objects within the system

b) The system shall support extra data fields of different data types, including string, integer, decimal, date/time and Boolean

c) The additional data fields shall be visible within the user interface

13.3 RUNNING AND SCHEDULING BACKUPS

a) The ACS shall include a facility for backing up system databases without requiring external tools

b) It shall permit individual databases to be selected and the destination path to be defined

c) It shall be possible to set up regular scheduled backups

13.4 DIAGNOSTICS

a) Each part of the ACS shall log its activity

b) The ACS shall include a diagnostics option that allows IT support staff to view detailed information about the system in real-time

c) The diagnostics utility shall be configurable to permit various levels of detailed reporting

14 TENANCY

14.1 GENERAL

a) The ACS shall support multi-tenancy configuration, where parts of a building are owned and/or accessed by different organisations

b) It shall appear to each Tenant organisation that they are running their own ACS. The Landlord and each Tenant organisation shall have their own system users, system user groups and log-ins so they can control system security within their own organisation

c) Each Tenant shall only be able to access data relevant to them, never data associated with other tenants

14.2 LANDLORD ACCESS

a) The ACS shall only ever support one Landlord within a multi-tenancy structure

b) The Landlord shall be responsible for setting up the subsidiary tenant structure
c) The Landlord shall be permitted to create data and make it visible to a tenant

d) The Landlord shall be permitted to create data and assign ownership of it to a tenant

e) The Landlord shall be permitted to see all incidents and events occurring anywhere on the entire system

f) The Landlord shall be permitted to see all tokens for all Tenants, and can control all tokens. The Landlord can suspend any token at any time

14.3 TENANT ACCESS

a) Each Tenant organisation shall be permitted to see only data relevant to them, never data associated with other tenants

b) Tenants shall be permitted to create their own data

c) Tenants shall be permitted to view data that has been made visible by the Landlord, but cannot edit it

d) Tenants shall be permitted to edit and manage data that has been created by the Landlord and assigned to that Tenant

e) Tenants can see incidents and events occurring within their tenancy

15 INTEGRATION OPTIONS

15.1 EVENT BASED INCLUDING CCTV

a) The ACS system shall support specific interfaces available to permit events and commands to be sent to a third party system including CCTV systems

b) Supported interfaces shall include, but not be limited to, the following: exacqVision, Honeywell Maxpro, IndigoVision, Mirasys, SeeTec and Verint

15.2 ELEVATORS

a) The ACS system shall support specific interfaces in order to integrate with elevator systems

b) Supported interfaces shall include, but not be limited to, Otis and Kone elevator control systems

c) The interface shall support events and state changes from the elevator control system being passed to the ACS

d) The interface shall support status information from the elevator control system being displayed in the ACS
15.3 FIRE PANEL

a) The ACS system shall support specific interfaces in order to integrate with third-party fire panels

b) Supported interfaces shall include, but not be limited to, Simplex fire panels

c) The interface shall support events and state changes from the fire panel and its associated monitoring points being passed to the ACS

d) The interface shall support status information from the fire panel being displayed in the ACS

e) The system shall support the user being able to monitor and manage the fire panel and associated alarms

15.4 ALARM PANEL

a) The ACS system shall support specific interfaces available to integrate with third-party alarm panels

b) Supported interfaces shall include, but not be limited to, Galaxy fire panels

c) The interface shall support events and state changes from the fire panel and any of its associated alarms being passed to ACS

d) The interface shall support status information from the alarm panel being displayed in the ACS

e) The system shall support the user being able to monitor and manage the alarm panel and associated alarms and outputs

15.5 DATABASE IMPORT

a) The ACS system shall provide a method of importing data from external databases, including HR, ERP and Visitor systems

b) The interface shall support the addition, deletion and editing of cardholder and card/token data

c) The interface shall provide logging and audit of database changes

15.6 WIRELESS LOCKS

a) The ACS system shall support specific interfaces in order to integrate with wireless lock systems

b) Supported interfaces shall include, but not be limited to, Salto and Aperio locks

c) The interface shall support the synchronisation of data between the lock system and the ACS
d) The interface shall support the representation of wireless locks and associated hardware in the ACS

e) The interface shall support the issue and updating of cards/tokens from within the ACS

f) The system shall support events and state changes from the lock system being displayed in the ACS

16 WARRANTIES, MAINTENANCE AND SERVICE

16.1 WARRANTY

a) The contractor shall warrant the ACS according to the manufacturer's Terms and Conditions of Sale

b) Support contracts to extend the warranty coverage shall be available from the installing system integrator

c) The system integrator shall be the focal point for all service issues and questions (with the manufacturer's support). The system integrator shall be approved by the ACS manufacturer to install and support the system

16.2 MAINTENANCE AND SERVICE

a) The integrator shall provide all services required and equipment necessary to maintain the entire ACS in an operational state as specified for a period of one (1) year after acceptance of the system, and shall provide all necessary material required for performing scheduled adjustments or other non-scheduled work

b) The adjustment and repair of the ACS shall include computer equipment, software updates, and signal transmission equipment, access control equipment, facility interfaces, and support equipment. Responsibility shall be limited to integrator supplied and/or installed equipment. The integrator shall provide the manufacturer's required periodic maintenance and other work as necessary

16.3 QUALITY ASSURANCE

a) The manufacturer of all hardware and software components shall be established vendors to the access control/security industry for no less than five (5) years

b) All hardware equipment shall conform to the applicable international standards for EMC compliance. The manufacturer shall be certified to ISO9001 or similar

c) The integrator shall have been regularly engaged in the installation and maintenance of integrated access control systems similar in size and scope to that outlined herein for a period of no less than five (5) years
d) The integrator shall supply certification that they are an authorised dealer for the proposed system

e) The integrator shall supply certification that the installation and service personnel have been factory trained in the installation and maintenance of the ACS

f) The integrator shall provide a minimum of three (3) references whose systems are of similar complexity and have been installed and maintained by the system integrator in the last three (3) years

g) There shall be a factory-authorised service organisation which stocks a complete inventory of spare parts, and which can provide maintenance for the system