

Access Control System Specification

Table of Contents

| | |
|---|----|
| Access Control System Specification | 1 |
| Scope..... | 4 |
| Terminology..... | 4 |
| Card..... | 4 |
| System Overview | 5 |
| Identification..... | 5 |
| Component specifications..... | 6 |
| Door hardware | 6 |
| Cards and Readers..... | 6 |
| Infra-red | 7 |
| Proximity..... | 7 |
| Mag-stripe | 7 |
| Mifare (serial-number reader)..... | 7 |
| Mifare (sector reader) | 7 |
| Biometric with Mifare..... | 7 |
| Cabling..... | 8 |
| ACUs..... | 8 |
| General description | 8 |
| Features provided..... | 8 |
| Software | 12 |
| General description | 12 |
| Database..... | 12 |
| Communications | 12 |
| User-interface..... | 12 |
| Equipment set-up | 13 |
| Card-holder details..... | 13 |
| Access rights | 13 |
| Configuration and other database reporting..... | 13 |
| Roll-call reporting..... | 13 |
| Attendance Reporting | 14 |
| Real-time event reporting | 14 |
| On-demand event reporting | 14 |
| Alarm reporting..... | 14 |
| CCTV interface..... | 14 |
| System Operators | 15 |
| Multiple tenants | 15 |
| Photo-ID..... | 15 |
| Site Plans..... | 15 |
| System Parameters | 16 |

| | |
|--|----|
| Technical specification of ACUs | 16 |
| Maximum capacities of ACUs | 16 |
| Maximum capacities of System | 16 |
| Installation, commissioning and training | 17 |
| Warranties and standards | 18 |
| Standards | 18 |
| Electromagnetic Compatibility | 18 |

1 Scope

This document describes the requirements of a system that will control access to one or more rooms, areas, floors, buildings or sites.

1.1 Terminology

| | |
|--------------------|---|
| Card | Any token used to uniquely identify the person to whom it is issued. |
| ACU | Access Control Unit – the electronic hardware that is connected to the physical hardware installed at a door. |
| PIN | Personal Identification Number. |
| Workstation | A Personal computer connected to the system. |
| Door | Any kind of barrier fitted with an electric release mechanism to prevent free access; including turnstiles, sliding gates and vehicle-barriers. |

2 System Overview

The system shall comprise the following components:

| | |
|------------------------|--|
| Programming | The setting up of people, cards and access rights will be capable of being performed from a single workstation regardless of the number of doors in the system. It shall also be possible for this to be performed from several workstations simultaneously. It shall also be possible to program individual ACUs by using a local programmer, either for commissioning and diagnostics purposes or for re-programming the ACU in the event of failure of some other part of the system (e.g. PC-to-ACU communications). |
| Identification | This shall be achieved by providing each person with a uniquely numbered card. At the time of presenting the card to a reader, additional confirmation may be required showing that the correct person is in possession of the card. This confirmation may be in the form of a PIN or biometric template. |
| Decision making | <p>The decision to open a door upon presentation of a card at a reader shall be taken by the ACU to which the reader is connected. No communication with a central database will be required.</p> <p>The decision to raise an alarm on the occurrence of a specified event will also be taken by the ACU, except in cases where for logistical reasons an event on one ACU is required to trigger a relay on another ACU.</p> |
| Reporting | Reports will be available both on demand and automatically. On-demand reports will include personnel location, event data and system configuration data. A separate report for input-to-relay mapping will be available. Automatic reports will be restricted to specifically selected events, and as such are alarms intended for immediate notification. |

3 Component specifications

3.1 Door hardware

Apart from the reader, which is specified separately in the next section, the following items of hardware may be required at each door:

| | |
|-----------------|---|
| Lock | <p>Access through a door, turnstile, barrier etc. will be granted by either applying or removing power to an electric release mechanism. This will be controlled by the ACU and require no additional switching circuitry unless the power requirements for the mechanism exceed the specification of the ACU. On doors where emergency exit is required, only power-locked devices will be installed and these will be wired in series with an emergency release mechanism such as a break-glass unit or a fire-panel relay. The access control system will play no part in allowing emergency exit.</p> <p>The type of electric lock mechanism will depend entirely on the type of door and so is not specified in this document.</p> |
| Door sensor | <p>A door sensor will be fitted so as to monitor whether the door is open or closed.</p> |
| Egress button | <p>On doors where “door forced” monitoring is required, and where there is no need to monitor who is exiting a secure area, an egress button will be fitted to the secure side of the door, so as to signal to the ACU that someone wishes to exit. Pressing the button will cause the ACU to release the lock at which point the door can be opened.</p> <p>If “door forced” monitoring is required, and a door handle or crash-bar is specified instead of an egress button, then this shall incorporate a sensor which will be monitored by the ACU so that if the handle is turned before the door is opened then no alarm is reported.</p> |
| Break-glass | <p>On doors where there is a need to unlock the door to allow exit in an emergency, a break-glass device shall be installed on the insecure side of the door which cuts power to the release mechanism.</p> |
| Door ajar alarm | <p>Where required, a sounder will be installed close to a door to indicate when a door has been left open too long – typically after 15 seconds. If the door remains open for a significant length of time – typically several minutes – this will be notified as an alarm.</p> |

3.2 Cards and Readers

Each door shall be fitted with a reader of one of the following technologies:

- Infra-red
- Proximity
- Mag-stripe

- Mifare (serial-number reader)
- Mifare (sector reader)
- Biometric with Mifare

Cards will be available that are suitable for direct printing using dye-sublimation printers. Cards will be available with more than one machine-readable technology for compatibility with other systems that are, or may be, installed. Cards will not be manufactured with site codes and will (with the exception of mag-stripe cards) have an un-alterable identity fixed at the point of manufacture. With the exception of mag-stripe cards, cards will be available that are suitable for carrying on a key-ring.

Readers will be available that are suitable for installation outdoors; i.e. weatherproof and with a temperature range of -20°C to +50°C. All readers will be available with an optional keypad.

Readers will be available with one Bi-colour LED or two differently coloured LEDs, so as to provide clearly different signals for access granted and access denied. Proximity readers will have a sounder to signal when a card has been read.

Readers will be available with message displays. When a card is used, the display will show “access granted” or, if access is denied, the reason of denial.

The properties of each reading technology are specified as follows:

3.2.1 Infra-red

Where fitted, infra-red readers shall be capable of reading TDSi Microcard cards.

3.2.2 Proximity

Where fitted, proximity readers will read passive cards (i.e. cards with no battery). Mullion-mount readers will be available. Readers with different read-ranges up to 50cm will be available.

A vandal-resistant proximity reader of a mullion design (i.e. no wider than 40mm) and made of stainless steel (grade 316 or better) will be available.

3.2.3 Mag-stripe

Where fitted, mag-stripe readers will read high coercivity Track2 ABA encoded cards and utilise the last 8 digits preceding the first field separator or end sentinel.

Where required, it shall be possible to change which digits are read from the card.

3.2.4 Mifare (serial-number reader)

Where fitted, Mifare serial-number readers will read the serial number of any Mifare card and utilise at least the last 8 digits.

3.2.5 Mifare (sector reader)

Where fitted, Mifare sector readers will read 8 digits encrypted to the unique TDSi algorithm and stored in sector 9 of the Mifare card.

3.2.6 Biometric with Mifare

Where fitted, Biometric readers shall read a fingerprint and compare it with a template stored on a Mifare card. If the live finger matches the template, the unique card number will be sent to the ACU, which shall then decide whether to open the door. The readers shall be capable of being used for enrolment (i.e. encoding the template onto the card) as well as for identification. There shall be no need for linking biometric readers together. No keypad is required on these readers. It shall be possible to specify in advance which sectors in the Mifare card are designated for use with the biometric reader. It shall be possible to use Mifare cards already in circulation

provided that enough sectors are available and either the sectors are unlocked or the unlock codes are known. For newly supplied cards, unused sectors of the card shall be unlocked.

3.3 Cabling

All cabling shall utilise readily available shielded multi-core cable.

3.4 ACUs

3.4.1 General description

Readers and door hardware shall be connected to ACUs, which shall be autonomous devices that have sufficient processing power and memory to perform the following tasks without referring back to a central system controller:

- Accept programming commands from software or programming keypad
- Identify the person requesting access
- Make the decision whether or not to allow access
- Report activity, immediately or on demand

Each controller will be capable of controlling a door requiring both “in” and “out” readers, or two doors with one “in” reader at each door.

Where required, based on either cost considerations or for functionality, an ACU may control up to 7 “slave” ACUs. In such circumstances, the slaves will continue to allow access in the event of failure of master-slave communications but with a reduced level of security.

ACUs will also be capable of monitoring additional input devices and switching additional output devices.

ACU’s will be fitted with watchdog circuitry such that “processor lock-up” cannot occur.

3.4.2 Features provided

Anti pass-back

The ACU shall be capable of enforcing anti-passback on either a timed basis, or on a true (‘global’) basis, across at least 16 doors. A “forgiveness” feature will allow a “reset” to be carried out automatically every day.

Block-validate cards

In stand-alone operation, this feature will allow the block validation of a range of cards, all with the same time group and expiry limit, from a start number to an end number.

Block-void cards

This feature will void a range of cards.

Card+PIN

This feature is required to provide confirmation that the card is being presented by the rightful owner. The first time a card is presented, if this feature is turned on then the owner may type in any 4-digit PIN and this will be stored in the ACU. From that point on, when this feature is turned on access will only be granted if this PIN or the duress

PIN is entered. The duress PIN shall be a variation of the valid PIN that will still allow access but that will signal an alarm.

This feature will be capable of being turned on and off either on demand or automatically.

Clock and calendar

The ACU will maintain an accurate clock (+/- 1 seconds per month) and calendar.

Communication

PC-to-ACU communication will be possible via a number of interfaces, to allow for the most cost effective and reliable installation to be designed and implemented. Possible methods of communication will include RS232, RS485, TCP/IP and dial-up modems. Other methods of communication such as fibre-optic, wireless LAN etc will be supported provided that they introduce no changes to the protocols or timings of communications.

ACU master-to-slave communications will be by 2-wire RS485.

All communications links will have LED monitoring.

Configuration

Each ACU (including slaves) will be capable of operating in one of the following configurations:

- 1-door 2-reader
- 2-doors, 1-reader each
- Elevator controller

Control Card

It shall be possible to program one or more cards to turn on and off a relay.

Counters

A feature will be provided where the number of people entering and leaving an area can be counted, and where a relay can be triggered when a pre-defined level is reached. The relay shall be de-energised when the number of people drops below a certain level, which may not be the same level that caused the relay to be energised in the first place. In addition relay triggers, events shall be generated which shall be stored in the event database and may be treated as alarm events (see elsewhere in this specification for the significance of alarm events).

This feature shall also be capable for monitoring inputs in such a way that one or more inputs may increment a single counter, and other inputs may decrement the same counter.

Diagnostics

A built-in diagnostics feature will permit testing of various parts of the hardware.

Door ajar local time

It shall be possible to specify a maximum door-open time, after which a “door ajar (local alarm)” event will be generated.

Door ajar remote time

It shall be possible to specify a maximum door-open time, after which a “door ajar (remote alarm)” event will be generated.

Door sensor type

It shall be possible to use two types of door sensor:

- Door open = contacts open
- Door open = contacts closed

Elevator Control

An elevator control feature will be provided, whereby the presentation of a card at a reader will result in a combination of relays being energised. These relays will be used to either enable elevator-car buttons, or to signal to the elevator system which floors the elevator may be despatched. It will be possible to drive any combination of up to 36 relays in this mode of operation.

Holidays

It shall be possible to define holiday dates that may then be used to modify the operation of any weekly schedules.

Inputs

Each ACU shall provide at least 4 supervised inputs other than the ones used for door sense and egress. There shall be a choice of the type of supervision - either one-resistor (open circuit detection only) or two-resistor (open- and short-circuit detection). It shall be possible to expand this capability to 34 inputs. It shall be possible to trigger a relay and/or generate an event message as a result of a change of state at an input. It shall be possible to have more than one input trigger a single relay, and more than one relay triggered by a single input. It shall be possible to ignore changes of state lasting less than a defined period.

Language

When used stand-alone, it shall be possible to choose the language used for on-screen prompts, and messages printed at the printer.

Lock time

It shall be possible to define the maximum length of time the lock release relay will be energised for. The door must re-lock before this time has expired if the door opens and closes within that time.

Mantrap

It shall be possible to set up a mantrap configuration, which prevents one door opening unless another one is shut.

Memory options

It shall be possible to choose how much memory is used for Cards, Events and Time Control Lines (TCLs).

Messages

It shall be possible to disable unwanted event messages to minimise communications bandwidth and database storage. In stand-alone mode this feature will prevent excessive use of paper on a logging printer.

Password

When programming an ACU directly using the programmer, a password shall be required. It will be possible to define more than one level of access to the menu system, each with its own password.

PIN-only

It shall be possible to allow access using PIN-only entries with no need to present a card.

Printouts

In stand-alone mode, it shall be possible to send configuration data to a printer.

Reader type

ACUs will be capable of utilising a choice of reader technologies. It shall be possible to utilise more than one reader technology on a single ACU.

Relays

Each ACU shall provide at least two “spare” relays other than the ones required for controlling lock release mechanisms. It shall be possible to expand this capability to 34 relays. It shall be possible to trigger a relay from an input, event or schedule.

Time groups

It shall be possible to define at least 64 time schedules that may be used in up to 255 combinations to define times of permitted access.

Validate card

In stand-alone mode, it shall be possible to validate an individual card, or PIN-only number, together with its time group and validity dates.

Validate PIN-only

Same as VALIDATE CARD, but the user is not prompted for a pin.

Void card

If the card is in memory, you will be shown which door/s the card is valid in first by the "1" to "0", you will be required to change to "1" to "0" to remove card from memory.

Start up Programming

Each ACU shall provide quick-test feature whereby, immediately after installation, the card and reader technology are automatically detected the first time a card is used, and the lock strike relays are triggered on subsequent card usage provided no cards are in memory. This is needed to:

- Prevent the need for programming the ACU before tests can be carried out

- Prevent the need to unlock the door until the necessary cards are programmed into the ACU

3.5 Software

3.5.1 General description

The software provided as part of the system shall be capable of being utilised on one or more workstations simultaneously.

The software shall be suitable for use on Windows 98, ME, NT4, 2000 and XP.

The primary functions of the software shall be to:

- Permit setting up of ACUs.
- Permit programming of people, cards and access rights
- Provide on-demand reporting of events and system data
- Provide automatic notification of selected “alarm” events

In addition, the software shall permit Photo-id badge creation.

3.5.2 Database

There shall be a single database, of a suitably secure and reliable technology. It shall be possible to implement the database and all necessary client software on a single computer (subject to performance and capacity considerations).

Automated database back-up tools shall be provided that can back up the database each day to a different computer. The ability to limit the maximum size of the database, by limiting event storage, shall be provided.

Where multiple workstations are required, they shall connect to the database server utilising TCP/IP over LAN or WAN. Each workstation shall be capable of running ACU communications client software as well as user-interface client software.

3.5.3 Communications

It shall be possible to use multiple PCs as communication servers, such that the PC - although polling ACUs continuously - creates minimal TCP/IP traffic by communicating with the database only when there are events reported by the ACU or commands to send to the ACU.

3.5.4 User-interface

The user interface shall be primarily graphical and shall comply with the Microsoft Windows 95/98/NT/2000/XP design principles.

Object states will be reported graphically and include:

- Door open
- Door ajar
- Input on
- Relay on
- Object suspended
- Object off-line
- Object state unknown

An on-line help system shall be provided.

3.5.5 Equipment set-up

The software shall permit full setting up of all parameters relating to ACUs. These parameters shall be downloaded to the ACUs to allow the ACUs to function autonomously.

Unless specified otherwise, all of the features listed in the ACU specification in this document shall be capable of being implemented via the software.

3.5.6 Card-holder details

It shall be possible to capture a picture from a live video input or from a file and store the image against a cardholder's record.

It shall be possible to define up to 16 additional fields for storing cardholder details. Each field must be definable as free-text, date format or pick-list. It must be possible to search for a cardholder based on information in any of these fields.

It shall be possible to import and export cardholder details in text-file format.

It shall be possible to assign more than one card to each cardholder.

For each card assigned to a cardholder, it shall be possible to define start and end dates for the validity of the card.

3.5.7 Access rights

The software shall utilise the concept of Groups rather than requiring cardholder access rights to be specified individually.

The software shall utilise the concept of Areas rather than requiring Group access rights to be defined door-by-door.

3.5.8 Reporting

Any report that can be generated by the software shall be capable of being viewed on screen, sent to a printer or saved to a file in a variety of formats including but not restricted to RTF, CSV, HTML and PDF formats.

3.5.8.1 Configuration and other database reporting

The following reports are required:

- A single report showing all ACUs, doors, readers, inputs and relays.
- A single report showing all cardholders and their details (including last known location)
- A list of all the Groups that a Cardholder is a member of
- A list of all the Areas that a Cardholder may enter
- A list of all the cardholders currently in a chosen area
- A list of all the Groups that may enter a chosen area

3.5.8.2 Roll-call reporting

It shall be possible to produce a list of all cardholders whose last known location was on-site, together with the location, time of entry. It shall be possible to produce this as a printed report, paginated so that it is suitable for handing out to several people for a roll call. The criteria for deciding where the page breaks occur will be selectable; for example the area, or department, or muster point.

3.5.8.3 Attendance Reporting

The system shall be capable of producing totals of the length of time spent by each cardholder in each area, with subtotals for the period covered by the report.

3.5.8.4 Real-time event reporting

It shall be possible to display events in real-time. It shall be possible for an operator to choose whether to show:

- all events
- a selection of events based on object type
- events for a single object

It shall be possible to save real-time events lists to file.

3.5.8.5 On-demand event reporting

It shall be possible to define event report templates that can be saved and re-used. These templates shall include selection and sorting criteria.

3.5.8.6 Alarm reporting

The process of alarm management shall use the concept of alarm zones, so that a single operation (manual or automatic) to arm the zone results in all objects in that zone being armed.

It shall be possible to selectively define which objects, and which events for those objects, can generate alarms. It shall also be possible to define schedules that determine whether an event is an alarm or not, based on the time of day. Each alarm must be capable of having a priority level (from a range of 1-12) associated with it, and a set of instructions for the operator.

When an alarm occurs it shall cause an immediate visual and audible signal to the operator. It shall be possible to associate a sound file with an alarm, and to cause a relay to be triggered anywhere in the system. A further consequence of an alarm shall be that it can trigger a CCTV system to trigger a camera and its PTZ preset co-ordinates.

When an alarm has been notified, the operator shall be able to locate the object that raised the alarm on a site plan with a single operation. Where multiple alarms have been notified but not yet dealt with, the operator will be able to choose to deal with either the highest priority, or the most recent.

The system shall require the operator to action each step of the instructions associated with the alarm before the alarm is removed from the alarm list. It shall be possible to produce a report at a later date showing who performed each step, and when.

It shall be possible to suspend an object, to prevent it generating alarms until the suspension is removed. It shall be possible for an operator to set an alarm event as “acknowledged” so as to signal to other operators that the incident is being dealt with.

It shall be possible to see in a single display whether there are any alarms that have not been acknowledged or cleared.

3.5.9 CCTV interface

Where required, it shall be possible to connect a CCTV controller to the system using a serial command interface. This will permit both automated and manual control of the CCTV controller, for the purposes of selecting cameras and triggering PTZ presets.

3.5.10 System Operators

It shall be possible to define at least multiple operators with rights to use the system. The operator log-in name must not be the same as that person's name within the cardholder database. There shall be at least 20 different levels of authorisation, based on what objects an operator may deal with and whether they may add/modify/delete such objects or simply see their details.

3.5.11 Multiple tenants

It shall be possible to configure the system for multiple-tenancy buildings such that:

- Each tenant has at least one workstation
- Each tenant can administer their own cardholders, groups, areas and access rights
- Each tenant can administer access rights for their cardholders for shared common areas such as car parks and reception areas
- No tenant (other than the landlord) can administer the cardholders, groups, areas and access rights of any other tenant

3.5.12 Photo-ID

It shall be possible to design and create photo-id badges as part of the main system software.

It shall be possible to capture the cardholder photograph from either a live image, or a stored JPEG image from a digital camera without requiring any re-formatting.

For capturing live video, a high-quality camera shall be supplied together with any associated hardware required for transferring the image to the computer.

Photographs shall be visible when browsing cardholder information.

A badge design should be capable of being used for multiple cardholders without requiring modification in between printing successive cardholder badges. There should be capacity for at least 200 badge designs.

The ability to utilise the photograph during "objective authentication" will be provided, so that the picture of a user who has been denied access can be quickly retrieved, and the operator can then release the door from the software console without the need to access another part of the system.

3.5.13 Site Plans

It shall be possible to create graphical representations of site layout. Background images may be produced outside the software in JPEG format and imported.

It shall be possible to create multiple site plans, linked together so that the operator can easily jump from one plan to another – which may represent an adjacent plan, a zoomed-in view or a zoomed-out view.

It shall be possible to place objects on the plan, such as Areas, ACUs, Doors, Readers, Inputs, Relays, and Cameras. Objects on the plan must provide information and permit control directly from the plan, without the need to leave the plan.

4 System Parameters

4.1 Technical specification of ACUs

| | |
|----------------------------|---|
| Power | 220-240V input; isolated output 12V @ 2A for locks. Separate battery backup for ACU and locks. Mains-fail monitoring (reported by relay and by software) |
| Construction | Metal cased |
| Installation issues | Unpluggable rising clamp connectors. Quick grounding connectors. |

4.2 Maximum capacities of ACUs

| | |
|----------------|--|
| Readers | 2 per controller; 16 per sub-system |
| Cards | 15000 minimum; 45000 potential |
| Inputs | 4 spare supervised inputs per controller; expandable to 36 |
| Relays | 2 spare supervised relays per controller; expandable to 34 |

4.3 Maximum capacities of System

| | |
|---|---------|
| Workstations | 10 |
| ACUs | 400 |
| Doors | 1600 |
| Areas | 1600 |
| Groups (24-hour access) | 6000 |
| Groups (each with a unique time-restricted access pattern) | 128 |
| Cards (system) | 256,000 |
| Cards (at any one door) | 48,000 |
| Cardholders | 128,000 |
| Operators | 128 |
| Site Plans | 128 |
| Badge Designs | 128 |

5 Installation, commissioning and training

The system shall be programmed with the information supplied. The system must be fully working with all system parameters and card holder's information. It is the tenderer's responsibility to ensure that all the necessary information is obtained before commissioning the system.

At least two and up to four members of staff will be nominated as operators of the system. These operators must receive sufficient training on the operation and configuration of the system to enable these operators to train others. The training shall be conducted by the manufacturer's own training staff or by other certified training staff.

A copy of the final database of access control software shall be included at the final hand over of the system.

The tenderer shall supply detailed "as installed" drawings of the entire system.

Self-training materials shall be available for the software user interface.

6 Warranties and standards

The access control equipment, including door controllers, readers and software shall be warranted by the manufacturer against failure for at least three years. The access control cards shall also carry a warranty against failure.

It is accepted that the security system will require preventative maintenance.

6.1 Standards

The access control system / supplier shall comply with the following standards and regulations;

ISO9000/2

NACOSS or BSIA where applicable

6.2 Electromagnetic Compatibility

The access control system shall comply with the CE mark regulations regarding electromagnetic compatibility within the system and with other systems installed within the same locations.