
CUBE
CCTV
TM

DESIGNING AND INSTALLING ACCESS CONTROL SOLUTIONS

A practical guide for professionals

Installer

You want to offer your customers simple access control solutions, suitable for their professional or private requirements. You want to support your proposals with examples connected with their areas of business or similar uses, and you also want to have technical and practical information for carrying out the installation.

Why access control?

A site: a piece of land, enclosed area, etc.

A building: businesses, offices, warehouses or storage areas, public buildings (hospitals, hotels, courts, schools, museums, exhibition halls, conference centres or cinemas/theatres, etc.).

A closed room or area: entrance hall, car park, office, stockroom, double-entrance security doors, equipment room, computer room or clean room, laboratory, cellar, etc.

A tool: workstation, cabinet, computer, computer rack, etc.

To be appropriate for each situation, the access control system must answer 5 questions.

1. Where? For what place? What type of access (isolated, internal or external, room, building, floor, etc.), for how many doors?
2. Why? For what function, for whom? Management of visitors, groups, staff and events.
3. When? At what time? At what times is access permitted or refused? And for how long?
4. How many? How many people are concerned? How many sections or departments? How many people are there in the groups? Which visitors are authorised, and which are not?
5. How? Which readers to choose? What wiring infrastructure to use?

The basic components of an access control system

Readers:

1. Fingerprint reader
2. Badge reader
3. Coded keypad
4. The three main current technologies are used on their own or in combination.

What are the factors to consider in an access control system installation project?

Simplicity

You have a single offer comprising both standalone and centralised solutions.
The door controller uses the IP network infrastructure (Legrand Cabling System LCS2).
The supervision software is user-friendly and very easy to use.
The Legrand access control offer is easy to install and use.

Adaptability

The system you install can be adapted without changing the readers.
The centralised readers you have installed will be able to take other controllers on the market.
With Legrand solutions you can propose open, durable systems.

Standalone access control solutions

Standalone access control solutions are designed to manage and ensure the security of the flows of people in simple or small areas (meeting room, individual office, equipment room). The implementation of standalone solutions is also suitable for larger sized buildings for which no management of events or supervision is required (eg: hotels).

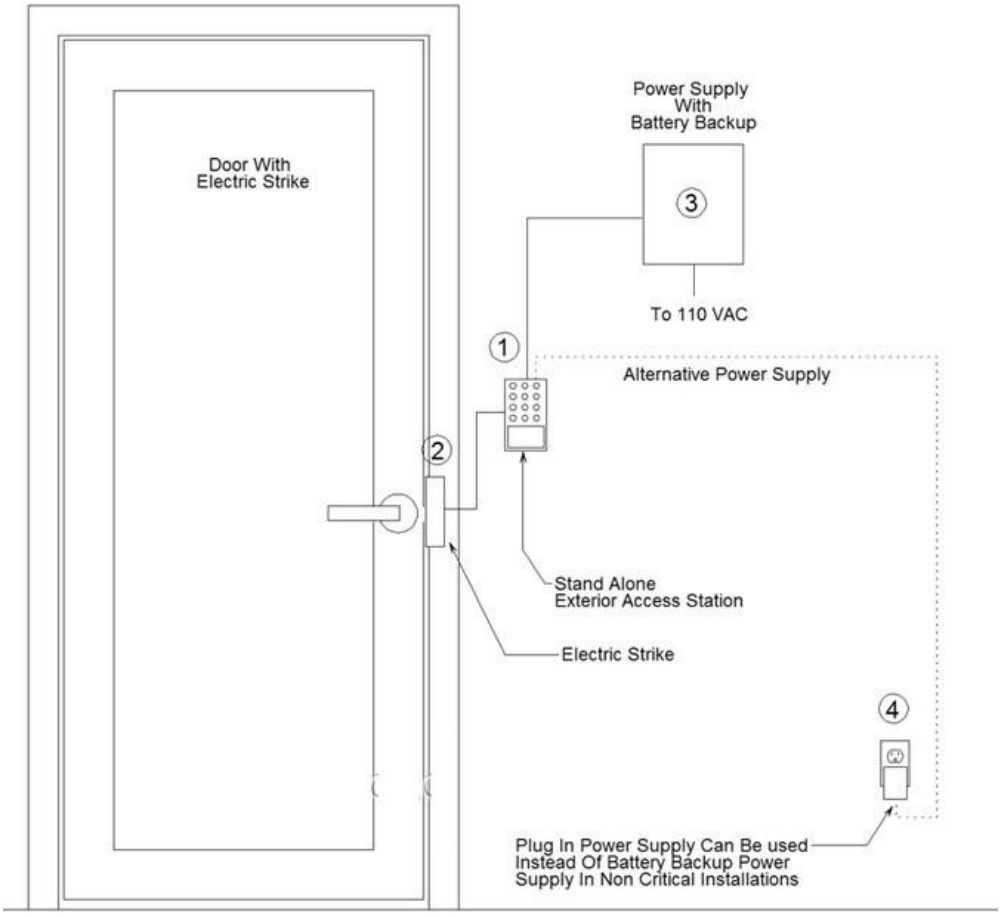


Figure 1.3 Standalone access control system with a keypad.

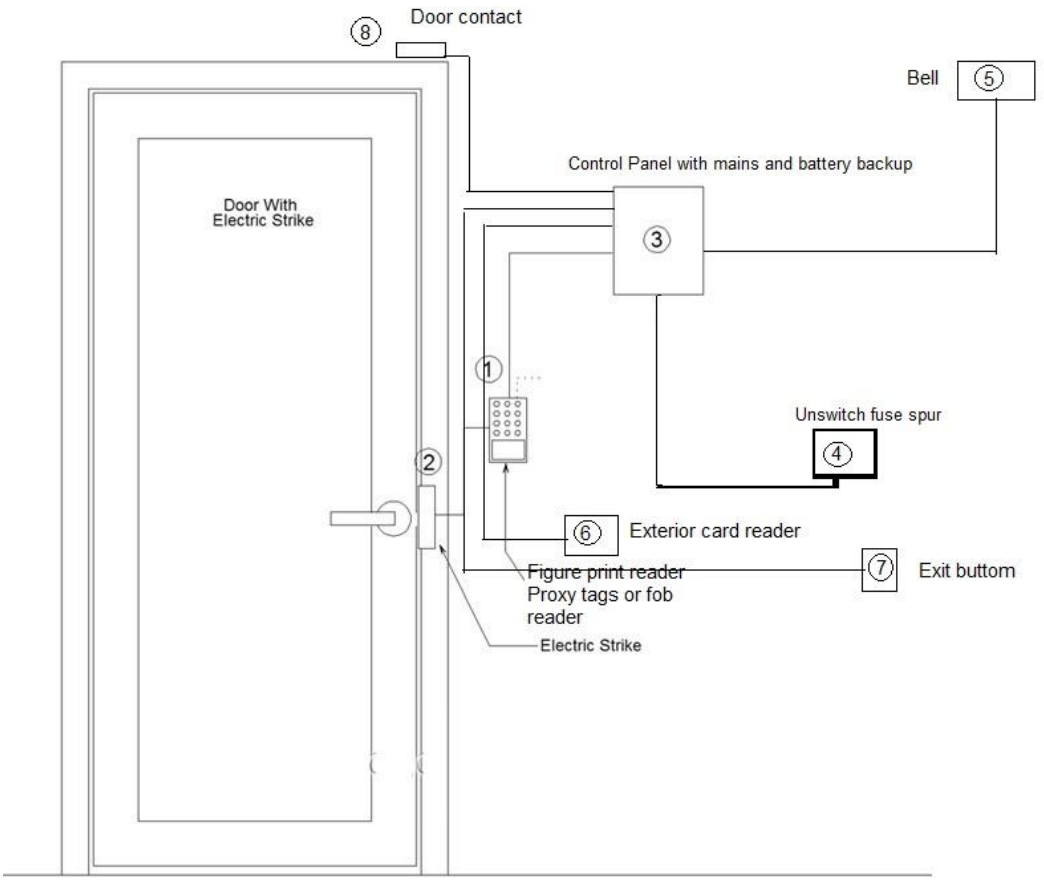


Figure 1.4 Standalone system to control one door.

Locations concerned

- Isolated entrance door
- Storeroom
- Computer room
- Meeting room
- Access to hotel rooms

Advantages:

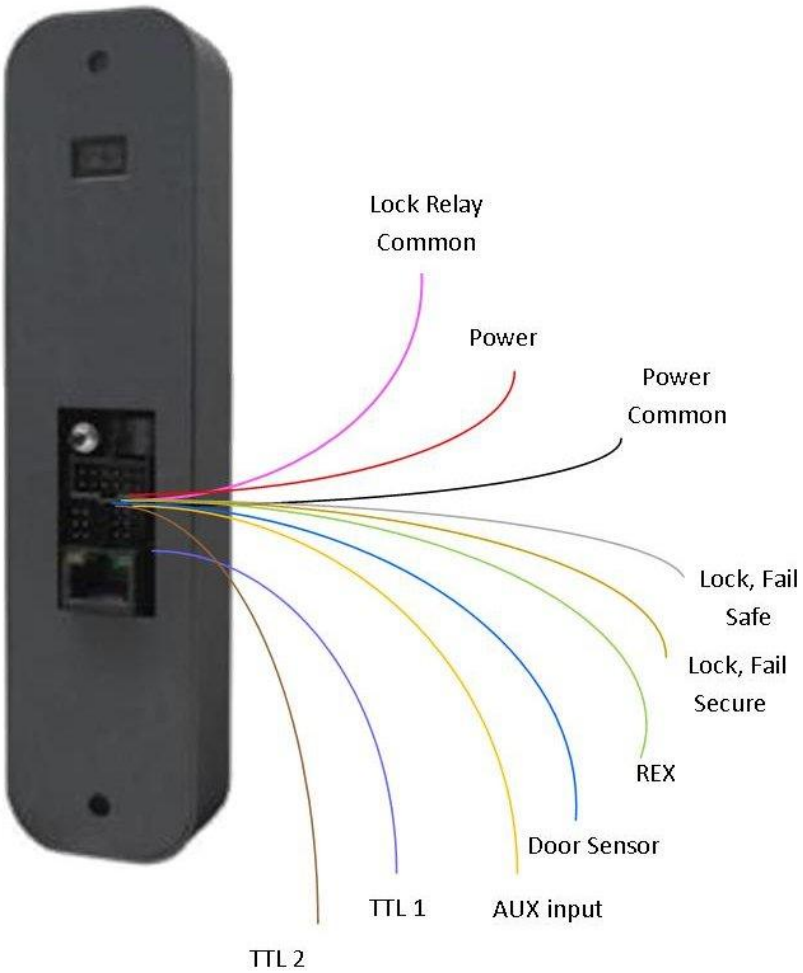
- Easy to install
- Optimised wiring
- Very simple programming

Operation & installation

How does it work?

A reader is defined as being standalone when it manages the information incorporated inside (stored code for example or fingerprint) and/or configured in a badge:

- IDs (code, badge or fingerprint) are read directly on the reader.
- The ID memory is integrated in the reader.
- The door is controlled directly from the reader



How is the device installed?

- The power supply is connected directly to the reader
- This reader is itself connected to the closing system (door release, electromagnetic lock, bolt, etc.) and to the pushbutton that is located inside the protected area (to enable the user, who has been allowed to enter, to leave)

How to select the right reader?

Below are some of the factors to be considered in buying a reader.

1. Indoor or Outdoor - Surface mounting or Flush mounting.
2. User capacity.
3. Door station buzzer and LED's.
4. Power consumption.
5. No. of relays.
6. Operation e.g. Length of the security code 4 digits, 6 digits or 8 digits.

What are the disadvantages of a standalone access control system?

1. Not suitable for a large application.
2. Difficult to design a bespoke solution. For example, defining the relationship between the doors and the times when a user has access through them will be difficult.
3. Lack of security.
4. Difficult to maintain.
5. It is difficult to expand it.

What are the advantages of a standalone access control system?

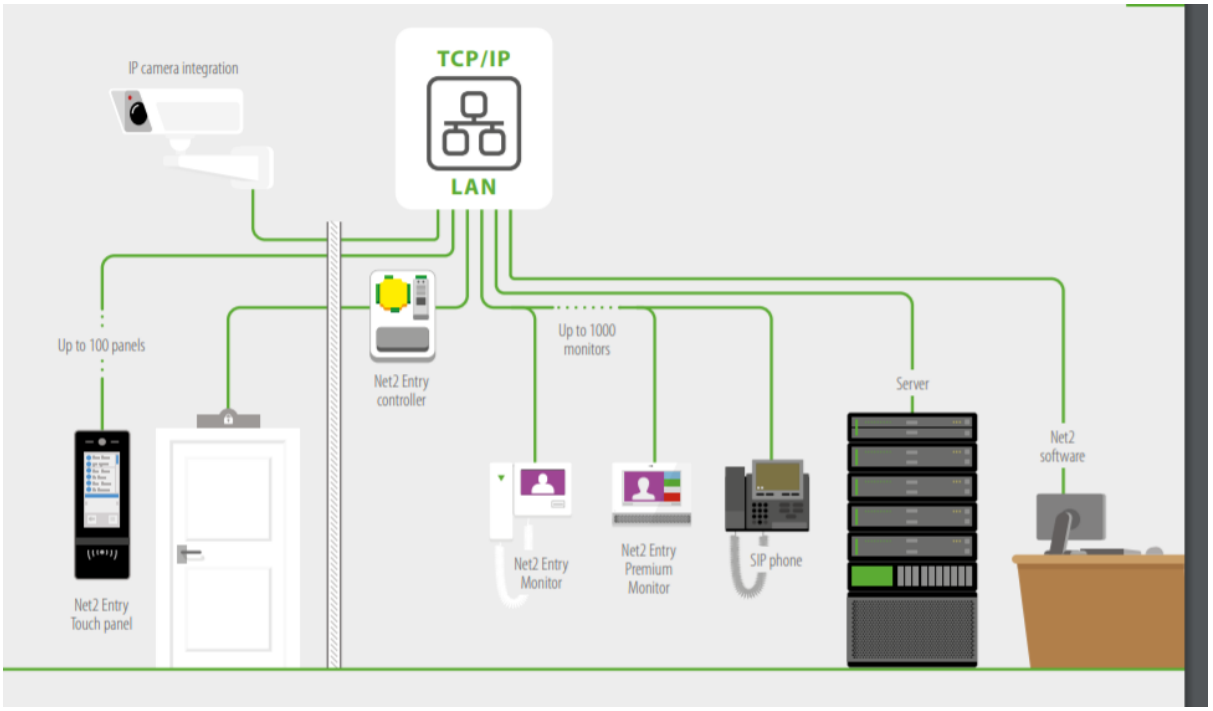
1. Easy installation.
2. Cost effective solution for a small application.
3. Easy to troubleshoot.

Centralised Access Control System

Centralised access control solutions are designed for organisations or companies which need to manage office buildings or healthcare or educational establishments from one or more control stations. This range meets the requirements for management of the flows of people both internally and externally.

Advantages

- The ability to supervise events on drawings and obtain an overview of all the flows in real time
- The wide variety of scenarios available (eg: creation of automatic control devices)
- Access to interoperability with other systems such as video surveillance



How does a centralised access control system works?

The CAC (centralised control access system) permits complex installations with several accesses and additional functions. It also makes it possible to integrate other services.

It allows for complete management of an installation with several doors and advanced access control functions: restrictions by user groups, both in terms of space (zones) and time (timetables), anti-return function, restriction of maximum capacity, greater user capacity, activation of devices from the reader, recording of incidents for subsequent consultation, control or security centre…

This also permits the integration of additional services into the access control: intercommunication, alarms, automation, etc.

- **INTERCOMMUNICATION.** For those entrances where it is necessary to permit access by external personnel. A button is pressed in order to contact the guard unit, and from there access is granted.

- **TECHNICAL OR INTRUSION ALARMS.** Each entrance and exit can be programmed with a detection and intervention time. The alarms can be viewed on the computer screen and in the guard unit.

- **AUTOMATION:** Relays can be activated in response to specific events. Activation of devices from the readers (activation/deactivation of alarms on entry or exit). Weekly programmer that can plan up to 32 daily activations of relays and activation of individual sensors or groups of sensors. Permits automatic connection of lighting, engines, heating, air-conditioning, sprinkler systems, etc.

A Central Unit is required for managing the system along with specific software (in a very intuitive Windows environment), for programming the installation via a PC.

The connection between the PC and the installation can be direct (RS-485) or remote (IP). The data can be updated and the installation monitored from different PCs (multi-station).

What are the basic components of a centralised access control system?

1. Door station:
    a. Video
    b. Audio
2. Panel
3. Power supply
4. Battery
5. Readers
    a. Indoor
    b. Outdoor
6. Servers
7. Locks
8. Bell
9. Exit button
10. Emergency exit
11. Door contacts

12. Software
13. Credentials

CLASSIFICATION OF ACCESS POINTS

General

Access points are classified by the requirements for successful legitimate access (see Class I, Class II, Class III and Class IV below). Classification is related to the level of security provided for each access point and the class can change according to the time of day or night.

For each class, access may be granted by the use of credentials permitted at higher classes, but not by the use of credentials permitted at lower classes.

You must determine the classification of each access point during the design stage.

You must include the location and classification of each of the access points making up an access control system in the system design proposal and in the asfitted document.

In all classes, data encoded within tokens must be protected against unauthorised change (for example by requiring an authorised person/manager to enter a password to gain access to software at the central processor to make changes).

In all classes, codes must be protected from repeated attempts to select the correct code (for example by limiting the number of attempts to a maximum).

Facilities to control readers from a central point, to record information regarding the access of individual token holders and to monitor the status of access points where this is required may be incorporated into any access control system.

Monitoring, 'access point held open' alarm, cable security and standby power operation are related to the level of security provided within a classification.

Class I (low risk)

At an access point to class I, access will only be granted following:

• The input of a correct common code (or the input of a correct PIN code) of not less than 10,000 differs.

10,000 differs requires a 4 digit code number such as 1234.

Class II (low to medium risk)

At an access point to class II, access will only be granted following:

• Option A - the input of a correct PIN code of not less than 1,000,000 differs;

OR

• Option B - the presentation of a valid unique token to a reader. 1,000,000 differs requires a 6 digit code number such as 123456.

Class III (medium to high risk)

At an access point to class III, access will only be granted following:

• Option A - the input of a correct PIN code of not less than 10,000 differs AND the presentation of a valid unique token to a reader;

OR

• Option B - the presentation of a valid biometric to a reader.

Class IV (high risk)

At an access point to class IV, access will only be granted following:

• Option A - the presentation of a valid biometric to a reader AND the presentation of a valid unique token using radio frequency identification (RFID)*;

OR

• Option B - the presentation of a valid biometric to a reader AND the presentation of a valid unique token to a reader AND the presentation of a correct PIN code of not less than 10,000 differs.

*** RFID must not rely on recognising the Chip Serial Number (CSN) only. Also the code to be read must be stored in the memory of the card. ***

Access control system design

Survey

The importance of a correct and adequate survey for installation is paramount.

You must ensure that all personnel visiting the facilities are protected by BS7858 and possess an identity card, which must include a photo of the owner, his signature, the name of his business and a date of registration. 'Expiry.

In this case, you should contact the responsible officials, eg. B. the person responsible for the information Technology and staff for the customer.

Access point design has a significant impact on the performance and reliability of access control system.

Access points must not:

- Conflict with fire regulations
- Restrict exit in such a way as to endanger people in an emergency

You should consider the following aspects when designing an access control System:

How do the access points work in the event of a mains power failure?
The period or number of transactions required under these circumstances;

whether access points should fail locked or fail unlocked;

Whether the secondary uncontrolled locks must be installed on exterior doors that can not be unlocked;

whether a key override is required for any critical doors to facilitate access in an emergency;
whether ACUs will retain data in the event of data bus or power failure until the central computer or processor is operational;

whether standby power is needed for the database (for example if held on a computer) to maintain its integrity during power failure;

the choice of access control technology to provide an appropriate level of security for the risk to be protected;

the choice of electronic equipment and its siting, taking into account environmental conditions and the potential for vandalism;

the selection of access point hardware, taking into account the volume of traffic, environmental conditions and the level of physical security required;

the numbers of users, access levels and time zones required, taking into account both present and predicted numbers of users and their needs;

whether certain equipment needs to be protected against malicious damage;

the need to site equipment such as controllers and printers in a secure area;

the number of access points required, taking into account peak periods of use;

whether an existing customer local area network (LAN) should be used;

ease of access to ACUs and power supplies for preventative and corrective maintenance.

Equipment selection and installation

Except where otherwise specified, you must select and install equipment to withstand the following air temperatures:
Internally sited equipment, 0 ºC to +40 ºC
Externally sited equipment, -20 ºC to +50 ºC

Wider temperature ranges may be specified for some commercial, industrial and/or military applications.

Equipment exposed to direct sunlight can exceed these temperatures and appropriate shielding may be required in such circumstances. When the temperature is not well maintained internally in premises, temperature may vary between -10 ºC to +40 ºC and you should consider using equipment suitable for external use or similar. In all cases equipment should be suitable for use in the environment in which it is installed.

You must use environmental housings according to BS EN 60529 so as to afford appropriate protection (for example to IP54 or IP65 as applicable) where the possibility of penetration by solid objects, dust or water exists.

Credentials
Credentials may be thought of in terms of something you know (code), something you have (token) or something you are (biometric).
The security, size and durability of a credential are dependent upon the technology used to encode it and the equipment required to read it.
Credential technology should be selected as appropriate to the risk being considered and the needs of the customer.
Several types of credential are available including:

1. memorized information such as common codes and PIN codes, which are input by hand to a keypad;
2. magnetic token, including Wiegand effect;

    Where magnetic tokens are powerful enough to corrupt other magnetically stored data in their immediate vicinity they should carry a printed warning to this effect. Limited life cards, for example cards carrying bank data, should not be

used as access control tokens without prior agreement to this by the issuing authority.

3. infra-red token;
4. hologram token;
5. proximity tokens using technologies such as radio or induction to allow the encoded data to be read within a specified operating range;
6. Biometric

Battery:
When selecting a battery powered active token you must take into account the life span of the battery and the environment in which the token will be required to operate and the frequency of its use.

Reader:
You must provide a reader or controller and/or its associated access point hardware or a central control with the following features:

an indication for access granted.
variable time available for access to be made.
tamper detection to detect access to the lock in circumstances where the lock can then be controlled from the insecure side.
response within 2 seconds of the valid completion of the necessary data entry associated with the credential.
(Note: Processing of more complex data such as those associated with biometric credentials may take longer than 2 seconds and this is acceptable provided the length of time is appropriate to the needs of the customer.)
re-locking of an access point if it is not used within a predetermined time.

You must mount readers:

- securely in position.
- adjacent to their access points and in positions convenient for all users to use, including those with disability.

(Note: We draw your attention to The Building Regulations 2000: Approved document M: access to and use of buildings.)

Cable type

Use	Max length	Type
RS485 data line	1000 yrds	2 x twisted pairs - Belden 8723 or Cat5 equivalent
Input/Output	100 yrds	2 conductor - Alpha 1172C (22AWG) or equivalent
Reader/Keypad	82 feet	8 core, shielded - Belden 9538, Alpha 1298C (22AWG) or equivalent
Reader/Keypad	328 feet	8 core shielded cable - Belden 9540/ Belden 5306FE (18 AWG) or equivalent

An RS485 data line has a 1000 yds maximum. This distance can be increased with the use of Paxton high speed repeaters or by using shorter independent data lines using multiple LAN connections controlled from the same PC.

End of line termination

120 ohm resistors must be linked across each data pair at the beginning AND end of the line. This can be done on many units with a switch or jumpers. If not, resistors are provided with the converter.

Reader & Data Cable Screens

- Data cable screens and spare cores MUST be connected throughout.
- Reader and keypad screens where provided, should be connected to the Black 0V terminal.

Electric Locks for fire doors

In the UK we need to keep fire exits clear at all times also they need to unlock at the push of a panic bar, ideally a single point of operation is required in which to operate the lock and get out.

Having a panic bar on the door may let people open the door and let anyone into the building which may compromise the security of the building.

Assuming you have this problem with your building what options are available to you that can keep the door secure but at the same time accessible in the event of an emergency.

Two electronic units are normally used to help with the problems above, one are magnetic locks and the other is solenoid bolts.

Magnetic locks can fit in the head of the door and keep the door closed with magnetic force. very simple and easy to fit and operate, can be connected to a fire alarm system so in the event of the alarm activating the magnet will fail-safe and the door can be opened via the standard procedures in the vent of an emergency.

Egress through a fire escape door

A person must be able to open a fire escape door in the event of a fire. This is normally accomplished with a handle that directly opens the lock. In buildings with a large number of occupants, such as theatres, the common practice is to use a crash bar to mechanically open the locking bolts.

There are no additional considerations when access control equipment is installed on a fire escape door with an overriding mechanical release. If a fire escape door has an electric lock, make sure there is a 'fail safe' method of opening it in the event of an emergency.

Mechanical locking is more susceptible to fire damage and potential failure than electronic locking.

The first step is to secure the door with a 'fail open' release. Because this type of device requires electricity to lock, it is unlocked when no electricity is available. Normally, magnetic locks fail to open. The next step is to have a 'fail safe' method of cutting the power to the lock to ensure that it releases in the event of an emergency.

Break Glass

Green and white break glass switches are commonly available. Red should not be used because it could be mistaken for the fire alarm system.

Doors will almost certainly be released by an interface with the fire alarm system in premises where large numbers of people may need to exit at once. (FIB stands for Fire Interface Board.) In most cases, a local override will be required at each door.

The access control systems and the fire alarm panel can be linked. When the Access Control System receives an alarm signal, it can send 'Open door' commands to specific doors. While this is often specified by building owners, it is not a "fail-safe" method of opening the doors because it depends on the access control system being fully operational. There will also be a need for a local release procedure.

The installer should be able to discuss these with the client and, if necessary, provide wiring details. However, it is the end user's responsibility, or that of their architect or other consultant, to define the fire escape routes and the standards of the local fire officer, as these may differ from authority to authority.

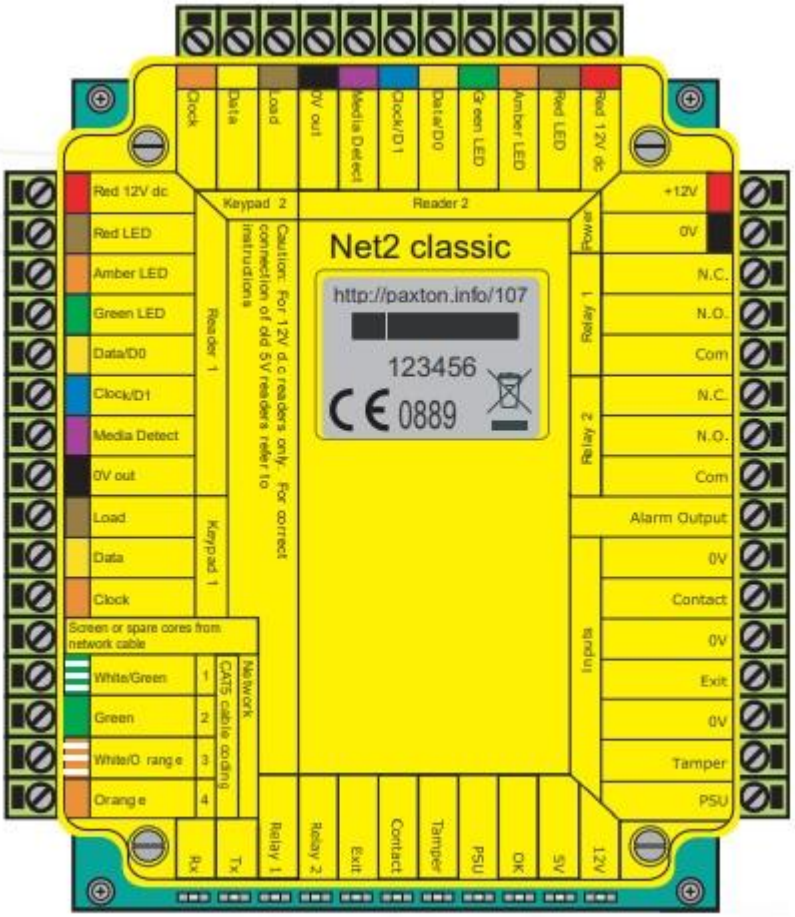
When doors are opened in response to a fire alarm, the access control system's security may be compromised. The door will remain unlocked if a break glass unit is used in an unauthorised way. When high security is required, locks, door contacts, or break glass units that are connected to a monitoring system should be considered.

Fail-open Locks

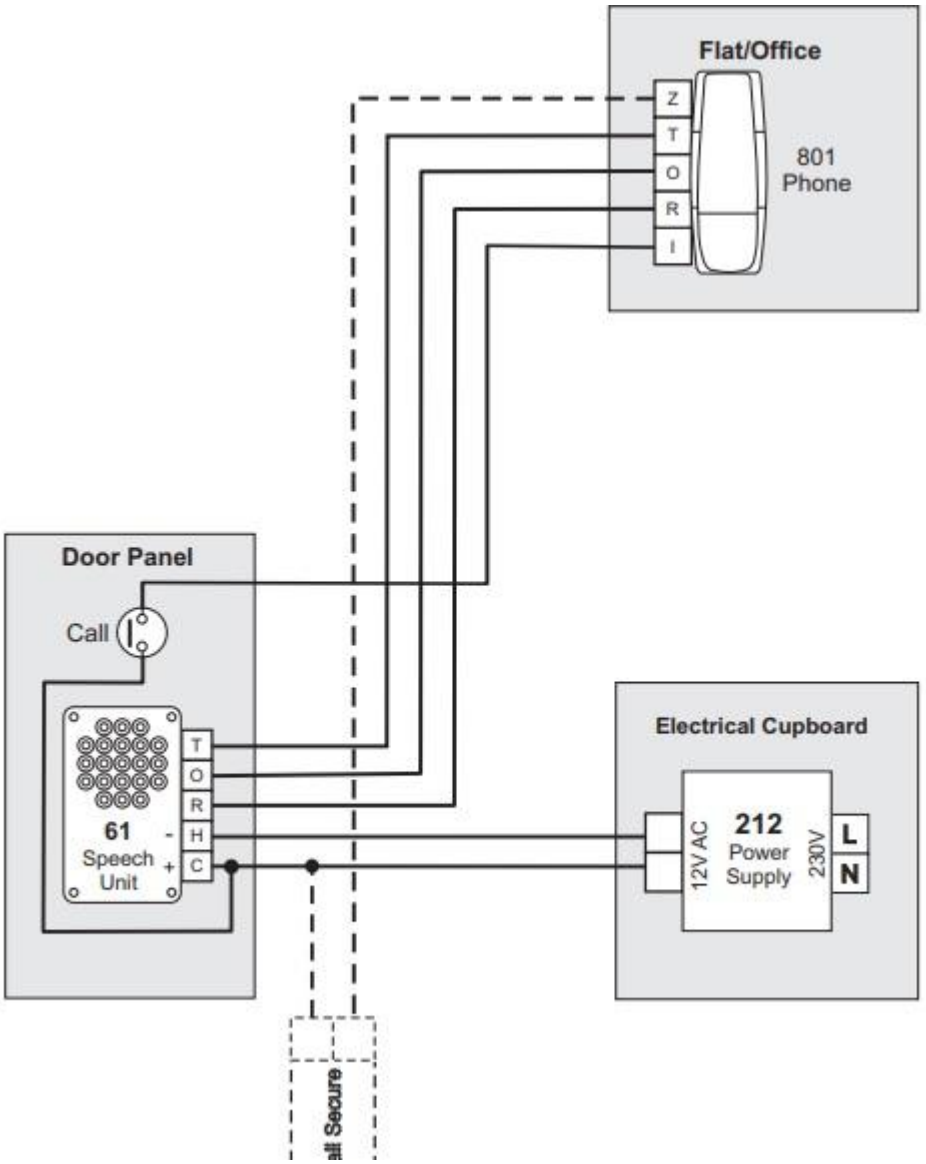
It is also critical that the locks on a fire exit do not jam when the door is unlocked due to side pressure. A panicked person operating the mechanical release or break-glass switch on a door may cause side pressure on the door. This is especially likely in an emergency where a large number of people arrive at the door in a matter of seconds.

In this situation, many electric motorised bolts, solenoid bolts, and some electric releases will jam. Models that have been designed, tested, and proved to open in these conditions are available. Obtain the manufacturer's information on this. Maglocks are intrinsically safe in this respect, though cheap models with residual magnetism in the armature may stick over time.

Appendix 1



Appendix 2


Flat/Office
Z
T
O
R
I
801
Phone
Door Panel
Call
T
O
R
H
C
61
Speech
Unit
-
+
Electrical Cupboard
12V AC
212
Power
Supply
230V
L
N
all Secure

The British code of practices.

- BS EN 60839-11-1 Alarm and Electronic Security Systems – Electronic Access Control Systems – Systems and Components Requirements.

- BS EN 60839-11-2 Alarm and Electronic Security Systems – Electronic Access Control Systems – Application Guidelines.

- BS EN 50486 Equipment for use in audio and video door-entry systems.

- EU Working Time Directive (officially: Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organisation of working time).

- BS 7671 IET Wiring Regulations (latest edition).

- LPS 1175 Requirements and testing procedures for the LPCB approval and listing of intruder resistant building components, strongpoints, security enclosures and free standing barriers, LPCB.

- NCP 109 NSI Code of Practice for Planning, Installation and Maintenance of Access Control Systems, NSI.

- PAS 24: 2012 Enhanced security performance requirements for door assemblies, British Standards.

- PAS 68: 2013 Impact test specifications for vehicle security barriers, British Standards.

- SSAIB Code of Practice for Access Control Systems, SSAIB.

- STS201: Enhanced security requirements for doorsets and door assemblies for dwellings to satisfy the requirements of PAS23 and PAS24, Warrington Certification.

- STS202: Requirements for burglary resistance of construction products including hinged, pivoted, folding or sliding doorsets, windows, curtain walling, security grilles, garage doors and shutters, Warrington Certification.

- Disability Discrimination Act 1995 (for Northern Ireland).

- Equality Act 2010.

- Regulatory Reform (Fire Safety) Order (FSO) 2005.