PAC 2200 Series Controllers

Installation Guide

17263 Ver 3.0 Nov 2004

PAC INTERNATIONAL LTD
A Stanley Security Solutions Business
1 Park Gate Close, Bredbury, Stockport, SK6 2SZ, England
Tel: +44 (0) 161 406 3400. Fax: +44 (0) 161 430 8658
www.pac.co.uk

Issue Record

Version	Date	Details
1.0	Nov 99	Initial release
1.1	Dec 99	Minor amendments to diagrams
1.2	Nov 00	Different enclosure options, isolator switch required if appliance outlet is used, usage of MOVs, update for MKIII AEM, standby power for battery backup added, 'Wiegand Readers' and 'Magstripe Readers' sections added, auxiliary output electrical rating and power heat dissipation figures added to Specification section, document references corrected, and 'door channels' changed to 'reader channels'.
2.0	May 02	PAC 2200 updates and PAC 2200IP option added. PAC 2204 removed to new document. CNC sites added to Multi-Function Door Controllers section. Installation, Commissioning and Test sections reorganised and updated. KeyPAC readers added to Readers section. Auxiliary output added to Other Connections section. Upgrading from PAC 2100 removed. Warning added to Troubleshooting section. Modem connection clarified in Connecting a Modem section. Transactions section removed (still in user guide).
2.1	Jan 03	FCC notice added in USA version.
2.2	Jun 04	External reader connections added. PIN reader section updated. Wiegand reader section updated. Locating and Installing readers added.
3.0	Nov 04	Disposal of lithium batteries added; MOV table added.

Version 3.0 **Nov 2004**

Changes are periodically made to the product, these changes will be incorporated into new editions of this document. PAC INTERNATIONAL LTD shall not be liable for errors contained herein or for any consequential damages connected with the use of this material.

Copyright and Protective Notices

1. The copyright of this document and the associated drawings is the property of PAC INTERNATIONAL LTD, and is issued on condition that it is not copied, reprinted or reproduced, nor its contents disclosed, either wholly or in part, without the consent in writing of, or in accordance with the conditions of a contract with PAC INTERNATIONAL LTD.
2. The publication of information in this document does not imply freedom from patent or other protective rights of PAC INTERNATIONAL LTD, or others.
3. Performance figures and data quoted in this document are typical, and must be specifically confirmed by PAC INTERNATIONAL LTD before they become applicable to any tender, order or contract.

Training and Technical Support

Training courses covering the installation and use of all PAC products are regularly held at PAC INTERNATIONAL LTD, Stockport. For further information on course availability, or to discuss your specific requirements, contact the Training Manager at the address below.

It is strongly recommended that any persons installing or commissioning PAC products attend a suitable training course beforehand.

Technical Support for all PAC products is available during normal office hours:

8:30am to 5:30pm (UK time) Monday to Friday, excluding public holidays.

Tel: 0870 7203400 **International +44 870 7203400**

Fax: 0870 7203411 **International +44 870 7203411**

Email: technical@pac.co.uk

This service is provided primarily for the use of trained engineers. End users of PAC products should first of all contact their installation or maintenance company before contacting PAC.

PAC INTERNATIONAL LTD
1 Park Gate Close
Bredbury
Stockport
SK6 2SZ
England

IMPORTANT:

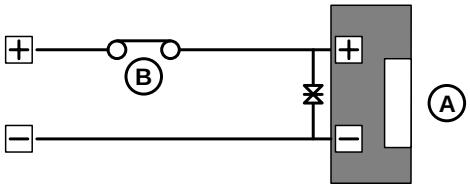
When installing the PAC equipment the following should be noted:

HEALTH AND SAFETY

Installation must wired in accordance with National Wiring Regulations (BS7671, IEE National Wiring Regulations in the UK). Failure to do so can result in injury or death by electric shock.

It must also comply with any local Fire, Health and Safety regulations. A secured door that may be part of an escape route from an area must be fitted with:

- **A fail-safe lock (A) so that the door will be released if the power fails. Ideally a magnetic lock should be used as these are less likely to jam or seize.**
- **A normally-closed break-glass or manual pull (B) in the lock supply wiring so that in an emergency the fail-safe lock can be immediately depowered.**



The controller must be earthed.

Isolate the controller supply before working on the controller.

CABLING

The cabling used in the PAC Access Control Systems (six wire bus, reader cables, etc.) are not prone to electrical interference. However, you should avoid routing cable close to heavy load switching cables and equipment. If this is unavoidable, cross the cable at right angles every 1-2m to reduce the interference.

Lithium Batteries

There is a danger of explosion if lithium batteries are incorrectly replaced or handled. Please read carefully the following guidelines. Failure to do so can result in injury.

1. Take steps to ensure that the batteries are never short circuited.
2. Always store the batteries separately in non-conducting materials.
3. Do not place lithium batteries with normal waste collections; dispose of them correctly.

For information on the disposal of used lithium batteries and your local disposal sites, call the Environment Agency Helpline (UK only) on 08459 333111.

RFID Devices

As similar RFID technology is now widely used in a number of other industries, for example automotive immobilisers, it is possible that interaction between your access control ID and other devices may cause one or the other to function incorrectly. Should you suspect that you have experienced such a problem the solution is to separate your access control ID from other RFID devices.

FCC Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The front panel complies with part 15 of the FCC rules. Operation is subject to the following two conditions (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Front Panel FCC ID OQL-P-FP

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This page is intentionally left blank.

Table of Contents

Table of Figures

Abbreviations Used in this Document

AC	Access Code
AEM	Alarm Event Manager
AVR	Automatic Vehicle Recognition
BAT	Battery
CH	Channel
CLK	Clock
CMD	Command
CNC	Central Network Controller
COM	Common
CTS	Clear To Send
D/C	Door Controller
DC	Door Contact
DL	Down Load
DOS	Disk Operating System
DTR	Data Terminal Ready
DR	Door
EMF	Electro-Motive Force
FIFO	First In First Out
GAPB	Global Anti-Passback
GND	Ground
HBC	High Breaking Capacity
ID	Identity
IP	Input or Internet Protocol
LED	Light Emitting Diode
LK	Lock
LRT	Lock Release Time
MOV	Metal Oxide Varistor
MS	Alarm Module Sensors
MS-DOS	Microsoft™ Disk Operating System
NC	Normally Closed
NO	Normally Open
OVRD	Override
PAL	Primary Access Level
PB	Pass Back
PB-TIM	Pass Back Timeout
PBC	Pass Back Controller
PC	Personal Computer
PIN	Personal Identity Number
PINTP	PIN Reader Time Profile
RDR	Reader
RTE	Request To Exit
RTS	Request To Send
RX	Receive
SIG	Signal
TAMP	Tamper
TP	Time Profile
TX	Transmit
VCA	Valid Code Accepted

1. Introduction

The document describes how to install a PAC 2200 Series Controller. Configuration and monitoring is performed from a PC and documentation for this is supplied with the administration software. For systems without a PC (i.e. standalone systems) configuration and monitoring is performed from a front panel and is documented in *17267 PAC 2200 Series Controller User Guide*.

There are several controllers in the series designated as follows:

- The first two numbers are 22 indicating the PAC 2200 series.
- The third number indicates the number of doors that can be controlled.
- The fourth number indicates the number of Alarm Event Managers (AEMs) supported by the controller.
- The suffix IP indicates a **built-in** TCP/IP interface.

Examples

Controller	Doors Supported	AEMs Supported	AEMs Supplied	Compatible with
PAC 2244IP	4	4	0	PAC 2244
PAC 2222IP	2	2	0	PAC 2222
PAC 2244	4	4	0	PAC 2100
PAC 2222	2	2	0	PAC 1100
PAC 2204	0	4	2	PAC 1300

Notes

1. PAC 2200 Ver 1 uses EPROM 13038. PAC 2200 Ver 2 uses EPROM 13074 and provides extra facilities (see Section 1.4).
2. The PAC 2204 Alarm Controller does **not** control access. Its function is to react to alarms raised by the system (e.g. switching cameras, activating lights, sirens, etc.). PAC 2204 is documented in *17329 PAC 2204 Alarm Controller Installation Guide*.

1.1 Access Control Components

Most PAC access control systems, very simply, consist of eight distinct parts:

1. The **ID Device** (i.e. a fob or card called the **key**) which is presented to (or swiped through) the reader to open a door. This has a unique code that identifies it to the system.
2. The **Reader**, usually fitted close to the door, that detects the unique code in the ID device and sends it to the door controller for verification. There are several types of reader available, suitable for different purposes and environments. It is usually situated close to the door.
3. The **Request to Exit (RTE) Switch** which is used to open a door from the secure side (sometimes a reader is used on each side of the door). When the switch is pressed a signal is sent to the controller to release the lock and open the door.
4. The **Controller**, that is the heart of the access control system. It compares the unique code in the ID device with the information stored in its memory and, if the ID device is valid, it activates the lock to open the door.
5. The **PSU** which powers the controller and locks.
6. The **Lock** which secures the door and is released when a valid ID device is presented to the reader. Locks can be divided into two main types:
   - **Fail Safe** - continuously powered with power removed to unlock. If power fails, the door will open.
   - **Fail Secure** - Power supplied to unlock. A separate power supply is required to open the door if there is a power failure.

7. The **Administration System** which is used to administer the system - program into the system who goes where and when. This may be built into the controller or be on a separate PC.

8. The **wiring** between the various components.

The PAC 2200 Series Controllers are multi-function, i.e. they can be configured to operate in a variety of different modes depending on the overall system. Some features of the access control system depend on the type of administration system used with some features (such as visitors, global anti-passback, transaction searching and reporting) only available on the PC-based administration systems.

Figure 1 shows the typical components of an access control system.

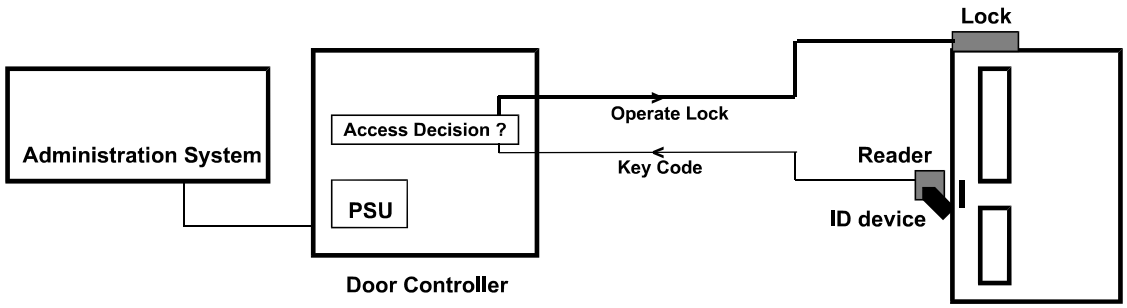


Figure 1 Typical Components of an Access Control System

1.2 Hardware Components

1.2.1 General Information

Figure 2 shows the typical connections made to a door controller. For full details of how door controllers are connected and administered, see Section 2.

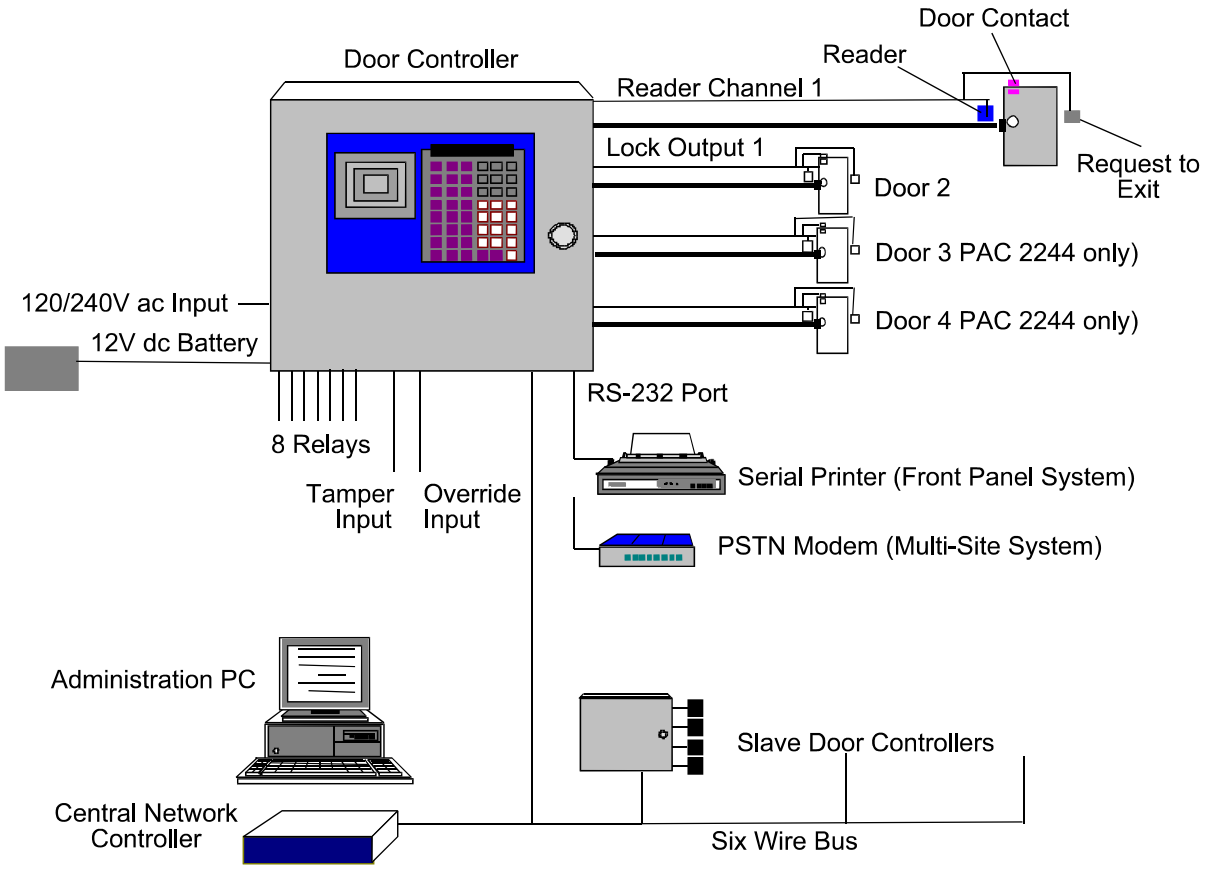


Figure 2 Typical Connections for a PAC 2244

The controller can operate in one of two ways, either as a **master** or as a **slave** providing the following administration options:

Operating as a master, the door controller can be administered:

- From the door controller's own front panel, controlling up to 16 doors if a PAC 2244 - 4 on board plus up to 3 slave door controllers.
- From a PC running administration software via a PC interface kit. This can control up to 16 or 32 doors - 4 on board plus up to 3 or 7 slave door controllers (depending on the administration software).
- From a PC running administration software via a Central Network Controller (CNC) over an RS-232 serial link. This can control up to 32 doors - 4 on board plus up to 7 slave door controllers. This can also accommodate up to 128 (dial-up) remote sites, each of which can control up to 32 doors.
- From a PC running administration software via a TCP/IP interface to an Ethernet network.

Operating from a CNC administered by a PC, each CNC will support up to 128 sites of which:

- PAC for Windows site 1 is always the six wire bus- there are no master controllers on a CNC six wire bus; only slaves.
- PAC for Windows sites 2-33 are RS- 232 sites with 1 master door controller and up to 7 slave door controllers per site.
- PAC for Windows sites 34-128 are RS-232 sites with only 1 master door controller and no slave door controllers per site.
- PAC Vision site 1 is always the six wire bus - there is no master controller on a CNC six wire bus only slaves.
- PAC Vision sites 2-128 are RS-232 sites and can be any combination of single controller or cluster sites.

Operating as a slave, the door controller can be administered:

- From another door controller configured as a master.
- From a PC running administration software.

1.2.2 Door Controllers

The door controller itself is made up of 4 individual components:

Secured to the metal base plate are the 110/240V **power supply** and **main circuit board**. Fitted to the main circuit board is a secondary “cover” board that protects the main board and has a label that identifies the various connectors on the main board. Attached to this is the **memory module** containing the software and database memory. Across the whole unit is a removable **front panel** with built-in key reader, keypad and display.

All connections are made to the door controller using **removable terminal blocks**.

Note

All controllers are available without a front panel. However, at least one front panel is required to configure the controllers in the system.

The door controller is the heart of the access control system and it:

- Decides whether a person has access at a particular door and at a particular time.
- Provides power to operate the lock and readers.
- Monitors doors for unauthorised access or door left open.
- Automatically unlocks and locks doors at certain times.
- Detects tamper conditions at the reader or its enclosure.

- Controls the 8 on-board relays.
- Programs and monitors any Alarm Event Modules (AEMs) that may be fitted.

What makes the door controllers so flexible is the ability to link controllers together to allow more doors to be administered. The number of doors that can be administered and the maximum number of personnel that can be controlled depends on the type of administration system, see Section 2.

Door controllers are connected together using PAC's six wire bus. This is a proprietary communications link that uses standard six-conductor signal or alarm cable. For full details, see Section 3.1. Each group of door controllers connected using the six wire bus requires one master controller and one or more **slave** controllers.

- For smaller systems (16 or 32 door administration systems), one door controller is the master with up to 3 or 7 slave controllers.
- For larger systems (up to 128 doors) the CNC becomes the master and **all** the door controllers (up to 32) on the six wire bus are slaves.
- Remote sites, connected to a CNC via an RS-232 serial link, are set up as a 32 door system with one door controller as the master, handling communications with the CNC, and up to 7 slave door controllers.

IMPORTANT

1. Every PAC 2200 Series Controller can be configured as a master **or** slave. You do **not** need to purchase different types of door controller.
2. If you are integrating the controller with older PAC systems, see *17443 Differences Between PAC 2100 Series and PAC 2200 Series.*
3. If you are upgrading an existing system, check with PAC Technical Support that all the components are suitable and whether any upgrades are required.

1.2.3 Readers

A reader is a device, usually fitted close to the door that detects the unique code in a key and passes it to the door controller where the access decision is made. There are several types of reader suitable for different purposes and environments.

Note

The PAC 2200 Series Door Controllers can have **two** readers per door channel (i.e. in and out readers) or standard access (e.g. dual height readers). However, if the reader output is in a Magstripe or Wiegand format, only one such reader per door channel is allowed.

KeyPAC Readers

These readers read **KeyPAC** electronic keys and ISO thickness ID cards they **do not** read the earlier **PAC** ID devices. Make sure that you specify **KeyPAC** whenever you purchase electronic keys and ID cards.

PAC Readers

These readers read **PAC ID** electronic keys and ID cards. They **do not** read the newer **KeyPAC** electronic keys and ID cards. Make sure that you specify **PAC ID (not KeyPAC)** whenever you purchase electronic keys and ID cards.

PIN Readers

These readers require a PIN number to be entered as well as a key to be presented, as an extra level of security. The need to use a PIN as well as a key can be controlled using a time profile.

Magstripe Readers

These readers convert the code in the magnetic stripe into a format recognisable by the door controller. The door controllers supports Magstripe cards which are encoded according to ISO 3554, Track 2.

Wiegand Readers

The door controllers supports the full range of Wiegand formats. Most Wiegand output devices will provide a sensor-compatible 26-bit output. If there is a choice, this format should be selected.

Automatic Vehicle Recognition (AVR)

This is a transmitter fitted to a vehicle that sends a unique code that is picked up by a buried loop aerial.

1.3 PAC 2200 Ver 1 Facilities

This section describes the features available on the PAC 2200 Series Controllers that have the EPROM 13038 fitted.

Note

Many of the PAC 2200 Series Controller features are only available via a PC.

1.3.1 Reader Channels

The 2200 series allow an in and out reader on each channel. Not applicable to Wiegand and Magstripe readers or PAC 2204.

1.3.2 Front Panel

The door controllers can be purchased without a front panel. However, at least one is required for basic configuration. It is recommended that controllers without panels are used only as slaves and that at least one controller on a site has a front panel. The front panel is detachable and can be fitted to any controller.

Pressing the **?** key on the front panel will produce the following display:

```
type  Mn   Vx-y
```

where

type is the controller type (e.g. *2222 or 2244*).

Mn refers to the system type:

n = 0 for master door controller (standalone system)

n = 1 for MS-DOS system (not available with PAC 2200 Ver 2)

n = 2 for PC-based system

n = 3 for slave door controller (any system)

Vx-y is the software version number.

Example

```
2244  M2   V1-0
```

This is a PAC 2244 with software version 1.0, running in mode 2.

1.3.3 Power Supply Unit (PSU)

The 8A PSU (PS159) provides the following features:

- **Automatic input voltage detection** - the power supply operates from a mains input of between 85V ac and 250V ac. There is no need for separate models for different mains supplies.
- **Lock output voltage - 12V or 24V dc detection** - the lock output voltage can be set to 12V or 24V dc.
- **Power indicator** - a red LED within the power supply indicates the presence of ac input voltage.
- **Mix and match locks** - provided you do not exceed the maximum allowed for the power supply.

Note

A 4A PSU (PS80) was used on older door controllers.

1.3.4 10K Memory Module

This memory module has capacity for 10,000 keys. Memory modules contain an EPROM that can be easily replaced (i.e. updated, see Section 1.3.16).

1.3.5 Onboard Relays

There are 8 relays fitted to the door controllers. These relays are as follows:

- Relay-1: invalid key on door-1.
- Relay-2: invalid key on door-2.
- Relay-3: invalid key on door-3.
- Relay-4: invalid key on door-4.
- Relay-5: door/anti-tamper on any door.
- Relay-6: time profile-1.
- Relay-7: door left-open alarm on any door.
- Relay-8: system tamper.

Notes

1. The default settings are applied when the database is initialised either at the front panel or from a PC.
2. Default setting for relays 1-4 do not apply to the PAC 2204 Alarm Controller.
3. Relays 1-4 are programmable to respond to a wide range of events when being administered via PAC for Windows.
4. Relays 1-8 are programmable to respond to a wide range of events when being administered via PAC Vision.

The PAC 2200 controllers automatically detect when they have been upgraded from a PAC 2100 and:

- Apply defaults to the main-board relays.
- Clear non-volatile system variables such as door and alarm states.
- Clear the update/download stack.
- Apply defaults to the reader configuration.
- Set the default First In First Out (FIFO) limits (for dial-back) to zero, i.e. disable dial-back on buffer full.

1.3.6 Alarm Event Managers (AEM)

AEMs can be attached to all controllers in the series. The PAC 2204 comes with two AEMs fitted as standard. Two more can be added to the PAC 2204.

It is possible to program the relays on each AEM to activate on certain events, including time profiles, door alarms, etc. For further details, see the documentation provided with the administration software.

1.3.7 Dial-Back

Only on **Multi-Site Systems administered by a CNC** connected through a dial-up (PSTN or LAN) modem to a CNC. If using dial-up modems, you can set any PAC 2200 controllers configured as a master to dial back to the CNC in the event of an alarm condition or access authorised event.

Note

Call PAC Technical Support when designing a dial-back system using LAN/WAN.

1.3.8 Protected Communications

This is administered by CNC where dial-up sites are used and only establishes communications with a door controller if the master key code from the CNC is recognised.

When selected at the door controller, this feature is 'self-programming' and:

- Allows the next dial-up by the CNC to be accepted.
- Stores the master key sent by the CNC in the door controller.

When the CNC next dials the master door controller, the controller will only establish communications if the CNC sends the same master key code as is stored in the door controller.

To set this feature, see Section 7.2.2.

1.3.9 Remote Acknowledgement

Only on **PC administrated systems.** All alarm events generated at the controller are not cleared until an operator has accepted them at a PC.

Whenever an alarm occurs at the controller, a relay is set. When the alarm is acknowledged at the PC and successfully communicated back to the master controller, the relay is reset.

When using a PC, it is possible to set alarms so that the relays are not reset until an operator accepts the alarm at the PC. This is particularly important if you are going to use the more extensive relay programming now available.

To set this feature, see Section 7.2.2.

1.3.10 Transaction Filtering

On busy systems, performance can be improved by filtering out the less important transactions such as request to exit, free exit, etc. Now there are 5 groups of transactions that the door controller can 'forget', i.e. **not** send to the administration system.

To set this feature, see Section 7.2.1.

1.3.11 Multiple Reader Formats

Readers with Wiegand or Magstripe output can be connected directly to the door controller (see Section 5.2.7 and 5.2.8 for details).

Note

When connecting Wiegand or Magstripe readers directly to the controller channel only one reader per channel is allowed. To connect two Wiegand or Magstripe readers to a controller channel use a Wiegand interface unit per reader. For more information contact PAC Technical Support.

1.3.12 Anti-Passback

Anti-passback is a security feature that prevents a single key being shared between multiple users. This commonly occurs when one user accesses an area and then either holds the door open or passes the key back so that other users can gain entry.

Once the anti-passback option is applied to an area bordered by access-controlled doors, each user having entering the area must exit it using their key. Failure to do so may result in the user not being able to regain entry to the area.

Local, timed and global anti-passback are available and these are described in the following sections.

1.3.12.1 Local Anti-Passback

Local anti-passback is anti-passback that is controlled by one controller that records which keys have been used to enter an area. This information is then used to determine whether or not a key can be used to enter or leave the area. This can be used to prevent keyholders passing their keys to others to gain entry.

Notes

1. Local anti-passback only operates between the doors on a single door controller with specific readers allocated as entry ("doors" 1 and 2) and exit ("doors" 3 and 4), i.e. one reader per channel, see Figure 3.
2. **Request to Exit** switches should not be used when anti-passback is required because they infringe passback security every time they are used.
3. If door monitoring is used, local anti-passback will only be set if a key is presented **and** the door is opened. Simply presenting a key will not set local anti-passback. If door monitoring is not used, local anti-passback will be set when a valid key is presented.

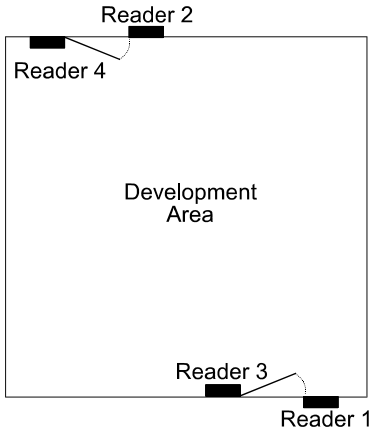


Figure 3 Possible Reader Locations for Local Anti-Passback

There are two types of local anti-passback available:

1. **Anti-Passback on Entry**. When this feature is active, any key used to enter an area cannot be used to enter the area again unless it has first been used to leave the area. Using the example shown in Figure 3, if you use your key to enter development, you cannot use the same key to enter development unless it has first been used to leave development. If the key is used again at an entry door, a `No Entry: Passback` transaction is generated and the lock will not operate. Access will continue to be denied until the key has been used at an exit reader or the passback timeout period has expired.
2. **Anti-Passback on Exit**. When this feature is active, a key cannot be used to exit an area unless it has first been used to enter the area. This is only available when anti-passback on entry is also active. Using the example shown in Figure 3, if you have not used your key to enter development (e.g. you came in with someone else), you cannot use your key to leave development. If the key is used again at an exit door, a `No Exit: Passback` transaction is produced and the lock will not operate. Access will continue to be denied until the key has been used at an entry reader or the passback timeout period has expired.

1.3.12.2 Timed Anti-Passback

Timed anti-passback is where the period for which a key is denied access is specified. After the specified period has elapsed the key will be allowed access again, even if it has not been used to leave the area. The time may be set to between 10 and 70 minutes in 5 minute steps (10, 15, 20, etc.).

Using the timeout period means you could use anti-passback without an exit reader. A car park, for instance, may have an entry barrier with a reader. When a key is used to raise the barrier, that key will not be able to gain access again until the time period expires. Provided that genuine use of the key is unlikely to be needed within the time period, no exit reader is required.

Note

Timed anti-passback also works with global anti-passback.

1.3.12.3 Global Anti-Passback

Global Anti-Passback (GAPB) is anti-passback that is controlled by more than one controller and is only available on cluster sites. These are sites where slave door controllers are administered by a master door controller.

Examples of where GAPB can be used:

- A controller cluster connected via a PC interface kit.
- A controller cluster connected to, or communicating back to, a CNC RS-232 port.
- A PC administration system using PAC for Windows or PAC Vision software.

Examples of where GAPB cannot be used:

- On CNC six-wire bus sites.
- Across multiple clusters.
- On controllers older than the PAC 2200 series (e.g. PAC 2100 series)
- With COS dataswitch clusters.
- With nested GAPB areas (i.e. areas within areas).

Up to seven areas per cluster (1 master and up to 7 slave controllers) can be programmed via a PC. Each area for which global anti-passback is to be in operation must be defined by specifying the entry readers into the area. For each reader the following must be specified:

- Direction, i.e. in, out or access (not direction specific). This is used to provide information on the transaction report.
- An “entry area” for the reader, i.e. the area to which the reader allows entry.
- An “exit area” for the reader, i.e. the area to which the reader allows exit.

The door controller uses the entry and exit areas specified for each reader to determine exactly where a person is. Once a person has entered an area for which global anti-passback has been set, re-entry is not allowed until that person has either left the area or until the passback timeout has elapsed.

1.3.13 Master Override Input

This feature, when active, “links” the override input of slave controllers to the master controller to which they are attached. If the override output is triggered on the master controller, the doors on any slave controllers with the option set are automatically opened.

1.3.14 Event Time Stamping

Accuracy can be selected to be to the nearest second. Default is to the nearest minute.

1.3.15 Compatibility with Previous Models

The PAC 2200 Series Controllers replaces the PAC 2100/1100 and is compatible with older PAC door controllers.

Note

It is recommended that different types of controllers are not mixed on a cluster.

1.3.16 Upgrading a Memory Module

The memory module used in the PAC 2200 Series Door Controllers is physically identical to that used in the PAC 2100 Series - only the software is new.

The memory module can be transferred from a PAC 2100 to a PAC 2244 to preserve the database. Once the transfer is complete, the software in the memory module **must** be updated in the memory module before it will work.

The backup battery can also be replaced without data loss. The backup battery is provided to maintain the system's memory when all power, mains and external battery backup is removed.

Replacing the Backup Battery

1. The module **must** be plugged into the door controller.
2. The door controller **must** be powered from the ac power line or the sealed lead acid backup battery in the panel case.

Upgrading from PAC 2100 to a PAC 2244

1. Power down both controllers.
2. Remove the memory module from both controllers.
3. Insert the PAC 2100 memory module into the PAC 2244
4. Upgrade the software in the memory module by replacing the old EPROM with the new EPROM.
5. Power up the PAC 2244 and the upgrade is complete.

1.4 PAC 2200 Ver 2 Facilities

EPROM 13074 can be fitted to a PAC 2200 Series Door Controller to provide the same facilities as described in Section 1.3 **plus** those described in this section **providing the appropriate administration software is used**.

1.4.1 50K Memory Module

This memory module has capacity for 50,000 keys and is for use with PAC Vision. When used with PAC for Windows, only 18,000 keys can be used. The memory module contains EPROM 13074 and replaces the standard 10K memory module.

1.4.2 Arming/Disarming Alarm Areas

Arming an area overrides any time profiles so that only people with arming privileges can enter the area. Arming/disarming an area is performed from an alarm panel or by presenting a key (and PIN number) and pressing an arming button to confirm. The arming/disarming signal can be via an arming relay or via a single serial link depending on the type of alarm panel.

The arming relay is a relay configured to send arming information to a non-intelligent alarm panel and is normally connected across the key-switch input of the alarm panel. Most key-switch inputs require a latched signal level but a few respond to edges.

The door controller's auxiliary serial port is used to communicate with intelligent alarm panels (e.g. DMP and Radionics).

Note

The main serial port, labelled PRINTER should not be used when connecting to an intelligent alarm panel.

The arming/disarming signal is the INHB/DR3 input on each reader channel of a door controller (see Section 5.2.1.3). When the INHB/DR3 input is connected to the alarm panel, this is typically across the arming relay output, so that a short to ground indicates when the system is armed or an exit delay is occurring.

It is important to know how the arming output of the alarm panel works. For example, if the arming output switches over during the exit delay rather than after it, ensure that users have the appropriate alarm privileges to leave the building while the exit delay is occurring.

Shorting INHB/DR3 to ground results in all overrides for the corresponding door being cancelled. This includes time profiles, emergency and manual (operator) overrides. However, the door controller override (fire) input still affects the door. In addition to overrides being disabled, access through the door is only permitted to users with appropriate alarm privileges.

If the affected door has been assigned to an alarm area, all doors with the same alarm area number are also affected by the state of INHB/DR3. The INHB/DR3 input must be situated on a master door controller if slave door controllers are also to be affected by the system being armed.

Note

The INHB/DR3 input can also be used to automatically arm the alarm panel provided specific options have been selected by the PC administration system. A normally-open non-latching switch can be connected between the INHB/DR3 input and ground. After a key with the appropriate arming privileges has been presented to an exit reader, the “arming” button can be pressed to arm the area associated with the door.

1.4.3 Alarm Panel Interface

Alarm panels can be integrated with the access control system via a single serial communications link to a door controller.

The alarm state input is the ALM/DR4 input on each reader channel of a door controller (see Section 5.2.1.3). This input is normally connected across the alarm output relay of the alarm panel and communicates alarm information to the PC administration system. Shorting ALM/DR4 to ground results in an `External Alarm` event being logged. Returning ALM/DR4 to its default state results in an `External Alarm Cleared` event being logged.

The relays on the door controller can be programmed to trigger if the alarm panel goes in to an alarm condition. Either main board relays 1 to 4 or the AEM relays can be configured to do this.

The shunting relays are the door controller's main board relays 5 to 8, where relay 5 is used for door channel 1, relay 6 for door 2, etc. The shunting relay is used to echo the state of the door contact of an entry/exit door to the alarm panel. This avoids the need to fit one door contact for the access control and one for the alarm monitoring system for the same door.

The relays 5 to 8 only act as shunting relays when the corresponding door channel is assigned to an alarm area. The following table illustrates the different actions of relays 5 to 8:

Relay	Non-Alarm Panel Behaviour	Alarm Panel Behaviour
5	Door 1 not assigned to an alarm area: Responds to any door forced open or tampered with.	Door 1 assigned to an alarm area: Responds to contacts on door-1 opening / closing.
6	Door 2 not assigned to an alarm area: Responds to time profile-1 going active/inactive	Door 2 assigned to an alarm area: Responds to contacts on door-2 opening / closing.
7	Door 3 not assigned to an alarm area: Responds to any door left open after a valid access by a user.	Door 3 assigned to an alarm area: Responds to contacts on door-3 opening / closing.
8	Door 4 not assigned to an alarm area: Responds to door controller case being opened – assuming a micro-switch has been fitted.	Door- assigned to an alarm area: Responds to contacts on door-4 opening / closing.

By default, the shunting relay follows the state of the door contact. Optionally, the shunting relay can be programmed to **not** trigger when a user accesses a building using a key. This allows personnel to enter the building without an entry delay and subsequently disarm the alarm panel using its own keypad.

1.4.4 TCP/IP Interface

A TCP/IP interface unit can be fitted to the door controller that allows the serial port to be connected to a PC across an existing Ethernet network. This interface will require some configuration before it can be used (e.g. it will require a TCP/IP address).

The PAC 2200IP Series have the TCP/IP interface built into the controller.

Configuration of the TCP/IP interface is performed using standard tools available with Microsoft Windows®, such as Internet Explorer or Telnet.

Information on how to configure a door controller is contained on the PAC Vision CD.

2. Administration Systems

This section looks briefly at the administration systems that can be used with the door controllers.

There are several ways of administering PAC Access Control Systems. Different methods allow greater numbers of doors or personnel to be controlled and door controllers to be located at greater distances from where the system is administered.

This section looks at the following systems:

1. **Front Panel**. This is a standalone system that allows up to 16 doors with administration carried out entirely via the front panel. This is only really suitable for small systems with small numbers of personnel.
2. **Direct**. This is a PC-based administration that allows up to 32 doors to be controlled from a PC. This provides a user interface that is much easier to use and also provides additional control over the controller relays and AEM inputs and outputs.
3. **CNC**. This is a PC-based administration that allows up to 128 doors (depending on the memory module and administration software). This provides the option of having multiple (remote) sites connected via dial-up modems. Both single and multiple site systems are described.

2.1 Front Panel - 16 door

The door controllers are normally supplied with a front panel containing a 48-key keypad, a 16-character display and a key reader. However, it is possible to purchase controllers without a front panel if required. PAC recommend that controllers without front panels are used only as slaves and that at least one controller on a site has a keypad to enable programming. The simplest way of administering an access control system is to use this panel to carry out all the programming. Keys are added by presenting them to the front panel reader, data is added, modified or deleted using the keypad and display.

When using this form of administration, a serial printer may be connected to the master controller, this will print events as they occur and can also be used to print the contents of the controller's database.

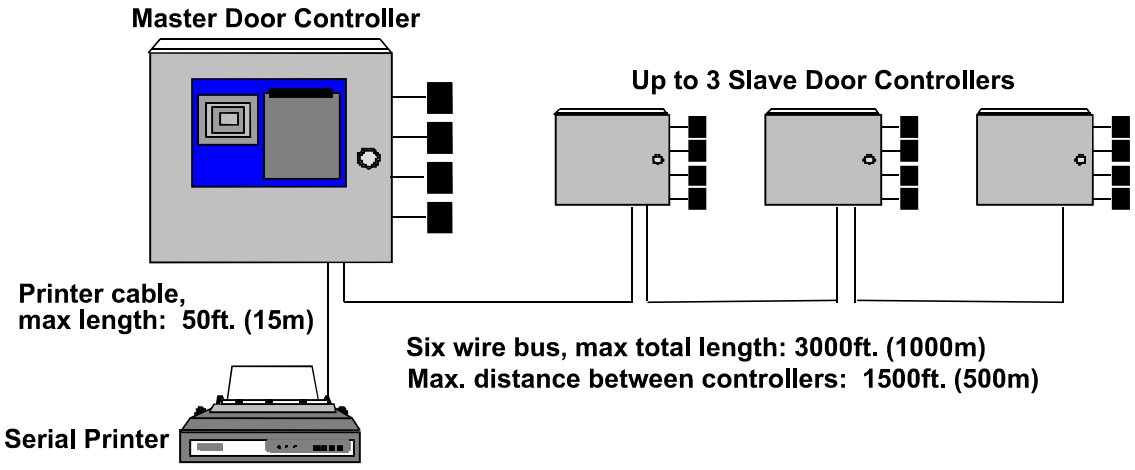


Figure 4 System Diagram - Front Panel Administration

The system limits are as shown in the following table:

Maximum Number of Controllers	4
Maximum Number of Doors	16
Maximum Number of Personnel	4000
Access Codes	128
Time Profiles	32
Editors	32 (plus master)
Auxiliary Alarm Points	32 per door controller
Global Anti-Passback	Not available

For further information on front panel administration, see *17267 PAC 2200 Series Controllers User Guide.*

2.2 Direct - 16 or 32 door

This system has a master door controller administered from a PC via a PC interface kit. The administration software, besides providing a much easier to use interface, also allows extra control of door controller relays and alarm module inputs and outputs.

The kit comprises; a PC interface unit, a desktop reader for key administration, a line driver for fitting to the master controller, cables for connection of the PC interface unit to the PC and software for running on the PC.

Two versions are supplied, allowing up to 16 doors or 32 doors to be controlled. A special device, a security block fitted to the printer port of the PC determines which version is being used.

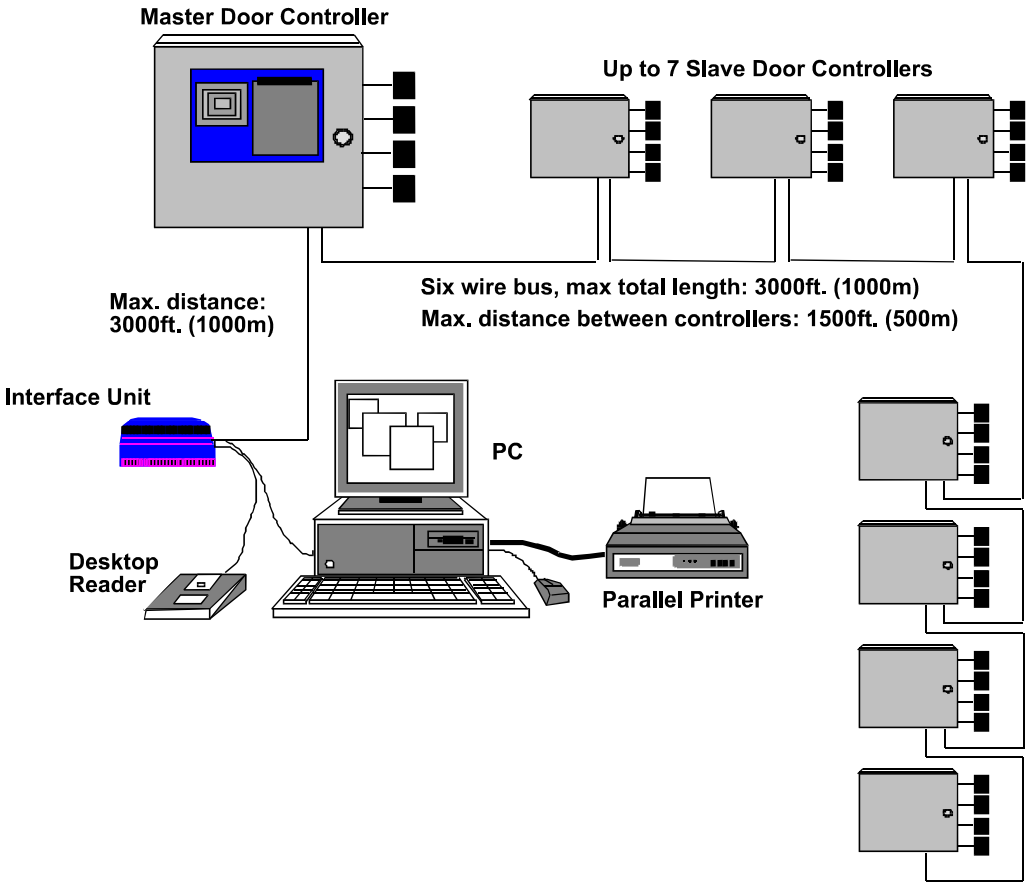


Figure 5 PC Interface Kit System

Note

The maximum distance between the PC and master controller can be increased by replacing the PC interface unit with modems or an Ethernet network.

The system limits are as shown in the following table:

Maximum Number of Personnel	10,000 (upgradeable to 50,000)
Maximum Number of Visitors	750
Maximum Number of Doors	32
Areas	128
Access Groups	128
Time Profiles	128 (if all PAC 2200 Series)
Editors	32 (plus master)
Auxiliary Alarm Points	32 per door controller
Global Anti-Passback	Available

For further information on administration, see the documentation supplied with the administration software.

2.3 CNC with Six Wire Bus - 128 doors

This system has a master CNC administered from a PC. Up to 32 door controllers, all configured as slaves, are connected using the six wire bus. The CNC has an integral reader for key administration and connects directly to the PC's serial port using the cable supplied. The administration software, besides providing a much easier to use interface, also allows extra control of door controller relays and alarm module inputs and outputs.

Note

A mixed system is not allowed, i.e. the slaves must all be PAC 2200 Series or all PAC 2100 Series.

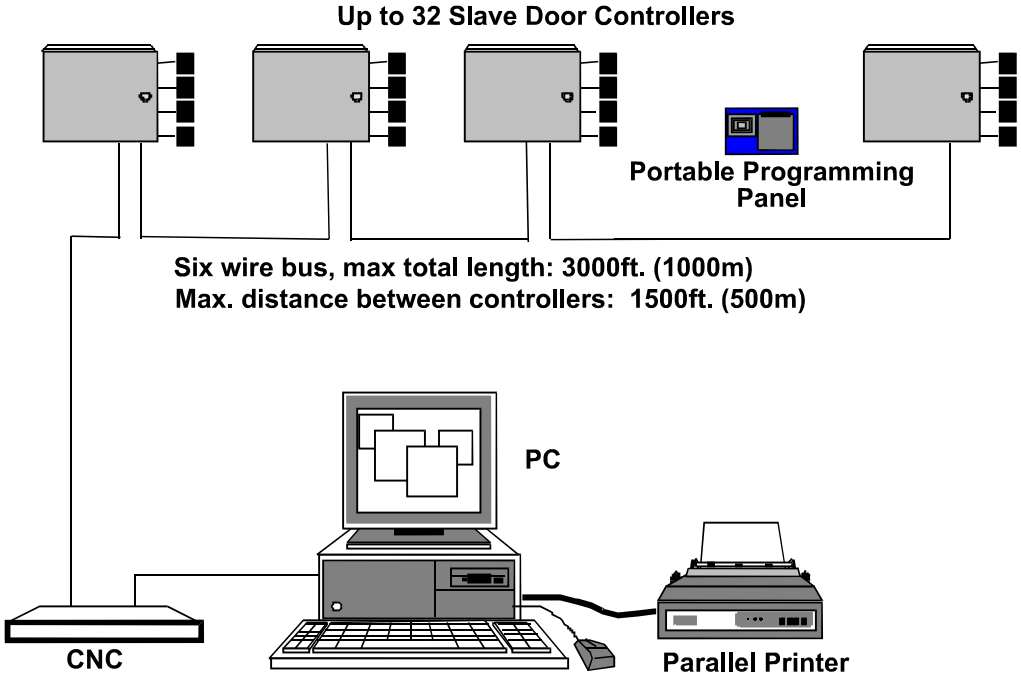


Figure 6 Single Site CNC System

This system limits are as shown in the following table:

Maximum Number of Personnel	10,000 (upgradeable to 50,000)
Maximum Number of Visitors	750
Maximum Number of Doors	128
Areas	128
Access Codes	128
Time Profiles	128 (if all PAC 2200 Series)
Editors	32 (plus master)
Auxiliary Alarm Points	32 per door controller
Global Anti-Passback	Not available

For further information on administration, see the documentation supplied with the administration software.

2.4 CNC with Multiple Sites - up to 128 Sites

This system has a master CNC for site 1 and a master door controller for each subsequent site. All sites are administered from a PC or PCs. Up to 128 sites can be controlled. The first of these sites is the 128 door (32 door controllers) six wire bus described in Section 2.3. The other sites are connected using RS-232 serial communication links.

There are 3 serial ports on the CNC, allowing up to 3 sites to be permanently connected. By using dial-up (PSTN or LAN) modems more than one site can be attached to each port. Once or twice a day, the CNC will dial-up each site, send updates and receive events.

Note

If using PAC for Windows, the first 32 serial sites may have up to 8 connected door controllers on each site, the remaining 95 sites may have just one door controller. If using PAC Vision, all 127 RS-232 sites can have 8 controllers.

Each site will consist of at least one master door controller with up to 7 slave door controllers attached using the six wire bus giving a maximum of 32 doors per site.

When using dial-up links, it is possible to set the master door controller to dial-back to the CNC in the event of an alarm. Normally all communications are made by the CNC dialling out to each site.

An alternative arrangement may be used when it is not possible to connect the door controllers at the remote site via the six wire bus. This system involves using a Code Operated Switch (COS), available in 4 and 8 port versions, to switch between door controllers. In this case, each door controller is set up as a slave.

Notes

1. Use of a dataswitch does **not** allow dial-back.
2. A mixed system is possible but different series controllers **must not** be mixed on the same cluster.

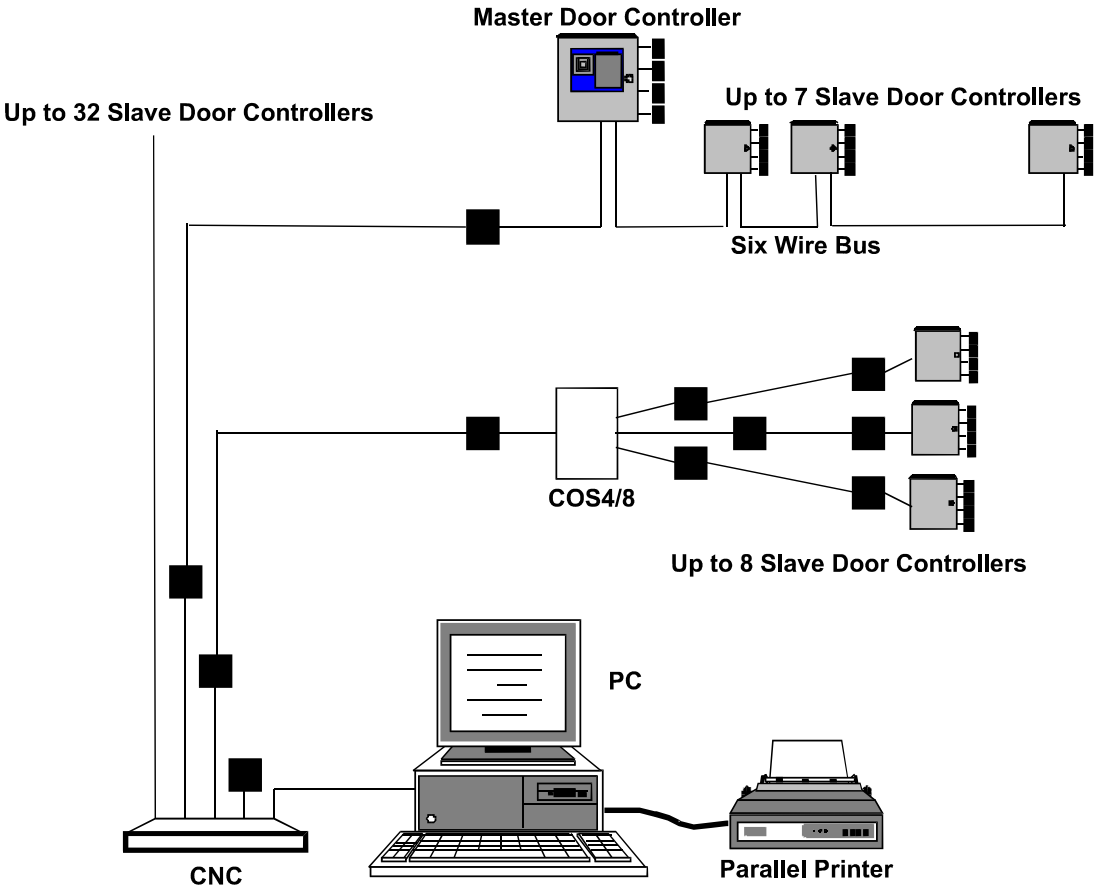


Figure 7 Multi-Site CNC System

The system limits for this type of system are detailed in the following table.

Maximum Number of Personnel	10,000 (upgradeable to 50,000)	
Maximum Number of Visitors	750	
Maximum Number of Doors	Site 1	128 doors (32 D/C) (6WB)
	Sites 2-32	32 doors (8 D/C) (RS-232)
	Sites 33-128	4 doors (1 D/C)(RS-232)
Access Codes	128 per site	
Time Profiles	128 per system	
Editors	32 (plus master)	
Auxiliary Alarm Points	32 per door controller	
Global Anti-Passback	Available only on sites with a master door controller	

For further information on administration, see the documentation supplied with the administration software.

3. Communication Systems

3.1 Six Wire Bus

The six wire bus is PAC's proprietary communications link for locally connecting door controllers. Each door controller has a built-in six wire bus interface.

3.1.1 Cable Specification

We recommend that you use multi-stranded, unshielded, 6/8-conductor 24AWG/0.22mm² alarm or signal cable. If you do use shielded cable, you should reduce the maximum distance by 2 to 3 times depending on the capacitance of the cable.

This is a linear bus and, where possible, should be set up as shown in Figure 8. The total length of the bus should not exceed 3000ft/1000m) and no single length should be longer than 1500ft/500m.

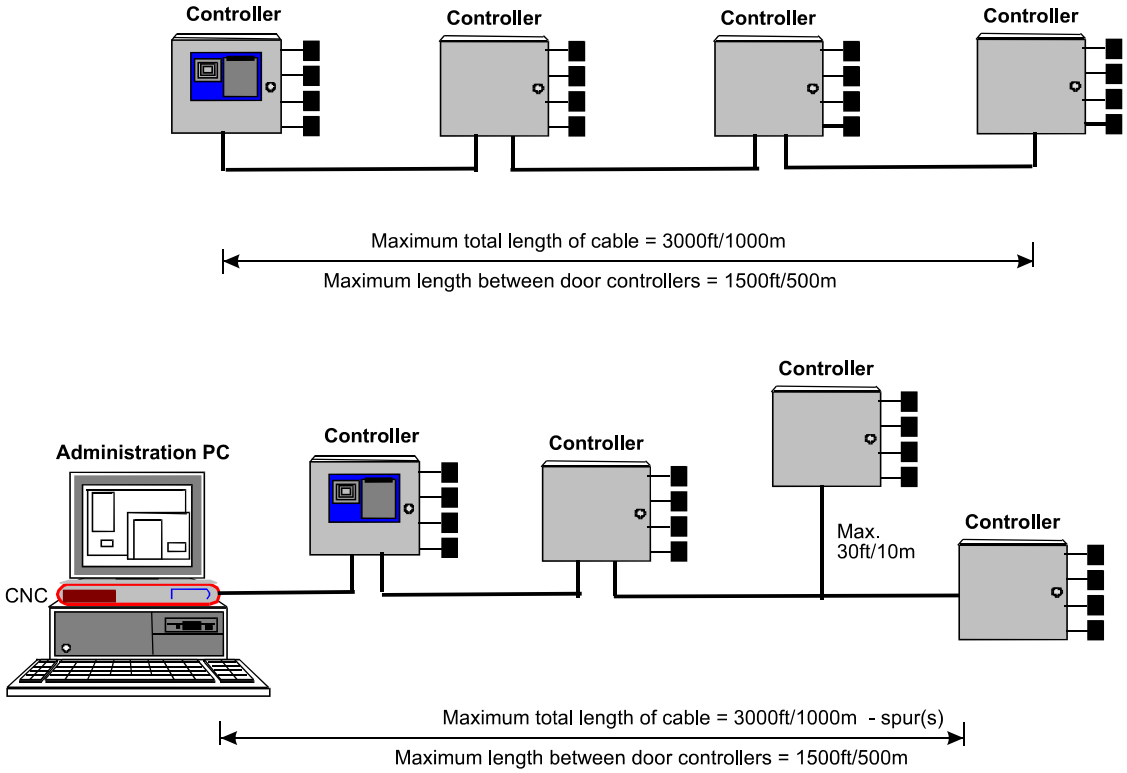


Figure 8 Six Wire Bus Configuration

Note

Branches/spurs are allowed provided they are no longer than 33ft/10m in length. The length of the spurs should be included as part of the overall length. A maximum of four spurs are recommended.

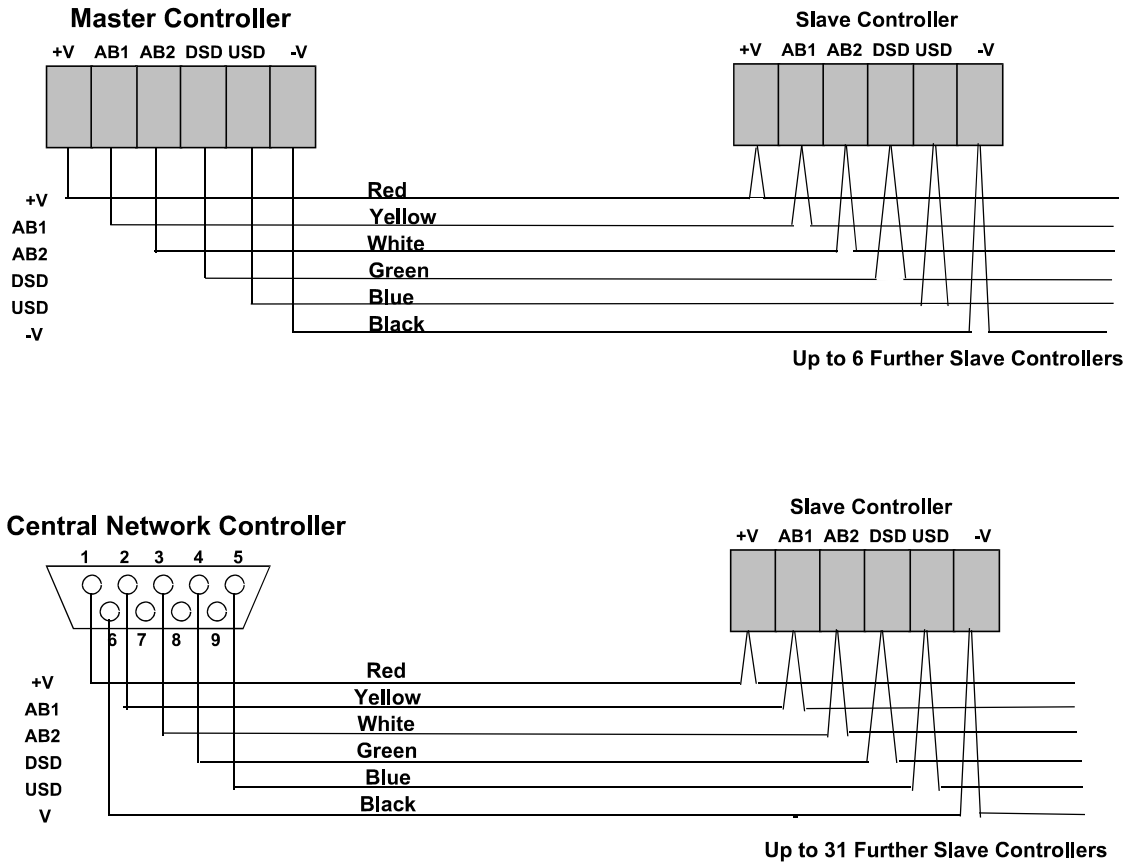


Figure 9 Six Wire Bus Wiring

3.1.2 Addresses

The six wire bus works by each door controller having its own unique address. The order in which door controllers are addressed does not matter nor do they have to be numbered consecutively. Depending on the type of administration, the following are possible:

Standalone

One master controller (system type 0) address 1 and up to 3 slave controllers (system type 3) addresses 2, 3 and 4.

16 Door

One master controller (system type 2) address 1 and up to 3 slave controllers (system type 3) addresses 2, 3 and 4.

32 Door

One master controller (system type 2) address 1 and up to 7 slave controllers (system type 3) addresses 2, 3, 4, 5, 6, 7 and 8.

Single-Site

Up to 32 slave controllers, addresses 1 to 32.

Multi-Site

Via the six wire bus:

Up to 32 slave controllers (system type 3) addresses 1 to 32.

Via the serial link:

Up to 32 sites comprising one master controller (system type 2) address 1 and up to 7 slave controllers (system type 3) addresses 2, 3, 4, 5, 6, 7 and 8.

Up to 95 sites comprising one slave controller (system type 3).

Notes

1. When being addressed by the CNC, a maximum of 32 controllers can be addressed. When polling, the CNC display shows the address as 0-9 and A-W (10 to 32).
2. A multi-site network has sites numbered according to the type of site as follows:

   Site 1 - via six wire bus, one master and up to 32 slaves.

   Sites 2-33 - via RS-232, one master and up to seven slaves.

   Sites 34-128 - via RS-232, one slave.

Site numbers allocated depend on the type of site and are not necessarily sequential, e.g. a network could comprise sites 1, 2, 3, 34 and 35.

3.2 RS-232 Serial Port

The RS-232 serial port can be used to connect the door controller to a variety of devices.

3.2.1 Printer

A printer can only be fitted to a door controller when the system is being administered from the front panel. When administered from a PC, the printer connected to the PC is used.

3.2.1.1 Report Printing

All the information stored in the door controller database can be printed. There are several printer commands, **P1** to **P9** (see *17267 PAC 2200 Series Controllers User Guide*), which will allow particular reports to be generated.

3.2.1.2 Transaction Printing

The door controller can store about 2400 transactions in its memory. Each transaction is printed out if a printer is connected. If the printer is not connected, the transactions will be stored. Once the maximum number of transactions is reached, the oldest ones will be lost. When the printer is reconnected, printing will continue with the oldest unprinted transaction and continue until all unprinted transactions have been output.

3.2.1.3 Printer Specification

An 80-column dot matrix printer with a **serial** interface is required. The serial interface must be set, using switches and/or jumpers with the following parameters:

- 4800 baud.
- 8 data bits, 2 stop bits.
- No parity.
- Hardware handshake using DTR/CTS. When the printer is busy, it should force DTR, usually pin 20, low.
- The printer must be capable of receiving at least 82 characters after a busy signal is sent (DTR going low).

PAC have used the EPSON LX series and the OKI Microline 182 printers successfully in the past.

3.2.1.4 Baud Rate

The baud rate between the printer and door controller (address 1) must be set to 4800 (see Section 7.2.2).

3.2.1.5 Printer Cable

The following cable is required:

Use 24AWG/0.22mm², 4-conductor, unshielded cable, maximum length: 50ft/15m.

PAC 2244		Printer	
5-pole terminal block		25-pin male D-type connector	
TXD	———	3	RX
CTS	———	20	DTR
RXD			
DTR			
GND	———	7	Signal Ground

3.2.1.6 Testing the Printer

Once the printer is connected and the parameters set as above, switch on the printer and make sure that is 'on-line'. If everything is set correctly, you should immediately get some transactions printed out.

3.2.1.7 Possible Problems

If you do not get immediate printing of events, check the following:

- Check the cable - it should be wired as described above.
- Check that the printer's serial port is being used. Most printers are sold with a parallel port as standard - the serial port is supplied as an add-on option. There may be a switch that selects which port the printer should use.
- Check that both the door controller and the printer are set to a baud rate of 4800. If you get random characters on the printer, the baud rates may not match. The printer will usually have DIP switches or jumpers that need to be set to give the correct baud rate. **Always switch off the printer before you change any settings.**
- If you get normal printout but after one or two pages the lines break up or you get random characters, the 'handshaking' may not be working. Check that the printer is using pin 20 for its DTR signal. Some printers allow you to select a different pin number (often pin 11).

3.2.2 Line Driver

When a PC interface kit is used to connect the PC to the door controller a line driver is supplied for connection to the door controller. This section describes the installation of the line driver at the door controller.

For further details, see the documentation supplied with the PC interface kit.

3.2.2.1 Cable Specification

Use multi-stranded, unshielded, 4-conductor 24AWG/ 0.22mm² signal cable.

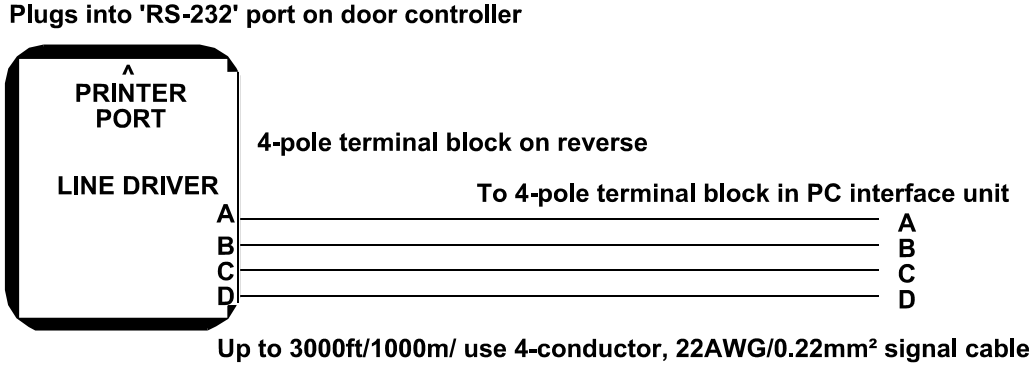


Figure 10 Line Driver Wiring Diagram

3.2.2.2 Fitting the Line Driver

IMPORTANT

For effective communications, ensure that both the PC interface kit and the door controller are properly earthed.

The line driver should be plugged directly into the door controller's RS-232 port, the 5-way socket at the bottom right of the circuit board.

The connection to the interface unit is made by connecting the terminals labelled **A B C D** on the line driver to the corresponding terminals in the interface unit using the 4-pole terminal blocks provided.

3.2.2.3 Baud Rate

The baud rate between the PC interface unit and the door controller (address 1) must be set to 4800 (see Section 7.2.2).

If communications are successfully established, a `1` flashing at the right of the display means the PC system is communicating with the door controller. From now on:

- All updates must be made from the PC.
- All transactions, including alarms, are sent to the PC.

3.3 Modems

See *17162 Central Network Controller Installation Guide* for details of communicating with a door controller over public (PSTN) phone line, the types of modem you can use, and the door controller configuration.

The modem should be fitted close to the door controller and connected using the following cable.

3.3.1.1 Modem to Door Controller Cable

Use 24AWG/0.22mm², 6-conductor, unshielded cable, maximum length: 50ft/15m.

Modem			Door Controller
25 pin male D-type connector			5-pole terminal block
RX	3	———	RXD
TX	2	———	TXD
GND	7	———	GND
CTS	5	———	CTS
RTS	4	┐	
DTR	20	┘———	DTR

3.3.1.2 Modem Settings

To use a modem for communicating requires setting the following during commissioning (see Section 7.2.2, particularly the handshake and baud rate settings):

- **`System Type`** **2 (Master) or 3 (Slave)**
- **`Connect Modem`** **Y**
- **`Baud Rate`** **Must match that set at CNC**

3.4 pIPer Units

pIPer serial Ethernet units can be used to connect a CNC with a door controller. Further information is given in *17407 pIPer Serial Ethernet Units*.

3.5 TCP/IP

The PAC 2200 Ver 2 door controllers can connect to an existing network via a TCP/IP interface.

The PAC 2200IP Series have a TCP/IP interface fitted in the door controller.

4. Appearance

4.1 PAC 2200 Series Door Controllers

All the door controllers in the series have a similar appearance with the main difference being in the number of reader channels and AEMs that can be supported.

Each controller can be ordered on a “skirt” or in a metal enclosure. In both cases, the unit comes complete with a power supply. It can also be ordered with or without a front panel (see Figure 11). However, at least one front panel is required for system programming. Figure 12 shows a door controller without a front panel.

The door controllers consist of:

- A printed circuit board and power supply both fitted to a steel baseplate.
- An optional, removable front panel fitted to the power supply and baseplate that connects to the circuit board via a ribbon cable.
- A memory module containing the database.
- A second, protective, “cover plate” sitting on top of the main circuit board. This cover protects the components on the main board and has a label that provides information on the connectors, status LEDs and so on.

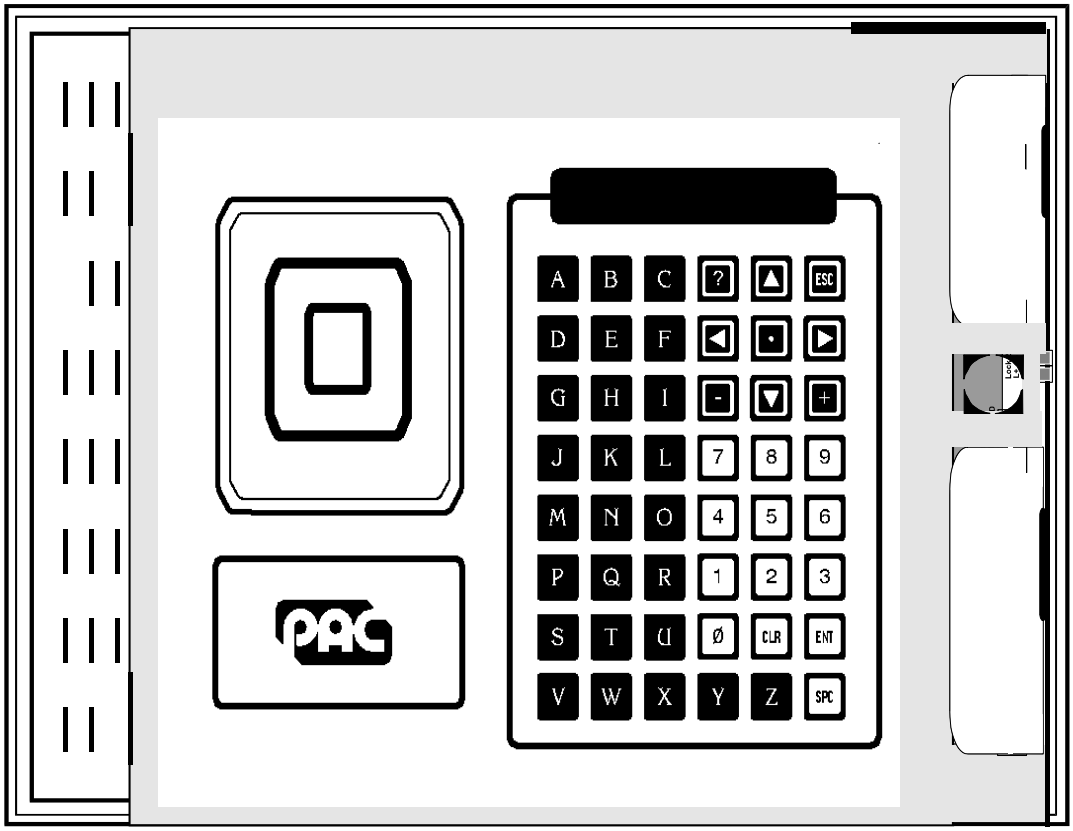


Figure 11 Door Controller with Front Panel

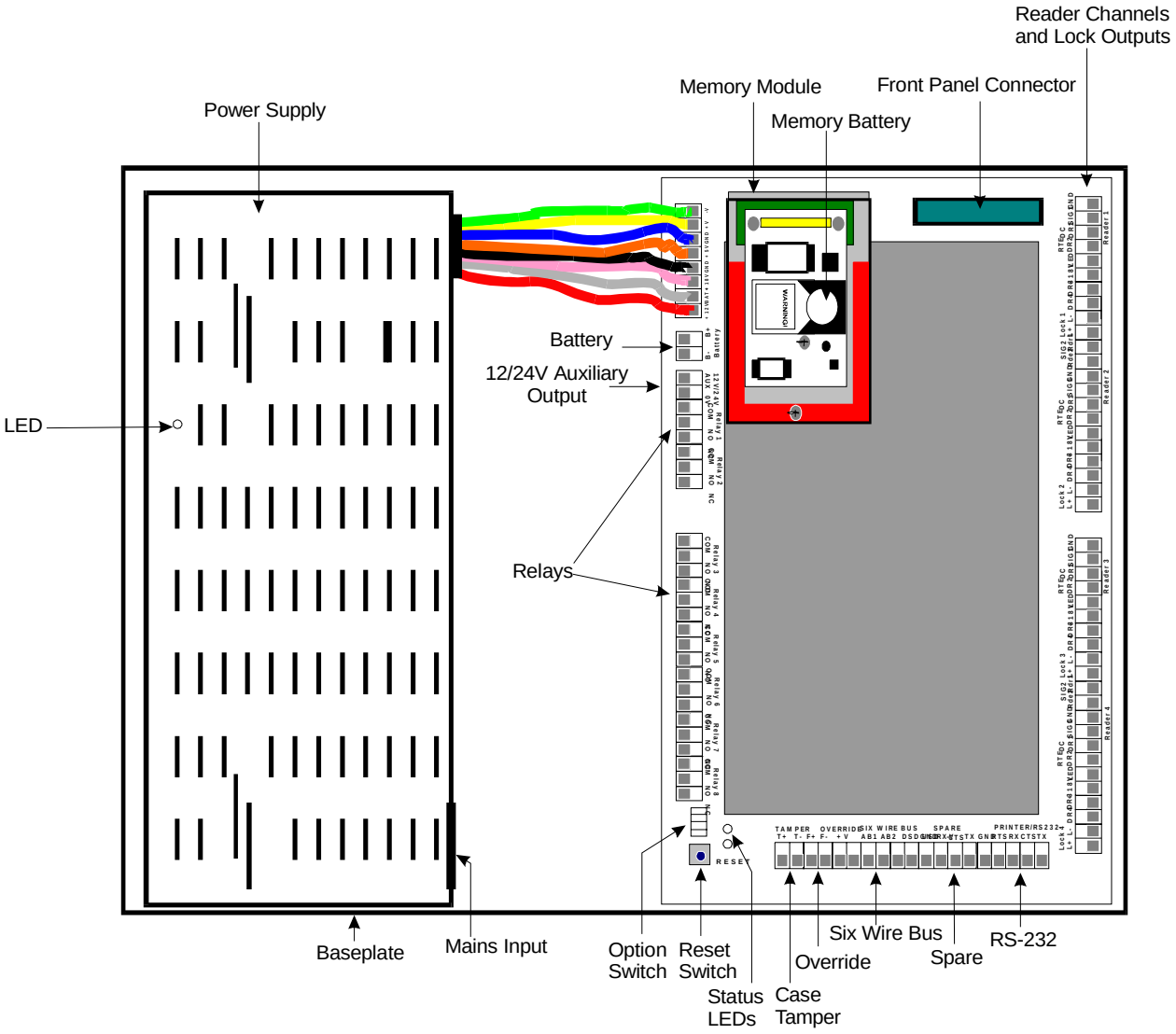


Figure 12 Door Controller without Front Panel

4.1.1 Power Supply

The metal-enclosured power supply unit is fitted on the left-hand side of the baseplate. This unit will automatically adjust to the local ac power supply, accepting input voltages between 85V ac and 250V ac at 50/60Hz. The power input uses a standard IEC connector; a right-angle socket is supplied.

The output from the power supply is fed to the circuit board by an 8-pole connector.

4.1.2 Front Panel

The removable front panel, if fitted, contains a key reader, a keypad and a 16 character display. The panel is secured by two tabs that fit into slots in the power supply on the left-hand side of the baseplate and by two spring clips on the right-hand side of the panel that attach to the baseplate. A ribbon connector plugs into a socket on the circuit board at the top right of the board.

The front panel and controller can be purchased as separate items but it is recommended that only slave controllers are purchased without a front panel. There should be at least one controller (master) on a site with a front panel.

4.1.3 Memory Module

This small board sits on top of the cover plate and contains the software and database memory. A small removable battery maintains the database memory for six months in the absence of mains or battery power.

4.2 PAC 2200IP Series Door Controllers

All the door controllers in the series have a similar appearance and are identified by their label. The PAC 2200IP Series have a fitted TCP/IP interface as shown in Figure 13. Cutouts in the cover allow LEDs and EPROM number and version to be seen. The Ethernet address is given on a label on the TCP/IP interface.

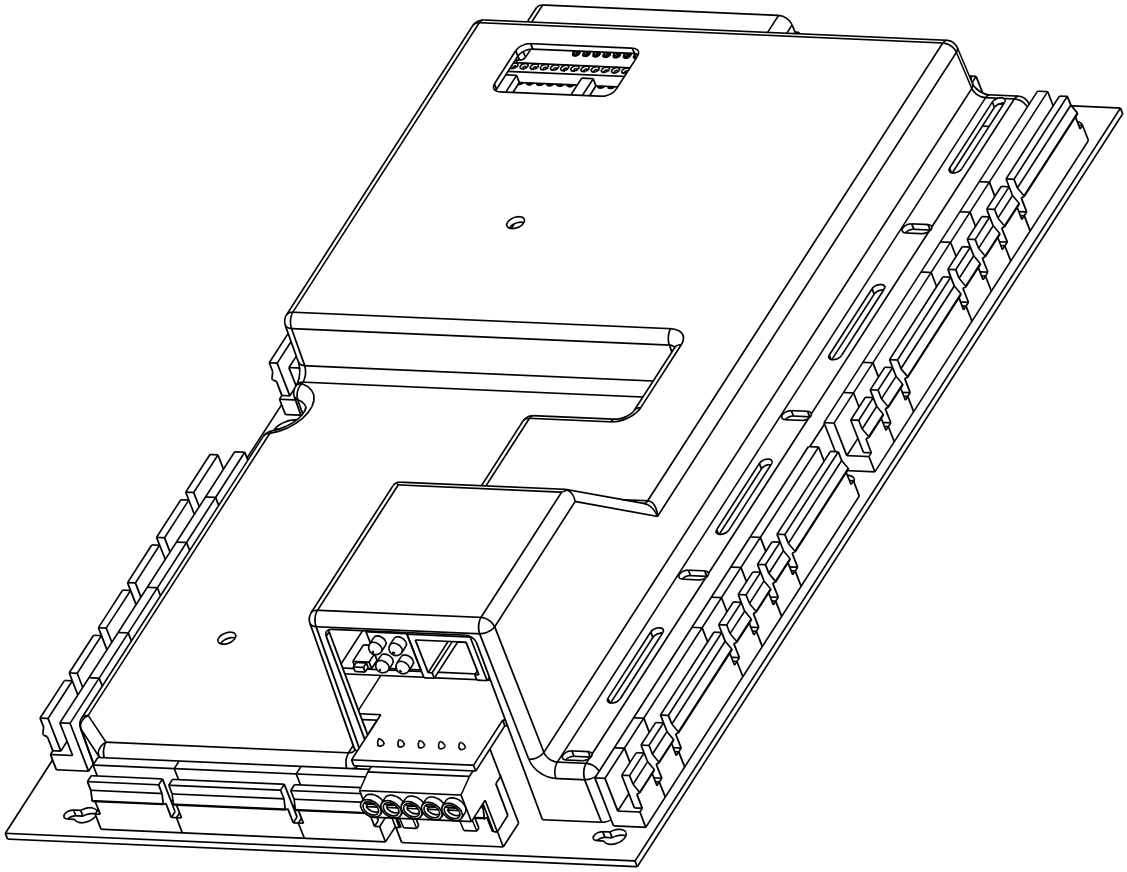


Figure 13 PAC 2200IP Door Controller with Cover

5. Installation

This is a brief outline of the steps that will be taken in the following sections that describe the installation, commissioning and testing of the door controller independently of the administration system.

It is possible to test all the reader and lock functions before making any network or communications connections. You are strongly advised to follow the order shown below. In this way you will be able to identify any problems before going on to the next stage.

1. **Install the Controller**, including fitting of the PAC metal enclosure if used.
2. **Install the Readers and Locks**, including door contacts, request-to-exit switches.
3. **Test the Readers and Locks**, etc.
4. **Make the Network Connections**, six wire bus and/or serial links where applicable.
5. **Connect to the Administration System**, PC interface kit, central network controller, modems, etc. where applicable.
6. **Commission the System**.

5.1 Installing the Controller

The door controllers may be fitted in the metal enclosure (part number 10260) supplied separately by PAC. Make sure that access can be gained to the door controller independently of the access control system itself.

If several door controllers are to be connected using the six wire bus, it is usually better to distribute the controllers so they are closer to the doors. This should reduce the length of cable needed for readers and locks.

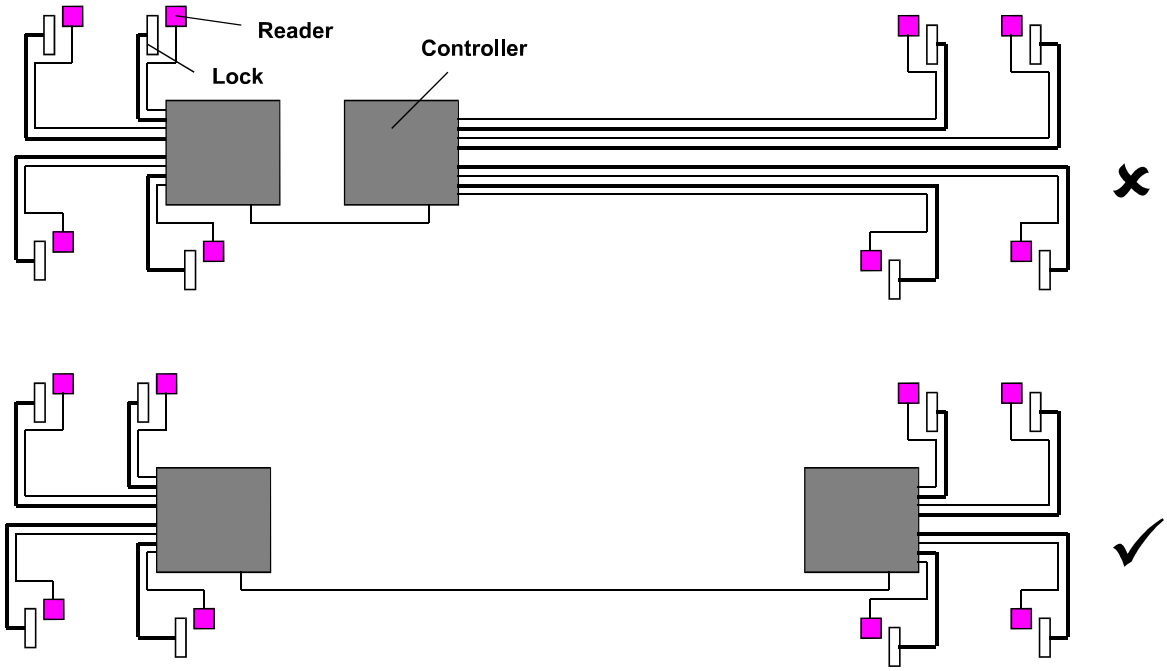


Figure 14 Recommended Wiring Layout

IMPORTANT

If the system is to be administered from the front panel, operators will be spending time programming at the controller. Therefore ensure that the controller is fitted in a suitably warm, dry and well lit location. The display should be at about eye level for most comfortable use.

5.1.1 Metal Enclosure

The door controller is contained in a metal enclosure. There are two metal enclosure options. The larger option allows room for AEMs to be fitted. Both options have space for two 12V 7Ah lead acid batteries if required. The metal enclosure dimensions for each option are shown in Figure 15 and Figure 16.

Note

Both options are UL approved.

The metal enclosure should be fitted to a wall using appropriate fixing screws. Use the central keyhole slot to hang the enclosure initially and use the remaining fixing holes as a template. There are several knockouts, shown in the following figures, provided for cable routing. Use conduit or trunking when bringing surface mounted cables into the enclosure.

Note

The metal enclosure is usually locked with only service engineers allowed access.

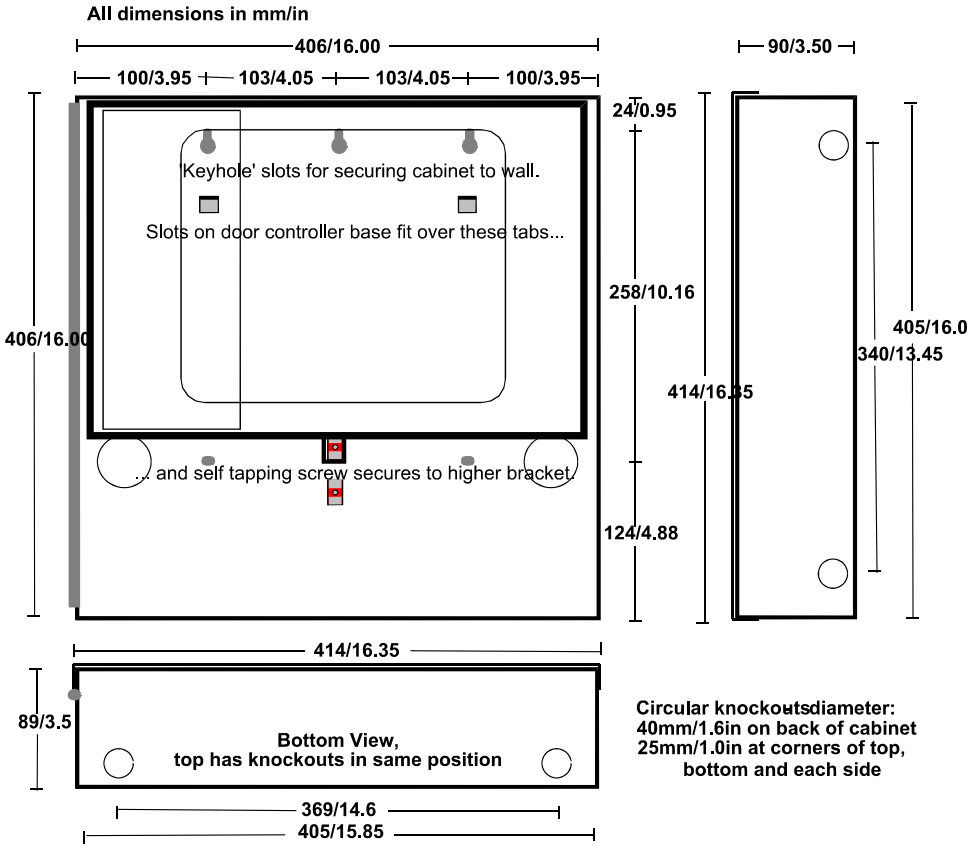


Figure 15 Metal Enclosure Option 1

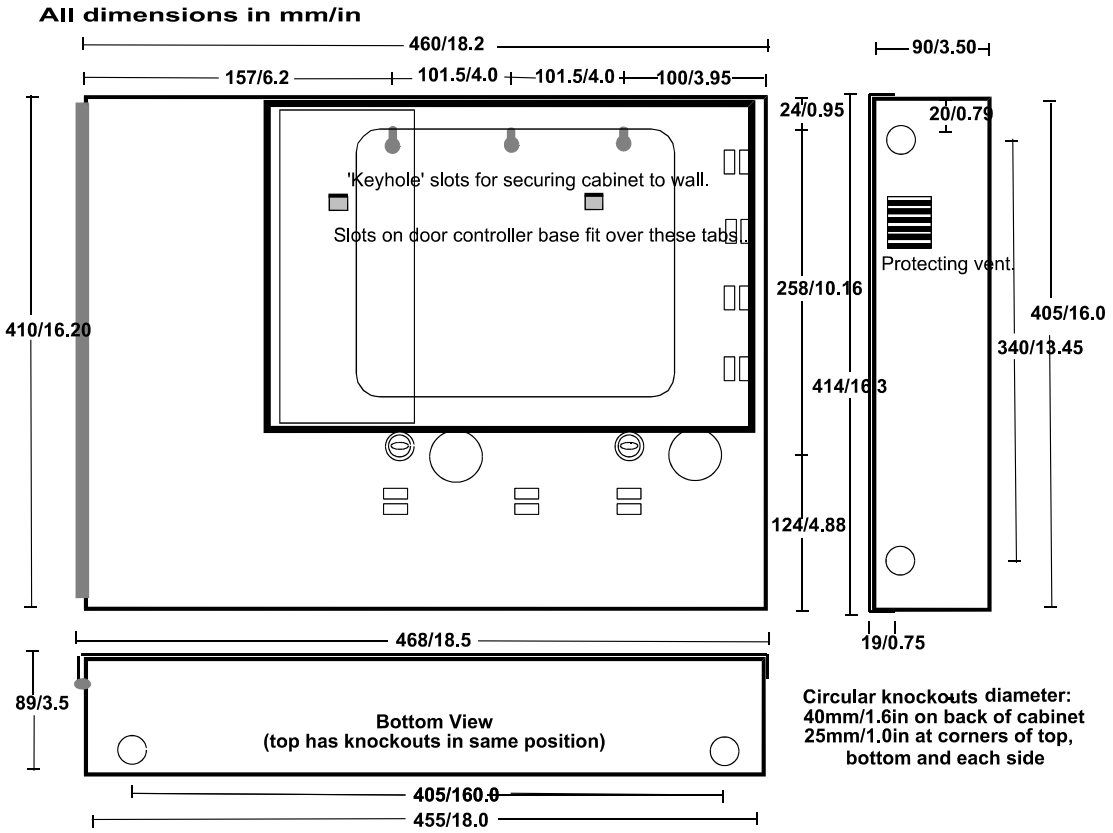


Figure 16 Metal Enclosure Option 2

5.1.2 Front Panel

The front panel is secured by two tabs that fit into slots in the power supply on the left-hand side of the baseplate and by two spring clips on the right-hand side that attach to the baseplate. The ribbon connector should be plugged into the socket on the circuit board at the top right of the board.

Note

When installing door controllers, be sure to check the lock output voltage before fitting the door controller in the enclosure. Check the switch, visible through the top of the power supply housing, is set for either 12V dc (factory setting) or 24V dc.

The door controller fits in the metal enclosure using two slots that fit over tabs on the back of the enclosure. You should ease the tabs on the enclosure forward slightly to make locating the door controller easier. The baseplate should then be secured using the single tab at the bottom of the baseplate using the self-tapping screw supplied.

5.1.3 Non-Standard Enclosure

The door controller can be fitted in an enclosure or cabinet other than one of the standard metal enclosures. Figure 17 indicates the position of screw slots and cable entry holes on the door controller.

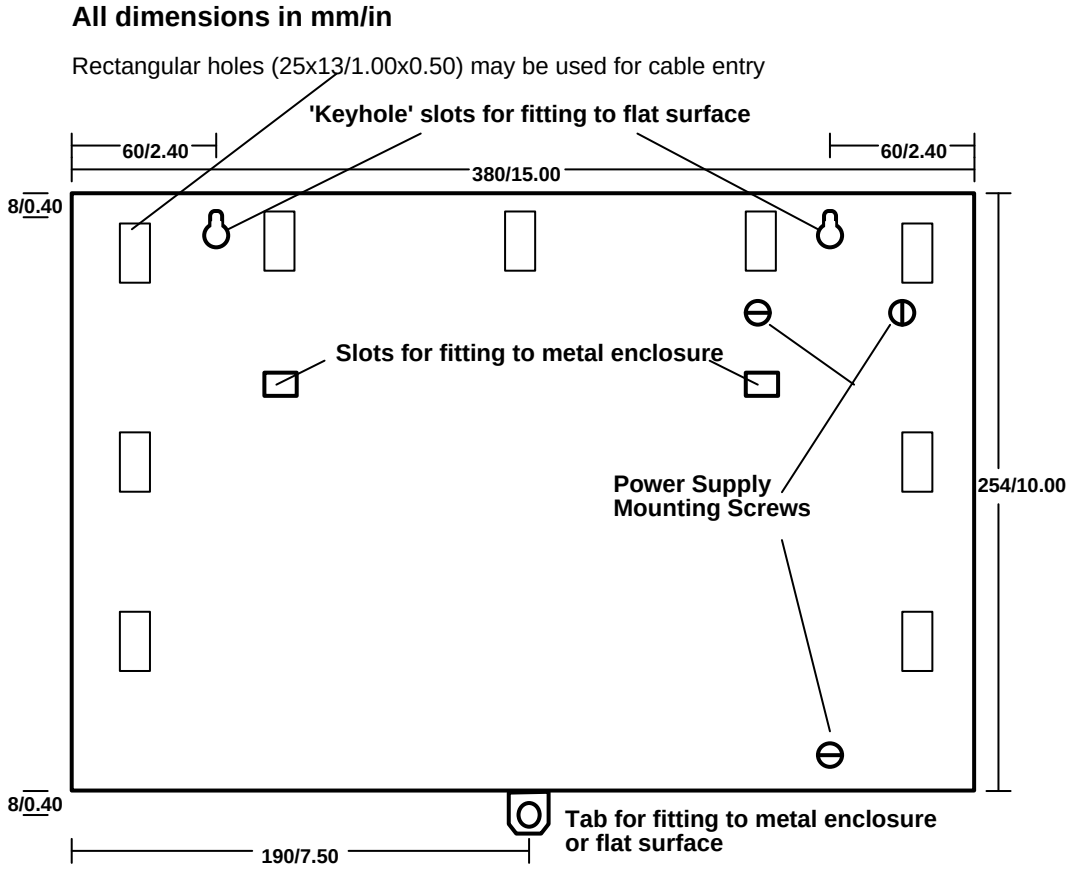


Figure 17 Rear View of Door Controller Baseplate

5.1.4 Power Supply

IMPORTANT

The database is stored in battery-backed memory and will be preserved whether the controller is powered or not. This backup will last up to 5 years provided that the controller is normally powered. The battery, located on the memory module, can be replaced without losing data. This is recommended every 3 years.

Note

The backup will be preserved for 6 months if the controller is not powered.

AC Supply

AC power, between 85V ac and 250V ac, 50/60Hz, should be supplied to the controller through an illuminated, unswitched outlet. A right angle IEC plug is supplied for wiring the mains lead.

WARNINGS

1. AN APPLIANCE OUTLET CAN ISOLATE THE UNIT BUT THIS LEAVES THE POWER CABLE LIVE; THEREFORE, THE ISOLATOR SWITCH **MUST** BE SWITCHED OFF BEFORE THE POWER SUPPLY UNIT IS OPENED.
2. THE INSTALLER **MUST** INCLUDE A LABEL ON THE POWER SUPPLY UNIT INDICATING THE LOCATION OF THE ISOLATOR SWITCH.
3. A GROMMET **MUST** BE FIXED TO THE HOLE THROUGH WHICH THE MAINS LEAD WOULD PASS. THIS IS TO PREVENT THE METAL ENCLOSURE CUTTING THE MAINS LEAD IF THE LEAD IS PULLED.

Power Indicator

A LED is situated within the power supply. It is visible through a small hole about 3in/75mm from the top on the left-hand side of the power supply case.

- If the door controller is operating off the mains supply, whether the battery is connected or not, **the LED will be lit**.
- If the mains supply fails and the unit is running from the backup battery, **the LED will be extinguished.**

Note

Always power up the controller using the main supply. This will activate the controller battery charging facility. Once this is done, ac power can be removed and the controller will operate from battery backup

5.1.5 Lock Output Voltage

The lock output voltage is set for all doors on the controller using a switch accessible through the top edge of the power supply. The controller has a power supply, 4A (PS80) or 8A (PS159), providing a (total) lock output of 48VA and 96VA respectively.

You can “mix and match” locks provided you do not exceed the maximum allowed for the power supply.

5.1.6 Battery Backup

The 12V 7Ah battery (if in a fully-charged, good condition) provides approximately 2.0 hours of standby time for a fully loaded system.

A battery charging facility is available that can provide up to 0.5A at 13.8V dc or 0.25A at 27.6V dc.

5.1.6.1 Door Controllers

IMPORTANT

The battery backup voltage **must** match the lock output voltage, i.e. 12V or 24V. You may use two 12V batteries in series to provide 24V dc.

The capacity of the battery required should be calculated based on:

- The current consumption of the door controller (1A).
- The current consumption of the devices attached to the reader channels (up to 800mA).
- The current consumption of the locks when operating normally (up to 2A each).
- The type of lock, continuous (fail-safe) or intermittent (fail-secure).
- The length of time the system should operate without mains power.

The following tables will help you estimate the current.

Lock Supply Current

For continuous, or fail-safe locks the continuous lock supply current is the current drawn by the lock. For fail-secure locks, however, you need to estimate the equivalent continuous current by using the following equation:

CLC=(Lock Current Rating x LRT) x NOP / 3600

where

CLC = Equivalent Continuous Lock Current
LRT = Lock Release Time (in seconds)
NOP = Number of Operations per hour

The lock current rating should be indicated in the lock specification.

Example

A 500mA lock strike with a 5 second lock release time, operating 50 times an hour would give:

CLC=(500 x 5) x 50 / 3600 = **35mA**

Note

If you have any doubt about the current drawn by a lock, you should measure it at the controller using a meter.

The maximum current that should be drawn from each lock output is:

2.0A at 12V dc
1.0A at 24V dc

Note

This is halved if you are using the 4A PSU (PS80).

In the table below record the type and current consumption of each lock fitted:

Channel	Type: Continuous/Intermittent	Continuous Lock Current
1		
2		
3		
4		
	Total	

Table 1 Continuous Lock Supply Current

Reader Supply Current

There is a maximum of 200mA available per reader channel on the 18V supply. PAC readers of all types draw approximately 90mA each continuously. If you fit Alarm Modules or AEMs, a reader combiner or Wiegand interface unit, ensure that the maximum current available, 800mA, is not exceeded.

In the table below record a current consumption for each device fitted:

	Channel				
	1	2	3	4	
Reader Current 1 35mA (see Note 1)					
Reader Current 2 100 mA (see Note 2)					
Wiegand/Magstripe Reader 50 mA					
Module Relays 30 mA					
Total					Must not exceed 200mA/channel

Table 2 Total Reader Channel Current

Notes

1. Reader current 1 applies to the standard plus, slimline readers and vandal resistant reader MKII (flying lead) (15mA idle, 35mA active).
2. Reader current 2 applies to the low profile reader, vandal resistant reader MKI (terminals) and panel mount reader.
3. When using a reader combiner, you should include the current of the combiner in its column plus the total current for both readers in the reader column.
4. Only include a value for the reader current if the Wiegand reader is powered from the Wiegand interface unit's 5V output or the 18V reader supply.
5. Include 40mA for each AEM that is connected to a reader channel.

Total Power

The door controller itself consumes 1A before the addition of any readers or locks.

For each 100mA of reader channel current, as determined above, an additional 150mA should be allowed. This is due to several factors involved in the generation of the 18V dc supply.

Door Controller	1	Amp
Total Continuous Lock Current, see Table 1		Amps
Total Reader Channel Current, see Table 2		Amps
Total Current Requirement		**Amps**

Note

The above figures are all stated in Amps, 1A = 1000mA.

5.1.6.2 Standby Battery Requirement

IMPORTANT

For door controllers, the battery voltage should match the lock output voltage.

Now that you know the total continuous current requirement of the door controller plus readers, locks and ancillaries, you should multiply this figure by the number of hours standby needed.

In the enclosure supplied, there is room for two 12V 7Ah batteries. If this does not provide sufficient backup, the batteries must be located outside the enclosure or the controller fitted in a larger enclosure.

Example

A door controller with a continuous current of 2A will require at least a 4Ah battery to provide 2 hours cover (2A x 2 hours = 4Ah).

IMPORTANT

The Ah rating of a battery is usually determined when discharged over a 10 or 20 hour period. If a fully charged battery is discharged over a shorter period than this, as in the example above, it will last for less time than its rating suggests. You should consult the battery manufacturer's correction factor charts to determine a more accurate figure. This means you will probably need a higher rated battery than expected.

5.1.6.3 External Charger

In order that a fully discharged battery can recover to a fully charged state within 24 hours, consider using an external charger when using more than a 7Ah battery. Use the wiring shown in Figure 18.

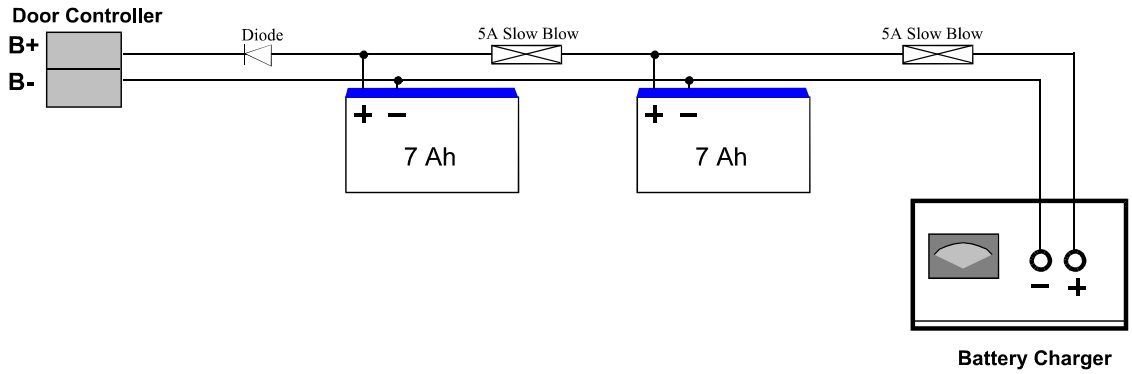


Figure 18 Using an External Battery Charger

The battery charger unit has to provide a trickle charge at the same voltage as the controller power supply. If the controller's power supply is set for 12V dc, the battery charger unit must provide a trickle charge at 13.8V dc. If the controller's power supply is set for 24V dc, the battery charger unit must provide a trickle charge at 27.6V dc.

Notes

1. If the battery charger and the door controller are not set to the proper output voltages as described, the door controller could be damaged.
2. It is recommended that a battery low-voltage isolator be fitted to each battery to monitor the battery and prevent deep discharge.
3. It is recommended that a diode is installed as shown in Figure 18.

5.1.7 External Reader

An external reader can be connected to the front panel. The external reader can be used in addition to, or in place of, the built-in reader for administration purposes. For example, if a standalone system uses PAC and KeyPAC readers but the built-in reader is PAC then a KeyPAC reader can be connected as an external reader.

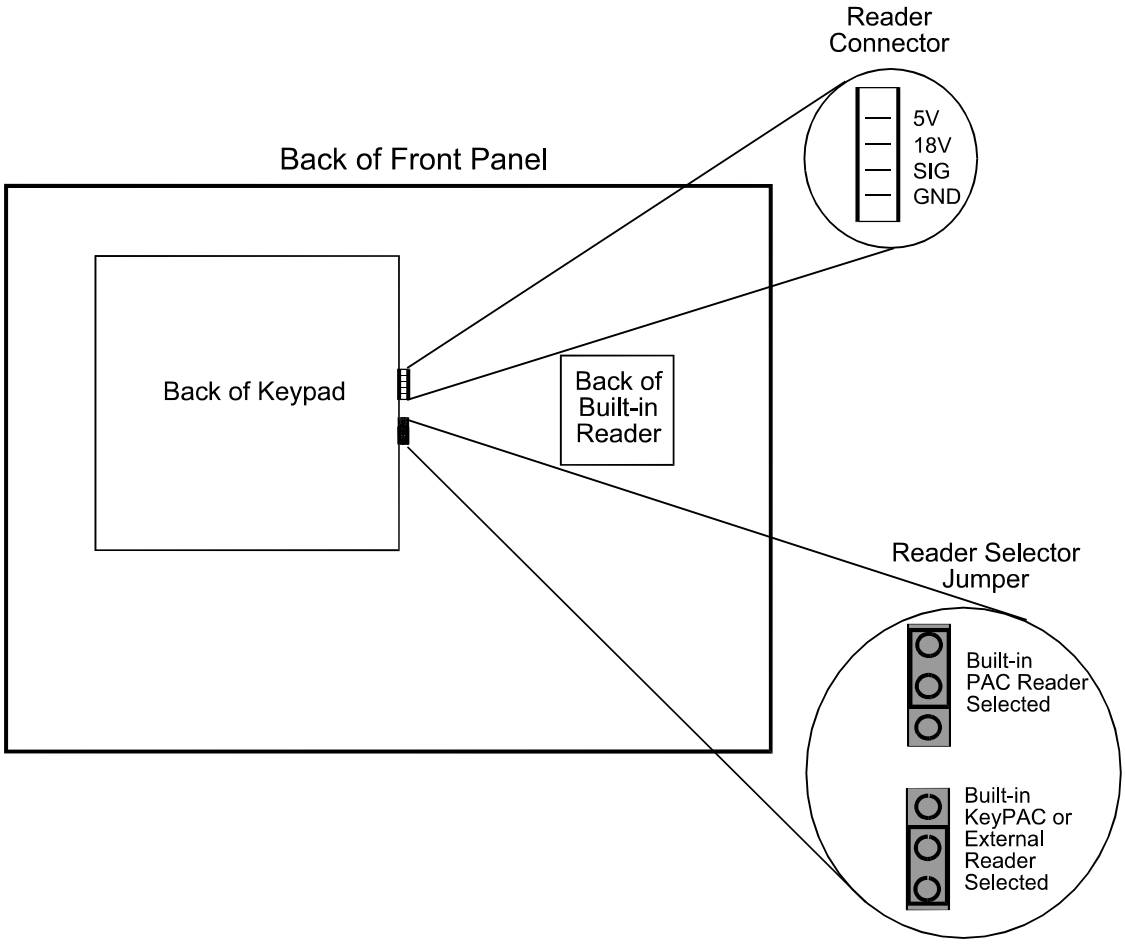


Figure 19 External Reader Connection

Notes

1. The jumper should be set for built-in reader or external reader as required.
2. When using the built-in reader, the connector from the built-in reader should be connected to the reader connector.
3. When using the external reader, a 2.54mm pitch Molex 4-way connector from the external reader should be connected (use the 5V or 18V power output as appropriate, see the documentation supplied with the reader).
4. When the external reader is a Wiegand reader, a Wiegand interface unit is required (see *17132 Wiegand Interface Unit Installation Instructions*).

5.2 Installing Readers and Locks

All the features described below can be programmed and tested, where necessary, at the front panel. Details of how to do this are given in *17267 PAC 2200 Series Controllers User Guide*. However, if the door controller is going to be administered from a PC, these features must be programmed at the PC as well. It is advisable to use the front panel to test the installation of the door controller, readers and locks and then, once communications are established, initialise the door controller and program the features at the PC.

How to fully commission a PC-based system is described in the documentation supplied with the administration software.

Use the most appropriate reader for the location bearing in mind, internal or external, vandal resistance, decor, panel mounting, etc.

See the documentation supplied with each reader for specific details for fitting that type of reader.

5.2.1 General Information

5.2.1.1 Locating a Reader

Be aware of the following when choosing the location of a reader:

- The readers are not suitable for mounting on surfaces containing metal. Readers can be mounted behind a non-metallic material such as glass, plastic or wood without affecting their reading range.
- Readers may be located inside or outside. Corrosion-resistant fixings should be used and a silicone sealant applied to the terminals to protect against damp.
- The cable distance from controller to reader should never exceed the distances given in Section 10.3. Also consider the maximum distance between the controller and the lock.
- If using a **Request to Exit** (RTE) switch, route the wiring so that it is not accessible if the reader is removed.
- Ensure that the LED is visible to the keyholder and avoid mounting the reader in direct sunlight.
- The best place for a reader is next to the door on the unhinged side at roughly the same height as the door handle.
- If the reader has a flying lead, leave enough room for it behind the reader.
- There should be a minimum 3ft/1m distance between readers (this includes in and out readers on opposite sides of a door).
- Readers can read in the same way from their back as they do from their front. Because of this, ID devices may work from the other side of the wall on which the reader is mounted.
- Consider future service requirements such as access to cables, etc.

5.2.1.2 Installing a Reader

1. Ensure that the reader cable is **not** connected to the controller.
2. Wire the cable as described in Section 5.2.1.5.
3. If the connections are in a location that may be damp, protect the connectors with a sealing compound, or use weatherproof crimps.
4. Using appropriate fixings, such as wall plugs, for the surface the reader is being mounted on. Install the reader on a flat surface using the screws provided or corrosion-resistant screws for locations that may be damp. Use the round hole first, then the oval hole to ensure the reader is straight.

5.2.1.3 Reader Channels on Door Controllers

Each reader channel on the controller is labelled as follows:

PAC 2200 Series	PAC 2200IP Series	Description
GND	GND	0V supply.
SIG1	SIG1	Signal from in reader.
DC/DR1	DC	Door contact for door monitoring.
RTE/DR2	RTE	Request to exit switch.
LED	LED	Valid Code Accepted (VCA). Illuminates the green LED at the reader when a valid key is presented.
+18V	+18V	18V supply.
DR3	INHB	Arm/disarm alarm areas or arming button connection.
DR4	ALM	Alarm state input.
L-	L-	Negative lock connection.
L+	L+	Positive lock connection.
RDR1/ RDR3	RDR1/ RDR3	**Channels 1 and 3 only.** Signal from out reader.
RDR2/ RDR4	RDR2/ RDR4	**Channels 1 and 3 only.** Signal from out reader on the next door.

5.2.1.4 Reader Cabling

Use unshielded, multi-stranded, tinned copper signal cable, the type commonly used in alarm installations. A minimum of 6-core, 24AWG/0.22mm², cable is required (reader, request to exit and door contact). It is recommended that 8/12-core cable is used depending on requirements. For example, some readers have a sounder which require an additional core to make use of the feature.

The maximum reader cable length depends on both the reader type and cable gauge as detailed below. For example, the cable length for the slimline and standard plus readers is:

Up to 750ft/250m	24AWG/ 0.22mm²
Up to 1500ft/500m	20AWG/0.50mm²
Up to 3000ft/1000m	18AWG/1.00mm²

Full details are provided in the documentation supplied with each reader.

Four conductors are used to connect the reader itself, the other conductors can be used for the optional request to exit and door monitoring signals (see Sections 5.2.2.1 and 5.2.2.2).

The readers are not prone to electrical interference, however avoid routing cable close to heavy load switching cables and equipment. If this is unavoidable, cross the cable at right angles every 3.3-6.6ft/1-2m.

5.2.1.5 Reader Connections

Proximity readers have a 6-core flying lead or 4 terminals (+V, VCA, SIG and -V). Each reader is connected to one of the reader channel terminal blocks on the door controller. Each reader channel has 2 further connections, DC and RTE. These provide door/cable monitoring and request to exit inputs respectively.

Readers with Terminals

Connects to Controller	Reader Marking	Description
6-pole terminal block	screw terminals	
GND	-V	0V supply.
SIG1	SIG	Reader to the controller.
DC		Door monitoring.
RTE		Request to exit.
LED	VCA	Valid code accepted, illuminates the green LED at the reader when a valid key is presented.
+18V	+V	18V supply.

Readers with Flying Leads

Connects to Controller	Colour	Signal	Description
6-pole terminal block			
GND	Black	-V	Power and signal return
	Yellow	SNDR	Sounder input, active low. Pull to ground to activate sounder
SIG1	White	SIG	Signal output. Connect to door controller reader channel SIG.
-	Green	DR2	Not used
LED	Brown	VCA	Valid code accept, operates LED. Connect to door controller reader channel, LED.
-	Blue	DR1	Reader tamper connection (not required on the PAC door controllers)
+18V	Red	**+**12V	Unregulated 12V dc input 9-28 V dc, 35 mA Max
	Orange	**+**5V	Regulated 5V dc input, 35mA Max

Note

If an in/out reader is being used, the **SIG** from the out reader connects to the relevant **RDRn** connection, see Figure 21.

5.2.2 Reader and Request to Exit

The door controllers have either four or two reader channels. Each reader is wired independently using up to 3000ft/1000m of 6-conductor cable.

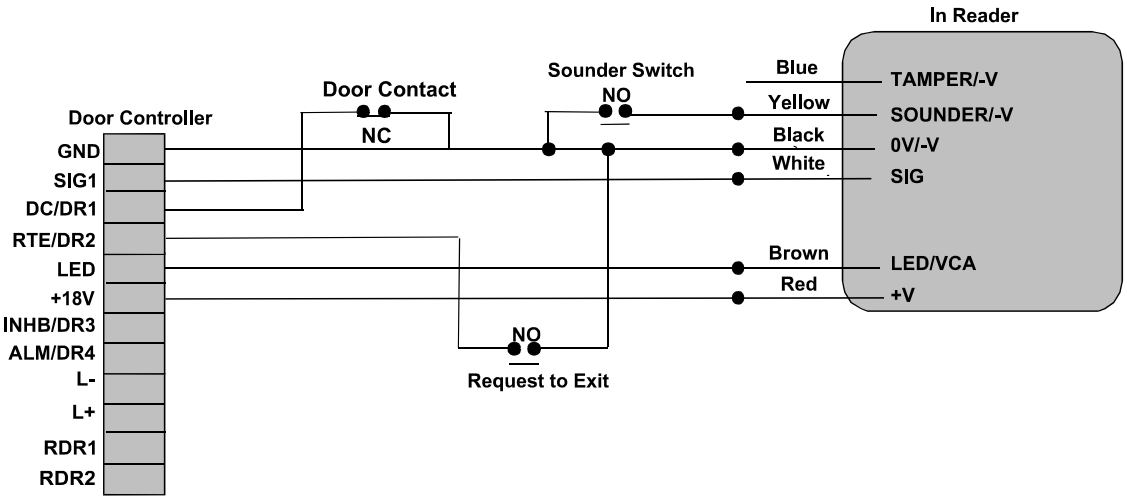


Figure 20 Reader with Request to Exit and Door Monitoring

The door contact is not required if door monitoring is not needed.

5.2.2.1 Request to Exit

If a **Request to Exit** switch is used, it will allow people within the area to leave by signalling the door controller to operate the lock without using a key. The switch is necessary when door monitoring is used (see Section 5.2.2.2) to enable the controller to distinguish between a forced door and a valid exit. The switch should be 'normally open' which closes momentarily when pressed.

Connecting RTE to ground (GND) will always operate the lock; ensure that the request to exit wiring is not accessible from outside the area (e.g. if the reader is removed from the wall, the request to exit wiring should not be exposed).

Notes

1. It is possible to locate the switch away from the door, at a reception desk or as part of a door entry system. In which case, it is possible to change the event report to `Request for Entry`.
2. More than one switch can be used if wired in parallel.
3. If an attempt is made to keep the door open by holding down the **Request to Exit** switch then the door will lock after 5 cycles of the lock release time and an `RTE Button Held Down` report is produced.

5.2.2.2 Door Monitoring

The door controller has the ability to monitor a door contact if a door contact is fitted:

- **Unauthorised Access Alarms** giving warning of a forced door.
- **Door Left Open Warning** after a set period of time. The time is set when the controller is programmed.
- **Cancellation of Lock Release Time** allows the door to lock after someone has passed through even though the lock release time has not expired.

The door contact should be a normally closed switch that is open whenever the door is open. Care should be taken when fitting door contacts to ensure that they operate only when the door is opened and close only when it is secure again.

To help prevent false alarms:

- Keep reed switches away from large magnetic fields, such as those generated by magnetic locks. This is a particular problem with metal door frames.

- Ensure that the switch does not operate if the door moves in its frame, in draughty or windy conditions.
- An efficient door closer should be fitted that secures the door once someone has passed through.

5.2.3 In and Out Readers

5.2.3.1 Without Arming

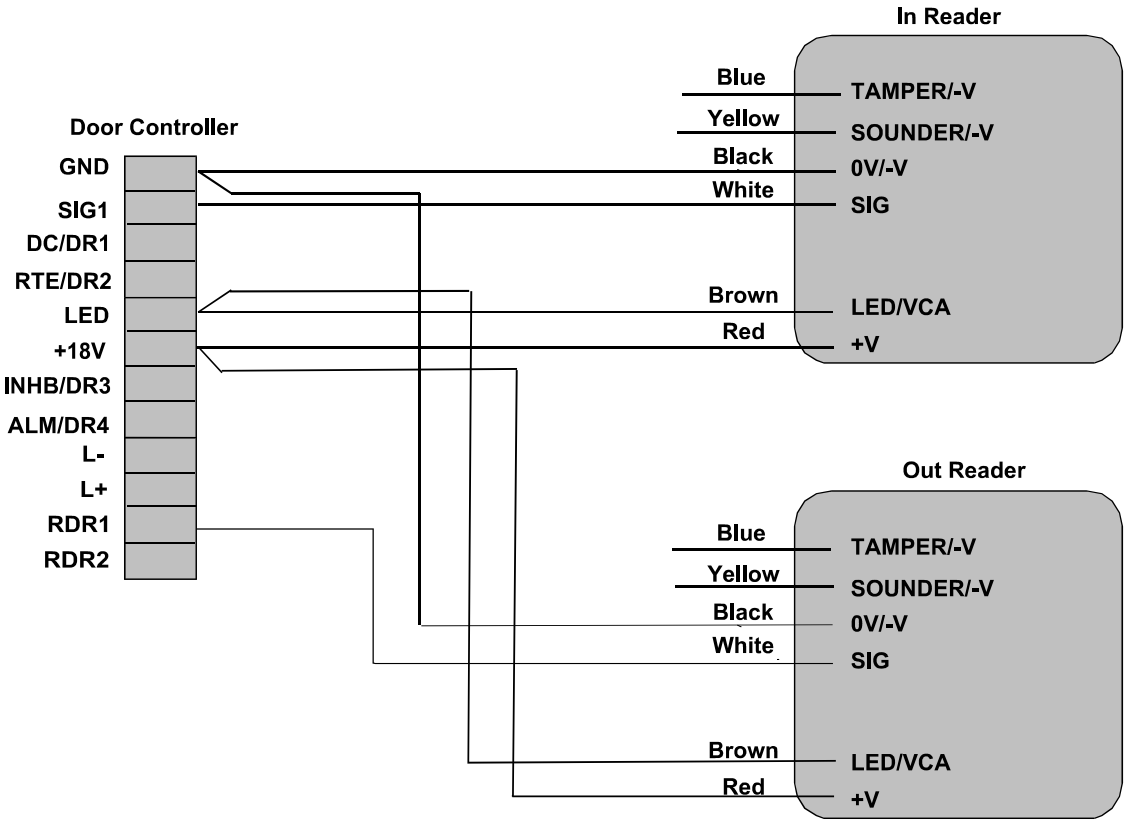


Figure 21 In/Out Readers Without Arming/Disarming

Only one Wiegand/Magstripe reader can be used either as the in or out reader.

If you are using Wiegand or Magstripe readers and require in/out readers, you **must** use a Wiegand interface unit for each reader. Call PAC Technical Support for details.

5.2.3.2 With Manual Arming/Disarming

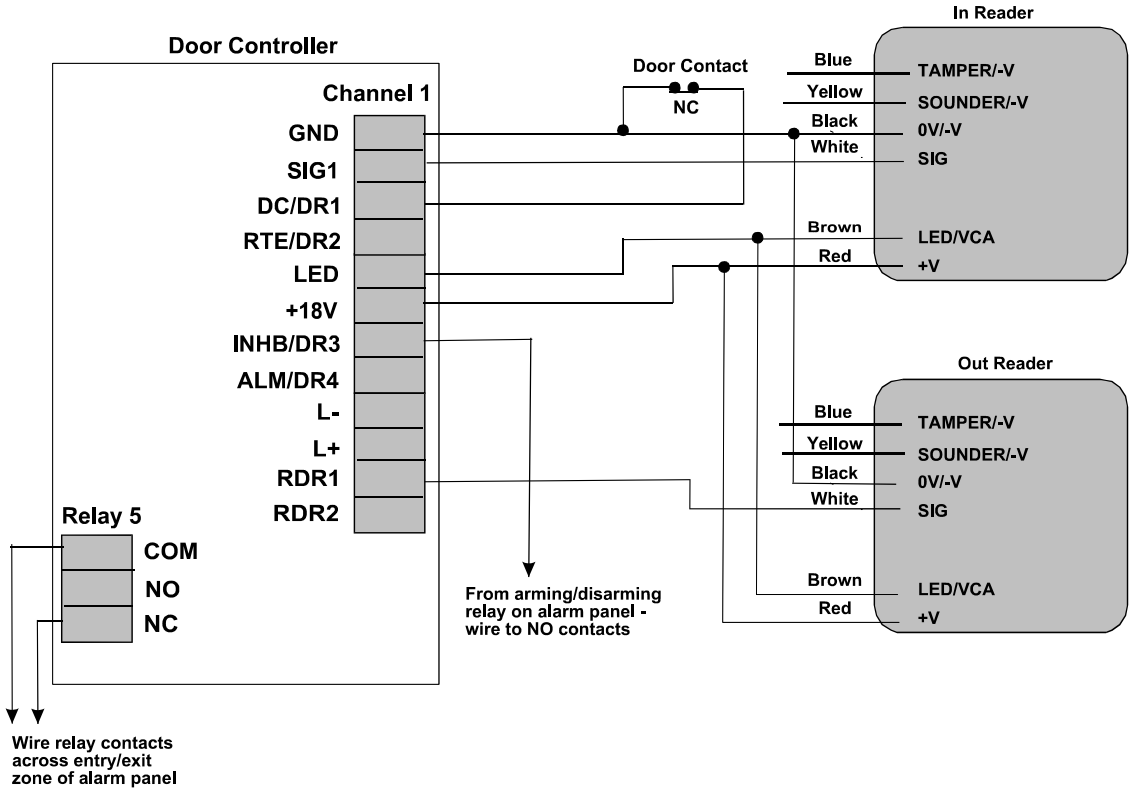


Figure 22 In/Out Readers With Manual Arming/Disarming

5.2.3.3 With Automatic Arming/Disarming

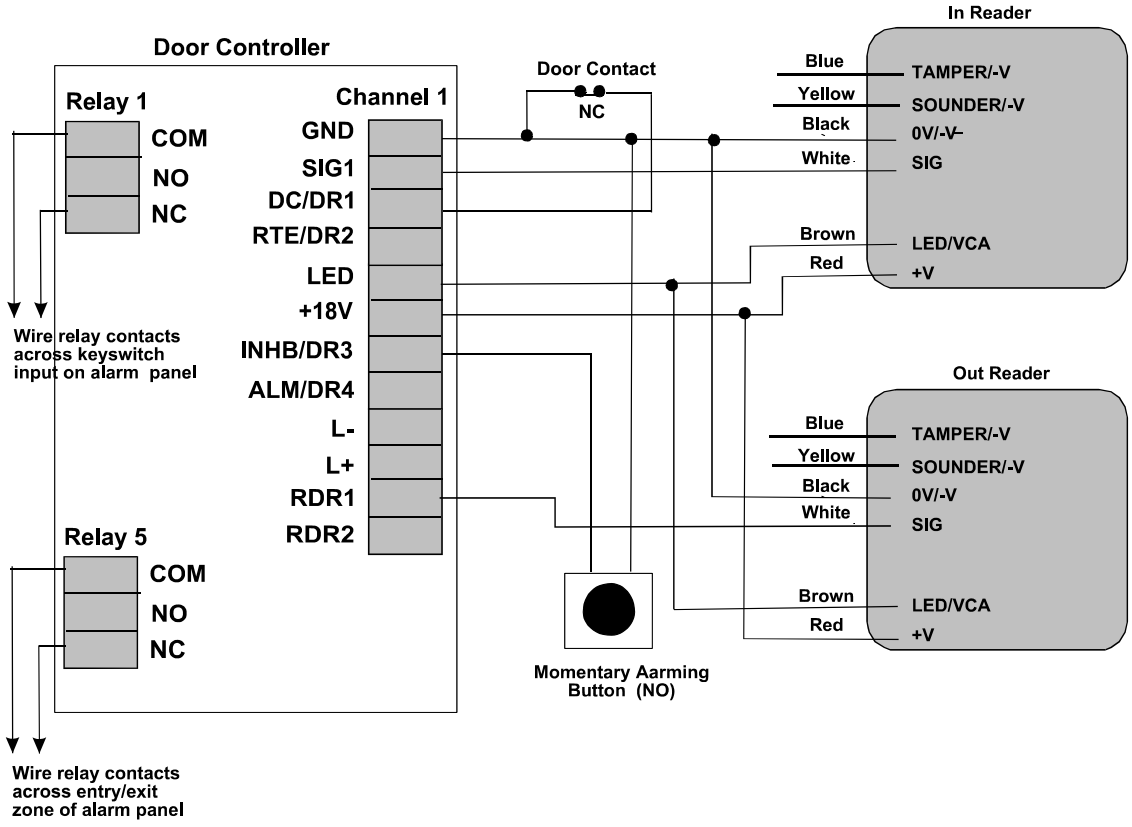


Figure 23 In/Out Readers With Automatic Arming/Disarming

It is recommended to use a PIN reader for extra security in case a key is lost.

5.2.4 Emergency Override/Free Exit

There is a special case where both the RTE and DC signals are interpreted differently to the way described for door monitoring in Section 5.2.2.2. The RTE signal is used to monitor an emergency switch, such as a break glass, and DC provides a `Free Exit` report.

Note

When this feature is used there is no door monitoring**.** For details on how to enable this feature, see the **D** command in *17267 PAC 2200 Series Controllers User Guide* or to the documentation supplied with the administration software.

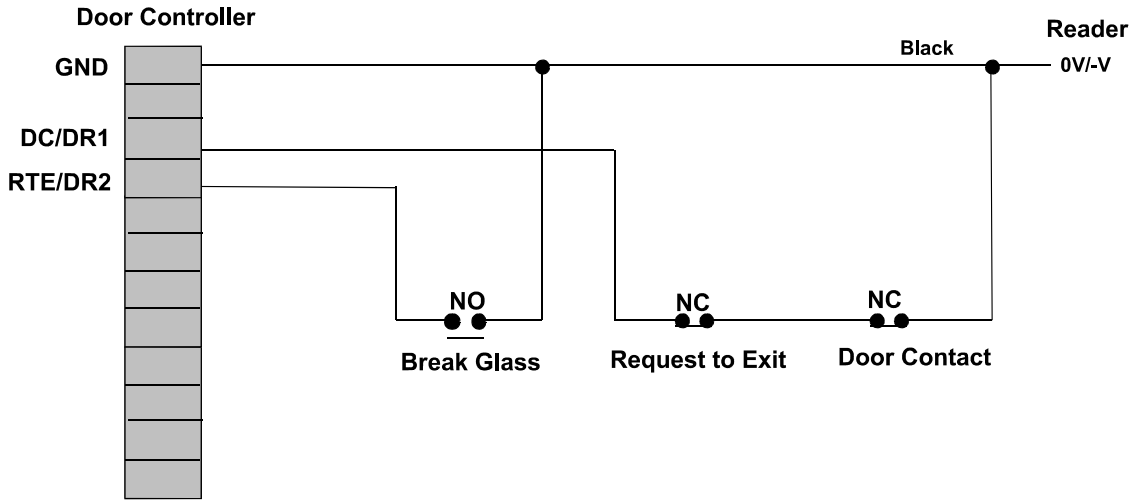


Figure 24 Emergency Override / Free Exit Wiring

Emergency Override

When connected as shown in Figure 24, operating the break glass will open the door and generate an `Emergency Override On` report. When the switch is restored, the controller will re-lock the door and generate an `Emergency Override Off` report.

WARNING

THIS FEATURE SHOULD NOT BE FITTED AS THE SOLE MEANS OF ESCAPE.

Free Exit

When this option is set, pressing the **Request to Exit** switch will produce a `Free Exit` report. The door contact will allow door left open warnings to be produced.

A normally closed switch may be used to operate as a request to exit switch, in addition to having a door contact switch in series (see Figure 24).

Notes

1. Using this arrangement, the lock will operate whenever DC is opened - this means that care should be taken that the door contact cannot be broken from the secure side of the door.
2. As free exit was designed to work with a door contact or pushbar the door contact “bounce time” is applied and the response will be slow if used like an **Request to Exit** switch (1.25 seconds).
3. For details on how to enable this feature, refer to the documentation supplied with the administration software.

5.2.5 Lock Output

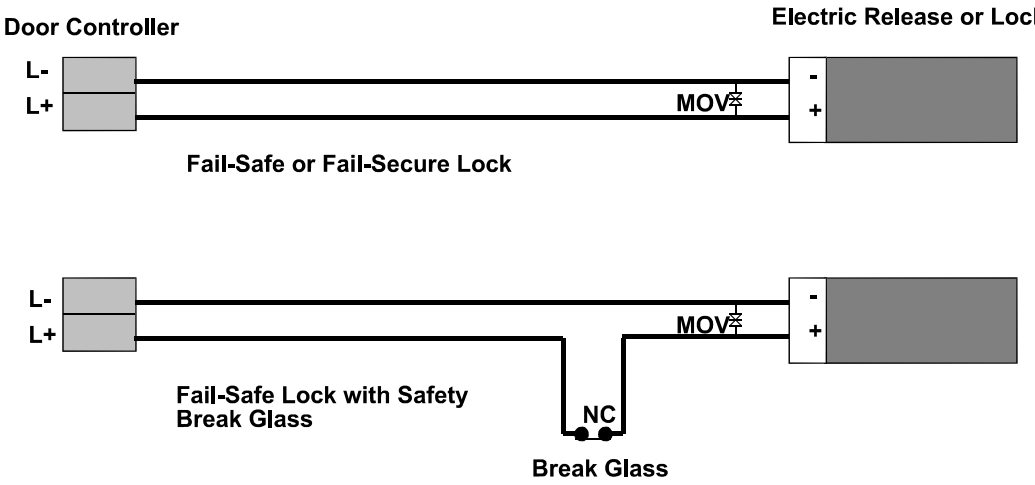


Figure 25 Lock Output Wiring

All locks should be fitted according to the manufacturer's instructions.

The door controllers provide a lock output for each reader channel. These outputs are capable of providing either 12V dc or 24V dc. The lock output on each channel must not be able to exceed 1.0A at 12V dc or 0.5A 24V dc. The lock voltage is set using a switch accessible through the top of the power supply unit.

Each lock output is protected by resettable fuse on the controller. Two status LEDs are also provided for each lock output.

The **red LED** indicates when the door controller is requesting power to be supplied to the lock output, this depends on the lock mode set. For fail-safe locks the **red LED** will be on until the lock is released by a valid access. For fail-secure locks the **red LED** will be off until the lock is released by a valid access. The **green LED** normally follows the **red LED** and indicates when power is actually reaching the lock.

If the **red LED only** is on, power is not reaching the lock even though the door controller has requested it. This indicates that the over-current circuit has tripped, perhaps due to a faulty lock or short-circuit on the lock output. It should not be possible for a **green LED** to light without the **red LED**. If this occurs, there is a problem with the controller hardware.

During normal operation the LEDs operate as follows:

- **Fail-Safe Locks**. Both the red and green LEDs are normally on. When a valid key is presented to a reader, both LEDs go off for the duration of the lock release time.
- **Fail-Secure Locks**. Both the red and green LEDs are normally off. When a valid key is presented to a reader, both LEDs come on for the duration of the lock release time.

Each output can be independently set as fail-safe (power to lock) or fail-secure (power to unlock).

The cable between the door controller and the lock should be of such a gauge as to provide at least the minimum voltage required to operate the lock. The resistance of the cable and the current drawn by the lock will determine the type of cable.

5.2.5.1 MOV - Lock Suppression

All locks **must** be fitted with a means of suppressing back Electro-Motive Force (EMF) 'spikes' generated by most electric releases, especially magnetic locks. All PAC door controllers and readers are supplied with Metal Oxide Varistors (MOVs). If large currents are used (i.e. >1A) use the large MOV supplied with the door controller. If small currents are used (i.e. <1A) use the small MOV supplied with the reader.

The MOV will prevent long term damage being done to the door controller. Whenever possible this device should be fitted across the lock terminals. If for any reason, the lock terminals are inaccessible, the MOV may be fitted across the lock output.

Note

The total current for all lock outputs on the door controller should not exceed the rating of the power supply, see the following table:

Power Supply Type	Voltage Switch Setting	Total Output for 4 locks
Light-duty power supply (no fan)	12V	4A
Light-duty power supply (no fan)	24V	2A
Heavy-duty power supply (fan visible)	12V	8A
Heavy-duty power supply (fan visible)	24V	4A

5.2.5.2 Safety

Any door that is considered a fire door or is on an escape route **must** have some means of overriding the electric release in an emergency. Usually this is achieved by the use of fail-safe locks (power to lock) fitted with a normally closed break-glass **in the lock supply**. When the break-glass is operated, the supply to the lock is broken and the door will be released without any intervention from the door controller.

5.2.6 PIN Reader

A PIN reader requires a 4-digit personal identification number to be entered after presenting a valid key to a reader. A PAC PIN reader that has a built-in PAC reader and keypad can be connected to a door controller as shown in Figure 26.

Notes

1. If an external reader (e.g. a KeyPAC reader) and/or external keypad is required, a PC interface unit replaces the PAC PIN reader, see the documentation supplied with the PIN interface unit.
2. It is possible to set a time profile so that a PIN is not required at certain times (e.g. during the office hours) but is required at all other times. For details on using time profiles with a PIN reader, see *17267 PAC 2200 Series Controllers User Guide* or the documentation supplied with the administration software.

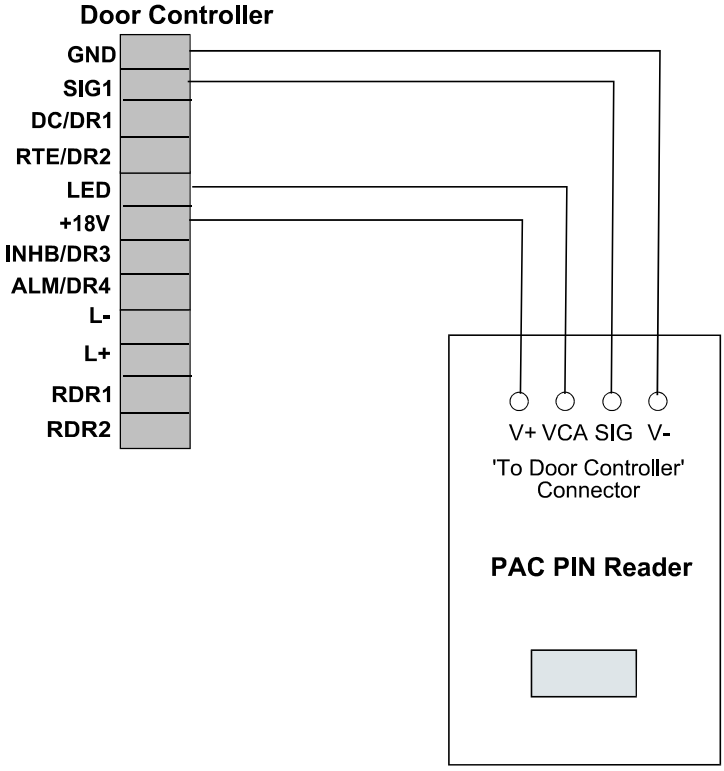


Figure 26 PIN Reader Wiring

5.2.7 Wiegand Readers

Wiegand readers with open collector D0, D1 can be connected to a PAC 2200 Series Door Controller as shown in Figure 27.

Notes

1. If the Wiegand output signals do **not** conform to the Security Industry Association Access Control Standard Protocol for Wiegand, a Wiegand interface unit is required, see *17132 Wiegand Interface Unit Installation Instructions.*
2. If the reader meets the above standard but has a signal output of 5V dc or 12V dc or has an output voltage restricted by design to less than 18V dc, a reader level converter module is required, see *17300 Reader Level Converter Module Installation Instructions*.

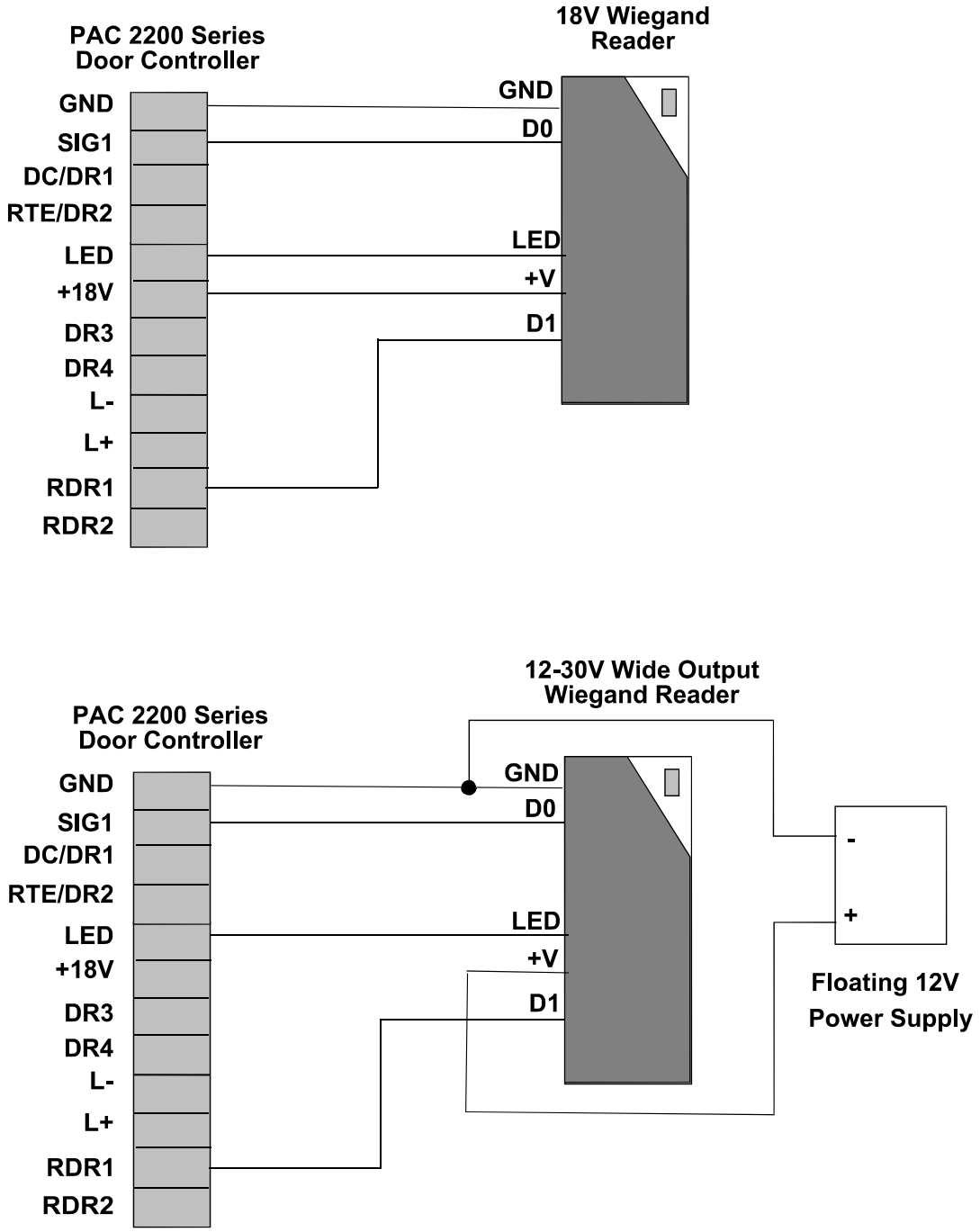


Figure 27 Wiegand Connections

5.2.8 Magstripe Readers

Magstripe readers with open collector CLK, DATA can be connected to a PAC 2200 Series Door Controller as shown in Figure 28.

Note

+5V and +12V Magstripe readers require a reader level converter module, see *17300 Reader Level Converter Module Installation Instructions*.

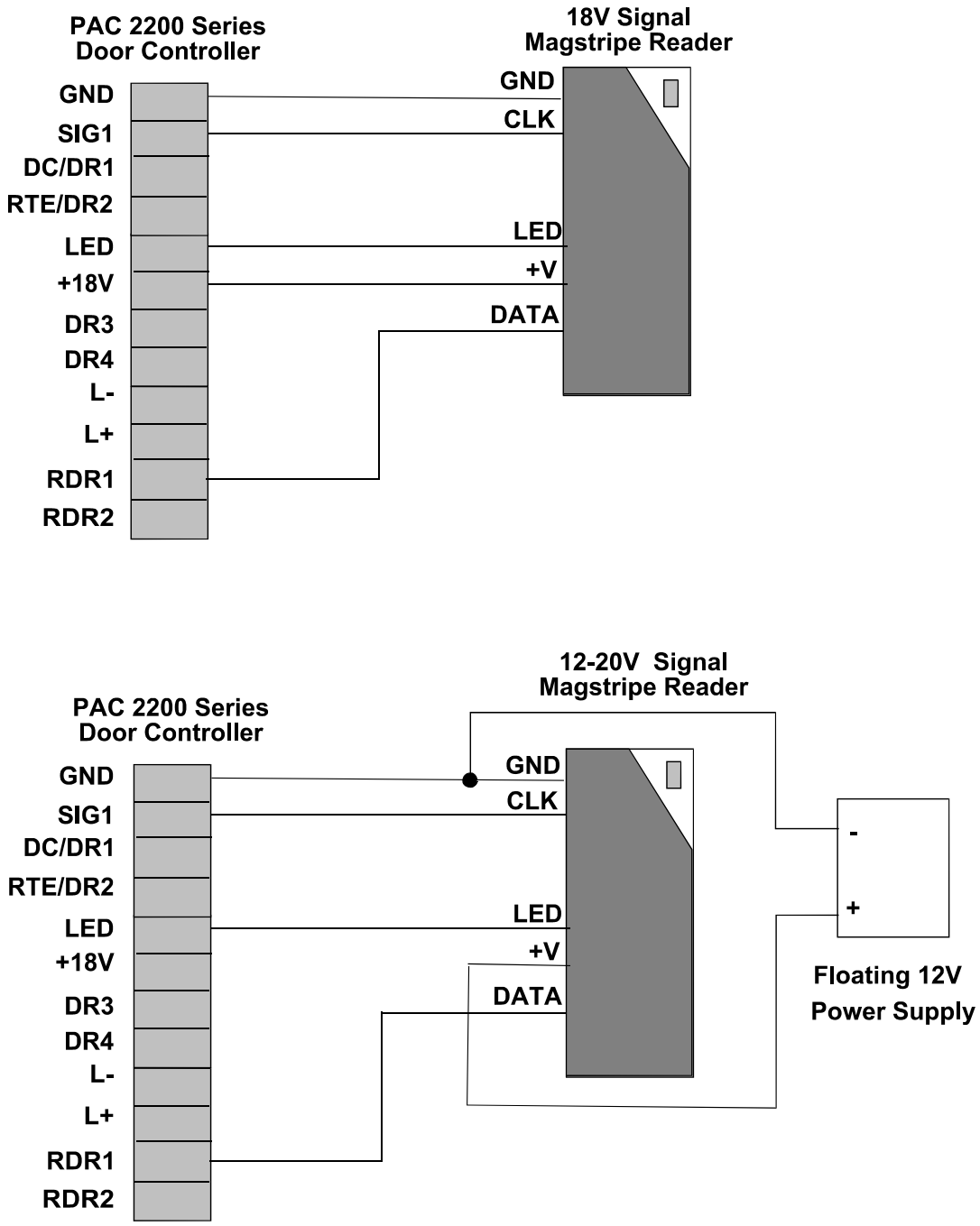


Figure 28 Magstripe Connections

5.3 Other Connections

This section describes the relay outputs, enclosure tamper, override input, and auxiliary power output. All these connections are made at removable terminal blocks along the bottom and left edge of the circuit board.

Also included in this section are brief details on the alarm event manager. This can be connected to any door controller but is primarily used in conjunction with the PAC 2204 Alarm Controller.

5.3.1 Relay Outputs

There are 8 relay outputs fitted to the left-hand edge of the door controller, each consists of a removable terminal block with Common, Normally Open and Normally Closed contacts. When a relay is activated the contact changes over from NC to NO. Depending on the type of administration system, these relays can be programmed to operate as a result of particular events happening.

Each relay is capable of switching 12V at 1A or 24V at 0.5A.

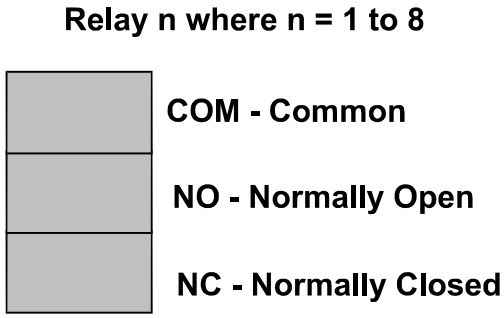


Figure 29 Relay Outputs

Without any programming, they will respond as follows:

Relay 1

Operates in the event of an invalid key being presented on door 1.

Relay 2

Operates in the event of an invalid key being presented on door 2.

Relay 3

Operates in the event of an invalid key being presented on door 3.

Relay 4

Operates in the event of an invalid key being presented on door 4.

Relay 5

Operates in the event of an `Unauthorised Access` at **any** door on the door controller. For an alarm controller, operates in the event of an AEM tamper (see the documentation supplied with the AEM).

Relay 6

Operates along with time profile 1.

Relay 7

Operates in the event of a `Door Left Open` at **any** door on the door controller. For an alarm controller, there is no default setting.

Relay 8

Operates in the event of an enclosure tamper (see Section 5.3.2).

Notes

1. The above default settings are applied when the database is initialised either at the front panel or via a PC. Default settings will also be applied automatically when

upgrading from a PAC 2100 Series to a PAC 2200 Series.

2. PAC for Windows can override the default settings for the first four relays. Relays 5-8 cannot be changed from their default settings.
3. PAC Vision can override the default settings for all eight relays.

The door controller will detect if it has been upgraded from a PAC 2100 and perform the following steps:

1. Apply system defaults to the on-board controller relays.
2. Clear (non-volatile) system variables such as door and alarm states.
3. Clear outstanding events (updates or downloads).
4. Reset the reader to its default settings.
5. Disable dial-back on buffer full.

5.3.2 Enclosure Tamper Input

This is a normally closed input that may be connected to a tamper switch fitted to the controller enclosure. If it is connected to a **Tamper** switch, a `Case Tamper` alarm is generated when the enclosure is opened.

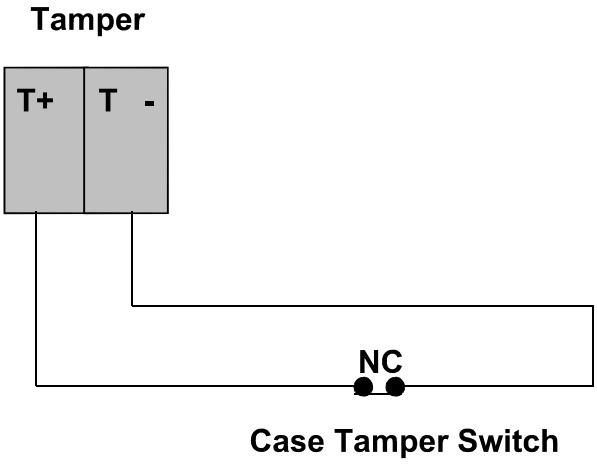


Figure 30 Enclosure Tamper Wiring

This is a normally closed switch therefore you should use a short piece of cable to link the two terminals before powering up. If not, you will get an immediate `Case Tamper` alarm.

5.3.3 Override Input

This is a normally open input that, when closed, will cause all the locks on the controller to operate. This may be fitted to the output of a **Manual Emergency Override** switch. All the doors on the door controller will remain open until the switch opens again.

If it is connected on a master controller, the doors on the master and those on any associated slaves will open and remain open until the switch opens again provided the master override input option has been programmed. For details, see *17267 PAC 2200 Series Controllers User Guide* or the documentation supplied with the administration software.

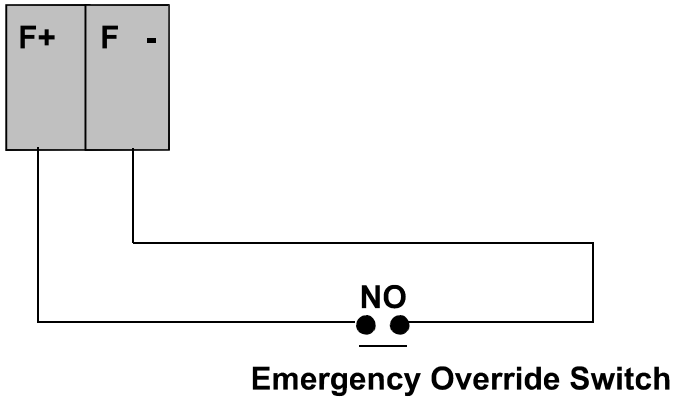


Figure 31 Override Input Wiring

WARNING

ANY FAILURE OF THE DOOR CONTROLLER OR CABLING WILL PREVENT THIS MEANS OF RELEASING THE DOORS FROM WORKING. THEREFORE THIS INPUT **MUST NOT** BE CONSIDERED AS A PRIMARY SAFETY MECHANISM - see Section 5.2.5.

5.3.4 Auxiliary Power Output

This connection can be used to provide power for auxiliary equipment. The electrical rating for the auxiliary power output is 500mA @ 12V and 250mA @ 24V.

Note

The auxiliary power output is not available on the PAC 2200IP Series because it is used to power the TCP/IP unit.

5.3.5 Auxiliary Serial Port

The auxiliary serial port is labelled SPARE and can be used to connect a DMP alarm panel.

5.3.6 Alarm Event Managers

An Alarm Event Manager (AEM) is a device that connects to a reader channel between the controller and the reader. Each AEM allows 8 supervised points to be monitored and provides 8 relays for programmable responses.

The PAC 2204 alarm controller, which is not used to control access, comes with two AEMs pre-wired in the enclosure. An additional two AEMs can be fitted to the alarm controller to provide up to 16 more programmable inputs and outputs.

Further details are given in the documentation supplied with the Alarm Event Manager.

6. Configuration

This section describes the various steps needed to configure the controllers before connection to the administration system.

Configuration involves:

1. Configuring the master controller, see Section 6.3.
2. Adding slave controllers, see Section 6.3.
3. Initialising and downloading slave controllers, see Section 0.

After each stage, the configuration should be tested as described in Section 8.

6.1 Initial Considerations

Before setting up the access control system, considered the items described in Sections 6.1.1 to 6.1.3). All the items can be adjusted at a later stage but it will save time in the future if they are considered at this stage.

6.1.1 Door Controllers

- Decide which door controller will be the master. In a mixed system, the master controller should be a PAC 2200 Series Door Controller. All the programming is performed at the master door controller.
- Decide which slave controllers will have which address (i.e. 2, 3 and 4). This is important as door numbering is determined by the address of each door controller.
- Decide if two readers will share the same lock output (e.g. in reader and out reader on the same door).
- Decide if anti-passback is required on a door controller.

6.1.2 Doors

For each door:

- Decide which doors will have door monitoring; this is essential for reporting alarms and door left open).
- Decide what type of lock is fitted to each door, fail-safe or fail-secure.
- Decide what should be the lock release time for each door.
- Decide which doors will open automatically at certain times.

6.1.3 Personnel Database

Determine the type of identification used for personnel keys. The choice is either 4-digit numeric (digits 0-9) or 12-digit alphanumeric (digits 0-9, A-Z and space). It is possible to change from one type of identification to the other at a later stage but it is wiser to choose one method and stick to it.

4-Digit Numeric

If you use 4-digit identification, **Editor** mode will automatically identify a key with the next available number between 1 and 4000, you will have no choice of the number assigned. For instance, if you have already added 85 keys, the next key added will be 86. If you have deleted (voided) keys 29 and 44, the next key added will be numbered 29 (the first available number), the next 44 and so on.

The advantage of this method is rapid addition of keys as the identification is automatic, the user **must** however ensure that a careful record is kept of the number assigned to each key.

12-Character Alphanumeric

This method requires the user to enter a unique identity for each key. This may be the name of the keyholder, or a reference number such as a personnel or payroll reference. Although it is more time consuming to administer, the advantages are that real names will appear on the printer and reports and a key can be found, for editing or deleting, by entering a name.

6.2 Initial Conditions

Ensure the following before starting the configuration:

1. The mains supply is present but **not** powered up.
2. The lock power supply is set to 12V dc or 2V dc.
3. The readers and locks to the door controllers, including, where required, **Request to Exit** switches, door contacts and any alarm modules are disconnected.
4. Any slave door controllers are connected to the master controller.
5. The **Enclosure Tamper** inputs (T**+**, T-) are linked - this will prevent any `D/C Tamper` alarms when first powered up.

6.3 Basic Configuration

Whatever the type of controller being commissioned, first set it up as a front panel administered system. This allows you to use the built-in editor commands to test the readers, locks and any alarm event managers before attempting to establish communications with other controllers in the system.

6.3.1 Option Switches

The option switches are fitted at the bottom right of the circuit board. Switch 4, the bottom switch, has a special purpose, se Section 6.3.3.

The top 3 switches **must** be set as shown in Figure 32.

- If the door controller is a master controller, the first 3 switches should be set to the right.
- If the door controller is a network slave, the first 3 switches should be set to the left.

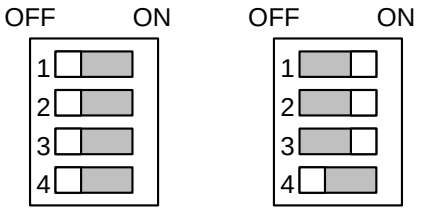


Figure 32 Option Switch Settings

If the option switches are not set correctly, you will probably experience unreliable six wire bus communications.

6.3.2 Powering Up - First Checks

Before applying power for the first time, loop the enclosure tamper terminals together (T**+** and T- at the bottom of the circuit board). This will prevent a `Case Tampe`r alarm when you switch on.

Leave all readers, locks and any six wire bus or serial port connectors disconnected.

Apply power to the door controller. There should be a short beep. The next response depends on whether the door controller has been programmed before or not.

- If this is a new controller that has not been programmed before, it should beep continuously and display:

```
*NO MASTER KEY*
```

- If the door controller has been programmed before, it may respond with an alarm indication, such as:

```
DOOR 01 ALARM
```

or:

```
CH1- A --------
```

If it detects several alarm conditions, the display will show each in turn.

- If the door controller contains a master key but there are no alarm conditions, the display will remain blank. In which case, check that the door controller has started by pressing **ESC** key on the keyboard - you should get a beep.

Check the front panel reader by presenting a key to the reader, a *T* should appear at the right of the display.

If there is no sound or display, check the front panel ribbon cable is properly connected, otherwise continue with the engineer's reset *(*see Section 6.3.3*)*.

6.3.3 Engineer's Reset

To get into the front panel **Editor** mode and issue commands without an editor key, you need to perform the engineer's reset as follows:

PAC 2200 Ver 1

- Press the **Reset** button **twice.**

PAC 2200 Ver 2

- Locate the option switches (see Section 6.3.1) and move option switch 4, the bottom one, to the right (ON).

The following is displayed:

PASSWD _	Type *PAC1990* or *PAC2001 a*nd press **ENT**. If a valid password is not entered within 10 seconds, the display is timed out. To redisplay the PASSWD prompt, move switch 4 to the left and then right.
CMD _	The CMD prompt is displayed.

If the door controller is being installed for the first time, initialise it with the **SYSTEM START** command.

6.3.4 SYSTEM START Command

This command completely erases and initialise all data from a controller. It is good practice to do this with any new installation. Once the controller is initialised, the **INST** command, which is used to change the system settings (see Section 6.3.5), is automatically started.

IMPORTANT

It is essential that **SYSTEM START** is used on a door controller that is going to be used with a dial-up modem. The door controller will be set to system type 2 or system type 3 to allow use of the modem, but the only way of initialising the communications settings is by using **SYSTEM START**.

CMD _	This is the CMD prompt. As this is a brand new controller type *SYSTEM START* and press **ENT**. (Press **SPC** between SYSTEM and START). **Note** You can only perform a system start on a standalone master (system type 0). If you get a message *INVALID SYS TYPE,* you will have to use the **INST** command (Section 6.3.5) to change the **System Type** to **0**. You will then be able to enter the SYSTEM START command.
ERASE ALL DATA _	Type Y and press **ENT** to initialise the door controller.
ERASING USR DATA *ERASING SYS DATA*	These two messages are displayed as the memory is cleared.

When the memory has been cleared, the **INST** command is automatically entered, see Section *6.3.5*.

When the **INST** command settings have been specified, the following system has been set up:

- Every door (1 to 16) is given a Lock Release Time (LRT) of 5 seconds.
- Access level 1 is set to all doors (1-16).
- Access code 1 is set to a primary access level of 1.
- The master key entered using **INST** is made user number 1 with an Access Code (AC) of 1.

This results in the master key having access through all doors. If you need more keys to help test the system, use the **A** command to add some more keys. Use Access Code 1 (AC = 1) with access everywhere. For full descriptions of these settings and what they mean, see *17267 PAC 2200 Series Controllers User Guide.*

Note

The above settings only apply when you leave **INST** after using the **SYSTEM START** command. Normally use of the **INST** command will not affect any personnel or access data.

6.3.5 INST Command

This command can be used at any time to change settings. It is also entered automatically after the SYSTEM START command.

The prompts displayed depend on the type of system being installed.

6.3.5.1 PAC 2200 Ver 1

`E0 KEY 00000000`	This is where the master key code will appear, there may already be a code here - it will consist of numbers 0-9 and letters A-F. Present a key to the front panel reader.
`E0 KEY 3A33642A`	The key code will appear, replacing what was previously displayed. Press the **+**.
`PASSWD _`	For a master key password, type the password. Press **ENT** then **+**. For no master key password, just press the **+** key.
`ID _`	Type a door name (up to a maximum of 12 characters)**.** This is what will appear on reports if the system is administered from the front panel. Press **ENT** then **+**.
`ALPHA ID N`	Leave as `N` for numerical idents; Type `Y` for user names. Press **ENT** then **+**.
`PRINTER TYPE 0`	Leave as `0` for Epson printer or no printer; Type `1` for Microline printer. Press **ENT** then **+**.
`ENTER SYS TYPE 3`	Leave as `3` for slave; Type `2` for master. Press **ENT** then **+**.
`POLL _ _ _`	For a master, type a list of slave controllers to poll, e.g. *234*. Press **ENT** then **+**. For a slave, just press **+**.
`ADDRESS 1`	Leave as `1` for a master; Type `2`, `3`, or `4` for a slave. Press **ENT** then **+**.
`DATE FORMAT 0`	Leave as `0` for European style (day-mon-yr); type `1` for US style (mon-day-yr); type `2` for other (yr-mon-day). Press **ENT** then **ESC**.

6.3.5.2 PAC 2200 Ver 2

For a standalone master:

PC ADMIN USED _	Type N for standalone. Press **ENT** then **+**.
PC MASTER DC _	Type Y for standalone master. Press **ENT** then **+**.
POLL	Type a list of slave controllers to poll, e.g. *234*. Press **ENT** then **+**.
E0 KEY 00000000	This is where the master key code will appear, there may already be a code here - it will consist of numbers 0-9 and letters A-F. Present a key to the front panel reader.
E0 KEY 3A33642A	The key code will appear, replacing what was previously displayed. Press **+**.
PASSWD _	For a master key password, type the password. Press **ENT** then **+**. For no master key password, just press **+**.
ID _	Type a door name (up to a maximum of 12 characters)**.** This is what will appear on reports if the system is administered from the front panel. Press **ENT** then **+**.
ALPHA ID N	Leave as N for numerical idents; Type Y for user names. Press **ENT** then **+**.
PRINTER TYPE 0	Leave as 0 for Epson printer or no printer; Type 1 for Microline printer. Press **ENT** then **+**.
DATE FORMAT 0	Leave as 0 for European style (day-mon-yr); type 1 for US style (mon-day-yr); type 2 for other (yr-mon-day). Press **ENT** then **ESC**.

For a standalone slave:

PC ADMIN USED _	Type N for slave. Press **ENT** then **+**.
PC MASTER DC _	Type N for slave. Press **ENT** then **+**.
ADDRESS 1	Type 2, 3 or 4. Press **ENT** then **ESC**.

For a PC-based system:

PC ADMIN USED _	Type Y for PC administration. Press **ENT** then **+**.
PC MASTER DC _	For a master, type Y, press **ENT** then **ESC**. For a slave, type N, press **ENT** then **+**.
ADDRESS 1	For a slave, type the address of the slave. Press **ENT** then **ESC**.

The system can then be commissioned. Commissioning is usually performed via administration software but can be performed at the front panel by presenting a master key (see *17263 PAC 2200 Series Controllers Installation Guide*).

6.4 Initialising and Downloading Slave Controllers

Once all the slave door controllers have been added and are communicating correctly with the master, initialise each one. Once initialised, perform a download. This will result in all the door controllers having the same database and provide a starting point from which the whole system can be programmed.

6.4.1 C Command - Clock

At the master door controller, present the master key (and enter the password if required):

```
CMD _
```

Type `C` to check the date and time.

Press **ENT**.

```
DATE    10-11-01
```

Enter the date:

Type the new date over the existing date, or use the left and right arrow keys to move the cursor to the figures you want to change.

Notes

1. The cursor moves over the separator character (-) to the next digit.
2. If **CLR** is pressed, re-enter the time with a space between the hours and minutes.

Press **ENT**.

If the date is invalid, it will be adjusted to the nearest valid date.

Press the **+**.

```
ENTER DAY    TUE
```

Enter the day of the week.

Type `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT` or `SUN`.

Press **ENT**.

If one of the above 3-character names is not entered, the display will default to `MON`.

Press the **+**.

```
ENTER TIME 16-01
```

Enter the current time.

Type the new time over the existing time or use the left and right arrow keys to move the cursor to the figures to change.

Notes

1. The cursor moves over the separator character (-) to the next digit.
2. If **CLR** is pressed, re-enter the time with a space between the hours and minutes.

Press **ENT**.

If the time is invalid, it will be adjusted to the nearest valid time.

Press **ESC**.

6.4.2 INITn Command - Initialise Door Controller

At the master door controller, present the master key (and enter the password if required):

`CMD _`	Type `INIT2` to initialise slave controller 2.
	Press **ENT**.
`INIT D/C NO 2 _`	Type `Y` to confirm.
	Press **ENT**.
	Press **ESC**.

Test the door controller as described in Section 8.

6.4.3 DL Command - Download

The **Download** (**DL**) command sends the contents of the master controller's database to all the slave controllers. Once this has been done, ensure that all the door controllers have the same information.

At the master door controller, present the master key (and enter the password if required):

`CMD _`	Type `DL` to download to all controllers.
	Press **ENT**.
`DLOAD TO ALL _`	Type `Y` to confirm.
	Press **ENT** .
`SENDING DATA CMD _`	This message will appear briefly returning to the `CMD` prompt.
	Press **ESC**.
`DOWNLOAD 26-9`	This is displayed when leaving **Editor** mode. It indicates the progress of the download, in this example 26.9%. The download will be complete when it reaches 100%.

Test the door controllers as described in Section 8.

7. Commissioning

7.1 PAC 2200 Series Engineering Mode

This mode is designed to assist in the commissioning of the door controllers. There are three distinct sections in **Engineering** mode:

1. **Status Display**

   This is for monitoring the state of all channel inputs and the number of events stored. On entering **Engineering** mode the controller, the prompts described in Section 7.2.4 will be displayed. Press **ESC** at any time to move to **Modem Configuration** mode.

2. **Modem Configuration**

   This is for setting modem parameters. To reach this mode, press **ESC** from any point in **Status Display** mode and the prompts described in Section 7.2.2 will be displayed. Press **ESC** at any time to move to **Forget Transactions** mode.

3. **Forget Transactions**

   This is for setting event filtering to prevent events being sent by the controller to the administration system and set which doors generate a dial-back for `Access Authorised` transactions.

To enter Engineering mode:

- Locate the **Option** switch at the bottom left-hand of the circuit board (above the **Reset** button).
- Move switch 4, the bottom one, to the right.
- Press the **Reset** button **once.**

To leave Engineering mode at any time:

- Move switch 4 back to the left.
- Press the **Reset** button **once**.

7.2 PAC 2200 Ver 2 Commands

PAC 2200 Ver 2 is primarily a PC-based system but the commands described in this section can be performed at a front panel **by presenting a master key** without entering **Engineering** mode.

Command	Description	Further Information
SYSTEM START	Erase database	See Section 6.3.4.
INST	Installation	See Section 6.3.5.
F	Forget transactions	See Section 7.2.1.
M	Modem configuration	See Section 7.2.2.
N	PIN display	See Section 7.2.3
S	Status display	See Section 7.2.4.

7.2.1 F Command - Forget Transactions

Five options are provided which can prevent certain types of transaction being sent by the door controller to the administration system. This can be useful in a busy system to speed up the communication of more important events, or on dial-up systems to keep connect times short. Below are described which transactions are **not** sent when `Y` is set against each option.

See *17267 PAC 2200 Series Controllers User Guide* for a full description of all transaction types.

At the *CMD* prompt, type F and press **ENT**.

`FRGT RTE N` Leave as N for reporting `Request to Exit/Entry` events; type `Y` to ignore these events.

Press **ENT** then **+**.

`FRGT FREE EXIT N` Leave as N for reporting `Free Exit` events; type `Y` to ignore these events.

Press **ENT** then **+**.

`FRGT TIME EVNT N` Leave as N for reporting `Time` events; type `Y` to ignore these events. e.g. `Automatic Lock` and `Auto Zone Disable`.

Press **ENT** then **+**.

`FRGT POS TRANS N` Leave as N for reporting `Positive Transaction` events; type `Y` to ignore these events, e.g. `Access Authorised, Entry Authorised, Exit out of Hours` and `Exit Authorised`.

Press **ENT** then **+**.

`FRGT NEG TRANS N` Leave as N for reporting `Negative Transaction` events; type `Y` to ignore these events, e.g. `No Access : 'reason'` events.

Press **ENT** then **+**.

`DIAL D/C1 DR----` Type the door numbers (reader channel numbers) for which dial-back is to be initiated in the case of a `Positive Transaction` event on door controller 1 (the door controller the modem is connected to).

For example, if a dial-back to be initiated when a positive event occurs on doors 1 and 3 on door controller 1, type `1` and `3`.

Press **ENT** then **+**.

`DIAL D/C2 DR----` As above for door controller 2.

`DIAL D/C3 DR----` As above for door controller 3.

`DIAL D/C4 DR----` As above for door controller 4.

DIAL D/C5 DR----	As above for door controller 5.
DIAL D/C6 DR----	As above for door controller 6.
DIAL D/C7 DR----	As above for door controller 7.
DIAL D/C8 DR----	As above for door controller 8.

Press **ESC**.

In order for dial-back on `Positive Transaction` events to operate a number of other settings need to be programmed:

In **Modem Configuration** mode, the following must be programmed:

CONNECT MODEM Y	Make sure that `Y` is programmed to indicate there is a dial-up modem connected to this door controller.
SETUP -D------	Make sure that the `D` setting is programmed to enable dial-back. In the event of an alarm condition, the door controller will dial-back to the Multi-Site CNC. If a dial-back on `Positive Transaction` events is also required, the additional settings described above must also be programmed.

In **Forget Transaction** mode**,** the following must be programmed:

FRGT POS TRANS N	This setting must be programmed to `N` in order that all positive transactions are not ignored and hence initiate dial-back to the CNC.

7.2.2 M Command - Modem Configuration

At the *CMD* prompt, type `M` and press **ENT**.

ADDRESS 1	Leave as 1 for a master; type the address for a slave controller. This is only required when a controller is set to system type 3. All other system types will have a setting here of 1. The values available for the address depend on the type of administration system: • A slave controller as part of a standalone or PC interface kit system will have an address of 2, 3 or 4. • A slave controller as part of a system type 2 will have an address of 2, 3, 4, 5, 6, 7 or 8. • A slave controller connected to a CNC six wire bus will have an address of 1 to 32. • A slave controller connected directly to a PAC Multi-Site CNC will have an address of 1. • A slave controller connected to a PAC Multi-Site CNC through a COS-4 or COS-8 dataswitch will have an address of 1 to 4 or 1 to 8. Press **ENT** then **+**.

`BAUD RATE 1200`

Available baud rate settings are 300, 600, 1200, 2400, 4800, 9600, 19200.

Depending on the system type the baud rate should be:

Printer attached to front panel administered controller (system type 0): `4800.`

Door controller attached to PC interface kit (system type 2): `9600.`

Door controller attached to Single-Site CNC (system type 2): `9600.`

Door controller attached to Multi-Site CNC (system type 2 or system type 3): the baud rate depends on RS-232 devices being used, modems, line drivers, etc. `300, 600, 1200, 2400, 4800, 9600, 19200.`

If a change is required, type the baud rate.

Press **ENT** then **+**.

`CONNECT MODEM N`

Type `N` for no dial-up modem connected to the door controller; type `Y` for a dial-up modem connected to this door controller.

This setting is important as it will ensure that a dial-up modem is correctly programmed to auto-answer. It is also important to ensure that if no modem is connected, this entry is set to `N`.

Press **ENT** then **+**.

`SETUP RDPHBTX-`

To setup remote acknowledge, dial-back and comms protection, type the required numbers (1 to 7). For example, entering `1, 2, 5` and `7` selects those options and displays `RD--B-X` to show the options selected. The options are:

R **When administered via a PC only.**
This indicates whether **Remote Acknowledgement** is required for alarms. In this case, if `R` is showing, a door alarm will only be cleared at the door controller if it is acknowledged by an operator at the administration system. This may be the front panel or a PC. If `R` is not showing, the alarm will be acknowledged at the door controller when it is passed to the master controller. This is important if you use the programmable on-board relays (PC-based systems only). These relays and those on any attached alarm module will only be reset when the alarm is accepted by an operator.

D **For use with Multi-Site CNC only. Dialback**. In the event of an alarm condition or `Access Authorised` (if set up) the door controller will dial-back to the Multi-Site CNC using the first number shown in **Dialback** specification in this section. If it fails to get through, it will attempt again on the first number. If it fails again, it will try the second number, if present, twice. This process will be repeated 5 times. If there is still no success it will give up, generating a `Comms Failed` transaction.

P **For use with Multi-Site CNC only. Comms Protection**. This setting activates the Comms protection facility.
See the **Protect Comms** specification in this section.

H **For use with Multi-Site CNC only.**
Hardware Handshake. Set this if the device being used to communicate with the CNC requires a hardware handshake (CTS/DTR). The door controller will not send, or stop sending, data when its CTS input is low.
See Section 3.3.

B **For use with Multi-Site CNC only**.
Auto Baud Rate Select. When a modem obtains a connection, it returns a message stating the baud rate at which it will communicate. This rate is usually 'negotiated' between modems when a line is established. When this option is selected, the door controller will adjust its serial baud rate to match the line speed See Section 3.3.

T **Transaction Restriction**. Use this setting only when installing the PAC 2200 Series Door Controller on older PAC systems that do not recognise transaction types such as Power On, Power Off, Auto Relay Set, etc.

X **Not used**.

Press **ENT** then **+**.

Note

It is recommended that the dial-back times are set via a PC.

Type the telephone number 1 for dial-back.
Press **ENT** then **+**.

Type the telephone number 2 for dial-back.
Press **ENT** then **+**.

PROTECT COMMS N

Type N for no protected communications; type Y for protected communications.

For this to operate, P must be specified for SETUP above**.**

This feature allows dial-up communications to be established only when the master key code sent by the CNC matches the master key code stored in the door controller.

Type N to allow the next dial-up to be accepted. The next master key that is sent by the CNC will be accepted by the door controller and stored. All future dial-ups must have a match between this code and the one sent by the CNC.

Press **ENT** then **+**.

Type up to 16 Hayes-compatible modem control characters. You should only need to use these if the modem connected requires more than the standard programming provided by default. Do not put any characters in here unless you understand their meaning, or are directed by someone who does.

To enter characters not provided on the keypad, you can use the • key, followed by the following letters:

- **+ A** gives **&**
- **+ D** gives **$**
- **+ E** gives **=**
- **+ P** gives **%**
- **+ Q** gives **?**
- **+ S** gives *****
- **+ B** gives ****

See Section 3.3.

Press **ENT** then **+**.

7.2.3 N Command - PIN Display

At the *CMD* prompt, type N and press **ENT**.

`* PRESENT KEY *`	Present a key to the front panel reader.
`PIN NO IS  1234`	The 4-digit PIN will be displayed for about 2 seconds.
	Either present other keys to determine their PIN codes or press **ESC**.

7.2.4 S Command - Status Display

At the *CMD* prompt, type S and press **ENT**.

`1=`	This is the **Test** mode.
	The following is displayed **if the appropriate conditions apply**:
	DC if DC displays, the DC circuit (door contact) is closed. If a door contact is fitted, DC means the door is closed.
	RT if RT displays, the RTE circuit (request to exit) is closed. If a request to exit button is fitted, RT means it is being pressed.
	EM if EM displays, the INHB/DR3 input is closed. This indicates that either an arming button is pressed down or the arming output of an alarm panel is active.
	LT if LT displays, the ALM/DR4 input is closed. This indicates that the alarm relay of an alarm panel is active.
	1/2 if 1 displays, a key is being presented to the reader1 connected to that channel. If 2 displays, a key is being presented to the reader 2 connected to that channel.
	Press the **+**.
`2=`	As above but for door 2.
`3=`	As above but for door 3.
`4=`	As above but for door 4.
`TRAN HI00 LO0000`	This shows many events are currently in the High Priority (HI) queue and how many in the Low Priority (LO) queue . If the door controller is communicating to the administration system, both these values should be 0.
	Press the **+**.
`CTS OVRD TAMP @`	OVRD if OVRD displays, the terminals F**+** and F- are closed, emergency override active.
	TAMP if TAMP displays, the terminals T**+** and T- are closed, enclosure tamper active.
	CTS if CTS displays, the serial port CTS signal is high.
	@ this character represents the last command received from the PC or CNC. It may be ? or / at times.
	Press the **ESC**.

8. Testing

This section describes how to test each reader channel and lock output, where applicable.

Ensure that the system is **not** in **Engineering** mode. To leave **Engineering** mode, see Section 7.1.

8.1 Checking Reader Channels

Connect reader channel 1:

- Present the master key (added to the system when you carried out a system start - see Section 6.3.5) to reader 1. *1* should appear on the right of the display. Presenting the master to reader 2 if fitted. *2* should appear on the right of the display.
- Operate the **Request to Exit** switch, if fitted. `RT` should appear on the controller display **while the switch is closed**.
- Operate the door contact, if fitted. `DC` should appear on the controller display **while the contact is closed.**

Repeat for each reader channel.

Note

Testing the reader channels can be done with a standalone “test” reader instead of using the actual readers fitted to the controller before connecting to the six wire bus. This means that the controller channels can be checked before the controller is taken on site to be installed.

8.2 Programming Readers and Locks

Having verified the operation of the readers and door inputs, now verify the lock operation. To do this, program some values against each door using the following commands that are described in detail in *17267 PAC 2200 Series Controller User Guide*.

DC Command - Door Control

This command sets up lock sharing (two readers sharing the same lock output) and anti-passback.

D Command - Door Options

This command sets lock release time, door open time, time profile for automatic opening and lock mode options such as fail-safe/fail-secure, etc.

RD Command - Reader Tamper and Formats

This command enables reader tamper and formats. Reader tamper is disabled by default and should only be enabled on readers that require it. On PC-administered systems, reader formats are specified using the administration software.

Notes

1. As these will be required when the system is operational, it is sensible to use the correct information for each door.
2. Ensure the system type of the controller is `0`.

8.3 Testing Readers and Locks

If you used the **SYSTEM START** command described in Section 6.3.4, the master key will have access through all doors. You can now use this key to check the operation of readers and locks.

8.3.1 Readers

Present the key to each reader:

- The green LED should light on the reader and remain on for the duration of the lock release time, 5 seconds or whatever other value you may have set.
- The lock should operate for the duration of the lock release time.

- The door controller should display the following (the numbers indicating which doors are open):

```
DOORS OPEN 1
```

8.3.2 Request to Exit

Repeat the above using the **Request to Exit** switch, if fitted, to operate the lock instead of a key.

8.3.3 Door Monitoring

If door monitoring is being used:

- Close the door before the lock release time expires, the green LED on the reader should go out and the door should lock.
- Leave the door open, the green LED on the reader will go out and the lock will lock. After the expiry of the door open time, you should get a door left open warning:

```
CH-1- O --------
```

- Open the door without a key or request to exit. You should immediately obtain a door alarm, flashing and sounding, indicating which door has been forced:

```
DOOR 01 ALARM
```

- You should get exactly the same effect by disconnecting the reader terminal block - causing a tamper alarm.

Note

If any problems are encountered, see Section 9.

9. Troubleshooting

This section is designed to help you establish if a fault exists within a door controller or not. To do this efficiently, we recommend the following equipment is available:

- A multi-meter capable of reading volts (0-300V ac, 0-30V dc), amps (0-3A) and ohms.
- A reader on a flying lead that can be plugged into a reader channel, this should also have buttons emulating a door contact (DC-GND, normally closed) and the **Request to Exit** switch (RTE-GND normally open).
- The usual collection of hand-tools, screwdrivers, wire strippers and cutters, etc.
- Replacement fuses.

WARNING

DO NOT REMOVE THE POWER SUPPLY CASE AS THIS WILL EXPOSE YOU TO LETHAL VOLTAGE AND INVALIDATE ANY WARRANTY.

9.1 Door Controller and Readers

The controller appears to be dead.

Before performing any of the following checks, remove any batteries and disconnect all readers, lock outputs, serial connections and six wire bus, where fitted.

1. Check the heartbeat LEDs located on the bottom left of the circuit board. If the green LED is flashing, it indicates that the controller is healthy. If the red LED flashes, this indicates that communications is occurring.
2. Press the **?** key on the keypad. If the door controller is operating correctly, there should be a beep and the software version should be displayed on the screen. If there is no reaction, check the ribbon cable between the front panel and the main circuit board is properly connected.
3. Check the ac power supply. This should be between 85V ac and 250V ac.
4. Check the power supply fuse. This is found in a pull-out drawer just below the ac cable socket. Replace with a 5A, 20mm fast-blow fuse (2A if the 4A PSU (PS80) is being used).
5. Check the battery output voltage at the battery terminals, this should be 13.8V dc **or** 27.6V dc depending on the lock output voltage.
   a) Check the power supply outputs. These are indicated on the circuit board next to the 8-pole connector, CN7.

b)	+V and -V (six wire bus supply)	**12V dc**
c)	Blue GND and +5V (logic supply)	**5V dc**
d)	Black GND and +18V (reader supply)	**18V dc**
e)	Black GND and BAT+ (battery supply)	**13.8V dc** or **27.6V dc**
f)	Black GND and +12V (lock output supply)	**12V dc** or **24V dc**

If the door controller fails on any of the above checks, the power supply is probably at fault, arrange for a replacement with your supplier.

If the door controller passes all the above tests, test each reader and lock output in turn, as described in the next section.

One or more readers or locks fail to operate.

Before carrying out the following tests, disconnect **all** the readers and lock outputs. Each reader channel should be tested in turn.

9.2 Checking the Reader

1. With no reader connected, check the voltage between GND and **+**18V. This should be at least **18V dc**.
2. Reconnect the reader. Check the voltage **at the reader**. This should be above **10.5V dc**. If not, check the gauge is correct for the cable distance from the controller (see Section 5.2.1.4).
3. Check the reader operation by presenting a key, if the door controller is in **Engineering** mode (see Section 0), a **1** or **2** should appear on the display while the key is being read by the reader.
4. If no key is read, disconnect the reader and connect a known working reader and repeat step 3.
5. If the working reader operates correctly, suspect a faulty reader, or wiring between the door controller and reader. Go to step 8 to check the wiring and reader.
6. If the working reader does not operate, suspect a faulty reader channel on the door controller.
7. Connect the reader to another channel, if the reader now operates, the original channel is faulty. Arrange for the door controller to be repaired. Go to step 10.
8. Disconnect the suspect reader. Disconnect the reader connector at the door controller. Check the cable for short circuits between all conductors, and all conductors and ground.
9. If the cable is to the correct gauge and free from short circuits, connect the known working reader in place of the suspect reader. If this reader operates, the original is faulty. Arrange for a replacement with your supplier.
10. Repeat for all four (two on a PAC 2222) reader channels.

9.3 Checking the Lock Output

If all the reader channels are shown to operate correctly, you should check the lock outputs. You should know whether the lock is fail-safe (power is removed to operate the device) or fail-secure (power is applied to operate the device). You should also know whether the door controller has been set to provide 12V dc or 24V dc. If interlock has been set on a pair of readers, channels 1 and 4 will operate lock output 1, and channels 2 and 3 will operate lock output 2.

1. For each lock output:
   - Make sure that the door secure, that is, the door controller display should **not** indicate that the door is open.
   - Make sure a lock release time has been set, it should be at least 5 seconds to allow measurements to be reliably made.
   - Establish whether lock sharing has been set.
2. Check the voltage at the lock output (L-, L**+**) on the controller. This should be **12V** or **24V** if the lock is **fail-safe**, or less than **0.5V** if it is **fail-secure**. (The door controllers have solid state lock outputs, these will not show exactly 0V when off).
3. Operate the lock, operate the **Request to Exit** switch or short the RTE reader input to GND. The lock output should operate. Check the voltage at the lock output. This should now show the reverse of the previous measurement, i.e. less than **0.5V** for **fail-safe**, **12V** or **24V** for **fail-secure**. If not, suspect the lock output to be faulty.
4. Repeat steps 2 and 3 above but this time measure the voltage **at the lock**. The lock should receive the minimum voltage required for it to operate (see the lock manufacturer's specifications). If the voltage is too low at the lock, the lock supply cable gauge may be too small for the distance from the controller.
5. Disconnect the cable from the lock. Check the cable for short circuits between the conductors, and between the conductors and ground.

6. Ensure there is a Metal-Oxide Varistor (MOV) fitted across the lock terminals. If large currents are used (i.e. >1A) use the large MOV supplied with the door controller. If small currents are used (i.e. <1A) use the small MOV supplied with the reader. Reconnect the lock.
7. Check the current drawn by the lock. This should not exceed 1.0A (12V dc) or 0.5A (24V dc). If it significantly exceeds the nominal current specified by the manufacturer, the lock may be faulty.
8. If the lock still fails to operate when the door controller is switching the correct voltage, suspect a faulty lock. Try fitting a known working lock in place of the suspect device.
9. Repeat for all four (two on a PAC 2222) lock outputs.

D/C n ERROR-1 (where n is 2 - 8).

This means the master is trying to communicate with a slave controller that has been entered in the poll table, but is getting no reply.

Check:

- The six wire bus connection between the master and slave.
- Check the option switches (bottom left of door controller circuit board) are set correctly. The top three switches should be to the right on the master, to the left on a slave.
- Check the address of the slave. Make sure no other slaves have the same address.
- Disconnect any other slaves on the six wire bus. If the fault goes away, check the connections and addresses of the other slaves.

No error is displayed on the master but the slave still fails to communicate

This probably means that the slave door controller is not in the master's poll table.

Check:

- Ensure the slave controller number (2-8) has been added to, or is enabled within the database.

10. Specifications

10.1 Environmental

Door Controller

Temperature	0ºC to **+**40ºC
Humidity	0% to 90% RH (non-condensing)

Readers

Temperature	-40ºC to **+**40ºC
Humidity	0% to 90% RH (non-condensing)

10.2 Power Supply

The PAC 2200 Series Controllers has an integral mains power supply. It is capable of automatically sensing the input voltage and will therefore operate on a 110-120V or 220-240V, 50Hz or 60Hz ac power supply without the need for switch setting.

The lock output is switch selectable between 12V dc and 24V dc. The lock output voltage applies to **all** the lock outputs.

Note

The switch selection affects locks, the battery charging output and the auxiliary output.

Electrical rating for the auxiliary output is 500mA @ 12V and 250mA @ 24V. The auxiliary output is not available on the PAC 2200IP Series because it is used to power the TCP/IP unit.

Full load power heat dissipation is 26W @ 250V ac and 115V ac door controllers.

AC Line Input

Voltage	85V ac to 250V ac 50/60Hz power input
Fuse Rating	3.15A 20mm HBC fuse (in ac connector) for 4A PSU (PS80) 5A 20 mm HBC fuse (in ac connector) for 8A PSU (PS159)
Connector	Standard IEC connector, right angle socket supplied

Lock Output

Output Voltage	12V dc or 24V dc, switch selectable.
Fuse Rating	Re-settable fuse on board, one per channel
Max. Current	1.0A per channel at 12V dc 0.5A per channel at 24V dc

Battery Backup

Input Voltage	12V dc or 24V dc, depending on lock output
Fuse Rating	Re-settable fuse on board

10.3 Cable

Reader Cable

Type	6 conductor, multi-stranded, unshielded cable			
Distance/Gauge	Up to 250m:	0.22mm²	Up to 750ft:	24 AWG
	Up to 500m:	0.50mm²	Up to 1500ft:	20 AWG
	Up to 1000m:	1.00mm²	Up to 3000ft:	18 AWG

Lock Output

Type	2 conductor, multi-stranded
Distance/Gauge	Depends on distance to lock and the current drawn by the lock. Usually 0.5mm² or 1.0mm² / 20 AWG or 18 AWG will be sufficient.

Six Wire Bus

Type	6 conductor, multi-stranded, unshielded cable.
Distance	Overall length of bus (max):1000m/3000ft Between controllers (max): 500m/1500ft
Gauge	24 AWG/0.22mm²

10.4 Mean Time Between Failures

>100,000 hours

11. Index

M

N

O

P

R

S

T

W

Declaration of Conformity			
Application of Council Directives	73/23/EEC		
Standard(s) to which conformity is declared	EN55022-B, EN55082-1, EN60950		
Manufacturer's Name	PAC INTERNATIONAL LTD		
Manufacturer's Address	1 Park Gate Close, Bredbury, Stockport, U.K. SK6 2SZ		
Type of Equipment	Access Control Systems		
Product Equipment	PAC 2200 Series and Power Supply		
I, the undersigned, hereby declare that the equipment specified above conforms to the above directive(s) and standard(s).			
Signed		**Date**	Nov 04
Full Name	Tim Gregory	**Position**	Managing Director