CS Technologies hardware installation guide

CS Technologies specialises in the design, manufacture and marketing of electronic access control equipment.

27 Bank Street (PO Box 1019) Meadowbank NSW Australia 2114
Telephone: +61 2 9809 0588
Facsimile: +61 2 9809 2446
Email: sales@cstech.biz
Website: www.cstech.biz

Table of Contents

1 Introduction

1.1 CS Access Control introduction

CS Technologies manufactures a range of electronic access control systems. This manual describes the systems and their components, and how to install and configure them.

A CS Access control system consists of three components.

Controller
The controller is the heart of the system. It is an intelligent 'black box' which contains all the programming necessary to allow people to enter the attached doors or other devices. Controllers come in two types, depending on the firmware which is loaded into them.

Door controllers have the capacity for up to four readers, to control doors. They also can have many alarm areas and inputs.

Elevator controllers have the capacity for a single reader controlling many outputs, to control an elevator.

There are a number of expansion options available for the controller which enhance its power and flexibility.

Reader + Credential
The reader and its associated credential is what identifies a user to the system. The CS controller recognises many different types of credentials. These include Silkey, Mag-stripe, Wiegand, various keypads, proximity cards and biometric credentials.

Software
The software is the 'front end' of the system. It runs on any Windows PC and allows configuration of the system, management of users and generation of reports. There are two software packages available, the entry-level PC3 software and the high-end Advent software.

This document describes the system, both from a conceptual viewpoint and also from the practical aspect of installing and maintaining the systems.

More information can be found in the following sections:

There is also a glossary of terms.

The applicable hardware, firmware and software details can be found in the Applicable revisions section.
More information on other CS Technologies products can be found on the More information page.

1.2 Applicable hardware and software

This manual refers to CS Technologies networked access control systems.

Board hardware: the board revision referred to is revision 2.3

Firmware: the firmware referred to is Universal 'Big Chip' firmware, revision UB474 (doors/alarms) and UBL475 (elevators) or greater

Software: the software referred to is Advent revision 352 or greater, or PC3 revision 188 or greater

Back to introduction

1.3 More information

More information on CS Technologies products can be found at http://www.cstech.biz.

There is a discussion forum on CS Technologies networked controllers at www.cstech.biz/cgi-bin/Ultimate.cgi?action=intro

CS Technologies can be contacted by email at support@cstech.biz.

or by writing to

CS Technologies
27 Bank Street (PO Box 1019)
Meadowbank NSW 2114
Australia

Tel: +61 2 9809 0588
Fax: +61 2 9809 2446

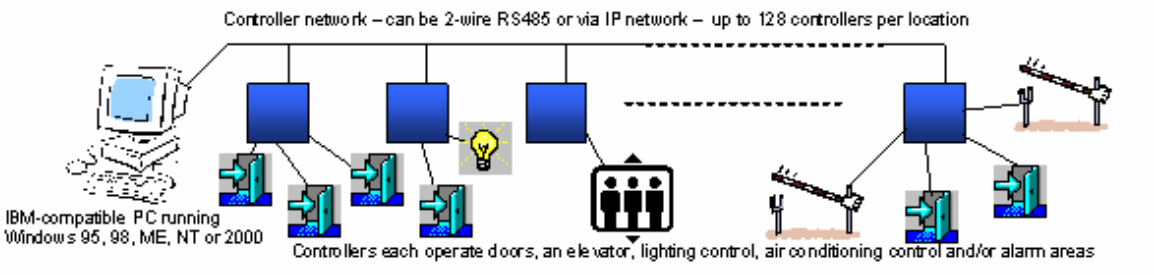
Back to introduction

2 Access Control components

2.1 System overview

The CS Technologies access control system allows powerful management of access to doors, elevators, alarm areas and also provides cost-effective energy management. The system consists of a network of intelligent 'black boxes' each of which controls a group of doors, an elevator or alarm processor. Each controller is fully distributed, and contains all programming necessary for seamless continuous operation regardless of the rest of the system.

Because the system is fully distributed, even the most complex access control or building management system can be broken down into small chunks to ensure that a dependable and cost-effective solution can be provided.



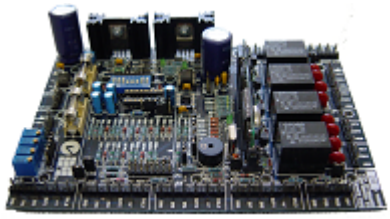
The PC runs software (either PC3 or Advent) which allows programming and monitoring of the activities in the controllers.
The controllers connect to readers and doors, or elevators, or alarm areas to provide control of the system.

The elements that make up the system are detailed in the following sections:

Controller
Reader/Credential
Output expansion
Input expansion
Software

2.2 Controller

The CS Controller is the heart of the CS access control system.



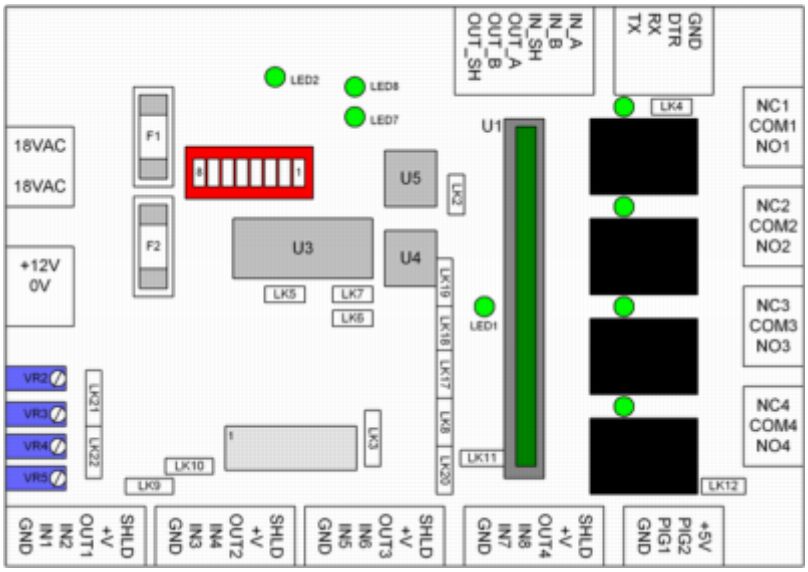
The controller contains:

- user credentials
- access levels
- timezones
- public holidays
- door settings

The key to the reliability and power of the CS system is the unique feature-set of the controller itself. Each controller contains all of the programming necessary to continue operation completely independent of the rest of the system meaning that in the event of failure of a PC, communication link or other part of the system, users can still gain access and a complex site can be broken up into segments each of which is very reliable.

Microprocessor - a reliable microprocessor module with integrated real-time-clock, battery backed RAM and ROM
AC or DC power input - the controller can operate from either 16VAC or 12VDC input. When powered by 12VDC the same power supply can be used for both the controller and electric strikes
Communication port - it can be configured to communicate in either RS232 or RS485 format, and has an in-built converter for either format.
Individually addressable - an expansion port allows the addition of relay and input expansion boards
Relay outputs - four heavy-duty relay outputs with 'form-C' contacts are provided on-board.
Buffered inputs - digital inputs on the board are buffered and diode-protected
Flexible configuration - many different firmware types are available to allow the controller to have a wide variety of functionality
Flash upgrade - the controller personality can be changed by downloading new firmware. This can even be done on an established network of controllers from the central PC.

The controller has 8 digital inputs (IN1-IN8), 4 digital outputs (OUT1-OUT4), 2 "Point identification gadget' ports (PIG1-PIG2) and four on-board relays (RELAY1-RELAY4). A diagram of the controller is shown below.



When installed, the controller interfaces to various items. These include:
Readers
Output expansion boards
Input expansion boards
Software

System overview

2.3 Reader/Credential

A credential is something like a key, card, PIN, fingerprint etc - anything which uniquely identifies a user to the system.

The reader is what accepts this credential and relays it to the controller for processing. A key feature of the CS system is that for every user a full 32-bits of data is stored. This means that

unlike other systems there is no necessity for a system 'site code' or 'degraded mode' - the system operates in full security mode at all times, and multiple site codes are supported as every single user effectively has their own individual site code.

The controller firmware can be configured to accept readers with formats including iButton, Clock+Data, Wiegand and Presco.

The system supports a very wide range of readers and credentials. The list below is by no means exhaustive. Some examples include:

Silkey reader (Silicon Key) The Silicon Key is a revolutionary access credential based on iButton technology. The keys and readers are manufactured from stainless steel and are extremely durable. They are also a high security device because they are impossible to duplicate and are guaranteed to be unique world wide. They carry a lifetime guarantee and can be 'branded' in the attractive keyfob to suit a particular client or application.	
Mag-stripe reader Mag-stripe format works with any mag-stripe card reader, or any reader with a clock and data interface. The firmware can be configured to read track 2, track 1 and a variety of proprietary card formats also. The mag-stripe programming is very flexible in that any part of the mag-stripe data string can be extracted and used as the user's credential. Card parameters set the start and length of the site code and the card number and thus the system can easily be configured to work with a wide variety of existing cards too.	
Presco keypad The Presco format is a 1-wire current loop used with a durable range of keypads and prox readers manufactured by Nidac Security. Using Presco format PIN numbers can be any length from 3-9 digits and the keypads are available as low-cost or vandalproof versions.	
Wiegand readers They system supports any type of wiegand reader. The system stores a full 32-bit credential for each user so it works with any site code, any combination of site codes, individual site codes for each user and any length of wiegand data. Different wiegand lengths can be mixed in the system and every user has an individual site code so there is no restriction on the cards required. Some typical formats used include 26-bit, 27-bit, 32-bit, 34-bit, 40 bit and the system also supports a wide variety of encrypted cards. The wiegand interface works with any wiegand reader including Sensor, HID, Keri, Ultraprox, Essex, Codeguard, Casi-Rusco, Motorola, Indala, Cotag and any other standard wiegand format device	
Smartcard readers The CS smartcard reader works with Infineer, Proton, eCard and various university card formats. The system also works with contactless smartcards including Mifare and Legic.	
Fingerprint reader The CS fingerprint reader provides a durable and reliable fingerprint reader for accurate biometric identification. Utilising a Silkey with the stored fingerprint for '1:1' verification the reader is fast and unlimited in capability because each user carries his/her own biometric template in the button.	

Detailed information on the installation of readers can be found in the reader installation chapter.

System overview

2.4 Output expansion

The controller is equipped with four on-board relays. This can be expanded in a number of ways. Expansion is always subject to the firmware within the controller and other constraints.

Output expansion is used with door/alarm firmware to increase the number of outputs which are available for reporting alarms, alarm area status and other types of alarm functions.
Output expansion is used with elevator firmware to increase the number of controlled floors. Up to 250 floors can be controlled per controller.

There are four types of output expansion possible.

4-way relay board
The 4-way relay board allows expansion of the outputs of the controller in groups of 4 relays. Up to three 4-way relay expansion boards can be added to the controller to make a total of 16 relays altogether.
Using 4-way relay boards it is not possible to mix these with any other types of output or input expansion nor to expand to more than 16 relays.

Expanding using 4-way relay boards 'uses up' inputs on the board as follows:

4-way expansion board	Relays added	Inputs used up
4-way expansion board 1	Relays 5-8	Uses up inputs IN3, OUT2, OUT3 and OUT4
4-way expansion board 2	Relays 9-12	Uses up inputs IN5, IN6, IN7 and IN8
4-way expansion board 3	Relays 13-16	Uses up inputs IN4, PIG1 and PIG2

For more details on the installation of the 4-way expansion boards see the 4-way expansion board topic.

16-way relay board
The 16-way relay board allows expansion of the outputs of the controller in groups of 16. Using 16-way relay expansion boards the controller can be expanded to have up to 250 relay outputs.

Expanding using 16-way relay boards uses up I/O on the board as follows: IN3, IN4, IN5, IN6, IN7, IN8, OUT2, OUT3, OUT4, PIG1 and PIG2. Effectively this means that only a single reader can be supported on a controller with 16-way relay expansion in place.

For more details on the installation of the 16-way expansion boards see the 16-way relay board topic.

PIG relay output
The system supports a CS innovation called the Point Identification Gadget or PIG. Essentially a PIG is an 'addressable' input or output. PIGs are arranged on a 'pig bus', sometimes driven by a 'pig booster' and allow very cost-effective expansion of the system because they can add as few as a single output and a single input to the system. They also have the advantage that they don't use up as many inputs and outputs on the board.

Output expansion using PIGs is done using the PIG-3 module which has a single relay output and a single input. Multiple PIG-3's can be added to the system on the PIG1/PIG2 bus to provide flexible expansion capabilities.

For more details on the installation of PIG relay see the PIG-3 topic.
More information on the PIG bus can be found in the Point Identification Gadgets topic.

Slave relays connected to unused I/O
With universal firmware any unused input or output can be used to drive a slave relay. There are many 'transistor-driven' relay outputs available, usually used as outputs driven by transistor outputs from alarm panels. Examples are the Nidac CR1 and the MCM slave relay. Any unused input or output port can be used to drive one of these and configured within the system as an additional relay output.

More information on the installation of slave relays can be found in the slave relays topic.

System overview

2.5 Input expansion

It is often desired to expand the number of inputs on the controller.
When the controller is a door/alarm controller additional inputs may be required for exit request, door status, alarm points or alarm control (arm/disarm) inputs.
When the controller is an elevator controller additional inputs may be required for floor destination reporting or for connection of intercom inputs to trigger the outputs.

There are three types of input expansion available.

On-board inputs
The controller has 14 general purpose digital inputs and outputs. These are designated as
IN1-IN8
OUT1-OUT4
PIG1-PIG2
In many cases all of these are 'used up' by readers, expansion boards or other functions. However unused inputs can always be utilised as inputs for any function in the program. For example a 3-reader system with Silkey readers will use up IN1, IN3, IN5 and OUT1, OUT2, OUT3 for the readers. This leaves IN2, 4, 6, 7, 8, OUT4, PIG1 and PIG2 as all spare inputs available for use as exit request, door status or alarm inputs.

16-way input expansion board
The 16-way input board allows expansion of the inputs of the controller in groups of 16. Using 16-way input expansion boards the controller can be expanded to have up to 250 inputs.

Expanding using 16-way input boards uses up I/O on the board as follows: IN3, IN4, IN5, IN6, IN7, IN8, OUT2, OUT3, OUT4, PIG1 and PIG2. Effectively this means that only a single reader can be supported on a controller with 16-way input expansion in place.

For more details on the installation of the 16-way input expansion boards see the 16-way input board topic.

PIG inputs
The system supports a CS innovation called the Point Identification Gadget or PIG. Essentially a PIG is an 'addressable' input or output. PIGs are arranged on a 'pig bus', sometimes driven by a 'pig booster' and allow very cost-effective expansion of the system because they can add as few as a single output and a single input to the system. They also have the advantage that they don't use up as many inputs and outputs on the board.

Input expansion using PIGs is done using various devices including the PIG-2, PIG-3 or PIGPEN modules. PIGs provide a powerful and effective way to expand the inputs.

The PIG-2 adds two additional inputs to the controller. For more details see the PIG-2 topic.
The PIG-3 adds a single additional input plus an output to the controller. For more details see the PIG-3 topic.
The PIG-PEN adds up to 48 addiitonal inputs to the controller. For more details see the PIG-PEN topic.
More information on the PIG bus can be found in the Point Identification Gadgets topic.

System overview

2.6 Software

The software runs on a PC which is connected to the controller network, and allows programming and monitoring of all activities on the system.

There are two software packages available for the system, Advent and PC3. Advent is the flagship product, providing signficantly enhanced capabilities. PC3 is the 'entry-level' software package for the system.

For more details on Advent see the Advent topic.

For more details on PC3 see the PC3 topic.

Comparison of PC3 and Advent software
PC requirements
System overview

2.6.1 Advent

CS Technologies Advent software provides advanced capabilities in the management and control of the CS Technologies access control system. The software runs on a PC and provides all the functionality to define the access control system including controllers, doors, elevators and alarm points. Management of users, timezones and public holidays is very simple, and the system monitors the controllers in the network and logs all transactions to the computer hard disk for retrieval via an easy-to-use report manager.
Advent builds on the reliable PC3 for Windows platform, adding a host of enhanced features including support for multiple communication servers, reporting and logging workstations and an attractive user interface.

As with PC3 for Windows, Advent software is designed to work with Microsoft operating systems under standard IBM-PC architecture. Multiple workstations and communications servers share data via standard 'file sharing' meaning that the system works with any Local Area Network. Advent introduces command buffering, meaning that controllers download 'in the background' allowing fast and convenient interaction with the program. Offline controllers automatically update to the correct information when they come online making the system robust and reliable.

A cornerstone of the CS Technologies system is its reliability which is guaranteed because all of the controllers are fully distributed – they all contain the information required to grant access at a particular door including timezones, public holidays, access levels and of course user credentials. Advent extends this feature by also permitting distributed communications servers. Multiple PC's can be linked together via a LAN with a central database, allowing large systems to be integrated via existing network cabling, without requiring additional dedicated security cables between buildings. If there is a LAN connection between the buildings then the system can encompass all required access points without the need for dedicated inter-building cabling. This can significantly reduce costs as well as making installation fast and simple.

The software incorporates a full range of features to allow comprehensive control of any facility. These include:

- control doors, lifts, alarms from a single integrated front end
- extensive operator control and logging. Operators only see the functions they are allowed to use
- display live status of door, elevator and alarm points
- external interfaces allow easy interfacing to other programs.
- A wide range of readers supported including silicon key, wiegand, mag-stripe (track 1 and 2), proximity, Presco, smartcard and many others. Very flexible configuration options allows just about any credential to be used.
- Multiple workstations and comms servers.

CS Technologies Advent software forms part of an integrated door, elevator, alarm and energy-management system and is the ideal solution for control of any facility.

Comparison of PC3 and Advent software
PC requirements
System overview

2.6.2 PC3

PC3 for Windows software is the 'entry level' software for CS Technologies access control systems. The software provides all the functionality to define the access control system including controllers, doors, elevators and alarm points. Management of users, timezones and public holidays is very simple, and the system monitors the controllers in the network and logs all transactions to the computer hard disk for retrieval via an easy-to-use report manager.

PC3 is a single user system, and any programming done requires that the controllers be online and communicating for the programming to be effective. It allows controls of doors, elevators and alarm areas.

Comparison of PC3 and Advent software
PC requirements
System overview

2.6.3 Comparison of Advent and PC3

Advent and PC3 both work with CS Controllers. However Advent is far more powerful. A summary of the main differences between Advent and PC3 is tabulated below.

Feature	PC3	Advent
Communication with controllers	Controllers must be online for commands to be effective	Commands are buffered for transmission to offline controllers automatically when they come online
Number of PCs	One	Many - one server and multiple workstations
Network layout	Simple - one PC, one com port, up to 128 controllers	Complex - as many PCs as are required. PCs can each have parts of the controller network connected, to form 'locations' each of which can have up to 128 controllers.
Locations	One with up to 128 controllers	Up to 50 each with 128 controllers
Timezones	Up to 20 standard and 20 extended timezones which are shared system-wide	Unlimited - timezones are automatically loaded only into the relevant controllers so many more timezones can be defined.
Access levels	Up to 1000 access levels	Unlimited - access levels are automatically loaded only into the relevant controllers so many more access levels can be defined
Access levels per user	1 door access level and 1 elevator access level	Up to 50 door and elevator access levels per user.
Log window	Yes	Yes
Alarm window	No	Yes
Disarmed areas window	No	Yes
Armed areas window	No	Yes
Toolbar	No	Yes
Alarm handling	No	Yes
Emailing of alarms	No	Yes (with optional email software plug-in)
Programmable macros	No	Yes
Global events	No	Yes
Workstation settings	No	Yes
Ability to change fonts	No	Yes
Modem connections	Rudimentary - a single location can be either directly connected or modem connected	Powerful - each location can be directly connected to one of the PCs in the network or connected via modem to one of the PCs in the network
External interfaces	Basic	Complex - multiple external interfaces defined
Backup	Copies 'DAT' files directly	Creates a zipped backup
Automatic archive	No	Programmable automatic backup occurring at a particular time each day
Auto-delete of backups	No	If enabled, automatically deletes backups more than a month old.

PC requirements

System overview

2.6.4 PC requirements

A typical PC requirement for efficient operation with either Advent or PC3 software would be:

- Intel Pentium II, Pentium III, Pentium 4 or greater
- Windows 95, 98, ME, NT, 2000 or XP operating system
- Minimum of 64MB RAM
- At least 50MB free hard disk space
- One serial (com) port for communications with controllers
- One parallel port for connection of a printer
- Floppy disk drive, CD-ROM, keyboard, mouse
- SVGA monitor configured for at least 800 x 600 screen resolution

Additional requirements for networked Advent
In addition, for networked copies of Advent, all PCs in the network running Advent must be able to 'map drives' for sharing of database and transaction files. The networking on a LAN is thus independent of the network protocol.

The controllers talk to a com port on a PC; the database files (a proprietary format) can reside on the C: drive which can be shared, or of course on a network drive. Other workstations must be able to access the same directory via drive mapping so that they can observe transactions and run reports on the system.

The polling frequency of the shared files can be specified in the software enabling the network overhead to be minimised. The packets being passed are only small and have a negligible impact on the network performance.

Notes
1. Advent and PC3 are both 16-bit applications. This is to ensure compatibility with a wide range of operating systems including Windows 95, 98, ME, NT, 2000 and XP; being 16-bit it will even run on Windows 3.1. Being a 16-bit application it runs in a '16-bit subsystem' (NTVDM) on Windows NT, 2000 and XP.

2. The CS Controller has an inbuilt RS232-485 converter but with Windows ME, NT, 2000 or XP this does not operate due to the hardware abstraction layer which is part of those operating systems. We recommend the use of a CS Technologies 'comms converter' with these operating systems for correct system operation.

3. Advent does not install as a 'service' on Windows NT, 2000 or XP. Advent should be left running on the PC permanently to ensure that transactions from controllers are not lost due to buffer overruns. System administrators should consider this when running on these operating systems as when an operator is not logged in the program will not run. Consideration should be given in these cases to the addition of a 'user' in the operating system which will allow the program to run while logged in while maintaining security for other parts of the system.

System overview

3 Installing the software

3.1 Software installation

Installation of the software is done using a standard Windows installer. The software is generally provided on a CD and there is a menu for the selection of the software package that you wish to install.

Note that all CS Technologies software must be licensed to work on a particular PC. Any of the CS Technologies software can be installed from the CD and will operate properly for 14 days. After this time it will revert to a demonstration mode where it is fully functional except that it will no longer communicate with the controllers. To purchase a license code for your selected program contact your dealer or sales@cstech.biz .

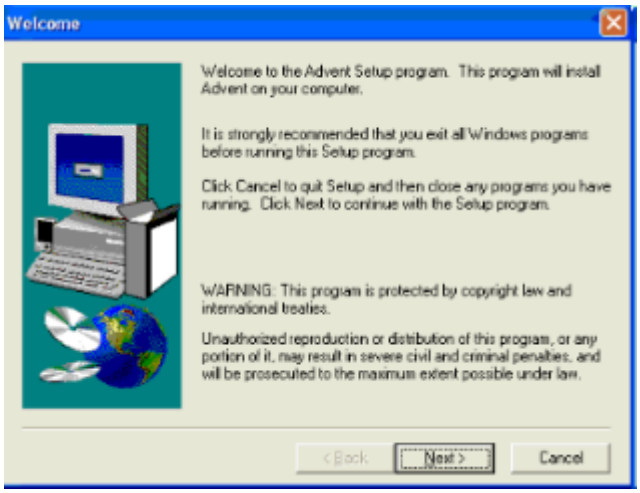
The installation of Advent is covered under the Advent installation topic.

The installation of PC3 is covered under the PC3 installation topic.

The licensing of the program is covered under the Licensing topic.

3.2 Advent installation

Selecting Advent for installation brings up the standard Windows installer.



Clicking 'Next' brings up the license agreement for the software. Read the agreement, and if you agree click 'Yes' to accept the terms of the license. Next an information screen will display with the default name and password. Click 'Next' and enter your name and company on the next page.

The next page asks for the default directory. The default directory will be 'C:\CSTECH'; the directory tree will be created under this. Unless you have a good reason it is wise not to change this as it makes support for the product easier if the location is not changed.

Next you will be asked for the program folder. Accepting the default setting will create a program group in your start menu for CS Technologies files and put Advent in it. Click Next again and a summary of the selected options will be displayed; click Next here and the program will be installed.

Note that if the installation is an upgrade from an earlier version of Advent the existing data files will not be overwritten by the installer. However to be certain it is strongly recommended that a backup of existing data be taken. When initially installed some default tables are created in the database; if the installation is an upgrade the existing data files will not be overwritten.

When the program is first run a default login name and password will have been created. The

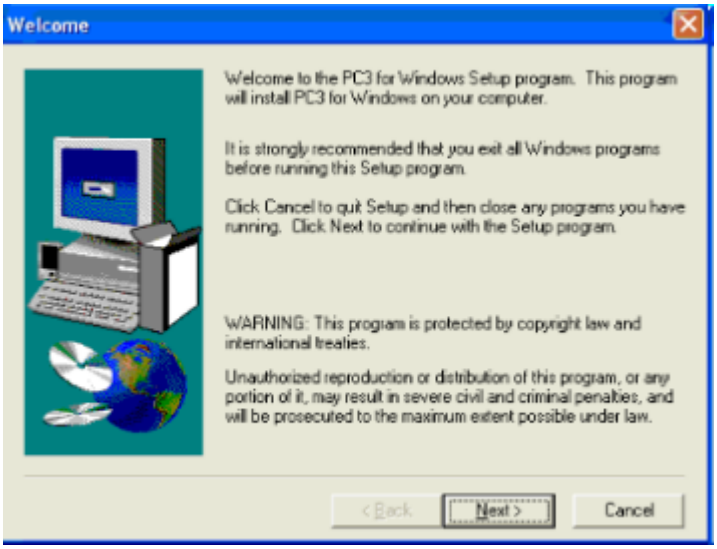
default login name is **123** and the default password is also **123**.

When first installed the program is in evaluation mode for 14 days. It must be licensed to continue to work after this time. You will have been provided with a license code (a number something like ADVENT1.0-ABCD-1234-5678-1234); see the section on licensing for more information.

Software installation overview

3.3 PC3 installation

Selecting PC3 for installation brings up the standard Windows installer.



Clicking 'Next' brings up the license agreement for the software. Read the agreement, and if you agree click 'Yes' to accept the terms of the license. Next an information screen will display with the default name and password. Click 'Next' and enter your name and company on the next page.

The next page asks for the default directory. The default directory will be 'C:\CSTECH'; the directory tree will be created under this. Unless you have a good reason it is wise not to change this as it makes support for the product easier if the location is not changed.

Next you will be asked for the program folder. Accepting the default setting will create a program group in your start menu for CS Technologies files and put PC3 in it. Click Next again and a summary of the selected options will be displayed; click Next here and the program will be installed.

Note that if the installation is an upgrade from an earlier version of PC3 the existing data files will not be overwritten by the installer. However to be certain it is strongly recommended that a backup of existing data be taken. When initially installed some default tables are created in the database; if the installation is an upgrade the existing data files will not be overwritten.

When the program is first run a default login name and password will have been created. The default login name is **123** and the default password is also **123**.

When first installed the program is in evaluation mode for 14 days. It must be licensed to continue to work after this time. You will have been provided with a license code (a number something like PC31.0-ABCD-1234-5678-1234); see the section on licensing for more information.

Software installation overview

3.4 Licensing

Overview

All software produced by CS Technologies is covered by licensing system, which ensures that each copy of any CS Technologies product is licensed for use on a particular computer. The introduction of licensing means that all products can be freely distributed, downloaded from the internet etc, but once installed will work as evaluation or demonstration versions unless they are authorised.

All of the programs are authorised using the CS Technologies "License" program. This is installed along with any of the other products, and enables licensing of the products for use on a particular computer.

When any product is first installed it will be set up as being in 'evaluation mode'. The evaluation period of the software depends on the product itself and is typically 14 days. After this evaluation period expires the software will revert to 'demonstration' mode where key functionality is not available. For example, the demonstration mode of PC3 software restricts the communications of the software with controllers so that it can be used to demonstrate the features of the system but not used to communicate with controllers.
Any program to be licensed will be provided with a 'license code' which is for that particular product. A license code is a number like the following:

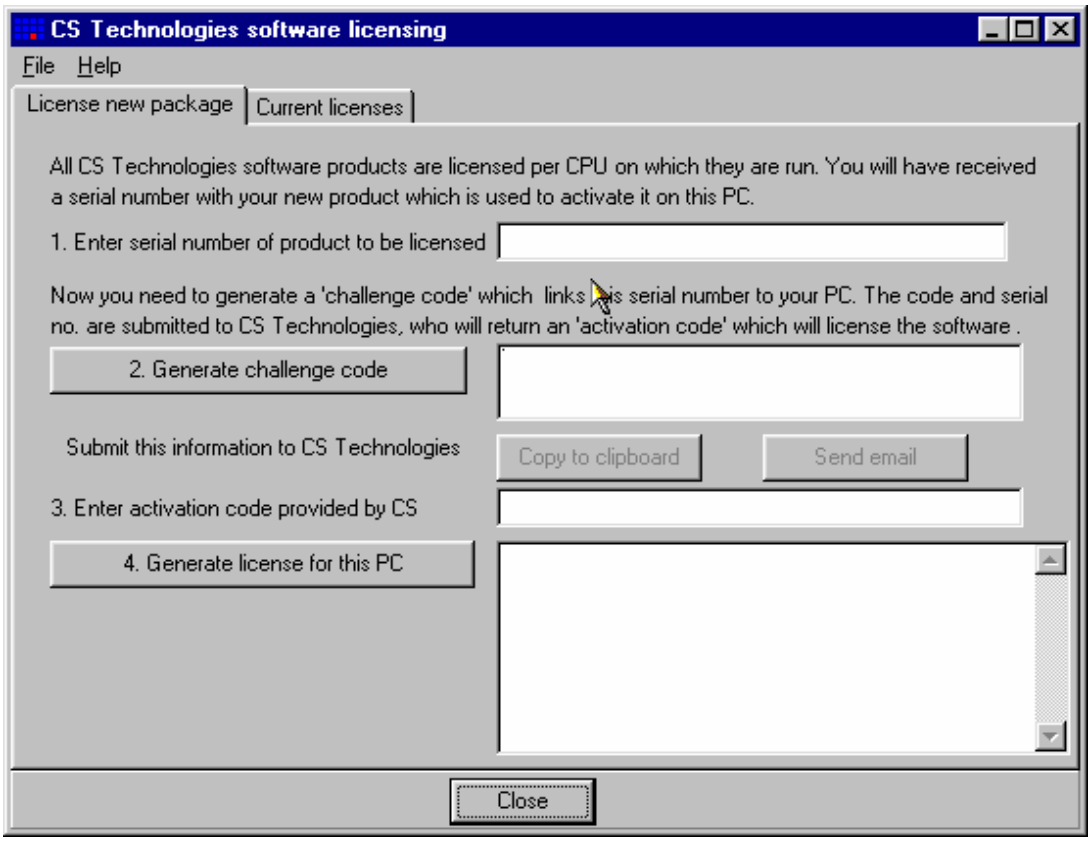
PC31.0-1234-4567-1234-BA12

The license code contains the product name and version, its serial number and details of the license period – unlimited or restricted to a certain time. All this information is encrypted into the license code.
In order to license the software to a particular computer, the licensing application is used. The license code is entered into the program and a 'challenge code' is generated. This challenge code along with the license code is sent to CS Technologies where it is validated and a 'response code' returned.
The response code is entered into the licensing application and this will license that particular program for use on that computer.

The licensing program
Software installation overview

3.4.1 The licensing program

The licensing program is called LICENSE.EXE. It is normally installed with the software to be licensed, but can also be installed separately. It resides in the C:\CSTECH\LICENSE directory. When the license program is run the window below is displayed.

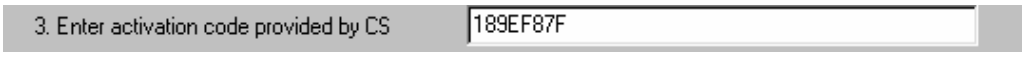


In order to license a software package, enter the serial number (license code) of the product to be licensed.

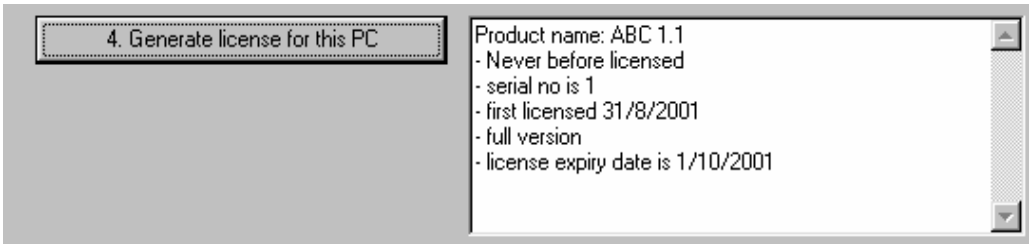
Then press the 'Generate challenge code' button. The license code will be checked for validity and if valid, a challenge code will be generated.

This information must be submitted to CS Technologies. This can be done by email (simply by clicking on the 'send email' button to open your email program with the relevant details to support@cstech.biz), or by fax, post etc. For convenience the license code and challenge code information can be copied to the clipboard for easy inclusion in a word processing program etc by clicking the 'copy to clipboard' button. You also need to detail the site name and contact details for future technical support.

CS Technologies will process the request and validate the serial number and challenge code. In the meantime the licensing program can be exited; the information entered will be saved for the next time it is run so that the license code will not need to be re-entered.
Once the activation code is received, run the program again and enter the activation code.



Now click the 'Generate license for this PC' button. If the activation code matches the license code then the software will be successfully licensed for use on that PC.



The license details will display, and the program can be exited.
Now when the program is run it will no longer be in evaluation mode. The Help/About screen will display the license details and the program will be fully operational.

Software installation overview

4 Installing controllers

4.1 Controller installation overview

Installation of the controller consists of several steps:

Mounting the controller

Connecting power supply

The circuit board

Configuring communications

Setting up the controller in software

4.2 Mounting/mechanical

The controller consists of a circuit board mounted in a lockable steel cabinet. The key to the cabinet is taped to the outside of the box.

The controller box should be mounted using heavy duty screws to a firm surface, probably a wall. For ease of access the controller should be in a well-lit easily accessible spot.

As with any electrical equipment the controller should not be mounted anywhere that water is likely to go. Also, when drilling holes in the box for cable entries etc it is wise to remove the circuit board to ensure that foreign matter such as steel shavings does not interfere with the electronics.

All cable connections to the circuit board are made using push-on connectors so removal and installation of the circuit board is very easy.

Controller installation overview

4.3 Power supply

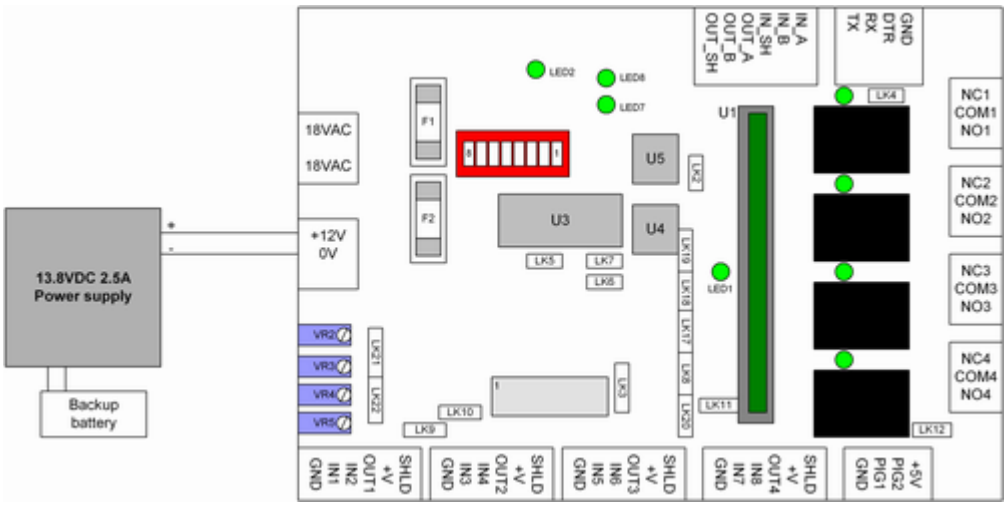
The system has two terminals for power connection. It can be powered by either 16-18VAC or 12-14VDC.

DC Power
It is strongly recommended that the controller be powered by 12-14VDC. This ensures that there is ample supply for both the controller and any peripherals as well as door strikes. For convenience, when powered by 12-14VDC the same supply can be used to power door strikes. Usually the power is provided by a 13.8V power supply which will also have an integrated battery charger. This ensures that battery backup is also provided for the system.

Reference should be made to the current requirements when calculating the size of power supplies required.

When power is connected to the controller the power LED (LED2) indicates that power is on.

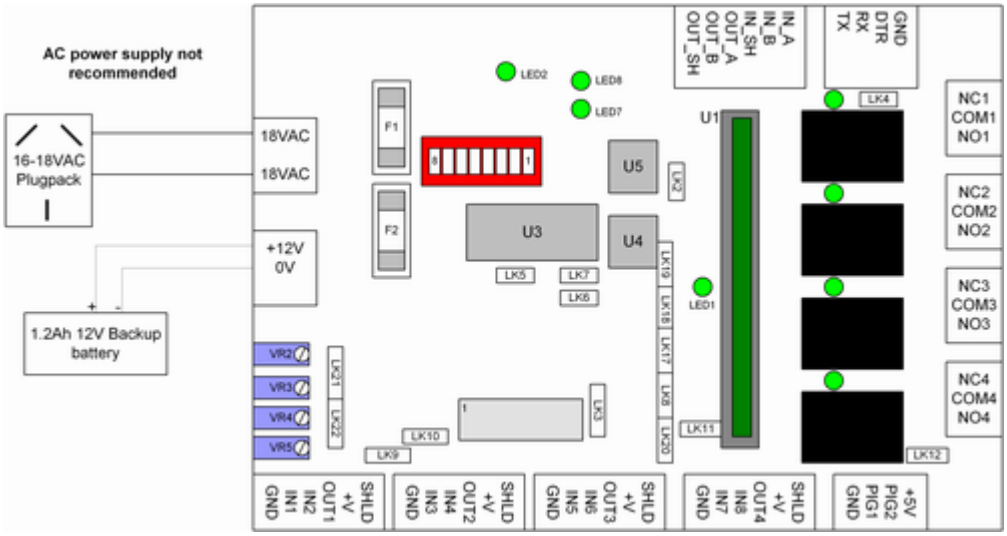
The diagram below shows the connections for a DC power supply for the controller.



AC Power

In some applications it is convenient to power the controller from an AC plugpack. This is not recommended as better results are obtained when the controller is powered by DC. In this configuration a 12V 1.2Ah rechargeable battery can be connected to the battery terminals to provide power to the controller in the event of an AC power failure. The plugpack should be dedicated to powering the controller, and the battery terminals must not be used to power electric strikes or other equipment in this configuration.

The diagram below shows the connections for an AC power supply for the controller.



Reference should be made to the current requirements when calculating the size of power supplies required.

Controller installation overview

4.3.1 Current requirements

When installing controllers and expansion boards consideration should be given to ensure that there is sufficient current capability within the power supplies to keep all equipment operating.

The table below gives the suggested allowances that should be made for each part of the system.

If door strikes are being powered by the same supply ensure that allowance is also made for the current draw of the door strikes also.

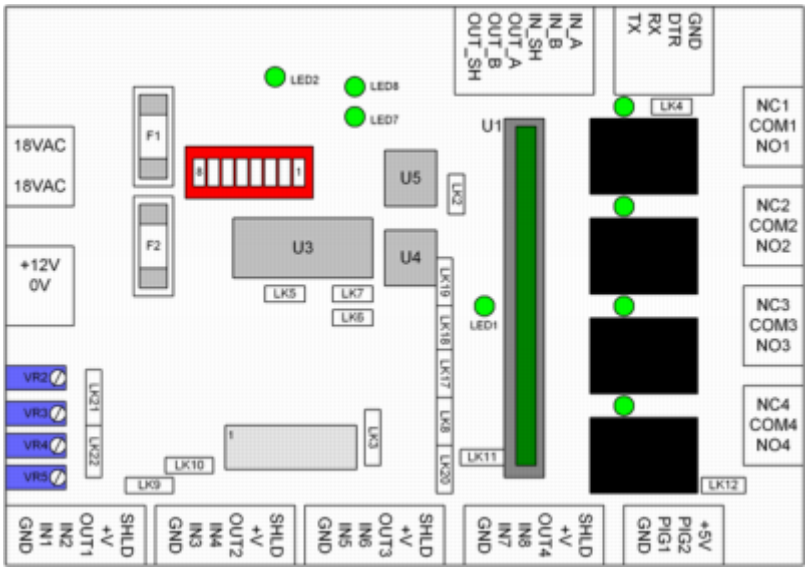
If multiple power supplies are used to provide power to expansion boards ensure that the 0V of all the supplies are tied together to ensure a common reference.

Device	Current draw
Controller	400mA
4-way relay expansion board	300mA
16-way relay expansion board	1A
16-way input expansion board	300mA
PIG-2 (2 inputs)	30mA
PIG-3 (1 input and 1 output)	50mA
Comms converter	200mA

Controller installation overview

4.4 The circuit board

A diagram of the circuit board is shown below.



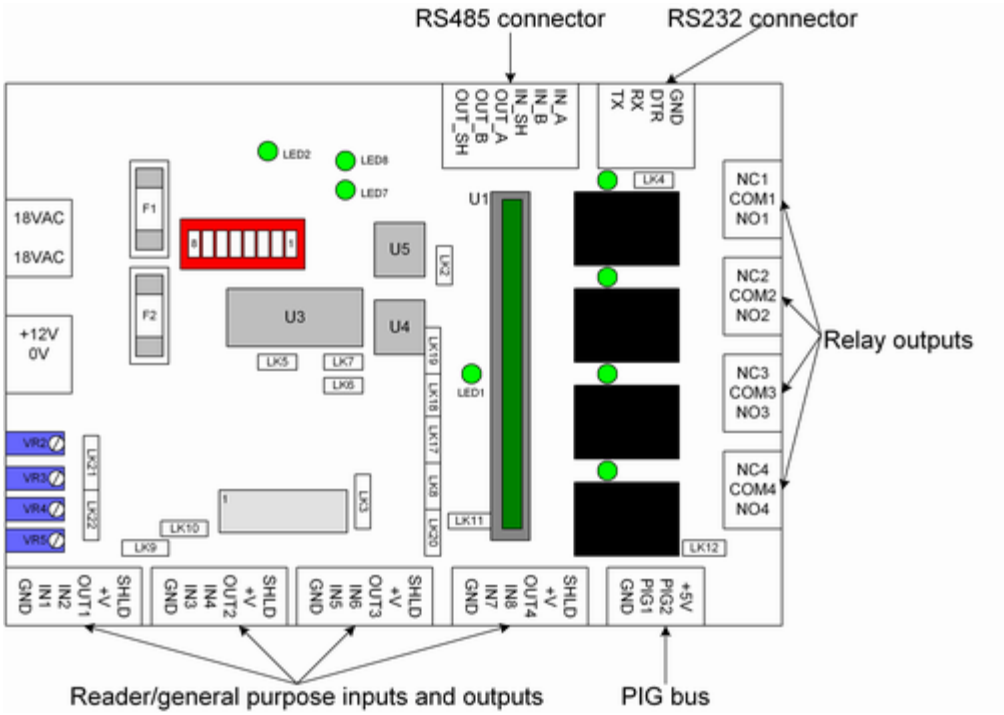
The various items on the circuit board are explained in the following sections.

Connectors
LEDs
Adjustable potentiometers
Expansion port
Fuses
Communications
The chip
Links

Controller installation overview

4.4.1 Connectors

The diagram below shows the connectors on the board.



The RS485 and RS232 connectors are used for connecting the controller to the communications bus. For more details on setting up communications see the communications topic.

The relay outputs are 'form C' contacts (voltage-free) for the four on-board relays. The relays are rated to switch up to 2A at 12VDC.

The four 6-way connectors on the bottom of the board are generally used for connection of readers. Inputs and outputs here which are not used for readers can be used for connection of exit buttons, door status inputs or other inputs on the board (subject to use of expansion boards and interrupts).

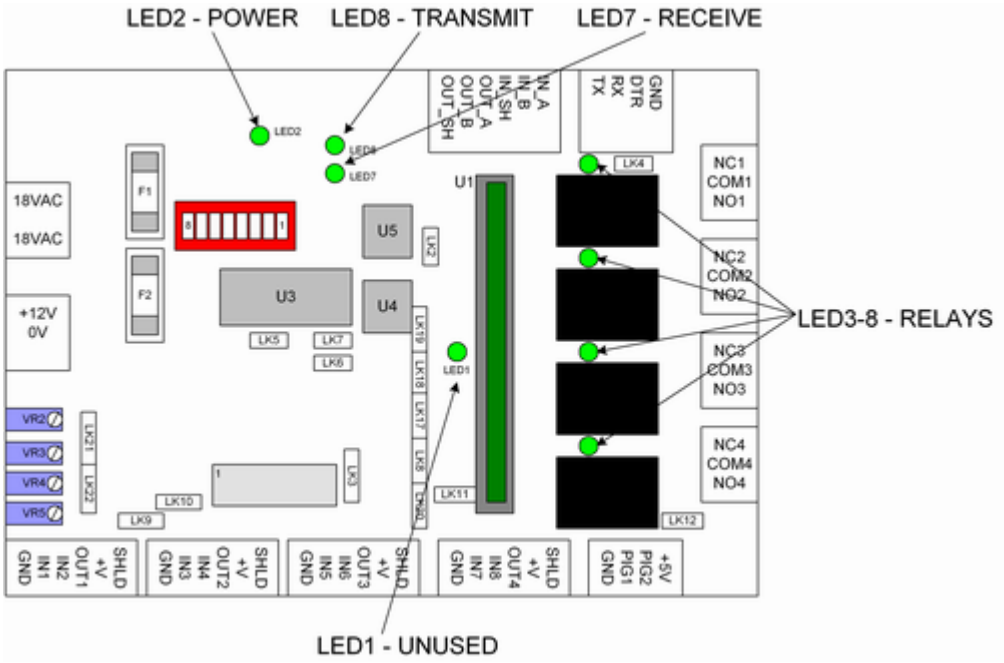
Finally the PIG bus contains two ports which can be used for connection of PIGs or as single inputs.

LEDs
Adjustable potentiometers
Expansion port
Fuses
Communications
The chip
Links

Controller installation overview

4.4.2 LEDs

There are a number of LEDs on the board which are used to indicate various conditions.



LED1 (to the left of the firmware chip) - with earlier versions of firmware this LED was used to indicate communications. With universal firmware this LED flashes during some memory accesses but is otherwise unused.

LED2 - this LED indicates power connection to the board

LED3, LED4, LED5, LED6 - there is one of these LEDs per relay. They indicate whether the associated relay is active.

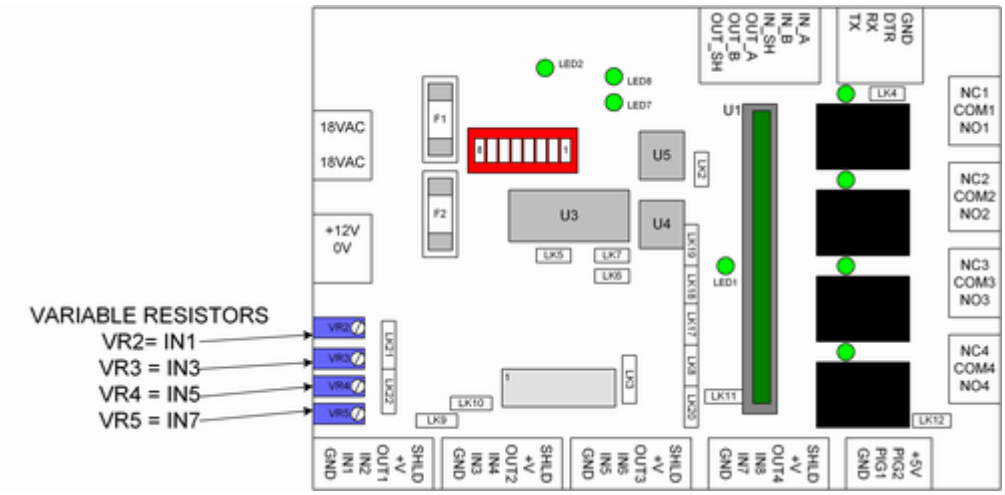
LED7, LED8 - these indicate communications in progress. LED7 is the 'Receive LED'; it flashes whenever the controller is receiving a message from the PC. LED8 is the 'Transmit LED'; it flashes whenever the controller is sending a message.

Connectors
LEDs
Adjustable potentiometers
Expansion port
Fuses
Communications
The chip
Links

Controller installation overview

4.4.3 Variable resistors

There are four variable resistors on the left hand side of the board. In earlier versions of the controller these were used to trim the input resistance for some Silkey applications where readers were a long way from the controller. However these are now no longer used, and Pig boosters are used instead to boost the distance for communications of Silkey readers. The diagram below shows the location of these variable resistors.



The variable resistors should be supplied from the factory set at 1.5K. No adjustment should be necessary; however for completeness the testing procedure for these is below.

To test this resistance, power down the controller and use a resistance (ohm) meter connected as follows:

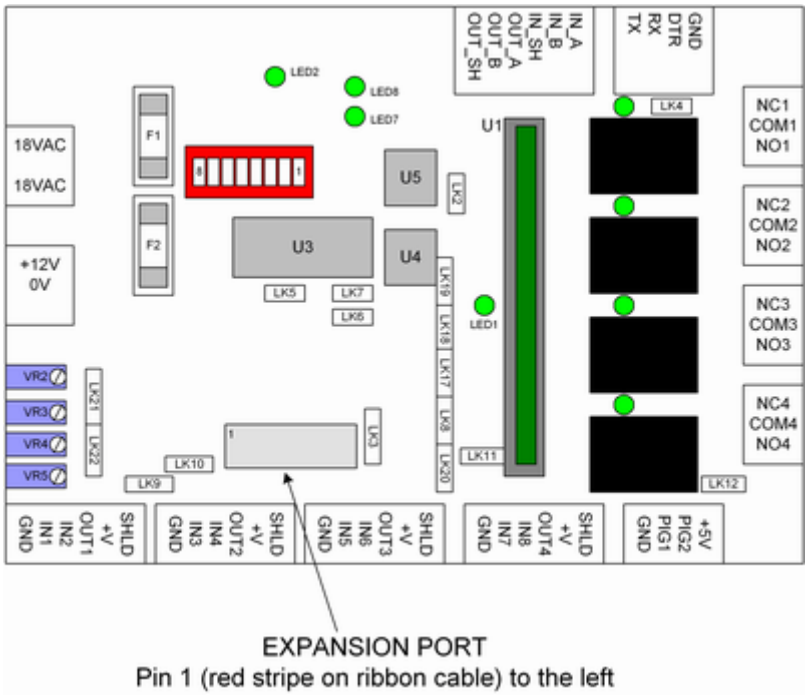
Variable resistor	Connections
VR2	IN1 and +V
VR3	IN3 and +V
VR4	IN5 and +V
VR5	IN7 and +V

Connectors
LEDs
Expansion port
Fuses
Communications
The chip
Links

Controller installation overview

4.4.4 Expansion port

The controller has a built-in expansion port for connection of 4-way relay boards, 16-way relay boards and 16-way input boards.



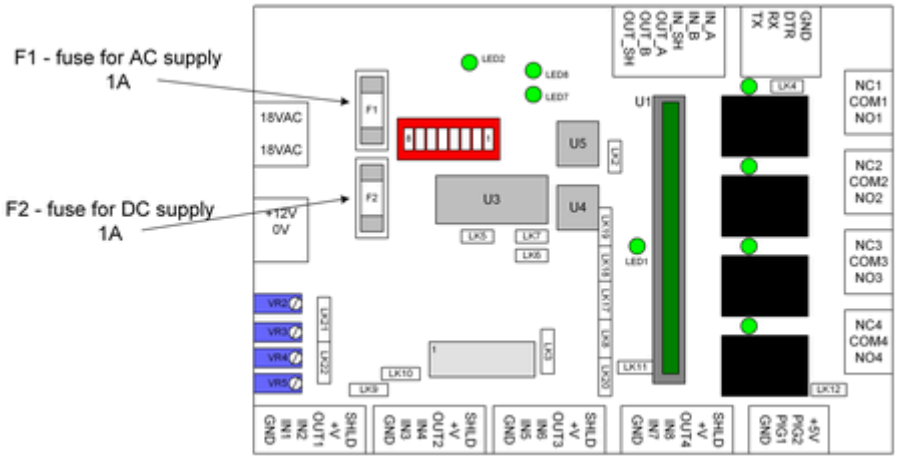
This expansion port is a 16-way header. Pin 1 on the header is always to the left, and when expanding the ribbon cable will have a red 'trace' which should also be to the left to ensure that correct polarity is maintained.

Connectors
LEDs
Adjustable potentiometers
Expansion port
Fuses
Communications
The chip
Links

Controller installation overview

4.4.5 Fuses

The controller has two on-board fuses. One of these is in series with the AC supply; the other is in series with the DC supply.



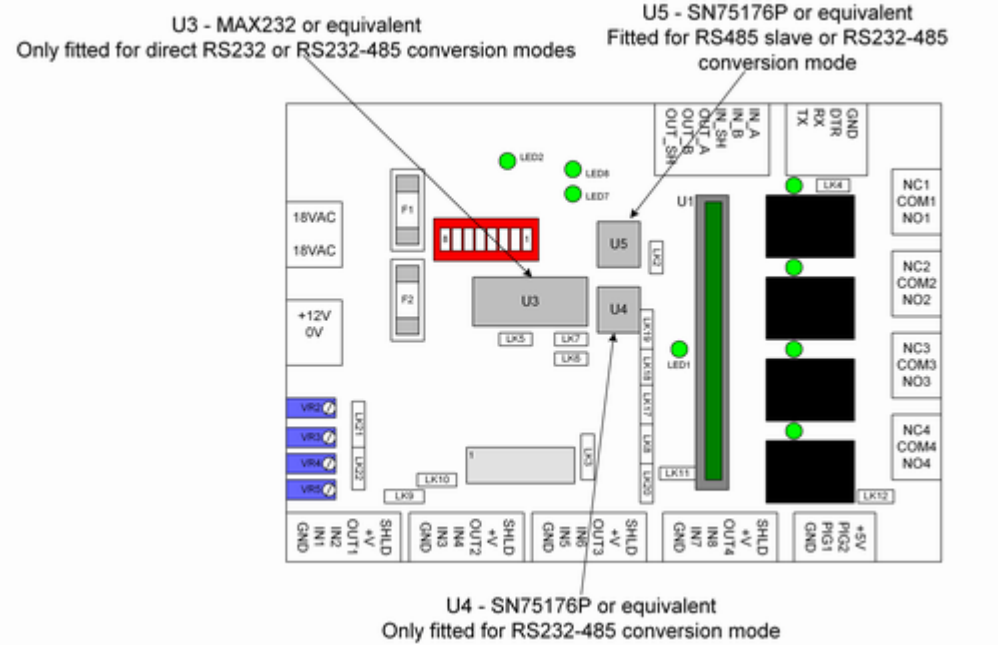
Both fuses are rated at 1A. If the controller is powered by DC (as recommended) only the DC fuse (F2) has any function.

Connectors
LEDs
Adjustable potentiometers
Expansion port
Communications
The chip
Links

Controller installation overview

4.4.6 Comms chips

There are sockets for three comms chips on the controller. These are labelled U3, U4 and U5 and are shown on the diagram below.



The controller can communicate in three modes:

Direct RS232 - only U3 is fitted
RS232-485 conversion - U3, U4 and U5 are all fitted
Slave RS485 - Only U5 is fitted

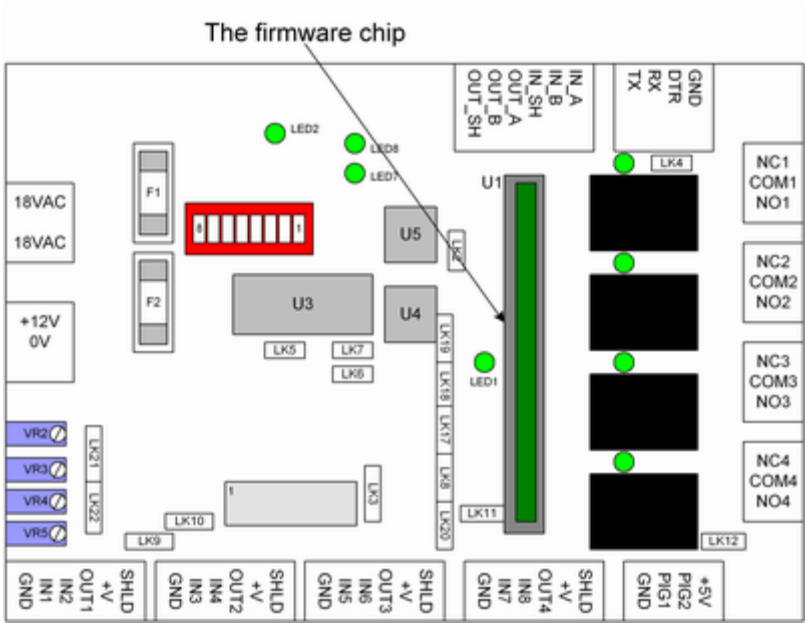
There are also link settings which are made in association with these different modes. For more details regarding configuration of these chips see the communications topic.

Connectors
LEDs
Adjustable potentiometers
Expansion port
Fuses
Communications
The chip
Links

Controller installation overview

4.4.7 The firmware chip

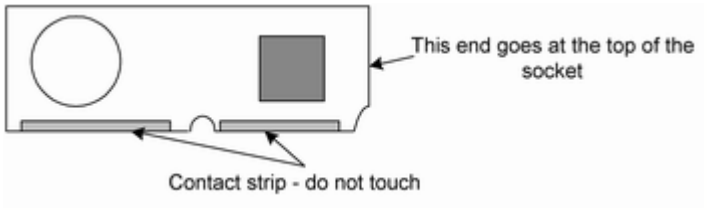
The firmware chip contains all the programming for the system. It is shown on the diagram below.

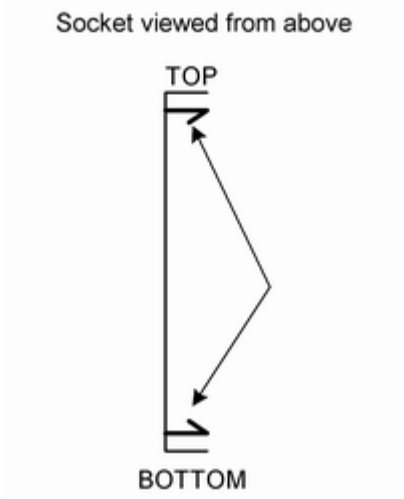


The firmware chip stands vertically adjacent to the on-board relays.

Changing the chip
Occasionally it may be necessary to change the chip in order to upgrade the firmware. This can be easily done provided a few simple precautions are taken.

The chip is shaped as below. The end with the curved section taken out goes at the top of the socket. The diagram below shows the socket.

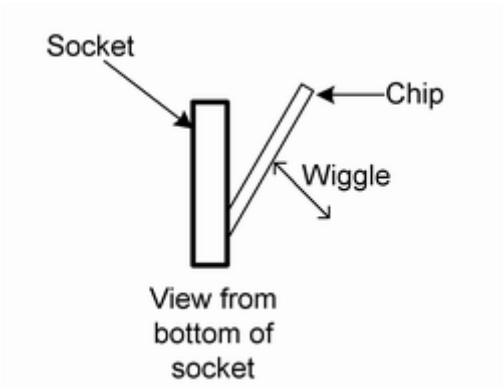




To REMOVE the chip
1. Remove all power from the system. This can be done by unplugging the two connectors on the left hand side of the board labelled AC and BAT.
2. Push back the two retaining clips at the top and bottom of the socket and gently push the chip sideways to the right. It will come free and be able to be removed.

To INSERT the chip
1. Remove all power from the system.
2. Place the chip, with the curved end at the top of the socket, on an angle as shown. Wiggle the

chip a few times to ensure that it is correctly seated, then stand the chip vertically so that it clips into place.

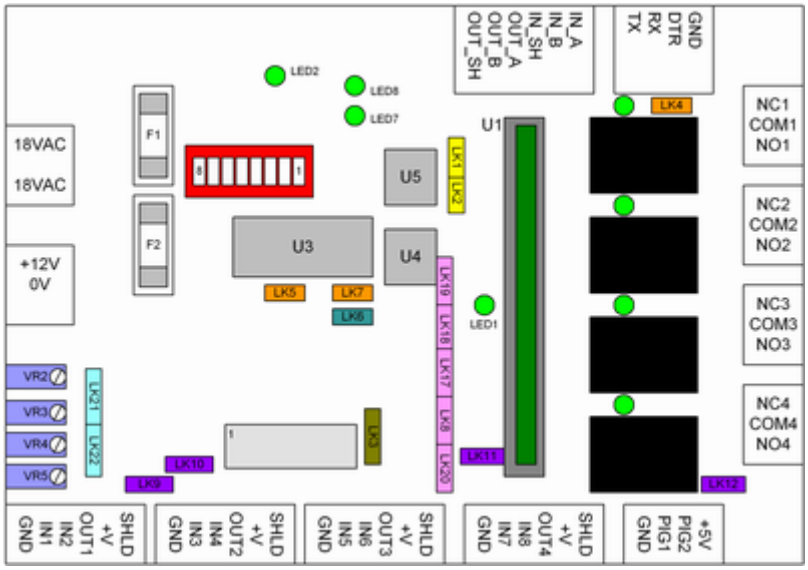


Connectors
LEDs
Adjustable potentiometers
Expansion port
Fuses
Communications
Links

Controller installation overview

4.4.8 Links

There are a number of links on the board, used to configure it for various functions. The diagram below shows the different links and the table describes their functionality.



Colour	Link numbers	Name	Function
LK1	LK1, LK2	Firmware downloading links	Used for downloading of firmware to the controller using CS Technologies 'DL' program. In normal operation both links are off. LK1 can also be used for connection of a normally open 'reset' switch.
LK3	LK3	SPK control link	This two-position link enables the speaker. When this link is DOWN, the speaker is enabled; when it is UP the speaker is disabled and the speaker signal is used to drive 16-way expansion boards. This link must be UP for 16-way expansion boards, or otherwise DOWN.
LK5	LK4, LK5, LK7	Comms links	LK4 is the 'end of line' termination for the RS485 bus. Generally left OFF. LK5, LK7 are ON if the comms is in RS232 direct mode, otherwise OFF. For more details see the communications topic.
LK6	LK6	Standalone keypad link	This link is always OFF for universal firmware. The only situation in which it is used is for a programming keypad with standalone firmware.
LK18	LK8, LK17, LK18, LK19, LK20	Reader interrupt links	These links are used to configure which inputs cause interrupts to the processor for different types of readers. For more details see the individual reader configuration topics. The links are associated with inputs as follows: IN2 - LK20 IN3 - LK19 IN4 - LK18 IN5, IN7 - LK17 IN6, IN8 - LK8 If 16-way expansion boards are fitted then LK19, 18, 17 and 8 must be OFF.
LK9	LK9, LK10, LK11, LK12	Reader LED resistor links	These links are used to short out a current limiting resistor in series with OUT1-OUT4. Usually OUT1-OUT4 are used to drive reader LEDs. With these links out then a LED can be placed directly between the respective OUT and +V. With these links in, the reader itself must provide current limiting for the resistor. Generally these links are IN.
LK21	LK21, LK22	Voltage selection links	LK21 should be DOWN (towards the centre) unless Presco keypads are being used. When in the UP position this provides a higher input voltage on IN1, IN3, IN5 and IN7 which is required by Presco keypads. For all other readers LK21 should be down. LK22 should be UP (towards the centre) to provide 5V to the '+V' connectors for each reader port. If it is DOWN then 12V is provided to the '+V' connectors. This is to provide flexibility in powering readers. When changing this always ensure that the reader voltage is suitable for the setting chosen.

Connectors
LEDs
Adjustable potentiometers
Expansion port
Fuses
Communications

The chip

Controller installation overview

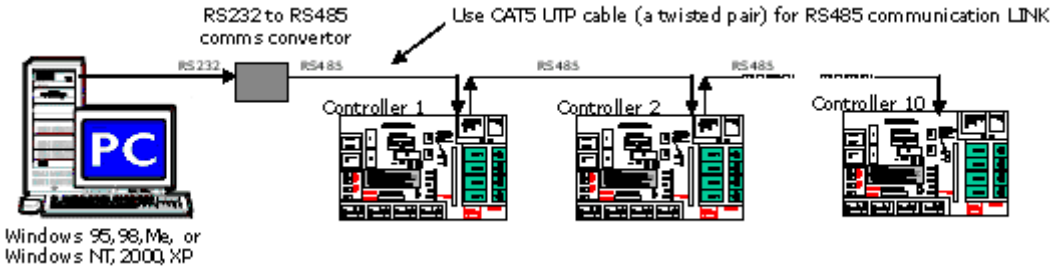
4.5 Communications

Once the controller is installed the next step is getting it communicating with the PC.

Controller addressing
Each controller has an 8-way DIP switch which is used to set the controller address. Controllers can be numbered from 1 to 128 using the DIP switches. Details of the addressing can be found in the controller addressing topic.

Controller modes
The controller can be configured for three different communication modes. The default mode is RS485 slave mode, where U5 is present, U3 and U4 are absent and LK5 and LK7 are absent. More detail about the communication modes can be found in the communication modes topic.

Setting up the communications network
The standard way of setting up the communications involves the use of a Comms Converter. This takes the RS232 output of the PC and converts it to RS485 for communicating with the controllers. Each controller is set up in RS485 slave mode. A schematic diagram of the system layout is below.

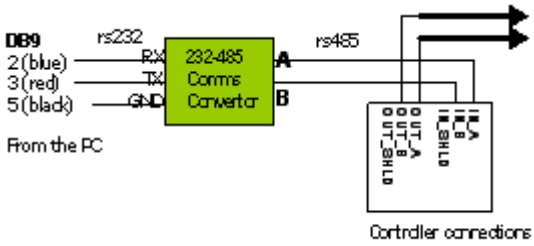


In this mode, the RS232 signals from the PC are converted to RS485 in the converter. A twisted pair links the controllers all in parallel. The controllers are all configured as RS485 slaves, and there is no connection to the RS232 connector on any of the controllers.
This will work with any Windows operating system.

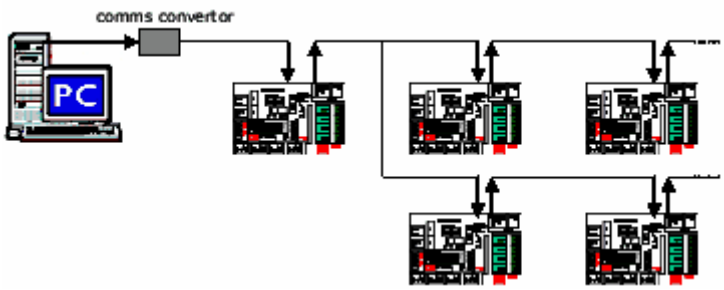
The PC connects to the comms converter using only the RX, TX and GND connectors. PC's generally have one or more serial ports which are either 9 or 25-pin male connectors. The signals from the serial port connect as follows:

9-pin serial port pin	25-pin serial port pin	Signal name	Comms converter connection
2	3	TX	RX
3	2	RX	TX
5	7	GND	GND
4	20	DTR	Not connected

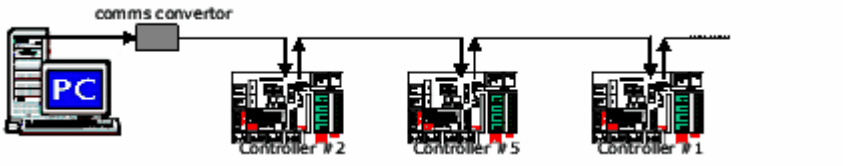
The comms converter converts the signals to RS485 which come out on the A and B wires and connect to the controller bus. Each controller has IN_A and IN_B signals, and OUT_A and OUT_B signals for sending the signal onto the next controller. A diagram of the setup is shown below.



The controllers must be connected in a 'daisy-chain' configuration, one to the next. If it is necessary to 'tee off' the bus for any reason this should be done using back-to back comms converters. The following configuration is **NOT acceptable**.



Controllers need not be numbered consecutively; as long as each controller has a unique ID then they will all communicate without conflicting.

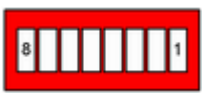


Controller addressing
Communication modes
Comms converter

Controller installation overview

4.5.1 Controller addressing

Each controller must be addressed with a unique DIP switch combination. The DIP switch is a blue or red array of 8 switches located to the right of the fuses.



The switches are DOWN to turn them ON and UP to turn them off, as labelled on the switch. Combinations of the switches are used to select a controller number as follows:

Switch 1	1
Switch 2	2
Switch 3	4
Switch 4	8
Switch 5	16
Switch 6	32
Switch 7	64

Switch 8 is not used.

For example, to address a controller as number 13, switches 4, 3 and 1 would be on because 13 = 8 + 4 + 1.

The table below shows the switches which are on for controllers up to 29.

Controller ID	SW 1	SW 2	SW 3	SW 4	SW 5	SW 6	SW 7
1	ON						
2		ON					
3	ON	ON					
4			ON				
5	ON		ON				
6		ON	ON				
7	ON	ON	ON				
8				ON			
9	ON			ON			
10		ON		ON			
11	ON	ON		ON			
12			ON	ON			
13	ON		ON	ON			
14		ON	ON	ON			
15	ON	ON	ON	ON			
16					ON		
17	ON				ON		
18		ON			ON		
19	ON	ON			ON		
20			ON		ON		
21	ON		ON		ON		
22		ON	ON		ON		
23	ON	ON	ON		ON		
24				ON	ON		
25	ON			ON	ON		
26		ON		ON	ON		
27	ON	ON		ON	ON		
28			ON	ON	ON		
29	ON		ON	ON	ON		

Communication modes
Comms converter

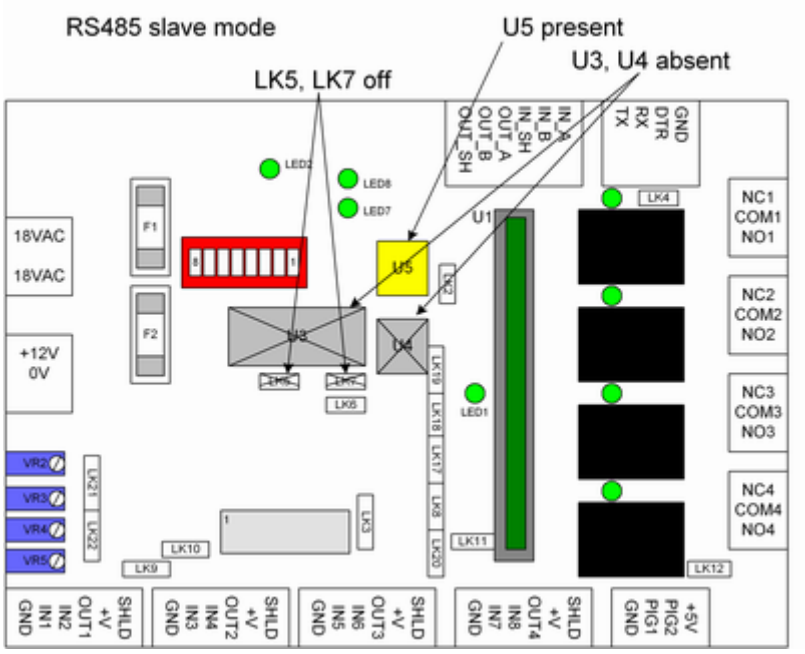
Communications

4.5.2 Communication modes

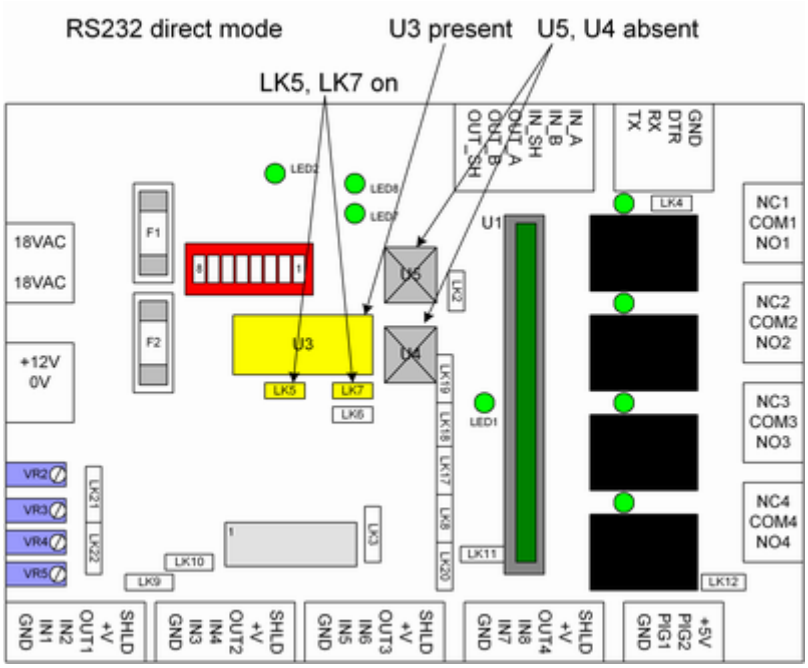
There are three possible communication modes for the controller.

RS485 slave mode
This is the most common configuration for the controller. In this mode, the RS485 bus is used for communicating and each controller is a slave. There is usually a comms converter between the PC and the controllers.

To set up a controller in this default mode, U3 and U4 are removed and U5 is present.
LK5 and LK7 are not present.

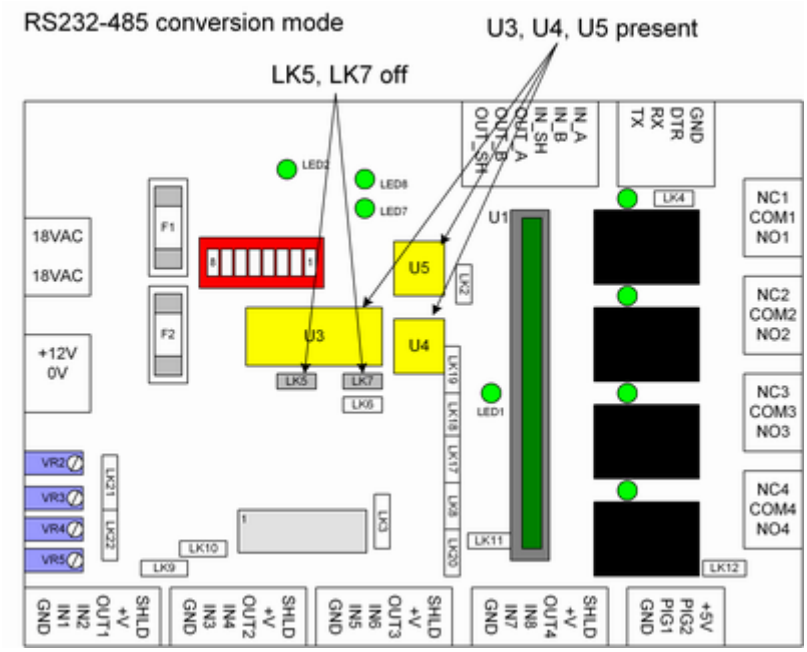


RS232 direct mode
In this mode the PC talks directly to the controller. Only a single controller can communicate with the PC in this way. Sometimes this is used to test the communications link from the PC.



RS232-485 conversion mode

In this mode the controller converts RS232 from the PC to RS485 for the controller bus. This mode **does not work** with Windows ME, NT, 2000 or XP because the required signals from the PC (DTR) are not generated by these operating systems. If this mode is used, only one controller can be configured in this way, and this is the controller which is connected to the PC.



Controller addressing
Comms converter

Communications

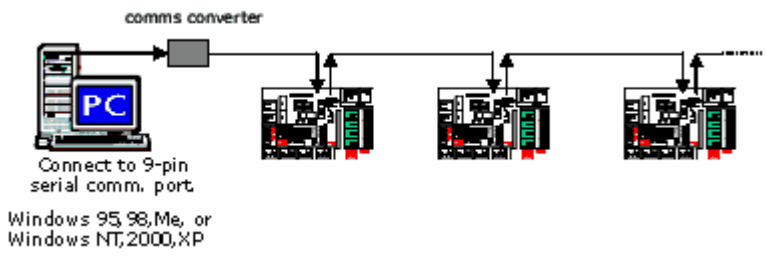
4.5.3 Comms converter

The CS Technologies RS232 to RS485 converter is a compact, easy to install device ideal for:

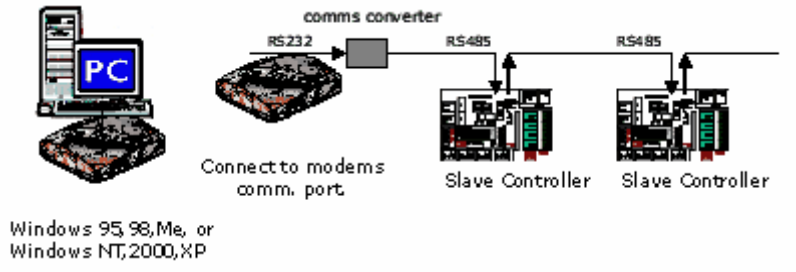
- connecting the controller and PC over large distances
- direct connection of the controller to a Windows ME, NT, 2000 or XP machine
- connection between modems and controllers

The converter has an RS232 input for connection to a PC or a modem, and an RS485 port which is used for connection to the communications bus on all the controllers.

A typical configuration of the comms converter communicating to multiple controllers is shown below.

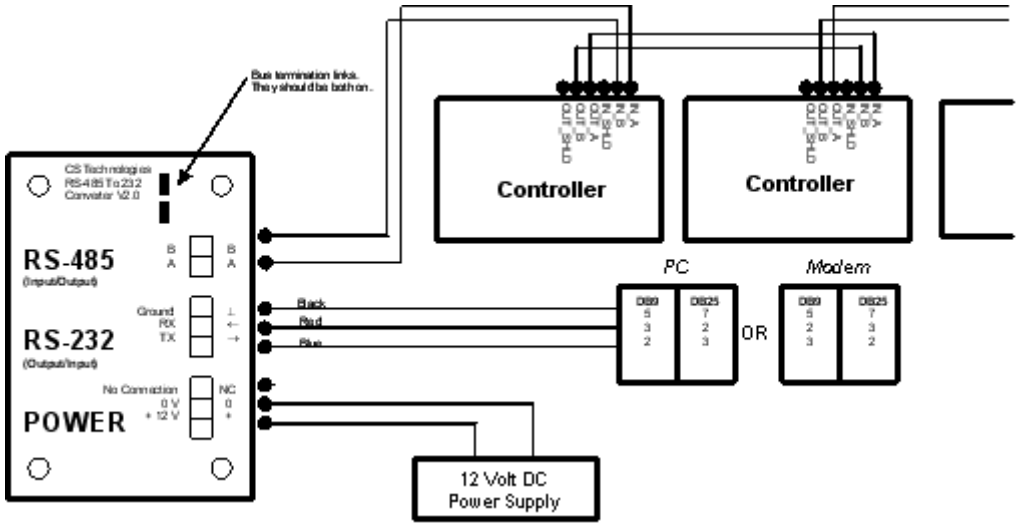


Another use of the comms converter is to facilitate modem communication. A typical configuration is shown below.



The port on the PC or modem will be a 9 or 25-pin com port. The TX, RX and GND signals from the com port connect to the comms converter. The converter also requires 12VDC for operation.

A diagram of the converter and its wiring is below. 12VDC is supplied to the converter. The RS232 device (PC or modem) connects to the RS232 port of the modem using the RX, TX and GND connections. The RS485 output from the converter A/B connects to IN_A and IN_B on the first controller and the communications continues from that controller OUT_A and OUT_B to the IN_A and IN_B of the next controller and so on.
The controllers are all configured as RS485 slaves (U5 in, U3 and U4 out and LK5+7 out).



Controller addressing
Communication modes

Communications

4.6 Configuration in software

Once the controllers are installed the next step is to get them communicating with the software (PC3 or Advent). Instructions for doing this are detailed below for both of these programs.

Configuring controllers in Advent

Configuring controllers in PC3

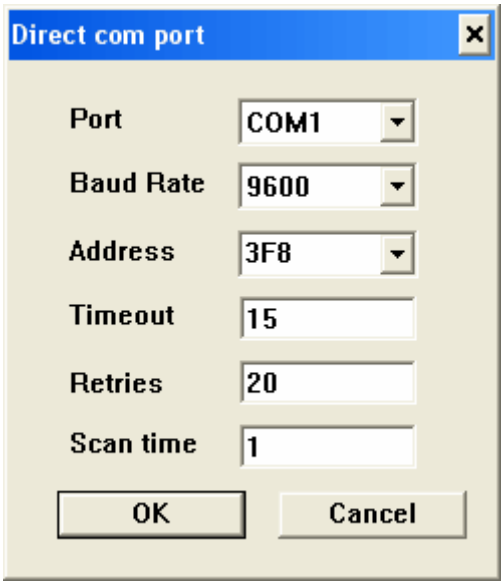
4.6.1 Configuring controllers in Advent

When you run Advent, the first thing to do is log in. This is done by clicking the 'key' which appears in the toolbar at the top of the screen.

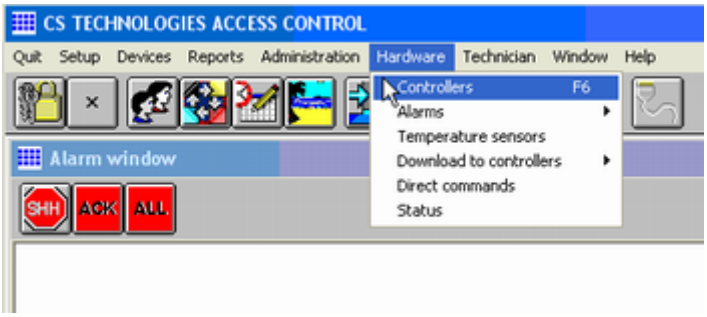
Clicking on this key brings up the login screen. The default login name is 123 and the password is also 123.

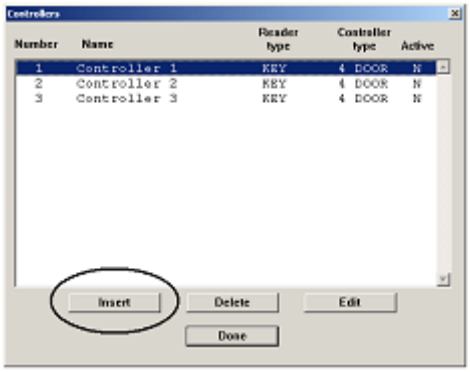
The com port selection is made by clicking the 'com port' icon in the toolbar.

Select the com port as the one to which the controllers are connected.



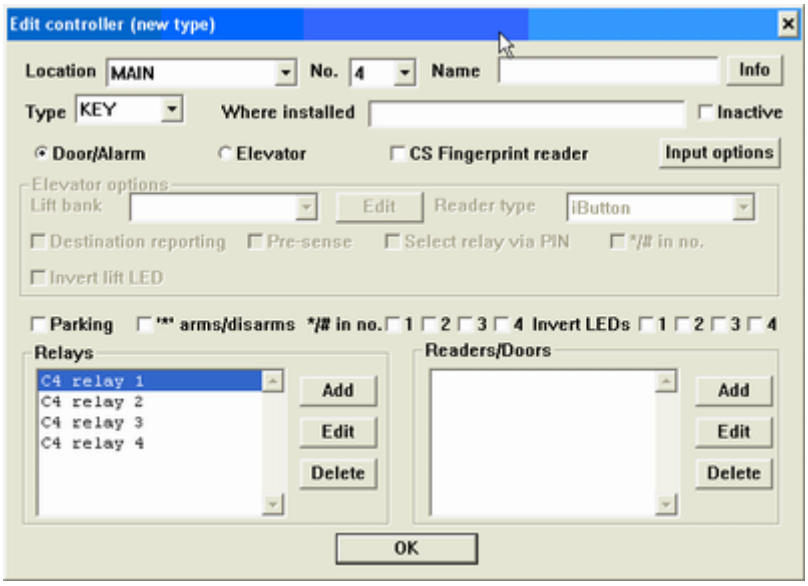
The next step is to add the controllers to the database (Hardware/Controllers/Insert).





For each controller you should

- Name the controller
- Select the type of reader (KEY = Silicon key, PIN = Keypad, CARD = wiegand card, ABACARD = a card where all digits are significant, ALARM = no readers, just alarms)
- Select whether it is Door/Alarm or Elevator firmware



By pressing the 'Add' button in the Readers/Doors group box it is now possible to add doors to the system. More information on door programming can be found in the Doors topic.

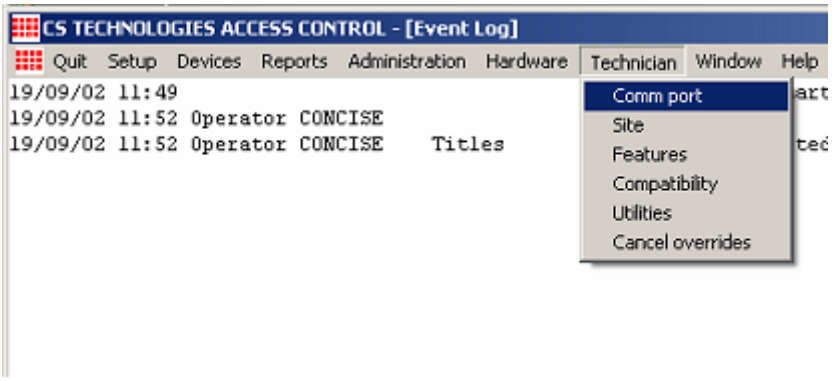
Once the controller has been added to the database it should start communicating with the PC. The communications leds on the board (see the LEDs topic) will flash and any transactions from the controller should start to appear in the transaction log.

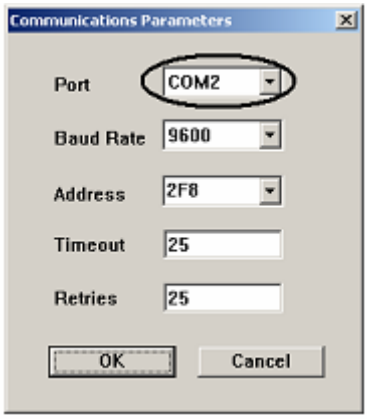
Further details of the configuration of the system can be found in the Doors, Alarms and Elevators topics.

4.6.2 Configuring controllers in PC3

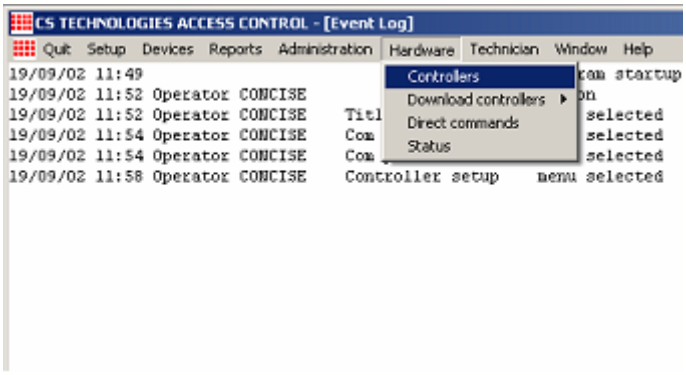
When you run PC3, the first thing to do is log in. The default login name is 123 and the password is also 123.

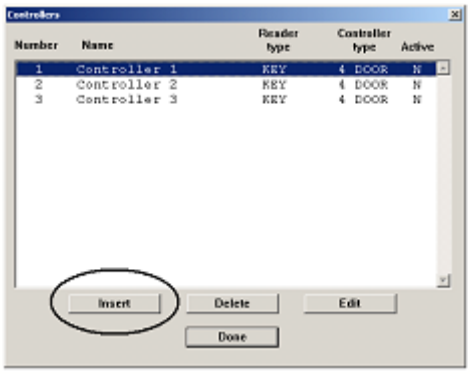
Select the com port (Technician/Com port) as the one to which the controllers are connected.





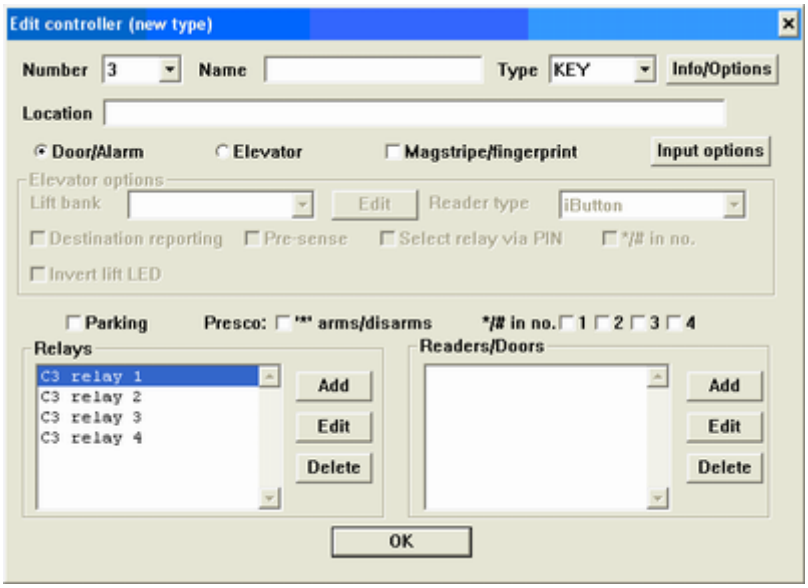
The next step is to add the controllers to the database (Hardware/Controllers/Insert).





For each controller you should

- Name the controller
- Select the type of reader (KEY = Silicon key, PIN = Keypad, CARD = wiegand card, ABACARD = a card where all digits are significant, ALARM = no readers, just alarms)
- Select whether it is Door/Alarm or Elevator firmware



By pressing the 'Add' button in the Readers/Doors group box it is now possible to add doors to the system. More information on door programming can be found in the Doors topic.

Once the controller has been added to the database it should start communicating with the PC. The communications leds on the board (see the LEDs topic) will flash and any transactions from the controller should start to appear in the transaction log.

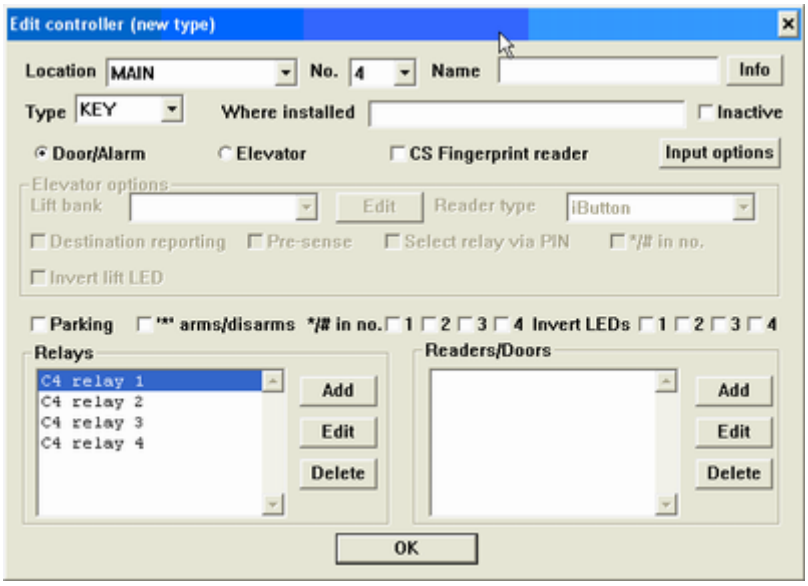
Further details of the configuration of the system can be found in the Doors, Alarms and Elevators topics.

5 Doors

5.1 Door overview

Once the controllers are in the database, doors and relays can be configured. With the CS system programming is very easy yet powerful. Multiple relays can be defined and assigned to doors and other functions including alarm outputs.

Relays and doors/readers are defined from the controller screen (Hardware/Controllers/Edit controller). Below is a view of the controller screen.



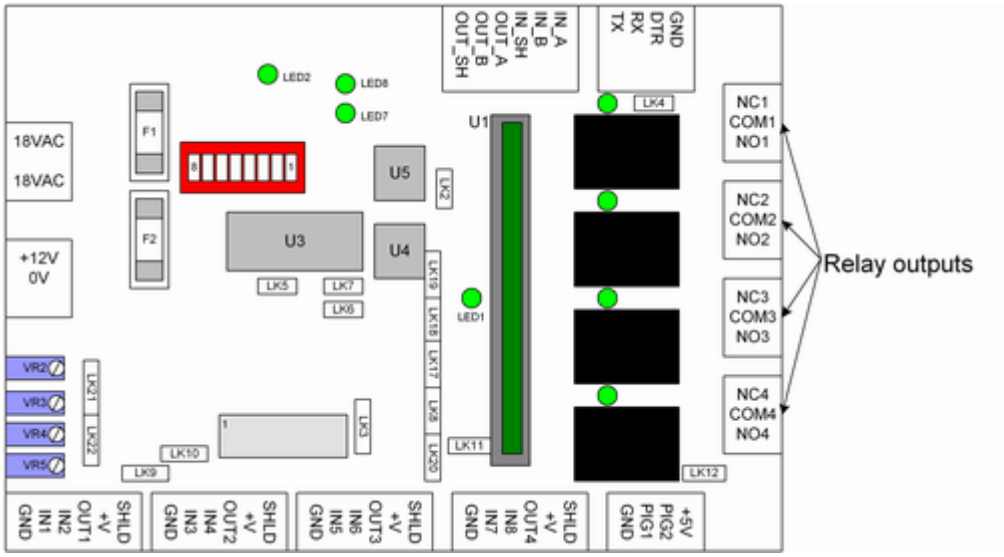
Relays are defined from the door screen and described under the Relays topic. When a new controller is created, four default relays are created for the four on-board relays. The relays can be managed by clicking on the 'Add', 'Edit' and 'Delete' buttons under the Relays group box.

Doors/readers are also defined from the controller screen. By clicking on the 'Add', 'Edit' and 'Delete' buttons under the Readers/Doors group box the doors can be managed.

Relays
Readers
Door strikes
Exit request inputs
Door status and alarms
Reader arming inputs

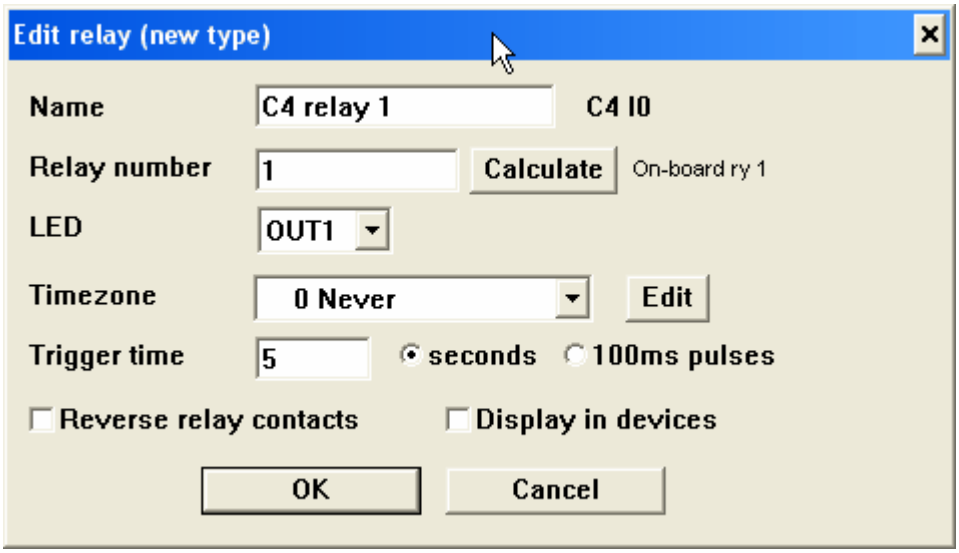
5.2 Relays

The controller has four on-board relays. These are 'form C' relays meaning that they have Common, Normally Open and Normally Closed connectors. The contacts on the relays are voltage-free.



Relays are generally used to control door strikes, link to alarm systems or other functions. The relays are rated at 2A 24VDC. Larger currents and voltages than these should be switched using slave relays. Whenever a device with a coil (relay or door strike for example) is switched by the relay it is essential that a diode be placed across the coil to minimise back-emf.
More information about the typical wiring of relays can be found in the door strikes topic.

Relays are defined from the door screen (Hardware/Controllers/Edit/Relays - add, edit, delete). Below is displayed the relay configuration screen.



The configuration possible for the relay here is:

- Name: - enter the name of the relay. The default name will generally suffice.
- Relay number: - this is where the number of the relay is set. For on-board relays these are numbered 1-4; expansion relays can be numbered by clicking on the 'Calculate' button.
- LED - select the LED output which is associated with the relay. The LED selected will be on whenever the relay is on.
- Timezone - select a timezone that you want the relay to be turned on - like a 'public access' timezone. The default setting is 0 (never).
- Trigger time - select the amount of time (in either seconds or 100ms pulses) that you want the relay to operate for when triggered by a reader, exit request or from the PC. The maximum time is 65536 seconds. The 100ms pulses setting is used to generate very short pulses, sometimes required for equipment like turnstiles. If 100ms pulses is selected it is not wise to have the trigger time greater than 5 (to generate a 0.5s pulse).

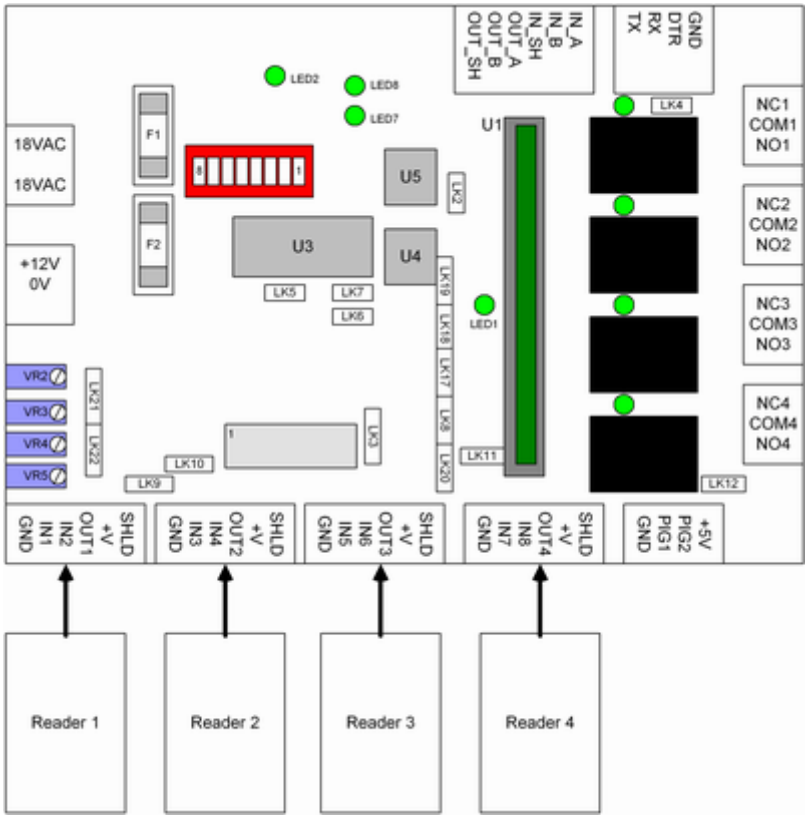
- Reverse relay contacts - changes the 'sense' of the relay, to make it fail-safe for some applications.
- Display in devices - if this setting is ticked then the relay will display under the Devices/Doors menu, allowing an operator to manually operate this relay. Normally this is not ticked, as the relay is usually associated with a door which itself appears in the Devices/Doors menu.

Readers
Door strikes
Exit request inputs
Door status and alarms
Reader arming inputs

Door overview

5.3 Readers

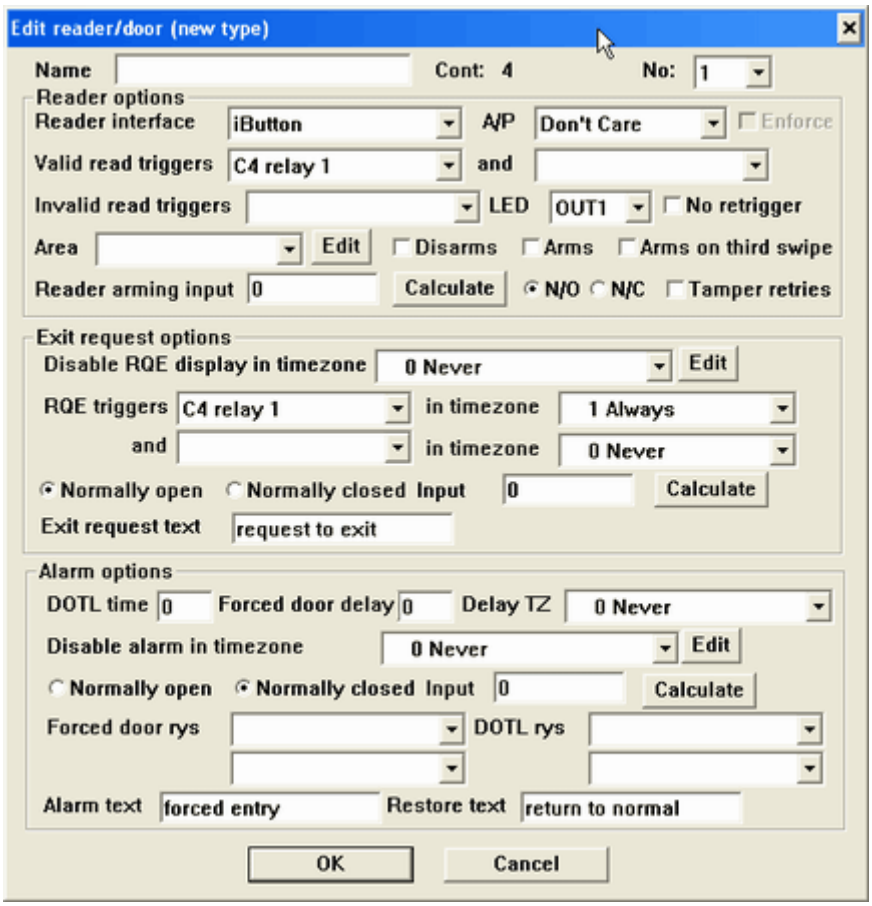
With door/alarm firmware, controllers can be equipped with up to four readers. The readers terminate at the bottom of the controller on the four 6-way termination blocks, as shown in the diagram below.



The system supports many different types of readers. Different readers use up different inputs and outputs. Unused inputs and outputs can be used for other functions including connection of exit request, door status and reader arming inputs.

Details of installation of specific readers can be found in the readers topic.

Readers/Doors are defined from the door screen. Below is shown the reader/door configuration dialog box.



The options for configuration of the reader are:

- Reader interface - select iButton, Wiegand, Clock and Data or Presco. Details of the particular setting for a particular reader can be found in the readers topic.
- A/P - antipassback for this reader - entry, exit, internal, external or don't care
- Enforce - if ticked, 'enforces' antipassback so that if someone is inside it won't let them enter again until they exit first
- Valid read triggers - allows selection of up to two of the defined relays to be triggered on a valid read.
- Invalid read triggers - allows selection of one of the defined relays to be triggered on an invalid read.
- LED - select the OUT which is used to drive the LED on this reader. This output will turn on momentarily on a valid read, and flash on an invalid read
- No retrigger - if this is ticked then a second read while the door is triggered by a first read will be ignored, stopping retriggering of the outputs. This is sometimes used where it is desired to have a single transaction recorded for each time the door is triggered, for example if it was triggering an air conditioning system for 30 minutes.
- Area, disarms, arms, arms on third swipe - these are covered in the alarms and inputs topic.
- Reader arming input - select the input which is used to arm the reader. For more information see the reader arming topic.
- Tamper retries - if this box is ticked then the reader is set up to monitor repeated invalid attempts and to lock out the reader after multiple invalid attempts. This is typically used if the reader is a keypad in an exposed situation where it might be subject to attacks by people attempting to guess codes. If this box is ticked then three consecutive invalid attempts to gain access will lock the reader out for 60 seconds.

Other things that can be configured for the door/reader include exit request and alarm options.

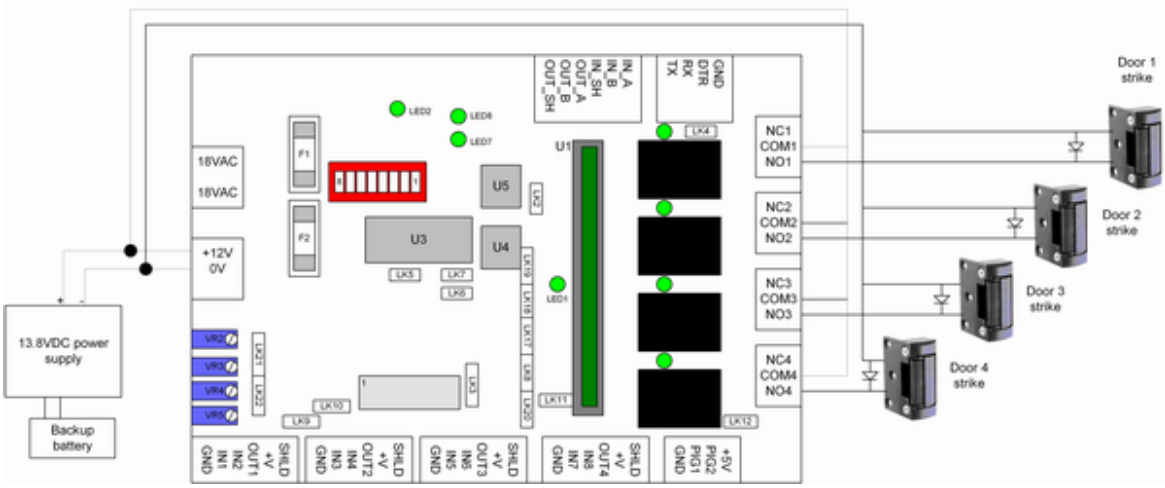
Relays
Door strikes
Exit request inputs

Door status and alarms
Reader arming inputs

Door overview

5.4 Door strikes

Door strikes or other outputs are connected to the relay outputs of the controller. The diagram below shows four electric strikes connected. These strikes are powered by the same power supply as the controller. The + output of the power supply connects to the common terminals of all of the relays, and the normally open contact connects to the door strike. The other side of the door strike connects to the - output of the power supply to complete the circuit. Note that all the strikes have a back-emf suppression diode which must be fitted across the coil. It is not acceptable to connect this at the controller; the emf must be suppressed as close to the coil as possible.



The trigger time and other settings for the strikes are set up under the relays topic.

Relays
Readers
Exit request inputs
Door status and alarms
Reader arming inputs

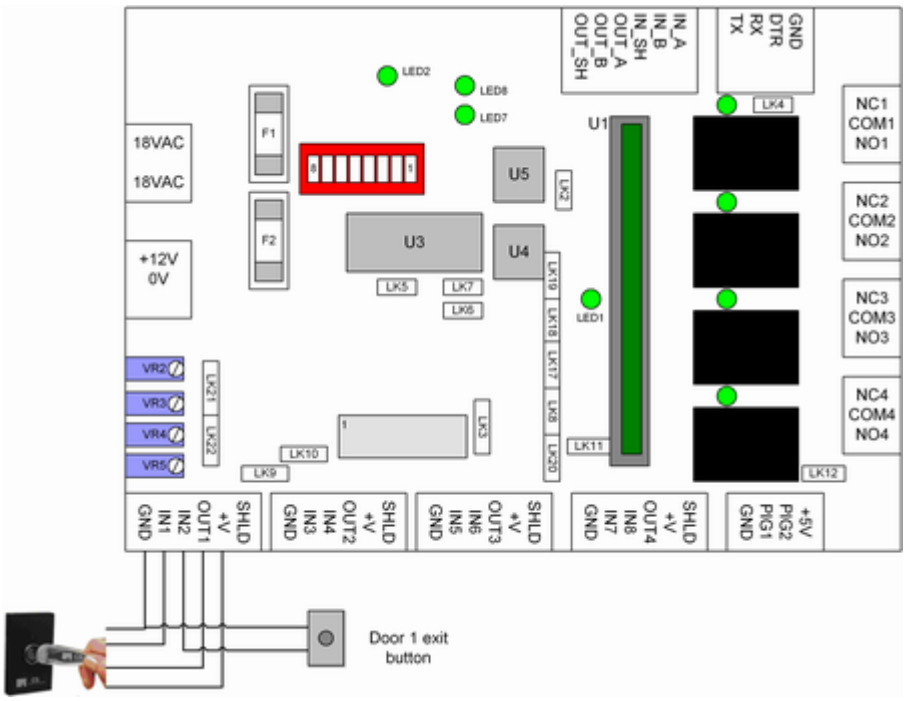
Door overview

5.5 Exit request inputs

An exit request, or RQE (request to exit) is usually a pushbutton or a detector which indicates that a particular door is about to be opened legally. Exit request inputs allow triggering of relays and also shunting of door alarms.

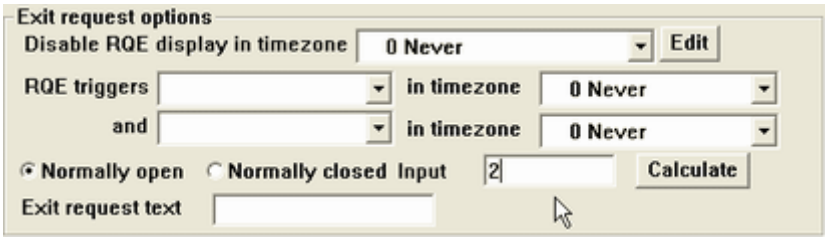
Exit requests can be connected to any input on the system including unused controller inputs and PIG inputs. They can be normally open or normally closed switches, and are configured from the Door/reader setup screen.

The best way to illustrate this is probably with an example. The system below has a single silkey reader which connects to IN1 and OUT1. This leaves all the other inputs and outputs free. An exit request button has been connected to the spare IN2.



The exit button can be normally open or normally closed, and connects between the selected input and the GND terminal.

To associate the exit request with a door, this is done from the doors screen (Hardware/Controllers/Edit/Edit door). The door screen is shown below, configured for this input.



In the 'Exit request options' part of the screen, input 2 is selected as the exit request which will make the configuration work as drawn in the schematic above. All inputs have a particular number in the system including expansion and PIG inputs. The particular input number for an input can be determined by pressing the 'calculate' button.

Parameters which can be defined for the exit request are:

- Disable RQE display in timezone - this allows a timezone to be defined which stops the display of exit requests. This might be used for example where an exit request is linked to a movement detector which creates many 'nuisance' transactions during the day, but after hours is desired to be still logged.
- RQE triggers - up to two of the defined relays can be selected to be triggered by this exit request. If no relay is selected the RQE will still mask any alarm on the door.
- RQE trigger timezones - for even more flexibility the RQE can have a timezone defined for its operation; it will only trigger the appropriate relay in the defined timezone.This might be used for example where the exit button is fitted to a reception desk as a door release; after hours this might need to be disabled.
- Normally open/normally closed - selects the type of contact for the RQE button.
- Input - selects which input this RQE is connected to.
- Exit request text - determines the message displayed on the screen when the exit request is logged.

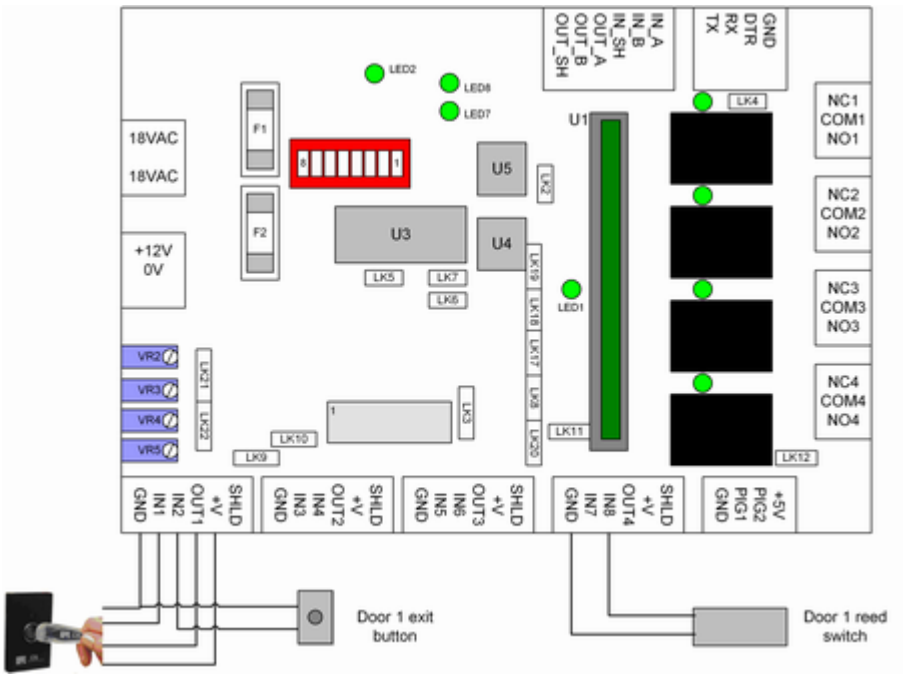
Note that if there is no exit request required for a particular door the input can be set to 0 which makes the exit request completely inactive.

5.6 Door status and alarms

A door can have an associated alarm input. This input is usually connected to a reed switch or other sensor which indicates that the door is open. Using this input it is possible to generate forced entry alarms (when the door has been opened without first a valid read or exit request) and door open too long alarms (when the door has been opened legally but then left open longer than a defined period of time).

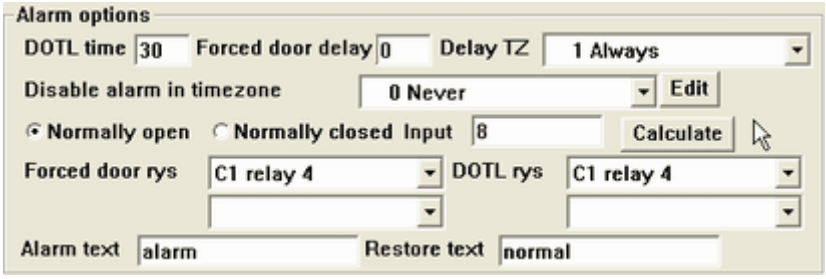
Door status inputs can be connected to any input on the system including unused controller and PIG inputs. They can be normally open or normally closed switches, and are configured from the Door/reader setup screen.

Continuing on with the example from the Exit requests topic, the system below has a single silkey reader which connects to IN1 and OUT1. This leaves all the other inputs and outputs free. An exit request button has been connected to the spare IN2. Now a reed switch has been connected to the spare IN8.



The alarm device (reed switch etc) can be normally open or normally closed, and connects between the selected input and the GND terminal.

To associate the alarm device with a door, this is done from the doors screen (Hardware/Controllers/Edit/Edit door). The door screen is shown below, configured for this input.



The alarm input is set up under the Alarm Options part of this page. Input 8 has been selected in this case to monitor the reed switch connected between IN8 and GND as in the example above. The system has also been set up with 30s door open too long (DOTL) time, and alarms have been set up to report to relay 4.

Parameters which can be defined for the door alarm are:

- DOTL time - the 'door open too long' time. After a legal opening of the door (folllowing a valid read or exit request) this determines the amount of time that the door can be held open for before a DOTL alarm is generated. Can be from 1-65536 seconds. If this is set to 0 then the door alarm is disabled.
- Forced door delay - a forced door alarm is generated if the door is opened without first a valid read or exit request. This setting determines the amount of time which elapses before that alarm is generated, allowing the door to be opened without a valid exit request or read if desired. It works in conjunction with the Delay TZ - the delay is only generated during the Delay TZ.
- Delay TZ - this works in conjunction with the forced door delay. During this timezone, the Forced Door Delay is applicable and the door can be opened for the delay time without generation of an alarm. When this timezone is not active the forced door delay is 0 which means that alarms occur immediately the door is illegally opened. The type of application for these parameters would be for a door with no exit request which can be opened from the inside legally during the day. During the day the Delay TZ would be active, with a forced door delay of say 20 seconds. If the door is opened and closes again during this 20 second time period no alarm is generated however if the door is left open then a forced door alarm is generated. However after hours (when the Delay TZ is not active), if the door is opened it will immediately generate an alarm.
- Disable alarm in timezone - allows the alarm to be turned off during the defined timezone
- Forced door relays - there are two relays here which can be selected from drop-down lists. The top one is a local relay i.e. it must be a relay defined as part of this particular controller. If a forced entry alarm is generated this relay will operate to indicate to a sounder or other alarm device, and will reset when the door is closed again. The second forced door relay is a 'global' relay - it can be any relay defined anywhere in the system. It will operate in the same fashion except that this global relay is operated by the PC and requires the software to be running for correct operation.
- DOTL relays - there are two relays here which can be selected from drop-down lists. The top one is a local relay i.e. it must be a relay defined as part of this particular controller. If a door open too long (DOTL) alarm is generated this relay will operate to indicate to a sounder or other alarm device, and will reset when the door is closed again. The second DOTL relay is a 'global' relay - it can be any relay defined anywhere in the system. It will operate in the same fashion except that this global relay is operated by the PC and requires the software to be running for correct operation.
- Alarm text and restore text - these define the messages which appear on the screen when the door goes into alarm or is restored.

Note that if there is no door alarm for that door then it does not need to be defined at all and can be set to 0.

Relays
Readers
Door strikes
Exit request inputs
Reader arming inputs

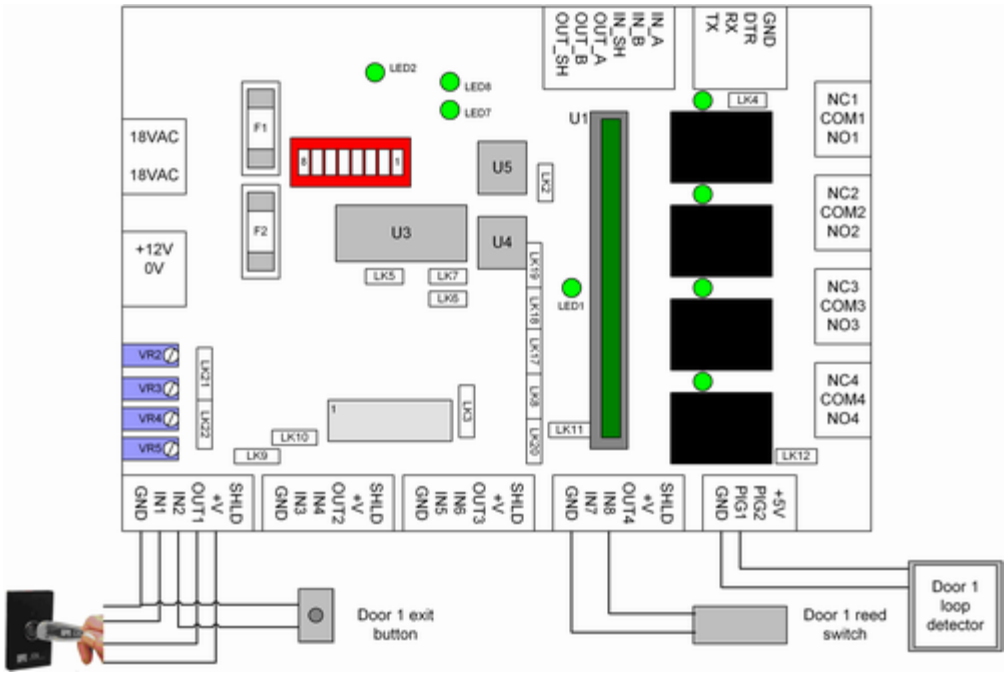
Door overview

5.7 Reader arming inputs

A reader arming input allows a reader to be 'disabled' unless a particular input is in a required state. Examples of where this would be used would be in a 'mantrap', where a particular reader is desired to be inoperative when a different door is open, or in a carpark where it is desired that a reader not work unless a vehicle is over a loop detector.

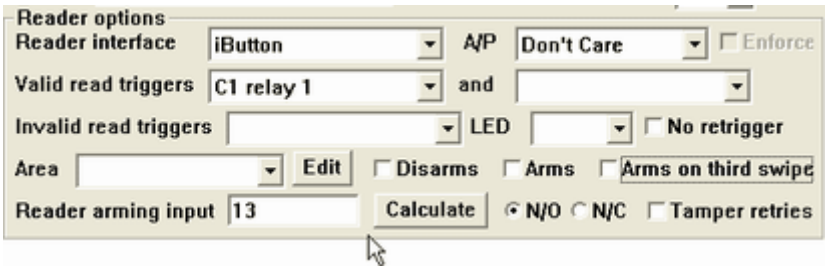
Reader arming inputs can be connected to any input on the system including unused controller and PIG inputs. They can be normally open or normally closed switches, and are configured from the Door/reader setup screen.

Continuing on with the example from the Exit requests and Door alarm topics, the system below has a single silkey reader which connects to IN1 and OUT1. This leaves all the other inputs and outputs free. An exit request button has been connected to the spare IN2. A reed switch has been connected to the spare IN8. Now a loop detector has been connected to the spare PIG1 port.



The reader arming device (loop detector etc) can be normally open or normally closed, and connects between the selected input and the GND terminal.

To associate the arming device with a door, this is done from the doors screen (Hardware/Controllers/Edit/Edit door). The door screen is shown below, configured for this input.



The arming input is set up under the Reader Options part of this page. Input 13 has been selected in this case to monitor the loop detector connected between PIG1 and GND as in the example above. This input number was 'calculated' by clicking the 'calculate' button and selecting

PIG1 to find the associated input number for that input.

Parameters which can be defined for the reader arming input are:

- N/O or N/C - whether the input is normally open or normally closed.

Note that if there is no arming input for that door then it does not need to be defined at all and the reader arming input can be left at 0.

Relays
Readers
Door strikes
Exit request inputs
Door status and alarms

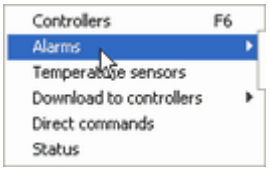
Door overview

6 Alarms and inputs

6.1 Alarms and inputs overview

The Door/Alarm firmware allows the controller to be used for both doors and for alarm areas. The controller firmware supports up to 250 alarm areas and 250 alarm inputs per controller. Because there can be up to 128 controllers and with Advent up to 50 locations this effectively allows millions of alarm inputs and alarm areas to be covered by the system.

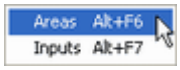
Once controllers have been defined then associated alarms are configured under the Hardware/Alarms menu.



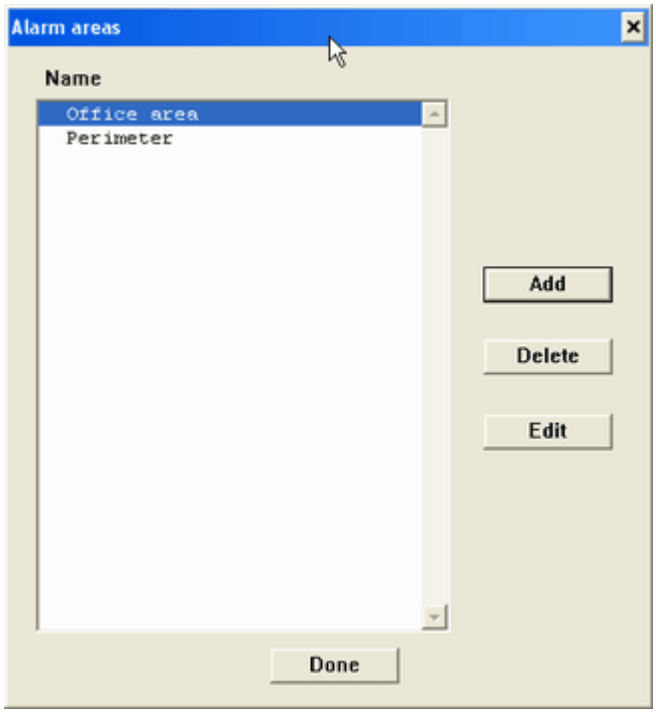
Alarm areas
Alarm inputs
Alarms and readers
The ideal integrated solution
Energy management

6.2 Alarm areas

Alarm areas are configured under Hardware/Alarms/Areas.

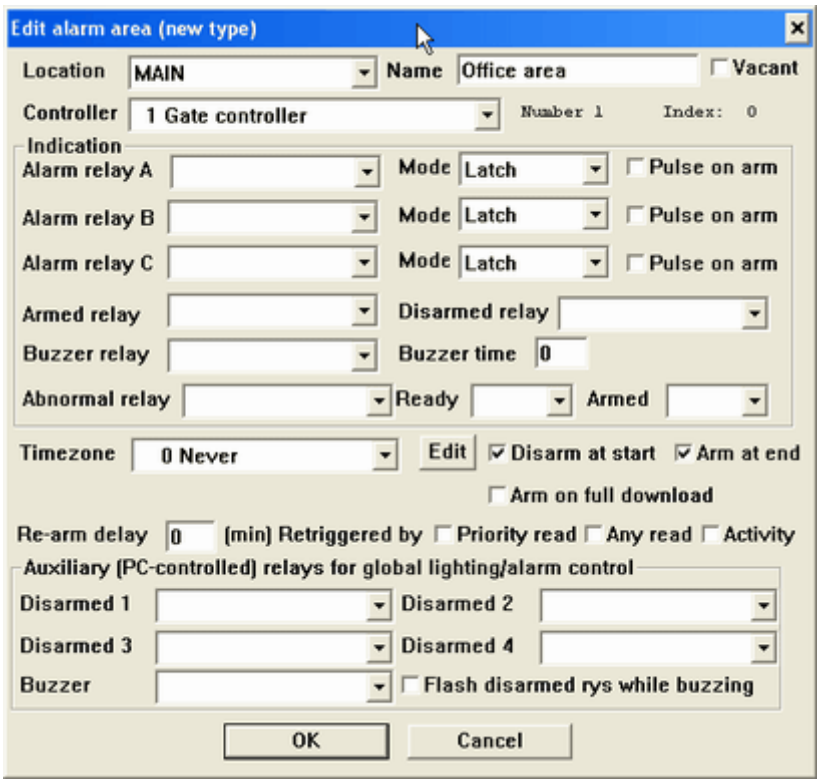


Selecting this brings up the area list.



From this list areas can be added, edited and deleted. When adding or editing an area the area

screen is displayed.



Options which can be set for the alarm area are as follows:

- Name - enter the name of the alarm area
- Controller - select the controller that this alarm area is part of. Note that all inputs which belong to an alarm area must also be connected to this same controller; areas cannot be distributed across multiple controllers.
- Alarm relays A, B, C - these relays operate when the area goes into alarm. The relays (which are on the same controller) are selected from the drop-down lists. They can be set to Latch, Pulse or Follow. They can also be set to 'pulse on arm' and if this is ticked then they do a momentary pulse on arming or disarming.
  - Latch means that the relay turns on when the area goes into alarm and stays on until the area is disarmed. Typical application of this would be for a strobelight.
  - Pulse means that the relay turns on for its pulse time (which is set under the relay settings). Typical application of this would be for a siren.
  - Follow means that the relay turns on whilever any alarm input in that area is in alarm and restores when the input restores. Typical application of this would be for connection to an alarm communicator.
- Armed relay - select from the drop-down list one of the relays configured for the controller. This relay turns on whilever the alarm area is armed.
- Disarmed relay - select from the drop-down list one of the relays configured for the controller. This relay turns on whilever the alarm area is disarmed.
- Buzzer relay - select from the drop-down list one of the relays configured for the controller. The buzzer relay turns on for the 'buzzer time' when the area is about to arm. Used to indicate a pre-arming warning.
- Buzzer time - set the time (1-255 seconds) that the buzzer relay operates for. When the alarm area is armed, if the buzzer time is defined the arming in fact just starts the buzzer timer; this operates the buzzer relay. After this times out the area arms.
- Abnormal relay - select from the drop-down list one of the relays configured for the controller. The abnormal relay turns on if any of the inputs in the area are abnormal (i.e. unsealed when the area is not armed).
- Ready LED - this output will turn on when the area is ready to arm i.e. all inputs are sealed.
- Armed LED - this output will turn on when the area is armed.
- Timezone - select the timezone for the alarm area. The timezone works in conjunction with

the 'disarm at start' and 'arm at end' tick boxes.

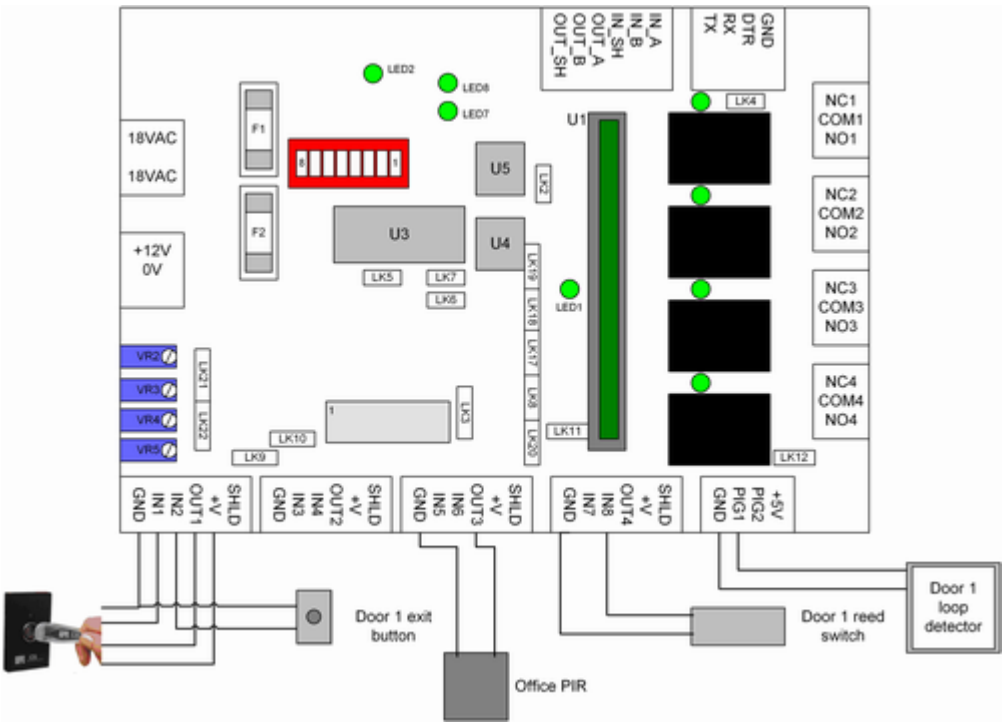
- Disarm at start - if this box is ticked then the area will be disarmed whenever the defined timezone starts.
- Arm at end - if this box is ticked then the area will be armed whenever the defined timezone ends.
- Arm on full download - if this box is ticked then whenever a full download is carried out, at the end of the download this area will be automatically armed.
- Re-arm delay - after hours (when the defined timezone is not active) it is possible for the alarm to be set to automatically re-arm after a defined time delay. This re-arm delay is to set the number of minutes before the area re-arms if disarmed after hours.
- Retriggered by - priority read - means that the re-arm timer is retriggered by a user with a credential at a reader associated witht he area which has the ability to disarm the area
- Retriggered by - any read - means that the re-arm timer is retriggered by any user with a valid credential at a reader associated with the area.
- Retriggered by - activity - means that the re-arm timer is retriggered by any activity on any inputs which are part of the area.
- Auxiliary (PC-controlled) relays - these relays will turn on if the area is disarmed. They are controlled by the PC and are usually used for global lighting control to turn on lights for many areas. There is also a global 'buzzer relay' which turns on as a pre-arm warning before any of the areas that have it defined begin to arm. It can even be set up so that the global disarmed relays flash during the buzzing period, to warn users that the area is about to arm.

Alarm inputs
Alarms and readers
The ideal integrated solution
Energy management

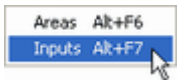
Alarms and inputs overview

6.3 Alarm inputs

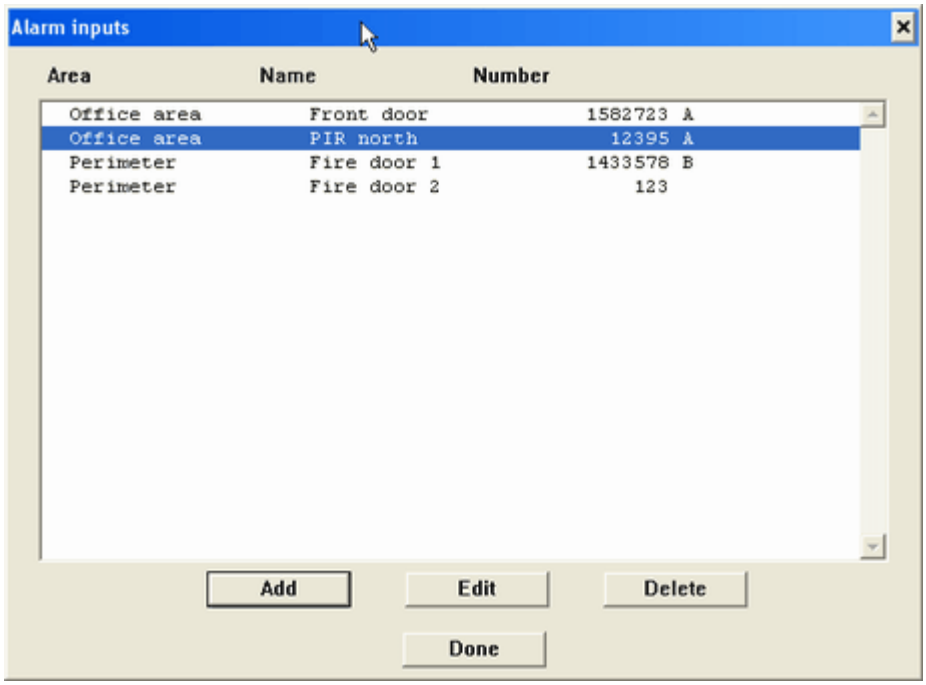
Any unused input on the system can be used as an alarm input. The example below shows a movement detector attached to OUT3 on the controller. More commonly alarm inputs are connected to PIGs or expansion inputs. More details on these can be found in the expansion overview topic.



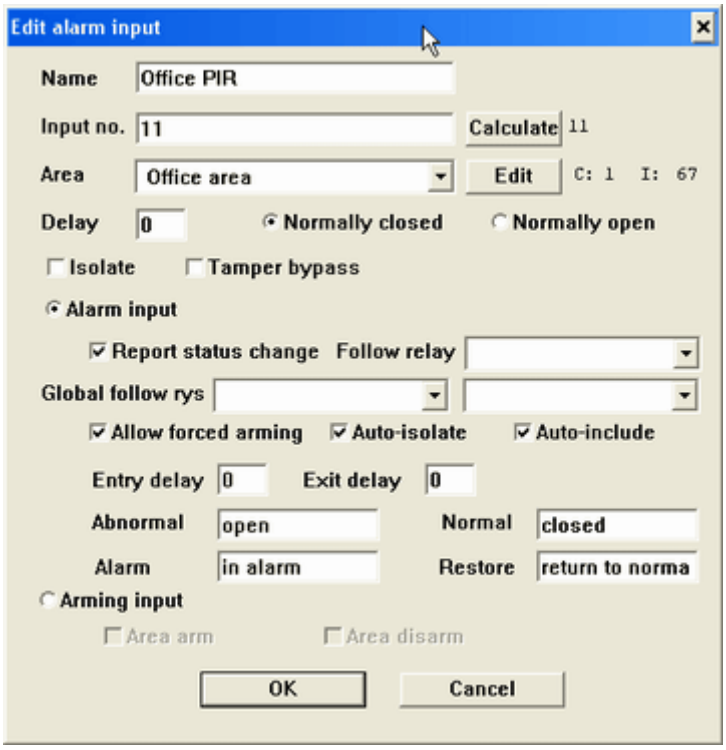
Alarm inputs are configured under the Hardware/Alarms/Inputs menu.



Selecting this brings up the input list.



From this list inputs can be added, edited and deleted. When adding or editing an input the input screen is displayed.



Options which can be set up for any alarm input are as follows:

- Name - enter the name for the alarm input
- Input number - enter the input that the alarm input is connected to. In the example above the

input is connected between OUT3 and GND. Clicking the 'calculate' button brings up OUT3 and associates it with input 11. Similarly the input can be set up as any PIG or expansion input too.

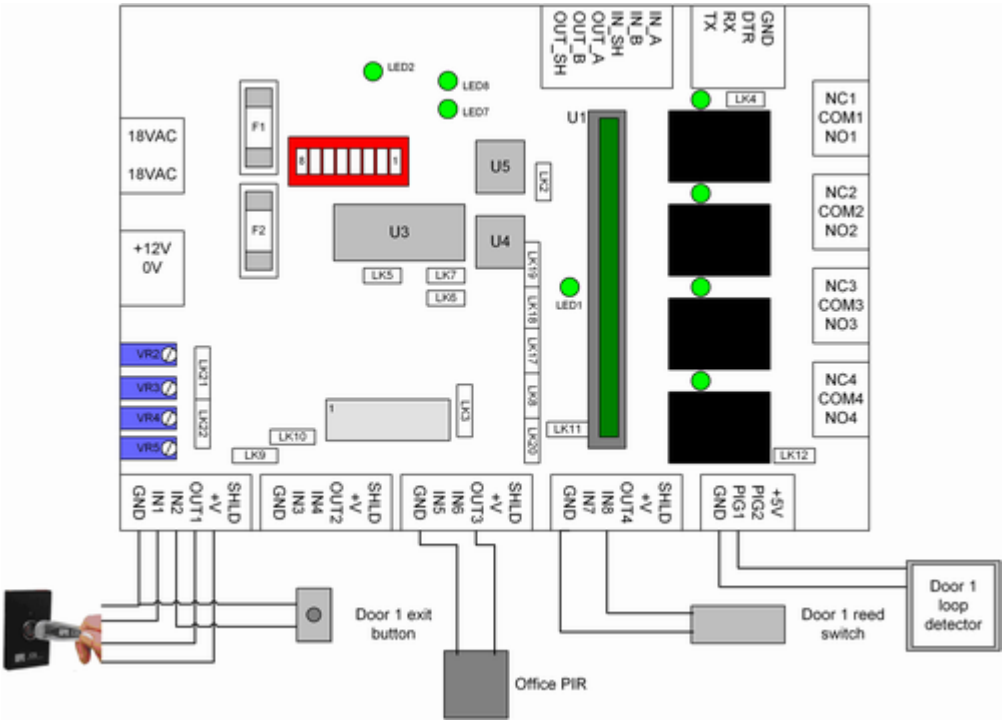
- Area - select the area that this input is part of. This will automatically set it up for a particular controller; the C: text to the right of this indicates the controller that the area is part of.
- Delay - set a time delay for the operation of the input. If this is set to 0 then the input will activate an alarm immediately when the area is armed; if it is set to another value then the delay will occur before the alarm activates.
- Normally closed/normally open - select whether it is a normally open or normally closed device
- Isolate - allows the input to be isolated
- Tamper bypass - tick this box to stop reporting of tampers (used with PIG inputs) on this input
- Alarm input - inputs can be configured to either be alarm inputs or used to arm and disarm a particular area. If selected for an alarm input the options are:
  - report status change - display a transaction of the input changing state even if the alarm is not armed
  - follow relay - activate a particular relay (selected from the drop-down box) when the input goes into alarm. The relay must be on the same controller
  - global follow relays - up to two relays (which can be on any controller) can be defined which will activate when the input goes into alarm. These require the software to be running at the time of the alarm to be effective.
  - allow forced arming - if this is ticked then the area will arm even if this input is abnormal.
  - auto-isolate - if this is ticked then when the area is armed (if forced arming is enabled) then the input will be automatically isolated.
  - auto-include - if this is ticked then following a forced arming and auto-isolation, if the area subsequently returns to normal it will be automatically de-isolated and included in the armed area.
  - entry delay - set the number of seconds that the input can be in alarm on 'entry' before going into alarm
  - exit delay - set the number of seconds that the input can be in alarm following arming of the area before being armed.
  - abnormal, normal, alarm, restore messages - set the text which displays when these inputs go into these various states.
- Arming input - if this is selected then the input can be used to turn on and/or off the associated alarm area. This is selected by the tick-boxes to say arm and/or disarm.

Alarm areas
Alarms and readers
The ideal integrated solution
Energy management

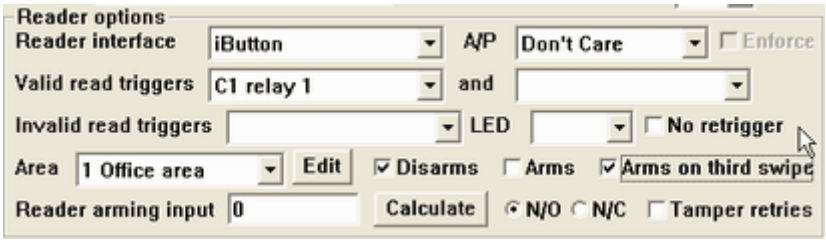
Alarms and inputs overview

6.4 Alarms and readers

When alarms are defined they can be associated with readers to allow powerful arming and disarming capabilities. The example below has the alarm area consisting of a PIR, controlled by a Silkey reader on input 1.



The reader can be used to control the alarm area. This is set up under the door settings (hardware/controllers/edit/edit reader).



In this example, the reader is associated with the Office area. The 'Disarms' box is ticked meaning that when a valid read occurs at that reader then the area will be automatically disarmed. The 'arms on third swipe' box is ticked meaning that a triple-read will cause the area to arm. Note that access levels can also be set up to interact with this, so that particular groups of credentials are not allowed to arm or disarm particular areas. This makes the system very powerful.

The options which can be selected here for reader/alarm interaction are:

- Area - select the area that this reader will control. The area must be on the same controller as the reader.
- Disarms - if this box is ticked then a valid read (by a suitably authorised credential) will cause the area to disarm.
- Arms - if this box is ticked then a single read (by a suitably authorised credential) will cause the area to arm. If both the 'disarms' and 'arms' boxes are ticked then the reader is effectively an 'alarm control reader' and does not need to control a relay as well.
- Arms on third swipe - this allows three consecutive reads to arm the area. This is used if the reader also controls a door.

Alarm areas
Alarm inputs
The ideal integrated solution
Energy management

Alarms and inputs overview

6.5 The ideal integrated solution

Because of the tight integration of access control and alarms with the CS system it provides the ideal solution for tenancy alarms and access control, combining ease of management with high security.

There are two major problems with any alarmed office area. These are:
- ensuring that the alarm is always armed after hours i.e. making people responsible to turn the alarm on
- false alarms because the alarm is turned on when people are still on site

The CS system provides the perfect solution to both of these problems. The key is in the features:
- alarm area timezone
- auto-rearm delay
- buzzer relay and buzzer time
- reader control of alarm areas

Firstly, users are able to control the alarm system using their access control credentials. If they are authorised, then when they enter the alarmed area the alarm system is automatically turned off. There is no need for separate management of alarm codes or two separate systems. Authorised users can enter the alarmed area and if the alarm is on it will be automatically turned off. If they are not authorised to enter then they cannot get in and cause false alarms because the access control system will deny them access.

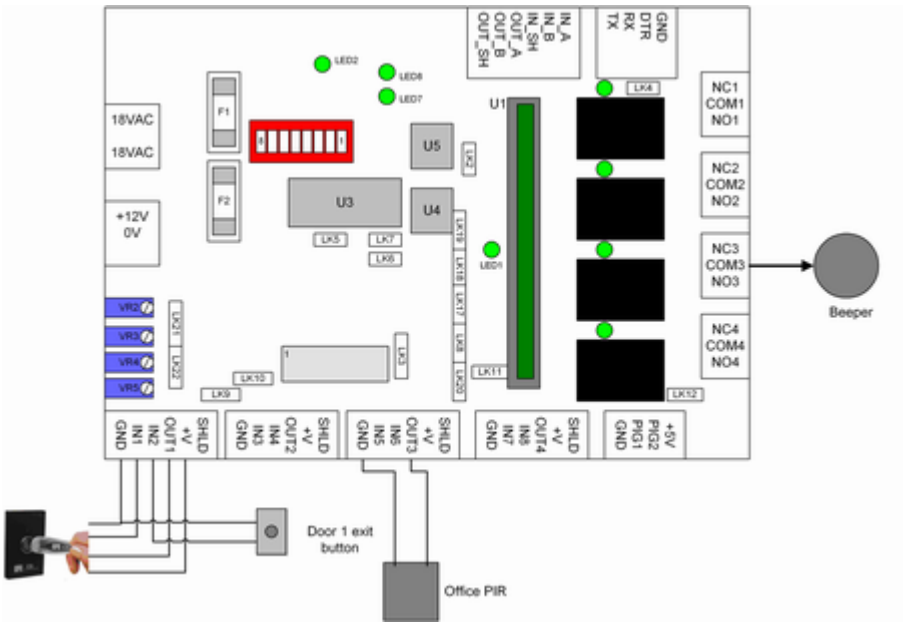
Secondly, the buzzer relay and buzzer time ensure that it is possible to 'warn' anyone on site whenever the alarm is about to be turned on. At the end of the alarm area timezone, if 'arm at end' is selected then the buzzer relay will turn on for the buzzer time. This can be linked to sounders which beep in the alarm area to warn anyone working there that the alarm is about to turn on. If they wish to stop the alarm from turning on they can simply present their (authorised) credential at one of the associated readers and the alarm will not turn on.

However after they do this and the auto-rearm delay elapses, the alarm will again attempt to arm and the buzzers sound and so on. If by this stage there is nobody on site then the alarm will arm as required.

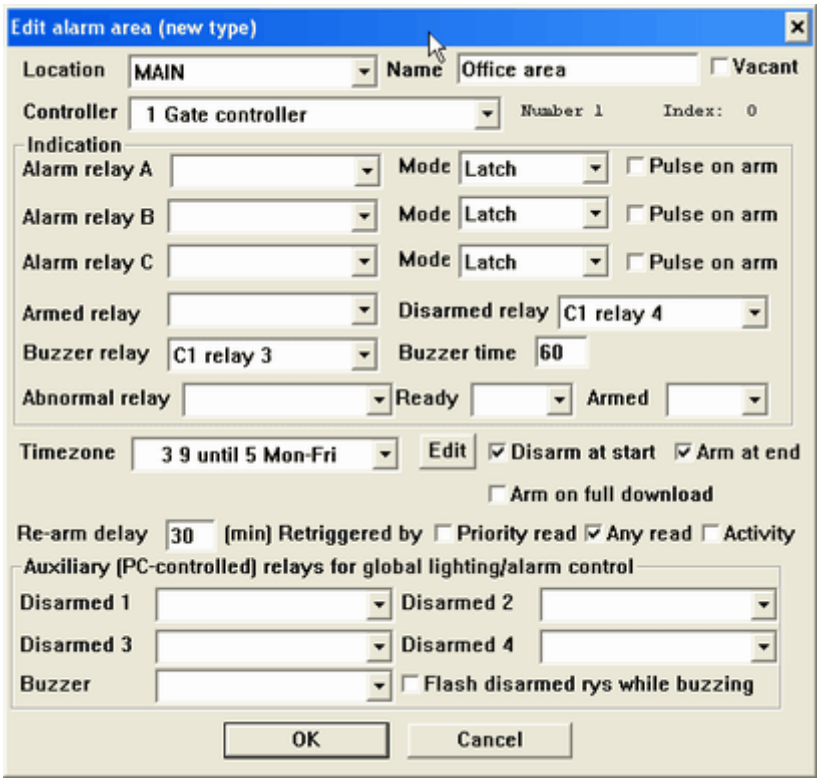
Similarly, if someone enters the premises after hours using an authorised credential the alarm will automatically be turned off. The auto-rearm delay will again start and once it elapses the buzzers will again operate and the alarm area will arm.

Moreover, users are able to manually arm the alarms simply by a triple-read at one of the readers. This also causes the buzzers to operate so if someone else happens to be within the tenancy they are warned of the impending arming and can either leave or present their credential at a reader to extend the alarm off time.

An example of setting this up using the system below is as follows:



In this system there is a single reader on the door of an office. The office has a movement detector (PIR). There are beepers triggered by relay 3.
The office alarm area setup is done under Hardware/Alarms/Areas.



In this setup, the alarm area timezone is set to 9-5 Mon-Fri and the 'disarm at start' and 'arm at end' boxes are ticked. This means that at 9am each day the alarm will automatically turn off. At 5pm each day the alarm will try to arm. When it does this, the buzzer relay (relay 3) will be triggered for the buzzer time (60 seconds in the above example). During this buzzer time staff can either leave or present their credential at the reader to disarm the alarm.

If they do disarm the alarm, the re-arm delay comes into action. In the example above it is set to 30 minutes. So 30 minutes later the beepers will again sound. However note also that the re-arm delay in the example is retriggered by any read. This means that during the re-arm delay if anyone uses their credential at the reader the re-arm delay will be reset again to 30 minutes and

will continue to count down.

Note that if the 'disarm at start' box is not ticked then the alarm won't turn off automatically at 9am, but will wait until the first authorised credential is used at the door. This will trigger the door and also turn off the alarm; if it is then after 9am the re-arm delay will not be active because the timezone is still valid.

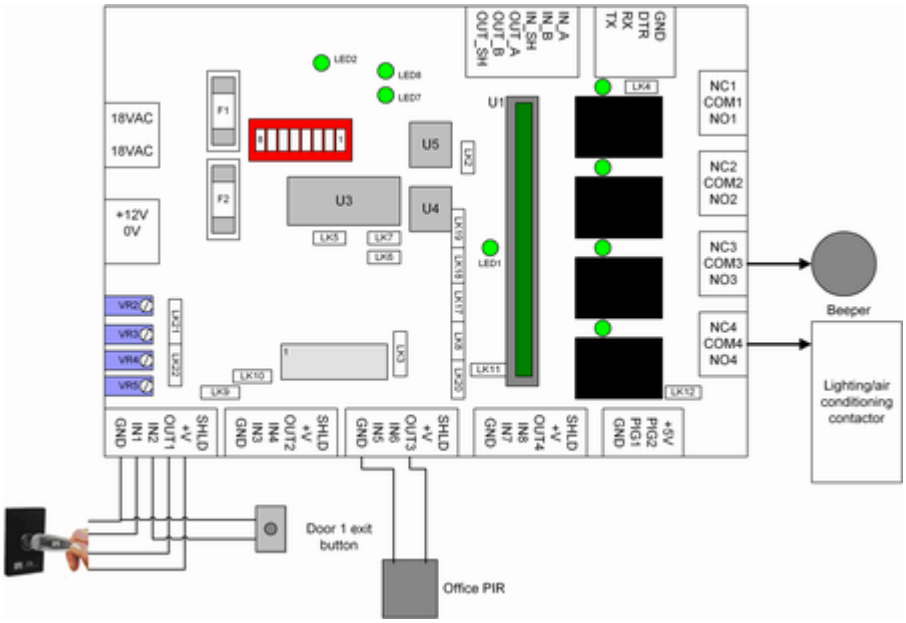
Alarm areas
Alarm inputs
Alarms and readers
Energy management

Alarms and inputs overview

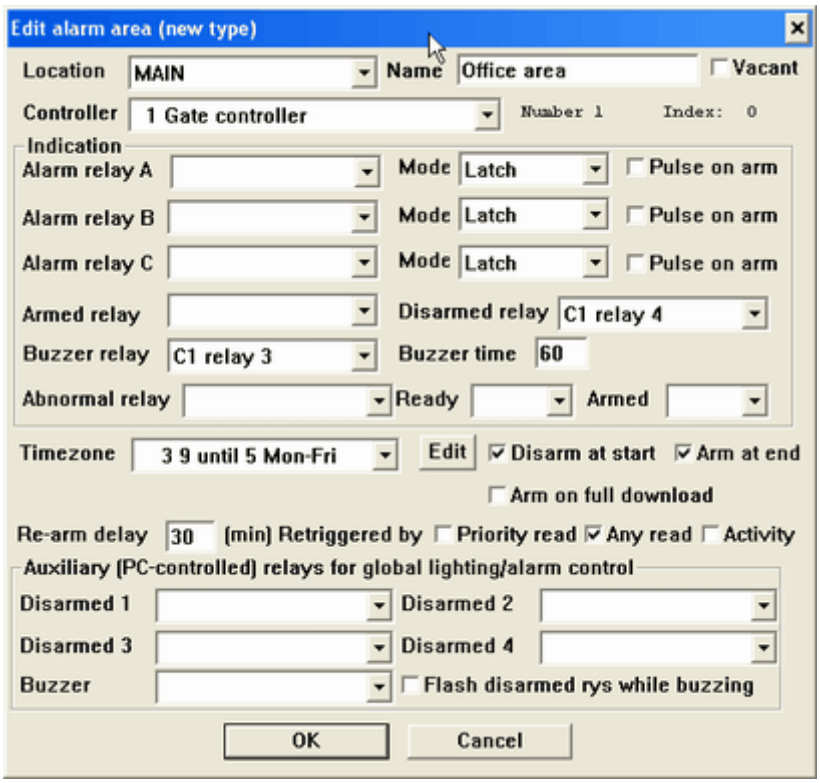
6.6 Energy management

An integrated CS Technologies access control and alarm system can have the added benefit of being able to reduce energy costs. If the system is set up as a fully integrated system (as detailed in the ideal integrated solution) then the system always knows when the alarm area is unoccupied. Accordingly the 'disarmed' relay for the area can be used to link to air conditioning, heating and lighting to ensure that no energy is being consumed unnecessarily when the premises are unoccupied.

An example of the setup of this is in the diagram below.



In this example relay 4 is linked to a contactor which in turn controls the lighting and air conditioning in the office. The setup is done under Hardware/Alarms/Areas.



In the screen above the 'disarmed relay' is selected as relay 4. This means that whenever the area is disarmed relay 4 will be active which will in turn allow the lights and air conditioning to operate. When the area is armed then relay 4 will not be active meaning that no energy will be wasted on lighting and air conditioning for an empty office.

Alarm areas
Alarm inputs
Alarms and readers
The ideal integrated solution

Alarms and inputs overview

7 Elevators

7.1 Elevator overview

CS Technologies are experts in the control of elevators, and the system includes many features which make management and control of elevators powerful, effective and reliable.

CS Technologies access control systems provide a reliable, high security and cost-effective solution to the problem of lift access control. From basic systems which provide access to all floors through to systems incorporating call destination reporting, high level interfaces and intercom release CS Technologies has the experience and products to make elevator access control easy.

Understanding elevators
Setting up an elevator system
Basic low-level interfacing
Low-level interfacing with call destination reporting - pre-sensing
Low-level interfacing with call destination reporting - post-sensing
High-level interfacing
Floor triggering inputs

7.2 Understanding elevators

Lift banks
In a building with elevators there are normally groups of elevators which service different groups of floors. For example, in a tall building there might be 'high rise' lifts and 'low rise' elevators. Each group of elevators is termed a 'bank' of elevators or a 'lift bank'.

With the CS system each elevator requires its own controller, reader, inputs and outputs. However in the software the controllers are grouped into 'banks' to make programming and control easy.

Floor call buttons
Normally within an elevator are a number of 'floor call buttons'. Each floor call button is used by someone travelling in the elevator to select a particular floor to which they wish to travel. The floor call buttons generally have lights which turn on when a particular floor is selected.

Landing call buttons
On each floor of the building are buttons which are used to call the elevator to that floor. These buttons are called 'landing call buttons'.

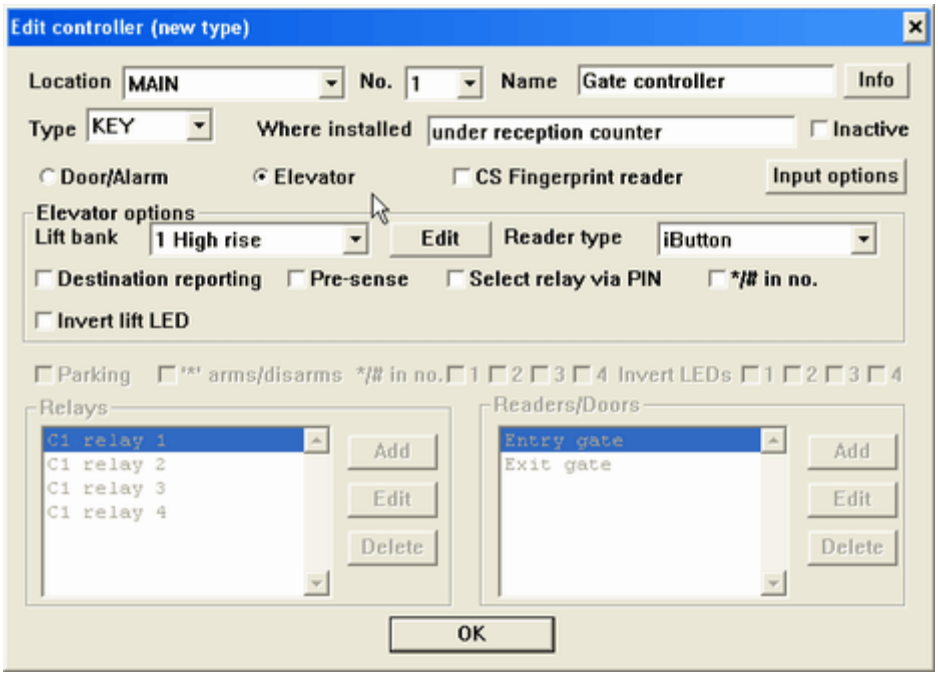
High level/low level interfacing
When a system is connected to an elevator it can connect using high level or low level interfacing. Low level interfacing uses relays (outputs) and inputs on the CS controller to send signals to and receive signals from the elevator. High level interfacing uses a communications link between the controller and the elevator system to send and receive information from the elevator.

Setting up an elevator system
Basic low-level interfacing
Low-level interfacing with call destination reporting - pre-sensing
Low-level interfacing with call destination reporting - post-sensing
High-level interfacing
Floor triggering inputs

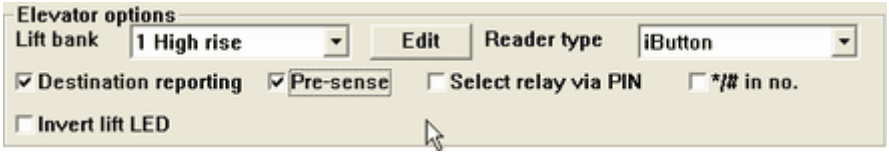
Elevator overview

7.3 Setting up an elevator system

To set up an elevator system a controller with Lift firmware must be used. When the controller is configured (Hardware/Controllers/Edit Controllers) select the Elevator radio button.



This will allow selection of the various Elevator options for the controller.



When initially programming the controller a lift bank must be selected; it is possible to create a lift bank from this screen too if necessary.

The options which can be selected here are:

- Lift bank - select the lift bank that this controller is part of
- Reader type - select the reader type for the elevator. Lift firmware only supports a single reader, which can have an iButton, Wiegand, Clock and Data or Presco interface.
- Destination reporting, Pre-Sense - these options determine the behaviour of the controller if it is connected to the elevator in such a way that it can sense the selected floors.
- Select relay via PIN - this is used if a keypad is used. If this option is ticked then users can append a relay number (1-10) on the keypad and if valid for that relay then only that relay will be triggered. For example if the user's PIN is 1234 they would enter 12341 to trigger relay 1.
- */# in no - tick this to use Presco base-12 cards on the system.
- Invert lift LED - usually the lift LED is on until a valid floor is selected. Ticking this box inverts the sense of the LED.

Following configuration of the controller in this way the individual floors in the lift bank need to be configured. This is done under Hardware/Lifts, and explained further in the topics covering the various interfacing options.

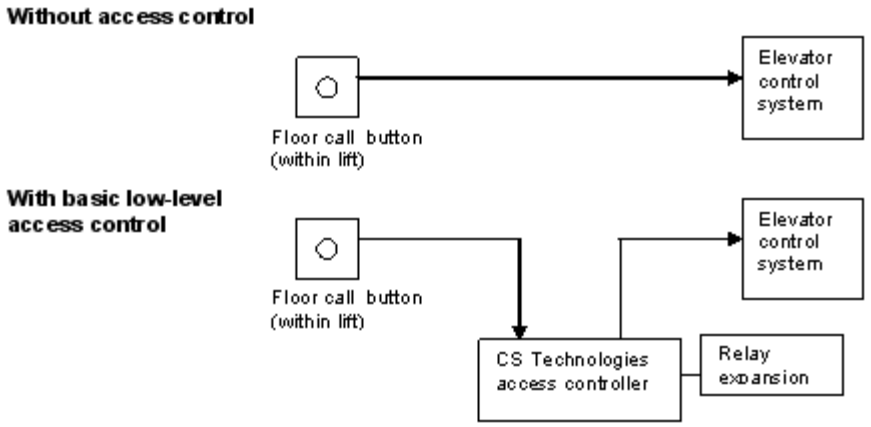
Basic low-level interfacing
Low-level interfacing with call destination reporting - pre-sense
Low-level interfacing with call destination reporting - post-sense

The other configuration which is possible is to use intercom inputs to trigger individual floors. The

details of this are covered in the topic Floor triggering inputs .

7.4 Basic low-level interfacing

The simplest way to interface to an elevator is to install a controller with relay expansion boards so that there is a relay for each floor in each elevator. The 'floor call' button signals from within the elevator are passed through the controller relay contacts, so that if the relay is not turned on then the floor call button does not send its signal to the elevator and the floor cannot be accessed. This method does not record where each person travelled and also does not stop someone selecting more than one floor at a time.



In the diagram above, with the access control system in place the signal from the call button cannot get to the elevator control system unless the access controller allows it to go through by turning on the relay. Each floor has a relay meaning that floors can be controlled by timezone or by credentials (users) in the elevator.

Disadvantages of basic low-level interfacing are that the system is only able to record that a particular person was in the elevator, and not the floor to which they travelled. When a person with access to multiple floors uses a credential all the relays associated with those floors turn on and any one (or more) of them can be selected.

CS Technologies software makes it very easy to program the system for access control. Each user (credential) has an elevator access level which defines the floors to which they are permitted to go. Elevator controllers are grouped in banks so when a user is added to the system their credential and the appropriate floors are automatically loaded into all the controllers for those banks. It is very easy to modify elevator access levels so that groups of users can be given additional access when required. And timezones are associated with all elevators in each bank, making it very easy to put a floor onto security when required.

With basic low-level access control the following equipment is required:
For each elevator

- one CS Controller with relay expansion boards to provide a relay output for each floor to be controlled. Each expansion board has 16 relays and a total of 15 boards can be added making a maximum of 250 controlled floors per elevator

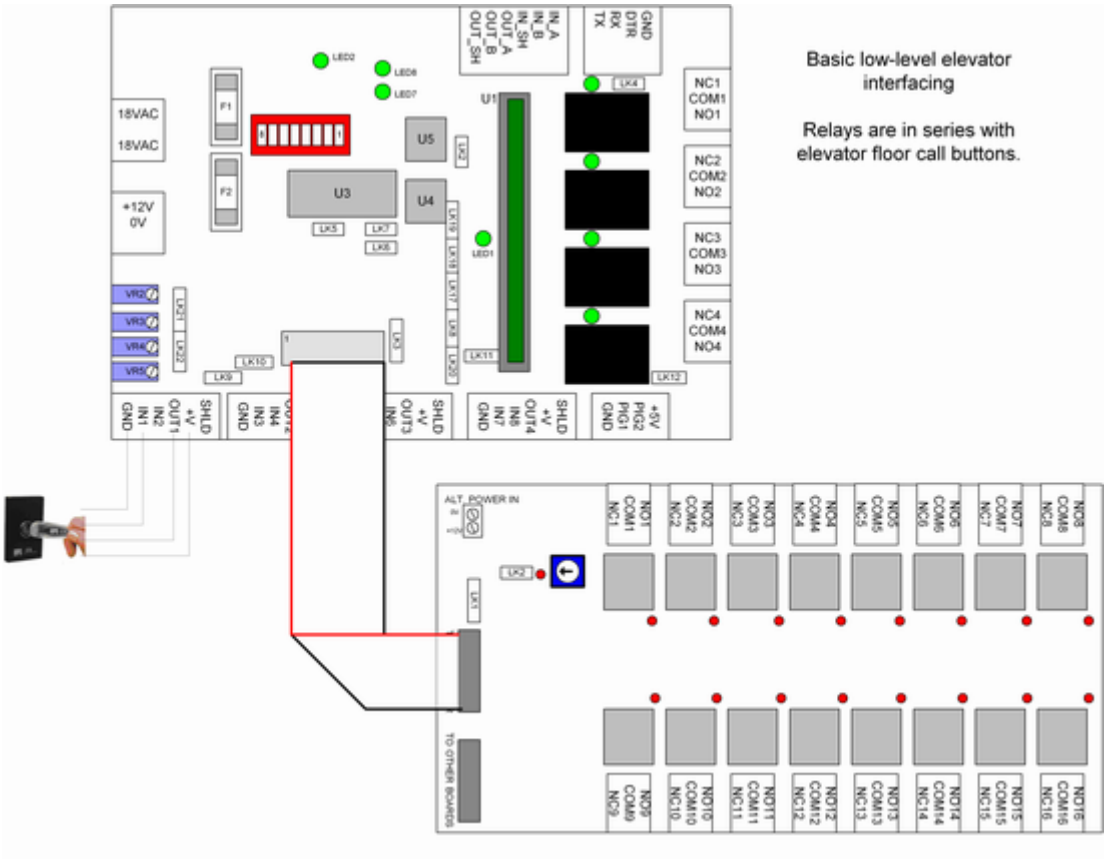
- one reader (can be silicon key, magstripe, wiegand, proximity, smartcard, etc etc)

The CS controller provides clean contacts for each floor in each elevator and the elevator company must provide connections so that these contacts can be interfaced in series with the floor call buttons.

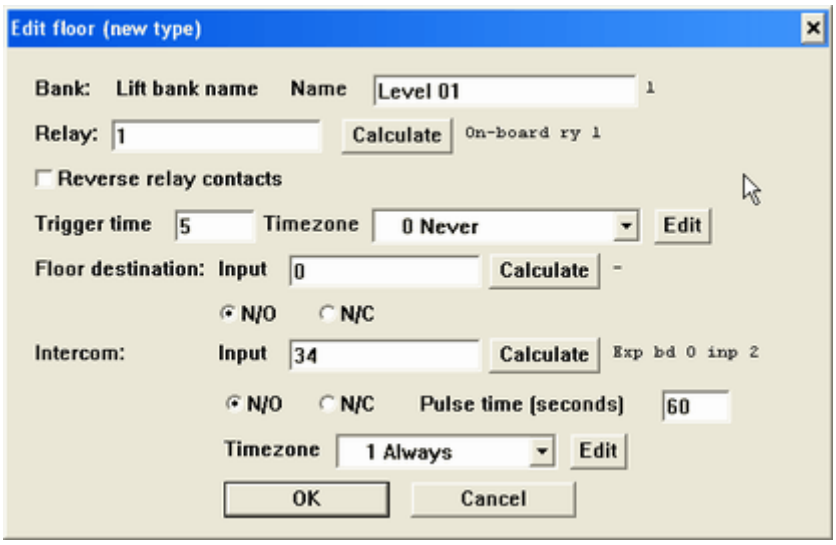
The relay contacts on the controller are rated for 30VDC switching; if the signals between the call button and the elevator are a higher voltage interposing relays must be used.

Setting up for low-level interfacing

The diagram below shows a controller with a 16-way relay board. This setup will control up to 20 floors of a building in one elevator. The relay contacts are wired in series with the floor call buttons so that floors cannot be selected unless the appropriate relay is on.



To set this up the elevator bank is programmed under Hardware/Lifts/Edit lift bank. Individual floors can be added to the elevator from this screen. The screen used to program the floors is below.



Parameters which can be programmed for each floor are:

- Name - enter the name of the floor
- Relay - use the 'Calculate' button to select any relay on the system
- Reverse relay contacts - this is used to make the relay 'fail-safe' so that when power is removed the relay can be left in a state where the floor is available. Sometimes fire regulations require this setting.
- Trigger time - set the amount of time that the floor will be triggered for on a valid read in the lift
- Timezone - select the timezone for public access for this floor. When the timezone is active then no credential will be required in the elevator and the relay will be active.

The floor destination settings are not used with basic low-level interfacing.

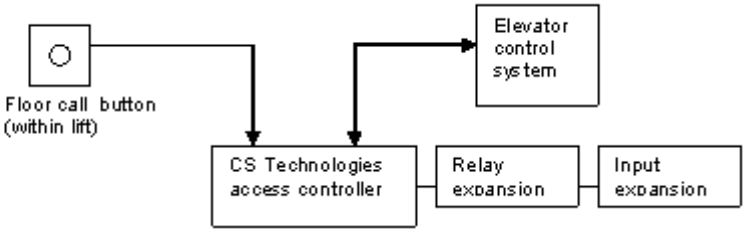
Understanding elevators
Setting up an elevator system
Low-level interfacing with call destination reporting - pre-sensing
Low-level interfacing with call destination reporting - post-sensing
High-level interfacing
Floor triggering inputs

Elevator overview

7.5 Low-level interfacing with call destination reporting - pre-sensing

The CS Technologies 16-way input board is able to sense the selection of a floor within the elevator. When a person presents a credential at the elevator reader the buttons for that person's valid floors are scanned; when one is selected the appropriate relay on the CS controller turns on to allow the call to be latched. This is called 'pre-sensing' because the buttons are scanned before the relay turns on. This provides the best way to control elevators because the system provides a record of where each person has travelled, and ensures that only a single floor can be selected for each credential presentation. However use of this method depends on the correct type of signals being available from the elevator company.

With low-level access control, call destination pre sensing



The signals from the floor call button are sensed by the access controller. When a credential is presented in the elevator all of the floor call buttons which are valid for that user are scanned; when the user presses one of the buttons the controller turns on the appropriate relay which allows the call to be latched by the elevator control system.

In order for this solution to work the voltage on the control wires from the elevator control system must change when someone presses the floor call button, whether or not a call is latched. The input board has the ability to monitor voltages from 5V to 150V AC or DC.

Major advantages of this method include:

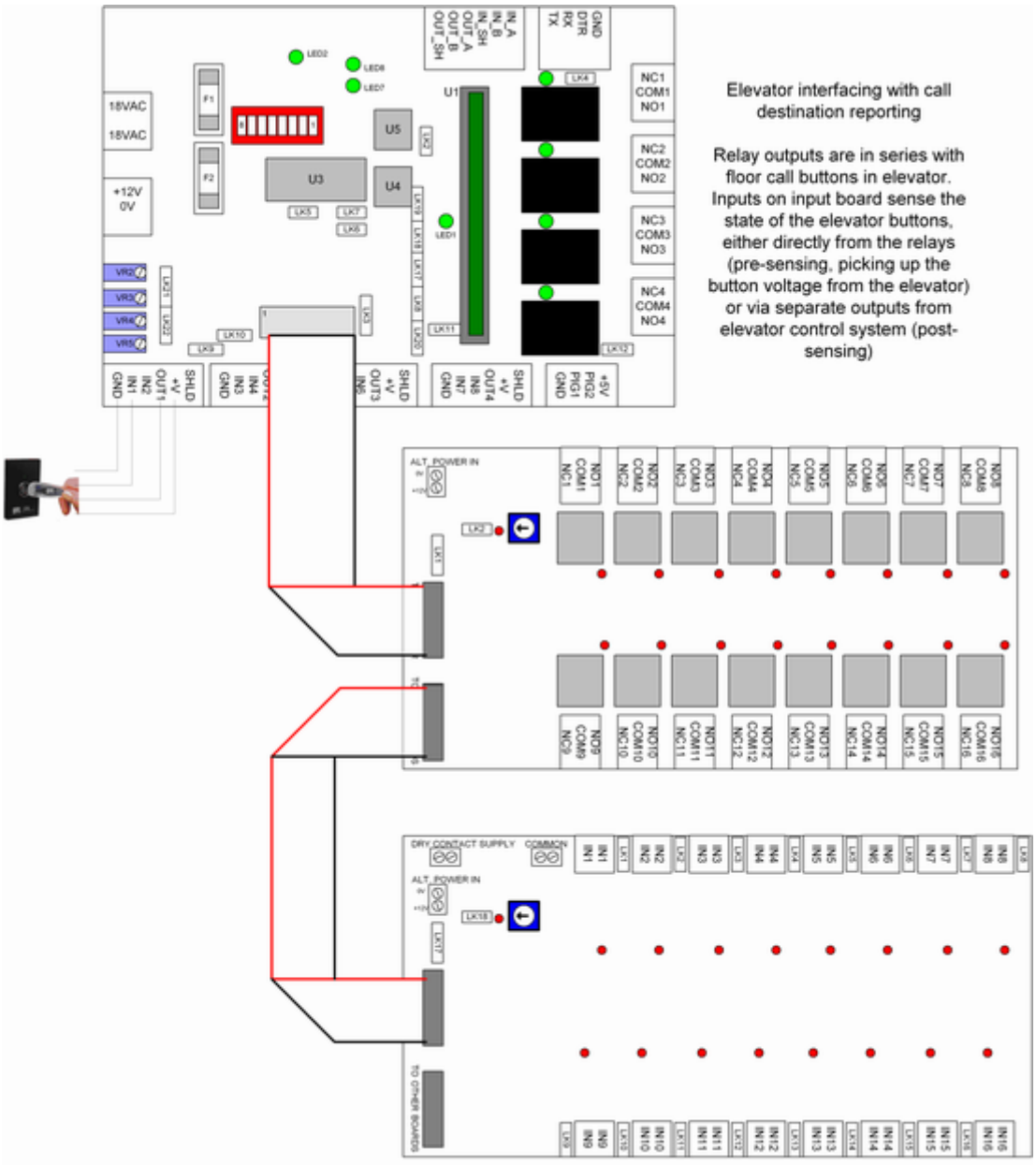
- high security – only one call can ever be latched per credential presentation
- low cost – the standard low-level interfacing cables from the elevator company are scanned for the call destination functionality, meaning that the elevator company do not need to provide any additional signals.

Equipment required for low-level interfacing with pre-sensing call destination reporting is as follows:
For each elevator:

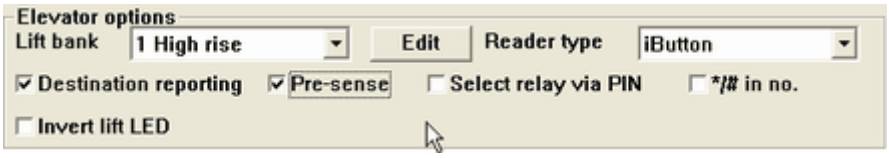
- one CS Controller with relay expansion boards to provide a relay output for each floor to be controlled. Each expansion board has 16 relays and a total of 15 boards can be added making a maximum of 250 controlled floors per elevator
- the controller also requires input expansion boards to provide an input for each floor to be controlled. Each expansion input board has 16 inputs and a total of 15 boards can be fitted to the controller.
- one reader (can be silicon key, magstripe, wiegand, proximity, smartcard, etc etc)

The CS controller provides clean contacts for each floor in each elevator and the elevator company must provide connections so that these contacts can be interfaced in series with the floor call buttons. For the call destination reporting to work the elevator connection cables must change voltage when the floor call buttons are pressed.

A diagram of a system with call destination reporting is below.

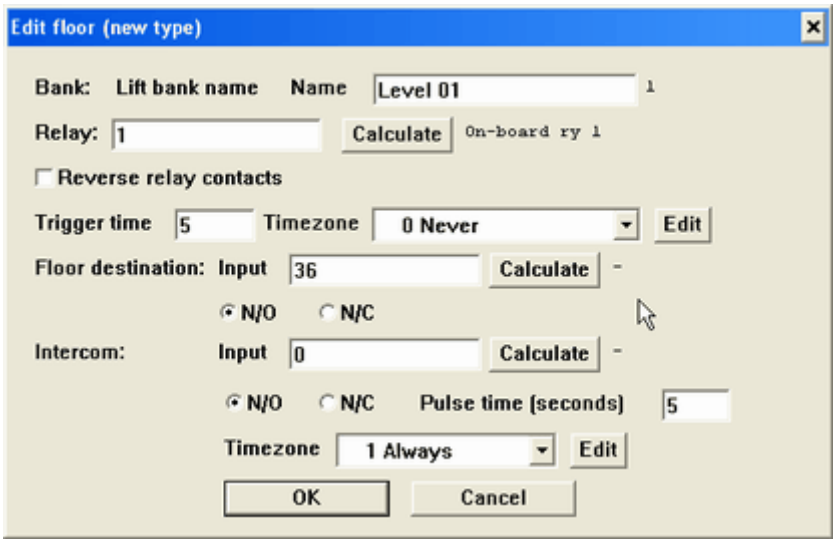


To enable floor destination reporting, tick the appropriate box under the Hardware/Controllers/Edit controller screen.



With the 'destination reporting' box ticked, when a credential is used in the lift no transaction will be reported until either a floor is selected or the trigger time elapses. If the 'pre-sense' box is ticked then the relays themselves will not operate until the floor destination inputs detect a floor being selected in the elevator.

The inputs for floor destination reporting are set up under Hardware/Lifts/Edit lift bank/edit floor.



Use the 'calculate' button to select any available input, and select whether it is normally open or normally closed.

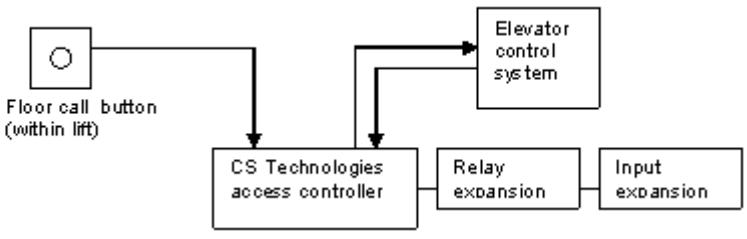
Understanding elevators
Setting up an elevator system
Basic low-level interfacing
Low-level interfacing with call destination reporting - post-sensing
High-level interfacing
Floor triggering inputs

Elevator overview

7.6 Low-level interfacing with call destination reporting - post-sensing

With some elevator control systems the floor button being pressed does not provide a signal with a changing voltage. In these situations the elevator company must provide additional separate outputs which indicate the latching of a floor call. CS Technologies equipment can operate with this scenario also; when a credential is presented at the lift all the relays for valid floors for that person turn on, and when the elevator control system indicates that a call has been latched then that relay stays latched and all of the other relays turn off. This is called 'post sensing' because the sensing of the floor destination occurs after the call has been latched by the elevator control system.
This method is not as secure as the 'pre-sensing' system because it is possible to latch more than one call by pressing two or more buttons simultaneously. It also requires additional signals to be provided by the elevator company and there is often a significant cost involved with this. However it does provide call destination reporting and is therefore a great improvement on the basic low-level interfacing option.

With low-level access control, call destination post sensing



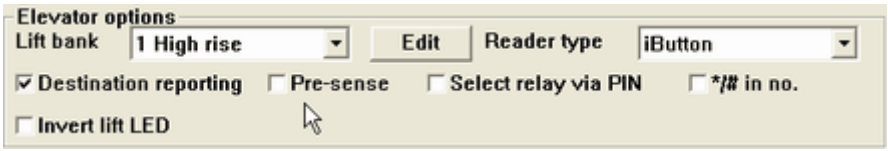
When a credential is presented in the elevator all of the relays which are valid for that user are

activated; when the user presses one of the buttons the elevator control system sends a signal to the CS Technologies access controller to indicate that a floor selection has been made, and then the access controller turns off all but the valid relay.

Equipment required for low-level interfacing with post-sensing call destination reporting is as follows:
For each elevator:

- one CS Controller with relay expansion boards to provide a relay output for each floor to be controlled. Each expansion board has 16 relays and a total of 5 boards can be added making a maximum of 84 controlled floors per elevator
- the controller also requires input expansion boards to provide an input for each floor to be controlled. Each expansion input board has 16 inputs and a total of 10 boards can be fitted to the controller.
- one reader (can be silicon key, magstripe, wiegand, proximity, smartcard, etc etc)

The CS controller provides clean contacts for each floor in each elevator and the elevator company must provide a separate signal to indicate a call being latched within the elevator control system. With post-sensing the 'pre-sense' box in the elevator options (Hardware/Controllers/Edit controller) is not ticked.



In this situation when a valid credential is presented at the reader all the associated relays for that user will operate, but once a floor is selected the other relays will drop out.

Understanding elevators
Setting up an elevator system
Basic low-level interfacing
Low-level interfacing with call destination reporting - pre-sensing
High-level interfacing
Floor triggering inputs

Elevator overview

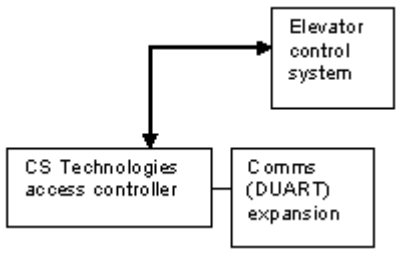
7.7 High-level interfacing

High level interfacing refers to the method where there are no relays or input boards involved, but a data communication link exists between the elevator and the access control system. In this situation a single access controller is used to provide the communication link to the elevator, and generally all of the elevators in a building, or all the elevators in a bank, have a single interface to control them.

CS Technologies supports high level interfaces in the Otis, Kone Type 1 and Kone Type 2 communication formats with full call destination reporting available.
A diagram depicting the high level interface is below.

With high-level interface

The elevator control system and the access control communicate using RS232 or RS485 signals. The access controller also communicates with readers in each lift which are fitted with additional communication boards (ACE-2)



There is a RS232 or RS485 communication signal between the access controller and the elevator control system. The signal provides the ability for the controller to activate and deactivate individual floors in individual elevators, as well as sending signals regarding selected floors from within the elevator for call destination reporting.

Disadvantages of the high level interface include

- all elevators controlled by a single interface – if there is any problem with the system all elevators go off security
- generally the interface is too slow to stop multiple floor selection
- the complexity of the system makes it expensive to service and maintain

Equipment required for high-level interfacing is as follows:
For each elevator:

- one reader (can be silicon key, magstripe, wiegand, proximity, smartcard, etc etc)
- one reader interface module (ACE-2) with RS485 daughter board

To manage the readers and the interface

- one CS controller with high level interface firmware
- one DUART communications expansion board
- appropriate communication daughter-boards RS232 or RS485 depending on elevator interface requirement
- comms hubs to split the RS485 signals between the elevators

In general each high level interface is subtly different and CS Technologies must be consulted regarding the configuration and exact requirements of a project involving high level interfacing.

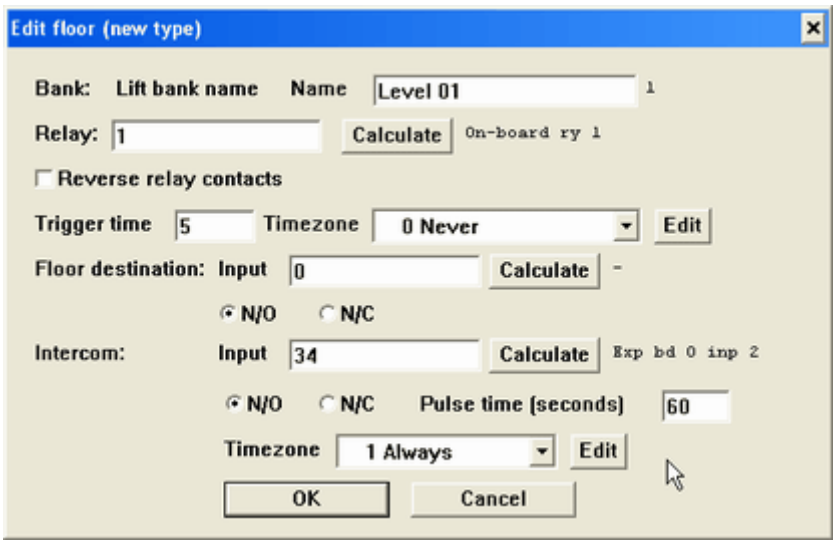
Understanding elevators
Setting up an elevator system
Basic low-level interfacing
Low-level interfacing with call destination reporting - pre-sensing
Low-level interfacing with call destination reporting - post-sensing
Floor triggering inputs

Elevator overview

7.8 Floor triggering inputs

For any floor in a lift bank it is possible to define an input on the associated controllers which will trigger that floor. This is typically used for interfacing with an intercom system. A unique feature is that it allows a separate trigger time for an pulse of this type as opposed to when someone uses a credential in the lift.

The floor triggering inputs are set up from the Hardware/Lifts/Edit lift bank/Edit floor screen which is shown below.



The floor triggering input parameters for the floor are under the 'Intercom' section.

- Intercom input - select the input which will trigger this floor. This can be any input on the system; it usually is on a 16-way expansion board but for smaller systems could be an available on-board input or a PIG input.
- N/O or N/C - select whether the device on the input is normally open or normally closed
- Pulse time - select the amount of time that the floor is activated for when the input is triggered. This is to give time for an intercom for example to allow the elevator to be called to the landing and still have the input triggered.
- Timezone - this parameter defines the timezone during which the intercom will work. This might be used for example if the pushbutton was on a reception desk and it was desired that the triggering only work during the day.

Understanding elevators
Setting up an elevator system
Basic low-level interfacing
Low-level interfacing with call destination reporting - pre-sensing
Low-level interfacing with call destination reporting - post-sensing
High-level interfacing

Elevator overview

8 Installing readers

8.1 Reader installation overview

The CS controller supports a wide range of readers. The reader types fall into four interfaces - iButton, Clock and Data, Wiegand and Presco. Door/alarm firmware supports up to four readers; elevator firmware supports a single reader.

8.2 Silkey

Overview
The Silkey (or Silicon Key) reader is a durable, cost-effective and high security reader. The reader face is manufactured from stainless steel and the credential is a convenient keyfob which can be easily branded for different applications.

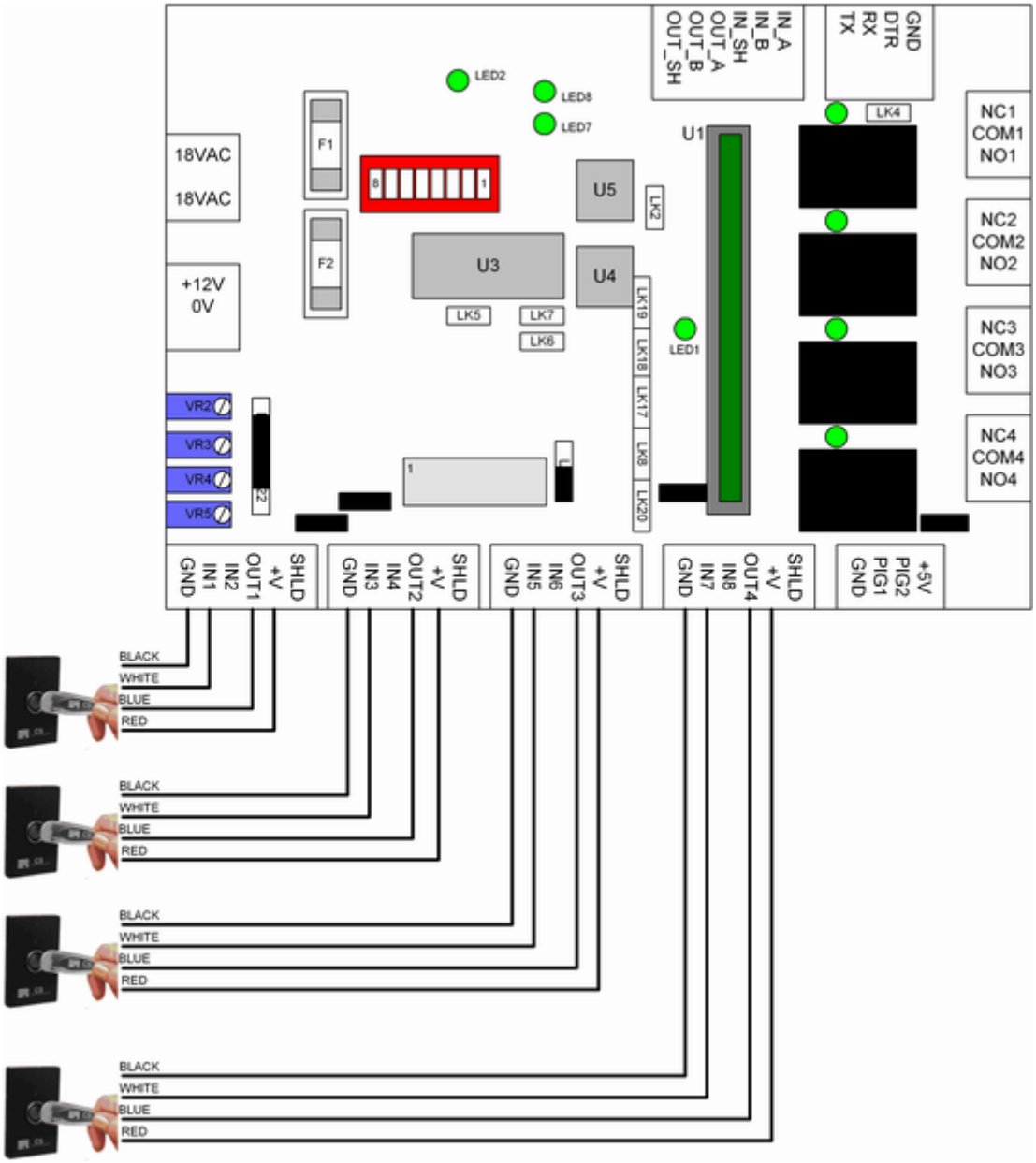
Silicon Keys provide a very high security credential because they are guaranteed to be unique world-wide.

Cable requirements
The readers require unshielded twisted pair cabling (UTP or CAT-5 cable) a maximum of 100m distance from the readers to the controller. The cable MUST be unshielded.

Terminations
The Silkey reader has four wires terminated as per the table below.

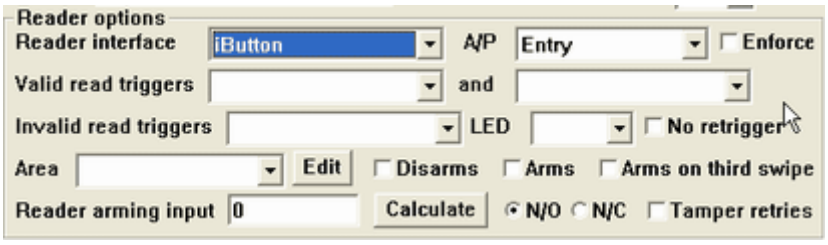
Colour	Name	Reader 1	Reader 2	Reader 3	Reader 4
BLACK	Ground	GND	GND	GND	GND
RED	+5V	+V	+V	+V	+V
WHITE	DATA	IN1	IN3	IN5	IN7
BLUE	LED	OUT1	OUT2	OUT3	OUT4

A diagram of the controller with four Silkey readers is below.



Link settings
Reader interrupt links - LK8, LK17, LK18, LK19, LK20 - all OFF
Reader LED links - LK9, LK10, LK11, LK12 - all ON
Reader voltage link - LK22 - UP
Reader pullup link - LK21 - DOWN

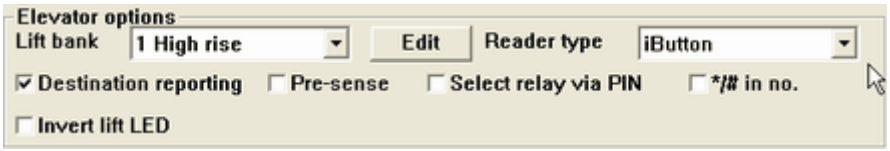
Configuration in software
To select a Silkey reader for a particular door, go to Hardware/Controllers/Edit controller/Edit door. Under the 'reader interface' drop-down menu select iButton.



This will automatically set up the input options so that scanning for PIGs is enabled on the

relevant port, so that the Silkey reader can be read.

Similarly for an elevator controller under Hardware/Controllers/Edit controller select the iButton reader type.



Boosting the signal
PIG-Boosters can be used to increase the reading distance and reliability of the Silkey readers. For more information see the PIG Boosters topic.

Mixing Silkey readers with other readers
It is possible to mix reader types. If Silkey readers are mixed with any other type of reader it is imperative that the input that the Silkey reader is placed on does not have an interrupt link associated with it. Accordingly if there are other reader types on the controller then:

IN1 - cannot be used for Silkey readers if other reader types are also on the controller
IN3 (door 2) - can be used for Silkey reader - LK19 must be OFF
IN5 (door 3) - can be used for Silkey reader - LK17 must be OFF
IN7 (door 4) - can be used for Silkey reader - LK17 must be OFF

Wiegand
Presco
Clock and Data

Reader installation overview

8.3 Wiegand

Overview
The Wiegand interface is a standard way for readers to interface to access control systems. Although fairly low-security there are many different types of readers which utilise the wiegand interface.

CS Technologies increases the versatility of the wiegand interface by storing a full site code and card number for each user.

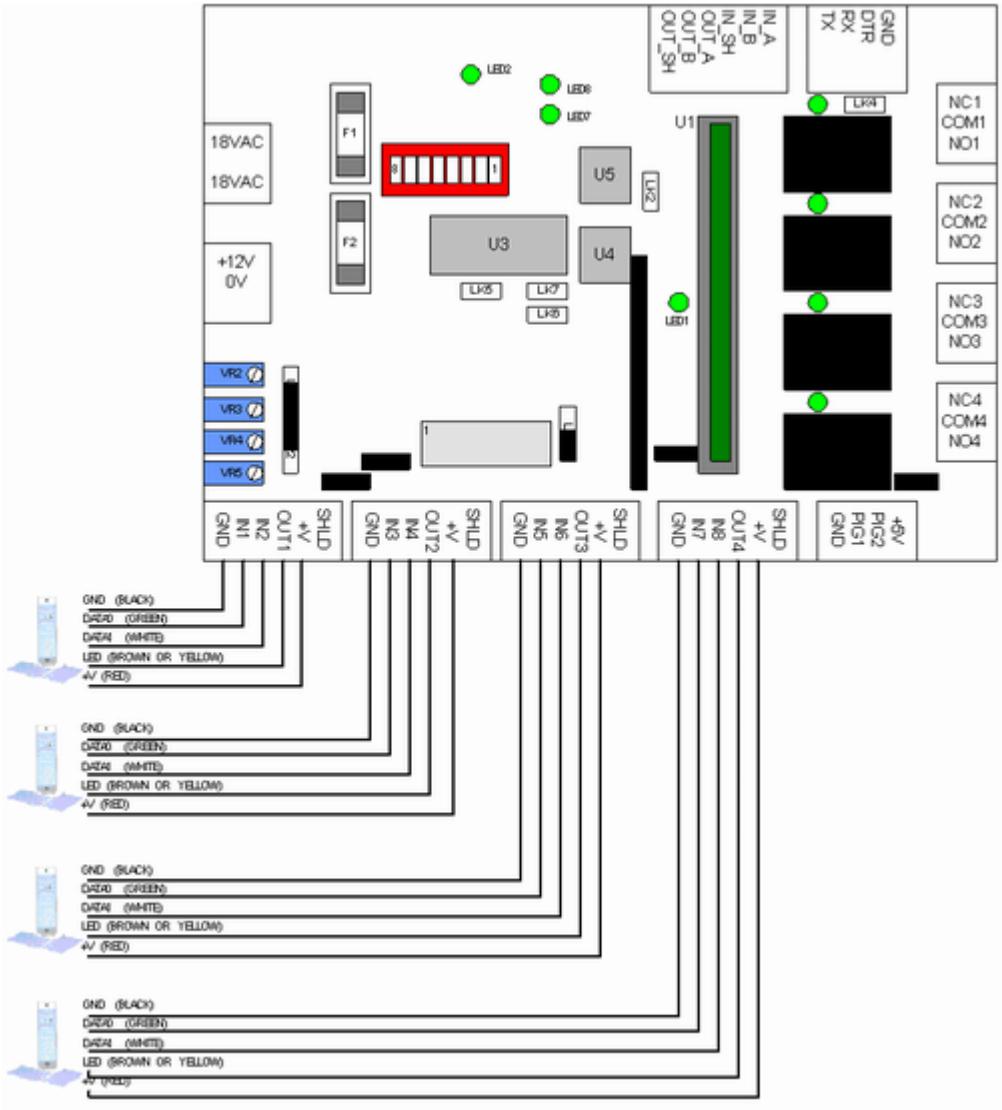
Readers which use the Wiegand interface include HID proximity readers, HID wiegand swipe readers, Motorola proximity readers, Keri proximity readers and many hundreds of others.

Cable requirements
Wiegand readers require 6-core shielded cable a maximum of 100m (500 feet) distance from the readers to the controller.

Terminations
Wiegand readers have five wires terminated as per the table below.

Colour	Name	Reader 1	Reader 2	Reader 3	Reader 4
BLACK	Ground	GND	GND	GND	GND
RED	+5V or +12V (check reader documentation)	+V	+V	+V	+V
GREEN	DATA-0	IN1	IN3	IN5	IN7
WHITE	DATA-1	IN2	IN4	IN6	IN8
BROWN or YELLOW	LED	OUT1	OUT2	OUT3	OUT4

A diagram of the controller with four wiegand readers is below.



Link settings

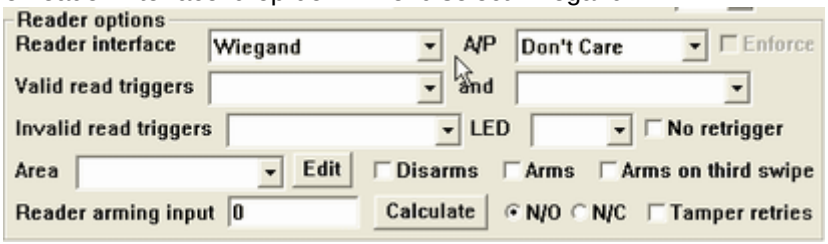
Reader interrupt links - These links are associated with particular readers as follows:
Wiegand reader 1 (IN1/2) - LK20 must be ON
Wiegand reader 2 (IN3/4) - LK18 and 19 must be ON
Wiegand reader 3 (IN5/6) - LK8 and 17 must be ON
Wiegand reader 4 (IN7/8) - LK8 and 17 must be ON

Note that any link in place for a reader stops that input being available for PIGs or other inputs. For example if IN7 is being used for an exit request button, LK17 must be OFF. This may mean that even though an input is not in use for a reader it is not available for an input.

Reader LED links - LK9, LK10, LK11, LK12 - all ON
Reader voltage link - LK22 - UP if reader voltage is 5V, DOWN if reader voltage is 12V. Check reader documentation.
Reader pullup link - LK21 - DOWN

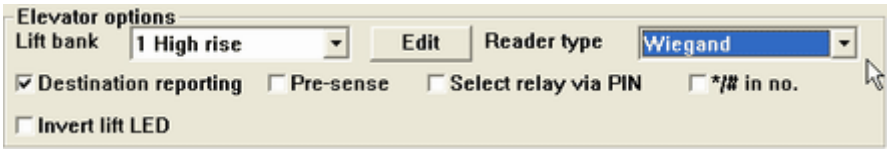
Configuration in software

To select a Wiegand reader for a particular door, go to Hardware/Controllers/Edit controller/Edit door. Under the 'reader interface' drop-down menu select Wiegand

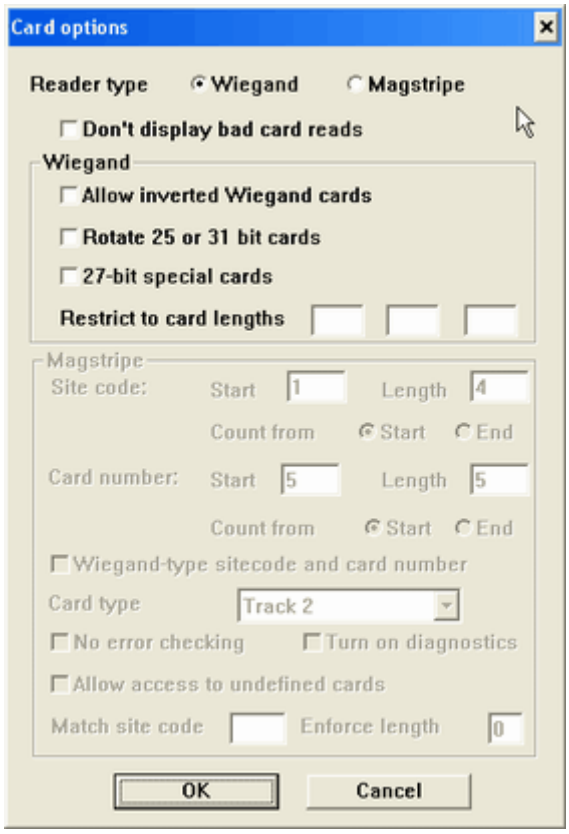


This will automatically set up the input options so that scanning for PIGs is disabled on the relevant ports.

Similarly for an elevator controller under Hardware/Controllers/Edit controller select the Wiegand reader type.



There are also some options available to change the behaviour of the system with Wiegand readers, under Technician/Site/Card options. The screen below is displayed.



The options which are available here and their meanings are:

- Don't display bad card reads - Wiegand readers pick up stray 'noise' pulses and the

controller can interpret these as bad card reads. Generally these indicate that there is noise but if they are genuine nuisance events they can be disabled by ticking this box.This stops the transaction log in the controller filling up with these spurious unnecessary events.

- Allow inverted wiegand cards - some wiegand readers (notably insertion key readers) have two different orientations for the credential, which send through the same information inverted. If this box is ticked then the 'inverted' version of any credential in the controller database will be interpreted correctly meaning that the system will be insensitive to the way that any particular credential is used.
- 27-bit special cards - some Motorola/Indala readers have a special format without start or stop bits. Ticking this box interprets these readers correctly
- Restrict to card lengths - allows the restriction of cards read to enforce a particular length of card read. Some sites will have multiple site codes but for higher security this allows the length of cards read to be restricted to a particular length or lengths. If all three of these boxes are empty then any length of wiegand data can be read and will be interpreted as a credential; if any one or more have a length in them then only cards of those length(s) will be interpreted as a valid credential; any other length will be interpreted as a bad card read.

Silkey
Presco
Clock and Data

Reader installation overview

8.4 Presco

Overview
The Presco range of keypads and proximity readers provides a powerful and convenient interface for readers which are very reliable and noise-immune. The CS Controller natively supports the use of the Presco range which therefore makes them very flexible and versatile because of the range of features offered by the Presco products.

There are three main products which utilise the Presco interface - the basic Presco keypad, the durable Vandal-resistant Presco keypad and the Presco Prox reader.

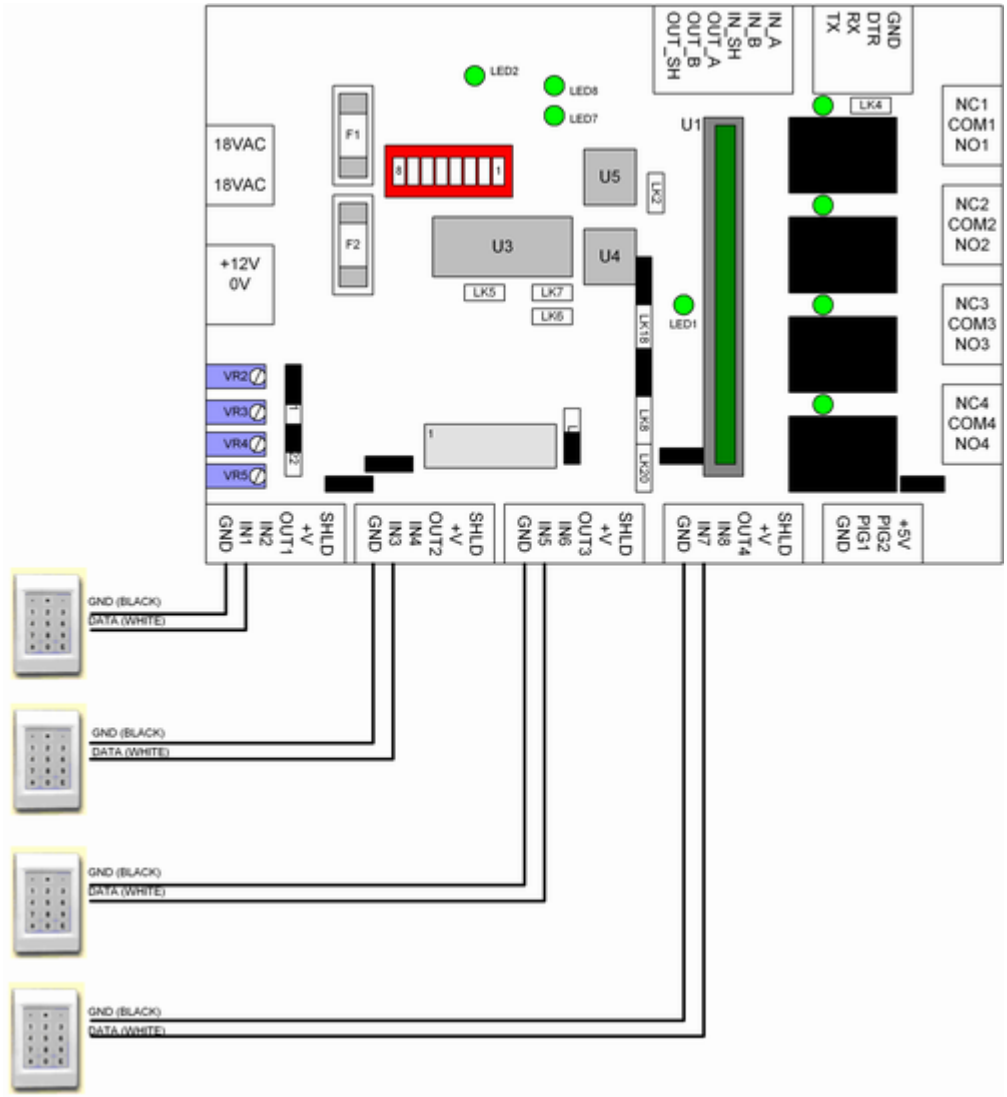
Cable requirements
The basic Presco keypad requires one pair of wires (figure-8) cable and the keypad can be up to 100m from the controller.
The vandal-resistant Presco keypad requires one pair of wires (figure-8) cable. The backlit version also requires a second pair to power the back-lighting in the keypads.
The Presco Prox reader requires two pairs of cable, one pair for the data and the other for power to the prox reader.

Terminations
Presco keypads have two wires terminated as per the table below.

Colour	Name	Reader 1	Reader 2	Reader 3	Reader 4
BLACK	Ground	GND	GND	GND	GND
WHITE	DATA	IN1	IN3	IN5	IN7

In addition the Presco prox reader requires 12VDC for power to the reader.

A diagram of the controller with four Presco keypads is below.



Link settings

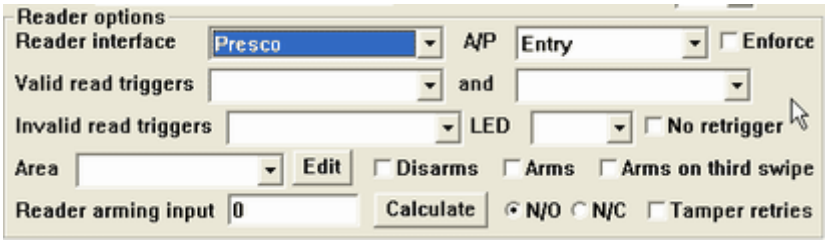
Reader interrupt links - These links are associated with particular readers as follows:
Presco reader 1 (IN1) - don't need any links on
Presco reader 2 (IN3) - LK19 must be ON
Presco reader 3 (IN5) - LK17 mst be ON
Presco reader 4 (IN7) - LK17 must be ON

Note that any link in place for a reader stops that input being available for PIGs or other inputs. For example if IN7 is being used for an exit request button, LK17 must be OFF. This may mean that even though an input is not in use for a reader it is not available for an input.

Reader LED links - LK9, LK10, LK11, LK12 - all ON. Not used unless there is separate indication (via a LED etc) for the door status.
Reader voltage link - LK22 - UP if Presco prox reader (reader voltage is 12V), DOWN for Presco keypads (which don't use the power connection)
Reader pullup link - LK21 - UP. This link is specifically to provide a higher pullup voltage for operation of the Presco keypads.

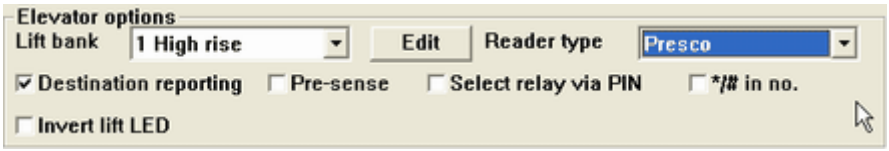
Configuration in software

To select a Presco reader for a particular door, go to Hardware/Controllers/Edit controller/Edit door. Under the 'reader interface' drop-down menu select Presco.



This will automatically set up the input options so that scanning for PIGs is disabled on the relevant ports.

Similarly for an elevator controller under Hardware/Controllers/Edit controller select the Presco reader type.



Silkey
Presco
Clock and Data

Reader installation overview

8.5 Clock and Data

Overview
The Clock and Data interface is a standard way for readers, typically magnetic stripe readers, to interface to access control systems. Clock and data readers transmit data in standard formats and allow more information to be stored on a card. Examples of clock and data readers include most mag-stripe readers; many other reader types also have clock and data versions.

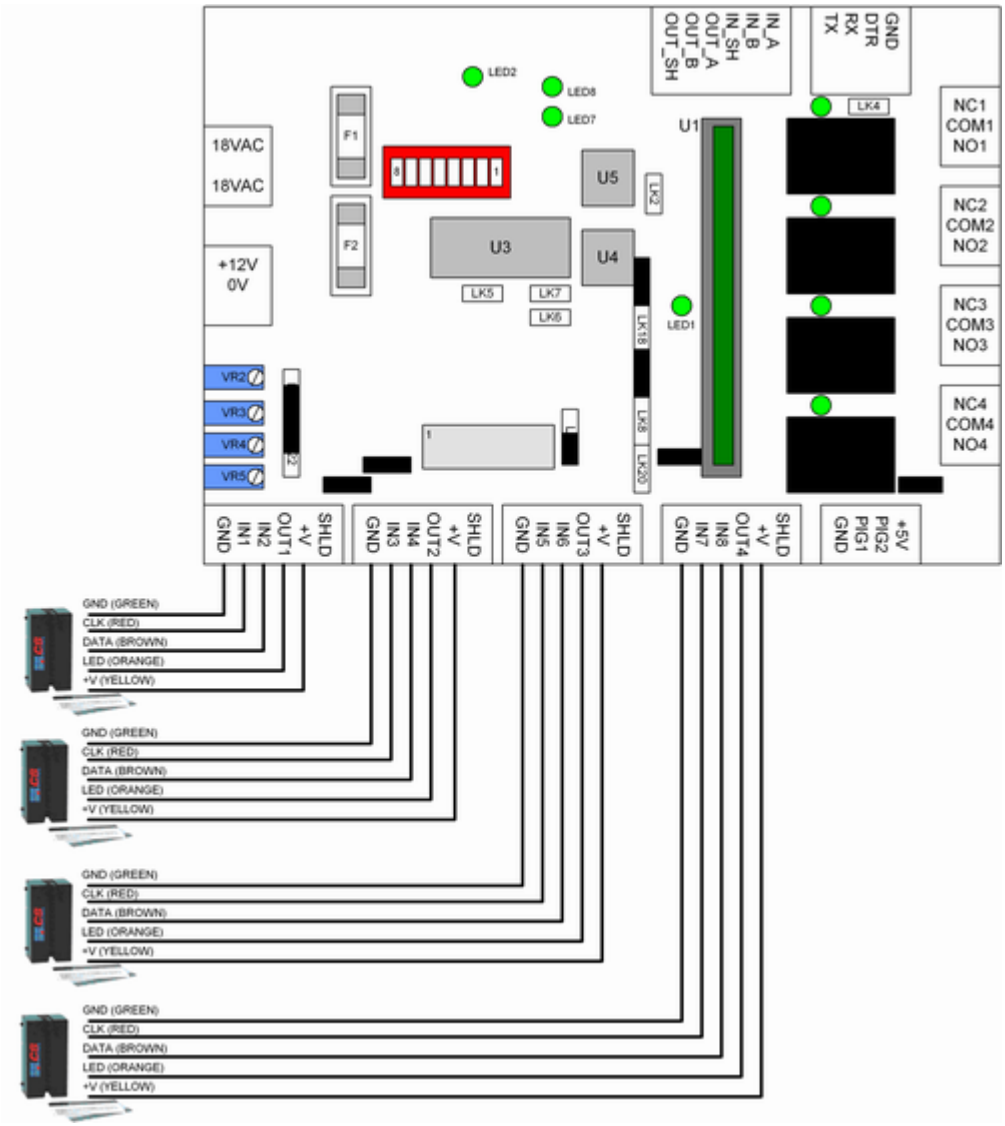
The CS system is very versatile when it comes to Clock and Data interfaces, because it allows extraction of any part of the information in the data stream as the site code and any other part as the card number. This makes it very adaptable to use for existing cards also.

Cable requirements
Clock and Data readers require 6-core shielded cable a maximum of 100m (500 feet) distance from the readers to the controller.

Terminations
Clock and data readers have five wires terminated as per the table below. Note that many different clock and data readers are available and they may have different coloured wires to those below.

Colour	Name	Reader 1	Reader 2	Reader 3	Reader 4
GREEN	Ground	GND	GND	GND	GND
YELLOW	+5V or +12V (check reader documentation)	+V	+V	+V	+V
RED	CLOCK	IN1	IN3	IN5	IN7
BROWN	DATA	IN2	IN4	IN6	IN8
ORANGE	LED	OUT1	OUT2	OUT3	OUT4

A diagram of the controller with four clock and data readers is below.



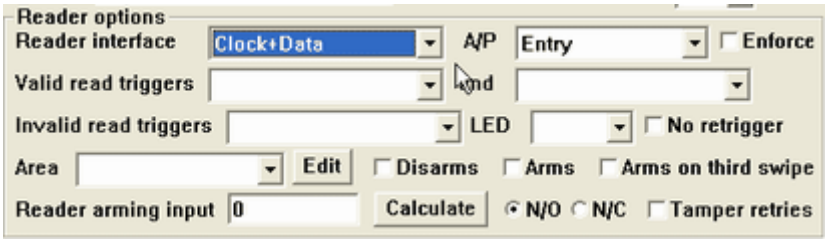
Link settings

Reader interrupt links - These links are associated with particular readers as follows:
Clock and data reader 1 (IN1/2) - don't need any links on; LK20 must be OFF
Clock and data reader 2 (IN3/4) - LK19 must be ON, LK18 must be OFF
Clock and data reader 3 (IN5/6) - LK17 must be ON, LK8 must be OFF
Clock and data reader 4 (IN7/8) - LK17 must be ON, LK8 must be OFF

Note that any link in place for a reader stops that input being available for PIGs or other inputs. For example if IN7 is being used for an exit request button, LK17 must be OFF. This may mean that even though an input is not in use for a reader it is not available for an input.

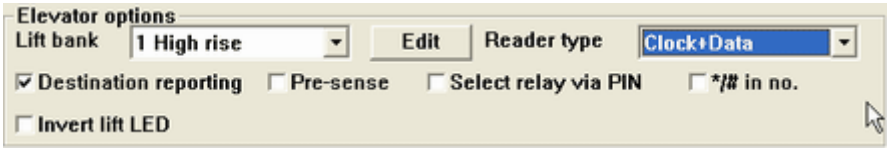
Reader LED links - LK9, LK10, LK11, LK12 - all ON
Reader voltage link - LK22 - UP if reader voltage is 5V, DOWN if reader voltage is 12V. Check reader documentation.
Reader pullup link - LK21 - DOWN

Configuration in software
To select a clock and data reader for a particular door, go to Hardware/Controllers/Edit controller/Edit door. Under the 'reader interface' drop-down menu select Clock and Data.

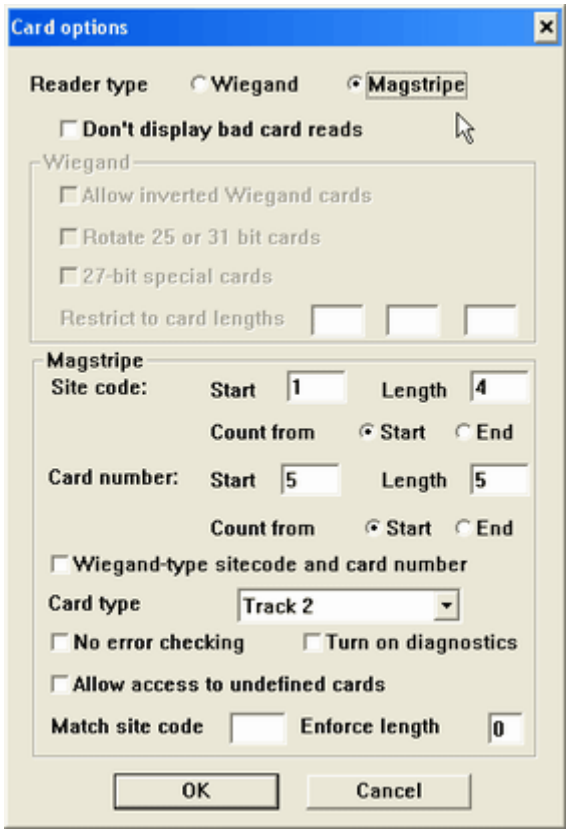


This will automatically set up the input options so that scanning for PIGs is disabled on the relevant ports.

Similarly for an elevator controller under Hardware/Controllers/Edit controller select the Clock and Data reader type.



There are also some options available to change the behaviour of the system with Clock and Data (magstripe) readers, under Technician/Site/Card options. The screen below is displayed.



The options which are available here and their meanings are:

- Don't display bad card reads - Clock and Data readers can pick up stray 'noise' pulses and the controller can interpret these as bad card reads. Generally these indicate that there is noise but if they are genuine nuisance events they can be disabled by ticking this box.This stops the transaction log in the controller filling up with these spurious unnecessary events.
- Site code parameters - these allow selection of the start and length of the site code from the Clock and Data 'data stream'. The data stream can consist of up to 40 characters. The user credential consists of a number up to 9 digits in length. The 'site code' allows the first part of this credential to be selected as any part of the data stream, and also allows selection of the number by counting digits from the start or the end of the number.
- Card number parameters - these allow selection of the start and length of the card number from the Clock and data 'data stream'. The 'card number' allows the second part of the user credential to be selected as any part of the data stream, and also allows selection of the number by counting digits from the start or the end of the number. For example, a typical card might have data as follows:

  ;3760095704930 14?3

  If the site code start is 1 and length is 4 then the site code selected from this data stream will be 3760.
  And if the card number start is 5 and length is 5 then the card number selected from this data stream will be 09570.
  The credential consists of these two numbers put together i.e. 376009570.
- Wiegand-type sitecode and cardnumber - if this is ticked then the sitecode is 'shifted' so it forms the top 16 bits of a 32-bit number, and the card number is 'shifted' so that it forms the bottom 16 bits of a 32-bit number.
- Card type - there are three different types which can be selected - Track 2 is the standard numeric data on most credit cards, Track 1 is the alphanumeric data on most credit cards, and Infineer is a proprietary format used on magstripe format cards sold by the smartcard company Infineer.
- No error checking - standard format of clock and data information includes parity bits for each character as well as a LRC (longitudinal redundancy check). If this box is ticked then this information is ignored; if the box is not ticked then if a card has an error in its parity or LRC it is interpreted as a bad card read.
- Turn on diagnostics - if this is ticked then the data from the card is transmitted out the serial port of the controller as it is processed. Sometimes this is used to interface with cash register systems.
- Allow access to undefined cards - if this is ticked then any card which is not in the database will be granted access. Cards which are in the database will have their access level checked and authorised if applicable. This allows a situation where cards can be 'hotlisted' as denied by adding them to the database without adding every single other possible card to the database.
- Match site code - this works in conjunction with the 'allow access to undefined cards' by enforcing a match of some part of the card format to have a particular site code.
- Enforce length - this works in conjunction with the 'allow access to undefined cards' by enforcing a match of the length of the card data.

Silkey
Wiegand
Presco
Clock and Data

Reader installation overview

9 Output and input expansion

9.1 Expansion overview

With the CS system each controller can be expanded to have additional inputs and outputs.

Additional inputs are used as alarm inputs, door status inputs, exit request inputs, reader arming inputs, elevator floor destination sensing inputs and elevator floor triggering inputs.

Additional outputs are used to control door strikes, for the various alarm area relay functions (alarms, armed, disarmed, buzzer etc), to control the various floors in an elevator and to indicate alarm conditions.

In some cases when input or output expansion is used this 'uses up' some of the inputs and outputs of the controller and reduces the reader capacity of the controller.

This part of the manual describes the installation of the various types of input and output expansion for the system.
A unique feature of the CS system is the ability to expand the inputs and outputs using Point Identification Gadgets or PIGs. PIGs are addressable devices, each with a unique ID, which can be monitored and/or controlled from the controller. Using PIGs the inputs and outputs of the controller can be easily expanded.

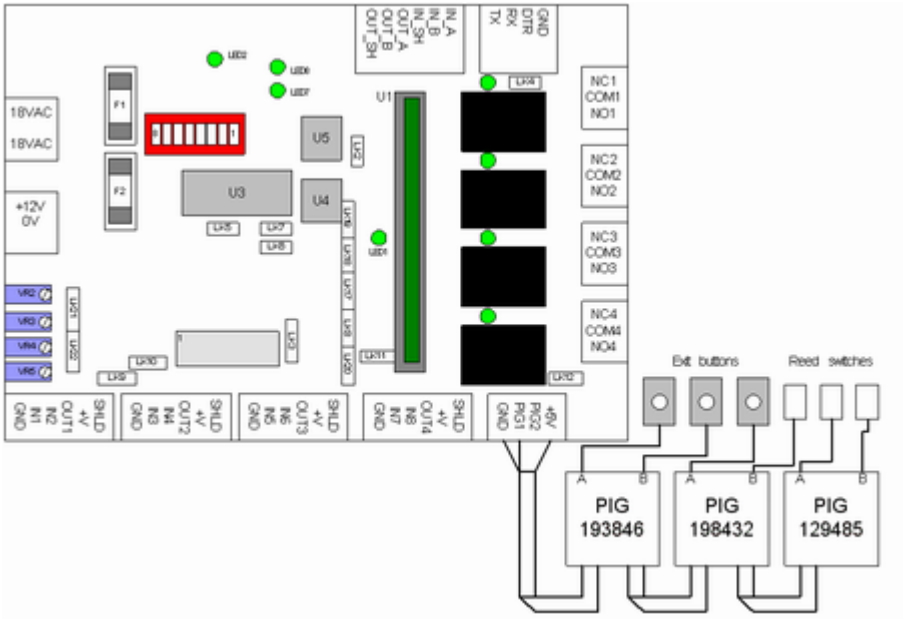
The following topics explain the PIGs and how they work and how they are configured.
Point Identification Gadgets (PIGs)
PIG boosters

The following topics describe the various ways of expanding the inputs and outputs of the system.

PIG-2
PIG-3
PIGPEN
16-way input board
4-way relay board
16-way relay board

9.2 Point Identification Gadgets

Point Identification Gadgets or PIGs are electronic devices each of which have a unique ID (or address). Multiple PIGs can communicate with the controller and provide additional inputs and/or outputs on a single bus. An example of the layout of a system utilising PIGs is below.



In the system above, the inputs on the controller have been expanded using a PIG bus connected to the PIG1 terminal. Three 2-port PIGs (PIG-2's) have been added. This gives six additional inputs which in this case are being used for connection to three exit buttons and three reed switches.

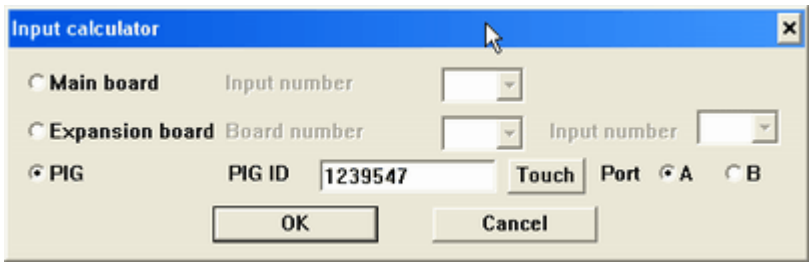
PIGs all have an ID which is unique. They have two ports A and B - on a PIG2 these are both inputs, on a PIG3 port A is a relay output and port B is an input. A PIGPEN has either 12 or 24 pigs each with two ports making a 24-input or 48-input board. PIGPENs also have a PIG configured with two relay outputs.

Cable requirements

PIG2's and PIG3's are supplied with RJ connected flat cable which can be used to connect them to the PIG bus. If for any reason it is desired to lengthen the PIG bus this should be done with 3 pairs of Cat-5 cable (unshielded twisted pairs or UTP). It is important that the cable be unshielded as otherwise the cable capacitance stops the PIGs from communicating.

Programming with PIGs

Pigs are programmed just like any other input. Anywhere that an input or output can be defined there will be a 'calculate' button. Below is shown the calculate input screen.



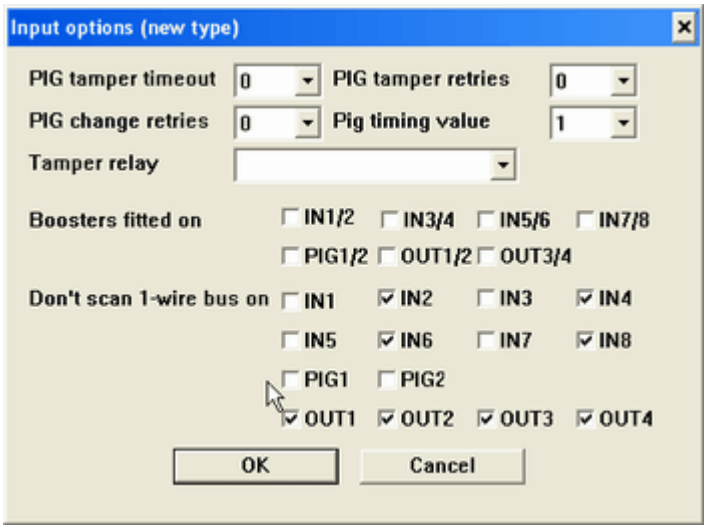
If the input is on a PIG the ID can be entered, and port A or B selected. In this case a PIG has been selected for the input, and port A will be used.

Registering PIGs

It is also possible to register PIGs from the input calculator by clicking the 'Touch' button. When this is clicked, the controller which is defined as the registration controller (in Advent under Admin/Workstation settings, and in PC3 under Technician/Site) will attempt to find any single PIG connected to one of its valid PIG buses. If it finds one the PIG ID will be read and placed into the PIG number field.

The PIG bus

In the example above it can be seen that the PIGs are all connected in a 'daisy chain' to a single input on the controller. In order for PIGs to be scanned on that port this must be enabled in the software. This is done under Hardware/Controllers/Edit controller/Input options. The input options screen is shown below.



On this screen, the '1-wire' bus refers to the PIG bus. Silkey readers and PIGs communicate using the 1-wire bus. In the example above, 'Don't scan 1-wire bus' is not ticked for IN1, IN3, IN5, IN7, PIG1 and PIG2. This means that PIGs can be monitored on any of these ports. The default setting is that PIG1 and PIG2 are available for PIGs and the other ports are not available but this can be changed from this screen.

Multiple devices can be monitored on a PIG bus. Any unused port can be used as a PIG bus. With a PIG booster fitted, up to 25 PIGs (= 50 inputs) can be monitored on a single PIG bus, with a maximum distance of up to 50m from the controller to the last PIG on the bus. The firmware supports up to 250 inputs (= 125 2-port PIGs) per controller.

Tampers
The PIGs are communicated with via digital signals. The controller can detect whether a PIG is online or not. If a PIG is not online it is referred to as being 'in tamper'. When it is in tamper the inputs or outputs on the PIG cannot be monitored or controlled.

Multiple buses
Any unused input on the controller can be used for PIGs. When a PIG is programmed the controller will search through all the available ports (the ones which do not have a tick in the 'don't scan 1-wire bus' in the Hardware/Controllers/Edit controller/Input options screen) for each PIG. If PIGs are moved from one bus to another then it may take a few seconds for the controller to recognise that they have moved.

PIG parameters
On the Hardware/Controllers/Edit controller/Input options screen (as shown above) there are a number of parameters which can be set for communication with the PIGs. The default settings for these will probably be correct. The settings are:

- PIG tamper timeout - this sets the number of seconds that a PIG can be in tamper (offline) before it is reported to the screen. If there are lots of 'nuisance' timeout messages this setting can be increased.
- PIG tamper retries - this sets how many times the controller will attempt to communicate with each PIG before reporting that it is in tamper. In a noisy environment it may be necessary to increase this.
- PIG change retries - this sets how many times the controller will attempt to verify a change in state on an input. This can be increased to reduce the incidence of false alarms due to electrical noise.
- PIG timing value - this sets an internal timing constant used when communicating with the PIGs. The default value of 1 should not need to be altered.

- Tamper relay - any relay on the controller can be defined as a 'tamper relay'. This relay will operate if any PIG goes into tamper.
- Boosters fitted on - this indicates where PIG boosters are fitted.
- Don't scan 1-wire bus on - unticked boxes here can have PIG buses fitted. Obviously PIGs cannot share ports with readers or other types of inputs, so only available ports should have these boxes unticked. Generally PIGs are connected to the PIG1/PIG2 ports.

Links
Any ports used for PIGs cannot have their respective interrupt links in place. The links which must be out are as follows:

Port used for PIG or booster	Link which must not be in place
IN2	LK20
IN3	LK19
IN4	LK18
IN5, IN7	LK17
IN6, IN8	LK8

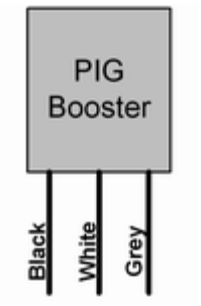
PIG boosters
PIG-2
PIG-3
PIGPEN
16-way input board
4-way relay board
16-way relay board

Expansion overview

9.3 PIG boosters

The PIG booster is used whenever it is desired to improve the reliability of communications with PIGs (or Silkey readers). Generally PIG boosters are recommended in any situation where the PIGs are not situated directly adjacent to the controller. PIGs can be up to 50m from the controller but must have PIG boosters fitted if there is any distance between the controller and the PIGs.

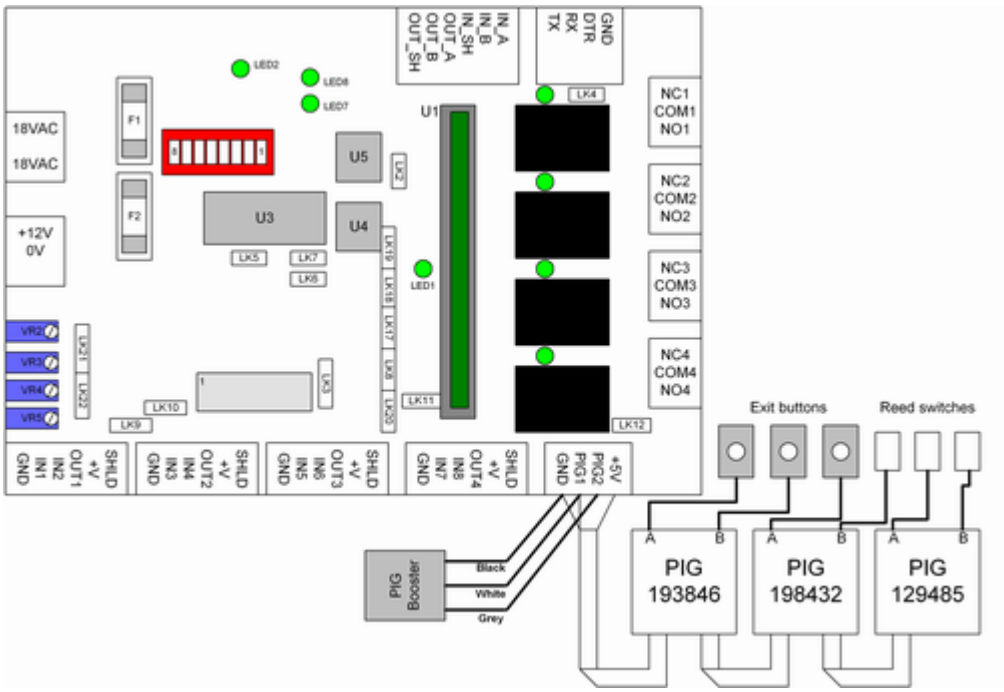
PIG boosters are fitted at the controller and use up an additional port to drive the signals to the PIGs further. Below is shown a diagram of a PIG booster.



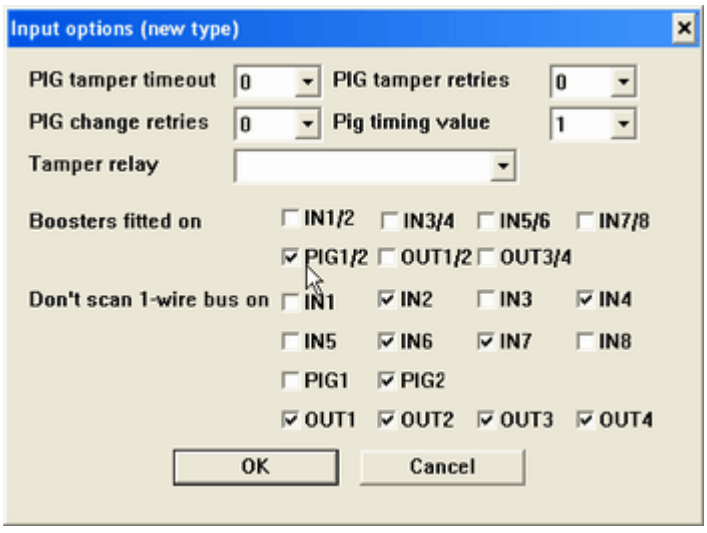
As shown, the booster has three flying leads. The black wire connects to GND, the white wire connects to the PIG port being used for the PIG bus and the grey wire connects to the adjacent port which is then used to drive the signals to the booster. A setting must be done in the software to tell the system that the bus is to be driven by this adjacent port.

Any unused input on the controller can be used for connection of a PIG bus. When a booster is fitted the adjacent port is 'used up' by the booster and extends the reliability of the bus. Because Silkey readers communicate using a similar protocol to PIGs the booster also can be used to extend the range of Silkey readers.

An example will help to illustrate this.



In the diagram above a booster has been fitted to the PIG bus being driven by PIG1. The booster connects to PIG1 and PIG2. This is set up under Hardware/Controllers/Edit controller/Input options. This screen is shown below.



Any unused input can be used for a PIG bus. If the bus is boosted then the adjacent input is used up by the booster; inputs are grouped with boosters as follows:

PIG bus input (white wire on booster)	Boosted input (grey wire on booster) used up
IN1	IN2
IN3	IN4
IN5	IN6
IN7	IN8
PIG1	PIG2
OUT1	OUT2
OUT3	OUT4

Boosters with Silkey readers
Boosters can also be used with Silkey readers to improve the reading distance of the reader. In this case the booster is fitted with the white wire on the relevant input and the grey wire on the adjacent port as in the table above; the appropriate 'boosters fitted on' setting must also be made under Hardware/Controllers/Edit controller/Alarm options.

Point Identification Gadgets (PIGs)
PIG-2
PIG-3
PIGPEN
16-way input board
4-way relay board
16-way relay board

Expansion overview

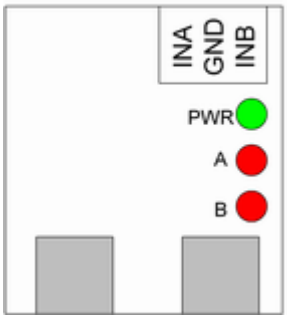
9.4 PIG-2

The PIG-2 is a modular device with two inputs. It attaches to the PIG bus and provides a low-cost convenient way to expand the input capacity of the system.

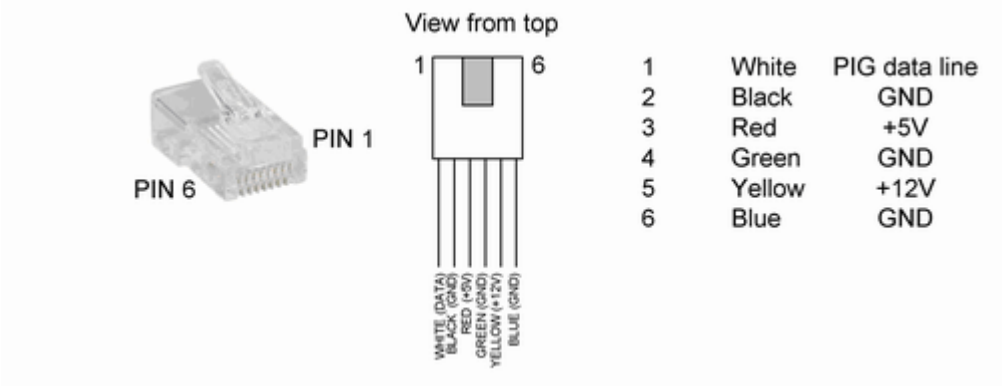
The PIG-2 is supplied in a white box with LED indicators. It has two 'RJ' connectors for connecting the PIG-bus.

The PIG-2 connects to the PIG-bus either directly to the controller or in a daisy-chain to the previous PIG in the bus. Up to 25 PIGs may be connected to a single bus. It is recommended that a PIG-booster also be fitted to ensure reliable communication with the PIGs.

The PIG-2 has two inputs which are indicated by the LEDs on the case. Each PIG-2 has a unique ID which is used when programming it into the system. A diagram of the PIG-2 is shown below.



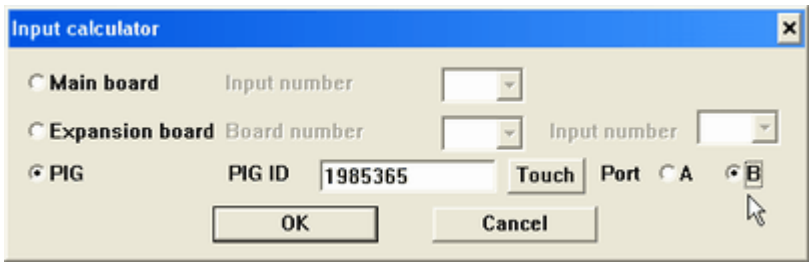
The connectors for the PIG2 are RJ-12 connectors with 6 conductors. The connections for them are as follows:



1	White	PIG data line
2	Black	GND
3	Red	+5V
4	Green	GND
5	Yellow	+12V
6	Blue	GND

The first PIG on the bus connects to the required port on the controller (in combination with a PIG booster if desired) and then subsequent PIGs connect in a daisy-chain using the modular connectors. Note that +12V is supplied in the RJ12 connector but is not actually used for PIG2's. It is however used for PIG3's and PIGPENs so it is recommended that the +12V be connected. It is also recommended that all the GND connections be made to ensure a good path for the ground return signals.

The PIG is programmed into the system in any place where an input can be used. The 'Calculate' button is pressed and this will bring up the input calculator. Select the PIG radio button and then enter the PIG number. Select the port A or B for the input and click OK. The calculator will work out the appropriate number and store it in the controller so that the PIG can come online.



The devices connected to the PIG are any item which has a voltage-free contact e.g. a reed switch, PIR etc.

For details about the PIG bus see the Point Identification Gadgets topic.

Point Identification Gadgets (PIGs)
PIG boosters
PIG-3
PIGPEN
16-way input board
4-way relay board

16-way relay board

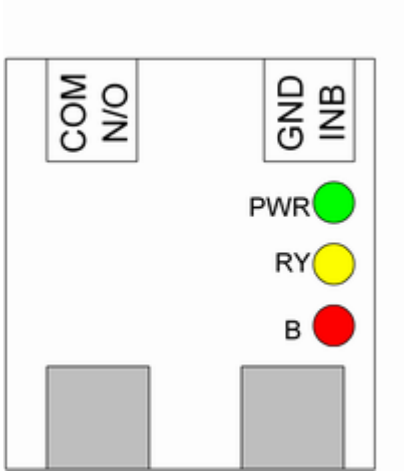
Expansion overview

9.5 PIG-3

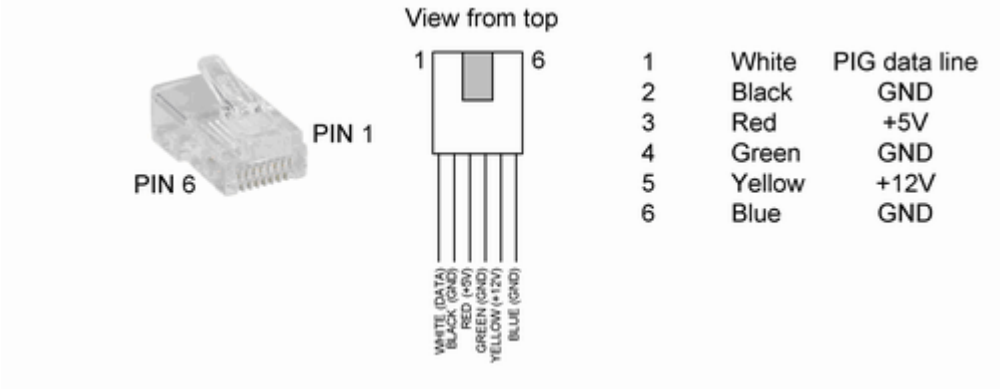
The PIG-3 is similar to a PIG-2 except that instead of two inputs, it has one input and one output. It connects to the PIG bus and allows easy expansion of the inputs and outputs of the controller.

The PIG-3 connects to the PIG-bus either directly to the controller or in a daisy-chain to the previous PIG in the bus. Up to 25 PIG devices may be connected to a single bus. It is recommended that a PIG-booster also be fitted to ensure reliable communication with the PIGs.

The PIG-3 has one relay output (port A) (yellow LED) and one input (port B) (red LED). Each PIG-3 has a unique ID which is used when programming it into the system. A diagram of the PIG-3 is shown below.



The connectors for the PIG3 are RJ-12 connectors with 6 conductors. Both connectors have the same terminations and loop in and out of each PIG. The connections for them are as follows:

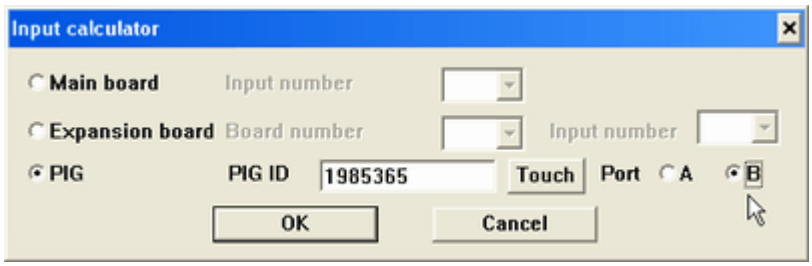


1	White	PIG data line
2	Black	GND
3	Red	+5V
4	Green	GND
5	Yellow	+12V
6	Blue	GND

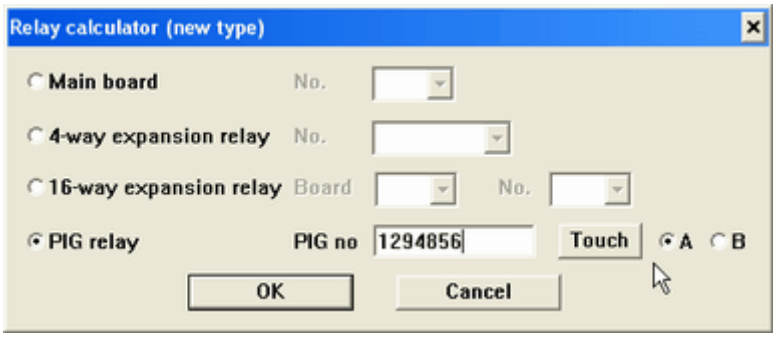
The first PIG on the bus connects to the required port on the controller (in combination with a PIG booster if desired) and then subsequent PIGs connect in a daisy-chain using the modular connectors. It is recommended that all the GND connections be made to ensure a good path for the ground return signals.

The PIG-3 has an input and an output. The input is on port B, and is programmed into the system in any place where an input can be used. The 'Calculate' button is pressed and this will bring up the input calculator. Select the PIG radio button and then enter the PIG number. Select the port B for the input and click OK. The calculator will work out the appropriate number and store it in the controller so that the PIG can come online. The devices connected to the PIG are any item which

has a voltage-free contact e.g. a reed switch, PIR etc.



The output is on port A and is programmed under the Hardware/Controllers/Edit controller/relay screen. Pressing the 'Calculate' button here will bring up the relay calculator. Select the PIG radio button and then enter the PIG number.



The relay has normally open contacts which are rated at 1A 12VDC.

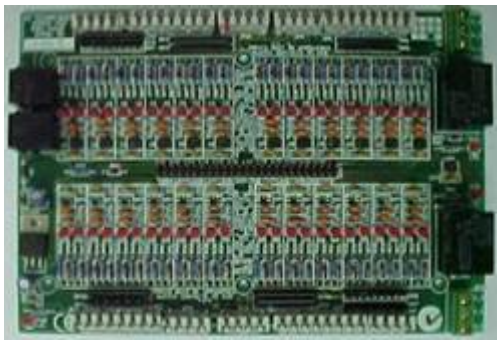
For details about the PIG bus see the Point Identification Gadgets topic.

Point Identification Gadgets (PIGs)
PIG boosters
PIG-2
PIGPEN
16-way input board
4-way relay board
16-way relay board

Expansion overview

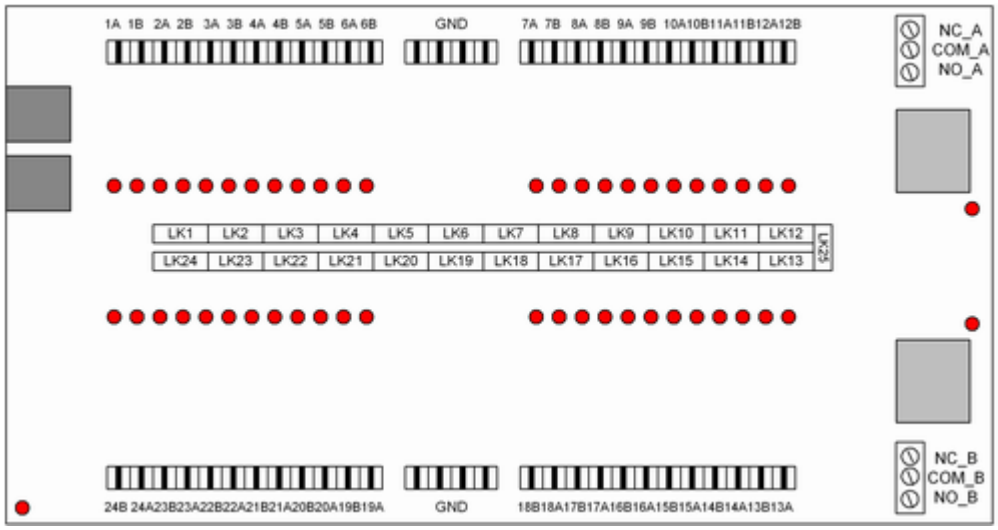
9.6 PIGPEN

The PIGPEN is a board which is fitted with either 24 or 48 inputs and two relay outputs.



Essentially the board is 12 or 24 PIG-2's plus a PIG with two relay outputs attached. Each individual PIG in the PIGPEN has an ID just like the PIG2 and the PIG3, and the board hangs off the PIG bus just like the other PIG devices.

A diagram of the PIGPEN is below.



On the left hand side of the PIGPEN are two RJ-12 connectors. These connectors are in parallel and allow the PIG bus to be connected to the PIGPEN, and to other PIGs on the bus.

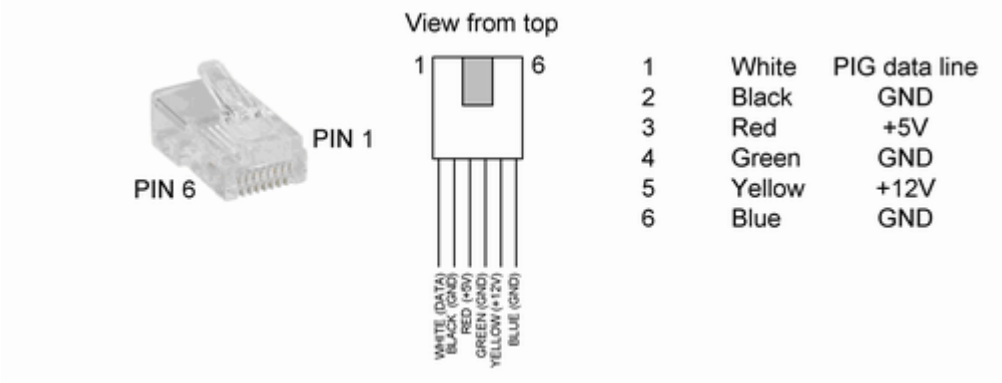
The connectors for inputs to the PIGPEN are modular 'Krone'-type connectors. A Krone tool is required to terminate inputs into these terminals. The terminals have a commong GND terminal. Maximum loop resistance for each input is approximately 20 ohms.

Each input has an LED indicator to show the status of the associated input.

There are links in the centre of the board for each PIG to allow the individual PIGs to be connected to the PIG bus.

On the right hand side are two C-form relay outputs controlled by the 25th PIG on the PIGPEN.

Connecting the PIGPEN to the PIG bus
The connectors for the PIG2 are RJ-12 connectors with 6 conductors. The connections for them are as follows:



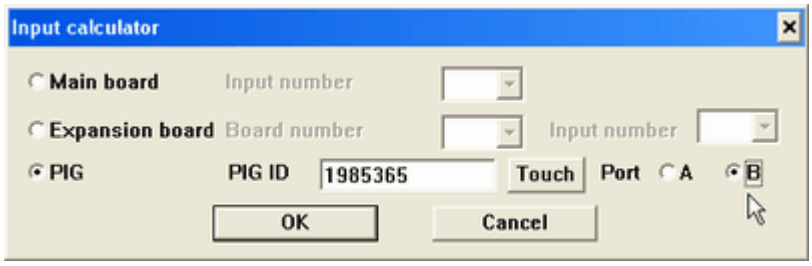
The first PIG on the bus connects to the required port on the controller (in combination with a PIG booster if desired) and then subsequent PIGs connect in a daisy-chain using the modular connectors. Note that +12V is supplied in the RJ12 connector but is not actually used for PIG2's. It is however used for PIG3's and PIGPENs so it is recommended that the +12V be connected. It is also recommended that all the GND connections be made to ensure a good path for the ground return signals.

Using the PIGPEN

The PIGPEN connects to any PIG bus on the controller. It is recommended because of the number of devices in the PIGPEN that a PIG-Booster be used. Up to 25 PIGs can be connected to a single PIG bus i.e. one PIGPEN-48 can be used on a single PIG bus.

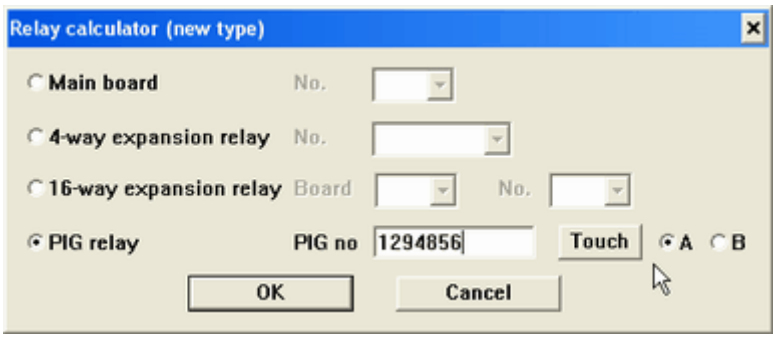
Programming the PIGPEN

The PIGPEN is supplied with a list of the PIG ID numbers for each PIG on the PIGPEN. The PIGPEN inputs are programmed into the system in any place where an input can be used. The 'Calculate' button is pressed and this will bring up the input calculator. Select the PIG radio button and then enter the PIG number. Select the port A or B for the input and click OK. The calculator will work out the appropriate number and store it in the controller so that the PIG can come online.



The devices connected to the PIG are any item which has a voltage-free contact e.g. a reed switch, PIR etc.

The PIGPEN relay outputs can be programmed under the Hardware/Controllers/Edit controller/relay screen. Pressing the 'Calculate' button here will bring up the relay calculator. Select the PIG radio button and then enter the PIG number. Select port A or B for relay A or B on the PIGPEN.



The relay has normally open contacts which are rated at 2A 24VDC.

Point Identification Gadgets (PIGs)
PIG boosters
PIG-2
PIG-3
16-way input board
4-way relay board
16-way relay board

Expansion overview

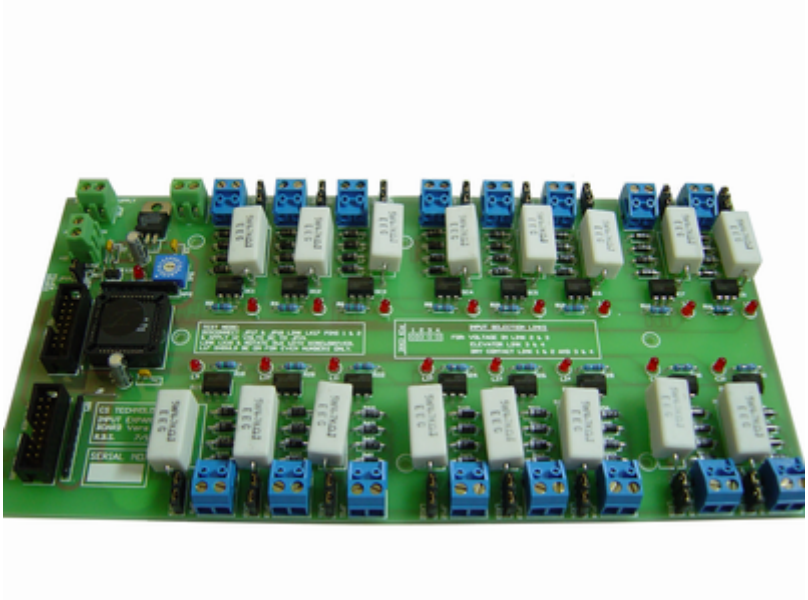
9.7 16-way input board

The 16-way input board allows expansion of the inputs on the controller in groups of 16. Each input board has an address and a maximum of 15 additional 16-way input boards can be added to the system to give up to 250 inputs on the system.

Input boards allow monitoring of 16 inputs. The inputs are opto-isolated and can operate in three modes:

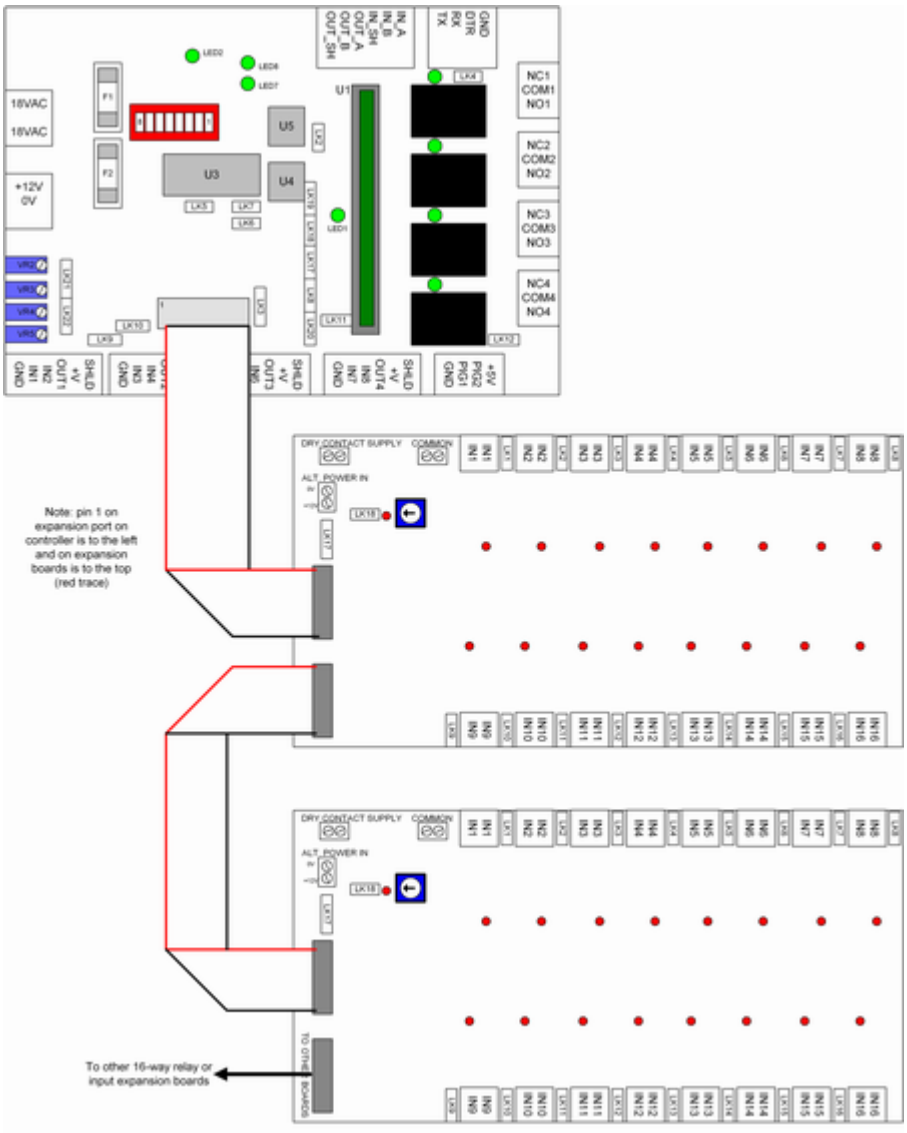
- dry contact, where the devices monitored have a relay or other type of voltage-free contact
- elevator mode, where the devices monitored have a voltage output with a common reference.
- voltage sensing, where the devices monitored have a voltage output

These modes are described in further detail below.



Connecting the 16-way input board

The 16-way input boards connect to the expansion port on the controller via a ribbon cable. Additional 16-way input or output expansion boards are added by connecting another ribbon cable from the output of the board to the input of the next one and so on, as depicted below. The ribbon cable must be connected so that pin 1 on the expansion port (on the left) connects to pin 1 on the expansion board (at the top) and so on.



Each input board must have its address selected on the 16-way rotary switch. Usually the first board is numbered as 0, the second board is numbered as 1 and so on. Input boards must all have a unique address; however input boards can be numbered the same as relay output boards.

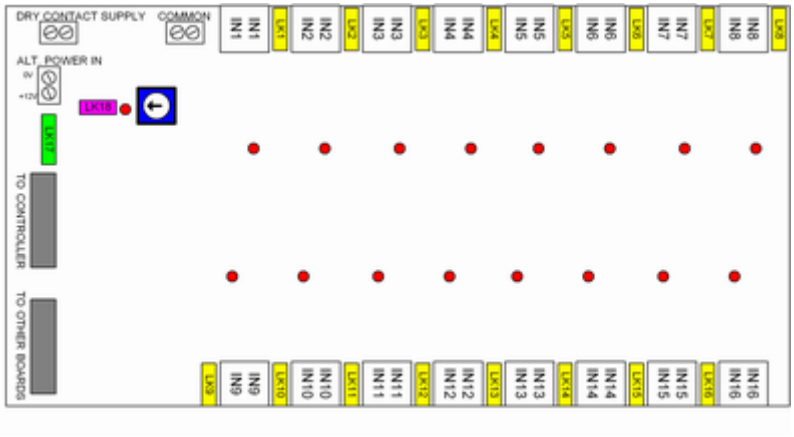
Controller configuration

Having input expansion boards fitted to the controller 'uses up' all the inputs on the controller except those for reader 1 (IN1, IN2 and OUT1). If 16-way input boards are fitted the on-board inputs are not available.

The controller must be configured with LK3 UP and LK19, LK18, LK17 and LK8 off.

Configuring the input board

A diagram of the input board is shown below.



The input board has 16 connectors for the inputs, links to configure the way the inputs work and connectors for power. The rotary switch is used to set the address of the input board. The links on the board are as follows:

- LK1-16 - these links are in pairs and allow configuration of the inputs for the various possible modes of operation (described below).
- LK17 - used to set the power supply input. LK17 is UP if the power is provided via the ALT POWER IN terminals (JP19). The power needs to be 12VDC. LK17 is DOWN if the power is provided via the ribbon cable. A maximum of three input boards can be powered via the ribbon cable.
- LK18 - this link is used for production testing of the board and is OFF in normal operation

Input board power

The input board can be powered either through the ribbon cable or from an external supply via the 'Alt Power In' terminals. The input board requires 300mA at 12VDC to operate. If powered by an external supply the link LK17 (green on the above diagram) should be UP; if powered through the ribbon cable the link LK17 should be DOWN.

If powered by an external supply all the 0V lines of the power supplies for the controllers and input boards should be tied together to give a common 0V reference.

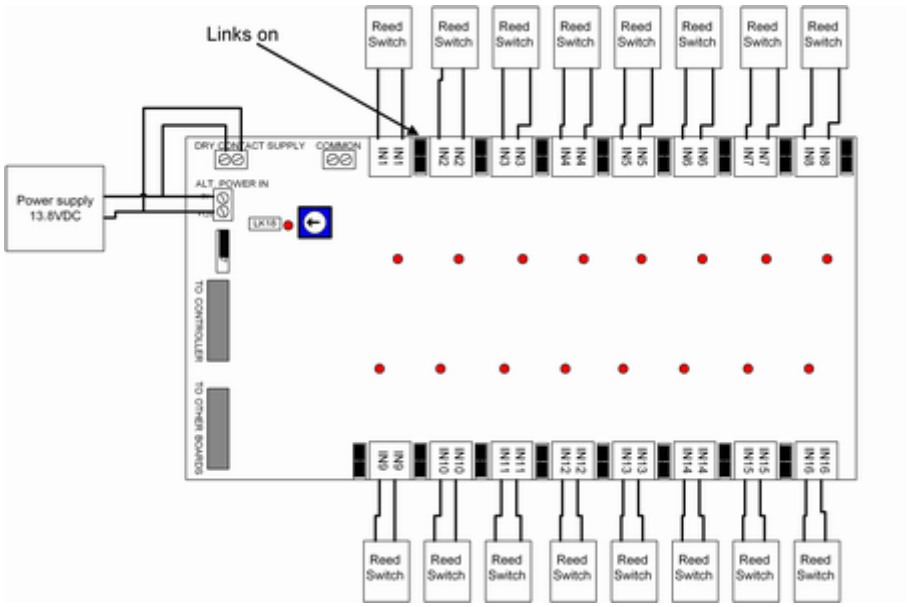
If powered by the ribbon cable a maximum of three input expansion boards can be connected (due to current requirements and voltage drop).

Input modes

The input board can operate in three modes, depending on the requirements. Regardless of the mode, whenever the input is abnormal the associated LED will be on. This provides convenient visual feedback of the input state.

- **Dry contact mode**

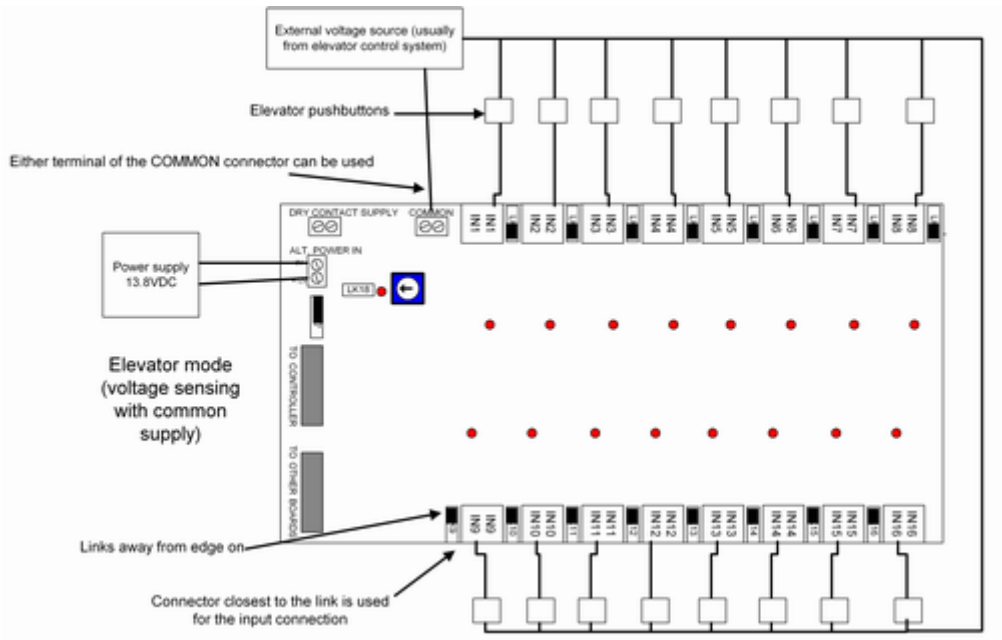
  In this mode voltage-free contacts (like reed switches or movement detectors) can be connected to each input. This requires a voltage to be provded to the 'dry contact supply' terminals. Most commonly this is looped around from the 'Alt Power In' terminals if the board is externally powered.
  In this mode the two links adjacent to each input must both be ON.
  The 'dry contact supply' can be any voltage 5-50VAC or DC. It is not polarity-sensitive.



- **Elevator mode (voltage sensing with common supply)**

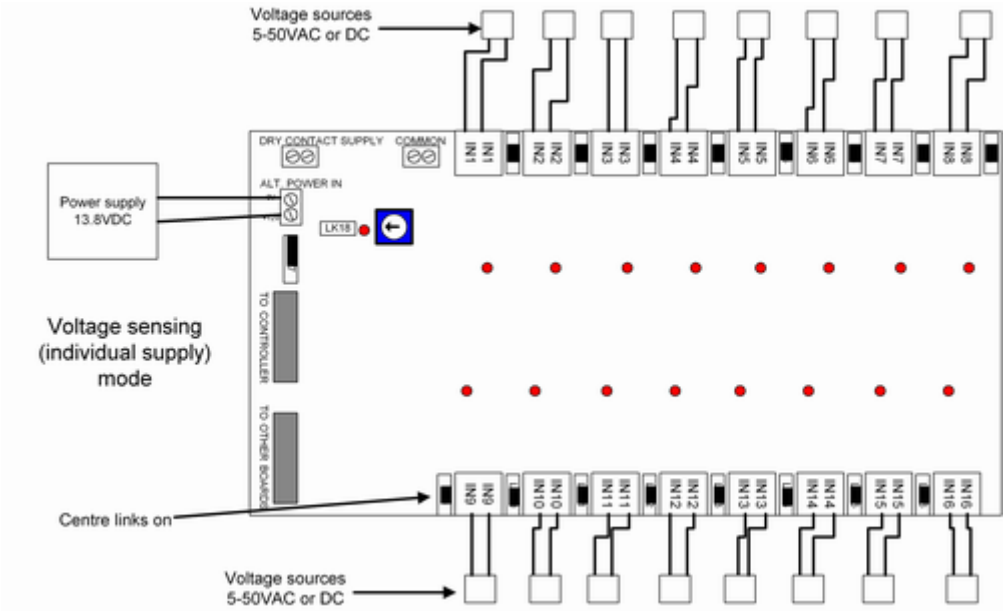
In this mode a common voltage can be sensed on all the inputs. The reference of the common voltage is connected to the COMMON terminals and the voltages to be sensed are connected to the input closest to the links. This is referred to as 'elevator mode' because this is typically how floor destination can be sensed from elevator control wiring.

In this mode the link furthest away from the edge of the PC must be on for each input as in the diagram below. The voltage to be sensed is terminated on the connector closest to the link for each input. There are two 'COMMON' terminals - either of them can be used for this mode.

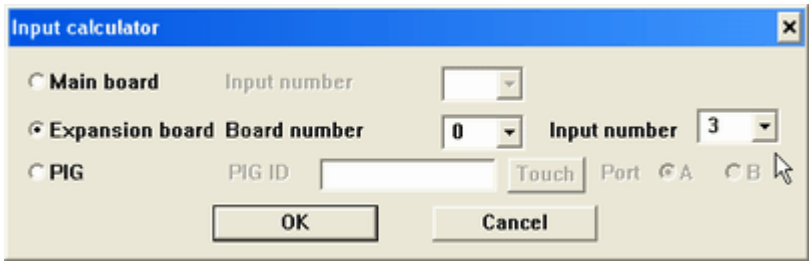


- **Voltage sensing (individual supply) mode**

In this mode each input can sense a voltage, and the voltages do not need to have a common. The middle two links for each input are connected, and the voltage is simply applied across the inputs.



Using 16-way input boards
16-way input boards are used as alarm inputs and with elevator systems for floor destination reporting and intercom inputs. Wherever an input can be used in the system a 'calculate' button will appear. Clicking this button brings up the 'input calculator'. If the input is on an input board click the 'expansion board' radio button, select the board number and input number. This will calculate the input number which corresponds to that input.



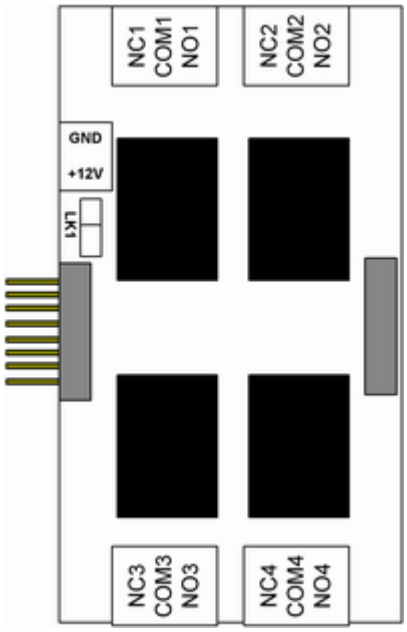
Point Identification Gadgets (PIGs)
PIG boosters
PIG-2
PIG-3
PIGPEN
4-way relay board
16-way relay board

Expansion overview

9.8 4-way relay board

The 4-way relay board provides a simple way to expand the number of outputs by just a few outputs. Up to three 4-way relay boards may be added to make a total of up to 16 relays. Note that each expansion relay board 'uses up' inputs and outputs on the board so generally only a single reader is fitted to controllers with 4-way relay boards being used. Also it is not possible to mix 4-way relay boards with 16-way relay or expansion boards.

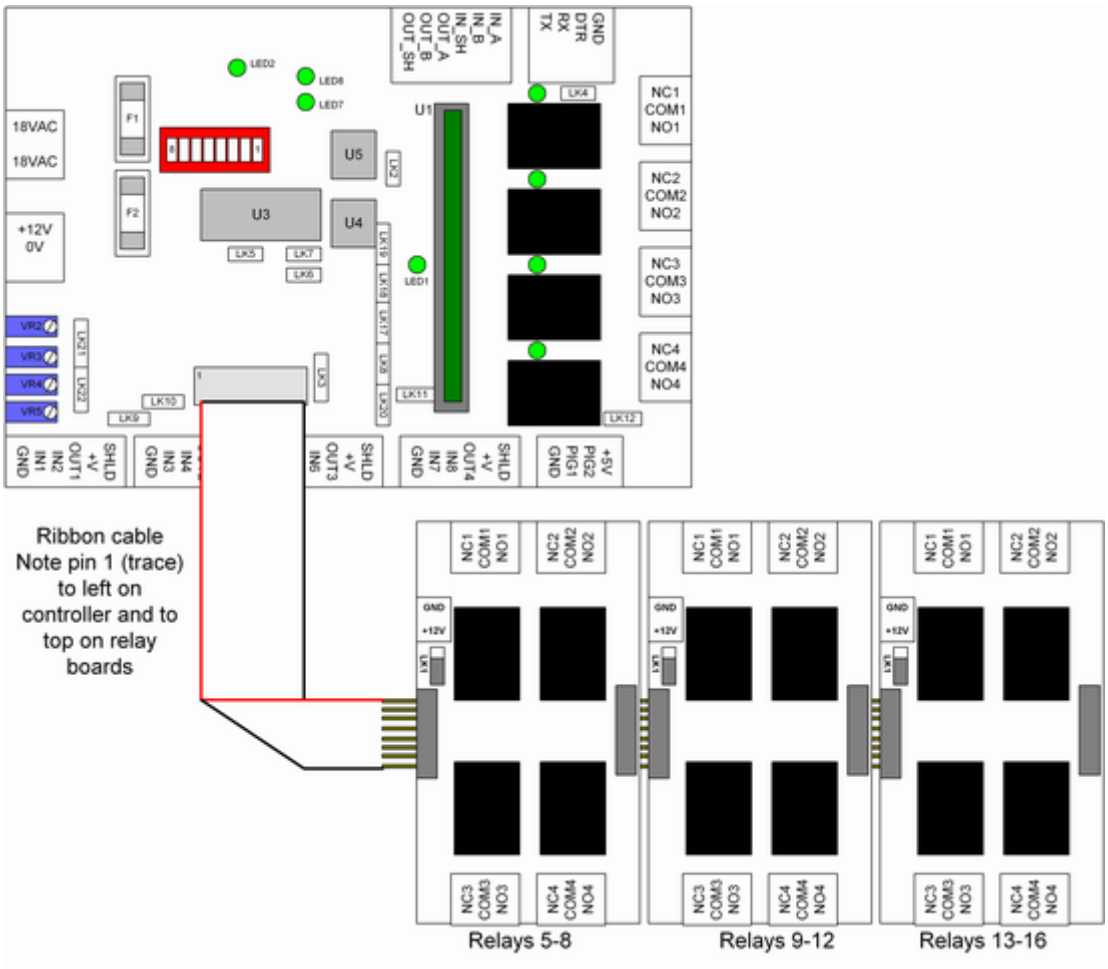
The 4-way relay board connects to the expansion port of the controller via a ribbon cable. Additional 4-way relay boards connect to the first one via the 16-way header on the edge of the board. A diagram of the 4-way relay board is below.



The board has four 'form-c' relay contacts, a connector on the left hand side for the ribbon cable (or to plug into the previous 4-way board), a connector for power and a link.

Power to the board can be provided either by the ribbon cable or from an external supply. If the power is supplied by the ribbon cable LK1 should be DOWN. If the power is supplied from the external GND/+12V connector then LK1 should be UP. If powered externally the 0V lines of the supply should be connected to the power supply for the controller to ensure a common 0V reference.

The first expansion board (relays 5-8) connects to the controller via a ribbon cable. The ribbon cable will have one wire which has a trace on it. This trace indicates pin 1 which is to the LEFT on the controller and to the TOP on the relay board. Additional relay boards simply plug into the first board to make a maximum of 12 expansion relays or 16 relays in all including the on-board relays.



Inputs occupied
4-way expansion relay boards 'use up' inputs and outputs on the boards as follows:

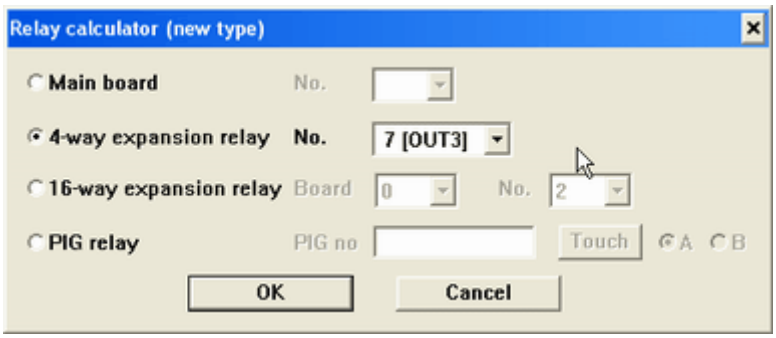
4-way expansion board	Relays added	Inputs used up
4-way expansion board 1	Relays 5-8	Uses up inputs IN3, OUT2, OUT3 and OUT4
4-way expansion board 2	Relays 9-12	Uses up inputs IN5, IN6, IN7 and IN8
4-way expansion board 3	Relays 13-16	Uses up inputs IN4, PIG1 and PIG2

Controller links
For the first expansion board fitted (relays 5-8), LK19 must be off.
For the second expansion board fitted (relays 9-12), LK17 and LK8 must be off.
For the third expansion board fitted(relays 13-16), LK18 must be off and LK3 must be UP.

More information about the controller links can be found in the controller links topic.

Power supply
Each 4-way expansion board requires about 300mA of power supply. 4-way relay expansion boards cannot be used if the controller is powered by AC as the regulator on the controller is unable to supply sufficient current.

Using 4-way relay boards
4-way relay boards are used as relay outputs for doors and with elevator systems for floor control. Wherever a relay can be used in the system a 'calculate' button will appear. Clicking this button brings up the 'relay calculator'. If the relay is on a 4-way relay board click the '4-way expansion relay' radio button, and select the relay from the drop-down list. This will calculate the relay number which corresponds to that relay.



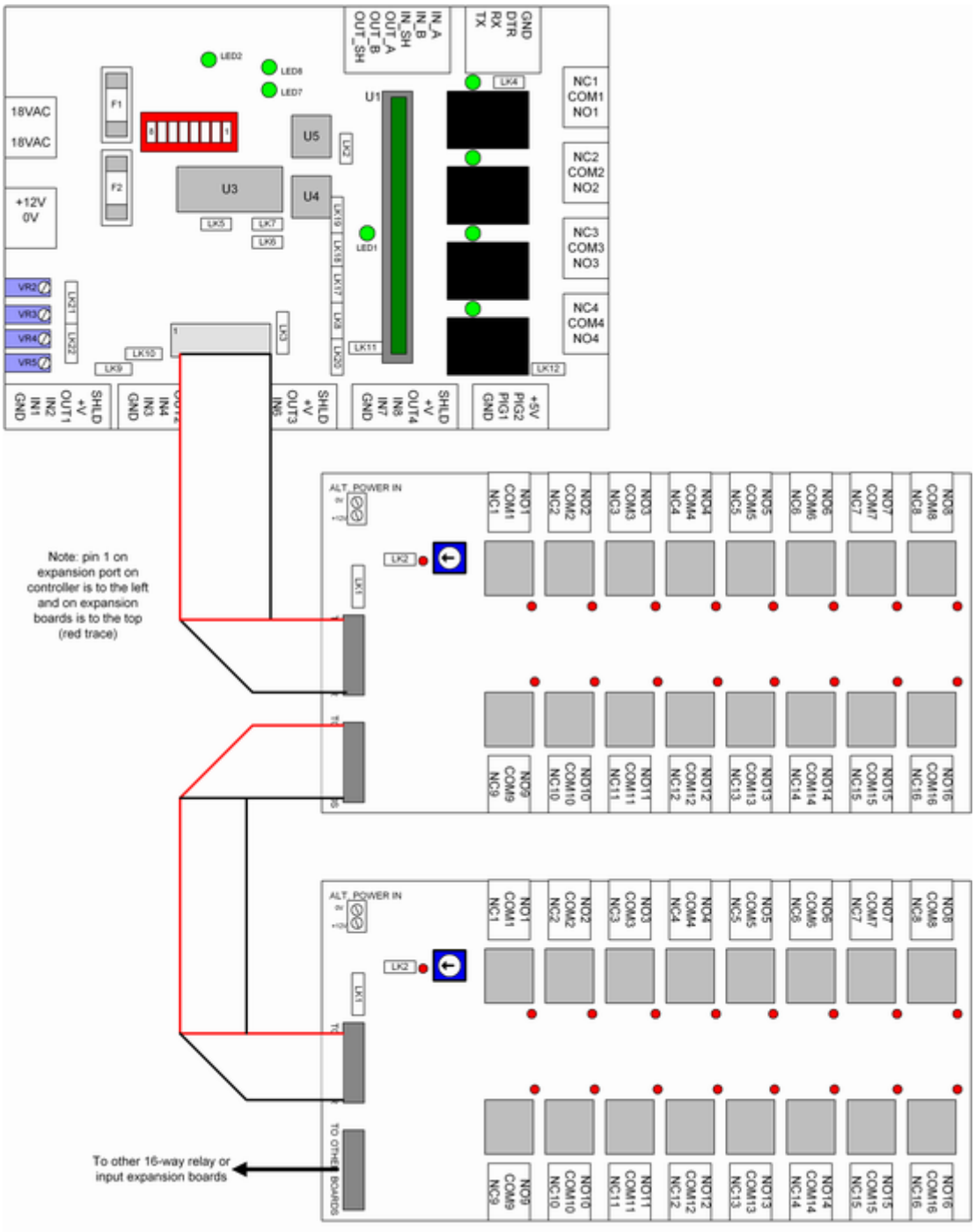
Point Identification Gadgets (PIGs)
PIG boosters
PIG-2
PIG-3
PIGPEN
16-way input board
16-way relay board

Expansion overview

9.9 16-way relay board

The 16-way relay board allows expansion of the relays on the controller in groups of 16. Each relay board has an address and a maximum of 15 additional 16-way relay boards can be added to the system to give up to 250 relays on the system.

Connecting the 16-way relay board
The 16-way relay boards connect to the expansion port on the controller via a ribbon cable. Additional 16-way input or output expansion boards are added by connecting another ribbon cable from the output of the board to the input of the next one and so on, as depicted below. The ribbon cable must be connected so that pin 1 on the expansion port (on the left) connects to pin 1 on the expansion board (at the top) and so on.



Each relay board must have its address selected on the 16-way rotary switch. Usually the first board is numbered as 0, the second board is numbered as 1 and so on. Relay boards must all have a unique address; however relay boards can be numbered the same as input boards.

Note that the above configuration shows two relay boards powered through the ribbon cable; in fact this is not recommended as each relay board requires 1A so powering through the ribbon cable is only recommended for a single relay board. Generally relay boards are externally powered.

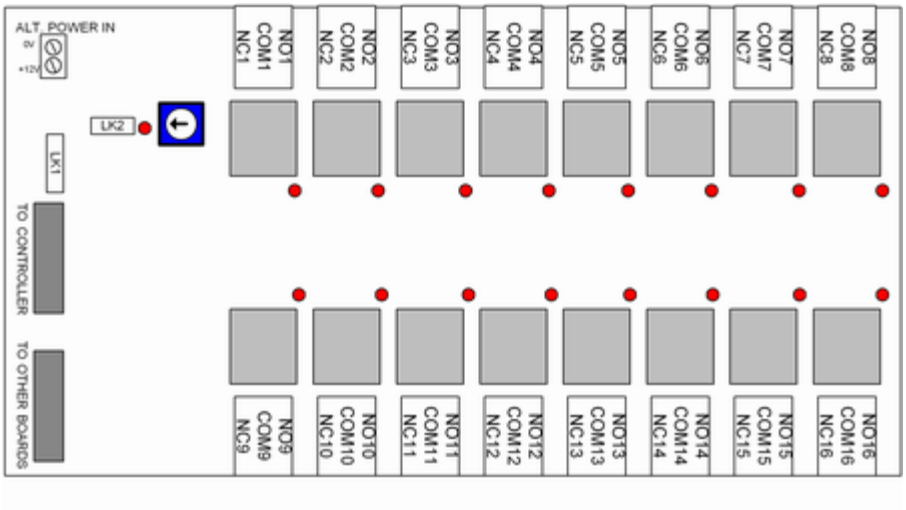
Controller configuration

Having relay expansion boards fitted to the controller 'uses up' all the inputs on the controller except those for reader 1 (IN1, IN2 and OUT1). If 16-way relay boards are fitted the on-board inputs are not available.

The controller must be configured with LK3 UP and LK19, LK18, LK17 and LK8 off.

Configuring the relay board

A diagram of the relay board is shown below.



The relay board has 16 voltage-free form-C relay outputs rated at 2A 24VDC. It also has for the inputs, links to configure the way the inputs work and connectors for power. The rotary switch is used to set the address of the input board (0-F = 0-15). The links on the board are as follows:

- LK1 - used to set the power supply input. LK1 is UP if the power is provided via the ALT POWER IN terminals (JP19). The power needs to be 12VDC. LK1 is DOWN if the power is provided via the ribbon cable. A maximum of one relay board can be powered via the ribbon cable.
- LK2 - this link is used for production testing of the board and is OFF in normal operation. If the link is ON and the ribbon cables are disconnected, with external power supplied, then the relay corresponding to the current position of the rotary switch will be ON.

Relay board power

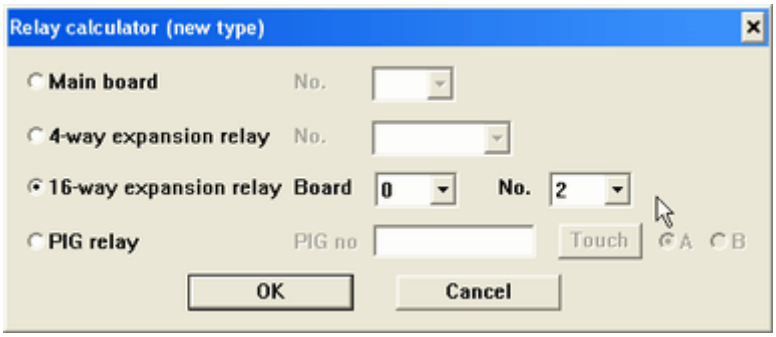
The relay board can be powered either through the ribbon cable or from an external supply via the 'Alt Power In' terminals. The relay board requires 1A at 12VDC to operate. If powered by an external supply the link LK1 should be UP; if powered through the ribbon cable the link LK171should be DOWN.

If powered by an external supply all the 0V lines of the power supplies for the controllers and input boards should be tied together to give a common 0V reference.

If powered by the ribbon cable only one relay board can be connected (due to current requirements and voltage drop).

Using 16-way relay boards

16-way relay boards are used as relay outputs for doors and with elevator systems for floor control. Wherever a relay can be used in the system a 'calculate' button will appear. Clicking this button brings up the 'relay calculator'. If the relay is on a 16-way relay board click the 'expansion board' radio button, select the board number and input number. This will calculate the relay number which corresponds to that relay.



10 Glossary

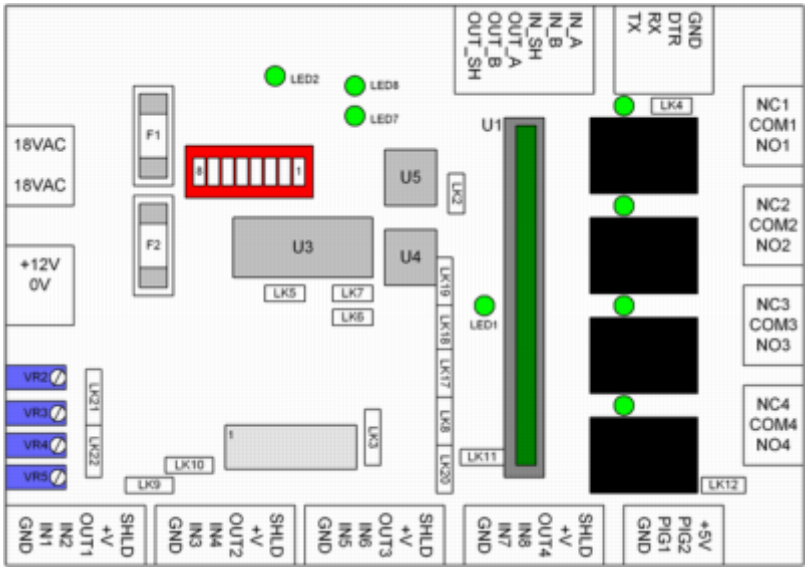
10.1 Glossary

The glossary contains definitions of commonly used terms in this manual.

Controller
Firmware
Reader
Credential
I/O
PIG

10.2 Controller

The controller is the 'intelligent' black box which is the heart of the CS system. The controller can operate up to 4 doors, or an elevator or a series of alarm areas.



Glossary

10.3 Firmware

Firmware is the electronic 'program' which is loaded into the controller. By changing the firmware it is possible to change the functionality of the controller.
There are two 'standard' types of firmware.

Door firmware - has capacity for up to four readers as well as alarm areas. This firmware is used for all applications except for elevators.

Elevator firmware - has capacity for a single reader which can trigger up to 250 outputs. This firmware is used for control of elevators.

Glossary

10.4 Reader

A reader is connected to the controller. It reads 'credentials' to identify a user to the system. Examples of readers include keypads, mag-stripe readers, silkey readers, fingerprint readers, proximity readers etc.

Glossary

10.5 Credential

The credential is what identifies a user to the system. It is read by the reader. Examples of credentials include silkeys, cards, PIN numbers, fingerprints etc.

Glossary

10.6 I/O

Refers to Input or Output. On the controller there are 8 digital inputs IN1-IN8,
four digital outputs OUT1-OUT4
two PIG bus drivers PIG1-PIG2

All these collectively are referred to as the controller Input/Output or I/O.

Glossary

10.7 PIG

A PIG is a Point Identification Gadget. Each PIG has a unique ID which is used to identify it on the PIG bus. PIGs can be used to expand the inputs and outputs of the controller in a very cost-effective and flexible manner.

Glossary

Index

- A -

- C -

- D -

- E -

- F -

- H -

- I -

- L -

- M -

- O -

- P -

- R -

- S -