Application note:

Firmware Functionality

- **The powerful CS access control system offers different features in different controllers through variations in firmware. This document describes those differences.**

Introduction

CS Technologies access control systems are built around powerful and versatile controllers. Each controller has a firmware chip which determines its capability – what type of readers it works with, whether it controls doors, elevators or alarms and other features. This document describes the different types of features offered by each type of controller.

There are several items of hardware which go to make up a networked CS Technologies access control system. These include:

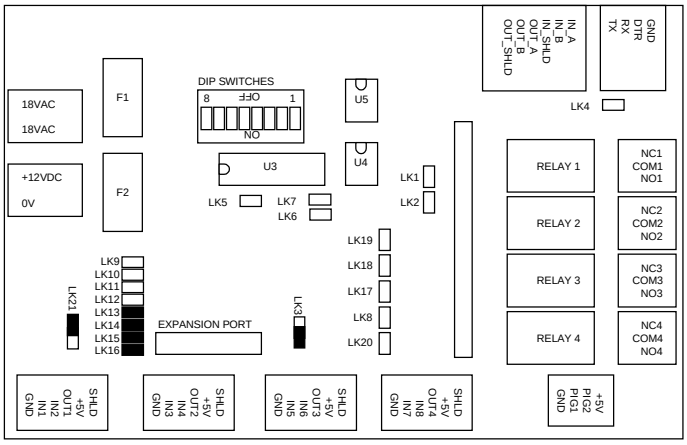
- the controller
- 4-way relay expansion boards
- 16-way relay expansion boards
- 16-way input expansion boards
- 2-input expansion boards (2-port PIGs)
- 1 input 1 output expansion boards (PIG-OUTs)
- 24 input PIG boards
- 48 input PIG boards
- miscellaneous other support devices including RS232-485 converters, PIG boosters etc

The expansion capabilities and reader capacity of each controller is determined by its firmware. As more features are added the user and history capacity of the controller changes. This document should help a designer to work out what firmware to use where to achieve the desired operation of the system.

This document refers to R2 door, R2 alarm, R2 elevator and R3 firmware revisions.

Controller description

The CS controller is a microprocessor-controlled electronic device. It has 14 bidirectional digital I/O points and four on-board relays. The I/O points are arranged in four groups (for four readers) and a fifth port for connection of expansion PIGs.



The I/O points are named IN1-IN8, OUT1-OUT4 and PIG1-PIG2. There is an expansion port for connection of 4-way and 16-way expansion boards. When this expansion port is used it takes the place of IN3-8 and OUT2-4.

Reader types

All different revisions of firmware are available in variations to support different types of reader interfaces. Currently supported readers are:

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.

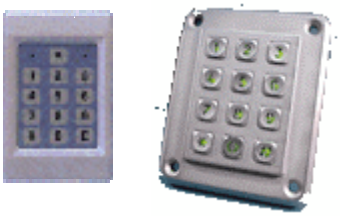
Wiegand

Wiegand firmware 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.

Mag-stripe

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



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 3-8 digits and the keypads are available as low-cost or vandalproof versions.

Smartcard

The smartcard firmware works with Infineer and Proton contact smartcards. Other types of contact smartcards are being interfaced and we are able to configure the system to read just about any smartcard. The system also works with contactless smartcards including Mifare and Legic.

Radio

Radio firmware supports standard radio transmitters and receivers. This allows carparks or garages to use access control with complete control of user identity. Each transmitter has its own ID and thus users can be individually granted or denied access with a full audit trail available.

Firmware general features

Features supported by all R2 and R3 firmware includes extended public holiday programming (up to 20 holiday periods starting and ending at a particular time and date) and timezones which work in 'reverse' as well as 'forward' (e.g. a timezone starting at 23:00 and ending at 06:00 will work properly).

Door firmware (R2)

Door firmware is the classic application of the controller. With R2 door firmware the controller supports up to four readers with associated door strike (relay) output, exit request and door status input. Inputs can be expanded using 2-port PIGs (inputs only). Outputs cannot be expanded beyond the four on-board relays. 4-way and 16-way relay and input expansion boards are not supported.

Readers

Up to four readers are supported. All the readers have to be the same interface type i.e. you cannot mix Silicon Key and Wiegand readers on the same controller. You may however mix them in a system; they just have to be on different controllers. Readers connect to the four reader connectors on the controller. Some readers use more inputs than others as follows:

Silicon Key – each reader uses one input and one output
Presco, Radio – each reader uses one input
Wiegand, Magstripe, Smartcard – each reader uses two inputs and one output

Door status inputs

Each door in the system can have a door status input defined. If defined, this input is measured to detect forced entry and door open too long. The door status input can be any unused input on the system or can be connected to a 2-port PIG expander.

Exit request inputs

Each door in the system can have an exit request input defined. If defined, this input is used to trigger the door or mask the alarm on exit. The exit request input can be any unused input on the system or can be connected to a 2-port PIG expander.

Note that where only 3 readers are connected to a system with mag-stripe, wiegand, presco or radio readers the inputs on the fourth reader port cannot be used for exit request or door status inputs; instead PIGs should be used to expand in these situations. This only applies where 3 readers are used with these reader technologies.

Relays

R2 door firmware does not allow expansion of the relays on the controller beyond the four on-board relays. It does allow definition of the alarm relay for each door but this can only be to one of the four on-board relays. The alarm relay for door open too long can be separately defined to the alarm relay for forced entry for each door.

Firmware features

Features supported in door firmware include:

- antipassback
- antipassback override for individual access levels
- parking/occupancy control
- mantrap/reader arming
- around 1700-2000 users

Summary

R2 door firmware supports up to four doors.
Each door can have an exit request and door open too long input which are programmable.
Unused inputs on the board can be used for the exit request and door open too long inputs (except if only 3 readers with wiegand, magstripe, presco or radio when the 4th reader ports can't be used).
PIG-inputs can also be used for the exit request and door open too long inputs.
Only the four on-board relays are supported. They can be used for door strikes or if unused for door open too long and forced entry alarms.
Depending on firmware up to 2000 users are supported with a standard chip.
Door firmware incorporates antipassback, parking control and reader arming inputs.

Example use of door firmware

1. 4 door silicon key system – each door with exit request and door monitoring

Each silicon key reader uses up one input and one output. The readers would be connected to IN1, IN3, IN5 and IN7 with the corresponding OUT1-OUT4 being used for the reader LEDs. Thus there would be unused inputs IN2, IN4, IN6, IN8 and also PIG1 and PIG2.

However we need 8 inputs in total – four for the exit requests and four for the door status inputs. So we don't have enough spare inputs on the board and so we would add two 2-port pigs to the pig port. This will give us four on-board inputs IN2, 4, 6, 8 for the exit requests (say), and four inputs on the PIGs for the door status.

All four of the relays on board would be used up for door strikes, so any alarms would have to report only to the screen of the PC. Using Advent software these could in turn be used to trigger relays on other controllers, send emails etc. Using PC3 software they would only be recorded on the screen of the PC.

2. 4 door wiegand system – two doors require exit request buttons

Each wiegand reader uses up two inputs and one output. The readers would be connected to IN1/2, IN3/4, IN5/6 and IN7/8 with the reader LEDs being connected to OUT1-4. So the only unused inputs are PIG1 and PIG2.

In this scenario we can simply connect our exit request buttons directly to PIG1 and PIG2. This makes these unavailable for the connection of PIGs but in this case we don't need them.

3. 3 door magstripe system with exit request and door monitoring on all doors and a single alarm relay

Each magstripe reader uses up two inputs and one output. The readers would be connected to IN1/2, IN3/4, IN5/6 and their LEDs controlled by OUT1-3. We have unused inputs IN7, IN8, OUT4, PIG1 and PIG2. However because it's a 3-door magstripe system we can't use IN7/8 either – the third reader means the inputs for the fourth reader can't be used for inputs.

So we need 6 inputs in total (3 exit request and 3 door monitoring) and have OUT4, PIG1 and PIG2 available. We need to expand using PIGs which will use up PIG1 (and PIG2 if we use a pig booster). We'd probably put in 3 2-port pigs for the inputs.

The fourth relay on the controller in this scenario could be set up as the alarm relay for either door open too long or forced entry or both.

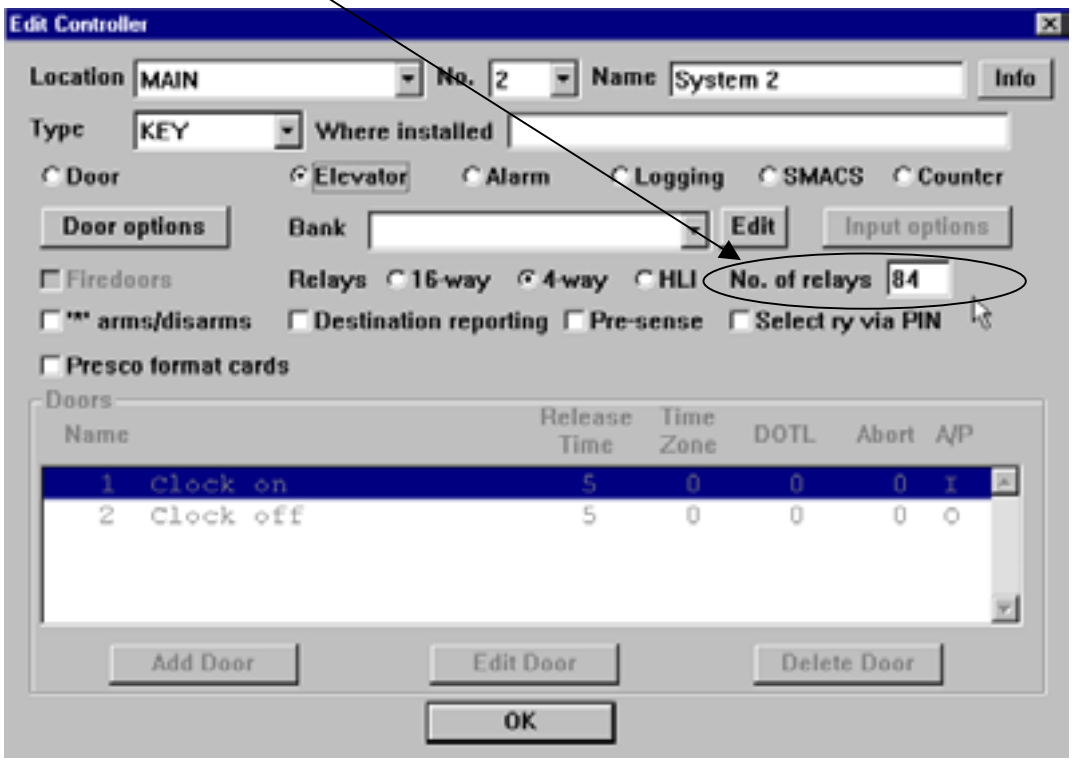
Elevator firmware

Elevator firmware allows a reader to trigger a combination of output relays which are usually used to grant access to particular floors in an elevator. The elevator firmware supports a single reader plus expansion boards – up to 5 16-way relay expansion boards and up to 10 16-way input expansion boards. Thus each elevator requires a reader, controller plus the appropriate expansion boards. This results in a highly reliable system because the elevators are all separately controlled.

This gives a total of 84 relays and 160 inputs which can be used. The relays control outputs which interface to the elevator call buttons; the inputs are used for sensing floor destination and also for allowing interfacing of intercom buttons to trigger individual floors.

It is also possible to interface 4-way relay expansion boards to the elevator controller. Up to 3 of these can be added to give a total of 16 relays. However 4-way relay boards do not work in conjunction with input expansion boards.

Using expansion boards 'uses up' IN3, IN4, IN5, IN6, IN7, IN8, PIG1, PIG2, OUT2, OUT3 and OUT4 so only one reader can be used on an elevator controller. However it is possible to set in the software how many relays are actually attached to the controller.



Thus if only 4 relays are required, no expansion boards are necessary and the inputs become available for use as floor destination and intercom inputs. Expansion boards are numbered starting at 0 so if you are setting up a system with 20 relays (one expansion board) you would state in the controller setup that there are 20 relays and set the relay expansion board number to 0. If for some reason you wanted to start numbering the expansion boards at 1 say then the controller still thinks that board 0 is available and counts it in the number of relays. So you have to tell the system you have 36 relays even though only 20 are actually in existence, because the space taken up by the first relay expansion board is still occupied within the firmware.

A summary of the relay numbering is below.

Main controller – relays 1-4
Expansion board 0 – relays 5-20
Expansion board 1 – relays 21-36
Expansion board 2 – relays 37-52
Expansion board 3 – relays 53-68
Expansion board 4 – relays 69-84

With 4-way relay expansion boards again unused inputs become available for call destination and intercom inputs. The table below lists the available inputs which can be used depending on the configuration of the system.

Expansion boards fitted	Unused inputs available for intercom/call destination (X = available)										
	IN3	IN4	IN5	IN6	IN7	IN8	OUT2	OUT3	OUT4	PIG1	PIG2
No expansion boards	X	X	X	X	X	X	X	X	X	X	X
16-way input or 16-way output expansion boards											
1 x 4-way expansion board (relays 5-8)		X	X	X	X	X				X	X
2 x 4-way expansion boards (relays 5-12)		X								X	X
3 x 4-way expansion boards (relays 5-16)											

Note that IN1, IN2 and OUT1 are used for the reader on the elevator controller.

Note also that where PIG1 and PIG2 are available they can also be used for connection of PIGs as inputs.

Example use of elevator firmware

1. 20 storey building, no call destination reporting, 2 floors require intercom access

In this scenario each elevator would require a controller with a 16-way relay output board (to give 20 relays total for the controlled floors). Using 16-way expansion boards uses up all the on-board inputs so you would also require a 16-way input expansion board to provide the intercom inputs for the two floors that require them.

2. 8 storey building with call destination reporting

There are a couple of ways to do this. Firstly you could set it up so that each controller has a 16-way relay output board (to give a total of 20 outputs of which we're only going to use 8) and a 16-way input board (of which we use 7 inputs to sense the call destination from the elevator).
The other way would be to have a controller with a single 4-way relay expansion board giving a total of 8 relays. Looking at the table above this leaves 7 spare inputs on the controller board itself. But we need more than this so noting that PIG1 is free we can connect a PIG to it to give two extra inputs (but losing the PIG1 as a separate input) meaning that we can implement call destination reporting for the eight floors using six on-board inputs plus two on a 2-port PIG.

3. 4 storey building with call destination reporting and intercoms for each floor

This can be done without any expansion boards at all. The table above shows that without any expansion boards (number of floors set to 4) there are 11 spare inputs – more than enough for 4 for call destination and 4 for intercom inputs.

4. 80 storey building with call destination reporting and intercoms for each floor

This will require a controller with 5 relay expansion boards (a total of 84 relay outputs) and 10 input expansion boards (a total of 160 inputs) to give two inputs per floor, one for call destination and the other for intercom.

Alarm firmware (R2)

R2 alarm firmware allows the definition of inputs and alarm areas in combination with readers. There are several variations of the firmware to provide different functionality. With R2 alarm firmware expansion relays and input boards are supported, as are PIGs for alarm inputs. But PIG-OUTs (expansion PIG relays) are not supported. With the added capabilities of alarm areas this reduces the user capacity also to about 350 users with a standard chip.

Alarm firmware with readers

Where readers are required to interface with alarms the R2 alarm firmware provides a powerful way to integrate access control with alarms. Each controller supports up to 4 readers, 32 inputs, 8 areas and 20 relays. The limitation is that the PIG relays are not supported so if you use expansion relays you then lose the use of the corresponding inputs on the controller similar to an elevator controller.

Alarm firmware with readers allows a user to arm and disarm the alarm from the reader. It also supports buzzer relays, auto-rearm, arming pushbuttons, disarmed relays, pulse relays, armed relays, 3 alarm relays, follow relays for each input and all inputs can have individual entry and exit delays programmed.

Up to 4 readers are supported but when 16-way expansion relay or input boards are used the system loses the use of IN3-8, OUT2-4 and PIG1-2 meaning only a single reader is supported.

The doors controlled by the system can have exit request and door status inputs similar to door firmware, and can also have defined door open too long/forced entry alarm relays. However the alarm firmware does not support antipassback or parking control features.

Alarm firmware also provides additional capabilities with regards to access levels. Users can be programmed so that they only have access to particular areas when they are already disarmed; alternatively they can be given authority to disarm (and arm) particular areas, or to access certain doors when associated areas are armed. This provides a great deal of power and flexibility in configuration of the system and minimizes false alarms because whenever an authorized person attempts to gain access the alarm is automatically disarmed; when someone who is not authorized to disarm attempts to gain access they will be denied until the alarm is disarmed.

Some examples are as follows:

1. 2 door system providing access to 2 separate alarm areas with 8 inputs

With this scenario the two readers are connected as normal, operating relays 1 and 2 to operate door strikes. This leaves 6 on-board inputs free (IN5, 6, 7, 8, OUT1, 2) plus connection for PIGs on PIG1/2 (with a pig booster). So a single 2-port PIG can be added to give 8 inputs (non-monitored). Alarms can be transmitted via relay 3 or 4 one of which might be configured as a sounder and the other as a dialer relay.

2. 16 input system with an arming/disarming reader, individual point reporting

To do this a single reader is connected plus a 16-way input board and a 16-way output board. The alarm points are connected to the input board and each point is defined as having a ‘follow relay’ so that when that point is in alarm the corresponding relay on the relay expansion board operates. Because there are expansion boards being used only 1 reader is supported; this reader can be used to arm and disarm the area. Four of the relays are still available (because we have 20 total) for use as buzzer (pre-arm warning), siren, strobe, disarmed, armed, pulse relay so can be used to arm and disarm an alarm panel also.

Alarm firmware without readers

Often used for self storage systems, alarm firmware without readers provides 254 inputs in 254 areas and up to 84 relays. Again PIG-relays are not supported by this firmware – only 16-way expansion boards. Any port on the controller can be used for connection of PIG buses (each bus will support up to 25 pig-2’s or 50 inputs) and the use of PIG-boosters is always recommended. Input expansion boards and relay expansion boards are supported but when these are used, PIGs cannot be connected to the ports which have been used up by the expansion boards (IN3-8, OUT2-4, PIG1-2).

Some examples:

1. 200 inputs in 200 areas with inputs via PIGs

This is a typical self storage scenario. To do this 100 2-port PIGs would be connected in groups of 25. These might be 2-port pigs or 48-input (24-PIG) pig-pens. On the controller 4 pig-buses would be configured each with a pig booster. Each bus would have up to 50 inputs connected either as 2-port PIGs or pigpens. Each input would belong

to its own area. Areas are armed and disarmed via the PC when users enter and exit the premises via a different (door) controller.

2. 72 units each with its own local alarm relay

To do this we would need relay expansion boards; it would make sense to use input expansion boards too. So the controller would be equipped with 5 16-way relay expansion boards and 5 16-way input expansion boards. Each input would be in its own area; the alarm relays for each area would be individually defined as the relays on the expansion boards. You would also be able to put some PIGs on the IN1/2 bus if more inputs were required (this is available because there are no readers supported).

Fire door firmware

Fire door firmware is another variation of this type of system. As the name implies it is usually used for control of fire doors. It supports up to 84 relays and 160 inputs. Each fire door defined can have

- a relay output to control a door strike
- an exit request input to trigger the door strike
- a door status input to sense when the door is in alarm or open too long
- a relay output to indicate an alarm

Fire door firmware does not support any readers, and being R2 also does not support PIG relays. It usually is used with expansion relay boards and expansion input boards.

R3 firmware

The limitation inherent in R2 firmware of only supporting the on-board and expansion relays has been obviated in R3 firmware which supports the use of PIG relays. This is a major change in the firmware and associated configuration screens in the PC3 and Advent software. R3 firmware is ideal for alarm systems with integrated access control readers as it allows definition of additional relays to perform functions like buzzer, disarmed and alarm relays and also thus provides indication of a wide range of input conditions via the extra relays. With R2 relays the on-board relay restriction meant that many alarm conditions had to be mapped to a single relay if any sort of external reporting is required; with R3 this is no longer the case. However because more space is taken up by the program the capacity is reduced.

Currently R3 firmware supports 4 readers, 4 areas, 16 inputs, 20 relays and 400 users with Silicon Key, Wiegand or Presco format readers. It does not support antipassback or parking control. Inputs can be via PIGs or input expansion boards. Outputs can be via PIG-relays or output expansion boards. As with the other firmwares, if input or output expansion boards are used then the corresponding on-board inputs (IN3-8, OUT2-4, PIG1/2) are not available for readers or connection of PIGs.

R3 firmware offers full programmability of relay outputs for all sorts of functions. For example when a reader grants access you can program it to trigger a particular relay so all 4 readers could trigger the same relay if necessary. Exit request buttons can trigger the same or different relays. It is also possible to program an ‘access denied’ relay which triggers when someone is denied access.

As with door and R2 alarm firmware, each door on the system can have fully configured inputs for exit request and door monitoring; R3 also allows any relay in the system to indicate door open too long and forced entry.

Some examples:

1. **4 doors for 2 separate alarm areas each with an arming buzzer and 3 inputs each with individual sector identification on the dialer**

The controller in this scenario will have four readers. Each reader will trigger its associated relay output for a door strike and also allow arming/disarming of the alarm area. Inputs required are 6 for the alarm, plus 2 for possible arming stations (pushbuttons which arm the alarm area). Outputs required are an additional 6 for input status plus another two to indicate open/close on the alarm system plus two for buzzers. Also possibly two for local screamers. So we would use a PIG-booster plus 12 PIG-RELAYS (each of which has an input and an output). This provides the inputs and relays required for the system.

2. **4 doors with exit request and door status and a local screamer at each door to indicate forced entry/door open too long**

Here the controller has 4 readers. Assuming mag-stripe or wiegand this uses up the reader inputs so we expand using PIGs. We need 8 more inputs (4 for exit request and 4 for door status) and 4 more outputs (for the local screamer at each door). So we install 4 pig-relays and 2 pig-2’s giving 8 inputs and 4 relays in addition. Again for reliability we would install a pig-booster here.

Summary

The table below summarises the basic differences between the different types of firmware

Firmware type	Readers	Users	Antipassback/ parking	Pig-relays	Inputs	Areas	Relays
DOOR	4	2000	YES	NO	-	-	4
ELEVATOR	1	1400-1500	-	-	-	-	84
R2 ALARM + READER	4	350	NO	NO	32	8	20
R2 ALARM	0	-	-	NO	254	254	84
R3	4	400	NO	YES	16	4	20

\\BRUCE\BRUCE D\My Documents\CS Technologies\Brochures\Technical notes\Tech note re firmware capabilities.doc