Karizma™

INTRODUCTION

Karizma is a micro processor based intruder alarm control system designed to comply with the installation requirements of BS 4737 1986/87. The Central Processing Unit (CPU) is housed in a plain metal box that may be sited anywhere in the protected area of the installation. Control and operation of the system is by remote keypads that have a four digit 7-segment LED display. Engineer programming of the system is performed using any of the remote keypads.

Before beginning any programming or installation work please read through these instructions. the user guide and the iD Engineering Information - checking that you fully understand every feature of the system and its operation.

Karizma features include;

- Identification and control of up to 30 iD points on a single 2 or 4 core cable
- Each iD point offers a choice of 9 detection types with 6 attributes
- Fully programmable part set routines (A,B and C)
- Up to 7 user codes, programmable 2-6 digits
- Compatible with standard plug-on communicators and Red Care STU
- Choice of up to 4 remote keypads each with 4 X 7 segment displays and back lit keys
- Full NVM protection with unique copy facility duplicates the system set up
- Keyswitch operation for setting and unsetting
- Remote reset features include Central Station reset code and STU Tell Back facility

Preliminary

Engineering Information

INSTALLATION

INSTALLATION DESIGN

Plan out the various areas and degrees of protection with regard to the point types, attributes, programs, entry/exit routes and keypad positions. The CPU may be sited anywhere within the protected premises but it should be convenient for a mains supply and access for future maintenance and service.

WIRING POWER UP

Site the CPU and wire in to it the remote keypad and at least one extension speaker.

1. Apply mains (or battery) power.

2. From initial power up Karizma will be in an alarm condition. Silence the alarm by entering the user code (the default is 0123 followed by [ENTER]). The display will now show the reason for the alarm, 'init' or system initialisation.

3. Reset the system using the engineer code (the default is 9999 followed by [ENTER]). Since there is at least one fault (lid tamper) Karizma will enter a fault lockout mode and display the number of faults.

4. Press [ENTER] at this stage to enter engineering mode. This is identified by the 'Eng' prompt.

5. You should now continue to wire the system, testing each section as complete including each detector and the operation of each of the iD biscuits (menu 1 section 3).

6. When complete, close all covers to defeat the tampers and press [ERROR]. If there are no faults present the system will return to Day mode.

   If any faults are present the system will remain in Engineering, and display the quantity of faults. Pressing any key will allow the faults to be displayed.

   When all faults have been cleared, return to Day mode by pressing [ERROR].

MAINS CONNECTION

The mains supply should be carefully wired using a 3 core cable of not less than 0.75 mm^2, from an unswitched fused spur outlet to the mains connector block in the base of the Control Panel. Use a 2A fuse in the spur.

Mains installation must be carried out in accordance with the current IEE wiring regulations by a competent person. If in doubt consult a qualified electrician.

FINAL COMMISSIONING

When the installation is complete the system should be fully tested and demonstrated to the end user.

Complete the Engineering details of the user guide and give it to the user.

PCB LAYOUT

AC. Connect to the low voltage secondary of the mains transformer. These terminals are not polarity conscious and may be connected either way around.

Battery. Labelled BATT + and - these terminals are for the connection of a 12V rechargeable battery, observing correct polarity.

Outputs P1 and P2. These terminals are programmable outputs, the function of which may be programmed by the engineer. Each output is normally held at 13V and switches to 0V when the programmed condition occurs. The outputs can source up to 1mA and sink up to 30mA. For direct use with a relay (or similar), connect the relay between the output terminal and the +13V supply. The relay will be energised when the programmed condition occurs.

Auxiliary Tamper. Labelled 'TAMP' these terminals provide a general purpose 24 hour tamper loop. This normally closed tamper loop may be used to provide tamper protection for the inside sounders, etc.

Bell Output. Terminals T, A, D and B provide the connection to the external bell or SCB. Observe the correct polarity :

T	=	-ve tamper return
A	=	-ve supply (permanent 0V)
D	=	+ve supply (permanent +13V, fused at 1A)
B	=	-ve bell trigger (switched negative in alarm)

Strobe. For connection to a 12V strobe, observing the correct polarity. This output will normally operate in full alarm conditions at the same time as the bell, but will continue after the bell cut-off until the reset code has been entered. This output is fused at 1A.

Inside Sounders. For connection to up to three 16 Ohm extension speakers, all wired in parallel. These terminals provide an audio signal to the speakers which produce several different alarm, warning and entry/exit tones. This output is fused at 1A.

13V Supply. Labelled 13V + and - these terminals provide a battery backed 13V supply suitable for powering all remote keypads, PIR's, electronic detectors, etc. This output is fused at 1A.

iD Line. Labelled L+ and L- these terminals provide the connection to the iD Line. By convention the L+ connects the yellow core and L- connects to the blue core of standard multicore alarm cable.

Communications. Labelled C+ and C- these terminals provide communications to the RKP's.

Volume Control. Alarm sounds are always generated at full volume, but other sounds, such as entry/exit, are generated at a level set by this small PCB mounted control labelled VOLUME.

Fuses. There are 5 PCB mounted fuses. The battery fuse, located near to the battery terminals, is rated at 1.6A. The other fuses are rated at 1A. All fuses are 20mm quick blow.

Communicator. The two rows of pins on the PCB labelled K11 permit a plug-on digital communicator to be plugged directly onto the PCB. A plug-on RedCare STU may also be used.

LED. The PCB mounted red LED provides a simple indication of the system status. Under normal conditions it will light. If the AC mains fails, and the system runs from battery, it will go out. If the keypad communications fail it will flash; this could be caused by a loss of power to the keypad, a break in the C+ and C- lines, the C+ and C- lines being swapped around, a faulty keypad, or a keypad with the wrong address.

SYSTEM DESCRIPTION

REMOTE KEYPADS

Connections. Each remote keypad has a 6 way terminal block. The 13V terminals (+ and -) connect to the 13V supply from the control panel. The C+ and C- terminals connect to the C+ and C- lines from the control panel.

Keypad Address. Each keypad must have a unique address. The address is set in the keypad by a small jumper and a row of pins (labelled K13) on the PCB . Markings on the PCB show the address adjacent to each jumper position. Where only one keypad is fitted its address must be set to '1'.

Volume Control. The keypad has a volume control which adjusts the volume of the key-beep and error beep sounds produced by the keypad. Turn clockwise to increase the volume.

Backlight Control. The translucent keys are lit from behind by red LED's which are controlled by the main control panel. In normal operation the backlight will be off. It is turned on either when a key is pressed, or the entry period is started.

To have the keys permanently off, cut one leg of the component marked OFF.

To have the keys permanently lit, cut one leg of the component marked ON.

CODES

All entry codes are variable length, 2 to 6 digits long. Karizma has 7 entry codes in all, with 5 different types:

Please note that from Engineering only the Engineer code can be changed. Control of all other codes is via the Manager routine.

Engineer. This code permits access to the engineer facilities for system programming and testing. The engineer code is also used to perform an engineer reset, but it cannot be used to set or unset the system.

User. Four separate user codes allow the user to set and unset the system, omit points during setting, select quick set, and perform a user reset after an alarm condition.

Manager. The first user code is also known as the manager code. This code functions as a standard user code but in addition it allows the manager to change any of the codes, and perform limited tests.

Cleaner. When the system is set, entering the cleaner code will unset only those points which have been programmed with the cleaner access attribute. The cleaner code gives restricted access to the protected premises.

Duress. For use where there is a risk of attack or pressure to set/unset the system the duress code will operate like a user code but will signal a silent PA condition using the communicator.

POINT TYPES

Each iD biscuit, and its associated detector (e.g. PIR),must be programmed to one of the types below;

Security Points. The majority of the points in a typical system will be security points. Security points are operative only when the system has been set. A security point can be made to function as a final exit point, an entry/exit inhibited point or an immediate point (In each program).

Personal Attack. Karizma has 2 types of PA points. A silent PA will only trigger the PA channel of the communicator. An audible PA also sounds the inside sounder and outside bell (without bell delay).

24 Hour. These points are typically used for perimeter protection (vibration sensors, window foil, etc.). When activated in day mode they cause the inside sounders to operate, and optionally trigger the Intruder channel of the communicator. When activated during the set period they cause a full alarm and trigger the Intruder channel of the communicator. Note that 24 Hour points cause immediate bells (no bell delay).

Fire Points. For the connection of smoke and heat sensors with a relay output, Fire points cause both inside sounders and, optionally, outside bells (pulsed 2 seconds on, 2 seconds off) without bell delay. They also trigger the Fire channel of the communicator.

Terminator. An iD device can be wired to a push button which is fixed outside of the exit route, and programmed to operate as a Terminator point. Pressing the button during the exit period, will cause the system to set within 3 seconds.

Control Point. A Control point is used to perform an intelligent shunt on a group of points so that they can be disabled or enabled by means of a keyswitch.

Keyswitch. A Keyswitch point is used to set and unset the entire system.

Door Bell. Produces a distinct Big Ben chime sound. Although intended for use as a door bell this could be used for other signalling applications.

PROGRAMS

When setting the system the user has a choice of setting one of three programs, called A, B and C. The engineer can set-up each program to allow the user to choose the way that the system sets and the detection points which will be enabled.

For example, in a domestic installation program A could be a full-set for when the premises are unoccupied, program B could be a night-time set which leaves upstairs detectors disabled, and program C could be an evening set which enables only the back door and garage door points.

This flexibility in setting the system is achieved by allowing the function of each security point to change with the program being set. Each program has separate final exit, entry/exit inhibited and immediate points, which function in the following way:

Final exit. Usually a magnetic contact on the main entry/exit door is programmed as a final exit point. During the exit period this point may be opened without causing an alarm. When the system has been set, opening this point will cause the entry period to start.

Entry/exit inhibited. These points are normally sited on the route between the entry/exit door and the keypad. During the entry or exit period these points are inhibited and can not cause an alarm. They become fully active once the system has been set.

Immediate. These points are not part of the entry or exit route. They will cause an exit fault condition to show during the exit period, or a full alarm once the system has set.

The setting mode of the system is determined by the program that is set; i.e. each program may have a different setting mode. The following setting modes are available:

Timed. The system will set when the exit time has expired.

Terminated. The system will only set when a Terminator point has been activated and all other points are clear.

Final Door. The system will set 5 seconds after a final exit point (the final door) closes. This 5 second period is to allow detectors on the exit route to clear before the system finally sets. If any points are active at the end of this period the system will not set. There is no time limit on this

GROUP CONTROL

An iD device may be programmed as a control point and used in conjunction with a secure switch (keyswitch or access type keypad) to intelligently shunt a group of Security or 24 hour points.

Group shunting is particularly useful where a system is set but access is required to a warehouse, garage or loading bay. The keyswitch which would be operated on entry into the building and then operated again on leaving the building to restore the group of points and allow full protection to resume.

To make full use of this facility you will need to programme one of the output ports to operate as a Group Fault output. Connect either an LED (with a 1K current limit resistor) or a small 12V buzzer between the +12V supply and the output port and locate this close to the keyswitch which operates the Control point. The LED will light, or the buzzer will sound, whenever the group points cannot be re-enabled.

KEY SWITCH SET/UNSET

An iD device can be located within a key switch or lock switch, and the iD point programmed as a Keyswitch point. The system may then be set or unset by means of the key switch.

Setting. The system may be set from Day mode by activating the Keyswitch point. Karizma will start to set program A, causing the exit period to start. The setting mode of program A will determine the way that the system becomes set.

Unsetting. The system may be unset by causing the Keyswitch point to clear, e.g. by closing a normally closed point. The system will returned to Day mode, and any audible alarm condition which was present will be silenced.

Reset. Although the key switch may be used to silence alarms, it does not reset the system; the system can only be reset by entry of a suitable reset code at a keypad.

CLEANER ACCESS

Day. With the system in Day mode (i.e. unset), the cleaner code works just the same as any other user code. The cleaner can choose the program to be set, omit points during setting (provided that they have the *omit permit* attribute set), and select a quick-set.

Set. If the system is set, then the cleaner may enter the premises by the designated entry route, causing the entry period to start. On entry of the cleaner code at a keypad the entry period will stop, and all points with the cleaner access attribute will be inhibited. The system is now said to be *cleaner unset*. The system indicates this by flashing the green Day LED on the RKP.

Cleaner Unset. Entry of a cleaner code when the system is already cleaner unset will cause the exit period to start. The same exit mode originally used to set the system will be used during cleaner exit. During cleaner exit activating an immediate point with the cleaner access attribute will cause an exit fault. Activating an immediate point which doesn't have the cleaner access attribute will cause a full alarm.

Alarm. Entry of the cleaner code during an alarm condition will silence the alarm. The cleaner code cannot be used to reset the system.

NVM RESET

The NVM can be reset back to the factory set defaults by removing both mains and battery power, shorting output port P1 to the Auxiliary tamper input with a wire link, and then applying power. The NVM will have been reset as soon as Karizma enters alarm. Don't forget to remove the wire link!

The manager code stored in the NVM can be reset back to its default (0123) by following the sequence described above but shorting output port P2 to the auxiliary tamper input. The rest of the NVM is left unchanged.

PROGRAMMING

To test or programme the system follow the instructions below. Each menu may be entered in any order from the Engineering mode with the 'Eng' message showing.

To enter Engineering during initial power up follow the power up instructions.

To enter Engineering from the Day mode, key in the Engineer code and press ENTER.

MENU 0 TESTS

From the 'Eng' prompt press [0] to enter the alarm test mode. Press [ERROR] to quit back to the 'Eng' prompt, or select one of the following functions:

tESt

Bell Test. Press [1] to start the bell (external sounder or siren). Press [ERROR] to stop.

bELL

Strobe Test. Press [2] to start the strobe. Press [ERROR] to stop.

Str

Sounder. Press [3] to start the internal sounder on low volume (the entry/exit sound). The level of the sound produced can be adjusted by a PCB mounted volume control. Press [ERROR] to stop. Press [4] to test the internal sounder on a high volume (the intruder alarm sound). Press [ERROR] to stop.

Lo

Hi

Outputs. Press [5] to turn on output #1, or [6] to turn on output #2. Press [ERROR] to turn off.

P 1

MENU 1 EXTRA TESTS

From the Engineer prompt press [1] to enter the Extra test mode. Press [ERROR] to quit back to the 'Eng' prompt, or select one of the following functions:

EtSt

Walktest. Press [1] to start the walktest. As each point is activated the display will show the point's number and the internal sounder will operate. When the point is cleared the sounder will stop but the display will show the last point to fault. When two or more points are active the display will show the lowest numbered point. Note that any type of point can be tested, provided that the point has first been *enabled* (see section 5.6). Walktest can also be used to test point tampers; in this case a higher pitched sound is used and the display will show 'Pt'. Press [ERROR] to stop the walktest.

PF09

Pt09

Soak Test. Security and 24 Hour points may be placed on soak test. Normal operation of that point will be inhibited and any activation of the point which would normally have caused an alarm will cause both a *point test* event and a point alarm event to be logged. A tamper condition will cause both a *point test* event and a point tamper event to be logged.

Press [2] to place a point on soak test. Key in the point number and press [ENTER]. Karizma displays the present setting of the attribute. Press [1] to place the point on soak test, [0] to remove the point from soak test, then press [ENTER]. Press [ERROR] to quit at any time without change. Point numbers 00 and 99 have special significance. Entering a point number of 00 (both digits are required) will remove the soak test attribute from all points. Point number 99 will add the attribute to all Security and 24 Hour points.

Pt02

02=0

iD Line Data Display. Press [3] for the iD line data display mode. Karizma prompts for a point number; key in the point number of the first point to be examined, and press [ENTER]. The display will now show the status of 4 iD points starting on the left with the point number just entered. The display will be updated as the status of each point changes. Press [ERROR] to quit at any time. The display shows:

Pt08

10_2

≡≡≡≡

_	for a point not present
0	for a point present and open
1	for a point present and closed
2	for 2 or more devices responding at the same address
≡	for a line short (short circuit across the iD line)

Unlike the walktest, the iD line data display displays the status of each iD device irrespective of how the iD point has been programmed.

MENU 2 COMMUNICATOR TESTS

From the engineer prompt press [2] to enter the digital communicator test mode. Press [ERROR] to quit back to the 'Eng' prompt, or select one of the following functions:

diGi

Fire. Press [1] to activate the Fire output to the communicator. Press [ERROR] to clear.

FirE

PA. Press [2] to activate the PA output to the communicator. Press [ERROR] to clear.

PA

Intruder. Press [3] to activate the Intruder output to the communicator. Press [ERROR] to clear.

Intr

Set. Press [4] to activate the set (closed/open) output to the communicator. Press [ERROR] to clear.

SEt

Tamper. Press [5] to activate the Tamper (Trouble) output to the communicator. Press [ERROR] to clear.

tA

Low Battery. Press [6] to activate the Low Battery output to the communicator. Press [ERROR] to clear.

bAtt

Line Fault Input. Press [7]. The display will show the current state of the Line Fault input from the communicator. 'F' means Fault, 'C' means Clear.

LF C

MENU 3 TIMERS

From the Engineer prompt press [3] to enter the system timer set-up mode. Press [ERROR] to quit back to the 'Eng' prompt, or select one of the following functions:

tSEt

Exit Time. Press [1]. The current value of the exit time is shown (in seconds). Key in the required exit time and press [ENTER], or press [ERROR] to quit without change. The allowable exit time is 0 to 999 seconds.

E030

Entry Time. Press [2]. The current value of the entry time is shown (in seconds). Key in the required entry time and press [ENTER], or press [ERROR] to quit without change. The allowable entry time is 0 to 999 seconds.

n030

Bell Time. Press [3]. The current value of the bell time is shown (in minutes). Key in the required time and press [ENTER], or press [ERROR] to quit without change. The allowable bell time is 1 to 99 minutes. The value 00 has special significance; it implies infinite bell time.

b 20

Bell Delay. Press [4]. The current value of the bell delay time is shown (in minutes). Key in the required time and press [ENTER], or press [ERROR] to quit without change. The allowable bell delay time is 0 to 99 minutes.

d 00

MENU 4 POINT PROGRAMMING

From the engineer prompt press [4] to enter the point programming mode which allows the type of each iD point, and the attributes of that point, to be programmed. Note that certain attributes can only be applied to Security points. Press [ERROR] to quit back to the 'Eng' prompt, or select one of the following functions:

PP

Point Type. Press [1] to programme the type of an iD point. Karizma will prompt you for the number of the point; key in the point number (1 to 30) and press [ENTER]. Karizma will display the present type of that point. The following types are used:

Pt23

23= 1

0 = Disabled
1 = Security
2 = Audible PA
3 = Silent PA
4 = 24 Hour
5 = Fire
6 = Control
7 = Terminator
8 = Keyswitch
9 = Door Bell

Press [ERROR] to quit without changing the type of the point, or key in the required point type and press [ENTER].

Normally Closed Attribute. The normally closed attribute can be applied to any iD point. Press [2], enter the point number and press [ENTER]. The display shows the current setting of the attribute for that point; press [1] or [0] to respectively set or clear the attribute then press [ENTER] to accept the displayed value. Press [ERROR] at any time to quit without change. Point number 00 (both digits are required) has special significance; it will clear the attribute from all points. Point number 99 will set the attribute on all points. By default all points have this attribute set, so you should only need to clear this attribute in special cases.

Pt08

08=0

Double Knock. The double knock attribute can only applied to Security points. Press [3], enter the point number and press [ENTER]. The display shows the current setting of the attribute; press [1] or [0] to set or clear the attribute, then press [ENTER] to accept the displayed value. Point numbers 00 and 99 operate on Security points only.

Pt08

08=0

Permit Omit. The permit omit attribute can be applied to Security and 24 Hour points. Press [4], enter the point number and press [ENTER]. The display shows the current setting of the attribute; press [1] or [0] to set or clear the attribute, then press [ENTER] to accept the displayed value. Point numbers 00 and 99 operate on Security points only. When set on a Security point this attribute permits the user to omit that point when setting the system. When set on a 24 Hour point it permits the manager to omit that point at any time that the system is unset. 24 Hour points which have been omitted are automatically re-instated when the system is set.

Pt09

09= 1

Cleaner Access. The cleaner access attribute can only applied to Security points. Press [5], enter the point number and press [ENTER]. The display shows the current setting of the attribute; press [1] or [0] to set or clear the attribute, then press [ENTER] to accept the displayed value. Point numbers 00 and 99 operate on Security points only.

Pt 10

10=0

Group Point. The group attribute can be applied to Security and 24 Hour points. Press [6], enter the point number and press [ENTER]. The display shows the current setting of the attribute; press [1] or [0] to set or clear the attribute, then press [ENTER] to accept the displayed value. Point numbers 00 and 99 operate on Security points only

Pt 11

11=0

MENU 5 PROGRAMS

From the engineer prompt press [5] to enter the programme set-up mode. The function of each Security point and the exit mode can be set-up for each of the 3 programmes. Press [ERROR] to quit back to the 'Eng' prompt, or select one of the following functions:

```
ProG
```

Programme A Points. Press [1] to set-up the points used in programme A. Karizma prompts for a point number. Key in a point number and press [ENTER]. If the point is a Security point Karizma will display the current type of that point when used by Programme A, with :

```
Pt20
```

```
20=0
```

0 = Not used in programme
1 = Immediate point
2 = Entry/exit inhibited
3 = Final exit point

Key in the required type and press [ENTER]. Press [ERROR] at any time to quit without change. Entering a point number of 99 will enable all Security points to operate as immediate points in this programme. Entering a point number of 00 will remove all Security points from this programme.

Programme B and C. Press [2] to set-up the points used in programme B, or [3] to set-up the points used in programme C.

Programme Exit Modes. Press [4], [5] or [6] to set-up the exit modes used by programme A, B or C respectively. The display shows the exit mode used by the programme. Key in the required exit mode and press [ENTER]. The following values are used:

```
A  = 1
```

0 = Program is disabled (note: programme A cannot be disabled)
1 = Timed Exit
2 = Terminate to Set
3 = Final Door Set

Programme Local Alarm Flags. Normally, when the system has been set using a programme, a violation of a security point contained in that programme will cause the system to report (ie communicate) to the central station. Any of the three programmes can be made to produce a local alarm only (without reporting to the central station) by setting the corresponding local alarm flag. Press [7], [8] or [9] to set-up the local alarm flag for programmes A, B or C respectively. Press either [1] or [0] to set or clear the flag and press [ENTER], or press [ERROR] to quit without change. When the flag has been set the programme will not report.

```
A  =0
```

MENU 6 EVENT LOG

From the engineer prompt press [6] to view the event log. The display shows the last event to occur, which is usually (ECod - engineer code). The event log stores the last 100 events in non-volatile memory. Press [1] to display the previous event in the log. Press [3] to display the next event in the log. Press [ERROR] to quit back to the 'Eng' prompt.

~~A summary of the event types and displays is provided at the back of these instructions.~~

MENU 7 CHANGE ENGINEER CODE

From the engineer prompt press [7] to change the engineer code. Key in the code (up to 6 digits) and press [ENTER] to confirm, or press [ERROR] to quit without changing the code. If the code is already in use the display will show 'Err' and the code will not be changed.

ECod

Err

MENU 8 SYSTEM FLAGS

From the engineer prompt press [8] to enter the system flags set-up mode. Press [ERROR] to quit back to the 'Eng' prompt, or select one of the following sub functions:

FLAG

Outside Fire Bell. Press [1]. The display shows the current setting of the flag; press [1] or [0] to set or clear the flag, press [ENTER] to accept the displayed value, or press [ERROR] to quit without change. When this flag is set a Fire alarm condition will cause the outside bells / siren to be pulsed on/off at 3 second intervals.

Fb=0

High Volume Chime. Press [2]. The display shows the current setting of the flag; press [1] or [0] to set or clear the flag, press [ENTER] to accept the displayed value, or [ERROR] to quit without change. When this flag is set both the chime sound, and the exit terminate sound, will be produced at high volume.

Ch=0

Engineer Reset. Press [3]. The display shows the current state of the flag; press [1] or [0] to set or clear the flag, [ENTER] to accept the displayed value, or [ERROR] to quit without change. When this flag is set Karizma will require an engineer reset after an intruder or fire alarm condition. PA alarms are handled differently, see below.

Er= 1

Entry Deviate. Press [4]. The display shows the current state of the flag; press [1] or [0] to set or clear the flag, [ENTER] to accept the displayed value, or [ERROR] to quit without change. When this flag is set Karizma will permit an entry route deviation; activating an immediate point during the entry period will cause an alarm sound to be produced from the inside sounder but the communicator will not be triggered immediately.

Ed=0

RedCare STU Remote Reset. Press [5]. The display shows the current state of the flag; press [1] or [0] to set or clear the flag, [ENTER] to accept the displayed value, or [ERROR] to quit without change. When this flag is set Karizma will allow a remote reset from the plug-on RedCare STU to reset the system.

Sr=0

Remote Reset Anti-Code. Press [6]. The display shows the current state of the flag; press [1] or [0] to set or clear the flag, [ENTER] to accept the displayed value, or [ERROR] to quit without change. When this flag is set the remote reset anti-code facility is enabled.

Cr= 1

User Reset after PA Alarm. Press [7]. The display shows the current state of the flag; press [1] or [0] to set or clear the flag, [ENTER] to accept the displayed value, or [ERROR] to quit without change. When this flag is set Karizma can be reset after a PA alarm by a user code even if all other alarms require an engineer reset. When this flag is clear the requirement for an engineer or user reset after a PA alarm is determined by the engineer reset flag

PA= 1

Report 24H Points. Press [8]. The display shows the current state of the flag press [1] or [0] to set or clear the flag, [ENTER] to accept the displayed value or [ERROR] to quit without change. When this flag is set a violation of a 24Hour point during Day mode will trigger the Intruder channel of the communicator or STU. Note: 24Hour points always report (ie communicate) when the system has been set

24= 1

QUICK REFERENCE PROGRAMMING

From the 'EnG' prompt:

0 - ALARM TESTS

1 = Bell on
2 = Strobe on
3 = Sounder on low volume
4 = Sounder on high volume
5 = Output #1 on
6 = Output #2 on

1 - EXTRA TESTS

1 = Walktest Mode
2 = Soak Test
3 = iD line data

2 - COMMUNICATOR TESTS

1 = Fire
2 = PA
3 = Intruder
4 = Set
5 = Tamper
6 = Low Battery
7 = Line Fault Status

3 - SYSTEM TIMERS

1 = Exit Time (10 to 999 seconds)
2 = Entry Time (10 to 999 seconds)
3 = Bell Time (0 to 99 minutes)
4 = Bell Delay (0 to 99 minutes)

4 - POINT PROGRAMMING

1 = Point type
    0 = Disabled
    1 = Security
    2 = Audible PA
    3 = Silent PA
    4 = 24Hour
    5 = Fire
    6 = Group control
    7 = Terminator
    8 = Keyswitch Set
    9 = Door Bell
2 = Normally Closed
3 = Double Knock
4 = Permit Omit
5 = Cleaner Access
6 = Group Point

5 - PROGRAMS

1 = Program A points
    0 = not used
    1 = Immediate
    2 = Entry/exit inhibited
    3 = Final exit
2 = Program B points
3 = Program C points
4 = Program A Exit mode
    0 = disabled
    1 = Timed
    2 = Terminated
    3 = Final door
5 = Program B Exit mode
6 = Program C Exit mode
7 = Program A Local Alarm
8 = Program B Local Alarm
9 = Program C Local Alarm

6 - EVENT LOG

1 = Display previous event (older)
3 = Display next event (newer)

7 - ENGINEER CODE

8 - SYSTEM FLAGS

1 = Outside Fire Bell
2 = Chime High volume
3 = Engineer Reset
4 = Entry deviate allowed
5 = RedCare STU Remote Reset enabled
6 = Remote Reset Code enabled
7 = User Reset after PA Alarm
8 = Report 24H Points in Day

9 - MISCELLANEOUS OPTIONS

1 = Enable RKP
2 = Write NVM to socket
3 = Read from NVM in socket
4 = Configure Output Port #1
5 = Configure Output Port #2
    0 = not used
    1 = System Set
    2 = Group Fault
    3 = Walktest
    4 = Engineering
    5 = OK for Set
    6 = Alarm Follow
6 = Remote Reset Site Code
7 = Re-arm counter

FACTORY SET CONDITIONS

Engineer code	9999
User code #1	0123
Bell Delay	0 minutes
Bell Time	20 minutes
Entry Time	30 seconds
Exit Time	30 seconds
Remote Reset Site Code	00
Re-arm Count	2
Outside Fire Bells	Yes
Chime High Volume	No
Engineer Reset	No
Entry Deviate	Yes
STU Remote Reset	No
Anti-code Reset	No
User Reset after PA	No
Report 24H Points	No

DISPLAY ROUTINES

The list below shows the RKP displays for each event created by the system. These will show when alarm conditions are unset or when reading the log.

AC — **AC Mains Fail.** The AC mains supply has failed. The system will now be operating from its internal standby battery.

AL23 — **Intruder Alarm.** Logged when a Security or 24 Hour point is violated. The number identifies the point.

bAtt — **Battery Fail.** The standby battery has failed, and the system can no longer operate. It will now shutdown.

CLUS — **Cleaner Unset.** The cleaner code has been entered causing the system to become cleaner-unset.

CrES — **Anti-code reset.** Logged when the system is reset by an anti-code.

CS — **Communication Successful.** The signalling device has successfully communicated with the central station.

dur — **Duress.** The duress code has been entered, causing the signalling device to communicate a PA alarm to the central station.

EnGr — **Engineer Code.** The engineer code has been entered.

Ent — **Entry Start.** An entry/exit point has been opened which caused the entry period to start.

Entd — **Entry Deviate.** Logged during the entry period when you have deviated from the designated entry route.

Ento — **Entry Timeout.** The entry period has expired before a valid code was entered.

Ento — **Engineer Reset.** Logged when the system is reset by an Engineer code.

F 09 — **Fire Alarm.** A Fire detection point has been activated. The number identifies the point.

FtC — **Fail to Communicate.** The signalling device has failed to communicate with the central station.

init — **System Initialisation.** The system has been re-initialised after being powered-up.

LF — **Telephone Line Fault.** The signalling device has detected a fault on the telephone line that it uses to communicate with the central station.

oP03 — **Omit Point.** A point has been omitted. The number identifies the point.

PA07 — **Personal Attack.** A PA button has been pressed.

PrGA — **Program.** Identifies the programme (A, B or C) which was selected by the user when the system was set.

rF2 — **RKP Failure.** A remote keypad has failed. The number identifies the RKP.

SEt 1 — **System Set.** The system has been set. The number identifies the user who set the system. This event is always followed by the programme event (Prg) which identifies the programme which was selected. It may also be followed by the omit point event (oP) which identifies those points which were omitted by the user.

SEt — **Key switch Set.** The system has been set by operation of the keyswitch.

Sh — **Group Shunted.** The group points have been shunted and are therefore disabled.

Shrt — **iD Line Short.** An attempt has been made to tamper with the alarm sensing line.

Sr — **Group Shunt released.** The points in the Shunt Group have been re-anabled.

tP 16 — **Soak Test.** A point on soak test has been activated when that point would normally have caused an alarm.

t 18 — **Point tamper.** An attempt has been made to tamper with the operation of a detection point, or the detection point has failed.

t Au — **Tamper.** The auxiliary tamper circuit has been opened. This may be due to an attempt to tamper with the system.

t bE — **Bell tamper.** The tamper circuit in the outside sounder (or bell) has been opened.

t CA — **Case tamper.** The control panel case (lid) has been opened.

t Co — **User Code Tamper.** Five or more unsuccessful attempts at entering a code have been made.

t r3 — **RKP tamper.** The cover on the RKP has been opened. The number identifies the RKP.

UrES — **User Reset.** Logged when the system is reset by a user code.

USEt — **Key switch Unset.** The system has been unset by operation of the keyswitch.

USt 1 — **System Unset.** The system has been unset by a user code. The number identifies the user.

---- — **End of Log.** Marks the end of the event log.

Due to continuous product development, ADE reserve the right to change specifications as and when required without prior notice.

ADE TM

Advanced Design Electronics Ltd.

TECHNICAL 0151-549 1550

EASEM

BSIA THE BRITISH SECURITY INDUSTRY ASSOCIATION

MENU 9 MISCELLANEOUS OPTIONS

From the engineer prompt press [9] to enter the miscellaneous options mode. Press [ERROR] to quit back to the 'Eng' prompt or select one of the following functions:

0Pt

RKP Enable. Press [1], enter the address of an RKP (2 to 4) and press [ENTER]. The display shows the current state of the RKP. Press [1] or [0] to enable or disable that RKP. Press [ENTER] to accept the displayed state, or [ERROR] to quit without change. Note that RKP 1 is always enabled and cannot be changed.

r2

r2=0

Write NVM. Press [2] to *Put* the contents of the system NVM into an NVM chip in socket K12. If an error occurs, of if the socket is empty, the 'Err' message will be displayed.

Put

Read NVM. Press [3] to *Get* the contents of the NVM chip in the socket into the system NVM. If an error occurs, of if the socket is empty, the 'Err' message will be displayed.

GEt

Output Ports. Press [4] or [5] to programme the output ports P1 and P2. The display shows how the output port is currently programmed. Enter the required value and press [ENTER] to accept or press [ERROR] to quit without change. The following values are used:

0 1=3

Val	Type	Description
0	Not used	Output port is not used
1	System Set	Active when the system is set
2	Group Fault	Active when a group shunt has been removed but the group could not be enabled due to a fault
3	Walktest	Active during walktest mode
4	Engineering.	Active during engineering mode
5	OK for Set	Active during the exit period when there are no faults
6	Entry/Exit Follow	Active during the entry and exit periods
7	Alarm Follow	Active during a PA, Fire or Intruder alarm. This output is normally used to trigger a single channel communicator.

Site Code. Press [6] to change the Site code. The display shows the current code as a 2 digit number. Key in the new number, press [ENTER] to accept the number, or press [ERROR] to quit without change. The site code is 2 digit number between 00 and 99 which is used in the remote reset code generator. The central station operator of the anti-code generator must know the site code in order to generate the correct anti-code for the remote reset.

C 00

Re-Arm Counter. Press [7]. The current value of the re-arm counter is shown. Key in the required value between 0 and 9 and press [ENTER], or press [ERROR] to quit without change. A re-arm count of 2 (the default value) will allow the system to re-arm twice, ie go into full alarm 3 times. A re-arm count of 0 allows just one full alarm

rE=2

PLUG ON STU OR COMMUNICATOR

The PCB has two 8-pin connectors labelled K11 which allow the use of a plug-on digital communicator or RedCare STU. Using a plug-on communicator with Karizma is usually fairly simple. The information given here is intended to be of use where the control panel and communicator don't work as expected.

Each of the communicator pins has a dedicated function. Some pins act as *triggers*, which will cause the commuicator to attempt to communicate with the central station. Other pins just carry power to the communicator. The table below describes the function of each of the 16 pins.

No	In/ Out	Function	Description	Usual Channel
1	Out	Fire	Positive trigger for Fire alarm	1
2	Out	PA	Positive trigger for Personal Attack	2
3	Out	Intruder	Positive trigger for Intruder alarm	3
4	Out	Set/Unset	Positive trigger when Set	4
5	Out	Tamper	Positive trigger for Tamper alarm	5
6	In	Tellback	Logs a Communication Successful event	
7	In	Comms. Fail	Logs a Fail to Communicate event. Cancels bell delay in alarm conditions.	
8	Out	Low Battery	Positive trigger when low battery voltage detected	
9	Out	+12V	Power supply	
10	Out	0V	Power supply	
11	Out	+5V	Permanent +5V	
12	Out	+5V	+5V Power supply	
13	Out	Engineer access	Positive trigger for Engineer access	8
14	Out		Not used	
15	In	Line Fault	Logs a Line Fault event. In alarm - cancels bell delay. Unset - produces an audible warning	
16	Out	Restart	Active high to restart the communicator	

The communicator uses data programmed into its NVM or PROM chip to assign a channel to each of the trigger pins. The table above shows the channels which are usually assigned to each trigger. This assignment may be altered by re-programming the communicator's NVM chip

If you do not want a particular trigger to communicate then the communicator NVM or PROM must be programmed to ignore triggers on that channel. This can be done by not assigning a channel to the trigger input.