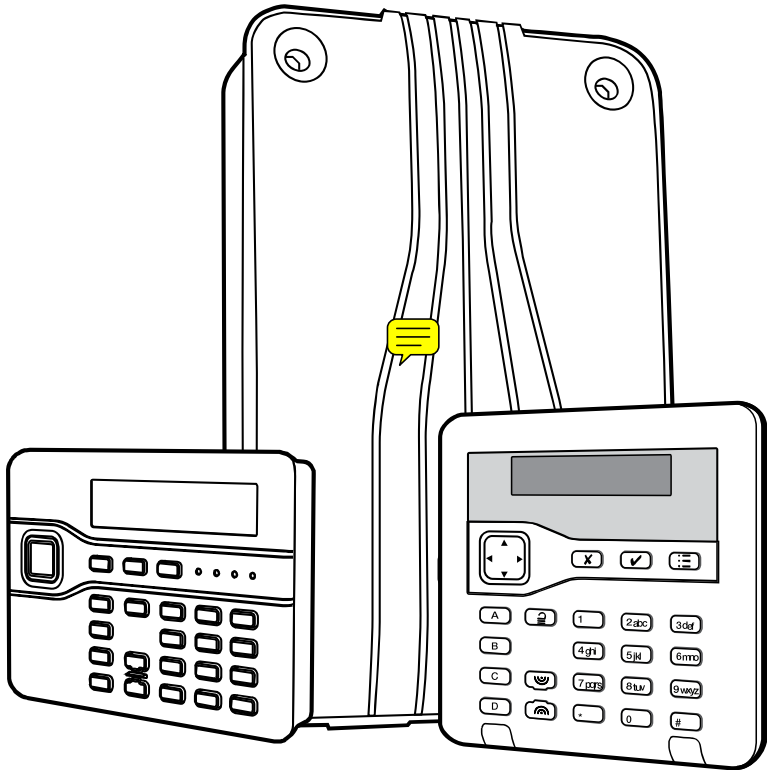


# i-on40

## Security System Installation Guide



Issue 7

**EATON**

*Powering Business Worldwide*

© Eaton's Security Business. 2014

IN NO EVENT WILL EATON'S SECURITY BUSINESS BE LIABLE FOR ANY SPECIAL, CONSEQUENTIAL, OR INDIRECT LOSS OR DAMAGE, INCIDENTAL DAMAGES, STATUTORY DAMAGES, EXEMPLARY DAMAGES, LOSS OF PROFITS, LOSS OF REVENUE, LOSS OF ANTICIPATED SAVINGS, LOSS OF BUSINESS OR OPPORTUNITY, LOSS OF GOODWILL OR INJURY TO REPUTATION, LIQUIDATED DAMAGES OR LOSS OF USE, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. EATON'S SECURITY BUSINESS'S LIABILITY FOR DAMAGES ARISING OUT OF OR RELATED TO A PRODUCT SHALL IN NO CASE EXCEED THE PURCHASE PRICE OF THE PRODUCT FROM WHICH THE CLAIM ARISES. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THESE LIMITATIONS AND EXCLUSIONS WILL APPLY WHETHER EATON'S SECURITY BUSINESS'S LIABILITY ARISES FROM BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING BUT NOT LIMITED TO NEGLIGENCE), STRICT LIABILITY, BY OPERATION OF LAW, OR OTHERWISE.

Every effort has been made to ensure that the contents of this book are correct. The contents of this book are subject to change without notice.

This manual applies to the i-on40 control unit with version 4.04 software.

### **For Your Safety**

This book contains several passages alerting you to potential problems or hazards. Each of these are marked by the words **Note**, **Caution** or **WARNING**:

**Note:** Describes conditions that may affect the proper functioning of the equipment (but will not damage the equipment).

**Caution:** Describes actions that will physically damage the equipment and prevent its proper function.

**WARNING:** Describes actions that are hazardous to health, or cause injury or death.

Please pay particular attention to these marked passages.

### **Terminology**

With the introduction of BS8243 and PD6662:2010, Eaton's Security Business have changed the name "panic alarm" to "hold up alarm" and "PA" to "HUA". A PA device is now called a "HUD" (hold up device).

### **Other Publications for the i-on40:**

The following guides are available from the Eaton's Security Business website: [www.coopersecurity.co.uk](http://www.coopersecurity.co.uk)

Quick User Guide	Brief instructions for setting and unsetting alarm systems based on i-on control units.
i-on Range Engineering Guide	A detailed description of the Installer's programming options available for i-on control units.
i-on Range Administrator's Guide	Detailed notes for the system administrator of an alarm system based on the i-on40, i-on30EX, i-on50EX and i-on160EX.
Web Server Setup Guide	Instructions on how to configure a Windows PC or laptop to use the i-on40, i-on50EX/EXD and i-on160EX's built-in web browser interface for installation programming.
Eaton's Security Business Downloader Quick Guide	Instructions for how to install Eaton's Security Business Downloader on your PC or laptop, and connect to i-on Control Units.
i-on Updater Installation and User Guide	Instructions on how to install i-on Updater on your PC and use it to update the software on your i-on40, i-on30EX/EXD, i-on50EX/EXD and i-on160EX control unit.

# CONTENTS

Terminology .....	ii	Security .....	26
<b>1. Introduction .....</b>	<b>1</b>	Radio .....	26
Communications .....	1	Power Supply .....	26
Level Setting or Partitioned System .....	1	EN50131-6 ratings: .....	26
Installer Programming Interface .....	2	Electromagnetic Compatibility .....	27
About this Guide .....	2	Outputs .....	27
<b>2. Before You Begin .....</b>	<b>3</b>	Fuses .....	27
Preparation .....	3	Electrical Safety .....	27
Radio Site Survey .....	3	Other .....	27
Siting the Control Unit .....	3	Compliance Statements .....	28
Siting Keypads .....	3	Compatible Equipment .....	28
Guided Tour .....	3	HUD .....	28
Opening the Control Unit Case .....	3	Detectors .....	28
Control Unit PCB .....	4	Sounders .....	28
i-KP01 Controls and Displays .....	5	Setting / Unsetting – Keypads .....	28
Opening the i-kp01 .....	5	Setting / Unsetting - Fobs .....	28
Power Availability .....	8	Communicators .....	29
<b>3. Installation .....</b>	<b>9</b>	Accessories .....	29
Step 1. Fit the Control Unit Case .....	9		
Caution: Static Electricity .....	9		
Fitting .....	9		
Installing the Lid/Back Tamper .....	9		
Step 2. Fit and Connect the Keypad(s) .....	9		
Siting the Keypad(s) .....	9		
Fitting Keypads .....	10		
Connecting Keypads to Control Unit .....	10		
Keypad Addressing .....	11		
Re-using a V2.0 Keypad From an i-onEX .....	11		
Backlight Control I-KP01 .....	11		
Backlight Control for KEY-K01/KP01/KPZ01 .....	12		
Tone Volume – All Keypads .....	14		
Step 3. Connect Control Unit to Mains .....	14		
Mains Cabling .....	14		
Mains Connection .....	15		
Step 4. Connect Wired Zones .....	15		
Four Wire Closed Circuit Connections .....	15		
Two-Wire Closed Circuit Connections .....	15		
Fully Supervised Loop Connections .....	15		
Connecting Wired Zones on KEY-KPZ01 only) .....	16		
Step 5. Connect Wired Peripherals .....	17		
Remote Loudspeaker (Optional) .....	17		
Wired External Sounders (Optional) .....	17		
Wired Outputs (Optional) .....	17		
Output on KEY-KPZ01 .....	17		
Step 6. Fit a Plug-By Communicator .....	17		
Step 7. Fit and Connect Battery .....	18		
Programming Before Installation .....	18		
Step 8. Initial Power-Up .....	18		
Step 9. Commission the System .....	20		
<b>4. Programming .....</b>	<b>21</b>		
Entering the Installer Menu .....	21		
Leaving the Installer Menu .....	21		
Important! Saving Changes .....	21		
Restoring Access Codes .....	21		
Restoring Factory Defaults .....	22		
Installer Menu .....	23		
<b>5. Maintenance .....</b>	<b>25</b>		
<b>6. Technical Specification .....</b>	<b>26</b>		
General .....	26		
Capacities .....	26		

This page is intentionally blank.

# 1. Introduction

The i-on40 is the control unit for a hybrid wired/wirefree alarm system intended for domestic and light commercial use.

The control unit comprises an ABS plastic case which contains the radio transceiver, power supply and backup battery. Up to four separate wired keypad(s) can connect to the control unit by standard alarm cable.

The i-on40 at release 4 uses i-kp01 keypads with software version 2.0 and above. The keypads allow end users to set and unset the system, and the installer to configure the control unit. The i-kp01 keypad also contains an integral proximity tag reader, allowing end users to control the system without having to remember access codes.

Note that to work correctly the i-on40 must be fitted with at least one wired keypad.

The following types of keypad are also available for connection to the i-on40:

- KEY-K01 This keypad has no internal prox reader, and is supplied in a square format case.
- KEY-KP01 This product, supplied in the same case as the KEY-K01, has an internal prox reader and also provides terminals for an external prox reader KEY-EP
- KEY-KPZ01 This product, supplied in the same case as the KEY-K01, has an internal prox reader and also provides terminals for up to two zones, a programmable output, and an external prox reader KEY-EP

A range of wireless peripherals is available for operation with the control unit. These include a door contact/universal transmitter, a passive infra red detector, smoke detector, external siren, 4 button remote control, and remote radio keypad.

The control unit supports up to 16 wired alarm zones, 24 wirefree alarm zones, up to 16 hardwired outputs, 50 four-button remote controls, 50 two-button radio panic alarms, and 50 users. See page 26.

This control unit is designed and approved to be used as part of a Security Grade 2 system.

## Communications

The i-on40 provides sockets for an add-on communication module. The available modules are:

i-dig02  
(ATS2)

A switched telephone network (PSTN) module that allows the control unit to report alarm information using standard protocols such as Fast Format, SIA and Contact ID, and can also send text messages over the Public Switched Telephone Network (PSTN). The i-dig02 also allows remote maintenance using Eaton's Security Business Downloader software.

i-sd02  
(ATS2)

A speech dialler and PSTN module that allows the control unit to send recorded speech messages and report alarm information using standard protocols such as Fast Format, SIA and Contact ID. The module can also send text messages over the PSTN. The i-sd02 also allows remote maintenance using Eaton's Security Business Downloader software.

i-gsm02  
(ATS2)

A GSM module that allows alarm reporting, speech messaging and SMS text messaging over the mobile phone network. Note that a SIM card is not included with the module.

The control unit also provides outputs that can be used to fit a "plug by" communicator.

To comply with EN50131 you must fit an ATS2 communicator.

## Level Setting or Partitioned System

The i-on40 offers two basic ways of behaving as an alarm system:

**Part Setting.** In a Part Setting system the i-on40 can set in one of four ways: either Full set or three varieties of Part Set. In Full set the control unit pays attention to all detectors. In each of the three Part Sets the control unit ignores detectors that do not have the appropriate Part Set attribute.

**Partitioned System.** In a Partitioned system the i-on40 provides the equivalent of four, smaller, independent alarm systems. Each system is a "Partition" of the i-on40. You can allocate any zone to each Partition. Each zone can also belong to more than one Partition. Each Partition can have a Full Set level and one Part Set Level. During installation the installer can allocate keypads, sounders or outputs to any of the partitions.

This manual shows the simple procedure required to install the control unit and its keypad. When you have completed the physical installation please consult the Programming section for details of configuring the system to meet your exact requirements.

For a detailed description of the Installer's programming menu please read *i-on Range Engineering Guide* available from [www.coopersecurity.co.uk](http://www.coopersecurity.co.uk).

Note: Some programming options can make the installation non-compliant with EN50131. The relevant options are noted in the *i-on Range Engineering Guide*.

### **Installer Programming Interface**

Once fitted and powered up, you can program the control unit through any wired keypad connected to the control unit. The Installer Menu allows you to specify all the operating parameters for an individual installation.

If you wish, you can also program the system from a PC or laptop connected to the Ethernet port on the control unit PCB. The control unit contains a web browser interface, and you can use any web browser to see a complete version of the Installer menu. Please see the *i-on Web Server Setup Guide* for more instructions.

Note that Eaton's Security Business recommends using Internet Explorer. Other browsers may not be fully compatible with the web browser interface.

In addition, it is possible to connect a PC or laptop to the mini USB port on the control unit PCB and use Eaton's Security Business Downloader software to program the control unit.

Note: Some programming options can make the installation non-compliant with EN50131. The relevant options are noted in the "Installer Menu" section of the *i-on Range Engineering Guide*.

### **About this Guide**

This guide shows the simple procedure required to physically install the control unit, connect keypads and power up the system for the first time.

When you have completed the physical installation please consult the *i-on Range Engineering Guide* for details of configuring the system to meet your customer's requirements. For your convenience page 23 of this installation guide contains a condensed reference table of the Installer menu.

---

## 2. Before You Begin

---

### Preparation

Before installation you should carry out a survey of the site. You need to know how many and what kind of detectors will be transmitting to the control unit. You also need to assess where the control unit must be placed in order to receive radio signals from the detectors successfully.

### Radio Site Survey

You should conduct signal strength tests before installation. Eaton's Security Business produce the Scantronic 790r hand held signal strength meter and 734r-01 test transmitter for this purpose. Please read the 790r manual for details.

Please be aware of the following:

- The 790r signal strength meter readings should be used only as an guide when initially checking the site.
- A reading of four green LEDs or higher indicates an acceptable signal strength.
- Once you have installed the alarm system you should put the control unit in the Installer test menu and test the received signal strength from each radio transmitter.
- A signal strength reading of two or more units by the control unit from each transmitter should provide reliable operation in the installed system. (**Note:** if you take the signal strength using i-on Downloader or the web browser interface while the panel is in user mode then the minimum acceptable signal strength is four units. Ensure that the control unit is in Installer mode when reading signal strengths remotely.)
- When you record the signal strength readings for later inspection, you should record the readings taken from the control unit of the installed system while it is in the Installer Menu.

Please be aware that the signal strength received from a transmitter can change after installation because of local environmental changes. For example, users switching on laptops nearby, or moving metal cabinets from their original position can all affect the signal from a transmitter. Please read Eaton's Security Business publication "Guidance Notes for Wireless Alarm System Installations" obtainable from [www.coopersecurity.co.uk](http://www.coopersecurity.co.uk) for more information about the factors affection radio signal strength.

### Siting the Control Unit

**Do site the unit:**

- Upright (battery at the bottom).
- Within a protected zone.

As high as possible. However, do make sure that the unit is on a similar level to the other transmitters or receivers.

**Do NOT site the unit:**

In the entry or exit zones, or outside the area covered by the alarm system.

Close to or on large metal structures.

Closer than one metre to mains wiring, metal water or gas pipes, or other metal surfaces.

Lower than two metres from the floor (ideally).

Inside metal enclosures.

Next to electronic equipment, particularly computers, photocopiers or other radio equipment, CAT 5 data lines or industrial mains equipment.

**Note:** Some window glasses, especially those sold as "insulating" or "energy conserving" may be coated with thin metal or conducting films. These glasses are particularly poor at transmitting radio waves.

If fitting two or more keypads then make sure that you do not place the keypads within one metre to each other. (The proximity tag readers in each keypad will interfere with each other.) Remember not to place keypads on opposite sides of the same wall.

### Siting Keypads

If fitting two or more keypads make sure that you place the keypads more than one metre apart from each other, or from any other type of prox reader. (At less than one meter separation the proximity tag readers will interfere with each other.) Remember not to place keypads or external prox readers on opposite sides of the same wall.

If you intend to fit external prox reader KEY-EP to a KEY-KPZ01/KP01, then do not site the external prox reader itself closer than one meter to any other keypad or other type of prox reader.

### Guided Tour

**CAUTION:** The printed circuit boards for the i-on40 and its keypads have been tested for Electromagnetic Compatibility (EMC). However, when handling the pcbs you must take the standard precautions for handling static sensitive devices.

### Opening the Control Unit Case

To gain access to the interior of the control unit undo the two screws at the top of the case. Pull the top of the lid down, and then lift the lid out of the retaining lugs at the bottom of the case.

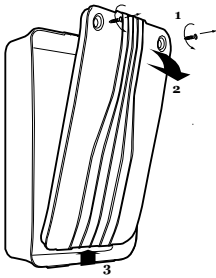
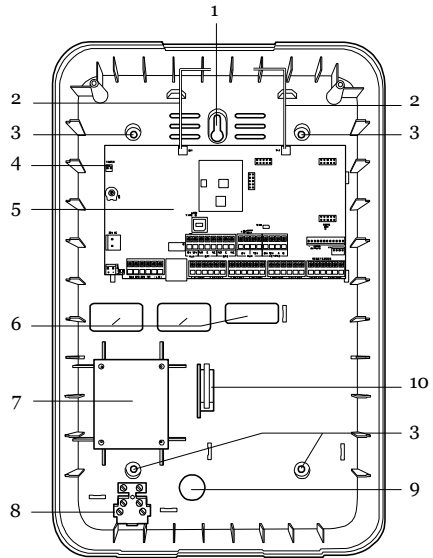


Figure 1 Opening the Control Unit.

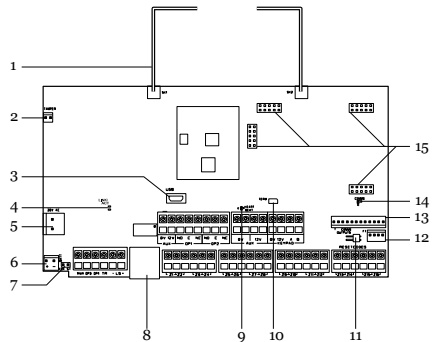
**WARNING:** When connected to the mains with power applied mains voltages are present on the shrouded heads of the terminal screws of the mains connector ("8" in Figure 2).



1. Central fixing keyhole.
2. Aerials.
3. Fixing holes.
4. Connector pins for Lid Tamper.
5. Printed circuit board (PCB).
6. Cable entry holes for detector and keypad wiring.
7. Transformer.
8. Mains connector block. Note yellow power rating label fitted next to the connector block.
9. Cable entry hole for mains.
10. Back Tamper switch (if fitted).

Figure 2 Control Unit

**Control Unit PCB**

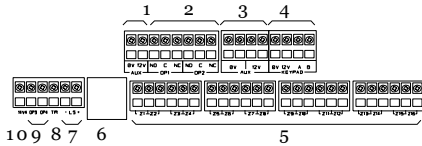


1. Aerials (**CAUTION: do not bend**).
2. Tamper connector.
3. USB socket (Mini B).
4. Ethernet link activity LEDs.



5. 20VAC input (from transformer).
6. Battery connector.
7. Kick Start pins.
8. Ethernet socket.
9. "Heartbeat" LED
10. RS485 terminator.
11. Reset Codes pins.
12. Plug by output connector pins 13-16.
13. Plug by output connector pins 1 to 12.
14. Plug on Comms activity LED.
15. Sockets for plug on module.

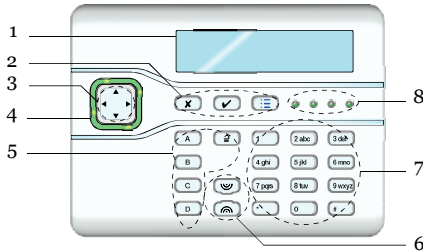
Figure 3 Control Unit Printed Circuit Board



1. Aux power.
2. Outputs (relay).
3. Aux power.
4. Keypad bus.
5. Wired zone connectors.
6. Ethernet connector.
7. Loudspeaker.
8. Wired siren tamper return.
9. Outputs (transistorised).
10. 14.4V Siren supply (not used in UK).

Figure 4 Control Unit Main Connectors

**i-KP01 Controls and Displays**



1. LCD display (2 x 20 characters).
2. Programming keys.
3. Navigation keys
4. Alert LEDs
5. Setting and unsetting keys.
6. Panic Alarm (PA) keys.
7. Number/text keys.
8. Set/Unset LEDs.

Figure 5 Controls and Displays

**Opening the i-kp01**

Note: For EN50131-3:2009, 8.7 the keypad is a type B ACE, fixed.

To open the keypad first gently prise off the trim on the front and remove the two screws. Next, carefully lever the front of the keypad (containing the pcb and display) away from the keypad rear housing.

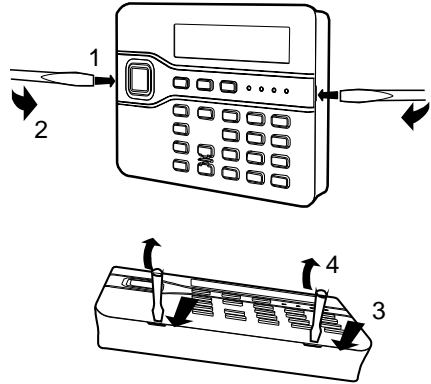
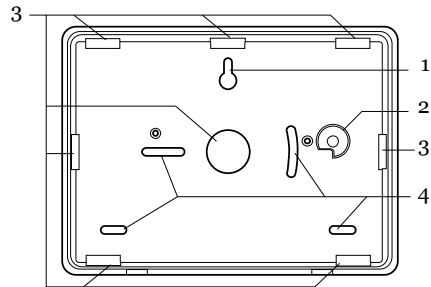
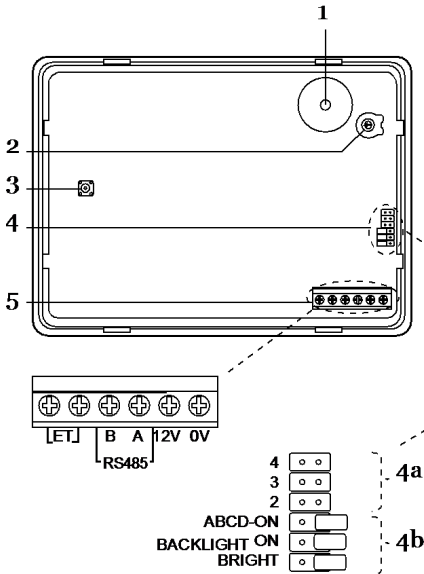


Figure 6 Opening the Keypad



1. Central keyhole.
2. Rear tamper shroud.
3. Cable entry.
4. Fixing holes.

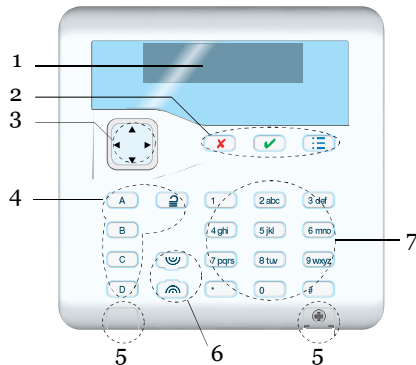
Figure 7 Keypad Rear Housing



1. Sounder.
2. Sounder volume control.
3. Tamper switch.
4. Jumpers for addressing and LED function:
  - 4a Addressing
  - 4b LED functions
5. RS485 termination jumper
6. Connector for control unit (note that the ET terminals are inactive).

Figure 8 Keypad PCB

**KEY-K01 and KEY-KPZ01 Controls and Displays**



1. LCD display
2. Programming keys.
3. Navigation keys. This key has built-in alert LEDs.

4. Setting and unsetting keys. The ABCD keys have built-in status LEDs that can show the setting status of a part setting system. These LEDs can be disabled, see page 12.
5. Plastic caps covering screws (shown closed and open).
6. Hold Up Alarm (HUA) keys.
7. Number/text keys.

Figure 9 KEY-K01/KP01/KPZ01 Controls and Displays

**Opening the KEY-K01/KP01/KPZ01**

To open the unit, unclip the caps covering the screws on the front. (You may need to gently push the bottom edge of the caps in with the end of a small screwdriver to start them.) Remove the two screws hidden underneath (see Figure 9). Gently swing the lower side of the front out from the back box by about 10mm and then slide the front upwards to disengage the top catches. (Be careful not to pull the lower side of the front more than about 25mm away from the back while the top catches are engaged, or you may break the catches.)

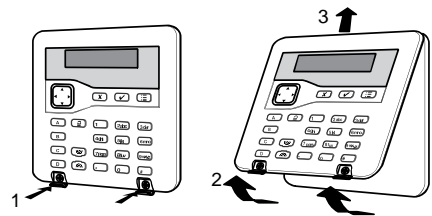
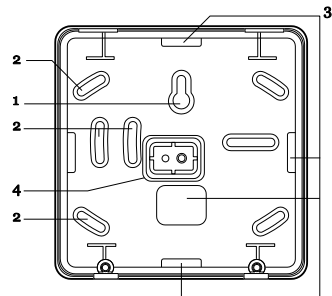
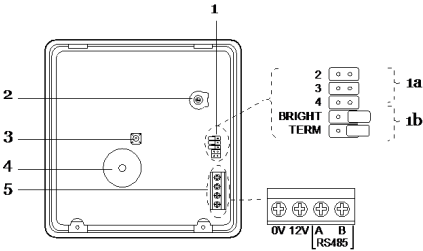


Figure 10 Opening the Keypad



1. Central keyhole.
2. Fixing holes.
3. Cable entry.
4. Tamper block

Figure 11 Keypad Rear Housing



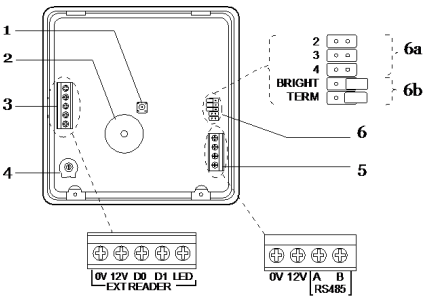
1. Jumpers for addressing and LED function:

1a Addressing

1b LED functions and RS485 terminate

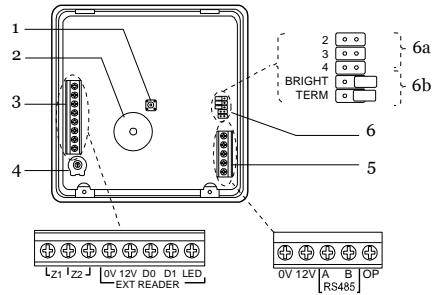
2. Sounder volume control.
3. Tamper switch.
4. Sounder.
5. Connector for control unit.

Figure 12 KEY-K01 Keypad PCB



1. Tamper switch.
2. Sounder.
3. Connector for KEY-EP.
4. Sounder volume control.
5. Connector for control unit bus.
6. Jumpers for:
  - 6a Addressing (not used in i-onEX control units).
  - 6b LED functions and RS485 bus termination.

Figure 13 KEY-KP01 Keypad PCB



1. Tamper switch.
2. Sounder.
3. Connector for KEY-EP. Terminals for zones
4. Sounder volume control
5. Connector for data bus and output terminal.
6. Jumpers for addressing and LED function:
  - 6a Addressing
  - 6b LED functions and RS485 terminate

Figure 14 KEY-KPZ01 Keypad PCB

## **Power Availability**

Before connecting any external devices to the control unit, you must make sure that the control unit can provide sufficient current to power the system during a mains failure for the time required to meet Grade 2 PD6662 or EN50131-1. The standard requires 12 hour standby, which includes two periods of 15 mins in alarm.

The amount of current available from the control unit depends on the battery fitted. The current taken by the control unit PCB, communicator and keypads is given in Technical Specifications on page 26.

For example: in an alarm system with an i-on40 control unit, two i-kp01 keypads, and 15 wired PIRs the system takes the following total quiescent current:

<b>Device</b>	<b>Current</b>
Control unit PCB	130mA
15 x PIRs at 15mA each	225mA
i-sd02 communicator (quiescent)	20mA
2 x i-kp01 at 30mA each (backlights off)	60mA
Siren (quiescent)	25mA
Total	460mA

During an alarm, these figures become:

<b>Device</b>	<b>Current</b>
Control unit PCB	220mA
15 x PIRs at 15mA each	225mA
i-sd02 communicator	50mA
2 x i-kp01 at 30mA each (backlights off)	60mA
Ext Siren & Strobe	400mA
Total	955mA

The total amp hours required =

$$(0.460A \times 11.5h) + (0.955A \times 0.5h) = 5.77Ah$$

A fully charged 7Ah battery can provide this amount of charge.

In this example a 7Ah battery should exceed the Grade 2 requirements.

*Note: All current drawn from the Aux terminals (12V and 14.4V) must be included in the overall calculation.*

## 3. Installation

### Exposure to Radio Frequency Radiation

The radiated output power of this device is below those levels considered safe by European exposure limits. Nevertheless, when fitting the product place it in such a manner as to minimise the potential for human contact during normal operation. To minimise exposure, users should be more than 200 mm from the device during normal operation

### **Step 1. Fit the Control Unit Case**

#### **Caution: Static Electricity**

Like many other electronic products, the control unit contains components that are sensitive to static electricity. Try not to handle the PCB directly. If you must handle the PCB, take the standard precautions against damage by static electricity.

#### **Fitting**

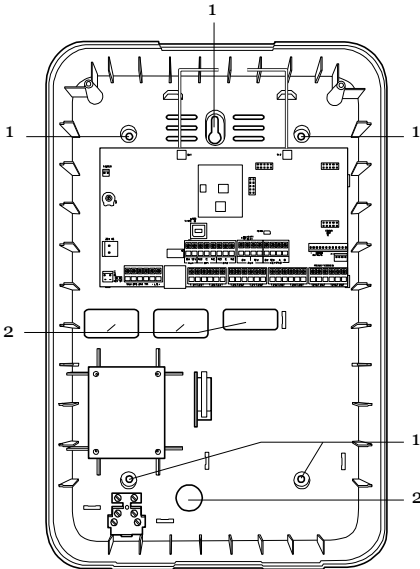


Figure 15 Fixing Holes and Cable Entries

1. Fixing holes.

2. Cable entries.

To prevent access to the inside of the control unit, you must mount the back of the control unit on a wall, using at least four fixing holes. Use No10/M5 countersunk screws at least 36mm long. Figure 15 shows the fixing holes and cable entries.

Protect the unit from dust and drilling debris when drilling the fixing holes.

#### **Installing the Lid/Back Tamper**

Fit and connect the combined lid/back tamper (provided). Ensure that the switch is oriented as shown in Figure 16.

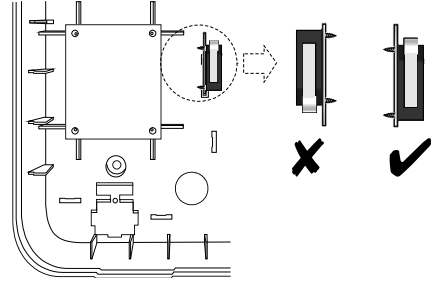


Figure 16 Lid/Back Tamper

Item 2 in Figure 3 shows the connector for the lid/back tamper.

### **Step 2. Fit and Connect the Keypad(s)**

*Note: If you are installing a keypad that was previously used on an i-onEX system, then make sure you default the keypad address BEFORE attaching it to the i-on40. See page 11 for detailed instructions.*

#### **Siting the Keypad(s)**

##### **Do site the keypad(s):**

Within the area protected by the alarm system.

At a convenient height and location for the user.

Out of sight of potential intruders.

##### **Do NOT site the keypad(s):**

Next to electronic equipment, particularly computers, photocopiers or other radio equipment, CAT 5 data lines or industrial mains equipment.

Where the cable run from the control unit will be longer than 100m (see Cable Configuration and Length).

*Note: Do not fit any keypad with an internal prox reader closer than one meter to any other type of prox reader. This includes other keypads with prox readers, external prox readers such as the KEY-EP, or prox readers used by other systems (for example access control systems). If you mount prox readers closer together than one meter (including on the other side of walls) then the two prox readers will interfere and may not work correctly.*

**Fitting Keypads**

Select which cable entry you are going to use and break out the appropriate plastic sections.

Use 4mm x 25mm countersunk screws with a thread suitable for the wall material in at least three fixing holes when mounting the back of the keypad on the wall.

**i-KP01**

For i-KP01 keypads on Grade 3 systems drill out the hole for the back tamper using a 7mm bit (see Figure 17).

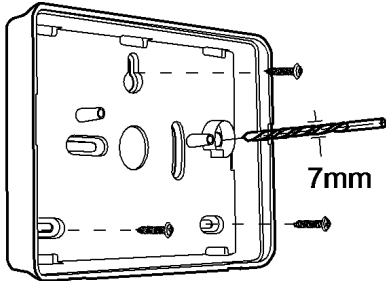


Figure 17 Screw i-KP01 Back Box to Wall

**KEY-K01/KP01/KPZ01**

Make sure the backplate is level and mark, drill and plug at least three fixing holes. Screw the backplate to the wall through the fixing holes using the M4 screws.

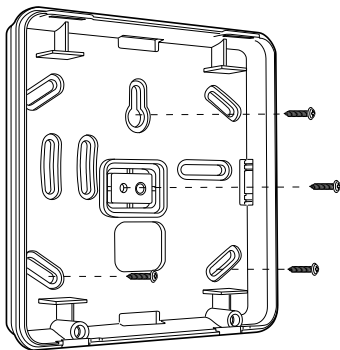


Figure 18 Screw KEY-K01/KP01/KPZ01 Back Box to Wall

**Connecting Keypads to Control Unit**

**Cable Type**

In general, the control unit requires standard 7/0.2 un-screened four core alarm cable for wiring to keypads.

For maximum performance in harsh environments use twisted pair cable with a characteristic impedance of 100-120ohms eg: CAT5 or cable designed for RS485.

Use one pair for data bus A & B. Use the other pair for 12V & 0V. For optimum performance the voltage at the keypad should be greater than 12V.

Screened cable may prove necessary if the installation site has equipment that produces high levels of R.F. (Radio Frequencies), for example welding equipment. If screened cable is required, you should keep to the following guidelines:

1. Avoid earth loops by connecting the screen on the cable to mains earth at the control unit but not at the keypad.
2. The continuity of the cable screen is most important and screens MUST be continuous along the full length of the cable.
3. If the cable enters any metal enclosure, ensure the screen is isolated from the case.

**Cable Segregation**

Segregate the keypad cabling from any other wiring, such as mains supply cables, telephone cables, computer network cables and R.F. cables. Use cable ties to keep cables separated.

Keep the keypad cable clear of cables supplying sounders or extension loudspeakers.

**Cable Configuration and Length**

You can connect up to four wired keypads to the control unit. You may connect the keypads either in daisy chain (serially), or in star (parallel) configuration at the control unit connector.

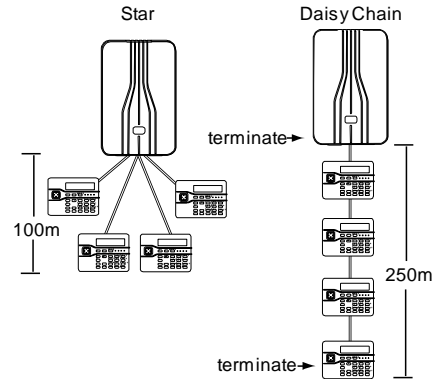


Figure 19 Keypad Wiring Configurations

For star configurations the cable length from control unit to the most distant keypad should not exceed 100m. For a daisy chain configuration the total cable length should not exceed 250m.

**Connection**

Figure 20 shows the wiring connections at the keypad and control unit.

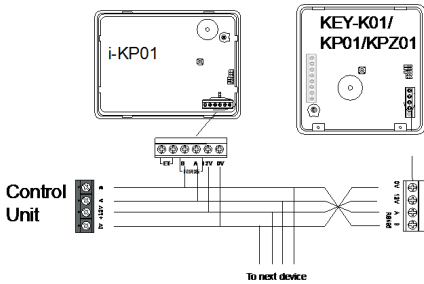


Figure 20 Keypad Connection

**Termination**

The i-on40 data bus uses the RS485 interface. Because of this the ends of the line in some configurations may be terminated to improve performance in electrically noisy environments or where there are long cable runs. Both control panel and keypads have a termination link on their PCBs (see 10 in Fig 3 for the control unit and 5 in Fig 8, 1b in Fig 12 and 6b in Fig 14 for the keypads). Fitting a jumper to the pins adds a termination to the cable.

In a daisy chain configuration terminate each end of the chain (see Fig 19 ).

In a star configuration:

If there are only two keypads then this is the same as a daisy chain configuration. If required terminate at each keypad.

If there are more than two keypads AND two cables are long while the remaining keypad cables are short (less than 10m) then it is possible to terminate at the two keypads with long cables.

If there are more than two keypads BUT each keypad cable is more than 10m then **DO NOT** terminate.

**Keypad Addressing**

Each keypad connected to an control unit must have a unique address. See Figures 8, 12 or 14 for the position of the addressing jumpers.

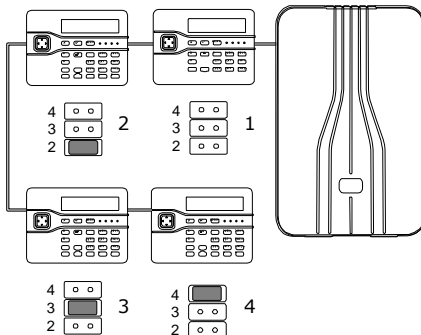


Figure 21 Keypad Addressing Jumpers

To add a wired keypad to the bus of an existing i-on40 installation, first remove all power from the control unit, both mains and battery. Make sure the address link on the new keypad is not fitted in the same position as any of the address links on keypads already connected to the control unit. Connect the new keypad and then apply power to the system.

**Re-using a V2.0 Keypad From an i-onEX**

If you wish to use a keypad that has previously been working on an i-onEX system, then you must first default the keypad address. Eaton's Security Business recommends that you do this by deleting the keypad from the i-onEX system using the Installer Menu. However, if this is not possible then you must default the keypad address manually as follows:



1. Remove the power and data connections from the keypad to the system bus.
2. Open the keypad and make sure that the keypad tamper switch is open. (It must stay open until step 9.)
3. Apply 12Vdc power to the 0V and 12V terminals on the keypad connector. **DO NOT** use the i-on40 bus for this. The navigation key LEDs flash rapidly.
4. Hold down keys D and X at the same time. After a few seconds you should hear a confirmation tone and the navigation LEDs start flashing about once per second.
5. Release the D and X keys.
6. Remove the 12V dc power from the keypad.
7. Select an address for the keypad by placing a jumper on the appropriate address pins (see Figure 21).
8. Connect the new keypad (see Figure 20).
9. Close the keypad and ensure that the tamper switch is closed.

**Backlight Control I-KP01**

You can control the appearance of the keypad backlights and set/unset LEDs by fitting links over the appropriate jumpers on the keypad PCB (see Figure 8 on page 6 for the position of the jumpers).

The jumpers have the following functions:

ABCD-ON <input type="checkbox"/>	The set/unset LEDs are disabled.
ABCD-ON <input checked="" type="checkbox"/>	The set/unset LEDs shows the setting status of the system. (Full set is the left hand LED.) See Note on next page.
BACKLIGHT ON <input type="checkbox"/> BRIGHT <input checked="" type="checkbox"/>	The key backlights are disabled. They will

		glow briefly for five seconds when a user presses a key.
BACKLIGHT ON BRIGHT		The key backlights glow all the time at normal intensity.
BACKLIGHT ON BRIGHT		The keypad backlights glow all the time, extra bright.

Note: To comply with PD6662:2010 at Grade 2 disable the ABCD LEDs

**Backlight Control for KEY-K01/KP01/KPZ01**

You can control the brightness of the keypad backlights by fitting links over the BRIGHT jumper on the keypad pcb (see 1b in Figure 12 or 6b in Figure 13 and 14).

- Jumper OFF The keypad backlights glow at normal intensity.
- Jumper ON The keypad backlights glow extra bright.

To program the backlights on or off see below.

**Programming Backlight, ABCD LEDs and Navigation Key LEDs**

You can set the function of the backlights in either of two ways:

- a) Use the *Installer Menu – Detectors/Devices – Wired Keypads – Edit Keypad – (Keypad n) – Backlight* option. See the Engineering Guide for more details.
- b) Enter a local keypad programming mode (this replaces the use of jumpers on the keypad PCB in the i-kp01).

In addition, the local keypad programming mode allows you to enable or disable the LEDs in the ABCD keys and the Navigation key.

It is possible to enter keypad programming mode when the keypad is not connected to a control unit, but simply powered by 12VDC connected to the keypad bus terminal (see Figures 12 and 14). If the keypad IS connected to a control unit then make sure that the control unit is in Installer Menu before entering the keypad's local programming mode.

**Entering Local Programming Mode**

1. Apply 12Vdc to the keypad.
2. Enter Installer Menu on the control unit, if the keypad is connected to a system.
3. Open the keypad tamper.
4. Press and hold down B and  together for at least two seconds.
 

The keypad is now in local	MENU ABCD	✓
----------------------------	--------------	---

programming mode, The display shows the current status.

**To Switch ABCD LEDs ON or OFF**

1. Enter local programming mode (see above).
 

MENU ABCD	✓
--------------	---
2. Press  or  to enable or disable the ABCD LEDs. The character at the right of the display shows "X" when the LEDs are disabled and "✓" when the LEDs are enabled. For example:
 

MENU ABCD	X
--------------	---
3. Leave local programming mode and save your changes (see page 12).

**To Change Backlight Settings**

1. Enter Local Programming mode (see above)
 

MENU ABCD	✓
--------------	---
2. Press . The display shows the current status of the backlight LEDs, for example:
 

MENU BACKLIGHT	✓
-------------------	---
3. Press  repeatedly to select one of the following:
 

Backlight LEDs ON (✓).	MENU BACKLIGHT	✓
Backlight timed (X).	MENU BACKLIGHT	X

The backlight will glow for 12 seconds after the last keypress. The action of the backlight depends on the programming of the control unit (which must have Release 3 software or higher installed).
4. Leave local programming mode and save your changes (see below).

**To Disable/Enable the Status OK LED**

1. Enter Local Programming mode.
 

MENU ABCD	✓
--------------	---
2. Press  repeatedly until the display shows:
 

MENU STATUS OK LED	✓
-----------------------	---
3. Press  repeatedly to select one of the following:
 

Status OK LED ON (✓).	MENU STATUS OK LED	✓
Status OK LED OFF (X).	MENU STATUS OK LED	X

The green status LED



under the navigation key will glow for 20 seconds after the last press (this may be useful when the keypad is placed in bedrooms that should be completely dark at night).

- 4. Leave local programming mode and save your changes.

**To Disable/Enable the Status Fault LED**

- 1. Enter Local Programming mode. MENU ABCD ✓
- 2. Press ▼ repeatedly until the display shows: MENU STATUS FLT LED ✓
- 3. Press ► repeatedly to select one of the following:
  - Status Fault LED ON (✓). MENU STATUS FLT LED ✓
  - Status Fault LED OFF (✗). MENU STATUS FLT LED ✗

The red Fault LED under the navigation key is disabled, and will not glow for any fault reports.
- 4. Leave local programming mode and save your changes (see below).

**To Leave Local Programming Mode and Save Changes**

**EITHER:**

Press ✓

**OR**

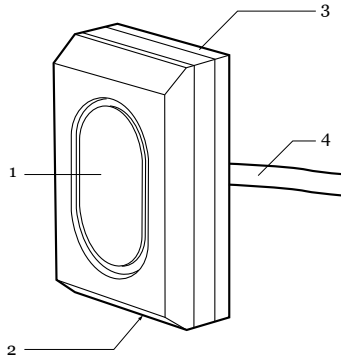
Close the keypad tamper.

The keypad saves the changes you have made in its local memory.

You can now remove 12V/dc power, if required, or leave Installer Menu on the control unit.

**KEY-EP External Prox Reader**

Figure 22 shows the outside details of the external prox reader KEY-EP used by the KEY-KPZ01:



- 1. LED window.
  - 2. Retaining Screw.
  - 3. Removable Fixing Plate.
  - 4. Permanently attached cable.
- Figure 22 External Prox Reader KEY-EP

**Siting the External Prox Reader**

Do site the External Prox Reader:

- At a convenient height and location for the user.
- Out of sight of potential intruders.

Note that the external prox reader is fitted with a length of 2m of the appropriate cable. The cable can be extended up to 50m by connecting an additional length of 7/0.2 un-screened alarm cable.

Do NOT site the External Prox Reader:

- Next to electronic equipment, particularly computers, photocopiers or other radio equipment, CAT 5 data lines or industrial mains equipment.

*Note: Do not site the external prox reader closer than one meter to any other kind of prox reader (for example an i-kp01, KEY-KPZ01 or another external prox reader). If you do so then the prox readers will interfere and be unable to read tags.*

**Opening the External Prox Reader**

To open the external prox reader (see Figure 23):

- 1. Undo the single retaining screw.
- 2. Tilt the edge of the fixing plate and then slide it a short distance parallel to the body of the prox reader.
- 3. Slide the fixing plate away from the reader body, along the cable.

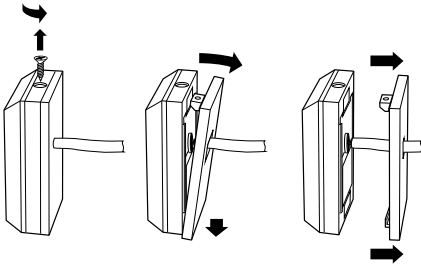
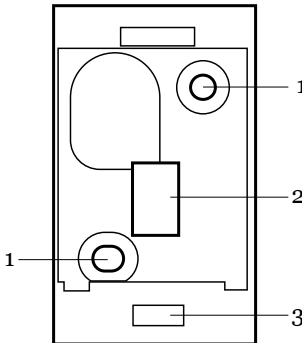


Figure 23 Opening External Prox Reader

Figure 24 shows the details of the external prox reader backplate:



1. Fixing hole.
2. Cable entry.
3. Anchor for retaining screw.

Figure 24 External Prox Reader Fixing Plate

**Fit External Prox Reader**

Use M4 25mm countersunk screws at both fixing holes when mounting the back of the keypad on the wall. Ensure the screw has a thread suitable for the wall material.

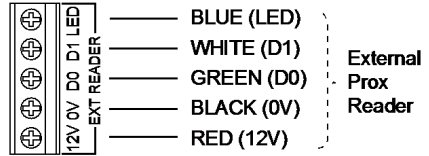
**Connecting Remote Prox Reader to Keypad**

Segregate the external prox reader cable from any other wiring such as mains supply cables, telephone cables, computer network cables and R.F. cables. Use cable ties to keep cables separated.

Keep the prox reader cable clear of cables supplying sounders or extension loudspeakers.

Figure 25 shows the wiring connections at the keypad.

**KEY-KPZ01/KP01**

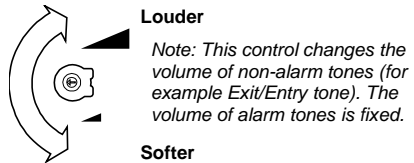


**Note: Do not connect the YELLOW wire as buzzer control is not available.**

Figure 25 Connecting the External Prox Reader

**Tone Volume – All Keypads**

To alter the volume of non-alarm tones from the keypad adjust the keypad sounder volume control (2 in Figures 8 and 12, and 4 in Figure 14):



**Step 3. Connect Control Unit to Mains**

**WARNING:** ENSURE THAT THE MAIN SUPPLY IS DISCONNECTED AND ISOLATED BEFORE MAKING ANY MAINS CONNECTIONS. All mains electrical connections must be carried out by a qualified electrician and must comply with the current local regulations (e.g. IEE).

**Mains Cabling**

Make sure that the mains supply cable does not run vertically behind the aerials within the control unit case.

If you wish run mains cable through the side of the case, make sure that they are horizontal for the last metre before entering the case.

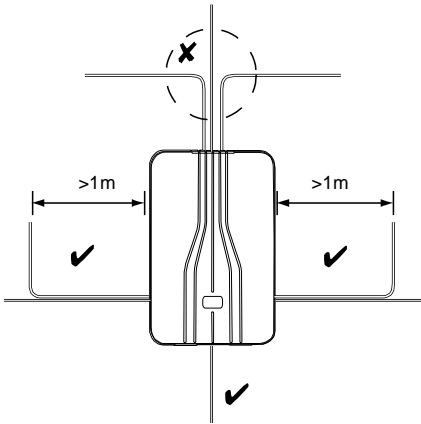


Figure 26 Mains Cabling Clearance

*Note: To avoid mains interference, the mains cable must enter the control unit through its own cable entry hole ( 9 in Fig 2) and must not be mixed with other cables.*

**Mains Connection**

Figure 27 shows the mains connection. Connect to a suitable supply using a double pole disconnect (isolation) device in accordance with EN60950-1.

**Caution:** Do not apply power at this point.

Anchor the mains cable with a strain-relief tie. There is a eye located near the mains cable entry hole for this purpose.

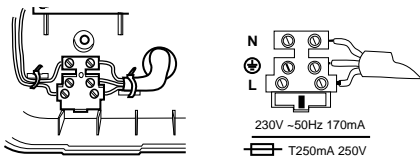


Figure 27 Mains Connection

**Step 4. Connect Wired Zones**

**Four Wire Closed Circuit Connections**

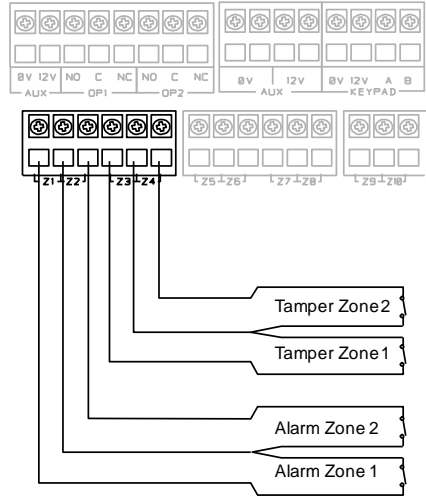


Figure 28 Closed Circuit Loop Zone Wiring

**Two-Wire Closed Circuit Connections**

With version 4.02 software you can connect two-wire CCL detectors to each pair of zone terminals. To specify the zone wiring type use the *Installer Menu – System Options – Wire Zone Type – Panel Zones* option and select “2-wire CC”.

If required you can use one pair of zone terminals as a common tamper, provided you program that zone with the type “Tamper” from the Installer Menu.

**Fully Supervised Loop Connections**

Figure 29 shows the wiring connections for Fully Supervised Loop zones. Note that the resistance values shown are examples.

The allowed values for Alarm Contact/End of Line are: 4k7/2k2, 1k0/1k0, 2k2/2k2, or 4k7/4k7.

Use the same pair of values for ALL FSL wired zone circuits.

When programming select the correspondings value in *Installer Menu - System Options - Wired Zone Type*.

If you wish to connect two or more detectors to a FSL zone, the diagram at the bottom of Figure 29 shows the connections required.

Figure 30 shows an example of wiring double doors with two door contacts to one FSL zone. Each door contact is a reed switch, connected between the outer terminals. The inner (shaded) terminal is not connected, and provides a spare terminal.

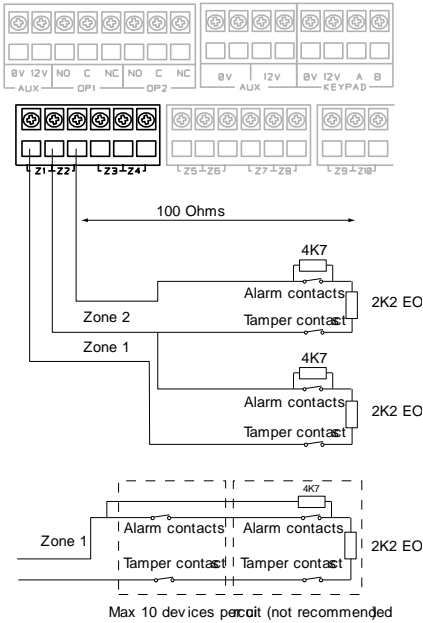


Figure 29 Fully Supervised Loop Zone Wiring

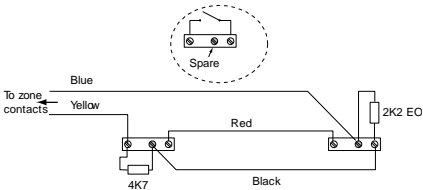


Figure 30 Example: Wiring Two Door Contacts to One FSL Zone.

Figure 31 shows an example of wiring a trouble/masking output using the “3-resistor method”. Note that you must use 2k2 and 4k7 resistors as shown. Other values will not work (See *System Options – Masking* in the i-on Engineering Guide).

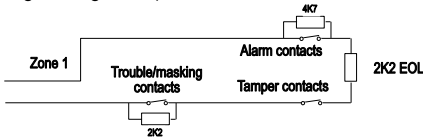


Figure 31 Example: Wiring a Trouble/Masking Zone, 3 Resistor Method.

**Connecting Wired Zones on KEY-KPZ01 only**

The KEY-KPZ01 provides terminals for up to two zones. You must enable the zones from the *Installer Menu – Detectors/Devices – Wired Keypads – Edit Keypad (keypad number) – Zones*.

Once the zones are enabled they occupy the zone numbers at the top of the numbering range, depending on the address of the keypad.

Keypad zone	Panel zone FSL	Panel Zone CCL
Keypad 1 Zone 1	39	39 Alarm
Keypad 1 Zone 2	40	39 Tamper
Keypad 2 Zone 1	37	37 Alarm
Keypad 2 Zone 2	38	37 Tamper
Keypad 3 Zone 1	35	35 Alarm
Keypad 3 Zone 2	36	35 Tamper
Keypad 4 Zone 1	33	33 Alarm
Keypad 4 Zone 2	34	33 Tamper

To select the wiring type for the keypad zones use *Installer Menu - System Options - Wired Zone Type – All Zones*. Alternatively, to select the wiring type for an individual keypad, use *Installer Menu – Detectors/Devices – Wired Keypads – Edit Keypad (keypad number) – Wired Zone Type*.

Figure 32 shows the wiring connections for FSL zones on a KEY-KPZ01. Note that the resistance values shown are examples.

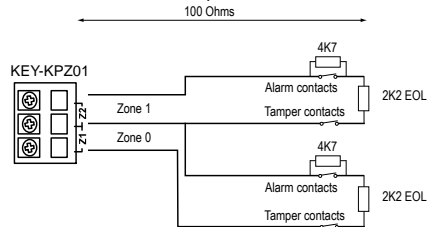


Figure 32 Wiring FSL Zones on KEY-KPZ01

Figure 33 shows the wiring connections for Closed Circuit Loop connections to the zones on a KEY-KPZ01.

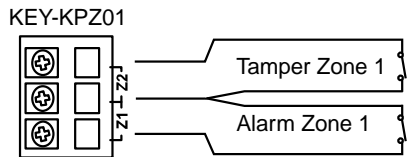


Figure 33 KEY-KPZ01 CCL Zone Wiring

## Step 5. Connect Wired Peripherals

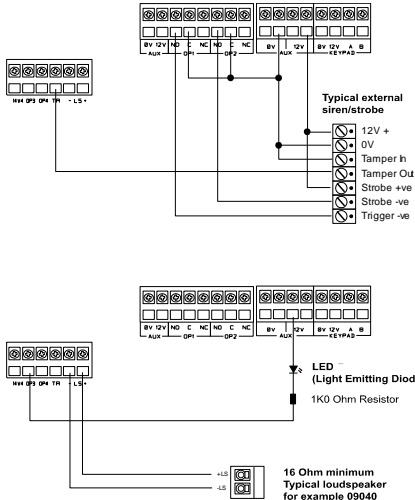


Figure 34 Connecting Wired Peripherals

The control unit PCB provides four connectors for wired outputs. Outputs 1 and 2 are voltage free relay outputs. Outputs 3 and 4 are driven by transistors, and are capable of sinking a maximum 500mA when active. By default outputs 3 and 4 are 0V when active, +12V when inactive. If you wish to reverse the polarity of these two outputs use *Installer Menu - Outputs - Wired Outputs - Output 3(4) - Polarity*.

### Remote Loudspeaker (Optional)

If you wish to add a 16 Ohm wired Loudspeaker unit, then connect it as shown in Figure 34. The control unit provides connections for one loudspeaker. Do not connect another loudspeaker in parallel. You may connect another loudspeaker in **series**, but this will decrease the maximum volume from the speakers.

*Note: Loudspeakers are not warning devices as described by EN50131-4. Although loudspeakers may mimic alarm tones, they also give alert tones and other progress tones when setting and unsetting the alarm system.*

### Wired External Sounders (Optional)

Wired external sounders differ in their methods of connection. Figure 34 shows an example of a general method of using the outputs to connect a wired sounder.

It is possible to program the TR terminal on the control unit (see item 8 in Figure 4) as either CC or FSL. Use *Installer Menu - System Options - Panel Tamper Rtn*. By default the terminal is CC. If you

program the TR terminal as FSL then make sure you connect a 2k2 resistor in series with the wire to the sounder.

*Note: If you do not wish to connect a wired external sounder then leave TR programmed as CC and make sure you link TR to 0V on the control unit. This prevents the control unit reporting Bell Tamper unnecessarily.*

### Wired Outputs (Optional)

Figure 34 shows an example of using the wired outputs to drive an indicator LED.

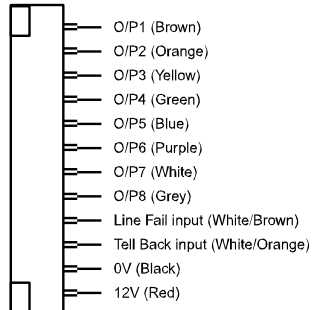
### Output on KEY-KPZ01

The output on a KEY-KPZ01 is not available for use with an i-on40.

## Step 6. Fit a Plug-By Communicator

The control unit can be connected to a separate communicator or speech dialler (for example, the Scantronic 8400, 8440, 660 or RedCare STU). Figure 35 shows the connections provided by the communications wiring harness.

Com Connector Ca ble, Part number 48521 0



Com Connector Ca ble, Part number 1196005 8

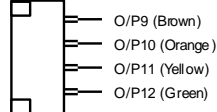


Figure 35 Plug-By Communicator Wiring

*Note: Comms O/P4 will be active when the system is unset. This is normal.*

To fit a communicator, follow the instructions below.

**Caution: Follow the instructions in the order shown, or you may damage the control unit and/or communicator.**

1. Disconnect mains power, remove the case lid, and disconnect the battery from the control unit if the system has already been installed.
2. Make any necessary connections from the communicator to the communication wiring harness. The default is a 12V positive voltage when the output is inactive.  
Refer to the next section if you are using a dual-path communicator.
3. Plug the Communication Wiring Harness onto the communications connector on the main PCB.

If the system has already been installed:

4. Re-connect the battery.
5. Fit the case lid.
6. Apply mains power.
7. Test communicator operation.

#### Line Fail Input

This input is designed to allow a plug by communicator to indicate to the control unit that the communications link has failed. The communicator should have an output capable of applying +12V to the Line Fail input while a line fault is present and 0V when the fault is absent.

#### Tell Back Input

This input is designed to allow a plug by communicator to indicate to the control unit that the user can reset the system after a system tamper. The communicator should have an output that, when triggered remotely, can apply +12V for at least 100ms to the input. See "Remote Reset (Redcare Reset)" in the i-on Engineering Guide for more information.

#### Line Monitoring for a Dual-Path Communicator

If a standalone dual-path (landline and mobile) communication device, such as a RedCARE STU, is connected to the plug-by connector, you need to do the following to obtain correct line fault reporting (this is not necessary if you are using a plug-on module):

1. Wire a panel output programmed as type "ATS Test" to the ATS Test input of the communicator.
2. Wire the Line Fault output of the communicator to the Line Fault input of the plug-by connector. The communicator must provide +12Vdc to indicate a line fault (for example, if the Line Fault output at the communicator uses a relay, connect the common terminal of the relay to +12Vdc and the normally-open terminal to the Line Fault input of the plug-by connector).

The panel will generate an "ATE L.F. Single" alert if only one of the networks is not available, or "ATE L.F. All" if both networks are not available.

## **Step 7. Fit and Connect Battery**

Fit a 7Ah Lead Acid battery into the battery compartment in the bottom of the control unit, see Figure 36.

Make sure that you secure the battery to the case with the strap provided. Connect the battery leads, red to the positive, black to the negative terminals of the battery.

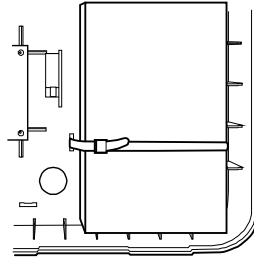


Figure 36 Fitting the Battery

*Note: Connecting the battery without mains power will not start the system. (See "Programming A Control Unit Before Installation" below if you wish to start the system on battery power.)*

#### **Programming Before Installation**

If you prefer, you can make the control unit learn the detectors and other peripherals before installing the system in its final location. You will need to temporarily connect a keypad to the control unit.

It is possible to operate the control unit from battery power (or a 12Vdc supply) without connecting the unit to a mains supply. However, in order to start the control unit processor running you must briefly short the Kick Start pins together after connecting the battery.

When programming the system while it is running on battery only, remember to leave the Installer Menu before removing power. If you do not do so all your changes will be lost, see *Important! Saving Changes* on page 21

If you wish to program the control unit from a laptop or PC you can do this by connecting the control unit to your PC via Ethernet. You will need a CAT 5 patch cable and a laptop or PC with a standard web browser. See the separate publication *i-on40 Web Server Set Up Guide* for instructions on how to set up your PC/laptop and the control unit.

## **Step 8. Initial Power-Up**

**WARNING:** During initial power-up all the keypad sounders and any internal loudspeaker MAY give

an alarm tone. If you are working at the top of a ladder make sure that the sudden noise does not startle you and cause a fall.

1. Apply battery then mains power to the control unit.

The keypads and internal sounder may give an alarm tone. The heartbeat LED (see fig 3) starts flashing.

**(If you are installing a UK version please go to step 6.)**

The display initially shows:

```
Language?
English
```

2. Press ▲ or ▼ to show other languages on the bottom line of the display, for example:

```
Language?
Nederlands
```

3. Press ✓ to select the language you wish to use.

From this point on, the display operates in the selected language. If you want to change the language later use *Installer Menu - System Options - Language*.

The display shows:

```
COUNTRY DEFAULTS
*UK
```

4. Press ▲ or ▼ to show other countries, for example:

```
COUNTRY DEFAULTS
Italy
```

5. Press ✓ to select the country you want.

The display shows:

```
A : Partition mode
B : Part set mode
```

6. Press A or B to select either a partitioned system or a Part Setting system.

*Note: To change to Partition or Part Set mode at a later date you will have restore factory defaults.*

The display shows:

```
Load Profile?
```

7. Either: Press ✓ to load the Profile.

Or: Press ✕ to start with a blank system

*Note: The Profile may not be EN50131 compliant. (The factory default is EN50131 compliant.)*

The control unit loads your choice of profile, and then shows:

```
WIRED_ZONE_TYPE
*2-wire FSL 2k2/4k7
```

8. Press ▲ or ▼ to show the range of wiring types available, for example:

```
WIRED_ZONE_TYPE
4-wire CC
```

9. Press ✓ to select the wiring type you intend to use for the wired zones

The display shows:

```
INSTALLER_EXIT_FLTS
Panel lid open
```

Note that the alert LEDs around or built-into the navigation key glow red. This is because the control unit lid is off and the tamper is active.

10. Press ✕.

The display shows:

```
INSTALLER_MENU
Detectors/Devices
```

11. Place a temporary link over the lid tamper.

*Note: Remember to remove the link before finishing the installation.*

12. Press ✕ to leave Installer Mode.

*Note 1: It is necessary to leave Installer Menu at this stage in order to make sure that the control unit will learn radio zones successfully during commissioning.*

*Note 2: If you do not have a suitable link to disable the lid tamper, then you can simply remove all power (mains and battery) from the control unit, and then re-apply power to the control unit.*

At this point you can carry on to commission the system. See the next page.

*Note: You can set the time and date from within the Installer Menu by using System Options – Set Time & Date.*

## **Step 9. Commission the System**

After installing the control unit you should commission the alarm system as follows:

1. Use the Installer Menu (see Chapter 4) to teach the control unit the identity of its radio detectors and any other peripherals. See the installation instructions supplied with each detector or peripheral.
2. Install detectors and peripherals at their selected locations.
3. Use the *Installer Menu – Test* option to:
  - a) carry out a walk test of the detectors.
  - b) test the operation of any other peripherals.
4. Program the system to suit user requirements. See the *i-on Range Engineering Guide* for a detailed description of the Installer Menu.
5. Assemble and close the control unit:
  - a) Hook the lid of the control unit into the bottom of the case.
  - b) Close the lid and then tighten the two fixing screws.

*NOTE: It is possible, for convenience, to place links over tamper contacts to inhibit tamper alarm during installation. Because of this feature make sure you test all lid tampers before completing installations, to ensure that no links are left fitted.*

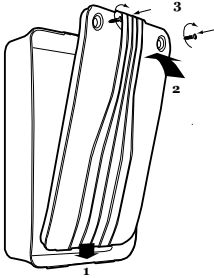


Figure 37 Replacing the control unit lid.

6. Leave the Installer Menu.
 

The red LEDs should go out, and the rim of the navigation keys glow green. The system is now ready to hand over to the user.
7. Instruct the user on how to operate the system. See the *i-on Range Administrator's Guide*. If necessary, show them how to set the time and date on the system.
 

Remember to leave the *i-on Range Administrator's Guide* with the user.



## 4. Programming

This section is summary of the Installer Menu on the i-on40. Please see the *i-on Range Engineering Guide* for a more detailed description.

### Entering the Installer Menu

1. Make sure the system is unset and showing the standby screen (time and date).
2. Key in the Installer access code. When delivered from the factory the default Installer access code is "7890". The default user code is "1234".

As you start to key in the code the display shows:

```
Enter Access Code:
(*)
```

When you key in the last digit of the Installer access code the display shows:

```
User Code Required
()
```

Notes:

1. You will see this screen the first time you enter the Installer menu on a new control unit, or if you have restored Factory Defaults. You can disable this feature by using the Installer menu option System Options - User Access – User Code Required.
2. If you set User Code Required to NO then the control unit no longer complies with EN50131. This option complies with BS8243 only if the user has given written consent.
3. If you key in an access code incorrectly, the display shows four "stars". Key in the code again. If you key in a total of four incorrect codes then the system locks you out for 90 seconds.

3. Key in the default user code (see Note below).

The display shows:

```
Installer Menu
Detectors/Devices >
```

4. Press ▲ or ▼ to display more items from the menu.

Each item appears on the bottom line of the display in turn, for example:

```
Installer Menu
Outputs >
```

5. Press ✓ to select that item of the menu.

The option you selected now appears on the top line. If there are any sub-options for that selection, then the first of them appears on the bottom line, for example:

```
Outputs
Edit Outputs >
```

You can press ▲ or ▼ to display the other sub-options.

### Leaving the Installer Menu

If you wish to leave the Installer Menu at any time.

1. Press ✕ until the display shows the words "Leave installer mode?".

```
Leave
installer mode?
```

2. Press ✓ to leave Installer menu. (Press ✕ if you do not want to leave the menu.)

The display shows the time and date.

```
i-on40
12:00 02/01/2008
```

The system is ready for use.

Note: If you attempt to leave the Installer Menu when a detector tamper is active then the keypad displays a fault message telling you which

detector is causing the problem. Press ✕ to return to the Installer Menu. You must either close the detector tamper or delete it from the system before you can leave the Installer Menu.

### Important!

### Saving Changes

When you make changes to the Installer Menu the control unit holds those changes in temporary memory until you leave the Installer Menu. As you leave the Installer Menu the control unit writes those changes into a permanent store. If you remove all power BEFORE you leave the Installer Menu then the control unit will lose your changes. Note that this does not apply if you restore Factory Defaults, that change takes place immediately.

### Restoring Access Codes

If the user and/or Installer codes are lost then you must restore all user information to its factory defaults. All prox tags, remotes and radio HUDs will be deleted.

1. If possible, enter the Installer menu.

Note: If you cannot enter Installer Menu then the control unit will start a tamper alarm when you open the control unit lid.

2. Remove mains power, then open the case and disconnect the battery.

Note: This procedure will not work if the control unit lid tamper remains closed.

3. Identify the Reset Codes pins on the main PCB (see Figure 3).
4. Short the Reset Codes pins together using a screwdriver or jumper link. (Keep the short on until step 6.)
5. Apply mains power.

The control unit loads the factory default access codes:  
 User 1: 1234, Installer: 7890.

(All other users have been deleted.)

After a short pause the keypad display shows the time and date. The red LEDs glow to show an alert that the panel lid is open. **The sounders operate.**

6. Remove the short from the Reset Codes pins.
7. Reconnect the battery.
8. Close the control unit lid (to restore the tamper switch).
9. Key in the Master User code, 1234, to silence the sirens.

The LEDs around the navigation glow red to show an alert for a tamper and a missing battery.

Press ✓ twice to (if necessary) acknowledge any alerts.

To force the control unit to check the battery:

10. Enter Installer Menu and then leave it again. The navigation key LEDs should now glow green.

*Note: The log is protected and cannot be erased by the Installer.*

## **Restoring Factory Defaults**

If you wish to restore all factory default options then:

1. From the Installer Menu select *System Options – Restore Defaults – Factory Defaults*.  
 The display asks for confirmation.
2. Press ✓ to load defaults.  
 (Press ✕ to go back to the Installer Menu without changing defaults.)  
 The display asks you to select Partition Mode or Part Set Mode.
3. Press A or B to select the desired mode.  
 The display asks you to select the zone wiring type.
4. Press ▲ or ▼ to display the desired wiring type on the bottom line of the display and then press ✓ to select it.  
 The system loads all defaults except for Access Codes and the Log.

The display shows:

```

Factory defaults
restored
    
```

5. Leave the Installer Menu to save the change (press ✕ until the display shows  
 "Leave Installer mode ?" then press ✓).

## Installer Menu

### 1 DETECTORS/ DEVICES

#### Detectors

- Add/Del Detectors
  - Zone 17...40
  - Delete all
- Program Zones
  - Zone 01...40
    - Name
    - Type
    - Partitions<sup>1</sup>
    - Attributes<sup>2</sup>

#### Wired Keypads

- Edit Keypad
  - Keypad 01...04
    - Name
    - Partitions<sup>1</sup>
    - Key A...D<sup>1</sup>
    - Zones<sup>20</sup>
    - Wired zone type<sup>20</sup>
    - Backlight<sup>21</sup>
    - External Prox<sup>22</sup>

#### Radio Keypads

- Add/Del Radio Keypad
- Edit Keypads<sup>3</sup>
  - Radio Keypad 01...04
    - Name
    - Partitions<sup>1</sup>
    - Key A...D<sup>1</sup>

#### External Sirens

- Add/Delete Ext. Siren
- Edit External Siren<sup>3</sup>
  - Siren 01...04
    - Name
    - Partitions

#### WAMs

- Add/Del WAM
- View WAM<sup>5</sup>

### 2 OUTPUTS

#### Radio outputs

- Add Outputs
- Edit Outputs
  - Output 01...08
    - Name
    - Type

#### Wired outputs

- Panel
  - Output 1...4
    - Name
    - Type
    - Polarity
    - Pulsed
    - Partitions<sup>1</sup>

- Keypad<sup>20</sup>
  - Name
  - Type
  - Polarity
  - Pulsed
  - Partitions<sup>1</sup>

#### Plug-by outputs

- Output 1...12
  - Name
  - Type
  - Polarity
  - Pulsed
  - Partitions<sup>1</sup>

### 3 SETTING OPTIONS<sup>4</sup>

#### Full Set

- Name
- Exit mode
- Settle time<sup>5</sup>
- Exit time<sup>5</sup>
- Entry time
- Siren delay
- Siren time
- Strobe on Set
- Strobe on Unset

#### Part Set B

- Name
- Exit Mode
- Settle time<sup>5</sup>
- Exit time<sup>5</sup>
- Entry time
- Alarm Response
- Siren delay
- Siren time
- Part Set Final Exit
- Part Set Entry Route
- Strobe on Set
- Strobe on Unset
- Volume

#### Part C, D

#### (See Part Set B)

### 3 PARTITIONS<sup>1</sup>

- Partition 1...4
  - Name
  - Exit Mode
  - Settle Time<sup>5</sup>
  - Exit Time<sup>5</sup>
  - Entry Time
  - Alarm Response
  - HUA response
  - Siren delay
  - Siren time
  - Strobe on Set
  - Strobe on Unset
  - Part Set Exit Mode
  - Part Set Settle Time<sup>5</sup>
  - Part Set Exit Time<sup>5</sup>
  - Part Set Entry Time
  - Part Set Alarm Resp.
  - Part set siren delay
  - Part set siren time
  - Part Set Final Exit
  - Part Set Entry Route
  - Part Set Strobe Set
  - Part Set Strobe Unset

#### Partition 2...4

#### Full Set Link

### 4 SYSTEM OPTIONS

#### Wired Zone type

#### User Access

- HUA keys active
- Quick Set
- Quick Omit
- User code reqd
- 2 Way Replies
- 2 Way Set Instant
- Duress Enable

#### User reset

- Zone alarms<sup>7</sup>
- Zone tampers

#### System tampers

#### Confirmation (-UK)

- Confirmation Mode
  - Basic
    - DD243
    - BS8243
  - Confirmation time<sup>8</sup>
  - After entry<sup>8</sup>
  - Entry keypad lock<sup>8</sup>
  - Sounder on
  - Siren on
  - Unconfirmed reset<sup>8</sup>
  - Confirmed reset<sup>8</sup>
  - HUA Confirm Time<sup>9</sup>
  - Tamper as Tamper only<sup>9</sup>

#### Confirmation (-EUR)

- Sounder on
- Siren on

#### Profiles

#### Masking

#### Mask Override<sup>10</sup>

#### Language<sup>11</sup>

#### Restore Defaults

- Factory defaults

#### Installer name

#### Installer code

#### Keypad text

#### Remote needs Entry

#### Remote Entry PrtSt

#### RKP Needs Entry

#### RKP Entry PrtSt

#### HUA Response<sup>12</sup>

#### Auto Rearm<sup>7</sup>

#### Panel Loudspeaker

#### Entry alarm delay

#### Abort Time

#### Supervision

#### Jamming

#### Force Set

#### Tamper Omit

#### CSID Code

#### Silence Alerts

#### Mains Fail Delay

#### Set Date & Time

#### Panel Tamper Rtn

### 5 COMMUNICATIONS<sup>13</sup>

- ARC Reporting<sup>15</sup>
  - Call Mode
  - Phone book
  - IP Network<sup>15</sup>
  - Account Numbers
  - Report Type
  - Fast Format channels<sup>16</sup>
  - CID/SIA Events<sup>17</sup>
  - Restorals
  - Burg Comms Rearm<sup>14</sup>
  - 21CN FF Ack time<sup>16</sup>
  - Send tamper as burg<sup>17</sup>
  - Dynamic Test Call<sup>18</sup>
  - Static Test Call<sup>19</sup>
  - Unset Comms
- Speech Dialler<sup>13</sup>
  - Call Mode
  - Messages
  - Phone Book
  - Triggers
  - Destinations

#### Call Acknowledge

#### SMS<sup>13</sup>

- Call Mode
- Messages
- Phone Book
- Triggers
- PSTN SMS<sup>13</sup>

#### Line Fail Response<sup>13</sup>

#### Line Fail Delay<sup>13</sup>

#### IP Network (Own)

- Web Server
  - Status
  - Port Number
  - VKP Instant<sup>23</sup>

#### Downloader

- IP Address
- Subnet Mask
- Gateway Address

#### GPRS<sup>13</sup>

#### Ethernet<sup>13</sup>

#### Downloading

- Account
- Connection Type
- Rings to Answer<sup>13</sup>
- Answer on one ring<sup>13</sup>
- Access Mode
- Phone Book<sup>13</sup>
- IP Network
- Secure Callback<sup>13</sup>
- Modem Baud Rate<sup>13</sup>

#### Plug-by

### 6 TEST

#### Sirens & Sounders

#### Wired Keypad

#### Radio Keypads

#### Walk Test

#### Zone Resistances

#### Signal Strengths

- Detectors
- Radio Keypads
- External Sirens
- WAMs

#### Outputs

- Radio Outputs
- Wired Outputs
- Plug-by outputs

#### Remotes

#### User HUAs

#### Prox Tags

#### ARC Reporting<sup>13</sup>

#### Speech Dialler<sup>13</sup>

#### PSU Current

### 7 VIEW LOG

#### All Events

#### Mandatory Events

#### Non-Mandatory Events

### 8 ABOUT

#### Panel

#### Keypads

#### Comms

- Module<sup>13</sup>

#### Panel Ethernet

- <sup>1</sup> Appears only in a Partitioned system (or when zones have a type other than "Not Used").
- <sup>2</sup> Appears when zone is given a type other than "Not Used".
- <sup>3</sup> Appears only when device learned in.
- <sup>4</sup> Appears only in a Level Setting system.
- <sup>5</sup> Appears only if Exit Mode is "Final Door" "Lock Set" or "Exit Terminate".
- <sup>6</sup> Appears only if Exit Mode is "Timed Set" or "Silent Set".
- <sup>7</sup> Appears only when System Options – Confirmation Mode is "Basic".
- <sup>8</sup> Appears only if System Options – Confirmation Mode is either "DD243" or "BS8243".
- <sup>9</sup> Appears only if System Options – Confirmation Mode is "BS8243".
- <sup>10</sup> Appears only when Masking is ON.
- <sup>11</sup> Appears only in EUR version.
- <sup>12</sup> Appears in this position only in part setting systems.
- <sup>13</sup> Appears only when communications module fitted.
- <sup>14</sup> Appears only when Report Type = Fast Format AND Confirmation Mode = Basic
- <sup>15</sup> Options visible depend on communications module fitted.
- <sup>16</sup> Appears only when Report Type=Fast Format.
- <sup>17</sup> Appears when Report Type=CID or SIA
- <sup>18</sup> Appears only when Static Test Call is disabled.
- <sup>19</sup> Appears only when Dynamic Test Call is disabled.
- <sup>20</sup> Appears only for KEY-KPZ01 keypads
- <sup>21</sup> Appears for KEY-K01, KEY-KP01 and KEY-KPZ01.
- <sup>22</sup> Appears for KEY-KP01 and KEY-KPZ01.
- <sup>23</sup> Appears only when Web Server is enabled.

---

## 5. Maintenance

---

The control unit should be inspected once per year. At each inspection:

Check the control unit for obvious signs of damage to the case or its lid.

Check the action of the back tamper.

Check the condition of the control unit standby battery.

Check the cabling to the keypad(s) for signs of damage or wear.

Check the keypads for obvious signs of damage.

Test the action of all buttons on all keypads.

Clean the keypad surface and display. To clean the keypad wipe the surface with a clean soft dry cloth. Do not use water, solvents or any proprietary cleaning materials.

Monitor the signal strength and battery condition of all detectors, radio keypads, remote controls, PAs and radio sounders.

Test each device. Replace batteries as recommended by the manufacturer's instructions.

Gently clean the lenses of any PIRs with a clean, soft dry cloth. Do not use water, solvents or any proprietary cleaning materials.

Walk test all detectors.

Test any external sounders and strobes.

### **Replacing or Removing Wired Keypads**

If you need to remove or replace a wired keypad from the system at any point then you must follow the correct procedure:

1. Enter the Installer menu and remove all power from the system, both mains and battery.
2. Disconnect the keypad from the control unit. At this point, if you are simply removing the keypad go to step 7.
3. Make a record of the keypad's jumper settings.

*Note: This step is important in order to retain any options you have programmed for the keypad.*

4. Take the new keypad and fit jumpers in the same pattern as used on the keypad have just removed.
5. Connect the new keypad.
6. Apply power to the system, both mains and battery.
7. Leave the Installer Menu.

By following this procedure the control unit should retain all programming options for the replaced keypad.

## 6. Technical Specification

### General

Product name	i-on40.
Product Description	40 zone hybrid endstation with remote keypads.
Manufacturer	Eaton's Security Business.
Environmental Class	Class II.
Operating temperature	Tested -10 to +55°C.
Humidity	0 to 93% RH, non-condensing.
Case material	ABS LG-AF342.

### Dimensions:

Control unit	384 x 245x94, mm HxWxD.
KP01	115x156x34, mm HxWxD
KEY-K01/KP01/KPZ01	128x128x29, mm HxWxD

### Weight:

Control unit	2.2 kg (without stand-by battery).
i-KP01	0.26 kg
KEY-K01	0.19 kg
KEY-KP01	0.19 kg
KEY-KPZ01	0.19 kg

### Capacities

Zones	16 wired, 24 radio
Keypads	4 wired, 4 radio
Outputs	16 wired (comprising two voltage free contacts, 14 transistorised of which 12 are provided on separate wiring harnesses). 8 radio output channels.
Internal Clock	±10 minutes over one year (depending on the accuracy of the mains supply frequency).
Remote controls	50
Panic Alarms	50
External Radio Sirens	4
Plug on communication modules	One only
WAMs	4
Log capacity	Up to 1,000 events: 750 mandatory events, 250 non-mandatory. Stored in EEPROM memory, available for at least 10 years without power.

### Security

Security Grade	Grade 2.
Radio detector differs	16,777,214 (2 <sup>24</sup> - 2).
Radio Supervision	Programmable.
Number of	50 plus installer

access codes	
Access code differs	10,000 differs. 4 digit codes, all four digits may be any number 0 to 9.
Code blocking	Blocked for 90s after four incorrect codes (or prox tags) in series. Blocked for a further 90s after each additional incorrect code or prox tag, until next correct code or prox tag entered.
Proximity tag differs	4,294,967,296 (2 <sup>32</sup> )

### Radio

Radio Section	Operating frequency 868.6625MHz Narrowband. EN 300 220-3. EN 300 330-2
Transmitter range	The range of the transmitters compatible with this control unit depends on the environment in which they are installed. As a guideline, most transmitters will work up 200m range in free space conditions.

### Power Supply

Integrated power supply. Monitoring includes mains fail, battery low voltage, aux output low voltage, battery failure.

Power supply type:	A
Mains power supply requirements:	230VAC +10%/-15%, 170mA max, 50Hz
Total power supply capacity:	1.5A
Aux power supply:	1.1A capability
14.4V output:	300mA capability
Comms power supply:	500mA capability
Keypad bus power supply rated output:	500mA capability

*Note: Under EN50131-6 the maximum total load that can be drawn from these outputs is 270mA i.e. the aux current that can be supplied for 12hrs by a 7 A-h battery under normal operating conditions.*

### EN50131-6 ratings:

PSU rated output:	270mA max
Independent power outputs (Normal operating conditions):	Total not to exceed 270mA for 7 Ah battery
CIE power requirement:	130mA min. 220mA max
i-kp01 power requirement:	30mA (normal/idle) 45mA (backlight low) 65mA (backlight high)
KEY-KPZ01/KP01/K01 power requirement	35mA backlight OFF, internal prox reader only. 65mA max backlight ON, external prox reader

	connected
Battery charging requirement:	270mA
Plug-on Communicator power requirement:	i-sd02, i-dig02: 20mA quiescent 50mA max
Plug-on Communicator power requirement:	i-gsm02: 150mA quiescent and max.
12V Aux output voltage range:	9±0.5V to 13.8V
14.4V output voltage range:	9±0.5V to 14.7V
Max p-to-p ripple voltage:	0.5V
Standby Battery:	12V, 7Ah sealed lead acid.
Max recharge time to 80% capacity:	Less than 72 hours.
'Low battery' fault at:	< 12V
Aux power output fault at:	< 9V
Deep discharge protection at:	9±0.5V
Serviceable components:	Mains fuse: 250mA (T)
Standby time:	See "Power Availability" on page 6.

## **Electromagnetic Compatibility**

Immunity	Conforms to EN50130-4.
Emissions	Conforms to EN61000-6-3.

## **Outputs**

O/P 1 - 2	Voltage free, single pole relay contacts rated 24VDC @ 1A.
O/P 3 - 4	Open collector transistor, +12VDC when inactive, 0V when active. 500mA max.
Plug-by O/Ps 1...12	Open collector transistor +12VDC when inactive, 0V when active, 50mA max.
LS (loudspeaker)	Min impedance 16 Ohm, current consumption from 12VAux = 280mA in alarm.
KEY-KPZ01 Outputs	Open collector transistor, +12VDC when inactive, 0V when active, 500mA max.

## **Fuses**

The control unit has a replaceable T250mA mains fuse.

## **Electrical Safety**

Conforms to EN60950-1.

## **Other**

If you wish to connect the i-on40 control unit to a PC using either the Ethernet or the USB port then make sure that the cables have the following specifications:

Ethernet	Cat5e patch cable, RJ45 male plugs at each end, suitable for 10/100Base-T.
USB	Mini-B plug for control unit end, USB-A for PC end. Max length 3m.

## **Compliance Statements**

This product is suitable for use in systems designed to comply with PD 6662: 2010 at grade 2 and environmental class II.

This product complies with the requirements of EN50131-3 at grade 2 and environmental class II.

This product complies with the requirements of EN50131-6:2008 at grade 2 and environmental class II.

When fitted with an i-sd02 this equipment is compliant with EN 50136-1. It allows the alarm transmission system to meet the performance requirements of EN 50131-1:2006 ATS 2 provided that:

- a) It is installed in accordance with the installation instructions.
- b) The connected PSTN is functioning normally.

When fitted with an i-sd02 this product provides options A, B and C at Grade 2 as noted in Table 10 of EN50131-1:2006+A1:2009.

*If the installer selects a non-compliant configuration then they must remove or adjust compliance labelling*

Third party approval carried out by ANPI.

## **Compatible Equipment**

### **HUD**

705rEUR-00	Two button HUD (single channel, top button is disabled)
706rEUR-00	Two button HUD/tilt switch transmitter
710rEUR-00	Two button HUD
726rEUR-50	Long range hand held HUD
726rEUR-60	Short range hand held HUD

### **Detectors**

713rEUR-00	Pet tolerant PIR
714rEUR-00	PIR Transmitter (Small case)
720rEUR-00	Smoke Detector Transmitter
734rEUR-00/01	CC/FSL Door Contact Transmitter (white)
734rEUR-05/06	CC/FSL Door Contact Transmitter (brown)
738rEUR-00/04	Spyder shock sensor (white/brown)
739rEUR-50	Sentrol glass break detector
DET-RDCS	Combined door contact shock sensor transmitter
xcelr	Radio PIR
xcelrpt	Pet tolerant radio PIR
xcelw	Wired PIR
xcelwpt	Pet tolerant wired PIR

### **Sounders**

760ES	External Wireless sounder
9040UK-00	Speaker boxed

### **Setting / Unsetting – Keypads**

i-rk01	Radio Keypad
i-kp01	Keypad (with internal prox reader, but without zones or external prox reader)
key-ep	External prox reader for KEY-KPZ01/KP01
KEY-K01	keypad
KEY-KP01	keypad with internal prox reader and terminals for external prox reader
KEY-KPZ01	keypad, with internal prox reader, two zones, one output and terminals for external prox reader

### **Setting / Unsetting - Fobs**

FOB-2W-4B	Two-way keyfob
i-fb01	Four button remote control
727rEUR-00	Four button remote control with encrypted code (HUD)



function not compatible with  
BS8243 or DD243)

**Communicators**

i-dig02	PSTN Communication (ARC only).
i-gsm02	GSM communications module
i-sd02	PSTN Communication module with speech dialling

**Accessories**

703rEUR-00	4-channel (2 zone) transmitter
762rEUR-00	Two Channel Receiver
768rEUR-50	Eight Channel Receiver
770rEUR-00	Wireless Accessory Module
771rEUR-00	Info Module
i-rc01	Relay Card

**NOTES:**

*i-on40*

**NOTES:**

[www.coopersecurity.co.uk](http://www.coopersecurity.co.uk)  
Product Support (UK) Tel: +44 (0) 1594 541978.  
Available between:  
08:30 to 17:00 Monday to Friday.  
Product Support Fax: (01594) 545401  
email: [techsupport@coopersecurity.co.uk](mailto:techsupport@coopersecurity.co.uk)  
Part Number 12435160

21/1/2014