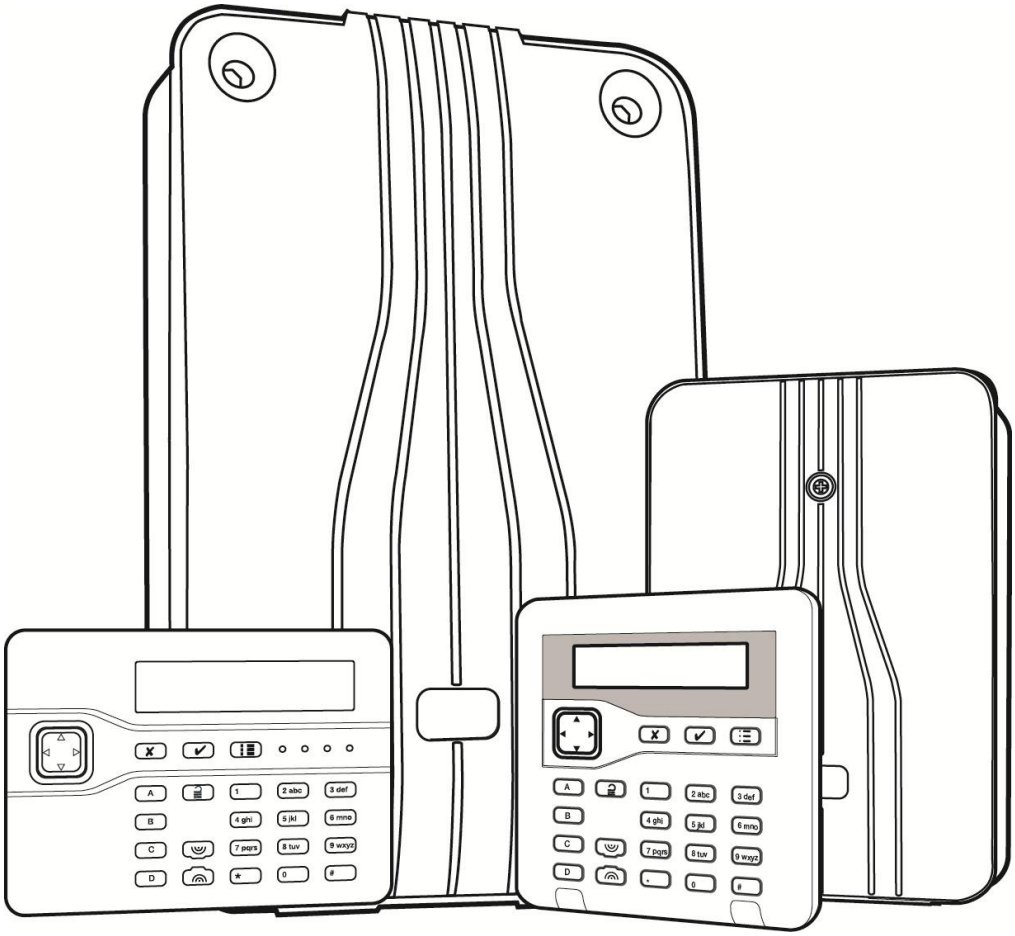
i-on Next Generation
Security System

Engineering Guide



Issue 1

Control unit software version 5.0

Powering Business Worldwide

About this Guide

This guide is a document for people who need to install or configure an i-on "Next Generation" intrusion system. The guide provides:

- Information about the capabilities of the i-on control units.
- Installation advice.
- Detailed information about options in the Installer menu.

Detailed connection information is provided in the installation instructions provided with each device.

Other Publications

The following additional publications are available:

- **i-on Administrator's Guide** - Provides detailed information about how to set and unset the system, manage alarms, omit zones, set up users, test the system and carry out other administration tasks.
- **i-on Quick User Guide** - Provides an overview of how to set and unset the system for end users.
- **i-on Web Browser Interface Setup Guide** - Explains how to configure the system using the web interface.
- **SMS Command Messaging User's Guide** - Describes how end users can control the system using SMS text commands (e.g. to set or unset the system).
- Separate installation instructions for each hardware device (e.g. control unit and keypads).

Contents

Chapter 1: Introduction

Introduction to i-on Next Generation control units

The i-on "Next Generation" range of control units have been designed to satisfy the most demanding requirements of alarm-systems professionals for domestic, commercial and industrial applications. The control units are flexible, easy to install and robust, and all are suitable for wired, wirefree or hybrid alarm systems. The modular approach of the system hardware ensures that the design can be customised to match site requirements and maximise cost-efficiency. All control units are grade 2 compliant.

Table 1 specifies the features and system limits for each control unit. The number in the name of the control unit (e.g. "30" in i-on30R) indicates the total number of "on-board" wired and radio zones available using only the control unit. Additional zones are available by using expanders and other bus devices.

An "R" at the end of a control unit's name indicates on-board support for radio zones only; an "H" indicates a hybrid device that includes on-board support for both radio and wired zones. All control units are "expandable" to provide additional zones and outputs.

Summary of features

The i-on "Next Generation" range of control units feature:

- Support for a wide range of peripheral devices, including keypads, detectors, external siren/strobe units, internal sirens, network cameras and expanders.
- Grade 2 compliance.
- A bus for connection to devices such as wired keypads, expanders and base stations (for 2-way radio keypads).
- An on-board radio transceiver, which has a range of up to 500m and supports devices such as radio detectors, Eaton radio siren/strobe units and radio outputs.
- Built-in Alarms Receiving Centre (ARC) IP communicator.
- Sockets for an optional plug-on communicator (required for grade 2).
- Terminals for a plug-by communicator (depending on the control unit).
- An Ethernet port for optional use of email, network cameras, web interface, IP alarm communication and other features.
- The ability to configure the system using:
    - A standard keypad on the bus.
    - An engineer keypad connected directly to the engineer keypad port.
    - The control unit's built-in web interface via a web browser.
    - A PC that has the Downloader software and is connected to the control unit via an i-dig02 module (over PSTN), USB port or Ethernet port.
- A micro-SD card for local mass storage of images from network cameras.
- Support for multiple partitions.

- On-board outputs and wired zones (depending on the control unit).
- On-board connections for a wired siren/strobe unit.
- On-board connections for an external loudspeaker.

Table 1: Overview of features

	Feature	i-on30R	i-on40H
	EN 50131 security grade	2	2
Zones	Max on-board radio zones	30	30
	Max on-board wired zones (Note 6)	0	10
	Max zones on expanders, keypads, etc.	30	40
	Max wired and radio zones (system wide)	60	80
Bus	RS485 Buses	1	1
	Max bus devices	20	20
Outputs	Max on-board radio outputs	10	10
	On-board transistor outputs	1	1
	On-board relay outputs	0	2
	Max outputs on expanders, keypads, etc.	30	40
	On-board plug-by outputs	0	12
	On-board siren\strobe connections	Yes	Yes
	Max custom outputs	4	4
	Max outputs (system wide) (Note 5)	30	40
Ports	Ethernet port	Yes	Yes
	USB port	Yes	Yes
	On-board loudspeaker connections	1	1
	Micro SD card slot	Yes	Yes
Devices	Max wired keypads and 2-way radio keypads (Note 2)	20	20
	Max 1-way radio keypads (Note 3)	4	4
	Max external radio siren\strobe units (Note 4)	4	4
	Max internal radio sounders (Note 4)	4	4
	Max Wireless Access Modules	4	4
Case	Control unit case	Plastic	Plastic
	Batteries	1 (7Ah)	1 (7Ah)
	Power supply	1.0A	1.0A
	Combined back/lid tamper	Yes	Yes
Software	Users	30	50
	Part sets (in part set mode)	3	3
	Max partitions (see Note 1)	4	4
	Mandatory log events	750	750
	Non-mandatory log events	250	250
	Calendar set events	10	10
	Calendar set exceptions	30	30
	Max shunt groups	4	4
	Max simultaneous keypad sessions	4	4
	Web browser interface	Yes	Yes
	Auto remote diagnostics (UK only)	Yes	Yes

Note 1: Each partition has one part set within it.

Note 2: A 2-way radio keypad (KEY-RKPZ) requires a KEY-RKBS base station wired to the control unit. Up to two radio keypads can connect to the same base station, but this feature cannot be used to increase the total number of wired and 2-way radio keypads beyond the limit shown in Table 1.

Note 3: The maximum number of 1-way radio keypads (i-rk01) is in addition to the maximum number of wired and 2-way radio keypads.

Note 4: The maximum number of external radio siren/strobe units is in addition to the maximum number of internal radio sounders.

Note 5: The system-wide maximum number of outputs includes on-board radio outputs, on-board relay and transistor outputs and outputs provided by expanders, keypads and other peripherals. It does not include plug-by outputs.

Note 6: The maximum number of on-board zones is for Fully-Supervised Loop (FSL) or 2-wire Closed Circuit (CC) wiring. If 4-wire CC wiring is used, the maximum number of on-board zones is halved, unless an optional ADP-10CC board is fitted.

System architecture and supported peripherals

This section provides an introduction to the architecture of i-on intrusion systems and the peripheral devices supported.

Note: Please refer to the device installation instructions for electrical specifications.

System bus

Each control unit includes connections for a four-wire RS485 bus, which is used to connect devices such as wired keypads, expanders, remote power supplies and base stations (for 2-way radio keypads). Devices can connect to the bus using a "daisy chain" or star layout, as shown in Figure 1.

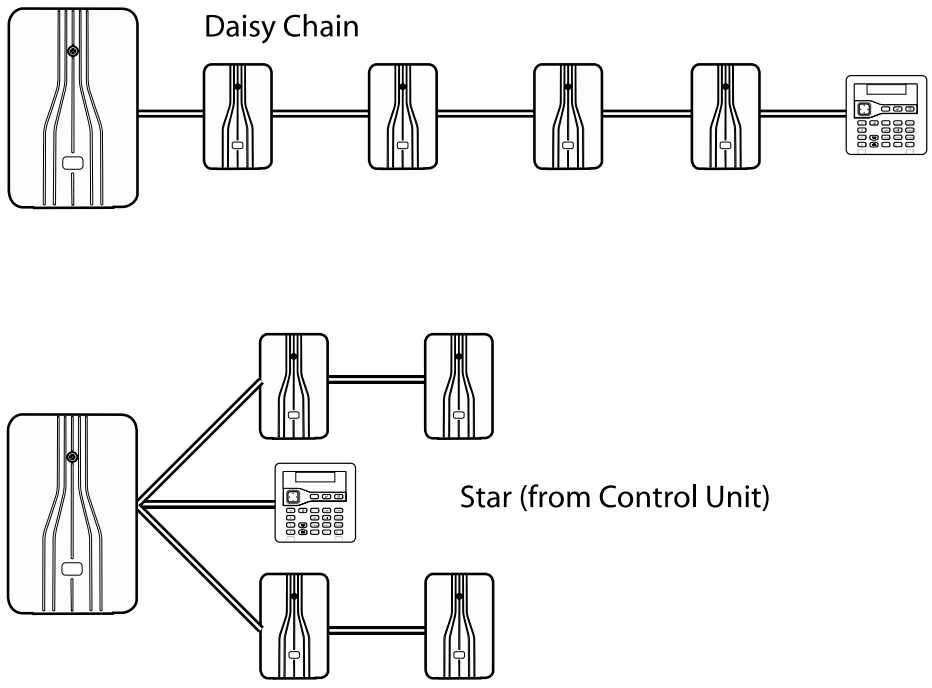


Figure 1. Daisy Chain and Star Connections

Each device on the bus has a unique address. A device obtains its address from the control unit either during the commissioning stage of a new installation, or when the installer adds the device from the Installer menu. Each device stores its address in non-volatile memory.

Part-setting and partitioned modes

An i-on control unit offers part-setting and partitioned modes:

Part-setting mode

In part-setting mode, the control unit can set in one of four ways: either full set or one of three part sets (part set B, C or D). Each zone can belong to one or more part sets (using the Part Set attribute; see page 49). When the system is full set, the control unit sets all zones, irrespective of the part set they belong to. When part set, the control unit sets only those zones that belong to the part set that you are setting.

In a part-setting system, the control unit responds to just one keypad at a time.

Partitioned mode

In partition mode, the control unit provides the equivalent of a set of smaller, independent alarm systems known as “partitions”. You can allocate any set of zones to each partition. Each partition can have a full-set level and one part-set level. During system configuration, you can allocate keypads, sirens, sounders or outputs to any of the partitions.

The fact that each zone can belong to more than one partition may produce un-expected results for users of the system. When designing a system, note that a zone will only be armed when ALL of the partitions that it belongs to are set. If a user unsets any of the partitions that a zone belongs to, the control unit will disarm the zone.

Table 1 specifies the number of partitions supported by each control unit.

For partitioned systems, users can use more than one keypad at the same time, provided that they are in separate partitions. Within each partition, the control unit responds to just one keypad at a time. The number of simultaneous keypad sessions each control unit can handle at any one time is shown in Table 1.

Keypads

Keypads connect to the bus and are used by installers to configure the system, and by users to set or unset the system. Table 1 specifies the number of keypads supported by each control unit.

There are three main types of keypad:

- **Wired keypads** – These connect to the bus. There are several different models of wired keypads that offer different styling and features.
- **Two-way radio keypads** – These communicate over a radio link to a base station, which is connected to the bus and acts as a communications bridge between the keypad and the control unit. You can use two-way radio keypads in the same way as a wired keypad to configure the system, set or unset the system, etc.
- **One-way radio keypads** – These can be used to set or unset the system and can communicate directly to a control unit that has built-in radio communications, or to a radio expander.

Features

The keypads feature:

- A two-line by 20-character backlit LCD display (not available on i-RK01).
- An illuminated four-way switch (the “navigation key”), which is used to navigate through menus (not available on i-RK01).
- LEDs behind the navigation key, which show the fault status of the system.
- A numeric keypad for entering access codes and keying in text.
- Dedicated A, B, C and D keys, which can be programmed to set individual partitions or part sets, or allocated to control outputs.
- Keys for “yes”, “no”, menu and unset functions.
- Hold-Up Alarm (HUA) keys.
- An automatic timeout from the user menu.

The keys are backlit by LEDs within the keypad.

Supported keypads

The following keypads are supported:

i-kp01	Wired keypad with built-in proximity reader. (Requires firmware v2.0 or above.)
i-RK01	One-way battery-powered radio keypad for setting/unsetting, with a built-in proximity reader.
KEY-K01	Wired keypad only.
KEY-KP01	Wired keypad, with a built-in proximity reader, and terminals for a KEY-EP external proximity reader.
KEY-KPZ01	Wired keypad, with built-in proximity reader, two on-board zones, one programmable output, and terminals for a KEY-EP external proximity reader.
KEY-RKPZ	Two-way battery-powered radio keypad, with built-in proximity reader and two on-board zones. This keypad uses a base station connected to the bus.
KEY-FKPZ	Wired flush-mount keypad, with built-in proximity reader, two on-board zones, one programmable output, terminals for an external loudspeaker, and terminals for a KEY-EP external proximity reader. The keypad is available in a range of colours and finishes.

Note: Do not install internal and external proximity readers closer than one meter to any other type of proximity reader, otherwise the devices may not work correctly.

Engineering keypad

An engineering keypad is a modified keypad that can be plugged into a dedicated connector on the control unit or on any expander. You can use an engineer keypad to configure the system, rather than a keypad on the bus. An engineer keypad does not need an address.

Before opening the control unit and plugging in an engineering keypad, enter your installer code at another standard keypad. Once you have plugged in the engineering keypad, other keypads are deactivated.

You cannot exit the Installer menu from an engineer keypad, so after you have finished, you will need to disconnect the engineer keypad and exit the Installer menu from a standard keypad.

KEY-EP external proximity tag reader

Many keypads include a proximity tag reader. The KEY-EP is an external proximity tag reader, which can connect to a keypad and allows the system to be to set or unset externally.

The KEY-EP is compatible with the KEY-KP01, KEY-KPZ01 and KEY-FKPZ keypads.

Alarm communicators

The control unit can communicate alarms externally (such as to an alarms-receiving site) using SIA IP (SIA over the network), a plug-on module or plug-by communicator (if supported by the control unit; see Table 1).

Plug-on modules supported

All control units support the following plug-on modules:

i-dig02	A PSTN module that allows the control unit to report alarm information using standard protocols such as Fast Format, SIA and Contact ID over a telephone network. This module also allows engineers to perform remote maintenance over the PSTN and sending of SMS alarm messages.
i-sd02	A speech dialler and PSTN (Public Switched Telephone Network) module that allows the control unit to send recorded speech messages and also report alarm information using standard protocols such as Fast Format, SIA and Contact ID. This module also allows remote maintenance over the PSTN and sending SMS messages.
i-gsm02	A GSM module that allows speech messaging, alarm reporting and SMS text messaging over the GSM mobile phone network. The module allows the system to be controlled using SMS text messages (e.g. to set or unset the system, or to switch outputs on or off).

Note: Using the i-gsm02 for Fast Format communications is not recommended, since the GSM network can introduce too great a variation in the delay between signal and response.

Note: Other communication modules are available from third-party manufacturers. Please contact the third-party manufacturer's support representative for further details.

Plug-by (digital communicator)

Table 1 shows the number of plug-by outputs available on each control unit. These are designed to control a separate digital communicator.

By default, the outputs are switched negative (from 12VDC to 0V) when active. You can program these outputs to be switched positive (from 0V to 12VDC) when active.

ADSL01 filter

The ADSL01 is a filter that can mount onto i-dig02 or i-sd02 plug-on modules. The ADSL01 reduces electronic noise caused by an ADSL broadband router sharing a PSTN line with a plug-on module.

Detectors (zones)

Detectors are the physical devices that detect alarm conditions. A zone is the lowest-level item within the intrusion system that can be set or unset.

Note: Although it is possible to connect detectors in series and therefore to have more than one detector in the same zone, it is not normal practice. Instead, there is normally only one detector per zone and for this reason, detectors are often referred to as "zones" within the intrusion system.

Table 1 shows the number of zones supported by each control unit.

Wired detectors

Wired detectors can connect (using standard alarm cable) to some models of control unit (see Table 1), wired expanders, some keypads and remote power supplies.

Please refer to page 14 for details of the different wiring methods you can use for wired detectors.

Note: If 4-wire CC wiring is used, this may reduce the available number of zones; see page 15.

Radio detectors

Radio detectors can communicate directly to control units that have built-in radio communications, or to radio expanders. Table 1 specifies the number of radio zones that each control unit supports.

The following radio detectors are supported:

DET-REXT-PIR30	Perimeter detector
705REUR-00	Hand-held dual-channel transmitter
706rEUR-00	10mW tilt switch and personal attack transmitter.
710rEUR-00	Dual-button personal attack transmitter
713rEUR-00	Pet-tolerant PIR
714rEUR-00	PIR
XCELR	PIR
XCELRPT	Pet-tolerant PIR
720rEUR-00	Smoke detector
DET-RSMOKE	Smoke Detector
726rEUR-50	Long-range hand-held personal attack transmitter
726rEUR-60	Short-range hand-held personal attack transmitter
734rEUR-00	CC door contact - white
734rEUR-01	FSL door contact - white
734rEUR-05	CC door contact - brown
734rEUR-06	FSL door contact - brown
738rEUR-00	Spyder shock sensor – white
738rEUR-04	Spyder shock sensor – brown
DET-RDCS	Spyder shock sensor and door contact combined

739rEUR-00	Sentrol glass-break without tamper
DET-RWATER	Flood detector
DET-RARB	Request-for-assistance button
703R	Universal transmitter

Expanders

Expanders provide additional connections for zones, outputs and loudspeakers, up to the limits specified in Table 1.

Wired expanders

Wired expanders connect directly to the bus. The EXP-W10 is supported, which provides connections for:

- Ten FSL, 4-wire CC or 2-wire CC zones.
- One wired loudspeaker.
- Four wired programmable outputs

Note: Previous-generation EXP-W10 expanders allow only five 4-wire CC zones. The new EXP-W10 is displayed as "EXP-WCC" in the menus.

Radio expanders

Radio expanders communicate directly to the control unit. EXP-R10 and EXP-R30 radio expanders are supported. The EXP-R10 provides 10 zones for radio detectors, and the EXP-R30 provides 30. Each radio expander also supports:

- Two i-rk01 one-way radio keypads.
- Two external radio sirens.
- Two internal radio sounders.
- Two Wireless Accessory Modules (WAMs).
- One wired loudspeaker.

The maximum number of expanders, detectors, keypads and WAMs on a system depends on control unit; see Table 1.

Note: The maximum number of radio detectors also depends partly on the density of radio transmitters within a given volume. Radio expanders must be at least 1 metre apart.

Outputs

Outputs allow you to program the system to control or communicate with external equipment when, for example there is an alarm in a specified zone, mains is disconnected or a combination of specified conditions occur.

The following types of output are available:

- Wired outputs. These are available on the control unit (see Table 1), expanders, some models of keypad and remote power supplies. There are two types of wired output:
    - Transistor (open collector) – By default, these are switched negative (from 12VDC to 0V) when active; you can program them to be switched positive (from 0V to 12VDC).

    - Relay – These provide voltage-free changeover contacts. You connect one side of the external device to the C (Common) terminal, and the other to either NO (Normally Open) or NC (Normally Closed) side of the relay, depending on the application.

- Radio outputs. These connect directly to a control unit that has built-in radio communications, or to a radio expander.
- Dedicated outputs on the control unit for a siren/stobe unit.
- Plug-by outputs (depending on the control unit), used for communicating alarms to an Alarms Receiving Centre (ARC).

Control unit USB and Ethernet ports

The control unit includes both USB and Ethernet ports.

You can use the USB port to:

- Program the control unit from a PC using the Downloader software (see page 23).
- Apply firmware updates to the control unit using the i-on Update Utility software. For European versions, the utility also allows alternate language text files for the keypad display to be installed.

Connecting the control unit to a network through the Ethernet port allows you to:

- Configure the control unit and update firmware using the web interface (see page 23).
- Communicate alarm information to an alarms-receiving centre using SIA-IP.
- Configure the control unit using the Downloader software (see page 23).
- Keep the time at the control unit automatically updated using an SNTP server located on the internet.
- Store images from network cameras (on the SD card).
- Send emails automatically when events occur.

Sounders

The i-on control units support external wired siren/strobe units, and internal radio sounders. Table 1 specifies the number of sounders of each type that each control unit supports.

External wired sirens/strobes

The control units have connections to drive a standard wired siren/strobe unit in Self-Activating Bell (SAB) or Self-Contained Bell (SCB) mode. Expanders also provide connectors for additional external wired sounders.

The following external wired siren/strobe units are supported:

SND-WEXT-G2	Wired Grade 2 Siren.
SND-WEXT-G3	Wired Grade 3 Siren.
Third-party units	With compatible connections.

External radio sirens/strobes

Radio siren/strobe units can communicate directly to control units that have built-in radio communications, or to radio expanders.

The following external wired siren/strobe units are supported:

760ES	External radio sounder.
SND-REXT	External radio siren/strobe unit.

Internal sounders

An internal sounder indicates alarms, entry tones, exit tones and other conditions. An internal sounder is intended for use in areas that are out of audio range of keypads, but where users need to hear system sounds.

The SND-RINT internal radio sounder is supported, which can communicate directly to control units that have built-in radio communications, or to radio expanders.

Loudspeakers

Control units, expanders and remote power supplies have connections for a loudspeaker, which you may want to use to increase the volume or location of setting and unsetting tones. The loudspeaker must have an impedance of 16 Ohms. You must not connect two loudspeakers in parallel to the same port

Cameras

You can configure the system to store images from a network camera when an alarm occurs. The following network cameras are supported:

CAM-INT-00	Internal box camera wired/Wi-Fi.
CAM-EXT-00	External bullet camera wired/Wi-Fi.

A micro-SD card is required to store the camera images.

Remote power supplies

The EXP-PSU remote power supply is supported, which provides:

- Extra power and more space for standby batteries in larger alarm systems.
- Connections for either 10 FSL zones, five 4-wire CC zones, or 10 2-wire CC zones.
- A loudspeaker output.
- Four wired programmable outputs.
- 16 plug-by outputs.

The EXP-PSU connects to the system bus (see page 18), and communicates with the control unit in the same way as a wired expander.

Remote controls

A remote control allows the system to be set or unset using a keyfob (similar to a device for locking/unlocking a vehicle).

The following devices are supported:

i-FB01	Remote control.
FOB-2W	2-Way remote control.

Other supported radio devices

The following additional radio devices are also supported

DET-RSURV01	Radio Site Survey Tool.
770REUR-00	Wireless Accessory Module (WAM).
762REUR-00	Radio receiver.
768REUR-00	Radio receiver.

Chapter 2: Planning the Installation

Choosing the installation locations

When planning the installation, consider the following recommendations concerning the locations of where to install the control unit and other devices.

Note: Also refer to the device installation instructions for any further guidance.

General requirements

Do not locate any device:

- Near to any source of electromagnetic or radio interference.
- Within 1 metre of high-voltage cables, metal pipes, computers, photocopiers, or other electrical or electronic equipment.
- In a location where maximum radio range or cable distances (see page 16) will be exceeded.
- In a metal enclosure or close to large metal structures, if the device uses radio communications.

Control unit

The control unit must be located:

- Within the protected area (but not in an entry or exit zone).
- Upright (battery at the bottom) on a wall or other flat surface (to discourage tamper attempts from the rear).
- Out of sight of potential intruders.
- Ideally, more than 2 metres from the floor.

Carry out a radio survey using the DET-RSURV01 Survey Tool to confirm that there will be sufficient signal strength between the planned location of the control unit and other radio devices.

Keypads and proximity readers

Keypads and proximity readers should be located at a convenient height.

Keypads must be within the area protected by the intrusion system and ideally out of sight of potential intruders.

Proximity readers or any keypad containing a proximity reader must not be located:

- Within 1 metre of another proximity reader (including one located within another keypad).
- Behind a door, coat rack or other covering.

External sirens

These must be located out of reach of intruders and vandals, but must be easily visible for maximum deterrence.

Checking power availability

You must make sure that:

a) The control unit's power supply will have sufficient capacity to power all connected devices. The power supply in i-on Next Generation control units is rated at 1.0A max, of which 180mA is reserved for battery charging, leaving 820mA available for the control unit's PCB and other devices.

b) The backup battery can provide sufficient power in the event of a mains failure. EN50131-1 or PD6662 Grade 2 requires the backup battery to be able to power the system for at least 12 hours, including two 15-minute periods in alarm.

When using a single 7Ah battery, the limiting factor is normally the power available from the backup battery during a mains fail.

If there is insufficient power available from the control unit or backup battery, consider the use of remote power supplies (see pages 10 and 18).

When considering the power drawn, include the control unit's PCB and all peripherals powered by the control unit, including any output devices (12V and 14.4V), plug-on/plug-by communicator, bus devices and wired detectors.

Each device's installation instructions specifies the current drawn by that device. Table 2 gives a summary of the current consumed by all i-on control unit PCBs and popular peripheral devices.

Table 2: Current Consumptions

Device	**Current Consumption**
i-on30R PCB	90mA
i-on40H PCB	110mA
i-dig02 or i-sd02 plug-on module	Quiescent: 20mA In alarm: 50mA
i-gsm02 plug-on module	150mA
Wired expander	20mA (no sounder connected)
Wired PIR	15mA
KEY-FKPZ keypad	Quiescent: 25mA In alarm: 65mA
i-kp01 keypad	Quiescent: 30/40/60mA (backlight off/on/bright respectively) In alarm: 45/45/65mA (backlight off/on/bright respectively)
KEY-KPZ01, KEY-KP01 or KEY-K01 keypad	Quiescent: 35mA (backlight off, no external proximity reader) In alarm: 65mA (backlight on, external proximity reader fitted)
KEY-RKBS two-way keypad base station	35mA (buzzer off)
SDR-WEXT external siren/strobe	Quiescent: 35mA In alarm: 225mA

Worked example

The following shows a simplified example of checking power availability.

Device	Current
Control unit PCB (i-on30R)	90mA
i-dig02 at 20mA	20mA
10 x PIRs at 15mA each	150mA
1 x wired expanders	20mA
2 x KEY_FKPZ at 25mA each (backlights off)	50mA
Siren (quiescent)	35mA
Total	365mA

During an alarm, the current consumptions are:

Device	Current
Control unit PCB (i-on30R)	90mA
i-dig02 at 50mA	50mA
10 x PIRs at 15mA each	150mA
1 x wired expanders	20mA
2 x KEY_FKPZ at 65mA each (in alarm)	130mA
Siren (in alarm)	225mA
Total	665mA

Since the control unit's power supply can provide 820mA, the above shows that the power supply is able to power the system during an alarm (665mA).

The total amp-hours required for the battery for Grade 2 is:

(0.365A x 11.5h) + (0.665A x 0.5h) = 4.53Ah

A fully-charged, 7Ah battery can provide the charge required by the above example to meet Grade 2 requirements.

Detector (zone) wiring types

Before installation, you need to choose the wiring type (method) to use for any wired detectors: Fully-Supervised Loop (FSL), 4-wire Closed Circuit (CC), or 2-wire CC, as described below.

The latest EXP-W10 wired expander allows you to mix FSL and 4-wire CC on the same expander. Other devices, including the control unit itself, require you to use the same wiring type for all wired detectors connected to the same device.

You will need to ensure that all detectors are wired correctly and that you select the default wiring type during the initial power-up procedure (page 20). If necessary, you can edit the wiring type for individual devices.

The wiring types are as follows.

Fully Supervised Loop (FSL)

This uses a single pair of wires for each detector, with resistors at the end of the line and across the alarm contact (Figure 2). The resistors allow the system to monitor for short-circuit or open-circuit conditions to guard against cable tampering.

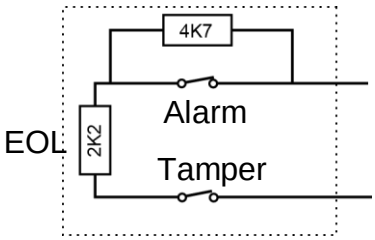


Figure 2. FSL Connections (using 2k2 and 4k7 resistors)

The End-of-Line (EOL) and alarm contact resistors can be any of the following values (respectively): 2k2 and 4k7, 1k and 1k, 2k2 and 2k2, or 4k7 and 4k7. The resistance bands for FSL are as shown in Table 3.

Table 3: FSL Resistor Bands (without Masking)

Zone State	**2k2/4k7 FSL**	**1k/1k FSL**	**2k2/2k2 FSL**	**4k7/4k7 FSL**
Tamper	0k0 – 1k759	0k0 - 0k799	0k0 – 1k759	0k0 – 3k759
Normal	1k76 – 4k08	0k8 - 1k4	1k76 - 3k08	3k76 - 6k58
Alarm	4k081 – 8k28	1k401 - 2k4	3k081 - 5k28	6k581 - 11k28
Tamper	> 8k28	>2k4	>5k28	>11k28

If a detector is able to report masking, connect the detector as shown in Figure 3. The detector must signal masking by closing both the Alarm and Fault contacts together. If the detector closes the Fault contact only, the control unit reports this as a detector fault.

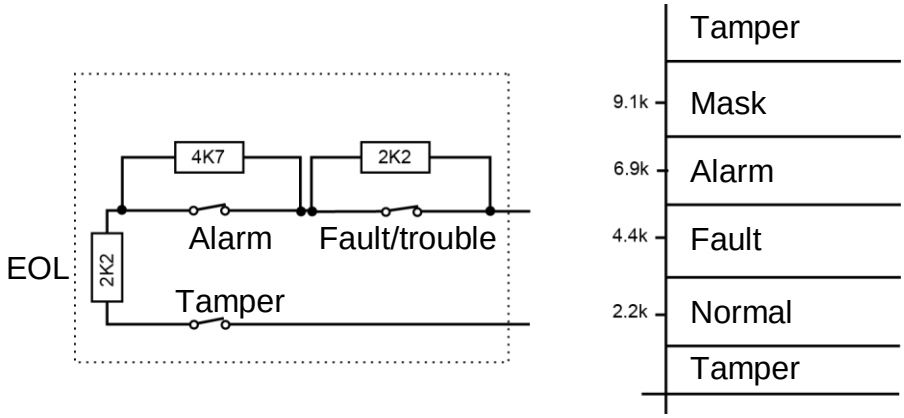


Figure 3. FSL Connections with Masking

4-wire CC

This uses a separate pair of wires for the alarm and tamper contacts. No end-of-line resistors are used. Selecting 4-wire CC may halve the maximum number of wired zones the device supports, as shown in Table 4.

An ADP-10CC board can be fitted to the control unit to convert the ten FSL zones (if available) to ten 4-wire CC zones. Without the board fitted, the control unit supports five 4-wire CC zones. If you are using an ADP-10CC board, select 2-wire FSL 2k2/4k7 as the wiring type.

Table 4: 4-Wire CC Zones

Equipment	FSL or 2-wire CC	4-wire CC
Panel with 10 on-board zones	10 zones	5 zones
EXP-PSU and original EXP-W10	10 zones	5 zones
EXP-WCC and new EXP-W10	10 zones	10 zones
Keypad with 2 on-board zones	2 zones	1 zone

2-wire CC

This uses a single pair of wires for each detector. No end-of-line resistors are used.

Checking cable requirements

Normally, the control unit requires standard 7/0.2 un-screened 4-core alarm cable for wiring to bus devices. Use one pair for data lines A and B. Use the other pair for 12V and 0V.

Screened cable

For maximum performance in environments where there is electromagnetic noise, use twisted-pair screened cable with a characteristic impedance of 100-120 Ohms, such as Belden 8132 or cable designed for RS485.

If screened cable is required:

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

Cable segregation

Segregate the bus cabling from any other wiring, such as mains cables, telephone cables, computer network cables and R.F. cables.

Keep the bus cable clear of cables supplying sounders, extension loudspeakers or any other high-current devices.

Cable configuration and length

You can connect devices either in daisy chain (serially), or in star (parallel) configuration at the control unit connector (Figure 4). For star configurations, the cable length from control unit to the most distant bus device should be kept short, and should not exceed 100m. There should be no more than four arms in the star.

For a daisy-chain configuration, the total cable length should not exceed 1,000m.

Note that if there are only two arms in a star configuration, this is equivalent to a daisy-chain configuration.

Bus termination

In some cases, the ends of the bus may need to be terminated to improve performance in electrically noisy environments or where there are long cable runs. The control unit and bus devices have a termination link on their PCB. Fitting a jumper to the link adds a termination to the cable.

In a daisy-chain configuration, fit the termination jumpers in the devices at each end of the chain. In a star configuration, terminate at the two devices on the ends of the longest cables (Figure 4).

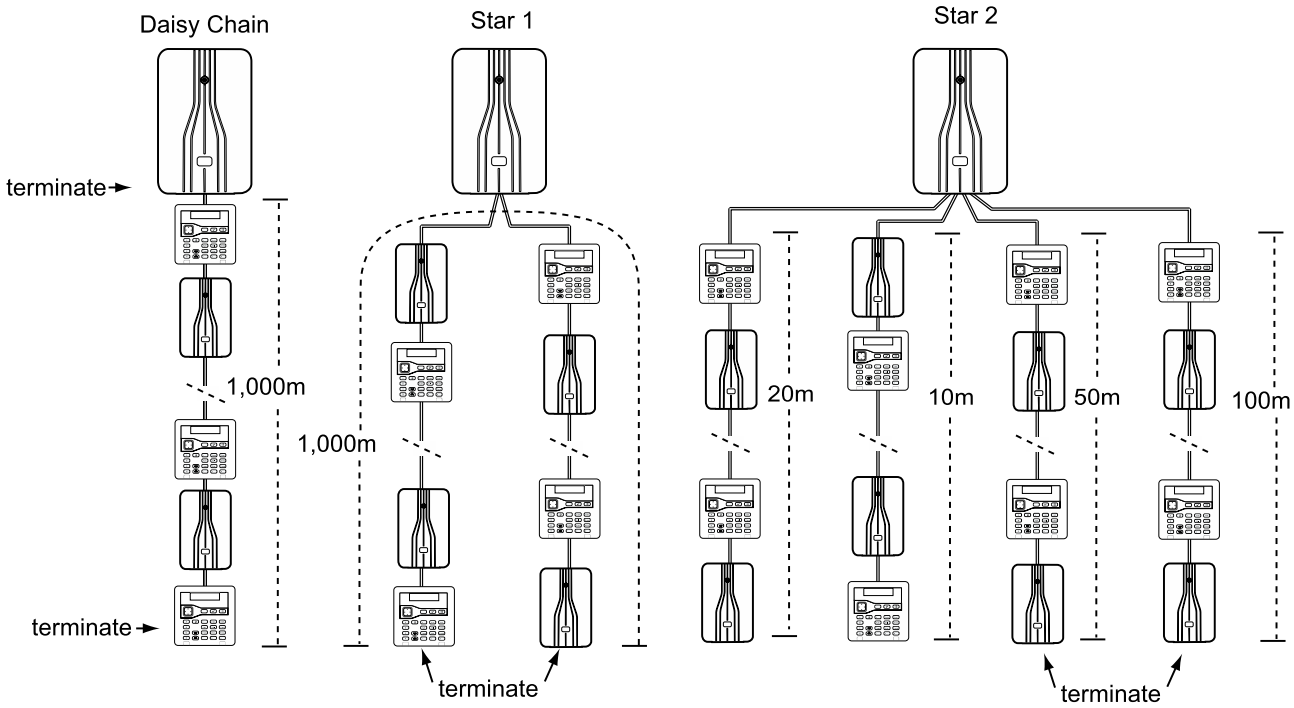


Figure 4. Bus Termination

Voltage drop

In order for the system to work correctly, the voltage at each device must NOT drop below 10.5V, even when running on the standby battery. Preferably, the voltage at each device should stay above 12V to avoid unexpected behaviour.

Standard 7/0.2 alarm cable has a resistance of 8 Ohms per 100m per core. The voltage drop is calculated using the following formula: V drop = Current drawn x cable length x 0.08 x 2.

Table 5 shows the voltage drop against the current drawn and cable length. The shaded area shows where the voltage drop would cause the bus voltage to fall from 13.8V to below 12.0V when using a single core.

Table 5: Voltage drop along cable

Current Drawn	Cable Length (Standard 7/0.2 alarm cable)									
	10m	20m	30m	40m	50m	60m	70m	80m	90m	100m
60mA	0.10V	0.19V	0.29V	0.38V	0.48V	0.58V	0.67V	0.77V	0.86V	0.96V
80mA	0.13V	0.26V	0.38V	0.51V	0.64V	0.79V	0.90V	1.02V	1.15V	1.28V
100mA	0.16V	0.32V	0.48V	0.64V	0.80V	0.96V	1.12V	1.28V	1.44V	1.60V
120mA	0.19V	0.38V	0.58V	0.79V	0.96V	1.15V	1.34V	1.54V	1.74V	1.92V
140mA	0.22V	0.45V	0.67V	0.90V	1.12V	1.34V	1.57V	1.79V	2.02V	2.24V
160mA	0.26V	0.51V	0.77V	1.02V	1.28V	1.54V	1.79V	2.05V	2.30V	2.56V
180mA	0.29V	0.58V	0.86V	1.15V	1.44V	1.73V	2.02V	2.30V	2.59V	2.88V
200mA	0.32V	0.64V	0.96V	1.28V	1.60V	1.92V	2.24V	2.56V	2.88V	3.20V
220mA	0.35V	0.70V	1.06V	1.41V	1.76V	2.11V	2.46V	2.82V	3.17V	3.52V
240mA	0.38V	0.79V	1.15V	1.54V	1.92V	2.30V	2.69V	3.07V	3.46V	3.84V
260mA	0.42V	0.83V	1.25V	1.66V	2.08V	2.50V	2.91V	3.33V	3.74V	4.16V
280mA	0.45V	0.90V	1.34V	1.79V	2.24V	2.69V	3.14V	3.58V	4.03V	4.48V
300mA	0.48V	0.96V	1.44V	1.92V	2.40V	2.88V	3.36V	3.84V	4.32V	4.80V
320mA	0.51V	1.02V	1.55V	2.05V	2.56V	3.07V	3.58V	4.10V	4.61V	5.12V
340mA	0.54V	1.09V	1.63V	2.18V	2.72V	3.26V	3.81V	4.35V	4.90V	5.44V
360mA	0.58V	1.15V	1.73V	2.30V	2.88V	3.46V	4.03V	4.61V	5.18V	5.76V
380mA	0.61V	1.22V	1.82V	2.43V	3.04V	3.65V	4.26V	4.86V	5.47V	6.08V
400mA	0.64V	1.28V	1.92V	2.56V	3.20V	3.84V	4.48V	5.12V	5.76V	6.40V

You can reduce voltage drop using either or both of these methods:

- Double-up the supply connections (12V and 0V). This will halve the resistance on each core and therefore halve the voltage drop.
- Supply power to the detection devices from the control unit's Aux output using two additional cores in the cable (that is, use 6-core cable). This reduces the current drawn by the bus devices and is the preferred method of reducing voltage drop, since detectors generally operate at lower voltages (9.5V).

If you cannot reduce voltage drop sufficiently, install one or more remote power supplies, as described next.

Using remote power supplies

When voltage drop along the bus cable exceeds requirements, or the demand on the control unit's power supply exceeds its capacity, you should install one or more EXP-PSU remote power supplies. Figure 5 shows the recommended method of connecting a remote power supply. It should be fitted close to the equipment it is powering.

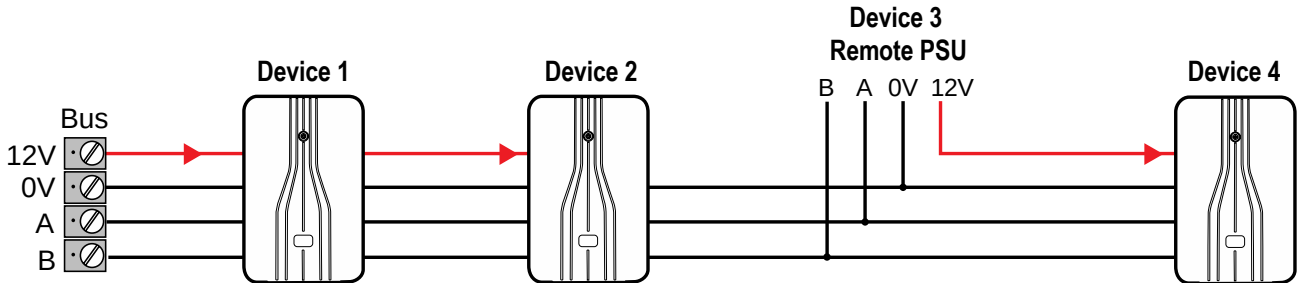


Figure 5. Connecting a Remote Power Supply

Chapter 3: Getting Started

Once all wiring is complete, the system is ready to be programmed. This section provides an overview of how to carry out this task. Later sections of this guide explain the configuration options in more detail.

About the user interface

The control unit displays configuration options in menus. The top-level Installer menu contains options such as *Detectors/Devices*, *Outputs* and *Partitions*. For example:

```
INSTALLER MENU
 Detectors/Devices
```

You can select an option by pressing ▲ or ▼ at the keypad until the name of the option or device you want is displayed. Pressing ✔ selects that option. Some options require you to press ▶ or ◀ to change the setting.

Selecting an option may display a menu of further options. For example, selecting *Detectors/Devices* displays the first option in the *Detectors/Devices* menu:

```
DETECTORS/DEVICES
 Detectors
```

You can repeat the process until you have selected the lowest-level setting you want to change.

Pressing ✘ at the keypad takes you back one level. For example, pressing ✘ when you are in the *Detectors/Devices – Detectors* menu takes you back to the *Detectors/Devices* menu.

The section starting on page 31 shows a "menu map", which gives the position of all menus and options in the Installer menu.

Entering text

You can use the numeric (1-9), * and # keys on a keypad to enter numbers and text. All numeric keys are labelled to show the characters you can enter using that key. For example, you can use the "2" key to enter A, B, C and 2 (where applicable). Also use (where applicable):

- # to change between capital and lower-case letters.
- 0 to enter a space or other characters such as "&", "@" and "/".

When you first select an option to enter text, the display shows the cursor at the beginning of the bottom line. If you press a key, the bottom line clears and the character you key-in appears at the beginning of the line.

A cursor on the display shows the position of the next character. If you are keying in capital letters, the cursor is a block. For lower-case letters, the cursor is an underline.

If you press ▶ when you first select an option to enter text, the existing text shifts right one character and you can insert a new character in the empty space. To move the cursor left or right, press ▲ or ▼ respectively. To delete a character, press ◀.

Initial power-up procedure

WARNING: During initial power-up, keypad sounders, internal loudspeakers and wired sirens 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.

Note:

- The following assumes that all wiring is complete, the control unit has not been previously configured and that all keypads have a "null" address (no address previously allocated). If required, please refer to page 24 for details of how to reset the system.
- The section titled "About the user interface" (above) gives information about how to select menu options.

To configure the system for the first time:

1. Connect the control unit's battery.
2. Close the lid of the control unit if there is no need to keep it open.
3. Switch on the mains supply.

   Note: Ordinarily, the control unit starts only after the mains supply is switched on, even if a battery is connected. If you want to operate the control unit temporarily using only the battery (or a 12VDC supply), start it by briefly shorting the kick-start link on the PCB.
4. Wait until you see:

   ```
   Press addr button(s)
     on wired keypads
   ```

   This message indicates that the keypad has a "null" address.
5. Go to the keypad you want to use for initial configuration. Obtain an address for this keypad by pressing and holding A and ✔ keys simultaneously ***for at least three seconds*** until you hear a sound. The display shows the address allocated by the control unit, such as “b1-d51”(bus 1, device 51).

   The address is now stored in the keypad.
6. Follow this step if you see the following (EU systems only):

   ```
   LANGUAGE
    English v0.11
   ```

   a) Select the language you want 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*.

   b) Select the country:

   ```
   COUNTRY DEFAULTS
   *UK
   ```
7. Press A or B to select either a partitioned system or a part-setting system (page 4):

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

8. Select the wiring type you intend to use for wired zones (page 7):

```
WIRED ZONE TYPE
*2-wire FSL 2k2/4k7
```

This determines the default wiring type for the control unit and any attached bus devices, such as wired expanders. You can change the control unit's wiring type through *Installer menu – System Options*, or specify a different wiring type for a bus device through the device's edit menu (e.g. *Installer menu – Detectors/Devices – Wired Expander – Edit Expander*).

Note: If you are using an ADP-10CC board (to provide ten on-board 4-wire CC zones instead of ten FSL zones), select 2-wire FSL 2k2/4k7 as the wiring type.

9. Specify an installer code:

```
NEW INSTALLER CODE
       (     )
```

When prompted, confirm the code. **DO NOT FORGET THIS CODE!**

10. You will see one of the following:

- If the lid of the control unit is closed, you will see the standby screen. For example:

```
     i-on40H-EU
  10:30 01/08/2016
```

- If the lid of the control unit is open, you will see:

```
INSTALLER EXIT FLTS
 Panel lid open
```

11. If the standby screen is displayed, enter the Installer code to enter the Installer menu. Otherwise, if the "Panel lid open" message is displayed, press ✘ to access the Installer menu.

The first option in the menu is displayed:

```
INSTALLER MENU
 Detectors/Devices
```

12. Use the Installer menu to carry out the required configuration tasks, such as to:

- Add the other bus devices, if used (page 50).
- Program zones.
- Configure outputs.
- Configure setting options.

13. Exit the Installer menu (page 23).

Entering the Installer menu

Entering the Installer menu allows you to configure the system using the options provided. While you are logged in:

- The system will not generate alarms. You are, for example, able to open the lid of the control unit without generating an alarm. All Hold-Up Alarms (HUAs), fire-alarm zones, 24-hour zones and tampers are disabled.
- Any other user trying to set the system from a keypad or access the user menu will see the message “Installer on Site”.

Entering the Installer menu from a keypad

1. Make sure the system is fully unset and showing the standby screen. For example:

   ```
       i-on30R
   12:00 01/07/2016
   ```

2. Enter the Installer code, as specified when the control unit was first configured:

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

3. You may prompted to enter a user code (default 1234):

   ```
    User Code Required
          (    )
   ```

   This is displayed if you have not used the Installer menu with the previous 30 minutes, or if the system has been armed and disarmed within that period. You can disable this feature using *System Options – User Access – User Code Required* (see page 84). You cannot enter a Set Only user code.

4. The bottom line displays *Detectors/Devices*, which is the first option in the menu:

   ```
    INSTALLER MENU
   Detectors/Devices >
   ```

5. Press ▲ or ▼ to display the next option in the menu, then press ▶ or ✔ to select that option. Continue this process until you have reached the sub-option you require.

Saving changes

Changes are saved only when you leave the Installer menu. If you remove all power before leaving the Installer menu, changes will not be saved. Note that this does not apply if you restore factory defaults; that change takes place immediately.

Code lockouts

If you (or any user) enter your code incorrectly or present an unrecognised proximity tag, the keypad shows the time and date again, gives an error tone and you can try again.

If there are four consecutive incorrect access codes or proximity tags, the system starts a tamper alarm and locks all users out of all keypads for 90 seconds. This event is recorded in the log as “Excess Keys Tamper”.

Once the lock-out time has expired, you can try again. If the next attempt is also invalid, system locks all keypads for another 90 seconds, but will not start another tamper alarm.

An “Excess Keys Tamper” can also occur while attempting to gain access from the web interface.

Transferring to another keypad

While in the Installer menu, you can transfer to any other keypad without leaving the Installer menu. To do this, simply go to any other keypad and enter the Installer access code. The new keypad will pick up your position in the Installer menu. The keypad you have left will exit the Installer menu.

Using Downloader or the web interface

This manual describes configuring the control unit from a keypad. You can also program a control unit using either of the following:

- The web interface, through a web browser. Internet Explorer 11, Google Chrome and Mozilla Firefox are supported. The i-on Web Browser Interface Setup Guide explains how to configure the system using the web interface.
- The Downloader software running on a PC. This can connect control unit via an i-dig02 module (over PSTN), USB port or Ethernet port. Downloader is available to registered users through www.touchpoint-online.com.

The settings and options provided through the web interface or Downloader have the same behaviour as those provided through the keypad.

Before you can use the web interface or Downloader, the Master User must enable remote access using *U*ser *Menu – System Config – Facilities On/Off – Remote Access*. If remote access is denied, the Master User can still start a call out to Downloader.

Exiting the Installer menu

To exit the Installer menu:

1. Replace the lid of the control unit or other devices (if you removed them) to close all tamper switches.
2. Press ✘ until the display shows:

   ```
        Leave
   installer mode ?
   ```

3. Press ✔ to leave Installer menu. (Press ✘ if you do not want to leave the menu.)

   Note: You must rectify faults (for example, the lid of the control unit is open) or delete the device from the system before you can leave the Installer menu.

   The control unit performs an automatic bus scan when you exit the Installer menu to detect duplicate bus addresses, or lost/found devices (see page 51).

   On completion, the display shows the time and date, and the system is ready for use.

Resetting (defaulting) the system

Restoring control unit factory defaults

You can remove all configuration from the control unit using *System Options – Restore Defaults – Factory Defaults* (see page 92). You must restore defaults from a keypad; you cannot do this from a PC.

Resetting device addresses

You can clear the address stored in a device's non-volatile memory as follows:

- **Keypads** – Press the D and ✘ keys together while the front cover is open.
- **Expanders** – Press the Request/Delete Address button while applying power. The tamper disable link must not be fitted.
- **Other devices** – Please refer to the device's installation instructions.

Defaulting access codes

You can use the Reset Codes link in the control unit's PCB to reset the user 001 and installer codes in the event that either has been forgotten.

Note: Resetting the codes also deletes all proximity tags, Hold-Up devices (HUDs) and remote controls.

The default user 001 code is 1234. There is no default installer code.

To reset the codes:

1. If you know the installer code, enter it to prevent a tamper alarm when you remove the lid of the control unit.
2. Remove mains power to the control unit.
3. Remove the lid of the control unit (the tamper must be activated for the procedure to work).
4. Disconnect the battery.
5. While shorting the Reset Codes link, apply mains power and keep the short in place until you see the following:

   ```
   NEW INSTALLER CODE
          (    )
   ```

6. Enter a code you want to use for the installer code. Confirm when prompted.
7. Reconnect the battery and refit the lid.

Chapter 4: Addressing and Zone Numbering

This chapter explains how the control unit assigns addresses, such as to bus devices, outputs, detectors. It also explains how the control unit maps zone numbers to detectors.

Bus device addresses

The control unit keeps a record of the address it allocates to each device on the bus. Each device also stores its address locally in non-volatile memory.

The address of each bus device is in the format An-dd (e.g. W1-03), where:

A = One or more letters showing the device type: K=keypad, W=Wired Expander, R=Radio Expander.

n = Bus number (always 1).

dd = Bus device number. Keypads have bus device numbers in the range 51 to 97. Expanders and other bus devices can have the following bus device numbers:

- i-on30R: 03 to 50
- i-on40H: 04 to 50

The maximum number of devices on the bus is shown in Table 1 on page 2.

Figure 6 shows an example of bus device addressing.

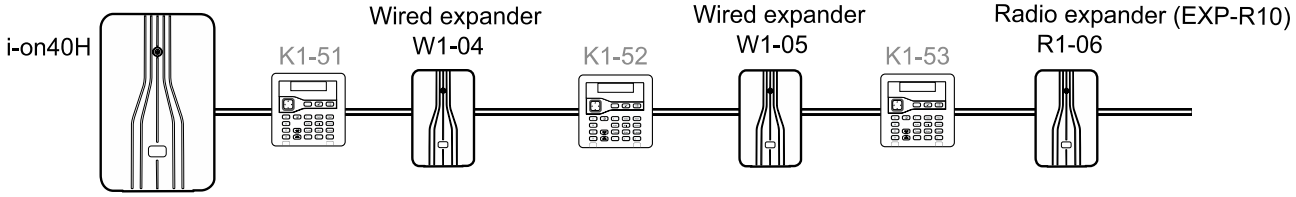


Figure 6. Bus Device Addressing Example

Note: An EXP-R30 expander takes three consecutive bus device numbers. In the Installer menu, the display shows only the first of these two/three addresses (e.g. “R1-04”), but also adds “(R30)” as a reminder.

Bus device address for devices that communicate through a radio expander

For devices such as sounders and WAMs that communicate through a radio expander, you select a specific radio expander to learn the identity of the radio device. The control unit refers to these devices in the form Rn-dd-zz (e.g. R1-06-01), where:

R = Fixed text to show that the device communicates through a radio expander.

n = The bus number of the radio expander (always 1).

dd = The bus device number of the radio expander (see above).

zz = Radio device number, starting from 01.

When reporting alarms to an alarms-receiving centre using CID or SIA protocols, the control unit reports each device as a number (not as an address). For example:

Radio Siren	Ext.01 to Ext.20
WAMs	WAM01 to WAM20

Note that the highest number will depend on the control unit.

Output addresses

Each output has an address. Outputs attached directly to the control unit (if applicable) take the address PAN>OP1 to PAN>OP8 (the number of on-board outputs is dependent on the control unit used; see Table 1 on page 2). Outputs attached to a bus device take the address An>dd>oo (e.g. W1>03>01), where:

A = One or more letters showing the device type: K=keypad, W=Wired Expander, R=Radio Expander.

n = Bus number (always 1).

dd = Bus device number (see page 25).

oo = Output number, starting from 01.

See Figure 7 for an example.

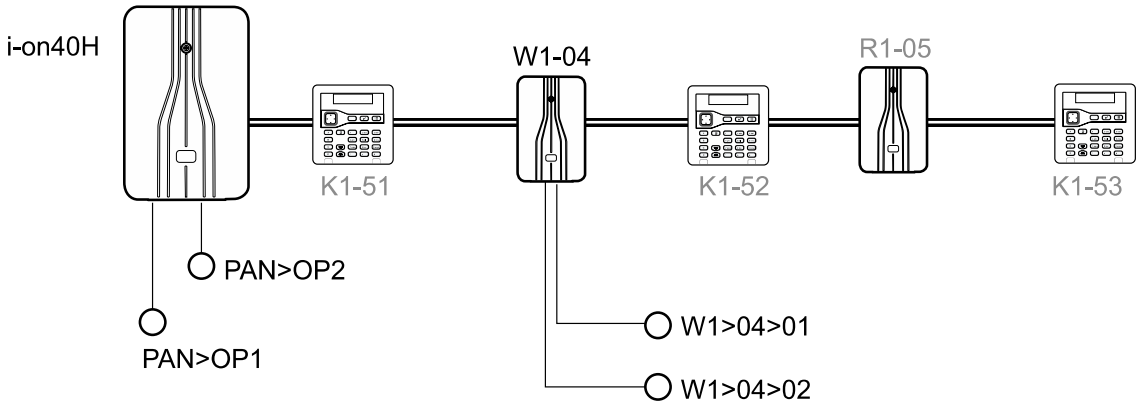


Figure 7. Output Numbering

Detector addresses and zone numbering

Figure 8 provides an example of detector addressing and zone numbering for on i-on40H. The next sections explain how the control unit assigns detector addresses and zone numbers.

Note: Zone numbers are used when the control unit reports alarms to an alarms-receiving centre using CID or SIA protocols. SIA cannot report any alarms on PAN<Z00. You might find this zone useful as a Log Only zone.

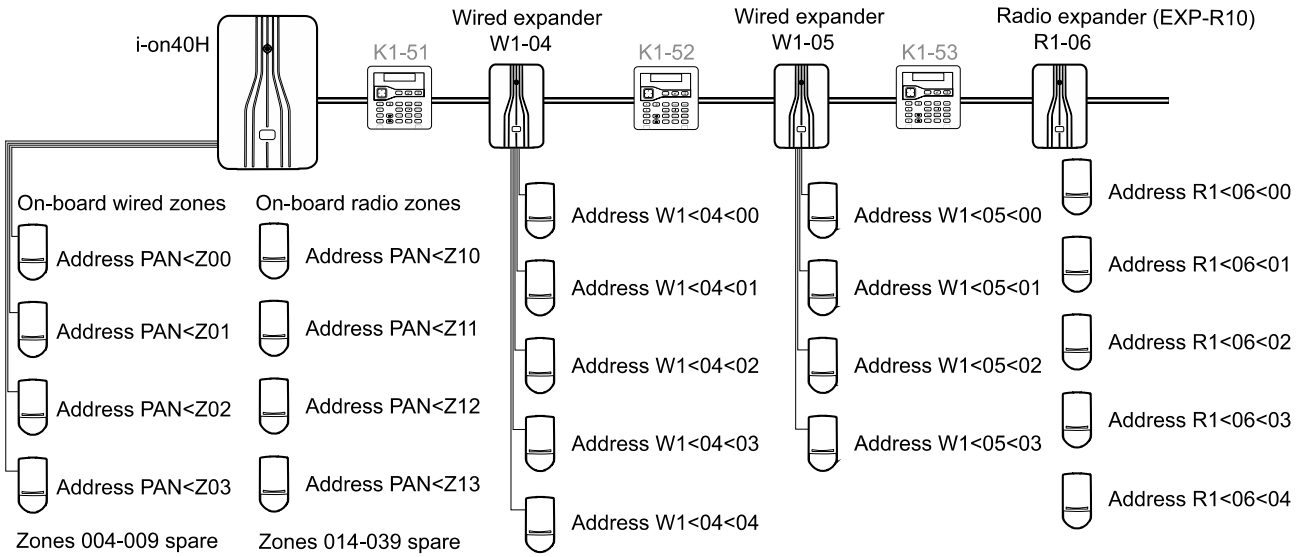


Figure 8. Example of Detector Addressing and Zone Numbering (i-on40H)

On-board wired detectors

Wired detectors attached directly to the control unit (if applicable) use the following address:

	On-Board Wired Detector Address	**Zone Number**
FSL* and 2-wire CC wiring	PAN<Z00 to PAN<Z09	000 to 009
4-wire CC wiring	PAN<Z01 to PAN<Z05	001 to 005

*If an ADP-10CC board is used, ten 4-wire CC zones can be used instead of ten FSL zones.

On-board radio detectors

Radio detectors that communicate directly with the control unit use the following addresses:

	On-Board Radio Detector Address	**Zone Number**
i-on30R	PAN<Z00 to PAN<Z29	000 to 029
i-on40H	PAN<Z10 to PAN<Z39	010 to 039

Detectors attached to an expander

Detectors attached to an expander take the address An<dd<ii (e.g. W1<04<00), where:

A = One or more letters showing the device type: W=Wired Expander, R=Radio Expander.

n = Bus number (always 1).

dd = Bus device number (see page 25).

ii = Input number. This can be any number from:

- 00 to 09 for wired expanders or the EXP-R10.
- 00 to 29 for the EXP-R30.

Zone numbering for detectors connected to an expander

Each expander takes a sequential block of zone numbers up to the capacity of the device, running on from any zones in the control unit or previous expander. The zone numbers are dd0 to dd9 (for FSL or 2-wire CC wiring) or dd1 to dd5 (for 4-wire CC wiring), where "dd" is the two-digit device number. Table 6 provides an example (refer also to Figure 8).

Note: Zone numbering for detectors connected to keypads is different; see the next section.

Table 6: Example of expander zone numbering (i-on 40H)

1st Expander (e.g. EXP-W10) Device number 04 Address W1-04		**2nd Expander (EXP-W10) Device number 05 Address W1-05**		**3rd Expander (EXP-R10) Device number 06 Address R1-06**	
Detector Address	**Zone No.**	**Detector Address**	**Zone No.**	**Detector Address**	**Zone No.**
W1<04<00	040	W1<05<00	050	R1<06<00	060
W1<04<01	041	W1<05<01	051	R1<06<01	061
W1<04<02	042	W1<05<02	052	R1<06<02	062
...etc.	*...etc.*	*...etc.*	*...etc.*	*...etc.*	*...etc.*
W1<04<07	047	W1<05<07	057	R1<06<07	067
W1<04<08	048	W1<05<08	058	R1<06<08	068
W1<04<09	049	W1<05<29	059	R1<06<09	069

Zone numbering for zones on keypads

Several keypads provide terminals for up to two zones using FSL or 2-wire CC wiring, or one zone using 4-wire CC wiring. To use the zones on the keypad, you must first enable them from the *Detectors/Devices – Wired* (or *Radio*) *Keypads* Edit menu. For wired keypads, you can use the same menu to select the zone wiring type of the keypad zones, independently of the zone wiring type used by the control unit or the wired expanders. The zone wiring type will affect the zone numbering.

When you enable the zones, the control unit assigns them to zone numbers starting from the top of the control unit's zone number range, as follows:

- **FSL or 2-Wire CC** – Using the i-on30R as an example, the highest possible zone number is 059. When the control unit gives an address to the first keypad to be added, it allocates the zone number 059 to terminals Z2 on the keypad, and zone

number 058 to terminals Z1. When you add the next keypad, the control unit allocates the zone numbers 057 to terminals Z2 and 056 to terminals Z1 on the new keypad. Table 7 shows an example.

Table 7: Keypad – FSL or 2-wire CC zones

Control Unit	First keypad Z2, Z1	Second keypad Z2, Z1	Third keypad Z2, Z1	Additional keypads
i-on30R	59, 58	57, 56	55, 54	*...etc.*
i-on40H	79, 78	77, 76	75, 74	*...etc.*

- **4-Wire CC** – When you wish a keypad to use 4-wire CC zone wiring, the control unit still assigns zone numbers at the top of the zone numbering range, but this time it uses only alternate zone numbers Table 8 shows an example. For each keypad, the Z2 terminals are the for the tamper contacts, and the Z1 terminals are for the alarm contacts.

Table 8: Keypad – 4-wire CC zones

Control Unit	First keypad Z2(T), Z1(A)	Second keypad Z2(T), Z1(A)	Third keypad Z2(T), Z1(A)	Additional keypads
i-on30R	59	57	55	*...etc.*
i-on40H	79	77	75	*...etc.*

Zone availability for keypads

It is possible that there may be no zones available to assign to a keypad. This can happen in two ways:

- When the control unit has expanders allocated to all the available zones on the bus.
- When the control unit has an expander already allocated to the zones at the top of its zone numbering range.

Figure 9 provides three examples of zone availability when using expanders and keypads connected to an i-on30R:

- Example a) – Since expanders use all available zones, there are no zones available to allocate to any keypads on the bus. This applies even if some of the expanders have unused zones.
- Example b) – A keypad takes up two zones at the top of the address range. The remaining zones are available for keypads. However, since the control unit allocates zones in groups of 10, the control unit will not allocate any of the remaining 8 zones in that group to an expander.
- Example c) – An expander takes up zones at the top of the numbering range. The control unit cannot allocate keypad zones to zone numbers below the expander.

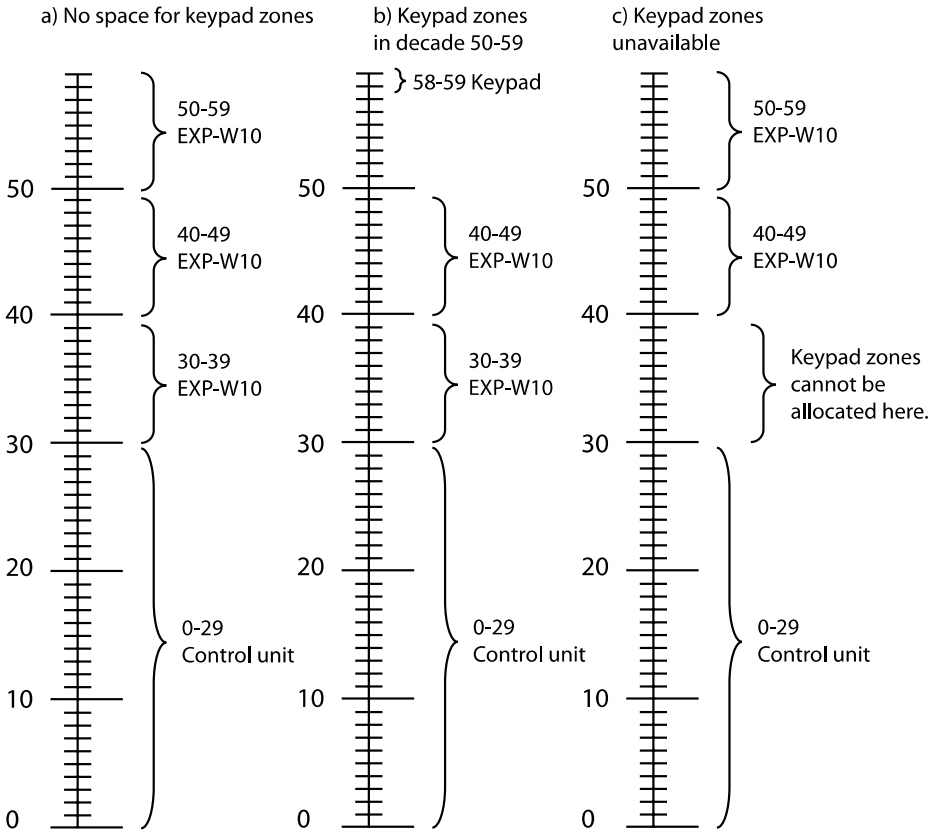


Figure 9. Example zone availability (i-on30R)

Chapter 5: Installer Menu Map

Important: Where noted below the defaults listed enable the control unit to comply with EN50131 requirements. If you change those settings, the installation may no longer comply. If the control unit does not comply with EN50131, you must remove any labelling that indicates compliance.

Some options are not always visible as the relevant hardware is not fitted, or not applicable to the control unit type.

MENU Option			Factory Default	Notes
1 Detectors/Devices				
Detectors	Add/Del Detectors	Exp. R1-nn		Visible only if a radio expander is on the bus.
		Zone nnn...		
		Delete all		
		Panel		
		Zone nnn...		
		Delete all		
		Delete all		
	Program Zones	Zone 000...		
		Name	"Zone nnn"	
		Type	Not used	
		Partitions	None	Visible only in a partitioned system and when zones have a type other than "Not Used".
		Attributes	All "off", except Supervision	Visible when zone is given a type other than "Not Used". Some attributes are only available on particular zone types. Double Knock does not comply with EN51031. Masking must be enabled in System Options.
		Resistance	2k2/4k7	
Address Bus Device				
Wired Expanders	Address Bus Device			
	Edit Expander	Expander W1-01...		
		Name	"Exp. W1-nn"	
		Partitions	Partition 1	Visible only in a partitioned system.
		Wired zone type	FSL 2k2/4k7	
		Loudspeaker volume	Zero when expander first added to bus	
		Battery 2	Disabled	Visible only for EXP-PSU.
	Delete Expander			
	Enable Expander		Yes	
	Replace Expander			

Radio Expanders	Address Bus Device			
	Edit Expander	Expander R1-01...		
		Name	"Exp. R1-nn"	
		Partitions	Partition 1	Visible only in a partitioned system.
		Loudspeaker Volume		
	Delete Expander			
	Enable Expander		Yes (all expanders enabled).	
	Replace Expander			
Wired Keypads	Address Bus Device			
	Edit Keypad	Keypad K1-51...		
		Name	"Keypad K1-nn".	
		Partitions	Partition 1	Visible only in a partitioned system.
		Key A	Name: "Key A" Setting: Partition 1 Full Set OR Full Set in a Part Setting System	
		Key B	Name: "Key B" Setting: Partition 2 Full Set OR Part Set B in a Part Setting System	
		Key C	Name: "Key C" Setting: Partition 3 Full Set OR Part Set C in a Part Setting System	
		Key D	Name: "Key D" Setting: Partition 4 Full Set OR Part Set D in a Part Setting System	
		Zones	Disabled	Visible only when a suitable keypad is fitted.
		Wired Zone Type	2K2/4K7	
		Loudspeaker Volume		
		Buzzer Volume		
		Backlight		
		External Prox	Disabled	
	Delete Keypad			
	Enable Keypad		Yes (all keypads enabled)	
	Replace Keypad			
Radio Keypads	i-rk01			
	Add/Del Radio Keypad			
	Edit Keypad	Radio Kpd 01...		
		Name	"Radio Kpd 0n"	
		Partitions	Partition 1	Visible only in a partitioned system.
		Key A	Name: "Key A" Setting: Partition 1 Full Set OR Full Set in a Part Setting System	
		Key B	Name: "Key B" Setting: Partition 2 Full Set OR Part Set B in a Part Setting System	
		Key C	Name: "Key C" Setting: Partition 3 Full Set OR Part Set C in a Part Setting System	
		Key D	Name: "Key D" Setting: Partition 4 Full Set OR Part Set D in a Part Setting System	
	KEY-RKPZ			
	Address Bus Device			
	Edit Keypad	Keypad K1-51...		
		Name	"Keypad K1-nn".	
		Partitions	Partition 1	Visible only in a partitioned system.

		Key A	Name: “Key A” Setting: Partition 1 Full Set OR Full Set in a Part Setting System	
		Key B	Name: “Key B” Setting: Partition 2 Full Set OR Part Set B in a Part Setting System	
		Key C	Name: “Key C” Setting: Partition 3 Full Set OR Part Set C in a Part Setting System	
		Key D	Name: “Key D” Setting: Partition 4 Full Set OR Part Set D in a Part Setting System	
		Zones	Disabled	
		Zone Type		Not used; use only 2-wire FSL.
	Delete Keypad			
	Enable Keypad		Yes (all keypads enabled)	
	Replace Keypad			
External Sirens	Add/Del Siren			
	Edit Siren	Name		
		Partitions	Partition 01	Visible only in a partitioned system.
Internal Sounders	Add/Del Sounder			
	Edit Sounder	Int. SNDR 01...		
		Name	"Int. SNDR nn"	
		Partitions	Partition 01	Visible only in a partitioned system.
		Volume	4	
WAMs	Add/Del WAM			
	Edit WAM			
Cameras	IP Cam 1...	Camera Triggers	None	
		Zone Follow		
		Zone Alarm		
		Trigger Partitions	All Partitions	Visible only in a partitioned system.
		IP Address		
		HTTP Port Internal	80	
2 Outputs				
Radio outputs	Add Outputs			
	Edit Outputs	EDIT RADIO O/P 1...		
		Name	"Output nnn"	
		Type	Not used	
		Pulsed	No	
		Partitions	All outputs allocated to all Partitions	Visible only in a partitioned system.
		Zones	None	
		Delay	0 seconds	Visible when Pulsed set to “Yes”.
		On Time	1 second	
Wired outputs	Panel	EDIT *output*		
		Name		
		Type	For dedicated siren and strobe outputs, "Type" is "Siren" or "Strobe" (as appropriate) and not editable. For odd-numbered panel outputs, the default "Type" is "Siren". For even-numbered panel outputs, the default "Type" is "Strobe".	
		Polarity	Normal	
		Pulsed	No	Not available for dedicated siren and strobe outputs.
		Partitions	All outputs allocated to all Partitions	Visible only in a partitioned system.
		Zones	None	
		Delay	0 seconds	Visible when Pulsed set to “Yes”.

		On Time	1 second	
	Exp. W1-nn	EDIT *output*		
		Name		
		Type	Not used	
		Polarity	Normal	
		Pulsed	No	
		Partitions	All outputs allocated to all Partitions	Visible only in a partitioned system.
		Zones	None	
		Delay	0 seconds	Visible when Pulsed set to “Yes”.
		On Time	1 second	
	Keypad k1-nn	EDIT *output*		Visible only when a suitable keypad is fitted.
		Name		
		Type	Not used	
		Polarity	Normal	
		Pulsed	No	
		Partitions	All outputs allocated to all Partitions	Visible only in a partitioned system.
		Zones	None	
		Delay	0 seconds	Visible when Pulsed set to “Yes”.
		On Time	1 second	
Plug-by outputs	EDIT PLUG-BY O/P1...	Name		
		Type	O/P1: Fire Alarm O/P2: Hold Up Alarm O/P3: Burglar Alarm O/P4: Open / Close O/P5: Zone Omit (System) O/P6: Tamper O/P7: Confirmed Alarm O/P8: General Fault O/P9: AC Fail O/P10: Battery Fault O/P11: Technical Alarm O/P12: Alarm Abort	
		Polarity	Normal	
		Pulsed	No	
		Partitions	All outputs allocated to all Partitions.	Visible only in a partitioned system.
		Zones	None	
		Delay	0 seconds	Visible when Pulsed set to “Yes”.
		On Time	1 second	
Custom Outputs	Custom Output 1...	Mode	Any (Or)	
		Inputs	None	
3 Setting options (only shown in a part-setting system)				Appears only in a part-setting system.
Full Set	Name		“Full Set”	
	Exit Mode		Timed Set	
	Settle Time		15 seconds	Visible only if Exit Mode is “Final Door”, “Lock Set” or “Exit Terminate”.
	Exit Time		40 seconds	Visible only if Exit Mode is “Timed Set” or “Silent Set”.
	Entry Time		40 seconds	
	Siren Delay		0 minutes	
	Siren Time		15 minutes	
	Strobe on Set		Off	
	Strobe on Unset		Off	
Part Set B/C/D	Name		“Part Set B”	
	Exit Mode		Instant Set	
	Settle Time		15 seconds	Visible only if Exit Mode is “Final Door”, “Lock Set” or “Exit Terminate”.
	Exit Time		40 seconds	Visible only if Exit Mode is “Timed Set” or “Silent Set”.
	Entry Time		40 seconds	
	Alarm Response		Siren	
	Siren Delay		0 minutes	

	Siren Time		15 minutes	
	Pt.set Final Exit		Final exit	
	Pt.set Entry Route		Entry Route	
	Strobe on Set		Off	
	Strobe on Unset		Off	
Remote Set	Exit Mode		Timed Set	
	Exit Time		30s	
	Local Set on ER		Off	
Calendar Set			None	
3 Partitions (only shown in a partitioned system)				Visible only in a partitioned system.
Partition 1...	Name		"Partition n"	
	Exit Mode		Timed Set (Partition 2 onwards defaults to the same as partition 1)	
	Settle Time		10 seconds	Visible only if Exit Mode is "Final Door", "Lock Set" or "Exit Terminate".
	Exit Time		40 seconds	Visible only if Exit Mode is "Timed Set" or "Silent Set".
	Entry Time		40 seconds	
	Alarm Response		Siren + Comms	
	HUA Response		Audible	
	PZ Unset Response		Silent	
	PZ Set Response		Silent	
	PZ Reset Time			
	Siren Delay		0 minutes	
	Siren Time		15 minutes	
	Strobe on Set		Off	
	Strobe on Unset		Off	
	Part Set Exit Mode		Instant Set	
	Pt.set Settle Time		15 seconds	Visible only if Part Set Exit Mode is "Final Door" , "Lock Set" or "Exit Terminate".
	Part Set Exit Time		40 seconds	Visible only if Part Set Exit Mode is "Timed Set" or "Silent Set".
	Pt.set Entry Time		40 seconds	
	Pt.set Alarm Response		Siren	
	Pt.set Siren Delay		0 minutes	
	Pt.set Siren Time		15 minutes	
	Pt.set Final Exit		Final exit	
	Pt.set Entry Route		Entry Route	
	Pt.set Strb Set		Off	
	Pt.set Strb Unset		Off	
Full Set Link	Partition 2…nn		No for all partitions	
	All Partitions		No	
Remote Set	Exit Mode		Timed Set	
	Exit Time		30s	
	Local Set on ER		Off	
Calendar Set	Add Event	Event 01...		
		Event Time	00:00	
		Event Days	No for all days	
		Event Actions	No for all partitions	
		Event Exceptions	No for all exceptions	
		Warning Time		
		Warning Tone		
	Edit Event	Event 01...		
		Name	"Event nn"	
		Time	00:00	
		Days	No for all days	
		Actions	No for all partitions	
		Exceptions	No for all exceptions	
		Warning Time	10min	

			Warning Tone	Audible	
	Delete Event				
	Add Exception	Exception 01...			
			Exception Start Time	00:00	
			Exception Start Date	01/01	
			Exception End Time	00:00	
			Exception End Date	01/01	
	Edit Exception	Exception 01...			
			Name	"Exception nn"	
			Start	00:00, 01/01	
			End	00:00, 01/01	
	Delete Exception				
4 System Options					
Wired Zone Type	Panel Zones			2 Wire FSL 2k2/4k7	Visible only if the control unit supports wired zones.
	All Zones			2 Wire FSL 2k2/4k7	Visible only if a device connected to the bus supports wired zones.
User Access	HUA keys active			No	
	Quick set			No	
	Quick omit			No	
	User code reqd			Yes	
	2 Way Replies			Yes	Used for FOB-2W-4B.
	2W Set Instant			Yes	Used for FOB-2W-4B.
	Duress Enable			No	
	Terminated Set			Yes	Used for KEY-EP.
User Reset	Zone alarms			Yes	Visible only if Confirmation Mode is "Basic".
	Zone tampers			Grade 2: Yes	
	System tampers			No	
Confirmation	Confirmation Mode	DD243			Not available for EU control units, which use Basic Confirmation.
		BS8243		Default for UK systems	
		Basic			
	Confirmation time			30 minutes	Visible for BS8243 or DD243.
	After Entry			1 zones	Visible for BS8243 or DD243. Default changes to 2 zones when Confirmation Mode = DD243.
	Entry Keypad Lock			Off	Visible for BS8243 or DD243.
	Sounder on			Unconfirmed	
	Siren on			Unconfirmed	
	Unconfirmed reset			User	Visible for BS8243 or DD243.
	Confirmed reset			Installer	Visible for BS8243 or DD243.
	HUA Confirm time			8 hours	Visible for BS8243 only.
	Tamp as Tamp-Only			Enabled	Visible for BS8243 only.
Masking				Grade 2: Off	
Mask Override				On	Visible only when Masking is On.
Language				English	
Shunt Groups	Shunt Group 1...				
Restore Defaults	Staged defaults	User			
		Zones			
		Radio Devices			
		Outputs			
		Setting Info			
		System Options			
		Communications			
	Factory defaults				
Installer Name				"Installer"	

Installer Code			Installer configured	
Keypad text			Panel name	
Remote needs Entry			Disabled	
Remote needs Entry PrtSt			Disabled	
RKP needs Entry			Disabled	
RKP Entry PrtSt			Disabled	
HUA Response			Audible	Visible only for part-setting system.
PZ Unset Response			Silent	Visible only for part-setting system.
PZ Set Response			Silent	Visible only for part-setting system.
PZ Reset Time				Visible only for part-setting system.
Auto Rearm			Never	Visible only in EU control units or when Confirmation Mode is “Basic”.
Panel Loudspeaker	Volume		4	
	Partitions		All	Visible only in a partitioned system.
Entry Alarm Delay			Yes	
Abort Time			120 seconds	
Supervision			Tamper	
Jamming			Tamper	
Force Set			Off	
Tamper Omit			Disabled	
CSID Code			0000	
Silence Alerts			User Code	
Mains Fail Delay			0 minutes	
Set Date & Time				
SNTP Time Sync	SNTP Enable		Off	
	Sync on Startup		Off	
	Sync Daily		Off	
	Manual Sync			
	NTP Server Names		ntp.exnet.com	
Panel Tamper Return			CC	
Level 4 Updates			Disabled	
Panel Upgrade				
5 Communications				
Contacts	Recipient A...	Name	Recipient A	
		Tel No 1	Empty	
		Tel No 2	Empty	
		Email	Empty	
		IP Address	Empty	
ARC Reporting	Call Mode		Single	
	Telecoms Priority	Panel Ethernet	1	
		Module *(only displayed if a plug on coms module is fitted)*	-	
	Recipients	Tel. Recipient 1	None	
		Tel. Recipient 2	None	
		IP Recipient 1	None	
		IP Recipient 2	None	
	Account Numbers	Account No W/P1…	000000	
	Report Type		Fast Format	

	Fast Fmt channels		Channel 1: Fire Alarm Channel 2: Hold Up Alarm Channel 3: Burglar Alarm Channel 4: Open / Close Channel 5: Zone Omit (System) Channel 6: Tamper Channel 7: Confirmed Alarm Channel 8: General Fault	Visible only when Report Type is Fast Format.
	CID/SIA Events		Fire Alarm: Yes Hold Up Alarm: Yes Burglar Alarm: Yes Technical Alarm: No Masking: Yes Tampers: Yes Set/Unset: Yes Part Set: Yes Reset: Yes Exit timeout: Yes Omit: Yes RF Supervision: Yes RF Jamming: Yes RF Battery/PSU: Yes Panel Battery: Yes Mains Fail: Yes Faults: Yes Installer Mode: Yes User Code Changed: Yes Time/Date Reset: No Downloading: No	Visible only when Report Type is SIA or CID.
	Restorals		Enabled	
	Burg Comms Rearm		Enabled	Visible only if Confirmation Mode is Basic and Report Type is Fast Format.
	21CN FF Ack time		800ms	Visible only if a PSTN or GSM module is fitted and Report Type is Fast Format.
	Send Tamp As Burg		Disabled	Visible only when Report Type is SIA or CID.
	Dynamic Test Call		Enabled	Visible only if Static Test Call is disabled.
	Static Test Call		Disabled	Visible only if Dynamic Test Call is disabled.
	Unset Comms		Enabled	
Speech Dialler	Call Mode		Disabled	Visible only if a suitable communications module is fitted.
	Messages		None	
	Triggers		None	
	Destinations			
	Call Acknowledge		Enabled	
SMS	Outgoing	Call Mode	Disabled	Visible only if a suitable communications module is fitted.
		Messages	Blank	
		Triggers	None	
		Destinations		
	Incoming	Remote Control	Disabled	
		Forwarding	None	
	PSTN SMS	Protocol	ETSI Protocol 1	Visible only if a suitable communications module is fitted. Own Telephone No is visible only if Protocol is UCP.
		Service Centre Tel	1470,17094009	
		Own Telephone No.	Empty	
Email	Call Mode		Disabled	
	Messages	Home Message	None	
		Message 1-4	None	
	Triggers	Message 1-4	None	
	Destinations	Message 1-4	None	
	Server	Server Name	None	
		Server Port Number	587	
		Account	None	
		Username	None	
		Password	None	
		SSL	Disabled	

Line Fail Response	Panel Ethernet		Audible	
	Module:		Audible	
	Plug-by		Audible	
Line Fail Delay	Panel Ethernet		9s	
	Module:		9s	
	Plug-by		9s	
IP Network (Own)	Web Server	Status	Disabled	
		IP Port Number	80	
		VKP Instant	Disabled	
	Downloader	IP Port Number	55132	
	M2M Interface	Status	Disabled	
		IP Port Number	1895	
	IP Address		192.168.0.100	
	IP Subnet Mask		255.255.255.0	
	Gateway IP Address		Blank	
	DNS IP Address		Blank	
Dynamic DNS	Status		Disabled	
	Provider		No-ip	
	Hostname		Blank	
	Username		Blank	
	Password		Blank	
	Last Update Status			
	Detected ext. IP			
Downloading	Account	Name	Blank	
		Serial Number	Blank	
	Connection Type	Remote		
		Local		
	Rings to Answer		5 rings	
	Answer on one ring		Disabled	
	Access Mode		Call Out Only	
	Phone Book	Tel No 01	Blank	
		Tel No 02	Blank	
	IP Network	IP Address 1	Blank	
		IP Port 1	Blank	
		IP Address 2	Blank	
		IP Port 2	Blank	
	Secure Callback		Disabled	
	Modem Baud Rate		Auto	
	Remote Servicing	Enable Service	Disabled	Visible only for UK systems. Downloader must be enabled by Eaton.
		Serv. On Exit Eng	Disabled	
		Service Call Num	Tel No 1	
		Time Window Start	00:00	
		Time Window End	06:00	
		Next Service Date	24/12/2015	
		Service Interval	180 days	
		Start Service Call		
6 Test				
Sirens & Sounders	Ext. Radio Sirens			
	Wired Sirens			
	Loudspeakers			
	Wired Keypads			
	KEY-RKPZ			
	Internal Sounders			
Wired Keypad				
Radio Keypads	i-rk01			
	KEY-RKPZ			
Expanders	Exp. W/ R1-...			
Walk Test	Chime		Once	
	System			

	Partition			
	Expanders			
	Zones			
Zone Resistances				Visible only is systems that have wired zones.
Signal Strengths	Detectors			
	Radio Keypads	i-rk01		
		KEY-RKPZ		
	External Sirens			
	WAMs			
	Internal Sounders			
Outputs	Radio Outputs			
	Wired Outputs			
	Plug-by outputs			
	Expander Outputs			
Remotes				
User Hold Up Alarms				
Prox Tags				
ARC Reporting	Panel Ethernet			
	Module			
Speech Dialler				
SMS				
Email				
PSU Current	Panel			
	External PSU			Visible only if EXP-PSU is fitted.
Locate Bus Device				
7 View Log				
All Events				
Mandatory Events				
Non-mandatory Events				
8 ABOUT				
Panel				
Expanders				
Keypads				
Comms	Panel Ethernet			
	Module			
Zone mapping	Zone Numbers			
	Zone Addresses			

Chapter 6: Detectors/Devices Menu

This chapter explains the options in the Detector/Device menu.

Detectors

Add/Del Detectors

This option allows you to add and delete radio detectors (zones).

Adding radio detectors

To add a radio detector:

1. Select *Panel* (if applicable) or a radio expander to assign that detector to.
2. Select a zone.

   A "*" to the left of a zone name indicates that the control unit has learned a radio detector for that zone.
3. When prompted, activate the detector's tamper switch to make the control unit learn the identity of the radio detector.

Deleting radio detectors

To delete a single radio detector, select the zone and choose one of the following:

Delete Detector ID

This deletes the ID of the detector, but leaves any zone configuration in place (such as zone type and attributes).

Default zone

This deletes the ID of the detector and sets all the zone configuration to default values.

Note: The deletion takes place immediately, and not when you leave the Installer menu.

When you delete a radio detector, the control unit sets the zone to Not Used, and deletes the identity of the radio detector that it has learned.

Up to three levels of *Delete all* options are provided (see the menu map on page 31). These allow you to delete all radio zones associated with a selected expander, all radio zones that communicate directly with the panel (if applicable), or all radio zones system-wide.

Program Zones

You can program (configure) each zone's behaviour at any time, whether or not a wired detector is connected, or the control unit has learned the identity of a radio detector. Select the zone you wish to program. Please refer to page 26 for details of the zone numbering scheme.

Note:

- If a wired zone does not have a detector connected to it, make sure that its zone type is Not Used (the default).

- If you program a radio zone but the control unit does not have a detector learned for that zone, the keypad displays “Zone programmed but not learned” when you leave the Installer menu.

Name

You can give each zone a 12-character name. The control unit displays this name when, for example, you select the zone or the zone generates an alarm.

Type

The list below shows the available zone types.

Note:

- When configuring zone types, the bottom line of the keypad display shows a “*” to the left of the zone’s current type.
- You can select a zone type quickly by entering the two-digit shortcut number shown in brackets after the type’s name in the list below. For example, enter “05” to select Final Exit. The number does not appear on the display.
- The abbreviation of the type name (e.g. HUA) appears in the top-right corner of the keypad's display when you select a zone.
- When the description specifies “system”, this means the alarm system itself in a part-setting system, or those partitions the zone is allocated to in a partitioned system.
- When several zones are activated at the same time, the control unit processes Hold Up Alarm and Normal Alarm zones first, followed by Fire, and then all other alarm types. The control unit always processes alarms before alerts.

Not Used - NU (00)

The alarm system will not respond when an event triggers this detector. This is the default zone type for all zones.

Hold Up Alarm – HUA (01)

Operating a device programmed as Hold Up Alarm (HUA) will start an alarm whether the system (or partition) is set or unset.

The alarm response for HUA (audible, silent or displayed) depends on the options selected by HUA Response (see page 74). (In a part-setting system, look for HUA Response under *System Options*; in a partitioned system, look in the sub-menu for each partition.)

If a communications module is fitted, there may also be an alarm transmission to the ARC, depending on how you have configured the *ARC Reporting* option (see page 102).

Fire Alarm - FA (02)

Smoke or heat detectors connected to Fire Alarm zones cause the internal sounders to give a pulsing fire signal. Fire alarms operate whether the system is set or unset, and will always trigger communications, if a communications module is fitted and enabled.

When the control unit first learns a radio smoke alarm (for example the DET-RSMOKE), the zone type defaults to “Fire”.

Note that a tamper from a hardwired smoke alarm on a Fire Alarm zone when the system is unset will cause an internal alarm (internal sounders and speakers only).

Normal Alarm - NA (03)

When triggered, a zone of type Normal Alarm will start an alarm provided the system is set.

When the control unit first learns a radio detector, the zone type defaults to Normal Alarm.

24 Hour Alarm - 24 (04)

Activating this zone while the system (or partition) is unset causes an internal alarm (internal sounders and speakers only). Activating this zone while the system (or partition) is set causes an alarm from internal and external sounders.

Final Exit – FE (05)

Zones of this type must be the last detector to be activated on exit, or the first to be activated on entry. You can use zones of this type to complete the setting of the system or partition, or to start the entry procedure. See page 72 to set the exit mode type.

Note: If you give a Final Exit zone any of the Part Set attributes, you can program that zone to behave like a Normal Alarm zone if the user part sets the system. See page 78.

Entry Route – ER (06)

Use this zone type for detectors sited between the Final Exit door/detector and the keypad. If the entry/exit timer is running when an Entry Route zone is triggered, no alarm occurs until the entry/exit timer expires.

Note: If you give an Entry Route zone one of the Part Set attributes, you can program that zone to behave like a Final Exit zone if the user part sets the system. See page 78.

Technical Alarm –TA (07)

Use this zone type when you want to monitor equipment, for example a freezer, without raising a full alarm. If a Technical Alarm zone is activated, the control unit logs the event, generates a fault condition, and (if the control unit is correctly programmed, see page 102) starts communication.

If the technical alarm occurs while the system is set, the system makes no audible alarm. When a user unsets the system, the keypad shows an alert.

If a Technical Alarm zone is activated while the system is unset, the system starts an alert immediately and gives a brief tone from the keypad every few seconds. When a user enters a valid access code, the keypad stops the tone and displays the zone causing the alarm.

When the user acknowledges the alert by pressing ✔, the control unit resets the technical alarm ready for the next event.

Note that a tamper on a Technical Alarm zone when the system is unset will cause an internal alarm.

Key Switch Moment. – KSM (08)

Use this zone type to connect a momentary keyswitch to a single zone.

In a part-setting system, the keyswitch can full set or unset.

In a partitioned system, you can allocate the keyswitch to one or more partitions.

Each time a user operates the keyswitch, the control unit changes the current set state.

Key Switch Latched – KSL (09)

Use this zone type to connect a fixed position keyswitch to a single zone.

In a part-setting system, the keyswitch can full set or unset. As with momentary keyswitches, you can allocate the zone to one or more partitions (see above).

When the user opens the keyswitch contacts, the control unit sets the allocated partition. When the user closes the contacts, the control unit unsets the allocated partition.

Note:

- The keyswitch zone types are intended for use on zones that connect to an access-control keypad, electronic key or other type of hardwired device used to set or unset the system.
- When the user operates the keyswitch while the system is unset, the control unit starts the programmed exit mode.
- When the user operates the keyswitch while the system is set, the control unit unsets the system immediately.
- The user cannot reset the system from a keyswitch zone.
- Do not assign more than one Key Switch Latched zone to a partition.

Tamper – T (10)

Use this zone type to monitor the tamper status of external equipment. The control unit monitors a Tamper zone at all times. When triggered in the unset condition, only internal sounders operate. When triggered in the set condition, the alarm response determines whether external sounders, strobe and communications also respond to the alarm.

External PSU A/C Fail – PAC (11)

Use this zone type to monitor the A/C Fail output of an external power supply unit. If a power supply unit triggers a zone with this type, the control unit treats this in a similar way to a mains fail at the control unit itself. The action taken depends on the values programmed into *System Options – Mains Fail Delay* (see page 98).

This zone type is not available for radio zones.

External PSU Batt Fault - PBF (12)

Use this zone type to monitor the Battery Fault output of an external power supply unit. If an external PSU triggers a zone with this type, the control unit activates any output of type Battery Fault and causes an alert that displays “External Battery Fault” on the keypad.

If the alarm system is set, the control unit logs the event, starts any programmed communication, but does not start an alert until the system is unset.

This zone type is not available for radio zones.

External PSU Low Volts – PLV (13)

Use this zone type to monitor the Low Voltage output of an external power supply unit. If a power supply triggers a zone with this type, the control unit activates any output of type Low Volts and causes an alert that displays “External Low Volts” on the keypad.

If the alarm system is set, the control unit logs the event, starts any programmed communication, but does not start an alert until the system is unset.

This zone type is not available for radio zones.

External PSU Fault – PF (14)

Use this zone type to monitor the fault output of an external PSU. (This zone type is available for power supplies that do not provide specific fault outputs that can be used by zone types 11, 12 and 13.) If a power supply triggers a zone with this type,

the control unit activates any output of type External PSU Fault and causes an alert that displays “External power fault” on the keypad.

If the alarm system is set, the control unit logs the event, starts any programmed communication, but does not start an alert until the system is unset.

This zone type is not available for radio zones.

External WD Fault – WD (15)

Use this zone type to monitor the fault output of an external warning device. If a warning device triggers a zone with this type, the control unit generates an alert that displays “Ext WD Fault” on the keypad.

A user can override this fault and set the system.

If the alarm system is set, the control unit logs the event, starts any programmed communication, but does not generate an alert until the system is unset.

This zone type is not available for radio zones.

HUD Fault – HUD (16)

Use this zone type to monitor the fault output of wired hold-up devices that are capable or reporting faults. When a detector triggers a zone with this type, the control unit generates an alert that displays “HUD Fault” on the keypad. If a user tries to set the system when this zone is active, the control unit displays the fault on the keypad. The user can override the fault and carry on setting.

If the alarm system is set, the control unit logs the event, starts any programmed communication, but does not generate an alert until the system is unset.

This zone type is not available for radio zones.

Log Only – LO (17)

When a detector triggers a zone with this type, the control unit logs the event and activates any outputs that are programmed to follow this zone. The zone is active whether the system is set or unset. Typical uses for this zone type are for integrating the alarm system with a CCTV system.

Note: Zone Follow outputs will activate on both alarm and tamper of a Log Only zone.

Log only zones can be allocated to one or more partitions, and can use the Chime attribute.

Exit Terminate ET (18)

Use this zone type to terminate setting when the system or partition exit mode is Exit Terminate (see page 72). This zone type is designed for a normally-open momentary switch.

Note that this zone type is armed during the setting time, but inactive both while the system is set, and while the system is unset. If you apply the Chime attribute to this zone, the system will give a chime tone when the zone is activated both while the system is unset and while the system is set.

Shunt Key Latching SKL (19)

In a part-setting system (one with no partitions):

- When a user activates this type of zone, the control unit “shunts” any zones in which the attribute Shuntable is set to Yes (see page 50), and activates any output of type Zones Shunted (see page 69).
- While zones are shunted, the control unit ignores the alarm signal from their detectors.
- The detectors remain shunted until a user restores the Shunt Key Latching zone.

- If a shunted detector is active at the time a user restores the Shunt Key Latching zone, the control unit ignores the state of the Shunt Key Latching zone. When all active shunted zones are restored, the control unit will recognise the Shunt Key Latching zone and un-shunt zones when the key is restored.

In a system with partitions, the behaviour of a Shunt Key Latching zone is limited by the partitions that the zone belongs to as follows:

- If the zone is allocated to one or more partitions, then when a user activates the zone, the control unit shunts only zones with the Shuntable attribute in the same partition(s) as the Shunt Key Latching zone.
- If the Shunt Key Latching zone is not allocated to any partitions, then when a user activates the zone, the control unit shunts only zones with the Shuntable attribute attached to the same bus device as the Shunt Key Latching zone. If the Shunt Key Latching zone is connected to the control unit and not assigned to a partition, it will affect only zones with the Shuntable attribute connected to the control unit.

For other ways of shunting zones see Shunt Groups on page 91.

Shunt Key Non-Latch SKNL (20)

This carries out the same function as a Shunt Key Latching, but differs in the method of restoring shunted zones. The control unit changes the shunted/restored state of zones each time a user activates a Shunt Key Non-Latch zone.

Lock Set LS (21)

Use this zone type to complete setting when the system or partition exit mode is Lock Set (see page 73). This zone type is designed for a normally-open switch (one that is open when the lock is locked). Note that this zone type is armed during setting and when the system is set.

A Lock Set zone can take the Inverted attribute.

Do not use Lock Set with a part set; the results may not function as described.

Occupancy OC (22)

This zone type is intended for use with access control systems. If the zone is active when a user tries to set the system, the keypad displays “Tick to continue Occupancy zone active”. By pressing ✔, the user can carry on to set the system and the control unit logs the event. In a partition-based system, an Occupancy zone can be allocated to a partition.

Security SC (23)

This zone type is intended for use if keypads are located in areas that are accessible to non-authorised people while the system is unset. When a Security zone is active, the control unit disables the buttons on all keypads. The display and proximity tag sensor continue to function normally.

If an authorised user presents a proximity tag to the keypad, the control unit activates the keys so that the user can operate the system. The control unit deactivates the keys when that user is finished.

The keypad buttons will work normally when the system is set.

In a partition-based system, you can allocate a Security zone to any partition. When activated, the control unit disables buttons on keypads in the same partition(s) as the Security zone.

Tamper Return TR (24)

This zone type makes it possible to monitor a tamper return wire from an external sounder. The control unit monitors a Tamper Return zone at all times.

When triggered in the unset condition, only internal sounders operate. When triggered in the set condition, the alarm response determines whether external sounders, strobe and communications also respond to the alarm.

This zone type is not available for radio zones.

Perimeter PZ (25)

This zone type intended to be used with external (perimeter) detection equipment. *PZ Unset Response* (see page 75) and *PZ Set Response* (page 76) determine the response to activations of the zone.

A Perimeter zone or the zone's tamper does not contribute to a burg or confirmed alarm.

Partitions

You can use this menu in a partitioned system to assign the zone to one or more partitions. By default, zones belong only to partition 1.

Note:

- This menu does not appear if the zone type is Not Used or you are not using a partitioned system.
- Any zone other than whose type is Not Used must be assigned to at least one partition.
- If you assign a zone to more than one partition, that zone will be set only when all the partitions it belongs to are set.

Press ▲ or ▼ to scroll through the list of partitions followed by ▶ or ◀ to assign/de-assign the zone to each partition as necessary.

An *All Partitions* option is available if the zone type allows the zone to belong to more than one partition (see the Table 9). You can use *All Partitions* to assign or de-assign the zone to or from all partitions.

Table 9: Zone types that can belong to one or more partitions

One partition only		**Any partition**	
01	HUA	03	Normal Alarm
02	Fire	05	Final Exit
04	24 Hr	06	Entry Route
07	Technical	08	Key Switch Momentary
10	Tamper	09	Key Switch Latched
11	External PSU AC fail	17	Log Only
12	External PSU Battery fault	18	Exit Terminate
13	External PSU Low Volts	19	Shunt Key Latched
14	External PSU Fault	20	Shunt Key Non Latching
15	External Warning Device Fault	21	Lock Set
16	Hold Up Device Fault	23	Security
24	Tamper Return	22	Occupancy
		25	Perimeter

Attributes

Table 10 shows the zone attributes and the zone types they apply to. You can assign more than one attribute to a zone. Some attributes may be unavailable for radio zones. The display shows only the available attributes for the zone type you select.

Table 10: Zone attributes available for zone types

	Zone Attributes														
	Chime1	Chime2	Soak Test	Double Knock	Part Set B	Part Set C	Part Set D	Part Set	Omittable	Force Set Omit	Masking	Inverted	Shuntable	Supervision	Reset
Zone Type															
Not Used															
Hold Up Alarm												Y		Y	
Fire Alarm												Y		Y	
Normal Alarm	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
24 Hour Alarm					Y	Y	Y	Y	Y			Y	Y	Y	
Final Exit	Y	Y			Y	Y	Y	Y			Y	Y	Y	Y	
Entry Route	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Technical Alarm	Y	Y			Y	Y	Y	Y	Y			Y		Y	
Key Switch Moment.												Y		Y	
Key Switch Latched												Y		Y	
Tamper			Y		Y	Y	Y	Y	Y	Y		Y		Y	
Ext PSU AC fail									Y	Y		Y			
Ext PSU Batt Fault									Y	Y		Y			
Ext PSU Low Volts									Y	Y		Y			
Ext PSU Fault									Y	Y		Y			
Ext WD Fault									Y	Y		Y			
HUD Fault									Y	Y		Y			
Log Only	Y	Y										Y		Y	
Exit Terminate	Y	Y										Y		Y	
Shunt key Latching												Y		Y	
Shunt Key Non-Latch												Y		Y	
Lock Set												Y		Y	
Occupancy												Y		Y	
Security												Y		Y	
Tamper Return			Y		Y	Y	Y	Y	Y	Y					
Perimeter	Y			Y	Y	Y	Y	Y	Y	Y		Y			

Chime1 and Chime2

When enabled, the system gives a non-alarm chime when the zone is triggered. For all but Exit Terminate zones, the chime operates only when the system is unset. For Exit Terminate, the chime operates when the system is set or unset.

Chime1 and Chime 2 have different tones, and can be used to distinguish zones.

Soak Test

Use this zone attribute if you want to place under long term test a detector that you suspect is giving false alarms. Zones with this attribute are disabled for 14 days after you return the control unit to user/unset mode. If the zone remains inactive for the

whole fourteen days then after midnight on the 14th day, the control unit returns the zone to normal use.

If the zone is activated during those 14 days while the system is set, the control unit logs the event as a "Soak Fail Znnn Alm" (nnn is the zone number, see page 26) without sounding any sirens or starting communications. The control unit also lights the red LEDs around the navigation key on the keypad to alert the user when they unset the system. An installer must key in their access code to reset the alert.

During setting, the keypad displays a brief message to inform the user that one or more zones are in soak test.

Note: If there is an output configured as type Zone Follow for a zone under Soak Test, the control unit will continue to operate the output if the soak test zone is triggered. The output will operate whether the zone is set or unset.

Double Knock

Zones programmed with this attribute will cause an alarm only if the zone is EITHER triggered, restored and triggered again within a five-minute period, or if the zone remains active for 10 seconds.

Note: Double Knock does not comply with EN50131.

Part Set B

(Not visible in a partitioned system.) When a user sets part set B, the control unit sets only those zones where the Part Set B attribute = "Yes". (See also "Part Set Exit Mode" on page 72.)

Part Set C

(Not visible in a partitioned system.) When a user sets part set C, the control unit sets only those zones where Part Set C attribute = "Yes".

Part Set D

(Not visible in a partitioned system.) When a user sets part set D, the control unit sets only those zones where Part Set D attribute = "Yes".

Part Set

(Only visible in a partitioned system.) When a partition is Part Set, zones in that partition with this attribute are set. Note that if a zone is in more than one partition, all partitions have to be set or part set before this zone will be set.

Omittable

When a zone has this attribute, a user can omit it before setting the system.

If a user tries to set the system when a zone with this attribute is open (active) the control unit alerts them and pauses the setting procedure. The user can acknowledge the alert by pressing ✔ and continue setting, providing the feature is enabled in *System Options – User Access – Quick Omit* (see page 84).

Note: Take care when assigning Omittable to an Entry Route zone when Quick Omit is enabled. There is a risk that the user may omit the Entry Route zone in error.

Force Set Omit

When this attribute is set to Yes, a user with a remote control can set the system while the zone is open (active), providing the feature is enabled in *System Options – Force Set* (see page 97).

Masking

Apply this attribute either if you have connected a detector that reports masking by changing the resistance between its mask/fault contacts, or if you have connected the masking/trouble contacts of a detector using the "3 resistor method" (see the

installation instructions). Note that you must enable *System Options – Masking* (page 89) to make this attribute visible.

Note: You cannot apply the Masking and the Inverted attributes at the same time.

Inverted

On FSL zones, the attribute makes the control unit treat resistances in the 6k9 band as “tamper”, and resistances below the 2k2 band as “alarm”. In 4-wire CC zones the attribute makes the control unit treat open alarm contacts as “no alarm” and closed alarm contacts as “alarm”. (Tamper contacts are not affected by the Invert attribute.)

You can apply this attribute to any zone type except Tamper Return and Not Used.

Note: You cannot apply the Inverted and the Masking attributes at the same time. The Inverted attribute does not apply to radio zones.

Shuntable

Apply this attribute to zones that you wish to be shunted.

If you give a zone this attribute, you may also want to assign the zone to a shunt group (see page 91).

If you wish to set up a shunt key, see page 45.

Supervision

This attribute is available for radio zones (not wired zones), and allows you to enable/disable supervision for individual zones.

When set to Yes (the default), supervision for this zone is the same as the selected option in *System Options – Supervision* (see page 96). When set to No, supervision is disabled for his zone.

Reset

Enable this attribute if you have connected a latching type of shock or vibration sensor to a zone. You will also need to program an output of type Shock Sensor Reset.

The control unit ignores the zone during setting while the Shock Sensor Reset output is active, and for an extra three seconds after the output restores.

Note: It is recommended that you set the exit time to a value not less than 10 seconds to allow detectors to reset correctly and avoid the possibility that the control unit will isolate a zone that has not reset.

If the exit time is less than 10 seconds and the detector does not successfully reset (it remains in an active state), the control unit will not add the detector back to the system until detector becomes inactive. This is to prevent false alarms.

Resistance

This option allows you to specify the resistance values used by an individual FSL zone on either the control unit, an EXP-W10/WCC or an EXP-PSU. This option is not available if the control unit or bus device is has been programmed as 4-wire or 2-wire CC connection.

Address Bus Device

You can use this option to add new bus devices to the system once they are physically wired to the bus, and to scan the bus for any found or missing devices. The control unit assigns a bus address (see page 25) to each device you add.

You can add any type of bus address using this option. An alternative method for wired expanders, radio expanders and keypads, is to use the specific *Address Bus Device* option (for example, *Detectors/Devices – Wired Expanders – Address Bus Device*).

Note: If you need to replace or remove a device, please refer to page 136.

To add new bus devices to the system:

1. From the Installer menu, select *Detectors/Devices – Address Bus Device*, and press ✘ when you see "Re-scan bus?". The following is displayed:

   ```
   Press addr button(s)
   on bus devices
   ```

2. When you see the above message, the control unit is ready to allocate an address to each additional bus device that has a "null" address. The control unit allocates the next available address when you press the following button/keys:
   - **At a keypad:** press and hold “A” and “✔” together. Release the keys when you hear a sound. The display shows the allocated address, such as "b1-d52" (bus 1, device 52).
   - **At an expander:** press and hold the “Request Address” button. Release the button when the display shows the bus address. If you do not want to use the address shown, press the button again as many times as necessary to display the required address. **Note:** An expander cannot obtain an address if the "Disable Tamper" link is fitted.
   - **At other types of device:** please refer to the device installation instructions.

   Note: Do not attempt to obtain an address for two devices at the same time.
3. When you have finished addressing all devices, press ✘.

Re-scanning the bus

The control unit keeps a record of every bus device that it has learned. To keep the list up to date, the control unit scans the bus during power up and when you leave the Installer menu. You can also scan the bus by pressing ✔ when you see the "Re-scan bus?" prompt after selecting *Detectors/Devices – Address Bus Device*.

During a scan, the control unit queries every device on the bus to report its bus address. The control unit then compares the reported addresses with those that is has stored and may report:

- **Duplicate bus addresses** – That is, devices that have the same address. You will need to change the address of one of the devices to make it unique.
- **Found and/or lost bus devices** – If the control unit finds that a device is on the bus that has not been added using the Installer menu, or that a previously-added device is missing, the display shows, for example:

  ```
  FOUND 0, LOST 1
   Lost R1-03
  ```

  The top line shows the number of new devices found, and the number of existing devices lost. The bottom line shows the first in the list of found and lost devices. You can use the up/down navigation keys to scroll through the list.

  If you see that there are found or lost devices:

  - **Either:** Press ✘ to return to the Installer menu to check that all devices are listed and addressed correctly. Make sure that the devices are powered up.

    Tip: To check the address of an expander, remove the lid and briefly press the addressing button. The two-digit display shows the bus address for a few seconds. For example “b1” followed by “08” is “bus 1 device 08”.

- **OR:** Press ✔ to make the control unit update its internal record of devices attached to the bus. The display shows:

  ```
  Accept all changes
        to bus
  ```

  Press ✔ to accept the changes, or press ✘ to return without making changes.
  Note: Accepting changes deletes all programmed information for any lost devices.

  Changes are not saved until you leave Installer menu. If the control unit loses power before leaving Installer menu, the bus re-configure does not take effect.

Wired Expanders

Address Bus Device

You can use this option to add a wired expander to the bus once it is physically wired to the bus. The following is displayed:

```
Press addr button(s)
on bus devices
```

Please refer to page 51 for details of how to proceed. The control unit assigns a bus address (see page 25) to each device you add.

Note:

- If the expander you are adding already has a bus device number stored within it, you may need to clear the address before adding it to the bus. You can do this manually by pressing the Request/Delete Address button while applying power to the expander, or by using *Delete Expander* (page 53).
- Use the *Detectors/Devices – Address Bus Device* to give an EXP-PSU a bus address.

Edit Expander

You can use this option to edit settings for a specific expander.

Note: If you wish to find out where the device is located, press "*". The displayed device will sound a continuous tone. Press "#" to stop the tone.

The following options are available.

Name

You can give each expander a name. The name appears in the log, in alerts and when configuring the expander.

Partitions

In a partitioned system, an expander must belong to at least one partition. You can use this option to assign each expander to one or more partitions. By default, an expander belongs only to partition 1.

An expander gives notification tones for every associated partition through the expander's loudspeaker (if one is connected).

If any associated partition is set, a tamper at the expander will cause an unconfirmed alarm. If there is an outstanding unconfirmed alarm, this will cause a confirmed alarm to be generated.

An *All Partitions* option is available to assign or de-assign the expander to or from all partitions.

Wired Zone Type

You can change the zone wiring method for each wired expander individually. The available options can depend on the expander type.

Please refer to page 14 for details of the wiring types.

Loudspeaker Volume

You can use this option to change the volume of notification tones from loudspeakers attached to expanders. Press ◄ to lower the volume or ► to raise the volume. The display shows the current volume setting by a row of stars (for example "****"). You can also press one of the number keys to specify the volume in a range 0 to 9 (for example, pressing "8" gives you eight stars on the display).

This volume control does NOT change the volume of alarm tones, the control unit will still give these at full volume.

Note: When you first add an expander to the bus, the control unit defaults the loudspeaker volume to zero.

Battery 2

This option is available when editing an EXP-PSU. You can use the option to enable or disable alert reporting on a second backup battery that may be fitted within the EXP-PSU.

If you select Enabled, the control unit will start an alert if battery 2 is missing or has low voltage. If you select Disabled, the control unit will ignore the presence or absence of battery 2.

Delete Expander

Always use *Delete Expander* when you wish to remove a wired expander from the bus. Using this option defaults the bus device number stored within the device (making the device safe to add to other systems) and deletes zones and outputs associated with the device. Exit the Installer menu to save the change.

Note: Remove all power from the system (battery and mains) before disconnecting any device from the bus.

Enable Expander

Set this option to No if you suspect that the device is faulty, and wish to remove it from service temporarily.

The effects of disabling any expander or keypad are as follows:

- The control unit ignores all signals from the device, but retains the zone numbers and other configuration allocated to the device.
- The control unit activates any output of type General Fault.
- A disabled keypad shows flashing red navigation LEDs (and will not accept any user input).
- Keypads (those that are enabled) show an alert (navigation key LEDs glow red). When a user reads the alert, the display shows "Tick to continue Disabled" followed by the device number of the disabled device. If a user tries to set the system, the

keypad displays the same alert message again, but will continue to set the system if the user presses ✔.

- The system omits all zones belonging to the disabled device.

Replace Expander

Use this option if you wish to replace an expander with a new expander, but leave the expander's configuration intact in the control unit.

When you use *Replace Expander*, the control unit disables the selected expander, but retains the expander's zones and other settings. You can then power down the system, disconnect the expander from the bus, and reconnect a new expander (of the same type) to the bus.

When you power up the control unit again, the keypads will show an alert that the expander has been disabled. Select *Replace Expander* again, select the *Add* option and then hold down the address request button on the new expander (with the tamper switch activated). The control unit will assign the bus device address of the device you removed to the new device, along with all the zones and other configuration from the old device. The new device will not need any further configuration.

Note: If you replace a radio expander, you must teach the identity of the new radio expander to any receivers (such as 762s, 768s or WAMs) that had previously learned the old expander's identity.

Radio Expanders

You can use *Detectors/Devices – Radio Expanders* to add, edit, delete, enable/disable and replace radio expanders. The options for radio expanders are similar to those for wired expanders, as described from page 54.

Wired Keypads

Address Bus Device

Use this option to add a wired keypad. The control unit assigns a bus address (see page 25) to each device you add.

If the keypad you are adding already has a bus device number stored within it, you will need to clear the address before adding it to the bus. You can do this manually by pressing the D and ✘ keys while the keypad's tamper switch is open, or by using *Delete Keypad* (page 56).

Edit Keypad

You can use this option to edit settings for a specific keypad.

Note: If you wish to find out where the device is located, press "*". The displayed device will sound a continuous tone. Press "#" to stop the tone.

Name

You can give each keypad a name. The control unit displays the name when it is reporting faults or other events, making it easier to locate the affected device.

Partitions

In a partitioned system, a keypad must belong to at least one partition. You can use this option to assign each keypad to one or more partitions. By default, a keypad belongs only to partition 1.

Note: If you do not assign a keypad to a partition (and there is no loudspeaker assigned to the partition), users of that partition will not be able to hear entry/exit tones and alerts for the partition.

Once you have assigned a keypad to a partition:

- The keypad will display messages and give tones for the assigned partition(s).
- A Partition User can use only keypads assigned to the same partition as the user's code or proximity reader tag.
- All other users can use any keypad. While they are using a keypad, the display shows information from partitions assigned to the user, not to the keypad. Once the user has finished with a keypad, the keypad reverts to showing information from the partition(s) it is assigned to. If you do not allocate keypads to the correct partitions, this may mean that a keypad will show alerts from a partition that a user is not authorised to set or unset.

An *All Partitions* option is available to assign or de-assign the keypad to or from all partitions.

Key A/B/C/D

These options allow you to program the A, B, C and D (quick-set) keys.

In a part-setting system, you can enable the quick-set keys to full set the system, or part set part sets B, C and D.

In a partitioned system, you can enable a quick-set key to full set or part set individual partitions.

Alternatively, in both part-setting and partitioned systems, you can program a quick-set key to trigger a user-defined output (see page 69).

Each keypad can have a different arrangement of quick-set keys. For example, the A key on keypad K-51 might part set partitions 1 and 2, but on keypad K-52, it could be programmed to full set partition 3.

Each quick-set key can have a name. The keypad displays this name while the system is setting after the user presses that key.

Note:

- The partition(s) that the keypad is allocated to does not influence the configuration of the quick-set keys. A user will be able to set any partition that the user is allowed to set.
- The ABCD LEDs at the keypad show the state of the quick-set keys. When all the partitions/part sets that a quick-set key is allocated to are set, the associated LED glows. For example, if quick-set key A is programmed to full set partition 1 and part set partition 4, then whenever partition 1 is full set and partition 4 is part set, LED A glows.
- If you enable the quick-set keys, the control unit no longer complies with EN50131. See page 83.
- The control unit logs the use of quick-set keys under a quick-set user identity (see page 130).

Zones
This option applies to keypads that have zone connections. You can use this option to enable or disable the zones. You can use *Detectors/Devices – Detectors – Program Zones* to give keypad zones the required properties (see page 41).

Please refer to page 28 for details of zone addressing for keypads.

If you disable the zones after enabling them, the control unit deletes all properties belonging to those zones.

Wired Zone Type
This option applies to keypads that have zone connections. Please refer to page 14 for details of the wiring types.

Loudspeaker volume
This option is available for keypads that have connections for an external loudspeaker. The option sets the volume of the loudspeaker.

Buzzer volume
This option is available for the KEY-FKPZ. The option sets the volume of all tones at the keypad that originate from the control unit (such as entry/exit tones). The keypad may have a local option for setting the volume of tones that originate from the keypad – please refer to the keypad's installation instructions.

Backlight
Use this option to control the brightness of the backlight on keypads such as the KEY-KPZ01 and KEY-FKPZ.

Mode

This controls whether the backlight is on or off. This can be set to:

- Timed – The backlight is normally off, but glows when a user presses keys. The backlight stays on for eight seconds after the last keypress or prox tag use. The backlight also comes on during the entry time and when the system is in alarm
- On – The backlight is permanently on.
- Off – The backlight is permanently off.

Note: The *Mode* option has no effect if you have set backlight behaviour locally at the keypad. Please refer to the keypad's installation instructions.

Brightness

This controls the brightness of the backlight. The option has no effect if you have set brightness locally at the keypad.

External Prox
This option appears for keypads that provide connections for an external proximity reader.

Use this option to enable or disable the external proximity reader.

You also need to configure *System Options – User Access – Terminated Set* (see page 84) if you are using an external proximity reader.

Delete Keypad
Always use *Delete Keypad* when you wish to remove a wired keypad from the bus. Using this option defaults the bus device number stored within the device (making the device

safe to add to other systems) and deletes zones and outputs associated with the device. Exit the Installer menu to save the change.

Note: Remove all power from the system (battery and mains) before disconnecting any device from the bus.

Holding down D and ✘ at a keypad while its tamper switch is open clears the address from the keypad. Normally, you should clear the address only by using *Delete Keypad*. If you have used D and ✘ at a keypad that is known to the system and still connected to the bus, you can either power the control unit down and up again for it to recognise the keypad (you will be prompted to press the A and ✔ keys), or go to another keypad and use *Delete Keypad* to delete the keypad.

Enable Keypad

Use this option and set the enable status to “No” if you suspect that the device is faulty, and wish to remove it from service temporarily.

The effects of enabling/disabling a keypad are described on page 59.

Replace Keypad

Use this option if you wish to replace a wired keypad with a new keypad, but leave the keypad's configuration intact in the control unit.

When you use *Replace Keypad*, the control unit disables the selected keypad, but retains the keypad's zones and other configuration. You can then power down the system, disconnect the keypad from the bus, and reconnect a new keypad (of the same type) to the bus.

When you power up the control unit again, the remaining keypads will show an alert that the old keypad has been disabled. Select *Replace Keypad* again, select the *Add* option and then hold down the A and ✔ keys on the new keypad. The control unit will assign the bus device address of the device you removed to the new device, along with all the zones and other configuration from the old device. The new device will not need any further configuration.

Radio Keypads

i-rk01

The i-rk01 1-way radio keypad is a transmitter that users can employ to set, unset and silence alarms on the system remotely. The radio keypad is a transmitter only, and does not display any system information or make any alarm, entry, exit tones etc. The LEDs on the radio keypad glow to show that it is transmitting a signal. There are no set status LEDs.

Note: When delivered from the factory, i-rk01 radio keypads transmit four-digit access codes. If you change the system to use six-digit access codes, radio keypads will no longer function with access codes (they will still function with prox tags). It is possible to change a radio keypad to transmit six-digit access codes. Please refer to the i-rk01 installation instructions.

When installing a radio keypad, you must first teach the control unit the radio keypad's identity. In addition, you can give each radio keypad a name. You can also program the control unit with the function of each of the radio keypad's A, B, C or D buttons.

In a partitioned system, you can assign a radio keypad to any combination of partitions, just as you can for the wired keypads.

When delivered from the factory, or if you restore the control unit to factory settings, all radio keypads belong to partition 1. The A, B, C and D keys operate on partitions 1, 2, 3 and 4 respectively.

After assigning a keypad to any other partition(s), you must re-program the A, B, C and D keys to make sure that they operate correctly. The A, B, C and D keys will work only with partitions that you have assigned to the radio keypad.

See page 25 for a description of radio keypad numbering.

To make the control unit learn a radio keypad's identity:

- From the *i-rk01* menu, select *ADD/DEL Radio Keypad*. Select the radio expander you wish to use, followed by the radio keypad address that you want to allocate the keypad to. You must then activate the radio keypad's tamper to make the control unit learn the identity of the keypad.

To remove a Radio Keypad from the system:

- From the *i-rk01* menu, select *ADD/DEL Radio Keypad*. Select the radio expander the keypad is allocated to, followed by the device address of the keypad that you want to delete.

To name a radio keypad:

- From the *i-rk01* menu, select *Edit Keypads – Name.*

To assign radio keypads to one or more of the partitions (if available):

- From the *i-rk01* menu, select *Edit Keypads – Partitions*.

  Once you have entered the *Edit Keypads – Partitions* option, press ▲ or ▼ to scroll through the list of partitions followed by ▶ or ◀ to allocate/deallocate the radio keypad to each partition as necessary.

  You can use *All Partitions* to allocate a radio keypad to all partitions.

To program the ABCD keys:

- In a partitioned system, the ABCD keys can be programmed in the same way as for a wired keypad. You can allocate each key to setting and unsetting any combination of partitions that the keypad belongs to. From the *i-rk01* menu, select *Edit Keypads.* Select the keypad you wish to edit. Select the key you wish to edit. Allocate partitions as required.
- In a partitioned system, the ABCD keys default to the following functions: A Full = Set Partition 1, B = = Full Set Partition 2, C = Full Set Partition 3, D = Full Set Partition 4.
- In a part-setting system, the ABCD keys default to the following functions: A = Full Set, B = part set B, C = part set C, D = part set D.
- In either part setting or partitioned systems, the ABCD keys can be configured to operate outputs of type User Defined.

Single-action unset for BS8243/DD243 from a radio keypad:

- The radio keypad is capable of providing single-action unset. You can enable or disable this feature by using a jumper on the "DD243 Single Action Unset" pins on the radio keypad's printed circuit board.

If the **jumper is fitted**, the radio keypad transmits an unset command two seconds after the user presents a recognised proximity tag. This feature is designed for use when the keypad is working with BS8243/DD243 compliant systems.

(Note that this delay does not apply to the setting procedure.)

If the **Jumper is not fitted**, the keypad transmits a command after a user has presented their proximity tag, and then pressed another key (A, B, or unset).

KEY-RKPZ

Address Bus Device

This option allows you to add a KEY-RKPZ 2-way radio keypad from another existing keypad. Select the option and then hold down the A and ✔ buttons on the new keypad. The control unit assigns a bus address and displays it at the keypad you are using (on the top line of the display). For further information, please refer to the keypad's installation instructions.

Edit Keypad

To program a KEY-RKPZ, use the *Edit Keypad* option and select the keypad. If you wish to find out where a keypad is located, press "*". The displayed keypad will sound a continuous tone. Press "#" to stop the tone.

The *Edit Keypad* menu contains the following options:

Name

To change the keypad's name, which appears in reported reports faults or other events.

Partitions (partitioned system only)

To assign the keypad to partitions. The procedure is similar to assigning wired keypads to partitions; see page 55.

Key A/B/C/D

To program the quick-set keys (A, B, C and D). The procedure is similar to configuring quick-set keys for wired keypads; see page 55.

Zones

To enable or disable zones that connect directly to a keypad. The procedure is similar to enabling or disabling zones for wired keypads; see page 56.

Zone Type

This is for future use. Use only 2-wire FSL.

Delete Keypad

Use this menu option to delete a radio keypad from the system. This clears the bus address stored within the keypad and deletes the record of that address from the control unit. After using this option, make sure you leave the Installer menu in order to make the control unit save the change(s) you have made.

Enable Keypad

You can use this option to disable or enable a keypad. You may want to disable a keypad if you suspect that it is faulty, and wish to remove it from service temporarily. While the keypad is disabled, the control unit ignores all signals or input from the device, but retains the name and other settings allocated to the device.

The navigation LEDs at keypads other than 2-way radio keypads glow red when a radio keypad is disabled.

If a user tries to set the system, the keypad displays “Tick to continue Disabled”, together with the address of the disabled keypad, but will continue to set the system if the user presses ✔.

Replace Keypad

Use this option if you wish to replace a damaged or malfunctioning keypad with a new one, and there is at least one other keypad on your system. When you use *Replace Keypad*, the control unit disables the selected keypad, but retains the keypad’s name and other settings.

To replace a keypad:

1. Select *Replace Keypad* at another keypad, and choose the keypad to replace. When prompted, confirm the replacement.
2. Pair the replacement keypad with the base station.
3. Select *Replace Keypad* again, and choose the keypad you replaced (the display shows "Add" in the bottom-right corner).
4. Hold down the A and ✔ keys at the new keypad. The control unit assigns the bus device address of the keypad you removed to the new keypad, along with the name and other settings from the old keypad. The new keypad will not need any further configuration.

   The control unit assigns the bus device address of the keypad you removed to the new keypad, along with the name and other settings from the old keypad. The new keypad will not need any further configuration.

External Sirens

This menu allows you to add, delete and edit external radio sirens.

To use an external radio siren, the control unit must either have built-in radio or you must add a radio expander first. Each radio expander can support up to two external radio sirens. See Table 1 on page 2 for the maximum number of radio sirens per control unit.

Add/Del Siren

To add or remove a radio siren, select *Add/Del Siren*, select the expander (if applicable), then choose one of the siren numbers (names). If you are adding a siren, activate the tamper switch when prompted or connect power to the siren (please refer to the siren's installation instructions).

Edit Siren

This contains:

Name

Allows you to name the device

Partitions (partitioned system only)

Assigning a siren to partitions causes the siren to activate when there is an alarm in any assigned partition. **Note:** If any assigned partition is set, a tamper to the radio siren will cause an unconfirmed alarm. If there is an outstanding unconfirmed alarm, this generates a confirmed alarm. You can use the “All Partitions” option to allocate or de-allocate the radio siren to all partitions.

Internal Sounders

This menu allows you to add, delete and edit internal radio sirens.

See Table 1 on page 2 for the maximum number of internal sounders per control unit.

Add/Del Sounder

To add or remove an internal radio sounder, select *Add/Del Sounder*, select the expander (if applicable), then choose one of the sounder numbers (names). If you are adding a sounder, activate the tamper switch (please refer to the sounder's installation instructions).

Edit Sounder

This contains:

Name

Allows you to name the device.

Partitions (partitioned system only)

This has the same purpose as allocating partitions to an external radio siren (see above).

WAMs

Each control unit can learn the maximum number of WAMs given in Table 1 on page 2.

Although the WAM provides five different modes, only mode 1, repeater module, is relevant. The installer must select the repeater mode when commissioning the WAM hardware.

When working as a repeater module, the WAM repeats the signals from any detectors within its range, amplifying them to a level that the control unit can detect. This allows you to increase the area covered by radio detectors.

Note: A WAM cannot repeat signals for other radio devices.

Use *Edit WAM* to give each WAM a meaningful name. The name can be up to 12 characters long.

Cameras

You can use this option to add up to four network (IP) cameras. When a specified trigger (event) occurs, the control unit acquires JPEG images from the camera and saves them to a locally-fitted SD card (purchased separately). For each trigger, 15 images are saved: one image per second for 5 seconds prior to the event, and one image per second for 10 seconds after the event.

Note:

- If you set up a corresponding email trigger (page 114), the control unit sends the images by email to specified recipients.
- You can view the images stored on the SD card using the web interface or by inserting the SD card into a computer.
- Before using this option, set up each camera as described in the camera installation instructions.
- The control unit periodically polls each camera and reports if there is no response.

IP Cam 1...

Select the camera you wish to configure. The following options are available for each camera:

Camera Triggers

Select the events that are to trigger images to be saved from the camera. For example, if you select Yes for Fire Alarm, the control unit will save images from the camera whenever a fire alarm occurs. You can select any one of the following events (these mimic the output types; see page 63 onwards):

- Fire Alarm
- Hold Up Alarm
- Burglar Alarm
- Technical Alarm
- 24 Hour alarm
- Perimeter
- Duress Code
- Tampers
- Full Set
- Part Set
- Unset
- Zone Follow
- Zone Alarm

Zone Follow

This is displayed only if *Camera Triggers – Zone Follow* is set to Yes. You can choose the zones for the Zone Follow trigger.

Zone Alarm

This is displayed only if *Camera Triggers – Zone Alarm* is set to Yes. You can choose the zones for the Zone Alarm trigger.

Trigger Partitions

In a partitioned system, you can choose the partitions the camera and camera triggers apply to.

IP address

Specify the IP address of the camera.

HTTP Port Internal

Specify the port used to communicate with the camera (default is 80).

Chapter 7: Outputs Menu

This chapter explains the options in the Outputs menu.

Radio Outputs

Add Outputs

To use a radio output, you must use this option to teach the identity of the receiver to the control unit.

Note: If you are teaching 762r or 768r receivers, make sure that you disable IR learn on the receivers first.

Note: Please refer to page 26 for details of how outputs are addressed.

Edit Outputs

Name

Specify a name for each output you want to use.

Type

Select the output type, as described below.

Note: You can select an output type quickly by entering the number shown in brackets after the type's name, for example:"04" to select Open/Close. The number does not appear on the keypad display.

Not Used (00)

The output is never active.

Fire Alarm (01)

Active when the control unit starts a fire alarm.

Hold Up Alarm (02)

Active when the control unit starts a hold up alarm.

Burglar Alarm (03)

Active when any of the following zones are triggered while set: Normal Alarm, Tamper (in a set system), Entry Route, Tamper Zone (in a set system), Entry time expires, 24 hour (in a set system).

Open/Close (04)

Active when the system (or partition) is unset. Inactive when the system (or partition) is set. If you allocate this output to multiple partitions, the output will deactivate if any one partition is set or part set.

Note: This output is inverted relative to other outputs, it is normally at 0V for an unset (open) system.

Alarm Abort (05)

Active when an alarm in the selected partition has been aborted by the user within the abort period. Deactivates when the alarm is reset.

Technical Alarm (06)

Active when there is a technical alarm. Deactivates when the zone causing the alarm is restored AND a user enters a valid access code to acknowledge the technical alarm alert.

Confirmed Alarm (07)

Active when there is a confirmed alarm. Deactivates when the system is reset. The operation of this output type depends on the option selected in *System Options – Confirmation – Confirmation Mode* (see page 86):

RF Low Battery (08)

Active when a wirefree detector reports a low battery. The output remains active until all detectors stop reporting low batteries.

RF Supervision (09)

Active when there is a supervision failure on any radio zone. The output remains active until all supervision failures are reset.

RF Jamming (10)

Active when the control unit detects jamming. The output remains on until all jamming disappears and the system is reset.

RF Fault (11)

Active when there are any of the following faults: RF Low Battery, RF supervision, RF jamming and the system is reset.

A/C Fail (12)

Active when either mains power is absent, or a zone of type External PSU A/C Fail has been triggered. The action of this output depends on the value programmed in *System Options – Mains Fail Delay* (see page 98).

Battery Fault (13)

Active when the control unit detects a fault with its backup battery, or a zone of type External PSU Battery Fault has been triggered. If the alert was caused by an External PSU Battery Fault zone, the control unit deactivates the output when the zone has been restored and a user has acknowledges the fault by entering a valid access code.

If the alert was caused by a fault with the control unit's backup battery, the control unit deactivates the output when it detects a good battery.

Ext PSU Low Volts (14)

Active when an external power supply has triggered an External PSU Low Volts zone.

The control unit deactivates the output when the zone has been restored and a user has acknowledges the fault by entering a valid access code.

Ext PSU Fault (15)

Active when an external power supply triggers a zone of type External PSU Fault.

The control unit deactivates the output when the zone has been restored and a user has acknowledges the fault by entering a valid access code.

Tamper (16)

Active when the control unit detects a tamper at the control unit (lid or back), or at a wired keypad, radio keypad, detector, expander, sounder, or when there is an activation of a zone of type Tamper.

The control unit deactivates the output when tamper is reset.

Zone Omit (Setting) (17)

Active when the user omits a zone while setting the system. The output deactivates when the control unit restores the zone.

Zone Omit (System) (18)

In the event of an unconfirmed alarm, the system will rearm itself when the confirmation timer expires. If the zone that caused the unconfirmed alarm is still active at the time of the rearm, the control unit will omit that zone and activate the output. The control unit will restore the zone and output when a user or engineer resets the system.

General Fault (19)

Active when there is any event that causes an alert indication on the keypad. This includes: RF Low Battery, RF Supervision, RF Jamming, AC Fail, Battery Fault, PSU Fault, Tamper and Masking.

Note that a General Fault output will trigger within a few seconds of an AC Fail, and is NOT affected by the Mains Fail delay setting.

ATS Test (20)

Active when the line fault input signal goes to 12V. The output remains active for one second. The operation of the Line Fault input and the ATS Test output complies with the requirements of BSIA form 175.

This output type appears only for plug-by outputs.

Siren (21)

Active when the control unit starts a full alarm, a hold up alarm or a fire alarm (the siren has a distinctive tone during a fire alarm). The control unit deactivates this output at the end of the siren time. See page 75 to choose the siren duration.

Strobe (22)

Active when either of the following occurs:

a) The control unit starts a full alarm, hold-up alarm or fire alarm. The output remains active until the user disarms the system.

b) Setting or unsetting, if you have selected “strobe on set” and/or “strobe on unset” (see page 77).

Entry Exit Follow (23)

Active when the entry or exit time starts and deactivates at the end of the entry/exit time, or if the entry/exit time is terminated. The output can be used for a separate entry/exit buzzer. Note that the output does not operate if the exit mode is silent set or instant set.

Armed (24)

Active when the system (or partition) is full or part set.

PIR Set Latch (25)

Active when the system or partition is set. Inactive when the system or partition is unset or an alarm condition occurs. The output is active for one second when a reset is performed or when the control unit leaves installer mode.

Note: By default this output is at +12V when active and 0V when inactive. Use the Inverted attribute if you wish to change this behaviour.

Shock Sensor Reset (26)

Active when the exit time starts. The output remains active for five seconds. Use this output to reset shock sensors (for example, the "Viper").

Walk Test (27)

Active when a user starts Installer or User Walk Tests. Also active during the time between silencing and resetting the system. This output can be used on movement detectors that are able to switch off the Walk Test lamp in any state other than a Walk Test.

Smoke Sensor Reset (28)

This output is active (0V) all the time except when a user acknowledges a fire alarm. After which, the control unit deactivates the output for three seconds. This output type is designed to be connected to low-voltage smoke detector reset terminals.

Note: Some smoke detectors (for example the Texecom OH 4W) require that the user reset the system twice after an alarm. This is to give the detector time to close its alarm contacts after the reset pulse.

24 Hour Alarm (29)

Active when the control unit starts a 24-hour alarm.

Setting Complete (30)

Active when the control unit finishes setting. Active for 10 seconds.

Unset Complete (31)

Active when someone unsets the system or disarms it after an alarm. The output is active for 10 seconds.

Full Set Ready (32)

Active when no detectors are reporting “alarm” signals.

Full Set (33)

Active when the system is full set. If the system is partitioned, the output is active only when all assigned partitions are Full Set.

Part Set (34)

Active when the system is part set.

Part Set B (35)

Active when setting Part Set B. Deactivated on unsetting Part Set B. (Available only in a part-setting system.)

Part Set C (36)

Active when setting Part Set C. Deactivated on unsetting Part Set C.(Available only in a part-setting system.)

Part Set D (37)

Active when setting Part Set D. Deactivated on unsetting Part Set D. (Available only in a part-setting system.)

Set Fail (38)

Active when a set command fails. Remains active until the user acknowledges the set fail.

Zone Follow (39)

Active when any selected zone is active, irrespective of whether the zone is set or unset. The zones can include Log Only zones. Specify the zones using the *Zones* option (see page 70).

Zone Alarm (40)

Active when any selected zone is in alarm. **Note:**

- The zone must be capable of causing an alarm, such as zones of type Fire Alarm, Normal Alarm, Entry Route, Tamper, 24 Hour and Technical. A Final

Exit zone will also cause an alarm if the Entry Time runs out before the user unsets the system.

- The zone must be set, unless it is a Fire Alarm zone. In a part-setting system, either the system must be full set, or the zone must belong to the part set that the user has selected. In a partitioned system, all the partitions that the zone belongs to must be set. If a partition is part set, the zone must belong to the part set that the user has selected

The output deactivates when the alarm is reset. Specify the zones using the *Zones* option (see page 70).

Masking (41)

Active when a detector is giving a mask signal (see page 89).

Autoset Warning (42)

Active when the control unit starts the period defined by a calendar set Warning Time (see page 80). Deactivates when the system sets, or if a user defers or cancels the calendar set.

User Defined (43)

Activated when by any one of the following events:

- A user presses a button on a remote control that has been configured to activate a user-defined output.
- A user operates the output from the *User Menu – Outputs On/Off* option.
- A user presses one of the A, B, C or D keys on a keypad that the installer has programmed to operate a user-defined output.

When you select this type, you can choose:

- Polarity – See page 69.
- Latched – When set to No, the output changes state when activated, but then returns to the normal state again after the period specified by *On Time* (see below). When set to Yes, the output changes state every time a user operates the output, or according to a schedule if you specify *On Time*, *Off Time* and *Days* (see below).
- On Time/Off Time/Days – If *Latched* is set to No, use *On Time* to specify the number of seconds you want the output to remain active. If you select an active time of zero seconds, the output will not operate.

  If *Latched* is set to Yes:

  - You can use *On Time, Off Time* and *Days* to specify a schedule for the output to activate and deactivate automatically. Use *On Time* and *Off Time* to specify the time you want the output to activate and deactivate. Use *Days* to specify the days of the week you want the output to operate.

    Note: If a user activates the output while it is deactivated, the output stays activated until the control unit reaches the next off time. If a user de-activates the output while it is activated, the output deactivates until the control unit reaches the next on time.
  - Leave *On Time, Off Time* and *Days* without values if you want the output to act as a simple on/off switch under the control of the user.

Line Fault (44)

Active when the control unit detects a communications fault. Deactivates when the communications fault clears

Courtesy Light (45)

Active when the entry or exit timer is running. The control unit activates this output when the entry or exit time starts, and deactivates the output 10 seconds after the entry or exit time stops.

Installer on Site (46)

The control unit activates the output when an installer enters the Installer menu, and deactivates the output once the installer has exited the Installer menu.

Duress Code (47)

Active when a user keys in a Duress code, and deactivates the output when a user or engineer resets the system.

HUA Confirm (48)

(Not available on EU control units. Operates only when BS8243 is enabled.)

Active when either of the following occurs:

a) Users have activated two separate Hold Up Devices (HUDs) within the HUA confirmation time.

b) A HUD and a tamper are activated (in either order) within the HUA confirmation time.

Note that the HUDs (and tampers) must both be in the same partitions as the output. The control unit deactivates the output when a user or engineer resets the system.

Lockset Unlocked (49)

The control unit activates the output when the Lock Set zone is activated, and deactivates the output when a Lock Set zone is deactivated.

Burg Confirm timer (50)

(Not available on EU control units. Operates only when BS8243 or DD243 is enabled.)

Active when a Burg confirmation timer is running. Inactive when the timer stops.

HUA confirm timer (51)

(Not available on EU control units. Operates only when BS8243 is enabled.)

Active when an HUA confirmation timer is running. Inactive when the timer stops.

Rearmed (52)

In a part-setting system, the control unit activates the output if the system re-arms at least once after the user armed it.

If *Confirmation Mode* (page 86) is set to BS8243 or DD243, the control unit activates the output as it rearms the system after the confirmation timer expires.

If *Confirmation Mode* is set to Basic, the control unit activates the output as it rearms the system when the bell/siren time expires.

The control unit deactivates the output when a user or installer resets the system/partition.

Burg Confirmed Alarm (53)

(Not available on EU control units. Operates only when BS8243 is enabled.)

Active when either of the following occurs:

a) Two separate Normal Alarm (Burgs) have activated in the same partition within the confirmation time.

b) A Normal Alarm and Tamper are active (in any order) from the same partition within the confirmation time.

Note that the Normal Alarms (and tampers) must both be in the same partitions as the output. The control unit deactivates the output when a user or engineer resets the system.

Remote Self-Test (54)

This output type is not currently used. The output type is used for the remote self-test feature on certain Grade 3 external wired sirens.

Perimeter (55)

Activates when a zone of type Perimeter is activated. Deactivates when the system is reset by a user.

Perimeter Timer (56)

Activates when a zone of type Perimeter is activated. Deactivates at the end of the period specified by *PZ Reset Time* (page 76) or when the system is reset by a user, whichever occurs first.

Zones Shunted (70)

Active when one or more zones have been shunted by a user, either by activating a Shunt Key zone, or by keying in a Shunt Code, or by using a Master User or Admin User code.

Entry Only (71)

Active when a partition (allocated to this output) is in entry mode.

Exit Only (72)

Active when a partition allocated to this output is in exit mode. Note this output will NOT activate if the partition allocated uses Instant Set exit mode.

Chime Tone Mimic (73)

Active when any zone with a chime attribute is active.

Alert Active (74)

Active when the LEDs around the navigation key on a keypad are red. The control unit deactivates the output when the LEDs go green.

Panel Lid Open (75)

Active when the control unit lid or back tamper is active. The control unit deactivates the output when the control unit lid or back tamper is inactive.

Custom Output 1 to n (81 onwards)

Use this type if you want the physical output to activate when the selected custom output activates. For example, if you use the type *Custom Output 1*, the physical output activates when custom output 1 activates. See Custom Outputs on page 71.

Polarity

(This option is not available for radio outputs.)

You can change the polarity of a wired output to suit the type of equipment that the output must work with. Selecting Normal causes the output to be +12V when inactive, and at 0V when active. Selecting Inverted causes the output to be 0V when inactive, and at +12V when active.

Note that any change in the polarity of an output does not take effect until you leave the Installer menu.

Pulsed

This option is available for some output types. Selecting Yes causes the output, when activated, to give a single pulse of a specified length after a specified delay. See *Delay*

and *On Time* below. If *Pulsed* is set to No, the output changes state when the zone changes state.

Note: This option is not available for output types that already have built-in pulse behaviour, including ATS test, PIR Set Latch, Shock/Smoke sensor reset, setting/unset complete, user-defined and courtesy light.

Partitions
This option is available for most output types. By default, the outputs are assigned to all partitions.

Zones
This option is available for some output types. Select the zones that apply.

Delay
This is visible when *Pulsed* is set to Yes. The delay can take any value from 0 to 999 seconds. If set to 0, the output operates immediately. When set to any other value, the output waits for the specified number of seconds before becoming active.

On Time
This is visible when *Pulsed* is set to Yes. *On Time* can take any value from 1 to 999 seconds. The output is active for the specified number of seconds. (A value of 0 seconds is not allowed.)

Wired Outputs

The Wired Outputs menu provides access to hardwired outputs in the control unit, expanders and keypads (if applicable). Select the device that contains the output you wish to program, and then one of the following.

Panel
Select one of the following options, as displayed on the top line of the display:

EDIT SIREN OUTPUT or EDIT STROBE OUTPUT

> Select these to edit the settings for the dedicated siren and strobe outputs. You can edit the output's *Name*, *Polarity* and *Partitions* in the same way as for a radio outputs (see the above descriptions).

EDIT O/P PAN>nn

> Select this to edit the settings for a wired output at the panel. You can edit each output's settings in the same way as for radio outputs (see page 63).

Note: Please refer to page 26 for details of how outputs are addressed.

Plug-By Outputs

Some models of control unit include on-board plug-by outputs (see Table 1 on page 2).

The plug-by outputs are designed for use by a standalone communicator to send alarm information to an ARC. You can edit each output's settings in the same way as for radio outputs (see page 63).

See page 34 for a list of the default output types assigned to the plug-by outputs.

Note: To make the plug-by outputs operate, you must select an alarm response that includes communications (see from page 74).

See page 85 for details of the Remote Reset input of the plug-by communicator port.

Plug-by outputs on an EXP-PSU

The plug by outputs on the EXP-PSU mirror those on the control unit. You cannot program the plug-by outputs on the EXP-PSU to behave independently from those on the control unit.

Custom Outputs

A custom output is a virtual logic gate within the control unit. It is similar to an AND gate or OR gate in digital electronics, but exists only within the configuration of the control unit. A custom output can have up to 10 inputs. An input is an event such as *Fire Alarm* or *Hold Up Alarm* (see page 63).

You can use a custom output to activate a physical output by assigning the custom output as the type of the physical output. For example, if you have set up *Custom Output 1* and wish to use it to activate a physical output at the control unit, assign *Custom Output 1* as the type for the physical output.

You must select a *Mode* for each custom output, which can be All(AND), or Any (OR). For the AND mode, all inputs to the custom output must be active for the custom output to be active. For the OR mode, any one of the inputs must be active for the custom output to be active.

The number of custom outputs available depends on the control unit (see page 2).

Note: An input can be the output of another custom output. However, you can select only custom outputs of higher number as the custom output you are defining. For example, if the control unit supports 4 custom outputs and you are defining *Custom Output 2*, it can use only the outputs of *Custom Output 3* and *Custom Output 4* as inputs.

Example

Requirement: To activate a physical output when any of three fire doors (zones 5, 6 and 7) is open, but also shunted.

Solution: Configure a physical output as type *Custom Output 1*, and configure two custom outputs as follows.

Custom Output	Mode	Input
1	All(AND)	Input 1 type=Custom Output 2 Input 2 type=Zones Shunted
2	Any (OR)	Input 1 type=Zone Follow (Zone 5) Input 2 type=Zone Follow (Zone 6) Input 3 type=Zone Follow (Zone 7)

Chapter 8: Setting Options and Partitions Menus

About these menus

If you are using a part-setting system, the Installer menu contains a *Setting Options* menu, which contains all the options to program entry, exit and alarm response for a single alarm system with a full-set and three part-set levels.

If you are using a partitioned system, the Installer menu contains a *Partitions* menu instead, which contains an option for each partition. Each partition behaves like a complete, independent, alarm system. However, each partition has only full set and one part set.

These two menus contain a similar set of options, but in a different order.

Note: The default settings for these options are compliant with EN50131, see page 31. Changes to some of the defaults may render the system non-compliant.

Full Set, Part Set and Partition options

Name

Use this option to give the full set, part set, or partition a name. The control unit displays this name to the user during setting.

Exit Mode

Note: By default, a FOB-2W-4B Set button instant sets its assigned partition, regardless of the exit mode chosen in the Installer menu. To program the FOB-2W-4B to follow the exit mode programmed in the Installer menu, set the *System Options – User access – 2W Set Instant* option to NO (page 84).

Timed Set

Use this setting to make the system set after a delay. Use Exit Time (see page 74) to specify the delay. The control unit logs the start of timed exit.

Note: This option does not comply with BS8243:2010.

Final Door Set

Use this setting to complete the setting of the system by closing a door fitted with a Final Exit zone detector. Once the door closes, the system sets after the Settle Time expires. Note that the exit time does not expire in this option.

The control unit logs the start of final door exit.

Note:

- To enable part setting, include a zone of type Final Exit as one of the part-set zones. Also select Final Exit in Pt.set Final Exit (see page 78).
- For partitioned systems, include a zone of type Final Exit in the partition.
- Do not use a radio PIR as a Final Exit. Radio PIRs have a “lock out” period after each activation to conserve battery power. When you set (or part set) the system,

a PIR may still be in lockout, during which it cannot send a signal to complete the setting process.

Instant Set

The system sets immediately and without any setting tone. The keypad(s) give confirmation tone when the system is set.

Note: This option does not comply with BS8243:2010.

Silent Set

The system sets after the time programmed in the Entry/Exit Time menu but does not give any exit tones over the loudspeaker or keypad. When the system sets, the keypad (but not the loudspeaker) gives a double-beep confirmation tone. (Keypads give a double-beep tone at the end of all setting modes.)

On entry, both keypads and loudspeakers give entry tones.

Note: This option does not comply with BS8243:2010.

Lock Set

Use this setting if you are using a lock to set the system.

To use *Lock Set*, you must:

- Configure a Lock Set zone (see page 46) that is activated by a suitable lock (located on the final exit door).
- Configure a Final Exit zone (see page 43) connected to the final exit door.

Note: It is recommended that you do not use *Lock Set* within a part set, since the results may not be predictable.

Setting: Once the user has started the setting sequence, the exit tone sounds, which continues until the user closes the Final Exit door and operates the lock. When the *Settle Time* (page 74) expires, the control unit sets the system and converts the Final Exit zone in the set partition to a zone of type Normal Alarm.

Unsetting: When a user de-activates the Lock Set zone, the control unit converts any zone originally programmed as Final Exit back to Final Exit (so that the entry time starts when the user opens the entry door) and starts a warning tone (distinct from the entry tone). If the user activates the Lock Set zone again without starting the Entry Timer, the control unit changes all Final Exit zones back into Normal Alarm zones and stops the warning tone.

Note: If you use *Lock Set*, you must set *After Entry* (page 87) to Never in order to disable confirmation and comply with BS8243.

Exit Terminate

Setting: The user must start the setting sequence in the normal way, and then complete setting in one of the following ways once they have left the protected area:

a) By activating an Exit Terminate zone (see page 45).

b) By presenting a proximity reader tag to a KEY-EP external proximity reader connected to a suitable keypad. This requires *System Options – User Access – Terminated Set* to be set to Y (page 84).

When the user starts the setting sequence, the control unit gives the exit tone for the selected partition(s) and the exit time does not expire. Once the user completes the setting sequence, the system sets when the Settle Time (page 74) expires.

Unsetting: The user can unset the partition using any of the following methods:

a) By presenting a proximity tag to an external proximity tag reader.

b) By using the Unset button on a remote control.

c) By activating a Final Exit zone allocated to the partition (to start an entry timer) and then entering an access code or presenting a proximity tag to a keypad. **Note:** This method does not comply with BS8243 clause 6.4.

As Partition 1

This option appears for all partitions except partition 1. If you select this option, the partition will use the same exit mode as partition 1.

Settle Time

This option is available only if *Exit Mode* is set to Final Door Set, Lock Set or Exit Terminate. This option allows you to define a time delay to allow detectors to settle before the system sets. During this period, the sounders stop and the control unit ignores any alarms generated by the detectors.

Enter two digits to specify a time in seconds, from 01 to 30. The default is 15 seconds to allow radio PIRs to send all the transmissions required to indicated that they are settled.

Exit Time

This option is available only if *Exit Mode* is set to Timed Set or Silent Set. The exit time can take any value between 10s and 120s.

Entry Time

The entry time can take any value between 10s and 120s. The entry time you select in this option applies to full set and all part sets.

To comply with EN50131-1 Clause 8.3.8.2, maximum is 45s for Entry Time.

Alarm Response

Note: In a part-setting system, the response for a full set is always Siren + Comms.

Internal

Keypads and loudspeakers.

Siren

Keypads, loudspeakers and siren.

Siren + Comms

Keypads, loudspeakers, siren and communication. Note that any Siren Delay (see page 77) applies to Siren+Comms, but not Internal or Siren alarm responses.

HUA Response

This option controls the audible alarm associated with Hold-Up Alarms (HUAs).

Audible

The control unit starts HUA alarm tones from the keypads and loudspeakers assigned to the partition in which the alarm occurs, and activates any siren outputs. The sirens follow the *Siren Time* (see page 75). The loudspeakers operate until a user silences the alarm.

Silent

The control unit keeps the HUA alarm silent: there are no alarm tones from keypads or loudspeakers and any siren outputs or HUA outputs remain inactive.

Displayed

All keypads display a HUA alert message immediately (a user does not have to enter an access code to see the message). If more than one HUA is active, the keypad display scrolls through the alert messages at approximately one-second intervals.

The control unit also starts HUA alarm tones from loudspeakers and keypads allocated to partitions in which the HUA occurred, activates siren and HUA outputs assigned to the partition.

Note:

- All HUAs are disabled when an installer is using the Installer menu.
- In a partitioned system, *HUA Response* applies to both a full-set or part-set partition.
- For a part-setting system, this option appears in *System Options*.

PZ Unset Response

Specifies the system response for activations of zones of type Perimeter in the unset state.

In a partitioned system, each partition can have different response. In a part-setting system, this option applies to the complete system.

Note: For a part-setting system, this option appears in *System Options*.

Silent

Activation inserted into non-mandatory log.

No keypad and internal sounders.

Outputs of type Perimeter and Perimeter Timer activate.

Outputs of type Perimeter Timer deactivate on expiry of *PZ Reset Time* (see below) or code entry.

Internal

Activation inserted into non-mandatory log.

Keypad and internal sounders activate.

Outputs of type Perimeter and Perimeter Timer activate.

Keypad and internal sounders silenced by user code, etc.

Outputs of type Perimeter Timer deactivate on expiry of *PZ Reset Time* (see below) or code entry.

Siren

Activation inserted into non-mandatory log.

Keypad, internal and external sounders activate.

Outputs of type Perimeter and Perimeter Timer activate.

Keypad, internal and external sounders silenced by user code, etc.

Outputs of type Perimeter Timer deactivate on expiry of *PZ Reset Time* (see below) or code entry.

Full

Activation inserted into non-mandatory log.

Keypad, internal and external sounders activate.

Outputs of type Perimeter and Perimeter Timer activate.

Communications active.

Keypad, internal and external sounders silenced by user code, etc.

Outputs of type Perimeter Timer deactivate on expiry of *PZ Reset Time* (see below) or code entry.

Communications restored by user code entry.

PZ Set Response

Specifies the system response for activations of zones of type Perimeter in the set state.

In a partitioned system, each partition can have different response. In a part-setting system, this option applies to the complete system.

Note: For a part-setting system, this option appears in *System Options*.

Silent

Activation inserted into non-mandatory log.

No keypad and internal sounders.

Outputs of type Perimeter and Perimeter Timer activate.

Outputs of type Perimeter Timer deactivate on expiry of *PZ Reset Time* (see below) or code entry.

Internal

Activation inserted into non-mandatory log.

Keypad and internal sounders activate.

Outputs of type Perimeter and Perimeter Timer activate.

Keypad and internal sounders silenced by user code, etc.

Outputs of type Perimeter Timer deactivate on expiry of *PZ Reset Time* (see below) or code entry.

Siren

Activation inserted into non-mandatory log.

Keypad, internal and external sounders activate.

Outputs of type Perimeter and Perimeter Timer activate.

Keypad, internal and external sounders silenced by user code, etc.

Outputs of type Perimeter Timer deactivate on expiry of *PZ Reset Time* (see below) or code entry.

Full

Activation inserted into non-mandatory log.

Keypad, internal and external sounders activate.

Outputs of type Perimeter and Perimeter Timer activate.

Communications active.

Keypad, internal and external sounders silenced by user code, etc.

Outputs of type Perimeter Timer deactivate on expiry of *PZ Reset Time* (see below) or code entry.

Communications restored by user code entry.

PZ Reset Time

This determines the maximum period of time that outputs of type Perimeter Timer will be active.

In a partitioned system, each partition can have different reset time. In a part-setting system, this option applies to the complete system.

The reset time can be set from 0-999 seconds. Setting the time to 0 requires a code at a keypad to deactivate outputs of type Perimeter.

Note: For a part-setting system, this option appears in *System Options*.

Siren Delay

When the system (or partition) is set and (for example) a zone is activated, the system waits for the programmed *Siren Delay* before operating the siren and sounders. The system then operates the siren and sounders for the programmed *Siren Time*.

Note:

- *Siren Delay* has no effect if *Alarm Response* (see above) does not require communications or if a line fault is detected.
- *Siren Delay* has no effect if *System Options – Confirmation Mode* is set to BS8243 or DD243 AND *System Options – Confirmation – Siren On* is set to Unconfirm (see page 88).
- Any keypad or expander sounder assigned to two or more partitions uses the shortest *Siren Delay* of the partitions the device is assigned to.

Siren Time

This option changes the length of time that the system operates the siren and sounders during an alarm.

Note:

- This applies to a siren wired directly to the control unit.
- Radio sirens have separate maximum sounder durations to preserve battery life. Please refer to the siren's installation instructions.
- Any keypad or expander sounder assigned to two or more partitions uses the longest *Siren Time* of the partitions the sounder is assigned to.
- To comply with EN50131-1 Clause 8.6, the minimum is 90s, and the maximum is 15mins. For INCERT approval, the minimum is 90s, and the maximum is 3mins.

Strobe on Set

When set to On, this option causes the control unit to activate any output of type Strobe, and the strobe on any wireless siren. The outputs/strobes are active for ten seconds after the system sets.

This option applies to full set and all part sets.

Strobe on Unset

When set to On, this option causes the control unit to activate any output of type Strobe, and the strobe on any wireless siren. The outputs/strobes are active for ten seconds after the system unsets.

This option applies to full set and all part sets.

Part Set Exit Mode
Pt.set Settle Time
Part Set Exit Time
Pt.set Entry Time
Pt.set Alarm Resp.
Pt.set Siren Delay
Pt.set Siren Time

These options control system behaviour when the system is part set. Please refer to the equivalent full-set options described above.

Pt.set Final Exit

This option controls how the system uses Final Exit zones when the system is part set.

Final Exit

In a part-setting system, any zones of type Final Exit with Part Set B, C or D attributes continue to act as Final Exit zones during part setting.

In a partitioned system, any zones of type Final Exit that belong to the partition and have the Part Set attribute continue to act as Final Exit zones during part setting.

Normal Alarm

In a part-setting system, any zones of type Final Exit with the Part Set B, C or D attributes act as Normal Alarm zones during part setting.

In a partitioned system, any zones of type Final Exit that belong to the partition and have the Part Set attribute act as Normal Alarm zones during part setting.

Pt.set Entry Route

This option controls how the system treats Entry Route zones when the system is part set..

Entry Route

In a part-setting system, any zones of type Entry Route with the Part Set B, C or D attributes continue to act as Entry Routes zones during part setting.

In a partitioned system, any zones of type Entry Route that belong to the partition and have the Part Set attribute continue to act as Entry Routes during part setting.

Final Exit

In a part-setting system, any zones of type Entry Route zones with the Part Set B, C or D attributes act as Final Exit zones during part setting.

In a partitioned system, any zones of type Entry Route that belong to the partition and have the Part Set attribute act as Final Exit zones during part setting.

Pt.set Strb Set
Pt.set Strb Unset

These options control strobe behaviour when the system is part set. Please refer to *Strobe on Set* and *Strobe on Unset* above.

Full Set Link

Some commercial premises include two or more separate areas linked by a common area such as a lobby. The *Full Set Link* option, which is available on partitioned systems,

enables you to configure the system so that the common area sets automatically when the last occupant leaves the premises.

Zones in partition 1 are always in the common area. You can link partition 1 to any of the other partitions. When all of the linked partitions are set, the control unit full sets partition 1. When any of the linked partitions is unset, partition 1 is also unset.

The system uses the alarm response allocated to partition 1.

Note: To avoid false alarms, it is recommended that you make the alarm response of the common area (partition 1) Siren+Comms and the other two partitions Siren only.

Remote Set

This determines how the system will set when it receives a setting command from a remote device, such as the virtual keypad in the web interface.

Exit Mode

Selecting Timed Set causes the system to set after time period specified by *Exit Time*. Selecting Instant Set causes the system to set instantly.

Exit Time

This specifies the time period used by Timed Set (30 to 60 seconds).

Local Set on ER

If there is an activation of an Entry Route zone during the setting period, the exit mode automatically converts to be the same as the standard exit mode, such as Final Door Set or Exit Terminate.

Calendar Set

This allows you to configure the control unit to set or unset the alarm system (or parts of it) at fixed times of day on a seven-day cycle. If the system is a part-setting system, you can use this option to full set or part set B, C or D. If the system is a partitioned system, this option allows you to full set or part set any collection of partitions.

There are two basic elements that you can program within the calendar set option: the “event” and the “exception”. An event defines an action (setting, part setting or unsetting) to occur regularly at set times and days. An exception defines periods such as holidays when you do not want the event to occur. The number of events and exceptions the control unit can store is shown in Table 1 (page 2).

Hint: Set up exceptions first, and then the events.

Note:

- You cannot program an event to change the system/partition directly from one part set level to another. You must program an event to unset the system/partition first, and another event to set the system/partition to a different part set level. For example, if event A part sets the system (or a partition), you cannot program event B to full set the system. You must program event B to unset the system and then use event C to full set the system.
- If you create an event to unset a partition, and another event to set the same partition again, you must program the setting event to occur at least 10 minutes after the unsetting event.

- The control unit adjusts its clock in Spring and Autumn to allow for Summer Daylight Saving Time. At the Autumn change-over, avoid configuring any unset events to take place during the changeover time on the Sunday morning. For UK systems, this time is 01:00 to 02:00. For EU control units, this time is 02:00 to 03:00. If the control unit unsets any part of the system at these times, it will NOT set the system again when the clock changes back to Winter Time.

Manually setting and unsetting partitions does not alter the times programmed in calendar sets. If a user sets a partition that is due to be set by a calendar event, the partition remains set when the calendar event time is past. Likewise, if a user unsets a partition before a calendar event is due to unset the partition, the partition remains unset.

Add Event

Use this option to create an event. When you select the option, the control unit will guide you through the following series of options:

Event Name

Enter up to 12 characters or press ✔ to leave the default name.

Event Time

Specify the time you want the event to occur, then ✔ to display the next prompt.

The time “00:00” is midnight, at the beginning of a new day.

Note that if you specify a start time that is less than 10 minutes from the current time shown by the control unit clock (that is, less than the period set by Warning Time), the event will not take action until the following day.

Event Days

Choose the days you want the event to occur.

Press ▲ or ▼ to scroll through each day of the week. Press ◀ or ▶ to specify Yes or No.

Event Actions

In a partitioned system, press ▲ or ▼ to scroll through each partition, and ◀ or ▶ to select No (no action), Full (full set), Part (part set) or Unset.

In a part-setting system, select one of: Full Set, Part Set B (or C or D) or Unset.

Event Exceptions

Choose the exceptions (set up using *Add Exception*) that you want to apply to the event.

Press ▲ or ▼ to scroll through the list of programmed exceptions. Press ◀ or ▶ to specify Yes (the exception applies to the event) or No.

Warning Time

Specify the period (in minutes) you want the control unit to sound the warning tone before the start of a setting event. Enter between 1 and 30 minutes. The default is 10. There is no specific warning indication for an unset event.

The warning tone sounds at the keypads and loudspeakers allocated to the partition(s) specified in the event.

At the beginning of the warning time, the control unit activates any outputs of type Autoset Warning (see page 67).

At the end of the period, the control unit stops the warning tone, sets the affected partition(s) without any delay and deactivates any outputs of type Autoset Warning.

Warning Tone

Press ▲ or ▼ to choose between Audible or Silent. When Silent, the control unit will NOT sound a warning tone for the event (although the warning timer will still operate).

If a warning tone for a partition is due from more than one event at the same time, and any of the tones is set to "Audible", the tone will be audible.

Edit Event

This option allows you to edit individual parts of an event.

Delete Event

Use this option to delete an event.

Add Exception

Use this option to create an exception. During the time specified by the exception, none of the events that have the exception will take place. When you add an exception, the control unit guides you through the following steps:

Name

Enter up to 12 characters or press ✔ to leave the default name.

Exception Start Time

Specify the time you want the exception to start, then ✔ to display the next prompt.

The time “00:00” is midnight, at the beginning of a new day.

Exception Start Date

Specify the date you want the exception to start (for example, 31/12 for 31st December).

Exception End Time

Specify the time you want the exception to end.

Exception End Date

Specify the date you want the exception to end.

Edit Exception

This option allows you to edit individual parts of an exception.

Delete Exception

Use this option to delete an exception.

Deferring Calendar Setting

During the calendar set warning time, a user can interrupt the setting process. To do this, they must enter their access code at a keypad (or present a prox tag). The user can then do one of the following:

- Press ◄ or ► to see details of which partitions are about to set.
- Press ✘ to allow the setting event to proceed.
- Press ✔ to defer setting for 30 minutes. Note that the user must belong to the partition that is due to be set.

- Press the Menu key to gain access to the setting menu to set another partition that is not involved in the current setting event. Note that if the user is allocated to a single partition, that partition may start setting immediately.

If the calendar set warning timer has been deferred by a user, the control unit halts the warning timer, and defers any consequent setting event for 30 minutes. At the programmed warning time, the control unit starts counting down the warning timer again. Users can defer a calendar set in this way a total of three times. After the third deferral, the control unit sets the system.

Note that deferring setting does not defer any unsetting events.

Setting Faults

If there is a fault that would normally prevent the system from setting, a calendar set event will also fail. Before the time of a setting event, the control unit starts the calendar set warning tone as usual, but at the setting time, the control unit will not set the system. The control unit will log the failure as “set fail”. At the same time, the control unit will activate any output programmed as type Set Fail.

Note that if you assign zones the Force Set Omit attribute, the control unit will omit those zones if they are active during a scheduled setting event.

Chapter 9: System Options Menu

This menu contains options that affect the working of the alarm system as a whole.

Note: The default settings for these options are compliant with EN50131, see page 31. Changes to some of the defaults may render the system non-compliant.

Wired Zone Type

The control unit prompts you to select the zone wiring type when you power up a control unit for the first time, or when you restore the control unit to factory defaults (see page 92). There are two options:

- Panel Zones – This option lets you change the zone wiring type for the control unit.
- All Zones – This option lets you change the zone wiring type for the whole system.

Please refer to page 14 for details of the wiring types.

User Access

Use this option to give users access to various system facilities

HUA Keys Active

This option allows users to start an HUA alarm from the keypads by pressing both Hold Up Alarm keys at the same time. This option applies to all keypads, both radio and wired, and is not affected by allocating keypads to specific partitions.

Select Yes to make the HUA keys functional. Select No to disable the keys.

Note:

- If HUA Confirmation has been enabled in *System Options – Confirmation – BS8243*, two separate HUA events are needed within the confirmation time to generate a confirmed HUA alarm. See page 89 for HUA Confirmation Time.
- To enable HUAs from a FOB-2W-4B or a 727r in UK control units, you must set *System Options – Confirmation Mode* to *Basic* (see page 86). EU control units, always use Basic confirmation mode. A Master User must then set *User Menu – System Config – Remotes – HUA Function* to *Enabled* (the option does not appear if Confirmation Mode is BS8243 or DD243).

Quick Set

Note: If you enable the quick set-keys, the control unit no longer complies with EN50131.

This option controls the operation of the A, B, C or D keys.

Yes – Allows users to set the alarm system by pressing A, B, C or D without entering an access code.

No – Users must enter an access code (or present a tag) before pressing the A, B, C or D keys.

Quick Omit

Yes – Allows users to omit a zone that is active while the user is setting the system. The zone must have the Omittable attribute (see page 47).

No – Users must use the *Omit* menu to omit a zone that is active before they can set the system.

User Code Reqd

Yes – After entering the installer code, the system prompts for a user code before allowing access to the Installer menu.

No – You can access the Installer menu simply by keying in the installer code.

Note: If you select this value, the control unit no longer complies with EN50131. This value complies with PD6662 only if the user has given written consent.

2 Way Replies

Use this option to decide whether the control unit can send status messages to a two-way remote control unit (FOB-2W-4B).

2 Way Set Instant

Use this option to specify how a two-way remote control unit (FOB-2W-4B) sets the system.

Yes – The partition or system sets instantly when the user operates the FOB-2W-4B.

No – The partition or system follows the setting mode programmed for it in *Partitions* or *Setting Options* (see page 72).

Duress Enable

Selecting Yes allows master users to assign the Duress user type to users.

A duress code can set and unset the system in the same way as a normal user. However, each time the code is used, the control unit triggers any output configured as type Duress, and (if applicable) communicates Duress and Set/Unset events.

Terminated Set

This option is relevant if you are using a KEY-EP external proximity reader connected to a keypad.

Yes – Select this if you want to start the setting procedure from a keypad and complete it at the KEY-EP. You will not be able to start the setting procedure from the KEY-EP. For this setting, also configure *Partitions – Exit Mode* (for a partitioned system) or *Setting Options – Full/Part Set – Exit Mode* to Exit Terminate.

No – Select this if you want to able to start the setting procedure from the KEY-EP (or from a keypad). In this case, choose an exit mode such as Timed Set or Instant Set. When you present the proximity tag to the KEY-EP, the system sets with no further action.

For both settings of Terminated Set, presenting a tag to the KEY-EP when the system is set immediately unsets the system.

User Reset

This option determines under what circumstances a user or the installer can reset the system after an alarm.

Zone Alarms

This appears when *System Options – Confirmation – Confirmation Mode* is set to Basic (page 86).

Yes – The user can reset the system after an alarm triggered by a zone's alarm circuit.

No – The installer must reset the system after an alarm triggered by a zone's alarm circuit. See also "Remote Reset" on page 85.

Note: Users can reset the system if they unset the system during an alarm, but before the Alarm Abort period has expired (see page 95).

Zone Tampers

Yes – The user can reset the system after an alarm caused by a zone's tamper circuits being triggered.

No – The installer must reset the system after an alarm caused by a zone's tamper circuits being triggered. The alarm abort period does not apply. **Note:** This setting is required for INCERT approval.

System Tampers

Yes – The user can reset the system after an alarm caused by a tamper.

No – The installer must reset the system after a system tamper alarm. The alarm abort period does not apply. **Note:** This setting is required for INCERT approval.

A system tamper can be caused by, for example:

- Operating a lid/back tamper switch on a device.
- Applying a voltage higher than approximately 3V to the TR input from a external sounder.
- Detecting Jamming or a Supervision failure when either of these options are set to Tamper see page 96.

If a tamper occurs when the system is set, the control unit classifies this as an unconfirmed or confirmed alarm. The reset follows the alarm reset option NOT the tamper.

Remote Reset (RedCare Reset)

If you select NO for System Tampers, then when a tamper occurs, the control unit enables the Remote Reset input pin on the plug-by connector. After an alarm, the user may silence the sounders, but to reset the system, the user must first contact the ARC. The ARC (after verifying the user's identity) can cause the Remote Reset input to go to +12V by way of the plug-by communicator. On receiving the signal, the control unit allows the user to reset the system.

If the ARC causes Remote Reset to go to +12V and it reverts back to 0V before the user resets the system, the control unit remembers that the signal has been sent and still allows the user to reset the system using their normal access code.

Confirmation

Confirmation Mode

The options in *Confirmation Mode* depend on whether you are using an EU or UK control unit:

- For EU control units, Basic confirmation mode is always used and *Confirmation Mode* contains two options: *Sounder On* (page 87) and *Siren On* (page 88).
- For UK control units, *Confirmation Mode* contains three options: *Basic*, *DD243* and *BS8243*. The options in the *Confirmation* menu depend on which of these three options you select.

The setting for *Confirmation Mode* determines the events the control unit requires to create a "confirmed alarm":

- Basic (default and only setting for EU control units) – A confirmed alarm is generated when a second zone alarm is activated while the partition is in an alarm state.
- BS8243 or DD243 (UK control units only) – A confirmed alarm is generated when a second zone alarm is triggered within the period of the *Confirmation Timer* setting, and in the same partition as the first zone alarm. If you select either of these options, additional options are displayed to define the meaning of a confirmed alarm.

  If the first ("unconfirmed") alarm is caused by the expiry of the entry timer, then for:

  - DD243 – A further two zones that are not on the entry route must be triggered to activate the output.
  - BS8243 – One zone not on the entry route must be triggered to activate the output.

Note:

- A confirmed alarm activates any output programmed of type Confirmed Alarm (page 64).
- A confirmed alarm is communicated only when the *Alarm Response* is set to Siren+Comms (see page 74).
- A confirmed hold-up alarm (generated by two hold-up alarms or a hold-up alarm and tamper alarm) only when *Confirmation Mode* is BS8243.
- The Master User can enable or disable hold-up functions for all FOB-2W-4Bs and 727rs by using *User Menu – System Config – Remotes – HUA Function*. Note that this is not compliant with DD243 or BS8243.

Confirmation Time

This is available for only for UK control units and when *Confirmation Mode* is set to DD243 or BS8243.

The option determines the length of the confirmation time for intruder alarms. You can select any time between 1 and 60 minutes. Confirmation times less than 30 minutes do not comply with BS8243 or DD243.

After Entry

This is available for only for UK control units and when *Confirmation Mode* is set to DD243 or BS8243.

Never

The control unit turns alarm confirmation off if the user enters by the entry door (used for DD243:2004 clauses 6.4.2 and 6.4.4 and BS8243:2010).

1 zone

The control unit starts a confirmed alarm if the intruder activates one or more zones (not on the entry route) after entering the premises through the final exit zone.

2 zones

The control unit starts a confirmed alarm if an intruder activates two or more zones (not on the entry route) after entering the premises through the final exit zone (used for DD243:2004 clauses 6.4.5) **Note:** This option is not available if you have selected BS8243 for Confirmation Mode.

Entry Keypad Lock

This is available for only for UK control units and when *Confirmation Mode* is set to DD243 or BS8243.

The option determines whether the user can unset the system by entering an access code after opening the entry door. Select one of the following:

Off

The user can enter an access code at the keypad after the entry door opens (used for DD243:2004 clause 6.4.4).

On

The user must unset the system by some means other than the keypad, such as a proximity tag, remote control or key switch (used for DD243:2004 clause 6.4.5 and BS8243:2010 6.4.5b).

Note: This option has no effect if the alarm response (for either full set or part set) is set to Siren or Internal. In those cases, the user will still be able to unset the system using an access code. *Entry Keypad Lock* is intended for use when the system can summon a police response.

Sounder On

Unconfirm

When the system is set, the control unit activates the internal sounders when an unconfirmed alarm occurs.

Confirm

When the system is set, the control unit does not activate the internal sounders until a confirmed alarm occurs.

Note: The control unit will not allow you to select *Sounder on – Confirm* at the same time as *Siren on – Unconfirm*.

Sounder and siren operation

The behaviour of internal sounders and external sirens is described in Table 11.

Table 11: Sounder and Siren Operation

Settings		Effect
Sounder On	**Siren On**	
Unconfirm	Unconfirm	Unconfirmed alarm: internal sounders and sirens start immediately and run for the *Siren Time* (see page 77). Confirmed alarm: the control unit restarts the sirens and internal sounders, which run for the full *Siren Time*, even if that had expired earlier.
Unconfirm	Confirm	Unconfirmed alarm: the internal sounders start immediately and run for the *Siren Time*. Confirmed alarm: the control unit waits for any *Siren Delay* (see page 77), and then starts both the internal sounders and the external sirens. These both run for the Siren Time.
Confirm	Confirm	Unconfirmed alarm: No sounders or sirens. Confirmed alarm: the control unit waits for any *Siren Delay*, and then starts both internal sounders and external sirens. These both run for the *Siren Time*.

Siren On

Unconfirm

The control unit operates the siren for all alarms (and overrides any *Siren Delay*).

Confirm

When the system is set, the control unit does not activate the siren(s) until a confirmed alarm occurs.

The behaviour of internal sounders and external sirens is described in Table 11.

Unconfirmed Reset

This is available for only for UK control units and when *Confirmation Mode* is set to DD243 or BS8243. The setting for this option overrides *System Options - User Reset – Zone Alarms* (see page 85).

User

The user can reset after an unconfirmed alarm.

Installer

The user cannot reset after an unconfirmed alarm; the installer must do it.

Note:

- If a user silences an alarm within the Abort Time (page 95), the alarm will not require an installer reset.
- These options apply to intruder alarms only and not to Hold-Up Alarms.

Confirmed Reset

This is available for only for UK control units and when *Confirmation Mode* is set to DD243 or BS8243. The setting for this option overrides *System Options - User Reset – Zone Alarms* (see page 85).

User

The user can reset after a confirmed alarm.

Installer

The user cannot reset after a confirmed alarm; the installer must do it.

Note: If a user silences an alarm within the *Abort Time* (page 95), the alarm will not require an installer reset.

HUA Confirm Time

This is available for only for UK control units and when *Confirmation Mode* is set to BS8243. This option determines the length of the confirmation time for confirmed HUAs.

If the confirmation time expires after an unconfirmed Hold-Up Alarm (HUA), and the Hold-Up Device (HUD) is still active, the control unit omits the active device and communicates “Omitted HUD” to the ARC. If the system is unset, the control unit displays an alert at the appropriate keypads.

If you wish to generate a confirmed HUA for test purposes only, you can set the HUA confirm time to 0.

Note: The time must be between 8 and 20 hours to comply with BS8243:2010 5.4.1.2.

Tamper as Tamper Only

This is available for only for UK control units and when *Confirmation Mode* is set to BS8243. The purpose of the option is to ensure strict compliance with BS8243 when reporting tampers to ARCs.

Enabled

When an unconfirmed tamper occurs, the control unit sends only “Tamper” to the ARC and activates any output configured as type Tamper (this follows Eaton’s understanding that BS8243, Annex H.7.1 applies to all Grades).

Disabled

When an unconfirmed Tamper occurs the control unit sends “Tamper”, “General Fault” and “Burg” to the ARC. In addition it activates any outputs of type Tamper and General Fault. (See also Jamming on page 96 and Supervision on page 96.)

Note: This option does not comply with BS8243.

The behaviour of the Disabled setting is used when *Confirmation Mode* is Basic or DD243.

Note: If you are using Fast Format communications, please ensure that one channel is allocated for tamper. If you do not do this, the control unit reports tamper as an unconfirmed Burg to ensure the condition is notified.

Masking

This option allows you to control whether the system responds to masking or trouble events from those detectors that are capable of reporting them, are connected correctly to the system, and are programmed with the Masking attribute.

The detector must use the wiring as shown in Figure 3 on page 15.

When masking is enabled, the alarm response depends on whether the system is set or unset, and which resistance range the detector is signalling with.

Off

The system hides the Masking zone attribute, and the *Mask Override* option (see below). The control unit treats masking signals from FSL detectors as alarms or tampers depending on the resistance.

On

The system makes available the Masking zone attribute and *Mask Override* option.

Alarm response when the system is unset

Detector output	Response
Mask (Alarm open, Fault open, resistance = 9k1)	The control unit treats a masking event as a fault, activates any outputs of type General Fault or Masking, and generates an Alert on the keypads. A user can reset the system once the masking is cleared. If user reset is disabled, the installer can reset this fault remotely.
Fault (Alarm closed, Fault open, resistance = 4k4)	The control unit treats this condition as a fault, activates any outputs of type General Fault, and generates an Alert on the keypads. The ability to reset the alert is governed by the *System Options – User Reset – System Tampers* option, see page 85. **Note:** There is a delay of about three seconds before the control unit starts the alert at the keypad. This delay is intentional, and is designed to confirm that the fault is a true fault, and not the first stage in the detector reporting a masking event. Two or more detector fault events occurring within three seconds of each other may prolong the delay up to 10 seconds (but no longer).

Alarm response when the system is set

Detector output	Response
Mask (Alarm open, Fault open, resistance = 9k1)	The control unit treats a masking event as an alarm condition (and also activates any output of type Masking). This will signal an unconfirmed alarm or will confirm an outstanding unconfirmed alarm. The unconfirmed and confirmed events must be from different detectors. The ability to reset the system after the alarm is governed by the *System Options – User Reset – Zone Alarms* option, see page 85. Note that the user can also reset this alarm provided they do so within the abort time.
Fault Alarm closed, Fault open, resistance = 4k4)	The control unit treats this condition as a fault and activates any outputs of type General Fault. When a user unsets the partition/system, the control unit generates an alert on the keypads. The ability to reset the alert is governed by the *System Options - User Reset – System Tampers* option, see page 85.

Mask Override

(The control unit hides this menu option if Masking is set to Off.) This option controls how the user can respond to a masking event once it is reported by the control unit.

On

A User can override a masking fault to set the system

Off

A User cannot override a masking fault to set the system. The system will not set until the masking fault has cleared.

Language

This option allows you to update or select the language used for the menus and options. For UK panels, there is only one language.

Changing the language does not affect any stored names for full/part set, detectors, outputs or users, and does not change any defaults.

If language files are in a folder named INSTALL on the SD card, you can choose to replace the existing language stored on the panel with a language from the SD card.

Changing the language does not affect any stored names for full/part set, detectors, outputs or users, and does not change any defaults.

Shunt Groups

Use this menu to allow users to shunt groups of zones.

First, make sure that all the zones you wish users to be able to shunt have the Shuntable zone attribute (see page 50).

Select the shunt group to edit, and then specify the zones you want to include in that shunt group. Note that it does not matter which partition the zone belongs to: the user with the necessary Shunt Code (see below) will be able to shunt that zone as part of the shunt group.

There are two ways of controlling shunt groups:

- Using a Shunt Code – Create a new user of type Shunt Code (see the Administrator's Guide) and assign the shunt group you have created to that user. When a user enters the shunt code, the control unit shunts all zones in shunt group(s) allocated to that code. When a user enters the code again, the control unit restores the zones in the shunt group(s) linked to that shunt code.
- By a Master User or Admin User using the *Shunt Groups* option in the User menu (see the Administrator's Guide).

The control unit logs the event each time a user shunts or restores a shunt group.

When the control unit activates any shunt group, it also activates any output of type Zones Shunted (see page 69).

If a shuntable zone is controlled by both a shunt key and a shunt group, the state of the zone may be unclear to the user. A shunt group cannot be deactivated if any of the group's zones are either open or shunted by a shunt key. In general, it is recommended that you ensure that each shuntable zone is controlled by either a shunt key or a shunt group, but not both together.

For other ways of shunting zones see Shunt Key Latched on page 45.

Restore Defaults

Staged Defaults

This menu option allows you to default parts of the control unit's configuration without affecting the whole system. You can choose to default the following:

User

Defaults all user access codes, their HUAs, proximity reader tags, and remote controls. User 001 access code changes to 1234 or 123456, as applicable.

This option also allows you to change between 4-digit and 6-digit codes. If you change to 6-digit codes, two additional zeros are added to the end of the existing installer code. If you change to 4-digit codes, the final two digits are removed from the end of the existing installer code.

Note: If you wish to make the i-rk01 use four-digit or six-digit access codes, please refer to the i-rk01 installation instructions.

Zones

Defaults all information relating to zones: types, attributes and partitions. For radio zones, the control unit retains the IDs of any detectors that the control unit has already learned.

Radio Devices

Deletes the IDs for learned radio devices. Scroll through the list of devices and select Yes for each type you want to delete, then press ✔ to action your selection. The *Keypads* option deletes one-way radio keypads only.

Outputs

Defaults all output configuration.

Setting Information

Defaults all setting options.

System Options

Defaults all options in the *System Options* menu.

Communications

Defaults all configuration for communications.

Factory Defaults

Tis removes all configuration from a control unit, including all names and stored texts, but not the log.

Note: You may wish to make a backup of the configuration before using *Factory Defaults*. You can do this using the Downloader software or the web interface.

To use the option:

1. Select *Factory Defaults* and confirm the operation when prompted.
2. Answer the configuration prompts. These are similar to those displayed when you first powered-up the control unit (see page 20).
3. To delete all users, remove and reconnect all power to the control unit immediately after using *Factory Defaults* (before you exit the Installer menu). You will need to repeat step 2 when you re-apply power.
4. Exit the Installer menu. The system scans the bus and finds the devices (see page 51).

Note:

- You will see PSTN Line Fault if the control unit uses PSTN communications. You will need to re-enter the appropriate telephone numbers (or disable communications using *Communications – ARC Reporting – Call Mode*).
- If you are using the web interface, re-enable the web browser interface and re-enter the control unit's own IP address (page 116). Note that you will also have to use *User Menu – System Config – Facilities On/Off – Remote Access* to enable remote access.

Installer Name

When logging in to the web interface, you must enter the username specified by this option. The username is case sensitive.

Installer Code

This code allows you to enter the Installer menu (which also carried out an Installer reset).

When logging into the web interface, you must key into the password field the same code as you have programmed into the *Installer Code* field.

The Installer code does not allow you to set or unset the system.

Keypad Text

This allows you to specify the text that appears on the first line of the display in the standby screen (such as your company name). See page 19 for editing text.

Remote Needs Entry

This option relates to the use of remote controls when unsetting a full-set system or full-set partition.

Enabled

The user must first trigger a Final Exit zone and start the entry timer before unsetting a full-set system or partition with a remote control. The system unsets those partitions the user is assigned to that have an active entry timer. If a partition that the user is assigned to does not have an active entry timer, the partition remains set.

Disabled

The user can unset the system or partition using a remote control without first starting the entry timer. The system unsets all partitions that the user is assigned to.

Remote Entry Part Set

This option relates to the use of remote controls when unsetting a part-set system or part-set partition.

Enabled

The user must first trigger a Final Exit zone and start the entry timer before unsetting a part-set system or partition with a remote control. The system unsets those partitions the user is assigned to that have an active entry timer. If a partition that the user is assigned to does not have an active entry timer, the partition remains part set.

Disabled

The user can unset a part-set system or partition using a remote control without first starting the entry timer.

RKP Needs Entry

This option relates to the use of one-way radio keypads when unsetting a full-set system or full-set partition.

Enabled

The user must first trigger a Final Exit zone and start the entry timer before unsetting the system (or partition) with a radio keypad. The system unsets those partitions the user is assigned to that have an active entry timer. If a partition that the user is assigned to does not have an active entry timer, the partition remains set.

Disabled

The user can unset the system using a radio keypad without first starting the entry timer. The system unsets all partitions that the user is assigned to.

RKP Entry PrtSt

This option relates to the use of one-way radio keypads when unsetting a part-set system or part-set partition.

Enabled

The user must first trigger a Final Exit zone and start the entry timer before unsetting a part-set system or partition with a radio keypad. The system unsets those partitions the user is assigned to that have an active entry timer. If a partition that the user is assigned to does not have an active entry timer, the partition remains part set.

Disabled

The user can unset a part-set system or partition using a radio keypad without first starting the entry timer. The system unsets all partitions that the user is assigned to.

HUA Response

This option is available only for part-setting systems. In a partitioned system, each partition can have its own HUA response. See page 74 for a description of this option.

PZ Unset Response

This option is available only for part-setting systems. See page 75 for a description of this option.

PZ Unset Response

This option is available only for part-setting systems. See page 75 for a description of this option.

PZ Reset time

This option is available only for part-setting systems. See page 76 for a description of this option.

Auto Rearm

This option is available when *System Options – Confirmation Mode* is set to Basic (page 86).

Use this option to specify the number of times that the system will re-arm when the siren time expires.

Select NEVER to make the system never re-arm (the system will go into alarm once only). Select one of the other options to make the system re-arm once, twice, three, four or five times, or always. The system re-arms all closed zones, but not detectors that are still sending alarm signals. (Note that this setting is required in order to comply with EN50131.)

If the system has rearmed, then when a user enters the system through the Final Exit door, the control unit will give an audible internal alarm in place of the normal entry tone.

Panel Loudspeaker

Volume

Use this option to change the volume of notification tones from a loudspeaker connected to the control unit. This volume control does NOT change the volume of alarm tones.

Partitions

In a partitioned system, you can assign the panel loudspeaker to any of the partitions. Any loudspeaker can belong to one or more partitions.

Entry Alarm Delay

Use this option to determine what the system will do if a user strays from an Entry Route zone during entry. (This option is available to provide compliance with EN 50131-1.)

Disabled

Makes the system give an alarm immediately a user triggers a zone other than the entry route zone during entry. **Note:** This is not compliant with EN50131.

Enabled

If the user triggers a zone other than the entry route zone during entry, the system waits 30 seconds before raising a full alarm. The system also gives an internal alarm during the 30-second wait.

If the user enters an access code or presents a tag before the end of the 30-second period, the user can reset the system.

Abort Time

Use this option to change Alarm Abort Delay period. The timer can take any value in the range 0 to 120 seconds.

The control unit starts the Alarm Abort Delay timer whenever it starts an alarm. If a user silences an alarm within the Abort Delay period, the alarm will not require an installer or remote reset.

If an alarm occurs and a user unsets the system **within** the Alarm Abort Delay period, the control unit activates any output of type Alarm Abort (page 63) and starts any Alarm Abort Fast Format communications programmed.

Supervision

If a radio detector loses contact for more than 20 minutes, the control unit generates an "RF Warning" event when the system is set. The event can be overridden during the setting process.

If a radio detector loses contact for more than two hours, the control unit may raise an alarm, depending on the setting you select:

Off

The control unit takes no action, irrespective of whether the system is set or unset.

Fault

With system set, the control unit logs the event, but does not display any alert or give a fault tone. With system unset, the control unit displays an alert, sounds a fault tone and logs the event. In both cases, any outputs of type RF Supervision or RF Fault activate.

Tamper

With system set, the control unit starts a tamper alarm and notifies the ARC with a "Supervision" message. With system unset, the control unit starts a tamper alarm and notifies the ARC with a "Supervision" message.

In both cases, if Tamper as Tamper Only is set to Disabled (page 89), any plug-by outputs of type Supervision or Fault activate. If the system is unset, plug-by outputs of type Jamming also activate. See page 89. If there is no Tamper channel allocated in Fast Format, the system sends an unconfirmed alarm.

Note that the *Tamper* option is required in Grade 2 systems to comply with PD6662.

Note: If you choose *Tamper* and also set *System Options – User Reset – System Tampers* to No, the user will not be able to reset the system after a loss of supervision event.

Jamming

This specifies the action the control unit should take when it detects jamming radio signals.

Off

The control unit takes no action, irrespective of whether the system is set or unset.

Fault

With system set, the control unit logs the event, but does not display any alert or give a fault tone. With system unset, the control unit displays an alert, sounds a fault tone and logs the event.

Tamper

With system set or unset, the control unit starts a tamper alarm and notifies the ARC with a "Jamming" message.

In both cases, if *Tamper as Tamper Only* is set to Disabled (page 89), any plug-by outputs of type Jamming or Fault activate. See page 89. If there is no Tamper channel allocated in FSL, the system sends an unconfirmed alarm.

Note that the Tamper option is required for PD 6662:2010.

Note: If you choose Tamper and also set *System Options – User Reset – System Tampers* to No, the user will not be able to reset the system after Jamming event.

Force Set

You may wish to allow a user with a remote control to set the alarm system when one or more of the detectors are not working or are active.

Note: If you enable Force Set, the system does not comply with EN50131.

Off

The remote control user cannot force set the system, even if you have applied the force set zone attribute to any zones.

Confirm

The remote control user can force set the system by pressing the appropriate button on the remote control, and when the system does not set, press it again to confirm setting.

On

The remote control user can force set the system by pressing the button on the remote control only once.

Note: The Confirm and On settings also allow a user with a remote control to set the system if a reset is required after an alarm. If any user is attempting to reset the system from a keypad when a remote user tries to set the system, the control unit will temporarily ignore the remote user.

Tamper Omit

If a user omits a zone, it may be necessary also to omit the tamper belonging to that zone.

Enabled

The tamper is omitted when a user omits a zone.

Disabled

The user cannot omit a tamper on a zone.

CSID Code

(Remote Reset)

The purpose of this option is to enable a user in conjunction with the ARC to perform an Installer reset. Enter any four-digit CSID (Central Station ID) code other than 0000 to enable the feature. The CSID code is normally supplied by the ARC and identifies the control unit to the ARC.

When an alarm occurs that requires an Installer reset:

1. A user can silence the sounders in the normal way.
2. When the user attempts to reset the alarm, the keypad prompts the user to call the ARC and quote a 4-digit number.
3. The user calls the ARC, provides the number and asks for a code to reset the system.
4. If satisfied with the user's identity, the ARC provides the code to the user.
5. The user enters the code into the keypad to reset the system.

Silence Alerts

This option controls the length of time that the keypad gives the alert tone (a brief 'beep' every second) when there is an alert.

Note: The control unit will not show keypad alerts while the system is set.

User Code

The keypad gives the tone until a user keys in an access code to acknowledge the alert.

30/60/120 minutes

The keypad gives the alert tone for the selected time. The status LEDs on the navigation key stay on for the selected time. The alert tone stops if a user enters a valid access code.

No Alert Tones

The keypad gives no alert tone. The red LEDs around the navigation key glow to show that there is an alert.

Mains Fail Delay

This option allows you to specify the length of time (0 to 60 minutes) that the control unit must wait after detecting a mains supply failure before reporting Mains Fail to the ARC.

When the mains supply fails, the control unit lights the red alert LEDs around the navigation key within a few seconds of the failure, activates any output programmed as General Fault and logs the Mains Fail event (in the mandatory log).

Note: Keypads do not show alerts while the system is set

The control unit does not report mains interruptions of less than 9 seconds to the ARC. If mains is restored within that time, the control unit switches off the red LEDs, deactivates the General Fault outputs and logs Mains Restore.

If a mains interruption lasts for longer than 9 seconds, the subsequent additional actions depend on the value in Mains Fail Delay:

- If *Mains Fail Delay* is set to 0, the control unit starts an alert tone ten seconds after the mains fail at the keypads and communicates a mains fail signal to the ARC (provided a communicator is fitted). At the same time, the control unit activates any outputs (including plug-by outputs) of type AC Fail.
- If *Mains Fail Delay* is set to 1-60 minutes, the control unit starts the mains fail delay time ten seconds after the mains fail.

  If mains power is restored before the end of the mains fail delay, the control unit switches off the red LEDs, deactivates any General Fault outputs and logs the mains restore. The control unit does not send any report to the ARC.

  If the mains fail condition is still present at the end of the mains fail delay, the control unit starts an alert tone at the keypads and communicates a mains fail signal to the ARC (provided a communicator is fitted). At the same time, the control unit activates any outputs of type AC Fail.

  A user can silence the alert by pressing the navigation key and entering a valid access code. The keypad displays details of the alert. The General Fault and AC Fault outputs remain active.

Once mains power is restored, the control unit deactivates any AC Fail outputs and logs the mains restore. A user can reset the alert and deactivate any General Fault outputs by pressing the navigation and entering the access code again.

External PSUs

If the system has an EXP-PSU fitted, or if an external PSU is connected to a zone with type External PSU AC Fail, the control unit treats a mains fail at the external PSU in the same way as a mains failure at the control unit, with one difference concerning reporting to the ARC:

If the control unit and external PSU both experience individual mains failures, but starting at different times, as long as those mains failures overlap and together last for more than the *Mains Fail Delay* period, the control unit will activate any AC Fail outputs and report a mains fail to the ARC. If the mains failures do not overlap, and are both individually shorter than the *Mains Fail Delay* period, the control unit logs the events and activates any General Fault outputs, but will not send a report to the ARC.

If the external PSU is allocated to a partition, and mains power at the external PSU is off for longer than the Mains Fail Delay period, the report to the ARC can show that the partition experienced a mains fail. This report is additional to any report the control unit might send concerning a mains fail at the control unit.

The control unit provides different methods of reporting to the ARC. For mains fail reporting each method differs in the detail that it can send:

- SIA/CID reports can indicate mains failure in individual partitions.
- Fast Format reports cannot show details of mains failure in partitions, only mains failure as a system-wide fault. This means that although the system can report that a mains failure occurred, it cannot show whether the failure was in the control unit or in an external PSU.
- Plug-by outputs cannot show details of individual partitions for a mains failure. Like Fast Format, they can only report mains failure as a system event.

Event Sequence	**Report Timing**
The control unit mains fails and the remote PSU mains fails within 10s.	The control unit waits for the mains fail delay and then starts a keypad alert and reports a mains fail.
There is a delay of more than 10s but less than the mains fail delay between a mains fail at the control unit and a mains fail at the remote PSU.	The control unit illuminates the red keypad LED after 10 seconds of the initial mains fail and then starts waiting for the selected mains fail delay. However, when the remote PSU mains fails the control starts a keypad alert and reports mains fail immediately.
There is a mains fail at the control unit, followed by a mains fail at the external PSU after the selected mains fail delay has expired.	The control unit lights the red keypad LED after 10 seconds of the initial mains fail and then starts a keypad alert and reports mains fail at the end of the selected mains fail delay. The control then logs the mains fail of the remote PSU.

The remote PSU experiences a mains fail.	After 10s, the control unit illuminates the red keypad LEDs, starts a keypad alert and reports a mains fail.
The remote PSU experiences a mains fail and then the control unit experiences a mains fail within the next 10s.	After the selected mains fail delay, the control unit illuminates the red keypad LEDs, starts a keypad alert and reports a mains fail.
The remote PSU experiences a mains fail and then the control unit experiences a mains fail AFTER the next 10s.	After 10s, the control unit illuminates the red keypad LEDs, starts a keypad alert, and reports a mains fail. When the control unit mains fails, the control unit logs the event after the selected mains fail delay.

Set Time & Date

This option lets you set the control unit's internal clock to the correct time and date. If you are not using an SNTP server (see below), you will have to re-program the date and time if the control unit loses power for an extended time and the battery is exhausted.

Note: The internal clock adjusts itself for daylight saving in Spring and Autumn.

SNTP Time Sync

You can use this option to keep the time at the control unit synchronised with the time at an SNTP (Simple Network Time Protocol) server on the internet.

The control unit uses the country setting (page 20) to adjust the time for the time zone.

SNTP Enable

Select On to enable SNTP time synchronisation.

Sync on Startup

Select On if you want the control unit to synchronise time automatically within the first few minutes after powering up.

Sync Daily

Select On if you want the control unit to synchronise time daily (every evening).

Manual Sync

Select this option if you want to synchronise time immediately. After using this option, use Set Time and Date to check the result.

NTP Server Names

Specify up to five SNTP servers to use. The control unit attempts each server in turn until one provides the time.

Panel Tamper Return

This option allows you to select either CC or FSL for the Tamper Return (TR) terminal on the control unit's PCB. By default, the terminal is CC. If you select FSL, you should insert a 2k2 resistor in series with the tamper return wire from the sounder.

Level 4 Updates

Setting this option to Enabled allows the level-4 user to update the firmware and language files at the control unit using the Web interface.

The first time you select Enabled, you are prompted to create the level-4 user by entering a user code. There can be only one level-4 user.

Once created, the level-4 user can log into the web interface and update the firmware and language files at the control unit, providing *Level 4 Updates* is enabled in the Installer menu and *System Config – Facilities On/Off – Level 4 Update* is enabled in the User menu.

The level-4 user is also able to log into the User menu or web interface and change the level-4 user name and code. The default user name is "Level4".

A level-4 user cannot perform other tasks, such as to set or unset the system, omit zones, etc.

Panel Upgrade

Selecting this option displays a list of .bin firmware files located in the INSTALL folder on the SD card (if fitted). You can use the option to upgrade the control unit's firmware. The current firmware is indicated by a *.

Note: The upgrade may default the control unit's configuration settings. Before using *Panel Upgrade*, it is recommended that you back up the system configuration using the Downloader software or the web interface.

Selecting a file begins the upgrade process. During the upgrade, the control unit will restart and the keypad's navigation LEDs may flash red. After the upgrade, the keypad returns to normal standby mode.

Chapter 10: Communications Menu

Contacts

You can use this option to define a Contacts List of up to 12 contacts (by default named Recipient A-L). The contacts are used by options such as *Communications – ARC Reporting* and *Communications – SMS* to specify the destination(s) for outgoing communications.

Each contact can have the following settings: *Name*, *Tel No 1*, *Tel No 2*, *Email Address* and *IP Address*.

ARC Reporting

This option allows you program the control unit for communications to an Alarms Receiving Centre (ARC) using either SIA, CID or Fast Format.

Note: If you have connected a plug-by communicator, use the *Outputs – Plug-by Outputs* menu to program the plug-by outputs to the communicator.

Call Mode

Use this option to choose the call mode for communicating with an ARC.

Disabled

The control unit disables all ARC communications.

Single

The control unit will contact the ARC using only Tel. Recipient 1 or IP Recipient 1, depending on Telecomms Priority (see below). If a connection to the ARC fails, the control unit re-attempts the connection up to a maximum of 15 attempts.

Alternate

The control unit will attempt to contact the ARC using Tel. Recipient 1 or IP Recipient 1, depending on Telecomms Priority (see below). If a connection to the ARC fails, the control unit re-attempts the connection using Tel. Recipient 2 or IP Recipient 2. If this connection fails, the control unit starts again using Tel. Recipient 1 or IP Recipient 1, for a maximum of 15 attempts of both recipients.

Telecomms Priority

If a plug-on module is fitted, the control unit has more than one communication method to the ARC (Ethernet and GSM, or Ethernet and PSTN). You can use this option to specify the priority of each communication method, or to disable a method entirely. You can set the priority to 1, 2 or - (disabled).

If possible, the control unit uses the method that has priority 1, but if this is not possible, the control unit uses the method that has priority 2.

Note: For communication to an ARC over Ethernet, currently, only SIA is supported (within a SIA-IP wrapper), developed to SIA DC-09-2013. Before using SIA-IP, please check that your ARC supports it. If not, please advise them to contact Eaton for assistance.

Recipients

Use this option to specify the telephone numbers and/or IP addresses to use to send messages to the ARC. You do this by selecting contacts from the Contacts List (page 102).

Tel. Recipient 1

If you want to send messages to the ARC by telephone, select a contact from the Contacts List, and then either the first or second telephone number defined for that contact. Otherwise, select None if you do not want to send messages to the ARC by telephone.

Tel. Recipient 2

You can specify a second telephone recipient in the same way as for Tel Recipient 1. The control unit can use the second recipient only if *ARC Reporting – Call Mode* is set to Alternate.

IP Recipient 1

If you want to send messages to the ARC over Ethernet, select a contact from the Contacts List, and then specify the port number (default 2749). The control panel communicates with the ARC using the IP address of the selected contact and the port number. Select None if you do not want to send messages to the ARC over Ethernet.

IP Recipient 2

You can specify a second IP recipient in the same way as for IP Recipient 1. The control unit can use the second recipient only if *ARC Reporting – Call Mode* is set to Alternate.

Account Numbers

Use this option to store an ARC account numbers.

If you are configuring a partitioned system, the control unit gives you the opportunity to store an account number for each partition. If you are configuring a part-setting system, you can store one account number.

With CID reporting, the system reports alarms using a four-digit account code.

With Fast Format and SIA reporting, you can use four-, five- or six-digit codes. The control unit pads five-digit codes to six digits using a leading zero. The control unit leaves four- and six-digit codes unchanged.

Note: If you need to add a letter to the account code, press the numbers keys repeatedly until the letter you want appears on the display. See page 19.

Report Type

Use this option to choose the report type to send to the ARC.

The report types available are: Fast Format, Contact ID, SIA 1, SIA 2, Scancom SIA 3, Extended SIA 3 and Extended SIA3 v2.

Fast Fmt Channels

(See Appendix A for a brief description of Fast Format.)

Note: Eaton does not recommend using the i-gsm02 for Fast Format communications. The GSM network introduces too great a variation in the delay between signal and response. Tests carried out by Eaton show that different cell towers from the same providers give different results.

If you selected Fast Format in *Report Type*, you can use *Fast Fmt Channels* to allocate an event to each of eight channels. Table 12 shows the default events for each channel. Table 13 and Table 14 show the events available. You can key-in the two-digit numbers shown next to each event in order to display that event type on the keypad.

Table 12: Fast Format Channel Factory Defaults

Channel	**Event**
Channel 1	Fire Alarm
Channel 2	Hold Up Alarm
Channel 3	Burglar Alarm
Channel 4	Open/Close
Channel 5	Zone Omit (System)
Channel 6	Tamper
Channel 7	Confirmed Alarm
Channel 8	General Fault

Table 13: Fast Format Events (UK Systems)

00. Not used
01. Fire Alarm
02. Hold Up Alarm
03. Burglar Alarm
04. Open/Close
05. Alarm Abort
06. Technical Alarm
07. Confirmed Alarm
08. RF Low Battery
09. RF Supervision (see note 4)
10. RF Jamming (see note 4)
11. Mains Fail (see note 5)
12. Tamper (see note 6)
13. Open (see note 1)
14. Close (see note 1)
15. Zone Omit (Setting) (see note 2)
16. Zone Omit (System)
17. General Fault
18. Masking
19. Zone Shunt
20. Duress Code
21. HUA Confirm
22. Burg Confirm Alarm
23. Perimeter Alarm
24. Burg Alarm P1 (partitioned system only)
.. up to the maximum number of partitions

Table 14: Fast Format Events (EU Control Units)

00. Not used
01. Fire Alarm
02. Hold Up Alarm
03. Burglar Alarm
04. Open/Close
05. Alarm Abort
06. Technical Alarm
07. Confirmed Alarm
08. RF Low Battery
09. RF Supervision (see note 4)
10. RF Jamming (see note 4)
11. Mains Fail (see note 5)
12. Tamper (see note 6)
13. Open (see note 1)
14. Close (see note 1)
15. Zone Omit (Setting) (see note 2)
16. Zone Omit (System)
17. General Fault
18. Masking
19. Zone Shunt
20. Duress Code
21. Perimeter Alarm
22. Burg Alarm P1 (partitioned system only)
.. up to the maximum number of partitions

Notes:

1. Open and Close provide the same functions as Open/Close, but on two separate channels.
2. Zone Omitted – the control unit sends this signal for five seconds when a user omits a zone.
3. The control unit delays reporting/logging either mains loss, or exiting Installer Menu with mains loss, by 15-18 min (chosen randomly).
4. The control unit communicates Jamming, Supervision when the system is unset.
5. The control unit communicates Mains Fail depending on the time programmed in *System Options – Mains Fail Delay* (see page 98 for a detailed description).
6. If there is no channel allocated for Tamper events then the control unit may report tampers as Burglar Alarms to ensure that the ARC is notified.

CID/SIA Events

(This menu appears only if you select “Contact ID” or any of the SIA versions in *Communications – Report Types*. See Appendix A for a description of the CID and SIA formats.)

To make configuration easier, the control unit groups CID/SIA telegrams together into Report Groups. Table 15 and Table 16 list the CID/SIA codes included in each report group. When you enable a Report Group, you are enabling the control unit to send any of the telegrams in that group.

CID/SIA alarm transmissions will take considerably more time than Scancom Fast Format since the system transmits extended alarm data to the ARC.

Note: The control unit delays reporting/logging either A/C mains loss, or leaving Installer menu with A/C mains loss, by 15-22 minutes (chosen randomly). The control unit delays reporting/logging either mains restore, or leaving Installer menu with mains restored, by 60-90 sec (chosen randomly).

Table 15: CID Report Groups

CID Code	**Includes:**	**CID Report Group**
110	Fire and fire restore	Fire Alarm
120	Zone HUA (PA) and restore Silent HUA (PA) and restore Keypad HUA (PA), Keypad HUA (PA) restore RF HUA (PA), RF HUA (PA) restore Radio keypad HUA (PA), radio keypad HUA (PA) restore	Hold Up Alarm
121	Duress code alarm	Hold Up Alarm
129	HUA (PA) confirm	Hold Up Alarms
130	Burg and Burg restore	Burglar Alarm
131	Burg-Perimeter and Burg-Perimeter restore	Burglar Alarm
137	Panel Lid tamper and restore Keypad tamper and restore Detector tamper and restore Bell tamper and restore Radio keypad tamper and restore External siren tamper and restore	Tampers

	WAM tamper and restore Missing bus device and restore Tamper bus device and restore	
139	Alarm confirmation	Burglar Alarm
150	Technical alarm and restore	Technical Alarm
300	Fail and restore for: Aux 12V, Aux 14.4V, Bell 12V, Bus 12V, System 12V	Faults
301	A/C power fail alarm (also called Mains fail) and restore	Mains Fail
302	Panel Battery low/fail and restore	Panel Battery
305	System or partition reset	Reset
311	Panel Battery low/ missing and restore	Panel Battery
311	External battery fault and restore	Faults
320	Zone External Warning Device fault and restore WAM trouble and restore	Faults
330	Bus device aux fuse fault and restore	Faults
337	Smoke/WAM psu fail and restore	RF Battery/PSU
337	Bus device low voltage fault and restore External PSU fault and restore via zone n	Faults
338	Ext Siren/WAM low battery fail and restore	RF Battery/PSU
338	External PSU low volts via zone n	Faults
342	External PSU AC fail and restore	Faults
344	Jamming fail and restore*	RF Jamming
351	Comms line fault and restore	Faults
373	Smoke fault and restore	Faults
375	Zone HUD Fault and restore	Faults
380	Masking fault and restore	Burglar Alarm Masking
381	Zone supervision fail and restore Radio keypad supervision fail and restore External radio siren supervision, fail and restore* Internal radio sounder supervision, fail and restore WAM supervision fail and restore	RF Supervision
384	Zone low battery fail and restore	RF Battery/PSU
389	4k4 Fault and restore on zone n	Faults Masking
401	System or partition set and unset	Set/Unset
401	System or partition part set	Part Set
406	Alarm Abort	Burglar Alarm
409	System or partition keyswitch set and unset	Set/Unset
409	System or partition keyswitch part set	Part Set
412	Downloading successful	Downloading
457	Exit timeout and restore	Exit Timeout

461	Four wrong user codes (also called “User code tamper” or “excess keys”)	Tampers
573	User/system zone omit. Zone omit restore.	Omit
575	Bypass (shunt)	Omit
625	Time and date reset	Time Date Reset
627	Installer mode start keypad (web)	Installer Mode
628	Installer mode end keypad (web)	Installer Mode

**Note:*

1. The control unit communicates Jamming, Supervision when the system is unset.

Table 16: SIA Report Groups

SIA Code	**Includes:**	**SIA Report Group**
AT, AR	Mains fail and restore	Mains Fail
AT, AR	External PSU AC fail and restore	Faults
BA, BR	Burg and Burg restore	Burglar Alarm
BB, BU	User/system zone omit. Zone omit restore. Burglary Bypass (shunt)	Omit
BC	Alarm Abort	Burglar Alarm
BT, BJ	Masking fault and restore	Burglar Alarm Masking
BV	Alarm confirmation	Burglar Alarm
BZ	Zone supervision fail and restore Radio keypad supervision fail and restore External siren supervision, fail and restore* Internal radio sounder supervision, fail and restore WAM supervision fail and restore	RF Supervision
CE	Calendar set deferred	Set/Unset
CL	System or partition part set	Part Set
CL, OP	System or partition set and unset	Set/Unset
CS	System or partition keyswitch part set	Part Set
CS, OS	System or partition keyswitch set and unset	Set/Unset
EA	Exit timeout and restore	Exit Timeout
EJ, ES	Missing bus device and restore Tamper bus device and restore	Tampers
ET, ER	Bus device aux fuse fault and restore	Faults
ET, ER YP, YQ	Bus device low voltage fault and restore External PSU fault and restore via zone n	Faults
FA, FR	Fire and fire restore	Fire Alarm
FT, FJ	Smoke fault and restore	Faults
HA, HR HV	Duress Hold Up Alarm Confirmed	Hold Up Alarm
IA, IR	4k4 Fault and restore on zone n	Faults Masking
JA	User code tamper (excess keys)	Tampers

JT	Time and date reset	Time Date Reset
JV JX RH	User a changed user b's code User a deleted user b User codes defaulted	User Code Change
LB (RB)	Installer mode start keypad (web)	Installer Mode
LR, LT	Comms line fault and restore	Faults
LS (RS)	Installer mode end keypad (web)	Installer Mode
OR	System or partition reset	Reset
PA, PR	Zone HUA (PA) and restore Keypad HUA (PA), Keypad HUA (PA) restore RF HUA (PA), RF HUA (PA) restore Radio keypad HUA (PA), radio keypad HUA (PA) restore	Hold Up Alarm
PT, PJ	Zone HUD fault and restore	Faults
RS	Downloading successful	Downloading
RU	Downloading failed	
TA, TR	Keypad tamper and restore Detector tamper and restore Lid tamper and restore Bell tamper and restore Radio keypad tamper and restore External siren tamper and restore Internal sounder tamper and restore WAM tamper and restore	Tampers
TA, TR	WAM trouble and restore	Faults
UA, UR	Technical alarm and restore	Technical Alarm
UA, UR	Perimeter and Perimeter restore	Burglar Alarm
UB, UU	Zone bypass and un-bypass (shunt)	Omit
XQ,HQ	Jamming fail and restore*	RF Jamming
XT, XR	Zone low battery fail and restore	RF Battery/PSU
YA, YH	Zone External Warning Device fault and restore	Fault
YM, YR	Control unit battery low/ missing and restore	Panel Battery
YM, YR	External battery fault and restore	Faults
YP, YQ	Smoke/WAM psu fail and restore	RF Battery/PSU
YP, YQ,	Fail and restore for: Aux 12V, Aux 14.4V, Bell 12V, Bus 12V, System 12V	Faults
YT, YR	Ext Siren/WAM low battery fail and restore	RF Battery/PSU
YT, YR	Control unit battery low/fail and restore	Panel Battery
YT, YR	External PSU low volts via zone n	Faults
YW	System error	Faults

*__Note:__ The control unit communicates Jamming and Supervision when the system is unset.

Restorals

When you enable a CID/SIA Report Group, or when you use Fast Format reporting, the control unit communicates both when an event occurs, and when the condition causing the event stops. The second communication is also called a “restore”.

You can enable or disable restoral reporting using this option.

Burg Comms Rearm

(This menu appears only if you select “Fast Format” in *Communications – Report Type*. AND if *System Options – Confirmation – Confirmation Mode* is set to “Basic”.) This menu option determines what the control unit does with the “Burg” Fast Format channel 3 at the end of the siren run time.

Disabled

The channel stays active until an Installer or user resets the system.

Enabled

The system rearms Channel 3 once the siren timer has expired. Once the Channel is rearmed, the system is ready to report any new alarm. The system bypasses any detectors that are still triggered.

Note: If a Final Exit Zone is triggered, Channel 3 becomes active at the end of the Programmed Entry time.

21CN FF Ack Time

(This menu appears only if you select Fast Format in *Communications – Report Type*. The menu does NOT appear if a GPRS or Ethernet module is fitted.)

A PSTN line connected to a BT21CN line (or equivalent) will take longer to acknowledge a Fast Format transmission. This option allows you to adjust the length of time that the control unit waits for the ARC acknowledgement. You can adjust the acknowledgement time from a minimum of 400ms up to a maximum of 1200ms in 100ms steps.

Send Tamp As Burg

When using CID or SIA reporting, this option allows you to program the control unit to send tampers as alarm.

If you select Disabled, (the default) then the control unit sends all CID/SIA messages as specified in *Communications – ARC Reporting – CID/SIA Events*.

If you select Enabled, then for full alarm response, the control unit sends tampers as burglary (BA) and sends Contact ID 130 in place of Contact ID 137.

Dynamic Test Call

Use this option to enable dynamic testing. In dynamic testing, the system makes a test call 24 hours after the last alarm communication.

Note: If this option is not visible, static test calls are enabled. To use dynamic test calls, disable static test calls first.

Static Test Call

Note: If this option is not visible, dynamic test calls are enabled. To use static test calls, disable dynamic test calls first.

In static testing the system makes a test call either on:

- Every day at one particular time of day or
- On the same day of every week, or
- On one day every month.

To make test calls at a set time every day select Daily, then select a number between 01 and 24 to choose the time of day for the call. For example, select 18 to program the control unit to make a static test call at 6:00pm every day.

To make test calls on the same day every week, select Weekly, then select the day of the week on which the call should take place. Next, key in the hour of the day (01 to 24) on which the test call should occur.

To make test calls on one day every month, select Monthly, then select a number between 1 and 31 to specify the day of the month on which the call should take place. Next, key in the hour of the day (01 to 24) on which the test call should occur.

For each of the three types of call, the control unit will add or subtract up to 16 minutes at random to the hour you specified. This is to make sure that the ARC is not overwhelmed with a flood of test calls from systems that have all been given the same time.

Select *Communications – ARC Reporting – Static Test Call – Disabled* to disable static test calls.

Unset Comms

Use this option to prevent the system sending excessive communications traffic while the system is unset.

Enabled

> The control unit communicates all signals regardless of whether the system is set or unset.

Disabled

> The control unit sends tampers, mains fail and other status signals when the system is set, but not when it is unset.

Speech Dialler

The i-sd02 and i-gsm02 have a built-in speech dialler. These modules can record five speech messages using their internal microphones and replay them to a specified telephone numbers to report an alarm. One message is called the “Home message”, and is always played at the beginning of a report. You should use this message to identify the control unit and its location. The other four messages (Message 1-4) allow you to record some indication of the type of event causing an alarm, for example: “Fire” or “Hold Up Alarm”. The control unit plays these messages after the Home Message.

Using the *Triggers* option, you link each Message 1-4 with a specific trigger (event category) you wish to report. You then select a set of destinations for each message. Each destination specifies one of the telephone numbers you wish the control unit to call when the event occurs.

If the control unit has *Call Acknowledge* enabled (see page 112), the person receiving the speech messages can control the link by sending DTMF tones back to the control unit (usually by pressing buttons on the telephone key pad). The commands available are:

Function	**Key**
End this call	DTMF ‘5’
Play ‘Home’ and ‘alarm’ message	DTMF ‘3’
Clear down	DTMF ‘9’

Note that when the called party answers a speech dialler call, there could be a six-second delay before the control unit starts playing the home message.

Call Mode

This option enables or disables the speech dialler feature.

Messages

Use this option to record the speech messages you wish the speech dialler to use.

There are five messages slots available: The Home Message and Messages 1 to 4. The i-sd02 and i-gsm02 plug-in module can record up to ten seconds of speech for the Home message, and up to five seconds of speech for each of the alarm messages. Within each message, you can use any of the following options:

Record Message

Press ▶ to start recording. The control unit starts recording from the module's built-in microphone. The display shows a progress bar indicating how long you have left to record. Press ✘ to end recording.

Play Message

Press ▶ to play back the message from the module's speaker.

Delete Message

Press ▶ to delete the message. When the display asks “Delete Message?” press ✔.

Use Lid Tamper

This puts the control unit into a special mode where the tamper switch controls the recording and playback of the current message. Use this mode if the control unit is an inconvenient distance from the keypad.

1. Start with the control unit lid off and the tamper switch open.
2. At the keypad select *Use Lid Tamper* and press ✔.
3. At the control unit hold down the tamper switch. When the red LED on the plug-in module glows, recite your message.
4. Release the tamper switch.
5. Pulse the tamper switch briefly. The plug-in module plays back your recording.
6. Go back to the keypad and press ✘.
7. If required, replace the control unit lid. **DO NOT** replace the control unit lid until you have left the “Use Lid Tamper” mode.

Triggers

For each Message 1-4, specify the event category that you want to associate with the message. You can choose any one of the following:

Fire Alarm (see page 63)

Hold Up Alarm (see page 63)

Burglar Alarm (see page 63)

Technical Alarm (see page 64)

Tampers (see page 64)

Mains Fail (see A/C Fail, page 64)

Soak Test Fail (see page 49)

Destinations

Use this option to specify the recipients of the messages:

1. Select a Message 1-4.
2. Select one of the four recipients. Each Message 1-4 can have up to four recipients.
3. Select a contact from the Contacts List (page 102), then one of the two telephone numbers defined for that contact.
4. If required, repeat the process from step 2 to specify additional recipients for the message.
5. If required, repeat the process from step 1 for another Message 1-4.

Call Acknowledge

If the called party answers a speech dialler call, they can end the call by sending back a DTMF ‘9’.

Enabled

The control unit ends the call when it receives a DTMF ‘5’ or ‘9’. If the control unit does not receive a DTMF ‘5’ or ‘9’ then it attempts to call again (up to three times).

Note that after receiving a DTMF ‘5’ the control unit will go on to call any other programmed speech dialler numbers. After receiving a DTMF ‘9’ the control unit will cancel all further calls for the current alarm.

Disabled

The control unit stops further call attempts to that number as soon as it detects a call being answered.

SMS

Outgoing

When an alarm or other event occurs, the control unit can send a report by SMS text to up to four recipients.

The report comprises:

- A Home Message of your choice (such as to identify the control unit and location).
- Another message of your choice (which may give other information about the event). You can define four of these messages (by default named Message 1-4).
- The text of the event (as it appears in the log).

Using the *Triggers* option, you link each Message 1-4 with a specific event category you wish to report. You then select a set of destinations for each message. Each destination specifies one of the telephone numbers you wish the control unit to call when the event occurs.

Call Mode
This option allows you to enable or disable SMS reporting.

Messages
Specify the text for the Home Message and for the additional four messages (Message 1-4). The Home Message can have up to 12 characters. Message 1-4 can have up to 30 characters.

Triggers
For each Message 1-4, specify the event categories that you want to associate with the message. You can choose one or more of the following:

Alarms

Includes all types of alarm, including 24 hour, Fire, HUA, Burg, test zone fail, Zone Alarm and Zone Follow. This also includes restores from those alarms. See page 61 for details of how Zone Alarm and Zone Follow are configured.

Tampers

Includes all types of tampers, including system, keypad, expander, sensor, user code (excess digits), siren, WAM and radio keypad.

Sets/Unsets

Includes any type of setting, part-setting or unsetting of a partition (or part set) by either keypad, remote control, or keyswitch.

System

Includes any type of system event that is not an alarm, tamper or set/unset. This includes bus device missing, jamming, supervision fail, communications failure or fault, AC lost, low or missing system battery, low battery on radio device and Aux 12V fail.

Destinations
Use this option to specify the recipients of the reports:

1. Select a Message 1-4.
2. Select one of the four recipients. Each Message 1-4 can have up to four recipients.
3. Select a contact from the Contacts List (page 102), then one of the two telephone numbers defined for that contact.
4. If required, repeat the process from step 2 to specify additional recipients for the message.
5. If required, repeat the process from step 1 for another Message 1-4.

Incoming
If the control unit uses an i-gsm02 plug-in module, users can change or query the status of the control unit using commands contained within SMS text messages sent from a mobile phone or other messaging device. This feature can, for example, be used to set/unset the system, activate/deactivate outputs, omit/un-omit zones or query the current status of the system. For full details of the commands, please refer to the SMS Command Messaging User's Guide.

Remote Control

Enables the feature.

Forwarding

Enables you to configure the control unit to forward SMS messages received from the network provider (such as low-credit warnings) to a specified telephone number. When you select Forwarding, the Contacts List (page 102) is displayed. Select a contact from the Contacts List, then one of the two telephone numbers defined for that contact.

PSTN SMS

If you are sending SMS messages by way of the PSTN line, you must program some extra information under this menu.

Protocol

This option allows you to select the protocol used by the Service Centre.

Service Centre Tel No

The option allows you to store the Service Centre's telephone number. The default number is 147017094009 for ETSI Protocol 1.

Consult the technical support department of the service provider that you wish to use. When asking for the service centre number ask which protocol they support. Press * to insert a two second pause, if required. The display shows this as a comma.

Own Telephone No.

This option appears when you select either of the UCP protocols. The option allows you to record the telephone number that originated the SMS message. This number is visible to the receiver of the message.

Email

When an alarm or other event occurs, the control unit can send a report by email to up to four recipients.

The report comprises:

- A Home Message of your choice (such as to identify the control unit and location).
- Another message of your choice (which may give other information about the event). You can define up to four of these messages (by default named Message 1-4).
- The text of the event (as it appears in the log).
- Images from a camera, if saved by a camera trigger (see page 61). For example, if a camera trigger saves images when there is a Fire Alarm, these images are automatically attached to any report that is generated by a Fire Alarm.

Using the *Triggers* option, you link each Message 1-4 with a specific event category you wish to report. You then select a set of destinations for each message. Each destination specifies an email address you wish the control unit to contact when the event occurs.

Call Mode

This option allows you to enable or disable email reporting.

Messages

Specify the text for the Home Message and for the additional four messages (Message 1-4). Each message can have up to 30 characters.

Triggers

For each Message 1-4, specify the event categories that you want to associate with the message. You can choose one or more of the following:

Alarms

Includes all types of alarm, including 24 hour, Fire, HUA, Burg, test zone fail, Zone Alarm and Zone Follow. This also includes restores from those alarms. See page 61 for details of how Zone Alarm and Zone Follow are configured.

Tampers

Includes all types of tampers, including system, keypad, expander, sensor, user code (excess digits), siren, WAM and radio keypad.

Sets/Unsets

Includes any type of setting, part-setting or unsetting of a partition (or part set) by either keypad, remote control, or keyswitch.

System

Includes any type of system event that is not an alarm, tamper or set/unset. This includes bus device missing, jamming, supervision fail, communications failure or fault, AC lost, low or missing system battery, low battery on radio device and Aux 12V fail.

Destinations

Use this option to specify the recipients of the reports:

1. Select a Message 1-4.
2. Select one of the four recipients. Each Message 1-4 can have up to four recipients.
3. Select a contact from the Contacts List (page 102); the control unit will use the email address of that contact.
4. If required, repeat the process from step 2 to specify additional recipients for the message.
5. If required, repeat the process from step 1 for another Message 1-4.

Server

Specify the details of your mail server (available from the email provider):

Server Name – The address of the outgoing mail server (e.g. mail.gmx.com).

Server Port Number – The port number of the mail server (e.g. 587).

Account – Your account name (e.g. fred@gmx.com).

Username – Your username to access the email account.

Password – Your password to access the email account.

SSL – Select Enabled if the mail SSL uses SSL.

Line Fail Response

Use this option to specify how the system should respond when the control unit detects a line-fail fault on a communications path from the control unit. You can specify different settings for Ethernet, plug-by and plug-on module communications.

Audible

If the system is unset then the system logs the event. The keypads produce a short audible tone every minute. Entering a valid access code silences the sounders and the display indicates a telephone line fault. The system can be set again with the line fault present.

If the system is set then the control unit logs the event but does not give any tone or display. The control unit cancels any programmed siren delay if the line is out of order when an alarm occurs.

Note: Eaton recommends audible response for line fault.

Silent

If the system is unset then the keypad display indicates a telephone line fault, the LEDs around the navigation key glow red, and the control unit logs the event. The system may be set again with the line fault present.

If the system is set then the control unit does not give any indication or tone but does log the event. The control unit cancels any programmed siren delay if the line is out of order when an alarm occurs.

Disabled

The control unit does not monitor the telephone line.

Line Fail Delay

Use this option to specify the length of time the control unit waits after detecting a line-fail fault on a communications path from the control unit before it generates an alert, actives communications and activates line-fail outputs. You can specify different settings for Ethernet, plug-by and plug-on module communications.

Note: The control unit may take a few seconds to recognise a line fail. The actual delay between line fail and the resulting alert will be slightly longer than the value you specify.

IP Network (Own)

This menu allows you to configure settings related to the Ethernet port of the control unit.

Note: Remember that changes are not saved until you exit the Installer menu.

Web Server

This controls the availability of the control unit's built-in web interface.

Status

Set to Enabled to enable the interface.

IP Port Number

This is the port that the control unit uses for the interface. The default is 80.

VKP Instant

This option is available only if *Status* is set to Enabled. Set *VKP Instant* to Enabled to enable the virtual keypad, known as the Virtual Keypad Instant or VKP Instant. When enabled, anyone on the network can access the virtual keypad through a web browser using the url: "https://[panel IP address:4433]/keypad.cgi". For example, "http://198.168.0.100:4433/keypad.cgi".

The virtual keypad allows users to perform the same functions as at a standard keypad, providing they have a valid access code.

Note: The browser must have cookies enabled for the virtual keypad to work correctly.

The Installer access code can use the virtual keypad only when the system is completely unset.

VKP Instant is designed for use on PCs, mobile devices and tablets.

Downloader

You can use this option to specify the port that the control unit uses for Downloader over IP. The default is 55132.

M2M Interface

This controls the availability of the control unit's Machine-to-Machine (M2M) interface, which allows real-time streaming of data to a machine via Ethernet. For further information, please contact your Area Account Manager.

Status

Set to Enabled to enable the interface.

IP Port Number

This is the port that the control unit uses for the interface. The default is 1895.

IP Address

This specifies the control unit's own IP address (e.g. "192.168.000.100"). Press "*" to key in a dot. Leave the IP address blank if you want a DHCP-assigned address. If you enter an IP address, also specify the *IP Subnet Mask*, *Gateway IP Address* and *DNS IP Address*.

Note: Changes take place only after you exit the Installer menu. If you are using DHCP, use *About Panel – About Comms – IP Address* to find out the IP address the control unit is using.

IP Subnet Mask

This option is displayed if *IP Address* specifies a fixed IP address. Enter the subnet mask (e.g. "255.255.255.000").

Gateway IP Address

This option is displayed if *IP Address* specifies a fixed IP address. Enter the IP address of the router that connects the local network, to the internet (or to a larger network).

DNS IP Address

This option is displayed if *IP Address* specifies a fixed IP address. Enter the IP address of the DNS server on the network.

Module Ethernet

This menu is available if there is another compatible (e.g. Chiron) module fitted.

IP Address

This specifies the module's own IP address (e.g. "192.168.000.001"). Press "*" to key in a dot. Leave the IP address blank if you want a DHCP-assigned address. If you enter an IP address, also specify the *IP Subnet Mask* and *Gateway IP Address.*

IP Subnet Mask

Enter the subnet mask (e.g. "255.255.255.000").

Gateway IP Address

Enter the IP address of the router that connects the local network, to the internet (or to a larger network).

Port Number

This is the port that the module uses when connecting to Downloader.

GPRS Module

This menu is displayed if you have fitted a Chiron or Chiron-compatible module.

IP Address

This specifies the module's own IP address (e.g. "192.168.000.001"). Press "*" to key in a dot. Leave the IP address blank if you want a DHCP-assigned address. (Eaton recommends that you leave this field blank.)

Port Number

Specifies the port number used by the module.

APN

Enter the GPRS Access Point Name.

Username

Use this option to store the GPRS User ID.

Password

Use this option to store the GPRS password.

Dynamic DNS

This option enables you to configure settings to use a dynamic DNS (DDNS) server, which will keep track of any changes to the external IP address of the control unit's internet connection (as supplied by the internet service provider). The feature allows other DDNS-enabled services on the internet to access the control unit, even if the external IP address changes.

To use this feature, you must first ensure that an account is available on the DDNS server that the control unit can use.

Status

Set to Enabled to enable the interface.

Provider

Choose the DDNS provider: no-ip, dyn or ChangeIP.

Hostname

Specify your hostname, as supplied by the DDNS provider.

Username

Specify your username, as supplied by the DDNS provider.

Password

Specify your password, as supplied by the DDNS provider.

Last Update Status

Gives the status of the last update to the DDNS provider.

Detected ext. IP

Gives the external IP address detected by the control unit for the network that the control unit is connected to.

Downloading

The Downloader software running on a PC can be used to:

- Inspect and/or change the configuration of the control unit.
- Monitor the state of the control unit and its zones.
- Perform a remote service, which generates a report to show the service status of the system.

Downloader can communicate through the control unit's USB port, Ethernet port or through plug-in communications module.

Note: When you have finished making changes to the control unit's configuration, use the Disconnect icon in Downloader to end the connection. DO NOT remove power from the control unit before disconnecting or all your changes will be lost.

Note: If *User Menu – System Config – Facilities On/Off – Remote Access* option is set to "No", the control unit rejects all attempts by Downloader to open a connection. This option does NOT prevent the alarm system user from starting a call to Downloader by using *User Menu – System Config – Call Downloader*.

If you intend to use an i-gsm02 module:

- For dial-in access, you must provide a SIM card that permits data traffic.
- A voice-only SIM card will allow a user to start a call to Downloader from the User Menu.
- To use both the speech dialler and remote dial-in access from Downloader, fit a SIM card that permits both voice and data traffic.

Note that when setting up a remote connection of any kind, it is advisable to test the connection before leaving the site.

In order to use the Downloader software, you must program following options:

Account

As part of ensuring the security of a connection, Downloader must uses a separate account name and serial number for each control unit. You can set up the account name and serial number at the control unit using this option.

Note: On the first connection, Downloader records the account name and serial number set up at the control unit. From that point on, Downloader must have the same account name and serial number as defined at the control unit.

Name

The account name can be any string of up to 16 alphanumeric characters and numbers.

Serial Number

The serial number must be an eight-digit numerical string. If the number you wish to use has less than eight digits, insert leading zeroes.

Connection Type

Use this option to enable a one-off connection to the PC running Downloader to inspect or change the configuration of the control unit, or monitor its current state. It is not used if you want to perform a remote service. The setting overrides *Access Mode*.

Choose which physical connection you wish to use.

Remote

Allows the control unit to accept an incoming IP connection, or a call from a remote PC over the telephone network. For a telephone connection, you will also need to program *Rings to Answer* and/or *Answer on One Ring*, as described below. (Note that *Secure Callback* does not work with this option.)

Local

Connect the control unit to a PC (for example a laptop) using a local USB cable.

Note: The control unit will leave the *Connection Type* menu if Downloader does not make a call within 30 minutes.

See *Access Mode* if you want the control unit to answer incoming calls from Downloader without an Installer being present.

Rings to Answer

Select the number of rings that the system waits before answering an incoming telephone call from the remote PC.

Answer On One Ring

Use this feature if the alarm system shares a telephone line with other equipment.

When enabled, Downloader “warns” the control unit that a call is coming by ringing the control unit number, waiting for between one and three rings and then hanging up. The control unit now knows to expect a call within the next 10 to 90 seconds. Downloader then rings the control unit again, within 10 to 90 seconds. The control unit answers after the first ring.

Note: When using *Answer on One Ring*. set the number of rings in *Rings to Answer* to a higher number than that used by the equipment sharing the telephone line with the control unit. If you do not, then the other equipment will never answer any incoming calls.

Access Mode

This function specifies the method to use to start communications over a telephone line or IP network from a remote PC running Downloader. For an IP connection, select the Unattended setting.

Call Out Only

Someone must start a call to the remote PC manually from within User Menu (select *User Menu – System Config – Call Downloader*).

Secure Callback

When the remote PC calls, the system waits for the set number of rings (see "Rings to Answer") and then answers. The remote PC sends a control unit ID, the Downloader software version, and indicates which of the two Downloader Telephone Numbers to use (see *Phone Book* below). The system checks that the remote PC is sending the correct control unit ID, and is using the correct Downloader software version. If these items don't match, the system hangs up. If the items do match, the system hangs up and, after a short delay, the system seizes the telephone line and calls the PC using the indicated Downloader Telephone Number.

Note: *Secure Callback* must be Disabled until the first “attended” upload has been performed. This first upload can be carried out either from the User or Installer menu.

Unattended

Select this setting if you are using an IP connection.

For a telephone connection, the control unit answers as soon as the number of rings set in *Rings to Answer* or *Answer on One Ring* have elapsed. **Note:** The Downloader operator can choose to use *Secure Callback*, even though the alarm system is programmed for Unattended Mode.

Phone Book

Use this option to program two separate telephone numbers that the system will use during downloading. When the remote PC operator makes a connection, they select one of these telephone numbers for the control unit to call back on (for example to the operator's home or office).

Press ▲ or ▼ keys to move the cursor backwards and forwards through the number if you wish to edit it.

Press ◄ to delete the digit to left of the cursor.

Press * to add a 2-second pause, if required. The display shows this as a comma.

Note that the control unit uses the numbers in the Phone Book when a user starts a call to Downloader from the User Menu.

IP Network

It is possible for Downloader to communicate with the control unit over an IP network. This menu allows you to store two IP addresses that the control unit can use to connect to a PC running Downloader. The user starts the call by selecting one of the IP address through the User menu.

IP Address

This option presents two sub-menus where you can key primary and secondary IP Addresses used by Downloader. Press "*" to key in the dot.

IP Port Number

This option also presents another two sub-options where you can key in the port numbers that Downloader "listens" to on the remote PC for the primary and secondary IP addresses.

Secure Callback

Select this option to allow Downloader to use a third callback number (independent of the telephone numbers in the *Downloading – Phone Book* option). Before making a Downloader connection, the remote PC operator keys in the third callback number. Once connected, Downloader transmits the number to the control unit. The control unit then uses that number to call back to the remote PC.

Modem Baud Rate

(This option is not present when an i-gsm02 module is fitted.) Over some noisy telephone lines Downloader communicates more effectively using a slower Baud rate from the control unit. Select *Modem Baud Rate* to change the baud rate to 300 baud.

Remote Servicing

The options available under *Remote Servicing* are for use with the Remote Servicing feature on Downloader.

Enable Service

Enabling remote servicing allows the control unit to initiate connections to a remote service PC.

Serv. On Exit Eng

When enabled, the control unit will automatically initiate a connection to the remote service PC when you exit the Installer menu.

Service Call Num

Determines which of the two telephone number specified by *Phone Book*, or which of the two IP address specified by *IP Network* to use to connect to the remote PC.

Time Window Start

This specifies the time that the panel starts to initiate a connection to the remote service PC.

If connection is not achieved, the panel continues to retry every 15 minutes between *Time Window Start* and *Time Window End* for a maximum of 3 retries. If a successful connection is not achieved, the procedure is repeated every 24 hours for 5 days, then every 48 hours for a further 5 days, up to a maximum of 30 retries. If no successful connection is achieved, the keypad displays a “remote service fail” message at the end of the retry sequence.

A manual remote service can be carried out to clear the retry sequence and keypad message.

Time Window End

This specifies the time that the panel will no longer attempt to initiate a connection to the remote service PC.

Next Service Date

Use this option to specify the date of the next service. (Although you can also specify a time, this is automatically adjusted to be the time specified by *Time Window Start*.)

Service Interval

The number of days between each remote service.

Start Service Call

Select:

- Remote Service – To start an immediate remote service. The control unit connects to Downloader and uploads the current configuration. Downloader then generates a Remote Service Report and disconnects.
- Connect Only – To make a connection to Downloader only.
- Upload – To connect to Downloader and upload the current configuration. Downloader then disconnects.

Chapter 11: Test Menu

Sirens and Sounders

This option allows you to test all the warning devices connected to the control unit. For most options, you can choose to operate all warning devices assigned to a specific partition, or all warning devices of the type selected.

Press ▶ to turn the device on. Press ▶ to turn the device off. The display shows On when the device should be operating and Off when the evice should be silent.

Ext. Radio Sirens

This option presents a list of the learned-in radio sirens. Select a siren for testing by pressing ▲ or ▼. Note that both siren and strobe should operate.

Wired Sirens

This option allows you to operate all outputs of type Siren and Strobe.
Loudspeakers

You can use this option to test any loudspeakers connected to the system.

Wired Keypads

Use this option to test the sounders on the wired keypads.

KEY-RKPZ

Tests the sounders in KEY-RKPZ two-way radio keypads.

Internal Sounders

Tests any internal sounders (SDR-RINT) that the control unit has learned.

Wired Keypad

Use this menu option to test the keypad you are currently working on (you cannot test a keypad remotely).

When you start the test, the bottom line of the display shows the keypad name and bus address. All four ABCD LEDs should glow. The LEDs around the navigation should all glow red. Every time you press a navigation key, the LEDs change colour. Press all the keys one by one. The display should show you the key you pressed.

To test the HUA keys, press them both at the same time. **Note:** An HUA alarm is not generated, since you are in the Installer menu.

Press ✘ to leave the test.

Radio Keypads

This option allows you to test the keys on i-rk01 and KEY-RKPZ radio keypads, as follows:

i-rk01

a) Press the A, B, C, D and Unset keys one after the other (wait two to three seconds between each press to allow the keypad to transmit each message). The transmit LED should flash for each key press. The display of the wired keypad from which you started the test should show the appropriate letters.

b) Press both keys of the two-button HUA. The wired keypad display shows “Hold Up Alarm Key”.

c) Press the Unset key. The wired keypad display shows “System Unset Key”.

d) Test all the numeric keys four at a time (six at a time if using six-digit codes) remembering to press A after each group of four (or six). For example, if you press “4567A” the wired keypad display should show “4567A”.

Note: You cannot test the “*” and “**#**” keys on an i-rk01 radio keypad.

KEY-RKPZ

This test behaves the same as for a wired keypad.

Expanders

The Expanders menu allows you to test individual expanders.

Radio and wired expanders

12V Input Voltage

> This option shows the voltage on the 12V line in the bus cable, at the connection to the expander.

Spare Zones

> This option shows the number of zones of type Not Used on the expander.

Load Current

> This option (wired expanders only) shows the current being drawn by from the 12V Aux connections on the expander. Note that the reading is in mA.

EXP-PSUs

Spare Zones

> This option shows the number of zones of type Not Used on the expander.

System Voltage

> This option displays the dc voltage present on the expander PCB just after the mains transformer and principal voltage regulator. If it shows anything other than 13.6V, this indicates that there may be either a mains fail or that the expander is running on its standby battery.

Aux 1 Voltage

> This option shows the voltage on the 12V line of the Aux 1 terminals.

Aux 2 Voltage

> This option shows the voltage on the 12V line of the Aux 2 terminals.

Comms O/P voltage

This option shows the voltage on the 12V positive terminal of the plug-by communications connector.

Bus Voltage

This option shows the voltage on the 12V line of the system bus going out of the expander.

Load Current

This shows the total current drawn by Aux 1, Aux 2, Comms O/P 12V supply, and the bus out 12V supply.

Mains Condition

This option shows the condition of the mains power at the expander. It shows "Healthy" when mains is present or "Missing" when mains is absent.

Battery 1 Status

This option shows the condition of battery 1. "Health" means battery present, in good condition and charged. "Low" mean battery present but discharged. "Missing" means battery is not connected.

Battery 2 Status

This option will be present if you have an EXP-PSU connected to the system and have enabled its battery 2 in *Detectors/Devices – Wired Expanders – Edit Expanders* (see page 53). The option shows "Healthy", "Low" and "Missing" with the same meanings as in Battery 1 Status.

Walk Test

The walk test menu provides several different ways of organising a walk test.

When you select a *Walk Test* option (apart from *Chime*), the display shows the first item in a list of the detectors available for test. Walk around the area you wish to test and trigger each detector. If *Chime* is set to "Yes", every time you trigger a detector the keypads and loudspeakers give confirmation tone. The bottom-right corner of the display shows an "A" if you trigger the Alarm input and a "T" if you trigger the Tamper.

Note that if a zone has the Masking attribute enabled and the device is masked during the walk test then the keypad display will also show a "T".

The top of the display shows the number of zones left to test. The control unit decreases the number of zones every time you trigger an individual Alarm input.

The bottom line of the display shows the zone name. To see the zone number press ◀ or ▶.

Press ✔ to end the test.

Note: Use *Walk Test* to test wired HUA switches. While you are using the Installer menu, activating a wired HUA switch will not cause a HUA alarm.

If you wish to see which zones have not yet been tested, press the menu key. The bottom line of the display will show the first in a list of those zones remaining to test. As you test each zone, it will disappear from the display. Press the menu key again to return to the full list of zones.

Chime

Use this option to select Once, On or Off. Once causes keypads and loudspeakers to chime only once for each zone that is triggered during the walk test. On generates a chime every time a zone is triggered. Off switches off chiming.

System

This option allows you to walk round the entire system and test all the zones.

Partitions

Use this option to select one or more partitions, and test the zones only within those partitions.

Use ▲ or ▼ to scroll up and down the list of partitions. Press ◄ or ► to display "Yes" at the end of the bottom line to mark the partition as one you want to test.

Expanders

Use this option to select an individual expander, and test the zones belonging to just that expander.

Zones

This option lets you select one or more individual zones, and test only those zones and no others.

Use ▲ or ▼ to scroll up and down the list of zones. Press ◄ or ► to display "Yes" at the end of the bottom line to mark the zone as one you want to test.

Zone Resistances

When you select Zone Resistance, the display shows the first of the available wired detectors. Press ▲ or ▼ to see the other detectors in the list.

The bottom line of the display shows the zone name. To see the zone number press ◄ or ►.

The end of the bottom line shows the resistance of the zone. For 4-wire CC zones, the display alternates between the Alarm resistance ("A") and the Tamper resistance ("T").

"O/C" means Open Circuit.
"0k00" means zero resistance or closed circuit.

Signal Strengths

This option allows you check the received signal strength from all the radio transmitters belonging to the system.

The keypad display shows first: the strength of the most recent signal it has received from a transmitter, and second: (in brackets) the minimum strength signal it has received from the transmitter since the records were last reset. The control unit is always recording signal strengths, whether or not you are using the Signal Strength menu.

Note: If you have fitted a WAM to act as a repeater for weak detector signals, you will not see any change in the signal strength reported for those detectors. However, you should note the signal strength of the WAM, since that device is now passing on the information from the detectors whose signal you are trying to amplify.

To reset the signal strength records press "D" while you are in the *Tests – Signal Strengths* menu. When you press "D" then the control unit resets the signal strength records for ALL transmitters.

You can also reset the signal strength record of individual transmitters. To do this press "#" while the display shows the signal strength of the transmitter you wish to reset.

Detectors

The display shows the strength of the most recently received signal from each learned radio zone. The bottom line of the display shows the zone name. To see the zone number press ◄ or ►.

Radio Keypads

The display shows a list of the received signal strengths from each radio keypad.

A minimum reading of 2 is acceptable. (When reading from the web interface or other software, a minimum reading of 4 is needed if the control unit is in User mode, or 2 if it is in Installer mode.)

External Sirens

The display shows a list of the received signal strengths from each radio siren.

WAMs

The display shows a list of the received signal strengths from each learned WAM.

Internal Sounders

The display shows a list of the received signal strengths from each internal radio sounder.

Outputs

Radio/Wired/Plug-by/Expander Outputs

Select the device type (such as *Radio Outputs*), then ▲ or ▼ to select the output you wish to test, followed by ► to activate the output. Press ► again to deactivate the output. Press ✔ to finish the test.

Note: If you have programmed one of the plug-by outputs as an ATS Test output, then when you test that output, the control unit will pulse the output active for the correct length of time to start a call in any connected dual-signalling communicator. You do not need to deactivate the output (This test applies to the UK only, and is compliant with Form 175).

When you complete testing the outputs, check that they are in the state you wish to leave them in.

Comms Channels

This option is available if the control unit is reporting to an ARC using Fast Format.

If you select this option, the bottom line of the keypad display will show you the first in a list of the Fast Format comms channels available. Press ▲ or ▼ to see the other entries in the list. For each channel that you wish to test, press ► to turn the channel "On". Once you have selected all the channels to be tested, press ✔. The control unit will then dial the ARC and communicate the selected channels.

During the call you should see the following progress messages on the display:

"Dialling" then "Connected" followed by "Call Successful". If the call does not succeed then the final message will be "Call Failed".

Remotes

This allows you to test user's remote control. The keypad display shows a message prompting you to press any button on the remote you wish to test.

Press one of the remote's buttons. The top line of the keypad display shows the remote's identity, the button you pressed and the remote's owner. When testing a FOB-2W-4B, the display identifies the buttons with a letter: "S" = Set, "U" = Unset, "?" = Query, and "*" = Part Set (or programmable).

The bottom line of the display shows the action assigned to that button and the signal strength. If the bottom line shows ">", press ▶ for more information.

Press all the other buttons on the remote to test them in the same way.

User Hold Up Alarms

This allows you to test user's HUA transmitters. You must have the HUA transmitter to carry out the test.

The keypad display shows a message prompting you to press the HUA buttons.

Press the HUA buttons, both at the same time. (The alarm system will not start a HUA alarm as a result.)

The keypad display shows the HUA's owner. The bottom line of the display shows the signal strength.

Prox Tags

This allows you to test a user's proximity tag.

The keypad display shows a message asking you to present the tag to the keypad.

Hold the prox tag up to the keypad.

The keypad display shows the user number and name of the prox tag owner.

ARC Reporting

This allows you to send a test call to either of the two telephone numbers you have programmed to receive alarm information. The control unit must have a suitable communications module fitted. ARC reporting must be enabled (see page 102).

From *ARC Reporting*, select *Tel No 01* or *Tel No 02*.

If the control unit uses SIA or CID reporting, the test starts when you press ✔. Press ✘ to abandon the test call.

If the control unit uses Fast Format reporting, then when you press ✔, the keypad displays the first in a list of the available Fast Format channels. Press ▲ or ▼ to scroll up or down the list. Press ◀ or ▶ to select a channel for testing. Press ✔ to start the test call. The control unit sends a "T" (Test message) and the channel(s) you selected. If you do not select any channels, the control unit sends a "T" by itself.

During the test call, the keypad display will show a sequence of progress messages.

If the call fails, the keypad display will show a brief message giving the reason for failure.

Speech Dialler

This option allows you to send a test speech call to any telephone number (not just the ones programmed to receive speech messages in the event of an alarm).

The option appears only if the control unit is fitted with a plug-on module that provides speech dialling.

The keypad display shows a message prompting you to key in a telephone number. Enter the telephone number of the phone that you wish to receive the test message, then press ✔.

When you press ✔,the control unit starts the test call. The keypad displays “Dialling...”.

When the person at the receiving end answers the call, the display shows “Connected...”.

The control unit will play the home message, followed by each of the four alarm messages, and then repeat all five messages three more times. While the control unit is playing the messages, the keypad displays “Playing messages...”.

The person receiving the messages call acknowledge (and end) the call by pressing “5” or “9” on their phone keypad.

If no-one acknowledges a test call, the keypad displays “No acknowledgement”.

SMS

This option appears only if the control unit is fitted with a plug-on module that provides PSTN or GSM communications.

You can use the option to send a test call to any telephone number (not just the ones you have set up to receive SMS alarm/event reports).

Email

You can use the option to send a test email to any email address (not just the ones you have set up to receive email alarm/event reports).

PSU Current

This option allows you to check how much current the control unit is consuming. The bottom line of the keypad display shows the current delivered by the PSU in the control unit.

If the alarm system has an EXP-PSU connected, this menu also lets you check the current used by the EXP-PSU itself.

Locate Bus Device

This option allows you to list all the devices connected to the bus, and to find out where they are located by activating their internal sounders.

The control unit presents the first item in a list of all the devices connected to the bus. The keypad display shows the expander bus number, and any name that has been programmed for it.

Press ▶ to turn on the device’s sounder (press ◀ or ▶ to turn it off again). You can also silence the sound by opening the case of the device (activating the tamper switch).

Chapter 12: View Log Menu

The control unit keeps a log of events (for example, alarms and times of setting/unsetting). An installer or master user can read the log when the system is completely unset. Note that no other user type can read the log.

Mandatory and Non-Mandatory Log Events

To comply with EN50131-1:2006 for Grade 2, the log is divided internally into two portions: mandatory events and non-mandatory events. The installer can view either of these lists separately, or see all log events in one list. Please refer to Appendix C on page 138 for a description of each log message.

Mandatory events are those that are recorded to comply with EN 50131. Non-mandatory events are other events not needed to comply with EN 50131.

The number of events each area of the log can store is given in Table 1 on page 2.

The entire log stores its records for at least 10 years without power.

The first three events of the same type (e.g. tamper alarms) that occur in the same unset or set period are logged in the mandatory log. Any further events of that type are logged in the non-mandatory log.

How the Log Displays User Identities

When you view the log, the display initially shows users by their number (for example User001). Pressing ▶ displays any name programmed for the user.

There are some user numbers that have special meaning; see the table below, which assumes a system that has 50 users.

User 000	Installer – displayed whenever an installer carries out an action.
User 001	Master User - displayed whenever a Master User carries out an action.
User 002-050	A User created by the Master User - displayed whenever a User carries out an action.
User 051	Quick set – displayed when the A,B,C & D keys are used to quick set.
User 052	Level 4 – used for remote firmware updates.
User 053	Control Panel action – displayed when the panel has carried out an action.
User 054	Keyswitch - displayed when a keyswitch zones is used to set/unset.
User 055	ARC remote reset – displayed when a 3rd party communicator applies a remote reset.
User 056	Downloader – displayed when the downloader carries out an

	action.
User 057	Virtual Keypad - displayed when the Virtual Keypad carries out an action.
User 060	SMS control - displayed when the SMS control carries out an action.
User 061	App control - displayed when the App carries out an action.

Note: The word “Web” appears in the log entry if the installer logged on using the web browser.

Downloader and the Log

When Downloader connects to a control unit, the control unit logs the event as “Rem Download”. This indicates that Downloader successfully connected and disconnected.

The control unit logs a separate event “Unn Config Change” if Downloader changes the configuration of the control unit. The user number recorded will be that for the Downloader (see table above).

Logging Tamper Events

Tamper events are normally logged. However please note that the type of events that are considered to be tampers depends to some extent on the options the Installer chooses in *System Options – Jamming* and *System Options – Supervision* (see page 95). When these options are set to “Tamper” then jamming or supervision failure events will be recorded as tampers.

Logging Software Updates

The control unit logs the software version every time the system starts up from zero power. To see the software version press ▶ or ◀ when the keypad displays the log message “System Startup”.

Chapter 13: About Menu

The *About* menu offers information on the version and status of the control unit and information about any modules fitted.

Panel

This option shows:

- The control unit model.
- The control unit's software revision.
- Whether the control unit is programmed as partition or part setting.
- The installed languages and their versions.

Press ▲ or ▼ to see each item of information.

Expanders

This option shows the first item in list of all the expanders known to the control unit. If you select an expander by scrolling up or down the list and then press ✔, the display shows the revision of software running on the expander.

Keypads

This option shows the first item in a list of the keypads known to the control unit. If you select a keypad by scrolling up or down the list and then press ✔, the display shows the revision of software running on the keypad.

If you find that the *Keypad* option does not display an individual keypad's software version, you can check the keypad by **briefly** pressing the "A" and "✔" keys at the same time.

Comms

The contents of this option depend on the plug-on communications module fitted to the control unit. When no module is present, the *Panel Ethernet* option is the only one visible.

Panel Ethernet

This shows information about Internet Protocol (IP) settings used by the control unit itself. You will need this information when you set up an Ethernet connection from a PC to the control unit in order to use the built in web browser interface. To change the settings use the *Communications – IP Network (Own)* menu (see page 116).

IP Address

This is the IP address the control unit uses when linked by Ethernet to a PC.

IP Subnet Mask

This is the subnet mask currently in use by the control unit itself.

Gateway IP Address

This is the gateway address being used by the control unit.

DNS IP Address

This is the IP address of the DNS server used by the control unit.

MAC Address

This is the unique MAC address of the control unit PCB. Each control unit PCB will have an individual MAC address.

IP Link Status

This option shows the current status of the Ethernet link between a PC and the control unit. The display shows “Fail” when there is no link, and “OK” when the Ethernet link is established. Note that “OK” only shows that the link is established, it does not show that the PC is logged into the control unit.

Module

For a GSM module, this provides:

- Network – Network name and signal strength.
- IMEI – IMEI number of the SIM card in use.
- IMSI – International Mobile Subscribed Identity (IMSI) to identify the GSM subscriber.
- Version – The firmware version of the module.
- Reset – Resets the module.

For a PSTN module, this provides *PSTN Link Status*, which shows the current status of the PSTN connected to the control unit. The display shows “Fail” when there is no link, and “OK” when there is a PSTN line available. Note that “OK” only shows that the line is available; it does not show if a call is possible.

Zone Mapping

This option allows you to check which zones are currently allocated to detector connection points, or which detector connection points have zone numbers allocated.

Zone Numbers

This shows a list of zone numbers (with names), with detector connection points for each zone.

Zone Addresses

This shows a list of detector connection points, with zone numbers and names, where allocated. (For an explanation of zone numbers see page 26.)

Appendix A: ARC Communication Formats

Fast Format

Fast Format is the format most widely used in the UK. When using the Fast Format, each message transmitted to the ARC consists of the following:

A 4,5 or 6-digit account number.

8 channels of data. Each channel communicates the status of an output, as programmed using the ”Fast Format Channels” option (see page 103). The value of the channel can be:
1 = new alarm and not previously reported
2 = status of output is open/unset
3 = alarm restored and not previously reported
4 = status of output is closed/set
5 = not in alarm
6 = in alarm but previously reported

A test signal.

Contact ID

The Contact ID format transmits data from the event log to the Alarm Receiving Centre (ARC). Examples of messages in the Contact ID format are:

Example 1 - 1234 18 1137 01 015 2

1234 is the account number, as specified in Account Numbers option (page 103).

18 is the message type used to identify the message as Contact ID.

1137 is the event qualifier for a new event (1), followed by the event code for a system tamper alarm (137).

01 is the partition number.

015 is the zone number.

2 is the checksum value, which the ARC needs to verify to confirm a valid message has been received.

Example 2 - 1234 18 3137 01 015 3

The only difference between this and the first example, is the event qualifier of 3 to indicate a restore of a system tamper alarm, and the checksum value.

SIA 1, SIA 2, SIA 3 and Extended SIA 3

When using the SIA formats, the control unit transmits data from the event log to the ARC. The four SIA formats differ in the amount of data transmitted with each message:

Type	**Format**
SIA1:	#AAAAAA|NCCcc
SIA2:	#AAAAAA|Nidnnn/rinn/CCcc
SIA3:	#AAAAAA|Ntihh:mm/idnnn/rinn/CCcc #AAAAAA|AS
Extended SIA 3:	#AAAAAA|Ntihh:mm/idnnn/rinn/CCcc/AS

Where:

AAAAAA	6-digit programmable account code (e.g. 123456).
“N”	New Event (always N).
“ti”hh:mm/	time (e.g. ti10:23/).
“id”nnn/	user number, if applicable; otherwise not sent (e.g. id123/ or id6/).
“ri”nn/	partition no. (e.g. ri12/ or ri3).
CC	event code (e.g. FA = Fire Alarm).
cc	zone number, if applicable; otherwise not sent (e.g. 23 or 5).
“A”S	text description of event, usually the log event description.

(The control unit sends those characters shown between “ and “ above literally as they appear in the text.)

For example, if there is a fire alarm on zone 2 of partition 4 at 10:15 (partition 4 account number is 10), the message would be:

SIA1:	#000010|NFA2
SIA2:	#000010|N/ri4/FA2
SIA3:	#000010|Nti10:15/ri4/FA2 #000010|AFire Zone 2
Extended SIA3:	#000010|Nti10:15/ri4/FA2/AFire Zone 2

Extended SIA3 V2

Some versions of the software that works in SIA receivers do not always recognise the “/” text delimiter. This can cause problems with spurious “Mains Fail” messages appearing to the ARC when the control unit sets, unsets or goes into or out or installer mode.

In version 2 of Extended SIA3, the “/” delimiter has been replaced by a “|”. So, for example, the string: #000010|Nti10:15/ri4/FA2/AFire Zone 2

becomes: #000010|Nti10:15|ri4|FA2|AFire Zone 2

If you have experienced problems with spurious “Mains Fail” messages try using this Extended SIA3 V2 option.

Appendix B: System Maintenance

Inspections

The system should be inspected at least 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 tamper switch.
- Check, and if necessary, replace the standby battery.
- Check keypads and other devices for obvious signs of damage.
- Test the action of all buttons on all keypads.
- Clean the surface and display of each keypad using a clean, soft, dry cloth. Do not use water, solvents or any proprietary cleaning materials.
- Where applicable, check cabling for signs of damage or wear.
- Monitor the signal strength and battery condition of all detectors, radio keypads, remote controls, radio HUDs and radio sounders. Test each device. Replace batteries as recommended by the device 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.

Note: You can use *Test – Locate Bus Device* to find the location of a bus device (the device emits a continuous sound).

Replacing or removing devices

Note: Make sure that you remove all power from the system before physically disconnecting any device.

Removing a plug-on module

If you wish to remove a plug-on module, ensure that you disable communications first in the appropriate menus (such as in the *Communications – ARC Reporting*, *Communications – Speech Dialler* and *Communications – SMS* menus). Otherwise, the control unit will continually report a communications failure.

Removing a bus device permanently

Before physically disconnecting the device, enter the Installer menu, and use the appropriate *Delete* option. For example, to delete a keypad, use *Devices/Detectors – Wired Keypads – Delete Keypad*. This ensures that the system does not report a missing device and the device's internal address is erased (allowing it to be used on another system).

Replacing a bus device

Before physically disconnecting the device, enter the Installer menu, and use the appropriate *Replace* option. For example, to replace a keypad, use *Devices/Detectors – Wired Keypads – Replace Keypad*. The control unit disables the selected device, but retains the configuration of the old device (such as the zone configuration). You can then power down the system, disconnect the device from the bus, and reconnect a new device (of the same type) to the bus.

When you power up the control unit again, the keypads will show an alert that a device has been disabled. Select the appropriate *Replace option* again, select the *Add* option and then hold down the address request button on the new expander (with the tamper switch activated). The control unit will assign the bus device address of the expander you removed to the new expander, along with all the zones and other settings from the old expander. The new expander will not need any further configuration.

Note: If you replace a radio expander, you must teach the identity of the new radio expander to any receivers (such as 762s, 768s or WAMs) that had previously learned the old expander's identity.

Note: If you are replacing a keypad on a single-keypad system, you will have to re-program the new keypad with all the functions of the old keypad, including any non-default ABCD key functions.

Using LEDs for Bus Diagnostics

You may notice an LED on the PCB of a device flashing unusually. Please refer to the device's installation instructions for the meaning of each LED.

Appendix C: Log Messages

Introduction

This Appendix gives short explanations of the messages that can appear in the control unit's log.

Please note that many of the messages refer to specific devices by the bus and device number. Therefore, it is not possible to show in this list the exact log message that you may be seeing on any given installation.

The list itself is sorted alphabetically by the text of the message. In the column "Event Log Text" you will see "==" or sometimes "#". These characters stand in for the zone, user or device number that the control unit has recorded for the event being logged. In the "Description" column this is shown as "nn" or "n". In the first seven messages listed the characters "$m" stand in for the type of communications module fitted.

Log messages

Event Log Text	Description
$m Alarm Fail	Communicator failed to send alarm.
$m Email Fail	Control unit failed to send email.
$m Line Fault	Communications line failed.
$m Line Restore	Communications line restored.
$m Modem Fault	Modem failed.
$m Modem Restore	Modem restored.
$m SMS Fail	SMS call failed to get to destination.
$m Speech Fail	Speech dialler failed to send alarm.
== A/C Fail Flt	AC mains fail.
== A/C Fail Rst	AC mains restored.
== Aux Fuse Flt	Aux fuse failed.
== Aux Fuse Rst	Aux fuse restored.
== Aux1 O/P Flt	Auxiliary output 1 fault.
== Aux1 O/P Rst	Auxiliary output 1 fault restored.
== Aux2 O/P Flt	Auxiliary output 2 fault.
== Aux2 O/P Rst	Auxiliary output 2 fault restored.
== Batt 1 Rstr	Battery 1 restored.
== Batt 1 Rstr	Battery 1 missing restored.
== Batt 2 Rstr	Battery 2 restored.
== Batt 2 Rstr	Battery 2 missing restored.
== Bus O/P Flt	Bus dc power output fault.
== Bus O/P Rst	Bus dc power output restored.
== Chargr 1 Flt	Battery 1 charger fault.
== Chargr 1 Rst	Battery 1 charger fault restored.
== Chargr 2 Flt	Battery 2 charger fault.
== Chargr 2 Rst	Battery 2 charger fault restored.
== Coms O/P Flt	Plug-by comms output fault.
== Coms O/P Rst	Plug-by comms output fault restored.
== Ex Keys Rstr	Excess keys (code attempts) tamper restore
== Load 1 Fail	Battery 1 failed load test.
== Load 1 OK	Battery 1 passed load test.
== Load 2 Fail	Battery 2 failed load test.
== Load 2 OK	Battery 2 passed load test.
== Low Batt 1	Battery 1 low.
== Low Batt 2	Battery 2 low.
== Low Voltage	PSU reports low voltage.
== Miss Batt 1	Battery 1 missing.
== Miss Batt 2	Battery 2 missing.
== RF OK	Radio signal restored for device nn
== RF Warning	Radio signal lost for 20 min for device nn
== Superv Fail	Radio signal fail for 2 hours for device nn
== Superv Rstr	Radio signal restored for device nn
== Sys Volt Flt	System voltage fault.
== Sys Volt Rst	System voltage fault restored.
== Voltage OK	Voltage OK.
24hr Z=== Alarm	24 hour alarm on zone n.
24hr Z=== Restore	24 hour alarm on zone n restored.
4K4 Fault Z==	Fault resistor active on zone nn
4K4 Rstr Z==	Fault resistor restored on zone nn
A/C Fail Ptn ##	A zone of type "AC Fail" was triggered in the specified partition.
A/C Fail	AC mains failed and was communicated.
A/C Restore	AC mains was restored.
A/C Rstr Ptn ##	A zone of type "AC Fail" was restored in the specified partition.
Al. Conf ==RKBS	Confirmed alarm with tamper on nn radio keypad base station.
Alarm Abort U--	Alarm aborted by user.
Alarm Conf ==ER	Alarm has been confirmed by a missing external prox reader on keypad nn.
Alarm Conf ==IS	Confirmed alarm with tamper on nn Internal Radio Sounder.
Alarm Conf Aux #	Confirmed alarm with tamper on Aux nn.
Alarm Conf Bell #	Confirmed alarm with tamper on Bell nn.
Alarm Conf SMS	Confirmed alarm with SMS Control user code tamper.
Alarm Conf Websvr	An alarm was confirmed by a user on the web browser interface typing the password incorrectly more than four times in a row,
Alarm Conf. ==	Confirmed alarm with tamper on keypad.

Alarm Conf. ==	Confirmed alarm with tamper on expander.
Alarm Conf. VKP	Confirmed alarm with tamper on virtual keypad.
Alarm Confirm RK==	Confirmed alarm with tamper on radio keypad.
Alarm Confirm Z==	Confirmed alarm on zone.
Alarm Confirm	Confirmed alarm.
Alarm Test Call	Periodic alarm test call made.
Alarm Test Call	Manual alarm test call made.
All Comms Pths Flt	All communications paths have a fault.
All Comms Pths Rst	All communications path faults restored.
Alm Conf Bus# Tamp	An alarm was confirmed by a bus tamper.
Alm Conf Panel Jam	Alarm confirmed by panel jamming.
Alm Conf Panel Lid	Confirmed alarm with tamper on control unit lid.
Alm Confirm SRN==	Confirmed alarm with tamper on radio siren n.
Alm Confirm WAM==	Confirmed alarm with tamper on WAM n.
AS defer U-- P#	User nn defered calendar setting on partition n.
ATE L.F. All	All lines to alarm transmission equipment failed.
ATE L.F. Restore	Line to alarm transmission equipment restored.
ATE L.F. Single	Alarm transmission equipment has a single line fault.
Auto Part Set #	The system was part set by calendar setting.
Auto Ptn # PtSet	Partition n was part set by calendar setting.
Auto Ptn # Set	Partition n set by calendar setting.
Auto Ptn # Unset	Partition n unset by calendar setting.
Auto System Set	The system was full set by calendar setting.
Auto System Unset	The system was unset by calendar setting.
Autoset defer U--	User defered calendar setting of system.
Autoset Fail P#	Calendar setting of partition failed.
Autoset Fail	Calendar setting of system failed.
Aux # Tamper Rstr	Aux Tamper terminals on main pcb closed circuit
Aux # Tamper	Aux Tamper terminals on main pcb open circuit
Aux. 14V4 # Fail	Control unit 14.4V supply failed.
Aux. 14V4 # Rstr	Control unit 14.4V supply restored.
Auxiliary 12V Fail	Control unit 12V Aux DC not working.
Auxiliary 12V Rstr	Control unit 12V Aux DC restored.
Bad checksum	There is an error on loading the control unit with its software.
Batt = Fault Rst	Control unit battery restored.
Batt = Load Fail	Control unit battery failed load test.
Batt = Low/Missing	Control unit battery missing or low.
Batt= Charger Fail	Control unit battery charger failed.
Batt= Charger Rstr	Control unit battery charger working again.
Battery Load OK	Control unit battery passed load test.
Bell # 12V Fail	12V DC supply to bell failed.
Bell # 12V Restore	12V DC supply to bell restored.
Bell # Tamper Rstr	External wired siren tamper restored.
Bell # Tamper	External wired siren tamper.
Burg Z== Alarm	Burglar alarm on zone n.
Burg Z== Restore	Burglar alarm on zone n restored.
Bus # 12V Fail	12V DC supply to Bus nn failed.
Bus # 12V Restore	12V DC supply to Bus nn restored.
Bus # Tamper Rstr	Bus n has been restored.
Bus # Tamper	Bus n has been tampered (for example wires cut or disconnected)
Codes Defaulted	All access codes were returned to factory defaults.
Comms 12V Fail	DC power to comms module failed.
Comms 12V Restore	DC power to comms module restored.
Configuration Fail	The current configuration is not compatible with the software revision level of the control unit.
Defaults Loaded	The control unit was returned to factory defaults.
Disabled ==	Expander/Keypad disabled.
Downloader Lockout	Downloader locked out for 30 mins due to 10 consecutive authentication errors.
Dup. == Restore	Duplicate bus device nn restored.
Duplicate ==	Duplicate bus device nn detected.
Email error ---	See "Email error messages" on page 142.
Email Test Call	Email test call initiated by Installer.
Enabled ==	Expander/Keypad enabled.
Entry Started Z==	Entry started by zone n.
Entry Stray Z==	Stray on entry alarm at zone n.
Exit Mode Changed	Local setting mode applied (from Remote set).
Exp. == deleted	Expander n deleted from bus.
Expndr == added	Expander n added to bus.
Expndr == found	New expander n found on bus.
Ext A/C Fail Z==	Zone n with type AC Fail activated.
Ext A/C Rstr Z==	Zone n with type AC Fail restored.
Ext Batt Fault Z==	Zone n with type Batt Fault activated.
Ext Batt Rstr Z==	Zone n with type Batt Fault restored.
Ext Low Volts Z==	Zone n with type Low Volts activated.
Ext PSU Fault Z==	Zone n with type Fault activated.
Ext PSU Rstr Z==	Zone n with type Fault restored.
Ext Volts Rstr Z==	Zone n with type Low Volts restored.
Ext WD Fault Z===	A warning device has reported a fault through zone n.
Ext WD Restr Z===	The fault reported through zone nn by a warning device has been restored.
Fire == Alarm	Fire alarm at keypad.
Fire Reset	User reset system after fire alarm.
Fire Restore	Fire alarm at keypad restored.
Fire Restore	Fire alarm restored from radio keypad.
Fire Z== Alarm	Fire alarm on zone n.
Fire Z== Restore	Fire alarm on zone n restored.
GSM CME Info --	The GSM plu-on module has a problem.
GSM CMS Info --	The GSM plu-on module has a problem.
HUA Cnf RF HD U---	Hold Up Alarm confirmed by radio HUD belonging to user nn.
HUA Cnf RF MD U---	Hold Up Alarm confirmed by radio Man Down transmitter belonging to user nn.
HUA Conf ==RKBS	Hold Up Alarm confirmed by a tamper on RKBS n.
HUA Conf Bus# Tamp	Hold Up Alarm by a bus tamper.
HUA Conf HD ==	Hold Up Alarm confirmed on keypad HUA keys.
HUA Conf HD RK==	Hold Up Alarm confirmed on radio keypad HUA keys.
HUA Conf Panel Jam	Hold up alarm confirmed by panel jamming.
HUA Conf Panel Lid	Hold Up Alarm confirmed by panel lid tamper.

HUA Conf. ==	Hold Up Alarm confirmed by tamper on expander n.
HUA Conf. ==ER	Hold Up Alarm has been confirmed by a missing external prox reader on keypad n.
HUA Conf. ==IS	Hold Up Alarm confirmed by a tamper on internal radio sounder n.
HUA Confirm ==	Hold Up Alarm confirmed on keypad HUA keys.
HUA Confirm Aux #	Hold Up Alarm confirmed by open circuit on AUX Tamp terminals on control unit PCB.
HUA Confirm Bell #	Hold Up Alarm confirmed by open circuit on TR terminal on control unit PCB.
HUA Confirm RK==	Hold Up Alarm confirmed by tamper on radio keypad.
HUA Confirm SMS	Hold Up Alarm confirmed by SMS Control user code tamper.
HUA Confirm SRN==	Hold Up Alarm confirmed by radio siren n tamper.
HUA Confirm VKP	Hold Up Alarm confirmed by VKP user code tamper.
HUA Confirm WAM==	Hold Up Alarm confirmed by tamper on WAM n.
HUA Confirm Websvr	A Hold Up Alarm was confirmed by a user on the web browser interface typing the password incorrectly more than four times in a row,
HUA Confirm Z===	Hold Up Alarm confirmed on wired zone nn.
HUA Confirm	Hold Up Alarm confirmed on device...
HUA Restore P#	Hold Up Alarm button has been restored.
HUA Restore P#	Hold Up Alarm has been restored.
HUA Restore	Hold Up Alarm has been restored
HUA U-- Alarm	Hold Up Alarm confirmed on User radio device n.
HUA U-- Low Batt	Low battery on User radio device n.
HUD Fault Rst Z===	A hold up device fault reported on zone n was restored.
HUD Fault Z===	A hold up device reported a fault on zone n.
IP Cam # Err 404	HTTP error 404 from IP camera.
IP Cam # Err Auth	Login details to IP camera incorrect.
IP Cam # HTTP Err.	HTTP error at IP camera.
IP Cam # Miss Rstr	Connection to IP cam n restored.
IP Cam # Timeout	Connection to IP cam n lost.
IP device connected	IP network device connected.
IP device disc.	IP network device disconnected.
IP Polling Fault	An Ethernet or other plug-on module is having a problem.
IP Polling Restore	The problem with the Ethernet or other plug-on module has been restored.
ISN== Battery Rstr	Low battery Restored on Internal Radio Sounder n.
ISN== Fault Rstr	Fault restored on Internal Radio Sounder n.
ISN== Fault	Fault on Internal Radio Sounder n.
ISN== Jamming Rstr	Jamming Restored on Internal Radio Sounder n.
ISN== Jamming	Jamming on Internal Radio Sounder n.
ISN== Low Battery	Low battery on Internal Radio Sounder n.
ISN== RF OK	Radio signal restored for Internal Radio Sounder nn
ISN== RF Warning	Radio signal lost for 20 min for Internal Radio Sounder nn
ISN== Superv Fail	Radio signal fail for 2 hours for Internal Radio Sounder nn
ISN== Superv Rstr	Radio signal restored for Internal Radio Sounder nn
ISN== Tamper Rstr	Tamper Restore on Internal Radio Sounder n.
ISN== Tamper	Tamper on Internal Radio Sounder n.
Jamming == Rstr	Jamming ceased.
Jamming ==	Jamming detected.
K== Excess Keys	Excess keys tamper at keypad n.
Key Sw Ptn # PtSet	Partition part set from keyswitch.
Key Sw Ptn # Set	Partition set from keyswitch.
Key Sw Ptn # Unset	Partition unset from keyswitch.
Key Sw System PtSet	System part set from keyswitch.
Key Sw System Set	System set from keyswitch.
Key Sw System Unset	System unset from keyswitch.
Keypad == added	New keypad added to system.
Keypad == found	New keypad found on bus.
Kpd == deleted	Keypad deleted from system.
Kpd == Jamming	Radio jamming detected at radio keypad n.
Kpd == JammingR	Radio jamming removed at radio keypad n.
Kpd == Low Batt	Low battery voltage at radio keypad n.
Lid Tamper Restore	Control unit lid closed.
Lockset Z=== Set	A zone with type "lock set" was closed. (If Inverted attribute is set to "normal".)
Lockset Z=== Unset	A zone with type "lock set" was opened. (If Inverted attribute is set to "normal".)
Low Batt = Restore	Control unit battery no longer low.
Low Batt Z== Rstr	Radio detector at zone has low battery restored.
Low Battery =	Control unit battery low.
Low Battery Z==	Radio detector at zone has low battery.
Mask Flt Z==	Masking detected on zone while partition unset?
Mask Rstr Z==	Masking restored on zone.
Mask Z==	Masking detected on zone while partition set.
Missing == Rstr	Missing expander restored to bus.
Missing ==	Expander missing from bus.
Missing ==ER Rs	An External prox Reader connected to keypad nn has been re-connected.
Missing ==ER	An External prox Reader connected to keypad nn has gone missing (possibly disconnected from the keypad).
Occupancy Set W#	Set but with Occupancy zone(s) open.
Panel A/C Fail	AC power failure at control unit.
Panel A/C Restore	AC power restored at control unit.
Override	User overrode set fail in part setting system.
PA U-- Low Bat	Hold up Device belonging to user has a low battery.
Panel lid open	Control unit lid open.
Panic == Alarm	Not used.
Panic Alrm Rst P#	Not used.
Panic Z== Alarm	Not used.
Panic Z== Restore	Not used.
Partn # Rearmed	Partition n was rearmed after an alarm by control unit.
Pend U-- Low Bat	Not used.
Pri Comms Path Flt	Primary communications path has a fault.
Pri Comms Path Rst	Primary communications path fault restored.
PRM Z=== Active	Perimeter zone n active.
PRM Z=== Restore	Perimeter zone n restored.
Ptn # Remote Rst	User reset partition remotely.
Remote Reset	User reset system remotely.

Remote U-- Low Bat	Remote control belonging to user has low battery.
Remsvc Comms Fail	A remote service call failed all attempts.
Remsvc Complete	A remote service call succeeded.
RF Failure Restore	Radio restored.
RF Failure	Radio failed.
RF Jamming Restore	Radio jamming removed.
RF Jamming	Radio jamming detected.
RK == HUA	Hold Up Alarm raised at radio keypad n.
RK== 4/6 Mismatch	Incorrect code length entered at 1-way radio keypad.
RK== Ex Keys Rstr	The system was restored after a user keyed in the wrong code more than four times in a row at radio keypad n.
RK== Excess Keys	Radio keypad n has been tampered by excess key presses.
RK== Fire	Not used.
RK== Low Battery	Radio keypad n has low battery.
RK== RF OK	Radio keypad n supervision OK.
RK== RF Warning	Radio keypad n about to fail supervision.
RK== Superv Fail	Radio keypad n failed supervision.
RK== Superv Rstr	Radio keypad n supervision restored.
RK== Tamper Rstr	Tamper on radio keypad n restored.
RK== Tamper	Tamper on radio keypad n.
RKBS Jam (==)	Radio jamming detected at radio keypad base station n.
RKBS Jam Rs(==)	Radio jamming removed at radio keypad base station n.
RKBS L V Rs(==)	Low voltage restored at radio keypad base station n
RKBS Low V (==)	Low voltage at radio keypad base station n
RKBS Tamp (==)	Tamper at radio keypad base station n.
RKBS Tmp Rs(==)	Tamper restored at radio keypad base station n.
RSN== Battery Rstr	Low battery Restored on Internal Radio Sounder n.
RSN== Fault Rstr	Fault restored on External Radio Siren n.
RSN== Fault	Fault on External Radio Siren n.
RSN== Jamming Rstr	Jamming Restored on External Radio Siren n.
RSN== Jamming	Jamming on External Radio Siren n.
RSN== Low Battery	Low battery on External Radio Siren n.
RSN== RF OK	Radio signal restored for External Radio Siren nn.
RSN== RF Warning	Radio signal lost for 20 min for External Radio Siren nn.
RSN== Superv Fail	Radio signal fail for 2 hours for External Radio Siren nn.
RSN== Superv Rstr	Radio signal restored for External Radio Siren nn.
RSN== Tamper Rstr	Tamper Restore on External Radio Siren n.
RSN== Tamper	Tamper on External Radio Siren n.
SD Card Error --	Error with SD card.
SD Card Missing	SD card missing.
SD Card Present	SD card present.
Sec Comms Path Flt	Secondary communications path has a fault.
Sec Comms Path Rst	Secondary communications path fault restored.
Set Fail Z==	Setting failed at zone.
Set Z=== Shunted	The system was set with zone nn shunted
Shunt Group ## OFF	User nn de-activated shunt group n.
Shunt Group ## ON	User nn activated shunt group n.
SMS Ex Keys Rstr	Excess keys tamper from SMS message restored.
SMS Excess Keys	Excess keys (code attempts) tamper from SMS message.
SMS Test Call	SMS test call made.
Soak Fail Z== Alm	Zone on soak test failed.
Soak Fail Z== Tmp	Zone on soak test tampered.
Software Changed	The installer has loaded a different version of the control unit's operating software.
Spch Tel = Ack All	All speech dialler destinations acknowledged calls.
Spch Tel = No Ack	Speech dialler destination did not acknowledge call.
Speech Tel = Ack	Speech dialler destination acknowledged call.
Speech Test Call	Speech dialler made test call.
SRN== Battery Rstr	External radio siren n low battery restored.
SRN== Fault	External radio siren n has a fault.
SRN== Fault Rstr	External radio siren n fault restored.
SRN== Jamming	External radio siren n jammed.
SRN== Jamming Rstr	External radio siren n jamming restored.
SRN== Low Battery	External radio siren n has low battery.
SRN== RF OK	Radio siren n supervision OK.
SRN== RF Warning	Radio n siren about to fail supervision.
SRN== Superv Fail	External radio siren n failed supervision.
SRN== Superv Rstr	External radio siren n supervision restored.
SRN== Tamper	External radio siren n tampered.
SRN== Tamper Rstr	External radio siren n tamper restored.
Superv'n Fail Z==	Supervision failed for radio detector at zone.
Superv'n Rstr Z==	Supervision restored for radio detector at zone.
System 12V Fail	Control unit 12V supply failed.
System 12V Restore	Control unit 12V supply restored.
System Error	Control unit has fault in main processor.
System Rearmed	User rearmed the system.
System Startup	The system restarted after a power fail (mains and battery).
System Tamper Rstr	System tamper restored.
System Tamper	System tamper.
Tamper == Rstr	Tamper at expander\keypad restored.
Tamper ==	Tamper at expander\keypad.
Tamper ==ER Rst	Tamper at external reader n restored.
Tamper ==ER	Tamper at external reader n.
Tamper Z== Restore	Zone tamper restored.
Tamper Z==	Zone tamper.
Tech Z== Alarm	Technical alarm on zone.
Tech Z== Restore	Technical alarm on zone restored.
Test Call Fail	Test call failed.
Test Call OK	Test call succeeded.
Trace ==	Not used.
U-- Change U==	User nn changed their password.
U-- Config Change	User nn changed programming configuration.
U-- Delete U==	User nn deleted another User nn from system.
U-- Download Fail	Downloader session failed.
U--- Duress Restr	User nn keyed in a Duress code to unset the system (part setting system).
U--- Duress	User nn keyed in a Duress code to set the system (part setting system).

U-- Log On Remote	M2M, SMS Control or virtual keypad logon.
U-- Off-Site (Web)	User nn logged out of Installer Menu from web server.
U-- Off-Site	User nn left Installer mode.
U-- On-Site (Web)	User nn logged into Installer Menu from web server.
U-- On-Site	User nn entered Installer mode.
U-- Ptn # Override	User nn overrode set fail at partition.
U-- Ptn # Override	User nn overrode set fail at partition.
U-- Ptn # PtSet	User nn part set partition.
U-- Ptn # Reset	User nn reset partition.
U-- Ptn # Set	User nn set partition.
U-- Ptn # Unset	User nn unset partition.
U--- Ptn ## Dur Rs	User nn keyed in a Duress code to unset partition n.
U--- Ptn ## Duress	User nn keyed in a Duress code to set partition n.
U--- Ptn ## Exit	User nn started the exit process for full set on partition n.
U--- PtSet # Exit	User nn started the exit process for part set on partition n.
U-- Rem Download	Downloader session completed successfully.
U-- Set Override	User nn overrode set fail.
U--- Shunt Code	User n Shunt code used.
U-- Spch Tel = Chg	User changed speech dialler telephone number.
U--- System Exit	User nn started the exit process for full set on a part setting system.
U-- System PtSet #	User nn part set system.
U-- System Reset	User nn reset system.
U-- System Set	User nn set system.
U-- System Unset	User nn unset system.
U-- Time/Date	User nn changed time and/or date.
U-- Z== Omit	User nn omitted zone.
U--- Z=== HUA Omit	User nn omitted Hold Up Alarm zone nn.
U--- Z=== Omit Rst	User nn included Hold Up Alarm zone nn.
U--- Z=== Omit Rst	User nn included (restored) zone nn.
VKP Connected	Virtual keypad connected.
VKP Disconnected	Virtual keypad disconnected.
VKP Ex Keys Rstr	Excess keys tamper at virtual keypad restored .
VKP Excess Keys	Excess keys (code attempts) tamper at virtual keypad.
WAM== Battery Rstr	WAM low battery restored.
WAM== Low Battery	WAM has low battery.
WAM== PSU Fail	WAM has low power supply.
WAM== PSU Restore	WAM low power supply restored.
WAM== RF OK	WAM supervision OK.
WAM== RF Warning	WAM about to fail supervision.
WAM== Sndr Tamper	Not used.
WAM== Sndr Tmp Rst	Not used.
WAM== Sndr Trb Rst	Not used.
WAM== Sndr Trouble	Not used.
WAM== Superv Fail	WAM has failed supervision.
WAM== Superv Rstr	WAM supervision restored.
WAM== Tamper Rstr	WAM tamper restored.
WAM== Tamper	WAM tampered.
Websvr Ex Keys Rst	The system was retored after a user keyed in the wrong password on the web browser interface more than four times in a row.
Websvr Excess Keys	Web server has caused a tampered by a user trying to log with the wrong password more than four times.
WSN== Trouble Rstr	Trouble message from wired siren restored.
WSN== Trouble	Trouble message from wired siren input to control unit.
Z== Alarm Photos	Photos from an IP camera are associated with a Zone Alarm event.
Z== Closed	Zone quiescent.
Z== Follow Photos	Photos from an IP camera are associated with a Zone Folllow event.
Z== Open	Zone activated.
Z== RF OK	Radio zone supervision OK.
Z== RF Warning	Radio zone about to fail supervision.
Z== Smoke Flt Rst	Smoke detector at zone has been restored.
Z== Smoke Flt	Smoke detector at zone has fault.
Z== Smoke PSU Flt	Smoke detector at zone has power supply fault.
Z== Smoke PSU Rst	Smoke detector at zone power supply fault restored.
Z=== Shunted	Zone nn is shunted.
Z=== UnShunted	Zone nn has been un-shunted.

Email error messages

The following shows the SMTP server response codes in "Email error ---" log messages:

200 Non-standard success response
211 System status, or system help reply
214 Help message
220 <domain> service ready
221 <domain> service closing transmission channel
235 Successful authentication
250 Requested mail action OK, completed
251 User not local, will forward to <forward-path>
252 Cannot VRFY user, but will accept message and attempt delivery
253 Pending message for node started
334 Server challenge

354 Start mail input, end with <CRLF>.<CRLF>
355 Octet offset is the transaction offset
421 <domain> service not available, closing transmission channel
432 A password transition is needed
450 Requested mail action not taken: mailbox unavailable
451 Requested action aborted: error in processing
452 Requested action not taken: insufficient system storage
453 No mail
454 TLS not available due to temporary reason. Encryption required for requested authentication mechanism
455 Server unable to accommodate parameters
458 Unable to queue message for node
459 Node not allowed: <reason>
500 Syntax error, command unrecognized
501 Syntax error in parameters or arguments
502 Command not implemented
503 Bad sequence of commands
504 Command parameter not implemented
510 Check the recipient address
512 <domain> cannot be found. Unknown host
515 Destination mailbox address invalid
517 Problem with senders mail attribute, check properties
521 <domain> does not accept mail (see RFC1846)
522 Recipient has exceeded mailbox limit
523 Server limit exceeded. Message too large
530 Encryption required for authentication mechanism
531 Mail system full
533 Remote server has insufficient disk space to hold email
534 Authentication mechanism is too weak. Message too big
535 Authentication unsuccessful/Bad username or password
538 Encryption required for authentication mechanism
550 Requested action not taken: mailbox unavailable
551 User not local, please try <forward-path>
552 Requested mail action aborted: exceeded storage allocation
553 Requested action not taken: mailbox name not allowed
554 Transaction failed
555 MAIL FROM/RCPT TO parameters not recognised or not implemented

TCP/IP error messages

The following table shows the TCP/IP error messages:

1001 General Error
1002 Invalid socket descriptor
1003 Invalid parameter

1004 It would have blocked
1005 Not enough memory in memory pool
1006 Connection is closed or aborted
1007 Socket is locked in RTX environment
1008 Socket, Host Resolver timeout
1009 Host Name resolving in progress
1010 Host Name not existing

Overview of the SSL-relevant messages

The following table shows SSL-relevant messages that are used in the SSL stack:

10064 Failed to get an IP address for the given hostname
10066 Failed to open a socket
10068 The connection to the given server / port failed
10070 Binding of the socket failed
10072 Could not listen on the socket
10074 Could not accept the incoming connection
10076 Reading information from the socket failed
10078 Sending information through the socket failed
10080 Connection was reset by peer
10082 Connection requires a read call
10084 Connection requires a write call
37520 A counter would wrap (eg, too many messages exchanged).
37648 Internal error (eg, unexpected failure in lower-level module)
37776 Unknown identity received (eg, PSK identity)
37904 Public key type mismatch (eg, asked for RSA key exchange and presented EC key)
38032 Session ticket has expired.
38160 Processing of the NewSessionTicket handshake message failed.
38288 Handshake protocol not within min/max boundaries
38416 Processing of the compression / decompression failed
38544 Hardware acceleration function skipped / left alone data
38800 The requested feature is not available
38928 Bad input parameters to function
39056 Verification of the message MAC failed
39184 An invalid SSL record was received
39312 The connection indicated an EOF
39440 An unknown cipher was received
39568 The server has no ciphersuites in common with the client
39696 No RNG was provided to the SSL module
39824 No client certification received from the client, but required by the authentication mode
39952 Our own certificate(s) is/are too large to send in an SSL message
40080 The own certificate is not set, but needed by the server

40208	The own private key or pre-shared key is not set, but needed
40336	No CA Chain is set, but required to operate
40464	An unexpected message was received from our peer
40592	A fatal alert message was received from our peer
40720	Verification of our peer failed
40848	The peer notified us that the connection is going to be closed
40976	Processing of the ClientHello handshake message failed
41104	Processing of the ServerHello handshake message failed
41232	Processing of the Certificate handshake message failed
41360	Processing of the CertificateRequest handshake message failed
41488	Processing of the ServerKeyExchange handshake message failed
41616	Processing of the ServerHelloDone handshake message failed
41744	Processing of the ClientKeyExchange handshake message failed
41872	Processing of the ClientKeyExchange handshake message failed in DHM / ECDH Read Public
42000	Processing of the ClientKeyExchange handshake message failed in DHM / ECDH Calculate Secret
42128	Processing of the CertificateVerify handshake message failed
42256	Processing of the ChangeCipherSpec handshake message failed
42384	Processing of the Finished handshake message failed
42512	Memory allocation failed
42640	Hardware acceleration function returned with error

www.touchpoint-online.com
Product Support (UK) Tel: +44 (0) 1594 541978
Available between:
08:30 to 17:00 Monday to Friday.
email: securitytechsupport@eaton.com
Part Number 12664354 31st May 2016