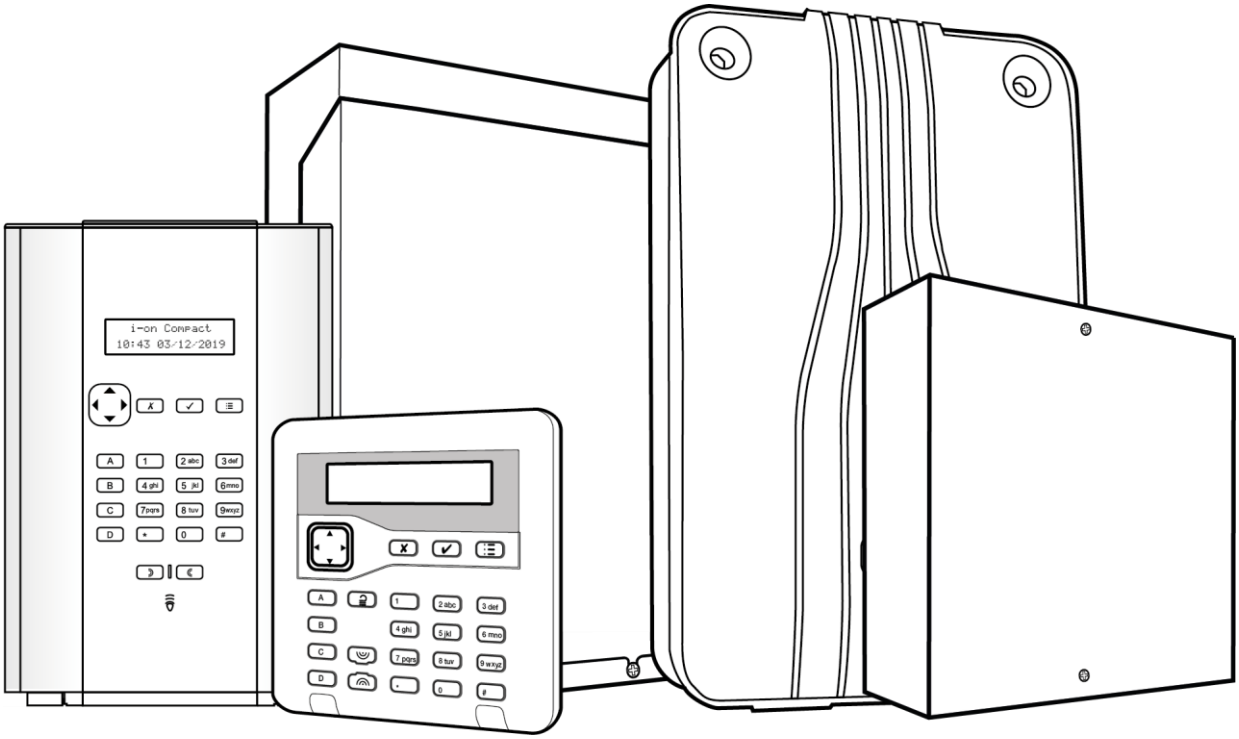
i-on Series
Security System

Configuration Guide

for i-on Compact, i-on30R+, i-on40H+, i-onG2SM, i-onG3MM and i-onG3LM



Issue 3

Control unit software version 7.02.xx

Scantronic

© Eaton 2022

The information, recommendations, descriptions and safety notations in this document are based on Eaton Corporation's ("Eaton") experience and judgment and may not cover all contingencies. If further information is required, an Eaton sales office should be consulted. Sale of the product shown in this literature is subject to the terms and conditions outlined in appropriate Eaton selling policies or other contractual agreement between Eaton and the purchaser.

THERE ARE NO UNDERSTANDINGS, AGREEMENTS, WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE OR MERCHANTABILITY, OTHER THAN THOSE SPECIFICALLY SET OUT IN ANY EXISTING CONTRACT BETWEEN THE PARTIES. ANY SUCH CONTRACT STATES THE ENTIRE OBLIGATION OF EATON. THE CONTENTS OF THIS DOCUMENT SHALL NOT BECOME PART OF OR MODIFY ANY CONTRACT BETWEEN THE PARTIES.

In no event will Eaton be responsible to the purchaser or user in contract, in tort (including negligence), strict liability or other-wise for any special, indirect, incidental or consequential damage or loss whatsoever, including but not limited to damage or loss of use of equipment, plant or power system, cost of capital, loss of power, additional expenses in the use of existing power facilities, or claims against the purchaser or user by its customers resulting from the use of the information, recommendations and descriptions contained herein. The information contained in this manual is subject to change without notice.

The i-on application includes the mbed TLS library, developed by a third party and licensed under the Apache 2.0 license. The Apache 2.0 license can be found at: http://www.apache.org/licenses/LICENSE-2.0

About this Guide

This guide is a document for people who need to configure an i-on30R+, i-on40H+, i-onG2SM, i-onG3MM, i-onG3LM or i-on Compact control unit. The guide provides detailed information about how to configure the unit using the options in the Installer menu of the user interface. The guide assumes that all hardware has been physically installed.

Other Publications

The following additional publications are available:

- **i-on Series User Guide** (for i-on30R+, i-on40H+, i-onG2SM and i-onG3MM) and **i-on Compact User Guide** – These provides an overview of the i-on intrusion system, including system components, key features and typical day-to-day tasks for end users.
- **i-on Series Administration and User Manual** – This provides detailed information about how to set and unset the system, manage alarms and use the User menu options.
- **Installation Instructions** – Included in the packaging of each hardware device (such as a control unit, module or sensor) are concise installation instructions that explain how to install that device.
- **i-on Series Installation Manual** – This gives full details of how to install i-on control units. It covers details about hardware installation, system architecture, the differences between each type of control unit, wiring requirements, supported peripherals, system limits, and system maintenance.
- **SecureConnect™ Installer Guide** – This provides an overview of SecureConnect, explains how to set up the system and describes how to manage panels (control units) using the SecureConnect web portal.

Contents

Chapter 1: Getting Started

Introduction

This chapter explains how to:

- Use the initial power-up procedure to configure the basic settings of the control unit.
- Enter and exit the Installer menu.
- Select options and change settings in the Installer menu.
- Reset the control unit.
- Upgrade firmware.

Initial Power-up Procedure

WARNING: During initial power-up, sounders and 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 15 for details of how to reset an existing system.

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.

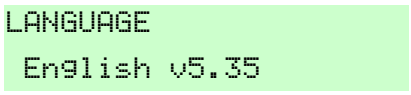
   Note: Ordinarily, the control unit starts only after the mains supply is switched on, even if a battery is connected. If you want to operate the control unit temporarily using only the battery (or a 12VDC supply), start it by briefly shorting the kick-start link on the PCB.
4. Wait until you see:

   ```
   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.

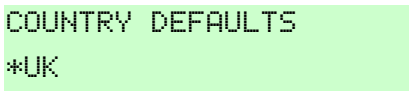
6. Choose the language:



You can change the language by pressing ▼ one or more times. Press ✔ to continue.

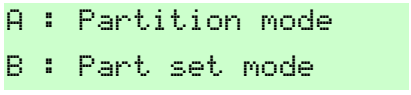
From this point on, the display operates in the selected language. If you want to change the language later, use *Installer menu – System Options – Updates – Language*.

7. Choose the country version you want to use:

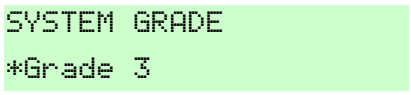


You can change the country by pressing ▼ one or more times. Press ✔ to continue.

8. Press A or B to select either a partitioned system or a part-setting system (these concepts are explained in the *Installation Manual*):

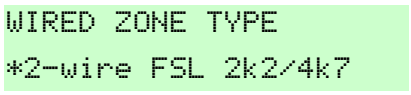


9. If you are using an i-onG3MM or i-onG3LM, leave the default of grade 3 or press ▼ if you want to use grade 2, then press ✔:



Selecting the grade sets various system options to configure the system for either grade 2 or grade 3.

10. Press ▼ one or more times to change the wiring type to use for wired zones (or leave the default), then press ✔:

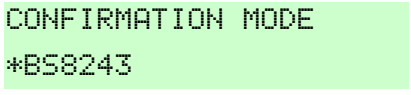


This determines the default wiring type for the control unit and any attached bus devices, such as wired expanders (if applicable). Wiring types are explained in the *Installation Manual.*

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.

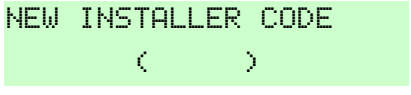
11. If you selected the UK as the country version, specify the alarm confirmation mode:



You can change the confirmation mode by pressing ▼ one or more times. Press ✔ to continue.

Please refer to page 83 if you need information about confirmation modes. You can change this setting later using *Installer menu – System Options – Confirmation – Confirmation Mode.*

12. Specify an installer code (four digits for grade 2, or six digits for grade 3):



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

Note: For a grade 2 system, you can change to 6-digit access codes using the System Options – *Restore Defaults – Staged Defaults – Users* option.

13. Specify a password for installer remote access to the control unit through the web interface (page 17), then press ✔ (or just press ✔ if you do not require remote access):

    ```
    SET REM. PASSWORD
    _
    ```

    See *Entering Text* on page 13 for details of how to enter text using a keypad).

    The password can be changed using the *System Options – Installer Options – Installer Remote Password* option.

    Note: Master users can also access the web interface. A master user's remote-access password can be configured through the User menu.

14. Specify a code for the default master user (four digits for grade 2, or six digits for grade 3):

    ```
    NEW USER 1 CODE
          (     )
    ```

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

15. 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-onG3MM
      12:00 01/11/2022
      ```

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

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

16. If the standby screen is displayed, enter the installer menu (as described in the next section). Otherwise, if the "Panel lid open" message is displayed, press ✘ to access the Installer menu.

17. Carry out the required configuration tasks in the Installer menu; for example, to:

    - Add the other bus devices, if used (page 38).
    - Program zones.
    - Configure outputs.
    - Configure setting options.

Entering the Installer menu

Entering the Installer menu allows you to configure the system using the options provided.

You cannot enter the Installer menu if:

- The system is set.
- Another user is accessing the control unit through the web interface or virtual keypad ("Remote Access" is displayed).

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”.

To enter the Installer menu:

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

   ```
        i-onG3MM
    12:00 01/11/2022
   ```

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

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

3. You may be prompted to enter a user code:

   ```
   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 Options – User Access – User Code Required* (see page 76). You cannot enter a Set Only user code.

4. You will see the following prompt if the control unit is connected to the internet and *Level 4 Update* is enabled in the Installer and User menus (see page 99):

   ```
        Check for
        Upgrade ?
   ```

   Press ✔ if the control unit is connected to the internet and you want the control unit to check whether there is new firmware (including language updates) available. Otherwise, press ✘ to continue without checking.

   If you press ✔ and new firmware is available, you are prompted whether to install the new version. You will need your level 4 code to do this.

   You can also upgrade firmware using an SD card and the *Panel Upgrade* option (see page 98).

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

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

   Refer to the next section for details of how to use the user interface.

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 display 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 out all users 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 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.

Understanding the User Interface

Selecting Options

The control unit displays configuration options in menus. The top-level Installer menu contains options such as *Detectors/Devices*:

```
INSTALLER MENU
 Detectors/Devices
```

You can select a different option by pressing the ▲ or ▼ key at the keypad until the name of the option or device you want is displayed. For example, pressing ▼ once when *Detectors/Devices* is displayed displays *Outputs*:

```
INSTALLER MENU
 Outputs
```

Pressing ▲ displays the earlier option in the menu. For example, pressing ▲ once when *Outputs* is displayed displays *Detectors/Devices*.

Pressing ✔ selects that option, which 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 appendix starting on page 152 shows a "menu map", which gives the position of all menus and options in the Installer menu.

Changing a Setting

To change the setting of an option, you normally follow the same procedure as above by pressing ▲ or ▼ one or more times to select the required setting and pressing ✔ to make the change. Some options require you to press ▶ or ◀ to change the setting from, for example, *Yes* to *No*. Other options may require you to enter text, as described in the next section.

Entering Text

You can use the numeric (0-9), * and # keys on the keypad to enter numbers and text when required to do so for an option. 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 zero, 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 ◀.

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.)
4. If there are no faults, the display shows the time and date, and the system is ready for use.

Exiting with Radio Zones not Learnt or Programmed

The following is displayed if you leave the Installer menu and there are radio zone(s) that are programmed (i.e. have a zone type other than *Not Used*) but are not learnt, or radio zone(s) that are learnt but not programmed:

```
CHECK RADIO ZONE(S)
 10
```

You can press ▲ or ▼ to scroll through the affected zone numbers. Return to the *Detectors/Devices* menu to learn (add) the detector or to change the zone type.

Exiting with Faults

You can exit the Installer menu, even if faults are present (such as the front of a detector being open). Exiting the Installer menu with faults present will not cause an alarm, but does keep the faults active.

If you attempt to exit the Installer menu with faults present, you will see:

```
    Cannot Exit.
   Faults Found.
```

This is followed by a list of faults, starting with the first. For example:

```
INSTALLER EXIT FLTS
 Z010T  Zone 010
```

Either:

1. Press ✘ to return to the Installer menu (for example, to rectify an issue that is causing the fault).

Or:

1. Press ✔ to display the next fault not yet displayed. You can also press ▼ or ▲ to scroll through the whole list of faults (whether previously displayed or not).
2. After you have displayed all faults, pressing ✔ displays:

   ```
    Leave installer
   mode with faults ?
   ```

   If all faults are then cleared, you will see:

   ```
   INSTALLER EXIT FLTS
    All Faults Cleared
   ```
3. Press ✘ to return to the Installer menu, or press ✔ to exit the Installer menu.

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 80). You must restore defaults from the control unit; 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.

Resetting Access Codes

You can use the Reset Codes link on the control unit's PCB to delete the installer and all user codes. You will be prompted to specify new codes for the installer and master user.

Resetting the codes also removes the assignment of all proximity tags, Hold-Up Devices (HUDs) and remote controls to users.

You may want to use this feature in the event that the installer code has been forgotten. Once you are in the Installer menu, you can use *System Options, Restore Defaults, Staged Defaults* to reset user codes (see page 80).

Note: You can disable the Reset Codes link by disabling *System Options, Hardware, Reset Codes Pins* (see page 92).

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. Place a jumper across the Kick-Start link.
6. While shorting the Reset Codes link, reconnect the battery and keep the short in place until you see the following:

```
NEW INSTALLER CODE
        (    )
```

7. Enter a code you want to use for the installer code. Confirm when prompted.
8. Enter a code you want to use for the master user code. Confirm when prompted.
9. Remove the jumper across the Kick-Start link.
10. Close the lid.
11. Reconnect the mains supply.

Upgrading the Firmware

You can upgrade the control unit's firmware in one of several different ways:

- Over the internet − When you enter the Installer menu, you are prompted whether to upgrade the firmware if *Level 4 Update* is enabled in the Installer (see page 99) and User menus.
- Via an SD card − If the firmware is loaded in an INSTALL folder on the SD card, you can upgrade the firmware using the *Panel Upgrade* option (see page 98).
- Using the control unit's web interface.
- For i-on Compact, by connecting the mini-USB port to a Windows computer that is installed with 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 the LAN or Internet

The control unit has a built-in Ethernet port, which can be connected to the Local Area Network (LAN). Connecting the control unit to the LAN allows the system to be configured and monitored from a web browser.

If a COM-DATA-WIFI or COM-DATA-4G-WIFI module is fitted, the control unit can access the LAN over a Wi-Fi network. If the control unit has both a Wi-Fi and Ethernet connection, the Ethernet port is used in preference, and Wi-Fi is used if Ethernet communication is not available.

If the LAN has a gateway to the internet, the control unit can connect to the internet, for example to report alarms to an Alarms Receiving Centre (ARC), for firmware updates, or for remote configuration and monitoring through Eaton SecureConnect.

If a COM-DATA-4G or COM-DATA-4G-WIFI module is fitted, the control unit can also access the internet over a mobile phone network. The control unit can be configured to use this method of communication as a backup in the event that internet access via the LAN is not available. Alternatively, the mobile network can be used in all cases.

Only one module can connect to the control unit. Therefore, if you have a COM-DATA-WIFI, Wi-Fi communication is available but not mobile communication. Similarly, if you

have a COM-DATA-4G, mobile communication is available but not Wi-Fi. The COM-DATA-4G-WIFI has the benefit of allowing both mobile communication and Wi-Fi.

About the Web Interface

This guide describes how to configure the control unit from a keypad (in the case of i-on Compact, the keypad is on the front panel of the control unit). However, if the control unit is connected to the LAN, installers can also configure many settings from the web interface (Figure 1), as the control unit has a built-in web server. The settings provided through the web interface have the same behaviour as described in this guide.

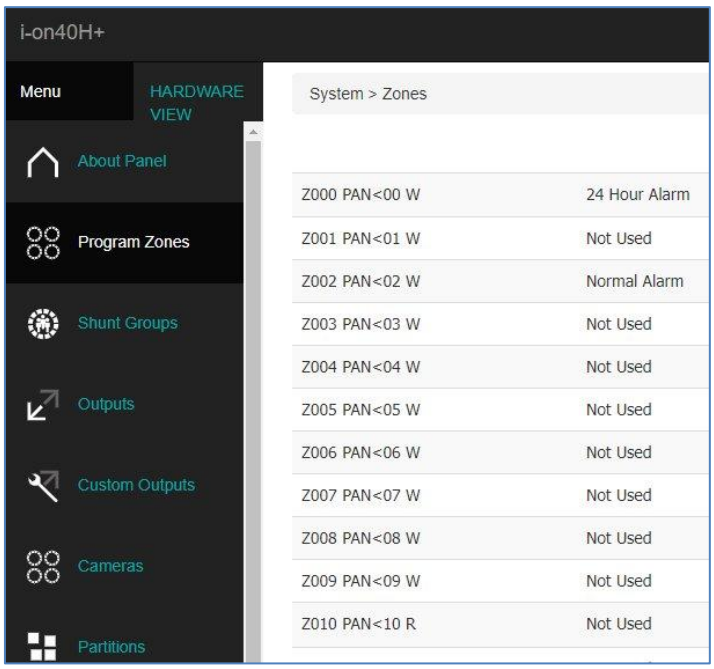


Figure 1 - Web Interface

You can access the web interface by entering the control unit's IP address in the address bar of a web browser, and then entering your user code and remote password in the login page displayed. Your remote password is defined during system setup (page 11) and can be changed using the *System Options – Installer Options – Installer Remote Password* option.

The web interface can be enabled using the *Communications – IP Options – LAN – Web Server – Status* option (see page 115). Remote access must also be enabled using *U*ser *Menu – System Config – Facilities On/Off – Remote Access*.

Master users can access a simplified version of the web interface, which allows operations such as to view the status of the system, examine the log, create users, create calendar sets and view detector signal strengths. Master users access the web interface in the same way as installers by entering their user code and own personal remote password, which can be configured using *U*ser *Menu – Users – Edit User*.

The *i-on Web Browser Interface Setup Guide* explains how to configure and use the system using the web interface.

Virtual Keypad

The virtual keypad (Figure 2) allows you to perform similar functions as available at a hardware keypad, including operation of user-defined outputs using the ABCD keys. The navigation and ABCD keys reflect the status of the system in the same way as for a hardware keypad.

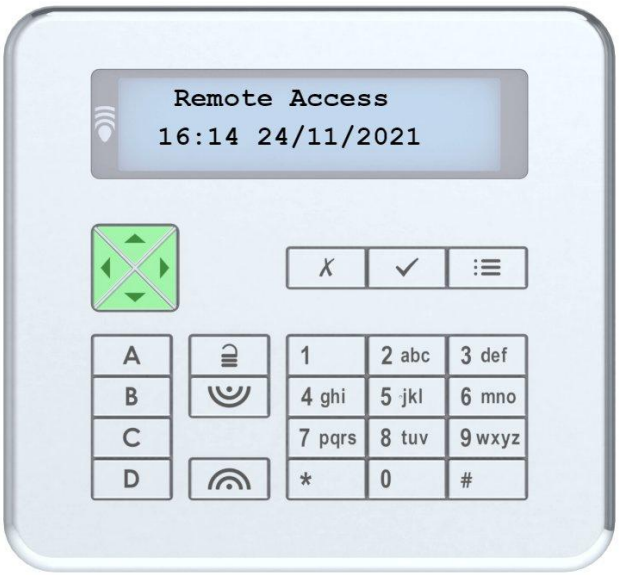


Figure 2 - Virtual Keypad

For installer and master users, the virtual keypad is access through a Virtual Keypad option in the web interface. For other users, the web interface is displayed directly after entering their user code and personal remote password in the login page of the web interface.

If a master user creates a new user and defines a remote password, it gives permission for the new user to access the virtual keypad. The new user can change the password using *U*ser *Menu – Users – Edit User* (if available to the user).

The virtual keypad can also be accessed through Eaton SecureConnect, as described in the *SecureConnect Installer's Guide*.

Chapter 2: Addressing and Zone Numbering

This chapter explains how the control unit assigns addresses to devices (such as expanders and radio keypads), detectors and outputs. It also explains how the control unit maps zone numbers to detectors.

Bus Device Addresses

Note: This section is relevant only for control units that have a bus for system expansion (all control units except i-on Compact).

The control unit keeps a record of the address it allocates to each bus device. 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. R1-03), where:

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

n = Bus number (1 or 2, depending which bus connector the device is connected to).

dd = Bus device number. Keypads have bus device numbers in the range 51 upwards. Expanders and other bus devices can have a bus device number in the range 1 to 50 (depending on the control unit, as specified in the *i-on Installation Manual*). Each time you add a new device, the device takes the lowest bus device number available, irrespective of which bus the device is connected to.

Figure 3 shows an example of bus device addressing.

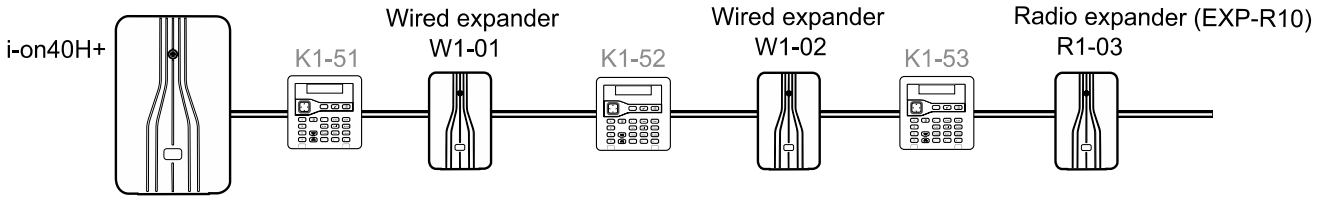


Figure 3 - Bus Device Addressing Example

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. R1-03-01), where:

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

n = The bus number of the radio expander.

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>01 to PAN>04 (the number of on-board outputs is dependent on the control unit used; see the *i-on Series Installation Manual*). Outputs attached to a bus device take the address An>dd>oo (e.g. W1>02>01), where:

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

n = Bus number.

dd = Bus device number (see page 19).

oo = Output number, starting from 01.

See Figure 4 for an example.

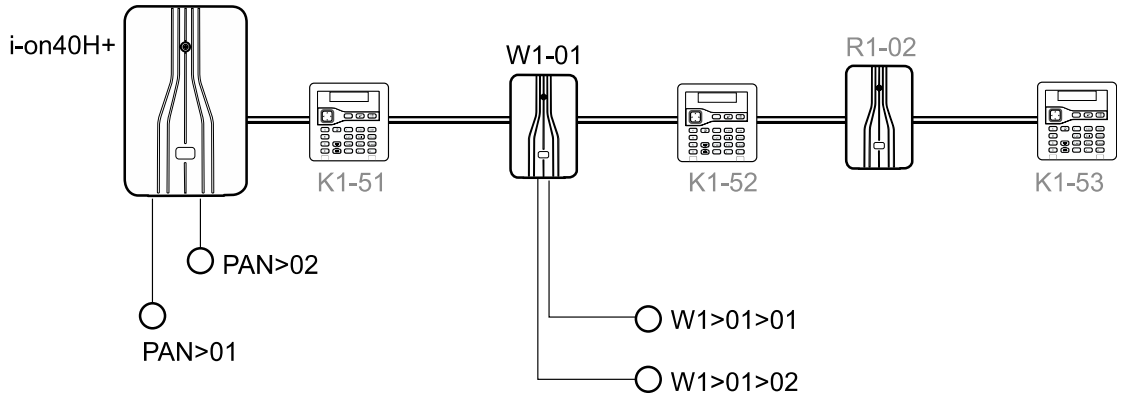


Figure 4 - Output Numbering

Detector Addresses and Zone Numbering

Figure 5 provides an example of detector addressing and zone numbering for an i-on40H+. The next sections explain how the control unit assigns detector addresses and zone numbers.

Note: Please refer to page 133 for important information concerning zone 000 if you are using the CID format to transmit alarm information to an alarms-receiving centre.

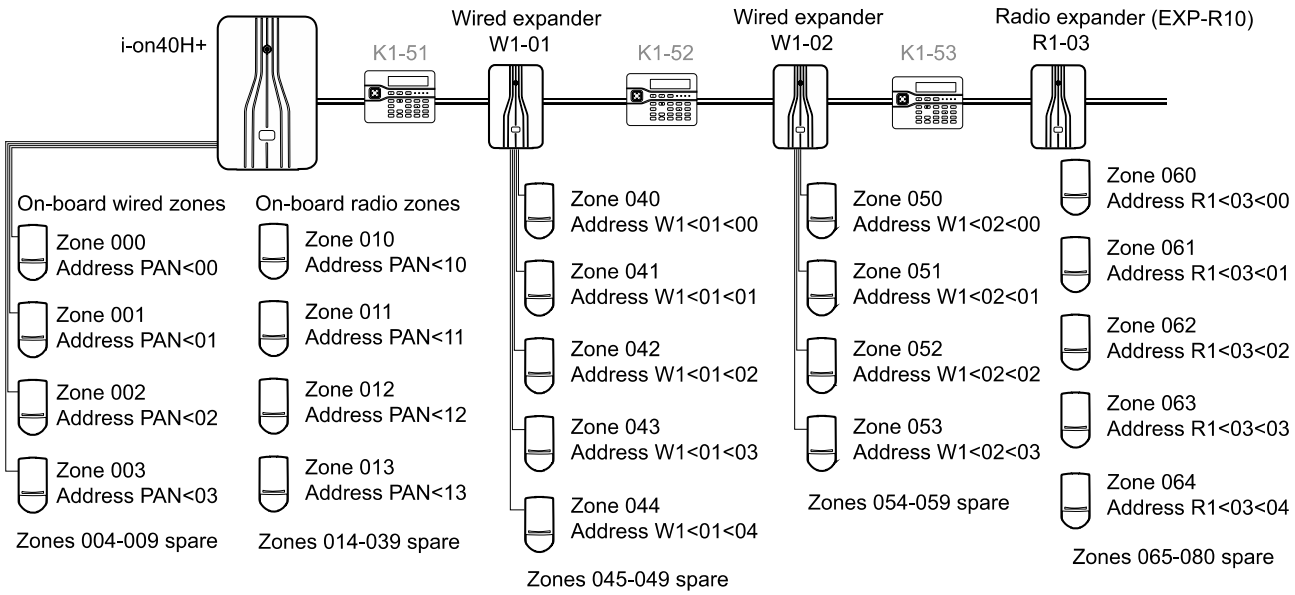


Figure 5 - Example of Detector Addressing and Zone Numbering (i-on40H+)

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<00 to PAN<09	000 to 009
4-wire CC wiring	PAN<01 to PAN<05	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<00 to PAN<29	000 to 029
i-on40H+	PAN<10 to PAN<39	010 to 039
i-on Compact	Not applicable	000 to 019

Detectors Attached to an Expander or PSU

Detectors attached to an expander (including remote power supply) 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.

dd = Bus device number (see page 19).

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.

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 dd0 to dd4 (for 4-wire CC wiring), where "dd" is the two-digit device number. Table 1 provides an example (refer also to Figure 5).

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

Table 1: Example of expander zone numbering (i-on 40H+)

1st Expander (e.g. EXP-W10) Device number 01 Address W1-01		**2nd Expander (EXP-W10) Device number 02 Address W1-02**		**3rd Expander (EXP-R10) Device number 03 Address R1-03**	
Detector Address	**Zone No.**	**Detector Address**	**Zone No.**	**Detector Address**	**Zone No.**
W1<01<00	040	W1<02<00	050	R1<03<00	060
W1<01<01	041	W1<02<01	051	R1<03<01	061
W1<01<02	042	W1<02<02	052	R1<03<02	062
...etc.	*...etc.*	*...etc.*	*...etc.*	*...etc.*	*...etc.*
W1<01<07	047	W1<02<07	057	R1<03<07	067
W1<01<08	048	W1<02<08	058	R1<03<08	068
W1<01<09	049	W1<02<29	059	R1<03<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 2 shows an example.

Table 2: 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.*
i-onG2SM	49, 48	47, 46	45, 44	*...etc.*
i-onG3MM	199, 198	197, 196	195, 194	*...etc.*
i-onG3LM	399, 398	397, 396	395, 394	*...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 3 shows an example. For each keypad, the Z2 terminals are for the tamper contacts, and the Z1 terminals are for the alarm contacts.

Table 3: 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.*
i-onG2SM	49	47	45	*...etc.*
i-onG3MM	199	197	195	*...etc.*
i-onG3LM	399	397	395	*...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 6 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, but zones 030 to 039 are available. This could happen if the default (lowest available) address was not accepted when the expander at the top of the range was added. The

control unit cannot allocate keypad zones to zone numbers below those used by the expander.

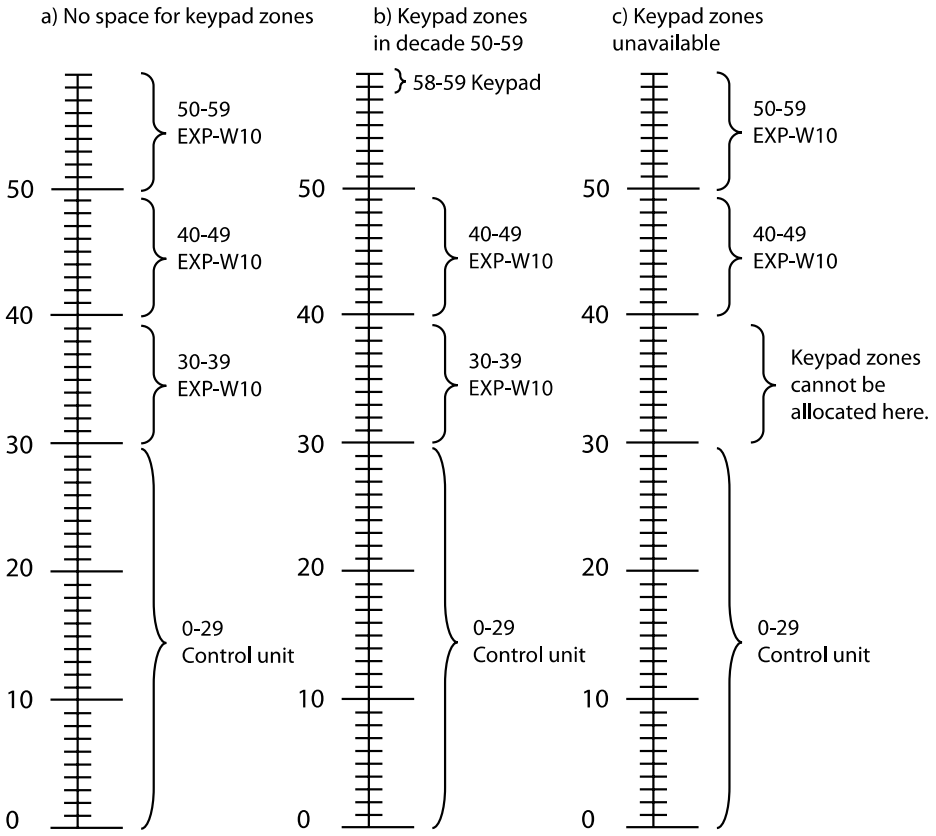


Figure 6 - Example zone availability (i-on30R+)

Chapter 3: 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.

Depending on the type of control unit, three levels of *Delete all* options are provided (see the menu map on page 19). These allow you to delete all radio zones associated with a selected expander (if applicable), 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 20 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).
- "CHECK RADIO ZONES" is displayed if you leave the Installer menu and there are radio zone(s) that are programmed (i.e. have a zone type other than *Not Used*) but not learnt, or radio zone(s) that are learnt but not programmed. See page 14.
- Please refer to page 133 for important information concerning zone 000 if you are using the CID format to transmit alarm information to an alarms-receiving centre.

Name

You can give each zone a name of up to 40 characters. 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 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 display when you select a zone.
- 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 part set 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 67). (In a part-setting system, *HUA Response* is under *System Options*; in a partitioned system, it is in the sub-menu for each partition.)

There may also be an alarm transmission to the ARC, depending on how you have configured the system.

HUAs have an alarm sound that is distinct from other alarm types.

Fire Alarm - FA (02)

Smoke or heat detectors connected to Fire Alarm zones cause keypads, internal radio sounders, loudspeakers and external sirens to give a pulsing fire signal (subject to the *Alarm Response*; see page 67). Fire alarms operate whether the system is set or unset, and will always trigger communications.

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 loudspeakers 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 part set or partition) is unset causes an internal alarm (keypads, internal radio sounders and loudspeakers). Activating this zone while the system (or part set or partition) is set causes an alarm from internal sounders and external sirens (subject to the *Alarm Response*; see page 67).

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 to start the entry procedure. See page 64 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 71.

Note: 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 the system (or part set or partition), a PIR may still be in lockout, during which it cannot send a signal to complete the setting process.

Entry Route – ER (06)

Use this zone type for detectors sited between the Final Exit door/detector and the location where the system is set/unset. 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 71.

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 display 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 at keypads, internal radio sounders and

loudspeakers every few seconds. When a user enters a valid access code, the tone stops and the display shows 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)

(This zone type is not available for i-on Compact.)

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

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

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.

Key Switch Latched – KSL (09)

(This zone type is not available for i-on Compact.)

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

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

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.

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 (see page 67) determines whether external sirens, strobe and communications also respond to the alarm.

External PSU A/C Fail – PAC (11)

(This zone type is not available for i-on Compact or radio zones.)

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 *Mains Fail Delay* (see page 89).

External PSU Batt Fault - PBF (12)

(This zone type is not available for i-on Compact or radio zones.)

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 “External Battery Fault” alert.

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.

External PSU Low Volts – PLV (13)

(This zone type is not available for i-on Compact or radio zones.)

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 “External Low Volts” alert.

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.

External PSU Fault – PF (14)

(This zone type is not available for i-on Compact or radio zones.)

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 “External power fault” alert.

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.

External WD Fault – WD (15)

(This zone type is not available for i-on Compact or radio zones.)

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 “Ext WD Fault” alert.

In a grade 2 system, a user can override this fault and set the system. In a grade 3 system, a user cannot override this fault.

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.

Once the zone is restored, in a grade 2 system a user can clear the alert by pressing ✔ and entering their access code. In a grade 3 system, the installer must enter the Installer Menu and leave it again to clear the alert.

HUD Fault – HUD (16)

(This zone type is not available for i-on Compact or radio zones.)

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 “HUD Fault” alert. 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.

Once the zone is restored, in a grade 2 system a user can clear the alert by pressing ✔ and entering their access code. In a grade 3 system, the installer must enter the Installer Menu and leave it again to clear the alert.

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)

(This zone type is not available for i-on Compact.)

Use this zone type to terminate setting when the system or partition exit mode is Exit Terminate (see page 64). 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)

(This zone type is not available for i-on Compact.)

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 35), and activates any output of type Zones Shunted (see page 60).
- 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 97.

Shunt Key Non-Latch SKNL (20)

(This zone type is not available for i-on Compact.)

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)

(This zone type is not available for i-on Compact.)

Use this zone type to complete setting when the system or partition exit mode is Lock Set (see page 65). 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.

Occupancy OC (22)

(This zone type is not available for i-on Compact.)

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 not available for i-on Compact.)

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 is not available for i-on Compact or radio zones.)

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 (see page 67) determines whether external sirens, strobe and communications also respond to the alarm.

Perimeter PZ (25)

This zone type intended to be used with external (perimeter) detection equipment. *PZ Unset Response* (see page 68) and *PZ Set Response* (page 68) 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 4). You can use *All Partitions* to assign or de-assign the zone to or from all partitions.

Table 4: 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	22	Occupancy
24	Tamper Return	23	Security
		25	Perimeter

Attributes

Table 5 shows the zone attributes and the zone types they apply to. You can assign more than one attribute to a zone. Some attributes are unavailable for i-on Compact and radio or wired zones. The display shows only the available attributes for the zone type you select.

Table 5: Zone attributes available for zone types

	Zone Attributes																					
	Chime1	Chime2	Soak Test	Double Knock	Activity Mon	Reset	Part Set B	Part Set C	Part Set D	Omittable	Force Set Omit	Masking	Inverted	Shuntable	Supervision	Linked Zone	Extended Entry Time	Double Doors	One Partition	Unset Logging	Force Set	HUD Dual Button	HUD LED Active
Zone Type																							
Not Used																							
Hold Up Alarm													Y		Y							Y	Y
Fire Alarm													Y		Y								
Normal Alarm	Y	Y	Y	Y	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		Y			
Final Exit	Y	Y			Y		Y	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			Y	Y	Y			
Technical Alarm	Y	Y					Y	Y	Y	Y			Y		Y								
Key Switch Moment.													Y		Y				Y		Y		
Key Switch Latched													Y		Y				Y		Y		
Tamper			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				Y	Y			
Shunt key Latching													Y		Y								
Shunt Key Non-Latch													Y		Y								
Lock Set													Y		Y				Y	Y			
Occupancy													Y		Y				Y	Y			
Security													Y		Y								
Tamper Return			Y				Y	Y	Y	Y	Y												
Perimeter	Y			Y			Y	Y	Y	Y	Y		Y			Y		Y					

Chime1 and Chime2

(i-on Compact has only one Chime attribute.)

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 20) 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, a brief message is displayed 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

(This attribute is not available for radio zones.)

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.

Activity Mon

Zones programmed with this attribute are included in social-care activity monitoring (see page 99).

Reset

This attribute is intended for wired zones only. 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.

Part Set B

When a user sets part set B, the control unit sets only those zones where the Part Set B attribute = “Yes”. (See also “Exit Mode” on page 64.)

Part Set C

When a user sets part set C, the control unit sets only those zones where Part Set C attribute = “Yes”.

Part Set D

When a user sets part set D, the control unit sets only those zones where Part Set D attribute = “Yes”.

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 Options – User Access – Quick Omit* (see page 76).

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

If this attribute is set to On:

- A calendar set can force set* the system while the zone is active (open), providing the feature is enabled in *Setting Options/Partitions – Calendar Set – Force Set* (see page 74).
- A user with a remote control can force set* the system while the zone is active, providing the feature is enabled in *System Options – Radio Options – Remotes – Force Set* (see page 94).
- A user radio keypad (not KEY-RKPZ) can force set* the system while the zone is active, providing the feature is enabled in *System Options – Radio Options – Radio Keypads – Force Set* (page 94).
- A zone of type Key Switch Momentary or Key Switch Latched can force set* the system while the zone is active, providing the zone has the Force Set attribute set to On.

*When a force set occurs, the system omits the active zone that is attempting to set, and sets the remaining zones normally.

Masking

(This attribute is not available for radio zones.)

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 Options – Masking* (page 95) to make this attribute available, and the zone wiring type must be FSL.

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

Inverted

(This attribute is not available for radio zones.)

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

(This attribute is not available for i-on Compact.)

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 97).

If you wish to set up a shunt key, see page 30.

Supervision

(This attribute is available only for radio zones.)

This attribute allows you to enable/disable supervision for individual zones.

When set to *On* (the default), supervision for this zone is the same as the selected option in *System Options – Radio Options – Supervision* (see page 92). When set to *Off*, supervision is disabled for this zone.

When a radio device is supervised, the control unit checks for periodic communications from the radio device.

Linked Zone

If a zone activates that has this attribute, a second zone with this attribute must also activate within the *Linked Zone Time* (see page 67) for an alarm to trigger. Both zones must be of the same type (*Normal Alarm* or *Perimeter*), and for a partitioned system, both zones must also be in the same partition.

This attribute is normally used only for an area protected by an array of infra-red beams, with each beam connected to a separate zone.

Extended Entry Time

This attribute is only for Final Exit zone types. If enabled and the zone is triggered to start the entry procedure, the system uses the *Extended Entry Time* setting (page 67). If disabled, the system uses the standard *Entry Time* setting (page 66).

This attribute allows for cases where you need to allow an increased length of time for the entry procedure for certain zones. For example, you may want to allow 40 seconds for a front door, and 90 seconds for a garage entrance.

Double Doors

This attribute is available only if the zone is configured to use the 2k2/4k7 FSL wiring method (e.g. see page 88). Setting this attribute allows the zone to monitor two detectors in series, providing each detector has a 4k7 shunt resistor and there is a 2k2 end-of-line resistor. Please refer to the *i-on Series Installation Manual* for wiring details.

To enhance system security, it is not recommended to use this attribute if only one detector is connected to the zone.

One Partition

This attribute causes the zone to set if any one of its partitions is set (normally, all the zone's partitions must be set for the zone to set).

Unset Logging

Setting this attribute causes the control unit to log when the zone opens and closes, providing the zone is unset.

The zone status can be reported to SecureConnect (to report the event to the SecureConnect mobile App, ARC or email recipient), or directly to an ARC from the control unit using the Zone Status SIA report group (see page 142).

A typical use for this attribute may be for a detector located in a room that requires special monitoring, so that a manager or other person can be informed of when someone enters the room while the system is unset.

Force Set

This attribute is for zones of type Key Switch Momentary and Key Switch Latched only.

You may wish to allow the key switch to set the alarm system even if one or more zones are active or have faulty detectors. This is known as a "force set". The detectors that are active or are faulty must have the *Force Set Omit* attribute set to Yes. When a force set occurs, the system omits the active or faulty zones and sets the remaining zones normally.

Note: If you enable *Force Set*, the system does not comply with EN50131.

If you select *Off*, the key switch cannot force set the system, even if you have applied the *Force Set Omit* attribute to any zones.

If you select *On*, the key switch can force set the system.

HUD Dual Button

This attribute is available only if the detector is an HUD-2B-FXD hold-up device that has the Hold Up Alarm zone type, and has been configured for two-way mode (using the DIP switches, as described in the *HUD-2B-FXD Installation Instructions*).

Selecting *Off* allows only one of the two buttons to be pressed to activate a hold-up alarm.

If you select *On*, both buttons need to be pressed at the same time to activate a hold-up alarm.

HUD LED Active

This attribute is available only if the detector is an HUD-2B-FXD hold-up device that has the Hold Up Alarm zone type, and has been configured for two-way mode (using the DIP switches, as described in the *HUD-2B-FXD Installation Instructions*).

Selecting *Off* disables the LED on the device.

Selecting *On* enables the LED on the device, as follows:

- A flashing amber LED indicates that the control unit has started an unconfirmed hold-up alarm.
- A flashing red LED indicates that the control unit has raised a confirmed alarm.

  Note: A confirmed hold-up alarm can be produced only if Confirmation Mode is BS8243 (see page 83).

  Please refer to the *HUD-2B-FXD User Guide* for details of how to generate confirmed hold-up alarms using HUD-2B-FXD hold-up devices.

Resistance

(This option is not available for i-on Compact.)

This option allows you to specify the resistance values used by an individual FSL zone on either the control unit (if applicable), an EXP-W10/WCC or a remote power supply. 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

(This option is not available for i-on Compact.)

You can use this option to add new bus devices to the system once they are physically wired to the bus. The control unit assigns a bus address (see page 19) 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 use the appropriate Delete or *Replace* Option, such as *Detectors/Devices – Wired Expanders – Delete Expander*, or *Detectors/Devices – Wired Expanders – Replace Expander.*

Adding bus devices

Note: If a bus device already has an address stored within it, you will need to clear the address before adding it to the bus. For example, for a keypad, 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 45).

To add new bus devices to the system:

1. From the Installer menu, select *Detectors/Devices – Address Bus Device*. 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 ✘.

Lost, Found and Duplicate Devices

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.

After power-up, an alarm is generated if the control unit recognises that a device is missing.

After exiting the Installer menu, the control unit queries every device on the bus to report its bus address. The control unit compares the reported addresses with those that is has stored and may report duplicate, found and lost bus devices, as described next.

Duplicate Bus Addresses

If two devices have the same address, you will see, for example:

```
Duplicate Addresses
 Exp.W1-05    (W10)
```

If you see this message, you 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 previously-added device is missing or a new device is present, the display shows, for example:

```
FOUND 0, LOST 1
 Lost W1-03
```

The top line shows the number of new devices found, and the number of existing devices lost. The bottom line shows the bus and address of 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 "*1-*" 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.

Wired Expanders

(This option is not available for i-on Compact.)

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 38 for details of how to proceed. The control unit assigns a bus address (see page 19) 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 41).

- Use the *Detectors/Devices – Address Bus Device* to give a remote power supply (EXP-PSU, EXP-PSU-SM, EXP-PSU-MM or EXP-PSU-LM) a bus address.

Edit Expander

You can use this option to edit settings for a specific expander or remote power supply.

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 device a name. The name appears in the log, in alerts and when configuring the expander.

Partitions

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

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

If any associated partition is set, a tamper at the device 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 device to or from all partitions.

Wired Zone Type

You can change the zone wiring method for each wired expander or remote power supply individually. The available options can depend on the device type.

Please refer to the *i-on Installation Manual* for details of the wiring types.

Loudspeaker Volume

Use this option to change the volume of chime, entry, exit, alert (such as low battery), confirmation and other tones from a loudspeaker connected to the expander or remote power supply. You can separately adjust the volume of each type of tone. This volume control does NOT change the volume of alarm tones, which are always sounded at full volume.

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

Battery 2

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

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 or remote power supply 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, remote power supply 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.
- 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 a wired expander or remote power supply with a new wired expander or remote power supply, but leave the existing device's configuration intact in the control unit.

The replacement does not have to be the same type as the device being replaced. However, note that although the EXP-WCC, EXP-W10 and remote power supplies support the same number of FSL and 2-wire CC zones, the maximum number of 4-wire CC zones can differ between the devices, and plug-by outputs are available only on the EXP-PSU and EXP-PSU-LM. Before replacing a device with another of a different type, please make sure that the replacement supports all hardware features being used on the current device.

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

When you power up the control unit again, the keypads will show an alert that the device has been disabled. Select *Replace Expander* again, select the *Add* option and then hold down the address request button on the new device (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.

Radio Expanders

(This option is not available for i-on Compact.)

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 42.

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.

Wired Keypads

(This option is not available for i-on Compact.)

Address Bus Device

Use this option to add a wired keypad. The control unit assigns a bus address (see page 19) to each keypad you add.

If the keypad you are adding already has an address 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 45).

Edit Keypad

You can use this option to edit settings for a specific keypad. The *Virtual Kpd* option is to configure settings for the virtual keypad, which can be displayed in the web interface (page 17).

Note: If you wish to find out where the physical keypad 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.

Name is not currently used for a virtual keypad.

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, users of that partition will not be able to hear entry/exit tones and alerts for the partition from keypads.

Once you have assigned a keypad to a partition:

- The keypad will display messages and give tones for the assigned partition(s). (Tones are not sounded at a virtual keypad.)
- A Partition User can use only keypads assigned to the same partition as the user's code or proximity reader tag.
- 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 set part sets B, C and D. To choose the setting method, select *Action*, *Set*, and then the required option.

In a partitioned system, you can enable a quick-set key to full set or part set individual partitions. To choose the setting method, select *Action*, *Set*, select the partition, and then press the left/right arrow key to choose the required option.

Alternatively, in both part-setting and partitioned systems, you can program a quick-set key to trigger a user-defined output (see page 61).

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 76.
- The control unit logs the use of quick-set keys under a quick-set user identity.

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 26).

Please refer to page 23 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 the *i-on Installation Manual* for details of the wiring types.

Loudspeaker volume

This option is available for the KEY-FKPZ. Use this option to change the volume of chime, entry, exit, alert, confirmation and other tones from a loudspeaker connected to the keypad. You can separately adjust the volume of each type of tone. This volume control does NOT change the volume of alarm tones, which are always sounded at full volume.

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).

Use this option to change the volume at the keypad of chime, entry, exit, alert, confirmation and other tones that originate from the control unit. You can separately adjust the volume of each type of tone. This volume control does NOT change the volume of alarm tones, which are always sounded at full volume.

Note: The KEY-FKPZ has a local option for setting the volume of tones that originate from the keypad (such as key and proximity reader beeps, and address request tones) – please refer to the KEY-FKPZ Installation Instructions.

Backlight

This option is available for the KEY-FKPZ and KEY-KPZ01. You can use this option to control the backlight.

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 a key or presents a proximity tag. The backlight stays on for eight seconds after the last keypress or proximity tag use.
- 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.

Internal Prox

This option appears for keypads that have an internal proximity reader.

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

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 Options – User Access – Terminated Set* (see page 77) 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 49.

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 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.

A keypad that has configured zones cannot be replaced by a keypad that does not support zones. In all other cases, a wired keypad can be replaced by a wired keypad of the same or different type. A wired keypad cannot be replaced by a radio keypad (including the KEY-RKPZ), or vice versa.

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.

On-board Keypad

(This option is available only for i-on Compact.)

You can use this option to change settings for the keypad fitted in the control unit.

Key A/B/C/D

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

You can enable each key to:

- Full set the system.
- Set part set B, C or D.
- Trigger a user-defined output (see page 61).

Each key can have a name. This is displayed while the system is setting after the user presses that key.

Note:

- The ABCD LEDs (if enabled) show the state of the keys. For example, if key A is programmed to full set, then whenever the system is full set, LED A glows.
- If you enable the quick-set keys, the control unit no longer complies with EN50131. See page 76.
- The control unit logs the use of quick-set keys under the quick-set user identity.

ABCD Led

You can use this option to enable or disable the ABCD LEDs at the control unit.

Audible Keys

You can use this option to enable or disable audible beeps that confirm key presses, as generated by the control unit's built-in sounder . **Note:** You can set the volume of the beeps using *System Options – Hardware – On-board Sounder – Volume*.

Status fault

If you set this to Enabled, the navigation key will illuminate red when there is an alarm. If you choose Disabled, the navigation key does not illuminate red.

Status OK

If you set this to Enabled, the navigation key will illuminate green when the system is normal; that is, when there are no alarms. If you choose Disabled, the navigation key does not illuminate green.

Backlight

This option controls the lighting on the display and behind the keys.

Mode

If you set this option to Timed, the backlight is normally off, but glows:

- When a user presses a key or presents a proximity tag. The backlight remains on for eight seconds after the last key press or use of a proximity tag.
- While the entry timer is running.
- While there is an alarm.

When set to On, the backlight is permanently on. When set to Off, the backlight is permanently off.

Brightness

This option allows you to set the brightness of the backlight.

Internal Prox

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

Radio Keypads

(This option is not available for i-on Compact.)

Note: If the system uses a radio keypad then it will not comply with security grade 3.

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 proximity tags). It is possible to change a radio keypad to transmit six-digit access codes. Please refer to the i-RK01 installation instructions.

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).

Add/Del Radio Kpd

To add or remove a radio keypad:

1. Select *Add/Del Radio Keypad*.
2. Select *Panel* (if applicable) or an expander name (if applicable).
3. If you are adding a keypad, select one of the available keypad addresses, then activate the radio keypad’s tamper to make the control unit learn the identity of the keypad.
4. If you are removing a keypad, select the name of the keypad to remove.

Edit Keypads

You can use this option to edit settings for a specific radio keypad. For an i-RK01, the *Edit Keypad* menu contains the following options:

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 (partitioned system only)

To assign the keypad to partitions. The procedure is similar to assigning wired keypads to partitions; see page 42.

Key A/B/C/D

These options allow you to program the A, B, C and D (quick-set) keys. The procedure is similar to configuring quick-set keys for wired keypads; see page 43.

KEY-RAS

The KEY-RAS allows users to set, unset and part-set the system, operate output devices, and query the current set/unset status of the system. No base station is needed for connection to the control unit's bus.

Using a DIP switch in the keypad, the KEY-RAS can be configured in either two-way or one-way mode. Two-way mode enables the KEY-RAS to display the current set or unset status of the system, and to sound entry, exit and alarm tones. One-way mode gives backwards compatibility with previous-generation i-RK01 arming stations, and cannot feed back the current status of the system or produce entry, exit and alarm tones.

Note: When installed in a partitioned system, the KEY-RAS can be used with only one partition.

For a KEY-RAS, the Installer menu provides the same options as an i-RK01 (see above), but also includes two additional options in the *Edit Keypad* menu:

Battery Only

Choose Yes if only a battery is used, or No if an external PSU is also used. Selecting Yes prevents an “RKU n PSU Fail” message, which indicates loss of power supply.

Sounder Volume

Choose the required volume of the internal sounder.

KEY-RKPZ

(This option is not available for i-on Compact.)

The KEY-RKPZ is a two-way battery-powered radio keypad, with built-in proximity reader and two on-board zones. This keypad uses a KEY-RKBS base station connected to the bus.

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 for a KEY-RKPZ contains the following options:

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 (partitioned system only)

You can assign the keypad to partitions. The procedure is similar to assigning wired keypads to partitions; see page 42.

Key A/B/C/D

These options allow you to program the A, B, C and D (quick-set) keys. The procedure is similar to configuring quick-set keys for wired keypads; see page 43.

Zones

You can enable or disable zones that connect directly to a keypad. The procedure is similar to enabling or disabling zones for wired keypads; see page 43.

Internal Prox

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

Wired Zone Type

You can change the zone wiring method for zones connected to the KEY-RKPZ.

Note: This option is available only if the KEY-RKPZ has firmware v5.09 or greater, and the KEY-RKBS base station has firmware v5.07 or greater.

Please refer to the *i-on Installation Manual* for details of the wiring types.

Delete Keypad

Use this menu option to delete a KEY-RKPZ 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 KEY-RKPZ 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.

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 KEY-RKPZ 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.

Please refer to the *i-on Installation Manual* for the maximum number of radio sirens per control unit.

Add/Del Siren

To add or remove an external radio siren:

1. Select *Add/Del Siren*.
2. Select *Panel* (if applicable) or an expander name (if applicable).
3. Select one of the siren numbers (names).
3. If you are adding a siren, select one of the available siren addresses, then activate the tamper switch when prompted or connect power to the siren (please refer to the siren's installation instructions).
4. If you are removing a siren, select the name of the siren to remove.

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.

Supervision

This allows you to enable/disable supervision for individual radio sirens.

When set to *Enabled* (the default), supervision for this siren is the same as the selected option in *System Options – Radio Options – Supervision* (see page 92). When set to *Disabled*, supervision is disabled for this siren.

When a radio device is supervised, the control unit checks for periodic communications from the radio device.

Internal Sounders

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

Please refer to the *i-on Installation Manual* for the maximum number of internal radio sounders per control unit.

Add/Del Sounder

To add or remove an internal radio sounder:

1. Select *Add/Del Sounder*.
2. Select *Panel* (if applicable) or an expander name (if applicable).
3. If you are adding a sounder, select one of the available sounder addresses, then activate the tamper switch in the sounder.
4. If you are removing a sounder, select the name of the sounder to remove.

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).

Supervision

This allows you to enable/disable supervision for individual sounders.

When set to *Enabled* (the default), supervision for this sounder is the same as the selected option in *System Options – Radio Options – Supervision* (see page 92). When set to *Disabled*, supervision is disabled for this sounder.

When a radio device is supervised, the control unit checks for periodic communications from the radio device.

Volume

Use this option to change the volume of chime, entry, exit, alert (such as low battery), confirmation and other tones from a loudspeaker connected to the internal sounder. You can separately adjust the volume of each type of tone. This volume control does NOT change the volume of alarm tones, which are always sounded at full volume.

WAMs

Please refer to the *i-on Installation Manual* for the maximum number of WAMs per control unit.

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:

- You can use the Email Alerts page in SecureConnect to send the images automatically to specified email addresses. For each email address in the Email Alerts page, you can select one or more event types. When a selected event occurs, any images associated with that event that have been captured using a camera trigger are automatically attached to the email.
- Stored images can be viewed through the web interface, using the SecureConnect app, 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 54 onwards):

Fire Alarm
Hold Up Alarm
Burglar Alarm
Technical Alarm
24 Hour alarm
Perimeter
Duress Code (not available for i-on Compact)
Tampers
Full Set
Part Set
Unset
Zone Follow
Zone Alarm
Medical Alarm (by pressing the button on a medical pendant)
Social Emergency (by pressing the button on a social-care pendant)
Social Inactivity

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 4: 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.

To add a radio output:

1. Select *Add Outputs*.
2. Select *Panel* (if applicable) or an expander name (if applicable).
3. Select one of the available output addresses, and follow the prompts.

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 20 for details of how outputs are addressed.

Note: You can delete an output by setting its *Type* to Not Used.

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 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 has been aborted by the user within the abort period. For a partitioned system, you can select the partitions that the output applies to. 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 83):

RF Low Battery (08)

Active when a radio 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 – Hardware – Mains Fail Delay* (see page 89).

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)

(This attribute is not available for i-on Compact.)

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)

(This output type is not available for i-on Compact.)

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. 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)

(This output type is not available for i-on Compact.)

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)

(This output type is not available for i-on Compact.)

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 68 to choose the siren duration.

Strobe (22)

(This output type is not available for i-on Compact.)

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 70).

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)

(This output type is not available for i-on Compact.)

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)

(This output type is not available for i-on Compact.)

The output deactivates five seconds after the setting procedure has started (such as five seconds after an instant set or five seconds after the exit timer starts). Use this output to reset shock sensors (for example, the "Viper"). The normal state of this output is active.

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 type is not available for i-on Compact.)

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.

This output type is available only if a zone has the *Part Set B* attribute set to *On*.

Part Set C (36)

Active when setting Part Set C. Deactivated on unsetting Part Set C.

This output type is available only if a zone has the *Part Set C* attribute set to *On*.

Part Set D (37)

Active when setting Part Set D. Deactivated on unsetting Part Set D.

This output type is available only if a zone has the *Part Set D* attribute set to *On*.

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 62).

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 62).

Masking (41)

(This output type is not available for i-on Compact.)

Active when a detector is giving a mask signal (see page 95).

Autoset Warning (42)

(This output type is not available for i-on Compact.)

Active when the control unit starts the period defined by a calendar set Warning Time (see page 73). 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 that the installer has configured to operate a user-defined output.

When you select this type, you can choose:

- Polarity – See page 61. (Not available for radio outputs.)
- 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 specify 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)

(This output type is not available for i-on Compact.)

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

HUA Confirmed Alarm (48)

Although this output type is always available in the menu, it operates only when BS8243 is enabled.

Active when there is an HUA Confirmed Alarm (see page 83). For a partitioned system, both alarms must be in the same partition as the output.

Lockset Unlocked (49)

(This output type is not available for i-on Compact.)

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)

(This output type is not available for i-on Compact or EU control units.)

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

Although this output type is always available in the menu, it operates only when BS8243 or DD243 is enabled.

HUA Confirm Timer (51)

(This output type is not available for i-on Compact or EU control units.)

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

Although this output type is always available in the menu, it operates only when BS8243 is enabled.

Rearmed (52)

(This output type is not available for i-on Compact.)

The control unit activates the output if the system re-arms at least once after the user armed it.

If *Confirmation Mode* (page 83) 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)

Active when there is a Burg Confirmed Alarm (see page 83). For a partitioned system, both alarms must be in the same partition 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 available for i-on Compact.)

This output type is not currently available. 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 69) or when the system is reset by a user, whichever occurs first.

Medical Alarm (57)

Activates when a "Medical" alarm is generated by pressing the button on a medical pendant.

Social Care (58)

Activates when a "Social Care" alert is generated by pressing the button on a social-care pendant, or insufficient activity during social-care monitoring (see page 99).

Zones Shunted (70)

(This output type is not available for i-on Compact.)

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)

(This output type is not available for i-on Compact.)

Active when the system or a partition allocated to this output is in entry mode.

Exit Only (72)

(This output type is not available for i-on Compact.)

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

Chime Tone Mimic (73)

(This output type is not available for i-on Compact.)

Active when any zone with a chime attribute is active.

Alert Active (74)

(This output type is not available for i-on Compact.)

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)

(This output type is not available for i-on Compact.)

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)

(This output type is not available for i-on Compact.)

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 63.

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.

Latched

Used for the User Defined output type - see page 58.

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 PIR Set Latch, Shock/Smoke Sensor Reset, Setting/Unset Complete, User-Defined and Courtesy Light.

Partitions

This option is available in partitioned systems only, and for most output types. By default, the outputs are assigned to all partitions.

Delay
This is available 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 available 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.)

Zones
This option is available for *Zone Follow* and *Zone Alarm* output types. Select the zones that apply

Wired Outputs

(This option is not available for i-on Compact.)

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 54).

Note: Please refer to page 20 for details of how outputs are addressed.

Plug-By Outputs

(This option is not available for i-on Compact.)

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 54).

See page 156 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 67).

See page 79 for details of the Remote Reset input of the plug-by communicator port.

Plug-by Outputs on a Remote Power Supply

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

Custom Outputs

(This option is not available for i-on Compact.)

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 54).

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.

Please refer to the *i-on Installation Manual* for the maximum number of custom outputs per control unit.

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 5: 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. You can configure different settings for the full-set level and each part-set B/C/D level.

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. In the *Partitions* menu, you can configure different settings for the full-set and part-set levels.

The *Setting Options* and *Partitions* 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 19. Changes to some of the defaults may render the system non-compliant.

Full Set, Part Set and Partition options

Name and Full Set Name

Use this option to give the full set, part set, or partition a name.

For a partitioned system:

- Keypads display the partition name when displaying a list of partitions, such as when you are choosing which partition a zone is in, and when selecting a partition to set.
- The *Full Set Name* and *Part Set B/C/D* names (the latter are available only if a zone has a Part Set B/C/D attribute) are displayed in the setting procedure (to choose whether to full set, or to set a part set), and while the system is counting down during a timed set. They are also displayed in the log when choosing to view additional information about a relevant event, and in Eaton SecureConnect.

For a part-setting system:

- The *Full Set* and *Part Set B/C/D* names are displayed in the setting procedure (to choose whether to full set or when selecting a part set to set), and while the system is counting down during a timed set. They are also displayed in the log when choosing to view additional information about a relevant event, and in Eaton SecureConnect.

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 Options – User Access – 2W Set Instant* option to *NO* (page 77).

Timed Set

Use this setting to make the system set after a delay. Use *Exit Time* (see page 66) 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:

- For partitioned systems, include a zone of type Final Exit in the partition.
- 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 71).

Instant Set

The system sets immediately and without any setting tone. Keypads and loudspeakers (but not internal radio sounders), give confirmation tone when the system is set or unset.

Keypads, loudspeakers and internal radio sounders give the entry tone.

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 or setting tones over keypads, internal radio sounders and loudspeakers.

Keypads, loudspeakers and internal radio sounders give the entry tone.

When the system unsets, keypads (but not loudspeakers or internal radio sounders) give a double-beep confirmation tone.

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

Lock Set

(This option is not available for i-on Compact.)

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 31) that is activated by a suitable lock (located on the final exit door).
- Configure a Final Exit zone (see page 27) connected to the final exit door.

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 66) expires, the control unit sets the system and converts the Final Exit zone 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 84) to Never in order to disable confirmation and comply with BS8243.

Exit Terminate

(This option is not available for i-on Compact.)

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 30).

b) By presenting a proximity reader tag to a KEY-EP external proximity reader connected to a suitable keypad. This requires *System Options – User Options – User Access – Terminated Set* to be set to Y (page 77).

When the user starts the setting sequence, the exit tone is sounded and the exit time does not expire. Once the user completes the setting sequence, the system sets when the *Settle Time* (page 66) expires.

Unsetting: The user can unset (e.g. a 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 indicate that they are settled.

Confirm Set

This option is available only if *Exit Mode* is set to Instant Set. Selecting On causes an audible confirmation beep at the end of the *Exit Time*. Selecting Off causes no audible confirmation beep at the end of the *Exit Time*.

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.

Extended Entry Time

This defines the entry time for Final Exit zone types that have the *Extended Entry Time* attribute enabled (see page 36).

Linked Zone Time

This defines the time within which two zones that have the *Linked Zone* attribute must activate to trigger an alarm. See page 36. This option is available only if there is a zone that has the *Linked Zone* attribute.

Alarm Response

Note: In a part-setting system, this is available only for a part set. The response for a full set is always Siren + Comms.

Internal

Keypads, internal radio sounders and loudspeakers.

Siren

External sirens, keypads, internal radio sounders and loudspeakers.

Siren + Comms

Communication, external sirens, keypads, internal radio sounders and loudspeakers.

Note that any Siren Delay (see page 70) applies to Siren+Comms, but not Internal or Siren alarm responses.

HUA Response

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

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

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.
- *HUA Keys Active* (page 76) must be enabled to generate HUA alarms from keypads.

Audible

The control unit starts HUA alarm tones from keypads, internal radio sounders and loudspeakers assigned to the partition in which the alarm occurs, operates HUA outputs assigned to the partition, and activates any sirens. The sirens follow the *Siren Time* (see page 68). The other sounders operate until a user silences the alarm.

Silent

The control unit keeps the HUA alarm silent: there are no alarm tones, and any sirens or HUA outputs remain inactive.

Displayed

All keypad displays show an 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 display scrolls through the alert messages at approximately one-second intervals.

The control unit also starts HUA alarm from keypads, internal radio sounders and loudspeakers assigned to the partition in which the alarm occurs, operates HUA outputs assigned to the partition, and activates any sirens.

PZ Unset Response

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

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

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

Silent

Activation inserted into non-mandatory log.

No keypads, internal radio sounders or loudspeakers activate.

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.

Keypads, internal radio sounders and loudspeakers activate.

Outputs of type Perimeter and Perimeter Timer activate.

Sounds 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.

Keypads, internal radio sounders, loudspeakers and external sirens activate.

Outputs of type Perimeter and Perimeter Timer activate.

Sounds 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 radio sounders, loudspeakers and external sirens activate.

Outputs of type Perimeter and Perimeter Timer activate.

Communications active.

Sounds 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.

No Action

The control unit will take no action.

Log Only

The control unit will insert activations into non-mandatory log only.

PZ Set Response

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

Note: For a part-setting system, this option appears in *System Options – Perimeter Options*. In a partitioned system, each partition can have different response. In a part-setting system, this option applies to the complete system.

Silent

Activation inserted into non-mandatory log.

No keypads, internal radio sounders or loudspeakers activate.

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.

Keypads, internal radio sounders and loudspeakers activate.

Outputs of type Perimeter and Perimeter Timer activate.

Sounds 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.

Keypads, internal radio sounders, loudspeakers and external sirens activate.

Outputs of type Perimeter and Perimeter Timer activate.

Sounds 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.

Keypads, internal radio sounders, loudspeakers and external sirens activate.

Outputs of type Perimeter and Perimeter Timer activate.

Communications active.

Sounds 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.

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

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.

Siren Delay

You can use this option to delay the sounding of a confirmed alarm.

If *System Options – Confirmation – Sounder On* is set to Confirm (see page 85), *Siren Delay* delays the sound at keypads, internal radio sounders and loudspeakers for the specified period after the confirmed alarm.

If *System Options – Confirmation – Siren On* is set to Confirm (see page 86), *Siren Delay* delays the sound at external sirens for the specified period after the confirmed alarm.

The system then operates the siren and sounders for the programmed *Siren Time*. See also "Sounder and siren operation" on page 85.

Note:

- *Siren Delay* has no effect if *Alarm Response* (page 67) is not set to Siren + Comms, or if a line fault is detected.
- 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 switch off whichever is sooner: the *Siren Time* or the time set locally at the siren (as described in 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 sirens. The outputs/strobes are active for ten seconds after the system 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 sirens. The outputs/strobes are active for ten seconds after the system unsets.

Part Set B/C/D

The Part Set B menu is available only if the partition has at least one zone that has a Part Set B attribute. The same applies to the Part Set D and Part Set D menus.

Name, Exit Mode, Settle Time, Confirm Time, Confirm Set, Exit Time, Entry Time, Alarm Response, Siren Delay, 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. If set to Final Exit, any zones of type Final Exit with Part Set B, C or D attributes continue to act as Final Exit zones during part setting. If set to Normal Alarm, any zones of type Final Exit with the Part Set B, C or D attributes 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. If set to Entry Route, 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. If set to Final Exit, any zones of type Entry Route zones with the Part Set B, C or D attributes act as Final Exit zones during part setting.

Strobe on Set and Strobe on Unset

These options control strobe behaviour when the system is part set. Please refer to *Strobe on Set* and *Strobe on Unset* on page 70.

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 the virtual keypad in the web interface or from the SecureConnect app.

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 option is not available for i-on Compact.)

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 the system. If the system is a partitioned system, you can use this option 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.

Please refer to the *i-on Installation Manual* for the maximum number of events and exceptions the control unit can store.

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

Note:

- You should not program an event to change the system/partition directly from one part set level to another. You should 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 01 part sets the system (or a partition), do not program event 02 to full set the system. Instead, program event 02 to unset the system and then use event 03 to full set the system.
- If you create an event to unset the system or partition, and another event to set or part set the system or same partition again, you must allow for the setting event's *Warning Time*. For example, if the *Warning Time* is 10 minutes (the default), the setting event must not occur within 10 minutes of 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. When the control unit country is set to the UK (see page 10), this time is 01:00 to 02:00. When the country is not the UK, 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.
- Setting does not take place if the control is in installer mode (i.e. if an installer is logged in).

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 displayed current 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 B/C/D (part set) or Unset.

In a part-setting system, select one of: Full Set, Part Set B/C/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, internal radio sounders 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 58).

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 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.

Force Set

You may wish a calendar set to set the alarm system even if one or more zones are active or have faulty detectors. This is known as a "force set". The detectors that are active or are faulty must have the *Force Set Omit* attribute set to Yes. When a force set occurs, the system omits the active or faulty zones and sets the remaining zones normally. An "Autoset omitted zone" message is displayed when the system is unset.

Note: If you enable *Force Set*, the system does not comply with EN50131. Set *Force Set* to OFF if your preference is for a set fail to occur when zones are active during setting.

Off

The calendar set cannot force set the system, even if you have applied the *Force Set Omit* attribute to affected zones.

On

The calendar set can force set the system.

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 or part of the system is about to set.
- Press ✘ to allow the setting event to proceed.
- Press ✔ to defer setting for 30 minutes. Note that for a partitioned system, 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 a user defers a setting event, the control unit halts the warning timer, and defers setting 30 minutes from the start of the warning time. At that time, the control unit starts counting

down the warning timer again. The user can defer setting 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.

Chapter 6: 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 19. Changes to some of the defaults may render the system non-compliant.

User Options

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 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.

HUAs have an alarm sound that is distinct from other alarm types.

Note:

- An HUA confirmed alarm can be generated by settng *System Options* – *Confirmation* – *Confirmation Mode* to BS8243. Please refer to page 84 for details about how an HUA confirmed alarm can be generated.
- To enable HUAs from a FOB-2W-4B or an i-FB01s in UK control units, you must set *System Options* – Confirmation – *Confirmation Mode* to Basic (see page 83). Other country variants 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 quick set, 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 key.

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 33).

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). This option is available after a remote control has been assigned to a user.

2W Set Instant

Use this option to specify how a two-way remote control unit (FOB-2W-4B) sets the system. This option is available after a remote control has been assigned to a user.

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 64).

Duress Enable

(This option is not available for i-on Compact, as i-on Compact does not have the Duress user type.)

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. The option is not available for i-on Compact.)

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 – Partition n – 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.

Tamper Omit

If a user omits a zone, it may be necessary also to omit the tamper belonging to that zone.

Yes – The tamper is omitted when a user omits a zone.

No – The user cannot omit a tamper on a zone.

Silence Alerts

This option controls the length of time that keypads, internal radio sounders and loudspeakers give the alert tone (a brief ‘beep’ every second) when there is an alert.

Note:

- Some alerts are associated with a specific part of the system (such as an alert generated by a detector of type Technical Alarm that is in a part set or partition). Other alerts are associated with the whole system (such as an alert generated by a low backup battery). **An alert is not sounded if all parts of the system the alert is associated with are set.**

- In a partitioned system, the alert can be sounded only at those devices that belong to the same (unset) partition as the alert. This means that if you hear the alert at, for example an internal radio sounder, the sounder must belong to the same unset partition as the alert, or if the alert is associated with the whole system, the sounder must belong to an unset partition. Note that by default, a loudspeaker belongs to all partitions.
- Keypad navigation keys glow red when there is an alert sounded at the keypad (or if there would have been an alert sounded if had not been for the selection of No Alert Tones).

User Code – The alert tone is sounded until a user keys in an access code to acknowledge the alert.

30/60/120 minutes – The alert tone is sounded for the selected time. The alert tone stops if a user enters a valid access code.

No Alert Tones – There is no alert tone.

Wi-Fi Setup

This option is available only if a COM-DATA-WIFI or COM-DATA-4G-WIFI module is fitted.

Yes – Causes the *Network* and *WPS* options (see page 114) to be made available in the master User menu, as well as in the Installer menu. This allows master users to choose the Wi-Fi network to use for the control unit.

No – Prevents the *Network* and *WPS* options from appearing in the master User menu. The options will be available only in the Installer menu

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 83).

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 79, and "CSID Code" on page 79.

Note: Users can reset the system if they unset the system during an alarm, but before the Alarm Abort period has expired (see page 87).

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 4V to the TR input from an external sounder (not available on i-on Compact).
- Detecting Jamming or a Supervision failure when either of these options are set to Tamper see page 92.

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)

(Not applicable to i-on Compact.)

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.

Code Tampers

Yes – The user can reset the system after an alarm caused by a code lockout (see page 12).

No – The installer must reset the system after an alarm caused by a code lockout.

CSID Code

(Remote Reset)

This option is applicable only if Fast Format communications is being used.

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 and sirens 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.

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 13 for editing text.

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:

Users

Defaults (removes) all user access codes, their hold-up devices, proximity reader tags, and remote controls, including for the master user. You are prompted to enter a new code for the master user.

You can also choose whether to use 4-digit or 6-digit codes. Six digit access codes are required for security grade 3.

If you change from 4-digit to 6-digit codes, two additional zeros are added to the end of the existing installer code. If you change from 6-digit to 4-digit codes, the final two digits are removed from the end of the existing installer code.

To comply with EN 50136-2, 6-digit access codes must be configured for access to SPT functions at level 2, 3 and 4.

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.

User 001

Defaults (removes) the master user settings, including the user access code, proximity reader tag, remote control, remote password, etc. You are prompted to enter a new code for the master user.

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.

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

This 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 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 9).

   Note: If you change the grade, you are informed that all user codes will be defaulted.

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. For all control units except i-on Compact, the system scans the bus and finds the devices (see page 38).

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 112). Note that you will also have to use *User Menu – System Config – Facilities On/Off – Remote Access* to enable remote access.

Part Set Mode / Partition Mode

Part Set Mode

This option is displayed if your system is a partitioned system. Selecting this option converts the system to a part-setting system.

The conversion ignores zone allocation to partitions, but uses zone allocation to part sets. For example:

- A zone that is in one or more partitions and has no *Part Set B/C/D* attributes set, converts to a zone that has no part sets.
- A zone that is in one or more partitions and has *Part Set B and Part Set C* attributes set, converts to a zone that is in part sets B and C.

The *Exit Mode*, *Entry Time* and other settings for the Setting Options menu are taken directly from the settings belonging to partition 1 only. This includes the part set B/C/D settings.

Similarly, programmable key actions, remote control actions and calendar set actions automatically convert so that they are valid for the new mode.

Note: It is essential to check system configuration fully after conversion.

Partition Mode

This option is displayed if your system is a part-setting system. Selecting this option converts the system to a partitioned system. All zones will be allocated to partition 1 only.

The *Exit Mode*, *Entry Time* and other settings for partition 1 in the Partitions menu are taken directly from the equivalent Setting Options in the part-setting system (including the part set B/C/D settings). The settings for partitions 2, 3 and 4 are set to the factory-default states.

Similarly, programmable key actions, remote control actions and calendar set actions automatically convert so that they are valid for the new mode.

Note: It is essential to check system configuration fully after conversion.

Installer Options

Installer Name

The installer name is recorded against installer events in the log. When viewing the log, you can toggle between showing the user (installer) number and name using left/right keys.

Inst Tel Number

You can specify the installer's telephone number. This is displayed when selecting *About – Installer*.

Installer Email

You can specify the installer's email address. This is displayed when selecting *About – Installer*.

Inst Contract Num

You can specify the installer's service contract number or other number used by the installer to identify a service agreement. This is displayed when selecting *About – Installer*.

Installer Code

This code allows you to enter the Installer menu (which also carried out an Installer reset).

The Installer code does not allow you to set or unset the system.

You also need to use this code when logging in to the web interface.

Installer Remote Password

Logging on to the web interface (see page 17) as the installer requires the installer's access code followed by the remote password.

Note: Master users can also access the web interface. A master user's remote-access password can be configured in the User menu.

Installer Timeout

The installer is automatically logged out of the Installer menu or web interface if there is no activity after the specified period.

Service Date

This option allows you to specify the date when the next maintenance service of the system is due. If *Service Banner* is enabled, the message "SERVICE REQUIRED" is displayed at keypads up to four hours after the start of the *Service Date*.

Service Banner

Enabling this option allows the "SERVICE REQUIRED" message to be displayed at keypads on the date specified by *Service Date*.

Confirmation

The options in the *Confirmation* menu depend on the *Confirmation Mode* you select.

Confirmation Mode

The options in *Confirmation Mode* depend on the country selected during the initial power up (see page 10):

- If the country is anywhere other than the UK, Basic confirmation mode is always used.
- If the country is the UK, *Confirmation Mode* contains three options: *Basic*, *DD243* and *BS8243*.

The setting for *Confirmation Mode* determines the events the control unit requires to create a "confirmed alarm":

- Basic (default and only setting if the country is not the UK) – A confirmed alarm is generated when a second zone alarm is activated while the system is in an alarm state. (Basic confirmation mode does not use a confirmation timer, and therefore the second activation can occur after the first.)
- BS8243 or DD243 (if the country is the UK) – A confirmed alarm is generated when a second zone alarm is triggered within the period of the confirmation timer setting (*Confirmation Time* or *HUA Confirm Time*, as applicable). 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 generate a Burg Confirmed Alarm.
  - BS8243 – One zone not on the entry route must be triggered to generate a Burg Confirmed Alarm.

Confirmed Alarm Output Types

The following output types are available:

- Confirmed Alarm (page 55) – Generated when there is a Burg Confirmed Alarm and/or an HUA Confirmed Alarm, as below.
- Burg Confirmed Alarm – Generated when any two of the following alarms have activated (in any order) while the system is set (subject to the entry timer not expiring, as described above):

  Normal Alarm

  24 Hour Alarm

  Entry Route

  Tamper (this must be on a different zone from the other alarm)

  For BS8243 and DD243 confirmation modes, the two alarms must occur within the *Confirmation Time*.

For a partitioned system:

- Both alarms must be in the same partition.
- The Burg Confirmed Alarm output type must be in the same partition as the two alarms.

- HUA Confirmed Alarm (operates only when BS8243 is enabled) – Generated when users have activated two separate Hold Up Devices (HUDs), or an HUD and tamper (in either order). For an HUD and tamper, the tamper must be on a different zone from the HUD alarm. The two alarms must occur within the *HUA Confirm Time.*

  For a partitioned system:

  - Both alarms must be in the same partition.
  - An output of type HUA Confirmed Alarm activates if it is in the same partition as the two alarms.

Note:

- A confirmed alarm is communicated only when the *Alarm Response* is set to Siren+Comms (see page 67).
- The Master User can enable or disable hold-up functions for all FOB-2W-4Bs and i-FB01s by using *User Menu – System Config – Remotes – HUA Function*. This requires Basic confirmation mode and is not compliant with DD243 or BS8243.

Confirmation Time

This is available only when *Confirmation Mode* is set to DD243 or BS8243.

The option determines the length of the confirmation time for Burg Confirmed Alarms. You can select any time between 1 and 60 minutes. Confirmation times less than 30 minutes do not comply with BS8243 or DD243.

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.

After Entry

This is available only 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 only 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, keypads, internal radio sounders and loudspeakers give the alarm sound when an unconfirmed alarm occurs.

Confirm

When the system is set, keypads, internal radio sounders and loudspeakers do not give the alarm sound 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 sounder and siren operation is described in Table 6.

Table 6: Sounder and Siren Operation

Settings		Effect
Sounder On	**Siren On**	
Unconfirm	Unconfirm	Unconfirmed alarm: keypads, internal radio sounders, loudspeakers and sirens sound immediately and run for the *Siren Time* (see page 70). Confirmed alarm: the control unit restarts the alarm sound at all devices, which runs for the full *Siren Time*, even if that had expired earlier.

Unconfirm	Confirm	Unconfirmed alarm: keypads, internal radio sounders, and loudspeakers sound immediately and run for the *Siren Time*. Confirmed alarm: the control unit waits for any *Siren Delay* (see page 70), and then starts the alarm sound at sirens and restarts the sound at all keypads, internal radio sounders and loudspeakers. This runs for the *Siren Time*.
Confirm	Confirm	Unconfirmed alarm: No alarm sounds. Confirmed alarm: the control unit waits for any *Siren Delay*, and then starts the alarm sound at all keypads, internal radio sounders, loudspeakers and sirens. This runs 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 sounders and sirens is described in Table 6.

Unconfirmed Reset

This is available only when *Confirmation Mode* is set to DD243 or BS8243. The setting for this option overrides *System Options – User Options – User Reset – Zone Alarms* (see page 78).

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 87), 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 only when *Confirmation Mode* is set to DD243 or BS8243. The setting for this option overrides *System Options – User Options – User Reset – Zone Alarms* (see page 78).

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 87), the alarm will not require an installer reset.

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 67 for a description of this option.

HUA Confirm Time

This is available only 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 only 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 Scantronic'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 93 and Supervision on page 92.)

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.

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 55) and starts any Alarm Abort Fast Format communications programmed.

Auto Rearm

This option is available when *Confirmation Mode* is set to Basic.

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.

Hardware

Panel Name

You can use this option to give the control unit a name. The name is displayed only when using the *About, Panel* option (page 129) and in the Welcome page of the control unit's web interface.

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 80).

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 the *i-on Installation Manual* for details of the wiring types.

On-board Speaker

(This option is available only for i-on Compact.)

Volume

This allows you to set the volume of the keypad's sounder located inside the control unit.

Note: Changing the setting affects only the volume of entry/exit, alert and other advisory tones; it does not affect the volume of alarm tones.

Partitions

In a partitioned system, you can assign the keypad's sounder to any of the partitions.

Panel Loudspeaker

Volume

Use this option to change the volume of chime, entry, exit, alert, confirmation and other tones from a loudspeaker connected to the control unit. This volume control does NOT change the volume of alarm tones. You can separately adjust the volume of each type of tone.

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.

A/C Fail Reporting

(This option is available only for i-on Compact.)

This determines how the control unit monitors the AC mains supply input.

On

The mains supply is monitored. A loss of supply is reported according to *Mains Fail Delay*, as described below.

Off

The mains supply is not monitored.

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. For SIA communications, mains restored is signalled to the ARC.

External Remote Power Supplies

If the system has a remote power supply fitted (EXP-PSU, EXP-PSU-SM, EXP-PSU-MM or EXP-PSU-LM), 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.

Ext DC Fail Reporting

(This option is available only for i-on Compact.)

This determines how the control unit monitors the DC supply input.

On

The DC supply is monitored. A loss of supply is reported according to *Ext DC Fail Delay*, as described next.

Off

The DC supply is not monitored.

Ext DC Fail Delay

(This option is available only for i-on Compact.)

This option allows you to specify the length of time (0 to 60 minutes) that the control unit must wait after detecting a DC supply failure before generating an alert tone and reporting Ext DC Fail to the ARC.

As soon as the DC supply fails (and *Ext DC Fail Reporting* is enabled), the control unit lights the red alert LEDs around the navigation key. **Note:** The control unit does not show alerts while the system is set.

If *Ext DC Fail Delay* is set to 0, the control unit starts an alert tone nine seconds after the power interruption. If *Ext DC Fail Delay* is set to 1-60 minutes, the control unit starts an alert tone the specified number of minutes after the power interruption.

At the same time as the alert tone, the control unit communicates an Ext DC Fail to the ARC and activates any outputs of type General Fault.

If power is restored before the alert tone, the control unit switches off the alert, logs Ext DC Restore and sends no report to the ARC.

A user can silence the alert by entering a valid access code. The control unit displays details of the alert. General Fault outputs remain active.

Once the DC supply is restored, the control unit logs Ext DC Restore. A user can reset the alert and deactivate any General Fault outputs by pressing entering the access code again.

Comms Antenna

This option is available only if a module that supports mobile or Wi-Fi communications is fitted (e.g. COM-SD-GSM, COM-DATA-4G or COM-DATA-WIFI). Select Internal if the internal antenna is used, or External if an external antenna is used. If the module supports internet connectivity, this option is also in the *Communications – IP Options – Module: 4G/2G* or *Communications – IP Options – Module: Wi-Fi* menu, as applicable. If the control unit uses a plastic enclosure, the default setting is Internal. If the control unit uses a metal enclosure, the default is External.

Panel Tamper Return

(This option is not available for i-on Compact.)

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.

Reset Codes Pins

This option allows you to enable or disable the Reset Codes link on the PCB. If you disable *Reset Codes Pins*, the Reset Codes link cannot be used to reset the installer and master user codes.

Warning: The control unit will need to be replaced if you disable *Reset Codes Pins* and then forget the installer code!

Radio Options

Supervision

When a radio device is supervised, the control unit checks for periodic communications from the radio device.

Note: Supervision can be disabled for individual radio detectors (page 36), internal radio sounders (page 51) and external radio sirens (page 50). If supervision for an individual radio device is disabled, the control unit takes no action if it loses contact with that device (same as the *Off* setting below). Supervision for KEY-RAS radio keypads cannot be individually enabled or disabled; they are always supervised unless the *Off* setting below is used.

Off

> If the control unit loses contact with a radio device (such as a radio detector or internal radio sounder) that is supervised, the control unit takes no action, irrespective of whether the system is set or unset.

Fault

> If the control unit loses contact with a supervised radio device for more than 20 minutes and an attempt is made to set the system, the control unit displays an “RF Warning” message. If the user continues to set the system, the event is logged.
>
> If the control unit loses contact with a radio device that is supervised for more than two hours with the system unset, the control unit logs a "Supervision Fail" event and sounds a fault tone.
>
> If the system set and contact is lost for more than two hours, the control unit logs the alert, but does not display the alert or give an alert tone.
>
> With the system set or unset, any outputs of type RF Supervision or RF Fault activate.

Tamper

> If the control unit loses contact with a supervised radio device for more than 20 minutes and an attempt is made to set the system, the effect is the same as the *Fault* setting – the control unit displays an “RF Warning” message, which is logged if the user continues with the setting procedure.
>
> If the control unit loses contact with a supervised radio device for more than two hours (with system set or unset), the control unit logs a "Supervision Fail" event, starts a tamper alarm, activates outputs of type Tamper, and notifies the ARC with a

"Supervision" message. Any outputs of type RF Supervision or RF Fault also activate, except plug-by RF Supervision and RF Fault outputs if *Tamper as Tamper Only* is enabled (page 87).

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 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.

If *Tamper as Tamper Only* is set to Disabled (page 87), any outputs of type RF Jamming or RF Fault activate. See page 87. If there is no Tamper channel allocated in Fast Format, the system sends an unconfirmed alarm.

Note that the Tamper option is required for PD 6662.

Note: If you choose Tamper and also set *System Options – User Options – User Reset – System Tampers* to No, the user will not be able to reset the system after Jamming event.

Remotes

This menu is available only if the control unit has learnt a remote control.

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.

Force Set

You may wish to allow a user with a remote control to set the alarm system even if one or more zones are active or have faulty detectors. This is known as a "force set". The detectors that are active or are faulty must have the *Force Set Omit* attribute set to Yes. When a force set occurs, the system omits the active or faulty zones and sets the remaining zones normally.

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 Omit* 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 appropriate 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.

Radio Keypads

This menu is available only if the control unit has learnt a radio keypad (excluding KEY-RKPZ).

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.

Force Set

You may wish to allow a user with a radio keypad to set the alarm system even if one or more zones are active or have faulty detectors. This is known as a "force set". The

detectors that are active or are faulty must have the *Force Set Omit* attribute set to Yes. When a force set occurs, the system omits the active or faulty zones and sets the remaining zones normally.

Note: If you enable *Force Set*, the system does not comply with EN50131.

Off – The radio keypad user cannot force set the system, even if you have applied the *Force Set Omit* attribute to any zones.

Confirm – The user can force set the system by pressing the appropriate button on the radio keypad, and when the system does not set, entering the user code and pressing the button again to confirm setting. For a KEY-RAS, enter the user code and press the A/B/C/D key while the ABCD keys are flashing green and red.

On – The user can force set the system by pressing the appropriate button on the radio keypad only once.

Note: The Confirm and On settings do not allow a user with a radio keypad to set the system if a reset is required after an alarm.

Masking Options

(This menu is not available for i-on Compact.)

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 method that is able to report masking, as shown in the *i-on Installation Manual.*

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. On a security grade 3 system, the Installer must reset the Alert. On a security grade 2 system, the ability to reset the alert is governed by the *System Options – User Options – User Reset – System Tampers* option, see page 78. **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 Options – User Reset – Zone Alarms* option, see page 78. 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. On a security grade 3 system, the Installer must reset the Alert. On a security grade 2 system, the ability to reset the alert is governed by the *System Options – User Options – User Reset – System Tampers* option, see page 78.

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.

Perimeter Options

This menu is available only for a part-setting system and if there is a zone of type “Perimeter”. The Partitions menu contains the equivalent options for a partitioned system.

See from *page 68 for* a description of *PZ Unset Response*, *PZ Set Response* and *PZ Reset time*.

Shunt Groups

(This menu is not available for i-on Compact.)

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 35).

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 *Administration and User'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 *Administration and User'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 60).

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 30.

Date and Time

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

If *Communications – IP Options – Cloud Access* is enabled, the control unit synchronises its time through Eaton SecureConnect. If *Cloud Access* is not enabled, you *SNTP Time Sync* to keep the time at the control unit synchronised with the time at the Eaton SNTP (Simple Network Time Protocol) server on the internet.

The control unit uses the country setting (page 10) 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 Interval

Select Daily if you want the control unit to synchronise time daily (every evening), 2 hours to synchronise every 2 hours, or Off to switch off automatic syncronisation.

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.

Updates

Language

Select

This option allows you to select the language used for the menus and options.

Replace

This option allows you to update or replace a language used for the menus and options. The new language file must be in a folder named INSTALL at the root (top) level of the SD card.

Changing the language does not affect any stored names for full/part sets, detectors, outputs or users, and does not change any defaults.

To use this option:

1. Select *Language*.
2. Select *Replace*.
3. Select the existing language version you want to replace.
4. Select the new language located on the SD card.

Panel Upgrade

You can use the option to upgrade the control unit's firmware. The new firmware (.bin) file must be in a folder named INSTALL at the root (top) level of the SD card.

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 web interface.

Note: If you need to update both the language files and firmware, make sure you update the language files first using the *Language* option above. Failure to do this may display an "incompatible language version" message, from which you cannot proceed. If you see this message, try entering your installer code.

To use this option:

1. Select *Panel Upgrade*.
2. The current firmware version is listed and indicated by a *.
3. Use the ▲ or ▼ key to select the new firmware version you want to use from the SD card.
4. Press ✔ to start the upgrade process, and confirm when prompted. During the upgrade, the control unit will restart and the keypad's LEDs may flash red. After the upgrade, the keypad returns to normal standby mode.

Level 4 Update

Setting this option to Enabled allows the control unit to automatically check for firmware and language updates when an installer enters the Installer menu (see page 12). It also allows the level-4 user to update the firmware and language using the web interface, providing *System Config – Facilities On/Off – Level 4 Update* is also enabled in the User menu.

The first time you select Enabled, you are prompted to create the level-4 user by entering a user code and a remote password. There can be only one level-4 user.

Note: If you need to update both the language files and firmware from the web interface, make sure you update the language files first. Failure to do this may display an "incompatible language file" message, from which you cannot proceed.

The level-4 user is also able to log into the User menu or web interface and change the level-4 user name, code and remote password. 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.

Backup/Restore

Backup to SD Card

You can use this option to produce a backup of the complete system configuration stored in the control unit. The backup is created on an SD card fitted in the SD card slot on the control unit's PCB.

You may want to produce a backup if, for example, you need to replace the control unit's PCB and want to restore the exiting configuration on the new PCB.

Note: A backup from an earlier i-on40H can be restored onto an i-on 40H+, and a backup from an earlier i-on30R can be restored onto an i-on 30R+.

Once you have produced the backup, you can use Restore from SD Card to restore the configuration.

The version of the firmware on the new PCB should be the same or greater than the version used on the existing PCB.

The backup is stored in a file on the SD card in a folder named "Config". The filename is in the format YYYY_MM_DD_HHMM. More than one backup can be stored in the Config folder.

Restore from SD Card

You can use this option to restore the complete system configuration backed up using the Backup to SD Card option. The backup must be located in the folder named "Config" on the SD card.

If there is more than one backup, use the ▲ or ▼ key to select the backup you want to restore.

Social Care

This menu allows you to configure:

- Social-care activity monitoring.
- Responses to social-care alerts and medical alarms.

Note: To ensure correct sounds, use firmware v3.00 or later for expanders and remote power supplies, and firmware v5.00 or later for wired keypads.

Start Monitor Hour

Specify the time that you want social-care activity monitoring to start each day.

The system monitors all zones that have the Activity Mon attribute, and generates a social-care alert if no zone triggers at least once every Monitoring Interval within the times specified by Start Monitoring Interval and End Monitoring Interval each day.

Note: A user can manually start a social-care alert by pressing the button on a social-care pendant.

End Monitor Hour

Specify the time that you want social-care activity monitoring to end each day.

Monitor Interval

To cause a social-care alert, at least one detector must trigger within each Monitor Interval. For example, if you set Monitor Interval to 4 hours, at least one detector must trigger every 4 hours between Start Monitor Interval and End Monitor Interval to prevent a social-care alert.

Social Alarm Response

This determines the response to a social-care alert.

Silent

> The control unit keeps the alert silent: there are no alarm tones. The control unit signals the alert using the communications device(s) and activates any outputs of type Social Care.

Audible

> As well as starting communications and operating outputs of type Social Care, the control unit causes internal sounders to beep quietly twice per second for the first 30 seconds, then chirp loudly twice per second. The first 30-second warning period allows a user to cancel the alert before it officially starts. For a partitioned system, only the sounders assigned to the partition in which the alert occurs are activated.

Displayed

> This has the same effect as Audible, but the display also shows the alert without a user needing to enter an access code. If there is more than one alert, the display scrolls through each alert message in turn.

Medical Alarm Response

This determines the response to a Medical alarm.

Silent

> The control unit keeps the alarm silent: there are no alarm tones. The control unit signals the alarm using the communications device(s) and activates any outputs of type Medical Alarm.

Audible

> As well as starting communications and operating outputs of type Medical Alarm, the control unit causes internal sounders to chirp loudly once per second. For a partitioned system, only the sounders assigned to the partition in which the alert occurs are activated.

Displayed

This has the same effect as Audible, but the display also shows the alarm without a user needing to enter an access code. If there is more than one alarm, the display scrolls through each alarm message in turn.

Chapter 7: 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* and *Tel No 2* and *IP Address.*

IP addresses are for ARC reporting over the internet (SIA-IP).

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 via a COM-SD-GSM or COM-SD-PSTN module, or over the internet (via the LAN or a COM-DATA-4G module).

Note: For communication to an ARC over the internet, 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.

Note: The use of a COM-SD-GSM module for ARC communication is not recommended, as the networks often distort the audio tones, which can cause the communication to fail.

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 through a plug-on module or internet.

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 Telecoms 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 Telecoms 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.

Telecoms Priority

If a COM-SD-GSM or COM-SD-PSTN module is fitted, the control unit has more than one communication method to the ARC (LAN and GSM, or LAN 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. You cannot set all priorities to disabled.

Recipients

Use this option to specify the telephone numbers and/or IP address to use to send messages to the ARC. You do this by selecting contacts from the Contacts List (page 102).

Tel. Recipient 1

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 the internet, 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 the internet.

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. Enter only four digits.

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 13.

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, Extended SIA 3 v2 and Extended SIA 3 v3. Extended SIA 3 v3 is similar to Extended SIA 3, except that "^" is used instead of "/" for the ASCII text delimiter.

Fast Fmt Channels

(See Appendix A for a brief description of Fast Format.)

If you selected Fast Format in *Report Type*, you can use *Fast Fmt Channels* to allocate an event to each of eight channels. Table 7 shows the default events for each channel. Table 8 shows the events available. You can key-in the two-digit numbers shown next to each event in order to display that event type.

Table 7: 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 8: Fast Format Events

Event Number	**Meaning**	
	All Control Units except i-on Compact	**i-on Compact**
00	Not used	Not used
01	Fire Alarm	Fire Alarm
02	Hold Up Alarm	Hold Up Alarm
03	Burglar Alarm	Burglar Alarm
04	Open/Close	Open/Close
05	Alarm Abort	Alarm Abort
06	Technical Alarm	Technical Alarm
07	Confirmed Alarm	Confirmed Alarm
08	RF Low Battery	RF Low Battery
09	RF Supervision (see note 4)	RF Supervision (see note 4)
10	RF Jamming (see note 4)	RF Jamming (see note 4)
11	Mains Fail (see note 5)	Mains Fail (see note 5)
12	Tamper (see note 6)	Tamper (see note 6)
13	Open (see note 1)	Open (see note 1)
14	Close (see note 1)	Close (see note 1)
15	Zone Omit (Setting) (see note 2)	Zone Omit (Setting) (see note 2)

16	Zone Omit (System)	Zone Omit (System)
17	General Fault	General Fault
18	Masking	-
19	Zone Shunt (HUA Confirm for i-on Compact)	HUA Confirm (Applicable only to UK panels with Confirmation Mode set to BS8243)
20	Duress Code	Burg Confirm Alarm
21	HUA Confirm (Applicable only to UK panels with Confirmation Mode set to BS8243)	Perimeter Alarm
22	Burg Confirm Alarm	Burg Alarm P1 (partitioned system only)
23	Perimeter Alarm	Burg Alarm P2 (partitioned system only)
24	Burg Alarm P1 (partitioned system only)	Burg Alarm P3 (partitioned system only)
25	Burg Alarm P2 (partitioned system only)	Burg Alarm P4 (partitioned system only)
26	Burg Alarm P3 (partitioned system only)	Medical Alarm (pressing the button on a medical pendant)
27	Burg Alarm P4 (partitioned system only)	Social Emergency (pressing the button on a social-care pendant)
28	Medical Alarm (pressing the button on a medical pendant)	Social Inactivity (see page 99)
29	Social Emergency (pressing the button on a social-care pendant)	Close/Open (see note 7)
30	Social Inactivity (see page 99)	-
31	Close/Open (see note 7)	-

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 – Hardware – Mains Fail Delay* (see page 89 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.
7. Close/Open is an inverted version of the Open/Close channel.

CID/SIA Events

(This menu appears only if you select “Contact ID” or any of the SIA versions in *Communications – ARC Reporting – Report Type*. See Appendix A for a description of the CID and SIA formats.)

Note: Only applicable events are available for i-on Compact.

To make configuration easier, the control unit groups CID/SIA telegrams together into report groups. Table 9 on page 135 lists 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).

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 – ARC Reporting – 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 option appears only if you select Fast Format in *Communications – ARC Reporting – Report Type*, and is relevant only if a COM-SD-PSTN or COM-SD-GSM module is fitted (but not the COM-DATA-4G, as this is for internet connectivity only).

It may take longer for the ARC to acknowledge a Fast Format transmission over a PSTN or GSM network. 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.

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 available, *Static Test Call* is enabled. To use dynamic test calls, disable *Static Test Call* first.

Static Test Call

Note: If this option is not available, *Dynamic Test Call* is enabled. To use static test calls, disable *Dynamic Test Call* 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 COM-SD-PSTN and COM-SD-GSM have a built-in speech dialler, which 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 109), 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 plug-in modules 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

This starts the 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.

Delete Message

This deletes 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 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*.
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. Go back to the keypad and press ✘.
6. If required, replace the control unit lid. **DO NOT** replace the control unit lid until you have left the “Use Lid Tamper” mode.

Test Call

This sends the current message to a telephone number that you can specify.

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 54)

Hold Up Alarm (see page 54)

Burglar Alarm (see page 54)

Technical Alarm (see page 55)

Tampers (see page 56)

Mains Fail (see A/C Fail, page 55)

Soak Test Fail (see page 34)

Medical Alarm (by pressing the button on a medical pendant)

Social Emergency (by pressing the button on a social-care pendant)

Social Inactivity (see page 99)

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

This menu is available only if a COM-SD-GSM or COM-SD-PSTN module is fitted. These are able to send SMS text messages.

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. The following options are displayed only if *Call Mode* is enabled.

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:

Tampers

Includes all types of tampers, including system, keypad, expander, sensor, user code (excess digits), siren, WAM and radio keypad.

Alarms

Includes all types of alarm, including 24 hour, Fire, HUA, Burg, test zone fail, Zone Alarm, Zone Follow, Duress, Social Emergency, Social Inactivity and Medical. This also includes restores from those alarms. See page 51 for details of how Zone Alarm and Zone Follow are configured.

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.

PSTN SMS

If you are sending SMS messages by way of a COM-SD-PSTN module, 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.

Incoming

This option is available only if a COM-SD-GSM module is fitted.

Forwarding

This 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.

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.

For plug-by communications, the control unit monitors for line faults by using the LF input on the plug-by port. The communicator should apply 0V to the LF input if there is no fault, and 12Vdc if a fault is present.

Audible

Scantronic recommends audible response for line fault. If the system is unset, the system logs the event. Keypads, internal radio sounders and loudspeakers produce a short audible tone after *Line Fail Delay* when the line response changes from OK to

fail. Entering a valid access code silences the tone and the display indicates a line fault. The system can be set again with the line fault present.

If the system is set, 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.

Silent

If the system is unset, the keypad display indicates a 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 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 Options

This menu allows you to configure settings to connect the control unit to the LAN and internet. For an overview of the purpose of connecting the control unit to a LAN and to the internet, please refer to page 16.

Cloud Access

This allows you to make the control unit accessible from SecureConnect.

Note: If you want to use SecureConnect, set Enabled (see below) to Yes, and also set up an internet connection using, for example, *Module:Wi-Fi*, *Module:4G/2G* or *Panel Ethernet* in the IP Options menu.

Enabled

If you set Enabled to Yes, you are prompted to specify the Cloud ID (as specified in the SecureConnect web portal) and Site ID (the name you want to give this control unit).

Cloud Time Sync

This specifies how often the control unit should synchronise its time via the SNTP time synchronisation service provided by SecureConnect.

Cloud Push Fail

This specifies how the control unit should react if a push notification (information sent by the server to the control unit) fails. You can choose Disabled (no alert), Silent (silent alert) or Audible (audible alert).

Offline Response

This specifies how the control unit should react if SecureConnect goes offline on all available paths (Ethernet, Wi-Fi and mobile internet, as applicable) and Offline

Reporting is enabled. You can choose Silent (silent alert) or Audible (audible alert). This setting is relevant only if Offline Reporting is enabled.

Offline Reporting

This specifies whether or not the control unit should generate an alert if SecureConnect goes offline on all available paths (Ethernet, Wi-Fi and mobile internet, as applicable). If enabled, Offline Response determines whether the alert is silent or audible. Offline events are recorded in the log, even if Offline Reporting is disabled.

Offline Delay

This specifies how long the control unit should allow SecureConnect to go offline before it carries out the Offline Response.

Module: 4G/3G/2G

This menu is available only if a COM-DATA-4G module is fitted (i.e. a module that supports an internet connection via a mobile network). The option allows you to configure the module and how it is used.

Note: If the option name is *Module:4G/2G*, you are using an older module that does not support 3G.

Data Mode

This option allows you to specify whether to use mobile data only as a backup if LAN communications (Ethernet and/ or Wi-Fi) are not available, or to use mobile data only.

Network Type

You can specify whether to allow the control unit to switch between 4G, 3G and 2G automatically, or to use 4G, 3G or 2G only. If the network does not support 2G or 3G, select 4G Only.

Network Selection

Select Auto if you want the module to select the mobile network automatically, or Preferred if you want to choose the network from a list of available networks.

Provider

Select the mobile provider. This automatically configures the provider's Access Point Name (APN) to access the internet over the mobile network. If your provider is not listed, select Other and specify the APN and login details manually.

Provider is the service provider that supplied the SIM and may not be the same as *Network Selection*. For example, you may have a multi-network SIM from the provider "CSL Group", which may allow access to several networks. In this case, you would set *Provider* to CSL, and if you wanted to use a specific network, such as EE, you would set *Network Selection* to EE.

If you have a single-network SIM, for example provided by Vodaphone, you would set *Provider* to Vodaphone, and *Network Selection* to Auto.

Edit APN

The APN is configured automatically when you select the provider, but in some cases, it may be necessary to edit the APN or your login details if, for example, the provider changes the APN details.

Comms Antenna

Select Internal if the internal antenna is used, or External if an external antenna is used. This option is also in the *System Options – Hardware* menu. If the control unit

uses a plastic enclosure, the default setting is Internal. If the control unit uses a metal enclosure, the default is External.

Primary Path Rpt (Reporting)

This is available only if Data Mode is set to Mobile as Backup. It determines whether or not the control unit generates an alert if the LAN path to the internet (Ethernet and Wi-Fi) go offline. Offline events are recorded in the log, even if Primary Path Rpt is disabled.

Secondary Path Rpt (Reporting)

This is available only if Data Mode is set to Mobile as Backup. It determines whether or not the control unit generates an alert if the mobile path to the internet goes offline. Offline events are recorded in the log, even if Secondary Path Rpt is disabled.

Module: Wi-Fi

This menu is available only if a COM-DATA-WIFI module is fitted (i.e. a module that supports LAN communication via Wi-Fi). The option allows you to configure the module, including the Wi-Fi network it connects to.

Network

This option allows you to select the Wi-Fi network to use. The signal strength of each network is shown in brackets.

An asterisk (*) displayed next to a network name indicates that it is the selected network; it does not indicate connection status.

Enter the password when prompted; use:

- 1-9 keys to enter numbers and letters, as labelled on the keys. For example, use the “2” key to enter A, B, C or 2.
- # to change between upper/lower case.
- 0 to enter 0, space, or other character (e.g. “&”, “@” and “/”).
- The Menu key to show the password when entering.
- ▲ or ▼ to move the cursor left or right, ▶ to add a space, or ◀ to delete the previous character.

A "Connected" message is displayed if the connection is successful.

Note: The *Network* and *WPS* options are also available in the master User menu if *System Options – User Options – User access – Wi-Fi Setup* is enabled in the Installer menu.

WPS

Select this option if you want to connect using WPS. When you see “Waiting to connect”, press the WPS button at the router. If no connection is made within two minutes, the control unit cancels the procedure.

DHCP

Set *DHCP* to *Enabled* if want the Wi-Fi module to acquire a DHCP-assigned IP address. Set *DHCP* to *Disabled* if you want to enter a specific IP address yourself.

Note: If you are using DHCP, you can use *About – Comms – Module – IP Address* to find out the IP address the module is using.

Setting *DHCP* to *Disabled* causes the following additional options to be displayed in the menu:

- IP Address – Specify the module's IP address (e.g. “192.168.000.100”). Press “*” to key in a dot.

- 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).
- DNS IP Address – Enter the IP address of the DNS server on the network.

Comms Antenna

Select Internal if the internal antenna is used, or External if an external antenna is used. This option is also in the *System Options – Hardware* menu. If the control unit uses a plastic enclosure, the default setting is Internal. If the control unit uses a metal enclosure, the default is External.

Module: 4G/3G/2G/Wi-Fi

This menu is available only if a COM-DATA-4G-WIFI module is fitted (i.e. a module that supports LAN communication via a mobile network or Wi-Fi). The option allows you to configure the module, including the Wi-Fi network it connects to.

4G/3G/2G

This contains the same options as for a COM-DATA-4G module to configure the settings for 4G, 3G or 2G communication. Please refer to *Module: 4G/3G*/2G on page 113.

Wi-Fi

This contains the same options as for a COM-DATA-WIFI module to configure the Wi-Fi settings. Please refer to *Module: Wi-Fi* on page 114.

Panel Ethernet

This menu allows you to configure the control unit's Ethernet connection to the LAN (if used).

DHCP

Set *DHCP* to *Enabled* if want the control unit to acquire a DHCP-assigned IP address. Set *DHCP* to *Disabled* if you want to enter a specific IP address yourself.

Note: If you are using DHCP, you can use *About – Comms – Panel Ethernet – IP Address* to find out the IP address the control unit is using.

Setting *DHCP* to *Disabled* causes the following additional options to be displayed in the menu:

- IP Address – Specify the control unit’s IP address (e.g. “192.168.000.100”). Press “*” to key in a dot.
- 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).
- DNS IP Address – Enter the IP address of the DNS server on the network.

LAN

This menu allows you to configure the control unit’s built-in web interface (see page 17).

Web Server

The following options are available:

- Status – Choose whether to enable or disable the built-in web interface. Note that this does not affect access from SecureConnect.

- Port – This is the port that the control unit uses for the built-in web interface. The option is displayed only if *Status* is *Enabled*. The default is 80.
- User Timeout – A master user of the web interface is logged out automatically if there is no activity for the length of time specified by User Timeout. (This setting does not affect the timeout of the virtual keypad itself, which is fixed at one minute.)

Send Tamp As Burg

When using CID or SIA reporting to an Alarms Receiving Centre (see page 102) or a plug-by communicator, this option allows you to program the control unit to send tampers as alarms to the ARC.

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.

Chapter 8: Test Menu

Sirens and Sounders

This option allows you to test all the warning devices. For most options, you can choose to operate all warning devices assigned to a specific partition (if a partitioned system is used), 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 device 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.

On-board Sounder

(This option is available for i-on Compact only.)

You can use this option to test the built-in sounder in the control unit. The sounder is used, for example, for setting, unsetting and alarm tones.

Wired Sirens

(This option is not available for i-on Compact.)

This option allows you to operate all outputs of type Siren and Strobe.

The *Remote Self-Test* option is available in grade 3 systems for sirens such as the SDR-WEXT that have a remote self-test feature. The test checks the condition of the siren's battery and sounder. The siren reports the results through a zone of type "External WD Fault". For further information, please refer to the siren's installation instructions.

Loudspeakers

(This option is not available for i-on Compact.)

You can use this option to test the sound from loudspeakers, keypads and internal radio sirens connected to the system.

Wired Keypads

(This option is not available for i-on Compact.)

Use this option to test the sounders on the wired keypads.

KEY-RKPZ

(This option is not available for i-on Compact.)

Tests the sounders in KEY-RKPZ two-way radio keypads.

KEY-RAS

Tests the sounders in KEY-RAS two-way radio keypads.

Internal Sounders

Tests any internal radio sounders (SDR-RINT) that the control unit has learned.

Wired Keypad

(This option is not available for i-on Compact.)

Use this menu option to test the keypad you are currently using (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.

Press ✘ to leave the test.

On-board Keypad

(This option is available for i-on Compact only.)

Use this menu option to test the keypad at the control unit.

When you start the test, 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.

Press ✘ to leave the test.

Radio Keypads

This option allows you to test the keys on i-rk0, KEY-RAS and KEY-RKPZ radio keypads.

i-RK01

Note: For i-on Compact, start the test from the keypad on the control unit. For other control units, start the test from any wired keypad. When you press a key at the radio keypad, the display of the keypad where you started the test should show the key you pressed.

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 keypad from which you started the test should show the appropriate letters.

b) Press both keys of the two-button HUA. The display should show “Hold Up Alarm Key”.

c) Press the Unset key. The display should show “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 display should show “4567A”.

Note: You cannot test the “*” and “#” keys on an i-RK01 radio keypad.

KEY-RAS

Note: For i-on Compact, start the test from the keypad on the control unit. For other control units, start the test from any wired keypad. When you press a key at the radio keypad, the display of the keypad where you started the test should show the key you pressed.

a) Press four or six numeric keys one after the other, followed by the A, B, C or D key. The display of the keypad from which you started the test should show the appropriate keys pressed. Repeat this step until you have tested all numeric and A, B, C D keys.

b) Press four numeric keys one after the other, followed by unset key. The display should show “System Unset Key” and the numeric keys you pressed.

c) Wait for all LEDs on the KEY-RAS to switch off, then press four numeric keys one after the other, followed by query key. The display should show “Query Status” and the numeric keys you pressed.

d) Press both keys of the two-button HUA. The display should show “Hold Up Alarm Key”.

KEY-RKPZ

(This option is not available for i-on Compact.)

Use this menu option to test the KEY_RKPZ keypad you are currently using (you cannot test a keypad remotely).

This test behaves the same as for a wired keypad.

Expanders

(This menu is not available for i-on Compact.)

The Expanders menu allows you to test individual expanders.

Radio and wired expanders

Spare Zones

This option shows the number of zones of type Not Used on the expander.

12V Input Voltage

This option shows the voltage on the 12V line in the bus cable, at the connection to 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.

Remote Power Supplies

(EXP-PSU, EXP-PSU-SM, EXP-PSU-MM and EXP-PSU-LM)

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 (EXP-PSU, EXP-PSU-MM and EXP-PSU-LM only) . A value other than 13.6V may indicate that there is either a mains fail or that the expander is running on its standby battery.

Aux1 Voltage

This option shows the voltage on the 12V line of the Aux 1 terminals.

Aux2 Voltage

This option shows the voltage on the 12V line of the Aux 2 terminals (EXP-PSU, EXP-PSU-MM and EXP-PSU-LM only).

Comms O/P voltage

This option shows the voltage on the 12V positive terminal of the plug-by communications connector (EXP-PSU and EXP-PSU-LM only).

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 (EXP-PSU, EXP-PSU-MM and EXP-PSU-LM only).

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 or EXP-PSU-LM connected to the system and have enabled its battery 2 in *Detectors/Devices – Wired Expanders – Edit Expander* (see page 40). The option shows “Healthy”, “Low” and “Missing” with the same meanings as in Battery 1 Status.

System Current

This option displays the current used by the remote power supply itself. This option is available for the EXP-PSU-SM only.

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, 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: You can use *Walk Test* to test wired HUA switches. While you are using the Installer menu, activating a wired HUA switch will not cause an 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.

If at least one zone is tested successfully, the log records a "Walk Test Complete" event, which shows the number of zones tested against the total number of zones system-wide.

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

(This option is available only for partitioned systems.)

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

(This option is not available for i-on Compact.)

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

(This option is available only for systems that have wired zones.)

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.

Zone Status

Wired Zones

You can use this option to display the current status of each zone. Select the zone you want to check. The zone status (OK, alarm, masked, fault or tamper) is shown in the bottom-right corner of the display. Masked and fault statuses are for zones that use the resistor configuration for FSL zones with masking (as described in the *i-on Series Installation Manual*).

Radio Zones

For radio zones, the Supervision status displays "OK" if the control unit has received communication from the detector in the last 20 minutes. The status changes to "Warn" if there has been no communication for more than 20 minutes, and then "Fail" if there has been no communication for more than two hours (see page 92).

By pressing ◄ or ►, you can also display:

- The signal strength. For example, 7(6) means the current signal strength is 7 (out of 9), and the lowest recorded signal strength since the last reset is 6.
- The battery state (OK or Low).

Signal Strengths

This option allows you check the received signal strength from all the radio transmitters belonging to the system.

The 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”, 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 a plug-by output 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.

Remotes

This allows you to test user's remote control. The 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 display shows the remote's identity, the button you pressed ("S" = Set, "U" = Unset, "?" = Query, and "*" = Part Set or programmable) and the user it is assigned to.

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.

Pendants

This allows you to test a user's medical or social-care pendant. The display shows a message prompting you to press a button on the pendant.

Press the pendant's button. The display shows the pendant's identity, the user it is assigned to, the function of the pendant and the signal strength.

User HUDs

This allows you to test user HUS (Hold-Up Devices). You must have the HUD to carry out the test.

The keypad display shows a message prompting you to press the HUD buttons.

Press the HUD buttons, both at the same time. (The alarm system will not start a hold-up alarm as a result.)

The keypad display shows the owner of the HUD. 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 proximity tag up to the sensor on the keypad.

The keypad display shows the user number and name of the proximity tag owner.

ARC Reporting

This option allows you to send a test call to either of the two recipients you have programmed to receive alarm information. ARC reporting must be enabled (see page 102).

After selecting *ARC Reporting*, select the recipient.

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. Press ✘ to abandon 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 COM-SD-PSTN or COM-SD-GSM plug-on module and speech dialling is enabled (see page 108).

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 COM-SD-GSM or COM-SD-PSTN plug-on module and SMS is enabled (see page 110).

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).

PSU Current

(This option is not available for i-on Compact.)

Panel

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.

Exp. Wn-...

If the system has a remote power supply connected, this option displays the current used by the remote power supply itself.

Panel PSU

(This option is available for i-on Compact and i-on20R only.)

This option allows you to test:

- The voltage of the external DC input.
- The voltage of the backup battery installed in the panel.
- The voltage at the terminal marked "12V WIFI" in the control unit, which powers an i-wifi01 Wi-Fi module (i-on Compact only).
- The voltage at the terminal marked "12V BELL" in the control unit, which powers an external wired siren (i-on20R only).

Battery(s)

(This option is available for i-on Compact only.)

This option allows you to perform a battery load test. When you see the *Panel* option, press ✔ to start the test. You will see either “Pass” or “Fail”.

Locate Panel

(This option is not available for i-on Compact.)

This option allows you to locate the control unit by activating its internal sounder.

Exit the option or open the case of the control unit to silence the sound.

Locate Bus Device

(This option is not available for i-on Compact.)

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).

Network

This option tests the network connection.

If *Communications – IP Options – Cloud Access* is enabled, only the current communications path to the internet is tested. This is to avoid interrupting the cloud connection.

If a COM-DATA-4G or COM-DATA-4G-WIFI module is fitted and *Communications – IP Options – Cloud Access* is not enabled, one of the following is tested:

- If *Communications – IP Options – Module – Data Mode* is set to *Mobile as backup*, you can choose whether to test the LAN or mobile (4G/3G/2G) connection.
- If *Communications – IP Options – Module – Data Mode* is set to *Mobile only*, the mobile (4G/3G/2G) connectionis tested.
- If *Communications – IP Options – Module – Data Mode* is set to *LAN only*, the LAN connection is tested.

Note: If you are running a LAN test and are using a COM-DATA-WIFI or COM-DATA-4G-WIFI module, you may want to disconnect the Ethernet cable or Wi-Fi connection before you start to be sure which path you are testing. Once that test is complete, you may want to swap to using the other path (Wi-Fi or Ethernet) and re-run the test.

The system checks each of the following in sequence during the test. Allow the test to complete, then press ▲ or ▼ to scroll through the results.

Gateway Ping

This tests whether the control panel can communicate effectively with the local network router.

Running this test will result in a time value in ms, or a fail if no ping response is received. As a rule, the lower the ping value the better (e.g. a 20ms response time is much better than 200ms response time). The value can vary greatly depending on the network conditions, topology, arrangement, etc. A value of between 50ms to 100ms can be considered good to average. A result beyond 150ms can be considered unsatisfactory.

If this test fails, check:

- Your network password
- Your network signal
- The Ethernet cable
- The IP address details of the control unit

If there is a high ping value, consider:

- The quality of the internet service
- Your internet connection speed
- The available bandwidth
- The firewall configuration settings
- The geographic location

DNS Ping

This tests the Domain Name System (DNS) response time of the router.

If this test fails, the DNS used by the network router is not responding or has very high latency. To resolve the issue:

- Check whether any other network-enabled device connected to the internet via the network router could be causing an issue.
- Check the firewall settings.
- Seek support from your internet service provider.

If this test results in a high ping value, consider the same factors as for a high *Gateway Ping* value.

Ping 8.8.8.8

This tests that the control panel is able to connect to the internet.

If this test fails, the control panel is connected to the local network router, but is not being provided with internet access. To resolve the issue:

- Check that other network-enabled devices can connect to the internet via the same network router.
- Check the firewall settings.
- Check the router settings.
- Seek support from your internet service provider.

If this test results in a high ping value, consider the same factors as for a high *Gateway Ping* value.

DNS Resolve

This tests the ability of the router to resolve DNS queries.

If this test fails, the network router is unable to resolve DNS queries where a URL is translated into an IP address. To resolve the issue:

- Check that other network-enabled devices can connect to the internet via the same network router. Attempt to access a website such as www.google.co.uk from a device connected to the router.
- Seek support from your internet service provider.

Cloud

This tests whether the control panel can connect to Eaton SecureConnect cloud services.

If this test fails, check for outstanding cloud outages.

Chapter 9: 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.

Log Events

To comply with EN50131-1:2006 for grade 2 and 3 systems, 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. Additionally, the EN 50136 Log stores SPT events to comply with this standard. Please refer to Appendix C on page 143 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 maximum number of events each area of the log can store is dependent on the control unit. Please refer to the *i-on Installation Manual* for details of system limits.

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.

When you are viewing a log event, pressing ▶ may display additional information.

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 – Radio Options – Jamming* and *System Options – Radio Options – Supervision* (see page 92). 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 10: About Menu

The *About* menu offers information on the version and status of the control unit and information about any communications.

Panel

This option shows:

- The control unit model (e.g. i-on40H+).
- The control unit's name, if defined in *System Options, Hardware, Panel Name* (page 88).
- The control unit’s software (firmware) version number.
- The control unit’s bootloader version number.
- The installed languages and their versions.
- Whether the control unit is programmed as partition or part setting (if applicable).
- The country configuration version of the control unit (e.g. UK).

Press ▲ or ▼ to see each item of information.

Installer

This displays the installer's name, telephone number, email address and contract number, as set up in the *System Options – Installer* menu (page 82).

Press ▲ or ▼ to see each item of information.

Bus

(This option is not available for i-on Compact.)

This displays the total number of devices on the bus, and the number of devices of each type.

Press ▲ or ▼ to see each item of information.

Cloud

This shows information about the connection to SecureConnect, including the status of the connection (normal is “Ethernet OK” or "Wi-Fi OK"), Cloud ID, Site ID and Panel ID (in two formats).

The Panel ID is used by SecureConnect to uniquely identify the panel.

Expanders

(This option is not available for i-on Compact.)

If you select an expander by scrolling up or down the list and then press ✔, the display shows the version of firmware running on the expander.

Keypads

(This option is not available for i-on Compact.)

If you select a keypad by scrolling up or down the list and then press ✔, the display shows the version of firmware 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 pressing the "A" and "✔" keys at the same time.

Comms

When no module is present, the *Panel Ethernet* option is the only option available in this menu.

Module

COM-DATA-4G or COM-SD-GSM:

- Network – The network name, signal strength and whether 2G or 4G is active. "Not Reg" is displayed if the module has not been able to connect to a network.
- IMEI – The International Mobile Equipment Identity number of the comms chip on the module.
- Subscriber Number – The telephone number of the SIM. The field is blank if the telephone number is not stored on the SIM (even though the SIM has a telephone number).
- IMSI – The International Mobile Subscriber Identity (IMSI) number, which identifies the user of the mobile network.
- ICCID – The Integrated Circuit Card Identification Number. This is a unique 18-22 digit code that includes a SIM card's country, home network, and identification number. You can normally find the ICCID printed on the back of a SIM card, but it may be in the packaging materials instead.
- Serial Number – The serial number of the comms chip on the module.
- IP Address (not shown for COM-SD-GSM) – The IP address of the control unit via the mobile data link. This is displayed only if the control unit is connected to the internet using a COM-DATA-4G module.
- Version – The firmware version of the module.
- Reset – Resets the TCP/IP stack. Do not use this option without guidance from Eaton product support.

COM-DATA-WIFI:

- Network – The Wi-Fi network name and signal strength.
- IP Address – The IP address of the control unit via the Wi-Fi link.
- IP Subnet Mask – The subnet mask of the network. "DHCP" is displayed if this was assigned by a DHCP server.
- Gateway IP Address – The IP address of the network gateway. "DHCP" is displayed if this was assigned by a DHCP server.
- DNS IP Address – The IP address of the DNS server. "DHCP" is displayed if this was assigned by a DHCP server.

- MAC Address – The MAC address of the module.
- Reset – Resets the module.

COM-SD-PSTN:

The PSTN Link Status 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.

Panel Ethernet

This shows information about the Ethernet Internet Protocol (IP) settings of the control unit (if used) and allows you to reset the Ethernet port. To change the settings, use the *Communications – IP Options – Panel Ethernet* menu (see page 112).

IP Address

This is the IP address of the control unit when linked by Ethernet.

IP Subnet Mask

This is the subnet mask currently in use by the control unit.

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 to 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.

Reset

This option shows the current status of the Ethernet link to 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.

Zone Mapping

(This option is not available for i-on Compact, as there are no bus devices.)

Zone Numbers

For each zone, this shows:

- The zone number (e.g. "Z000"), and where the zone is connected (e.g. "PAN<00 W" is panel zone zero, a wired zone).
- The name of the zone (e.g. "Zone 000").

Zone Addresses

This shows the same information as *Zone Numbers*.

Appendix A: ARC Communication

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 104). 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 Format

Note: The CID protocol specifies “Use 000 to indicate that no specific zone or user information applies”. Therefore, the ARC is not able to determine that a reported event for zone 000 is for zone 000. You might find this zone useful as a Log Only zone.

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 (always 00 for a part-setting system).

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 Formats

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). Not shown for a part-setting system.
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 Format

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.

Extended SIA3 V3 Format

Extended SIA 3 v3 is similar to Extended SIA 3, except that "^" is used instead of "/" for the ASCII text delimiter.

CID/SIA Report Groups

The following table lists the CID/SIA codes included in each CID/SIA report group selected for reporting using the *Communications – ARC Reporting – CID/SIA Events* option (see page 105).

Table 9: CID and SIA Report Groups

Event Group	Event Log Text (Scantronic)	Description	SIA Code	CID Code
Fire Alarm	"RK== Fire"	Not used	FA	110
	"Fire Restore"	Fire alarm restored from radio keypad	FR	110
	"Fire Z== Alarm"	Fire alarm on zone n	FA	110
	"Fire Z== Restore"	Fire alarm on zone n restored	FR	110
	"Fire == Alarm"	Fire alarm at keypad n	FA	110
	"Fire Restore"	Fire alarm at keypad restored	FR	110
Hold Up Alarm	"APP U--- HU Alarm"	Confirmed Hold Up Alarm from APP user	PA	120
	"HUA Restore P#"	Hold Up Alarm has been restored	PR	120
	"HUA Restore"	Hold Up Alarm has been restored	PR	120
	"RK == HUA"	Hold Up Alarm raised at radio keypad n	PA	120
	"HUA Restore P#"	Hold Up Alarm has been restored	PR	120
	"HUA Restore"	Hold Up Alarm has been restored	PR	120
	"U--- Ptn ## Duress"	User n keyed in a Duress code to set partition n	HA	121
	"U--- Ptn ## Dur Rs"	User n keyed in a Duress code to unset partition n	HR	121
	"U--- Duress"	User n keyed in a Duress code to set the system (part setting system)	HA	121
	"U--- Duress Restr"	User n keyed in a Duress code to unset the system (part setting system)	HR	121
	"HUA Conf ==RKBS"	Hold Up Alarm confirmed by a tamper on RKBS n	HV	129
	"HUA Confirm RK=="	Hold Up Alarm confirmed by tamper on radio keypad n	HV	129
	"HUA Conf HD RK=="	Hold Up Alarm confirmed on radio keypad HUA keys	HV	129
	"HUA Confirm Aux #"	Hold Up Alarm confirmed by control unit AUX tamper	HV	129
	"HUA Confirm Bell #"	Hold Up Alarm confirmed by control unit Tamper Return (TR)	HV	129
	"HUA Conf Bus# Tamp"	Hold Up Alarm by a bus tamper	HV	129
	"HUA Confirm"	Hold Up Alarm confirmed on device	HV	129
	"HUA Conf. =="	Hold Up Alarm confirmed by tamper on expander n	HV	129
	"HUA Confirm SRN=="	Hold Up Alarm confirmed by radio siren n tamper	HV	129
	"HUA Confirm =="	Hold Up Alarm confirmed on keypad HUA keys	HV	129
	"HUA Conf. ==ER"	Hold Up Alarm has been confirmed by a missing external prox reader on keypad n	HV	129
	"HUA Conf HD =="	Hold Up Alarm confirmed on keypad n HUA keys	HV	129
	"HUA Conf Panel Jam"	Hold up alarm confirmed by panel jamming	HV	129
	"HUA Conf Panel Lid"	Hold Up Alarm confirmed by panel lid tamper	HV	129
	"HUA Conf. REP=="	Hold Up Alarm confirmed by Radio Repeater lid tamper	HV	129
	"HUA Conf. ==IS"	Hold Up Alarm confirmed by a tamper on internal radio sounder n	HV	129
	"HUA Cnf RF MD U---"	Hold Up Alarm confirmed by radio Man Down transmitter belonging to user n	HV	129

	"HUA Cnf RF HD U---"	Hold Up Alarm confirmed by radio HUD belonging to user	HV	129
	"HUA Confirm VKP"	Hold Up Alarm confirmed by VKP user code tamper	HV	129
	"HUA Confirm WAM=="	Hold Up Alarm confirmed by tamper on WAM n	HV	129
	"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	HV	129
	"HUA Confirm Z==="	Hold Up Alarm confirmed on wired zone n	HV	129
	"HU == Alarm"	Hold Up alarm at keypad n	PA	120
	"HUA Restore P#"	Hold Up alarm at keypad restored for partition n	PR	120
	"HUA Restore"	Hold Up Alarm has been restored	PR	120
	"HUA Z== Alarm"	Hold Up alarm on zone n	PA	120
	"HUA Z== Restore"	Hold Up alarm restored on zone n	PR	120
	"HUA U-- Alarm"	Hold Up Alarm confirmed on User radio device n	PA	121
	"HUA Restore P#"	Hold Up Alarm has been restored in partition n	PR	121
	"HUA Restore"	Hold Up Alarm has been restored	PR	120
Medical Alarm	"RK== Medical"	Medical alert raised at radio keypad n	MA	100
	"Medical Restore P#"	Medical alert restored for radio keypad n	MR	100
	"Medical Restore"	Medical alarm in partition has been restored	MR	100
	"Medical K== Alarm"	Medical alarm at keypad n	MA	100
	"Medical Restore P#"	Medical alarm at keypad restored	MR	100
	"Medical Restore"	Medical alarm in partition has been restored	MR	100
	"U--- Medical Alm"	User n has triggered a medical alarm from pendant	MA	100
Social Care	"RK## Soc. Emergency"	Social Care alert raised at radio keypad n	QA	101
	"Soc Emergency K=="	Social-care alert issued from keypad	QA	101
	"U-- Soc. Emergency"	User n has triggered a social-care alert from pendant	QA	101
	"Social Inactive"	Social-care alert caused by inactivity at monitored zones	NA	
Burglar Alarm	"24hr Z=== Alarm"	24 hour alarm on zone n	BA	130
	"24hr Z=== Restore"	24 hour alarm on zone n restored	BR	130
	"Alarm Abort U--"	Alarm aborted by user n	BC	406
	"Al. Conf ==RKBS"	Confirmed alarm with tamper on radio keypad n base station	BV	139
	"Alarm Confirm RK=="	Confirmed alarm with tamper on radio keypad n	BV	139
	"Alarm Conf Aux #"	Confirmed alarm with tamper on Aux n	BV	139
	"Alarm Conf Bell #"	Confirmed alarm with tamper on Bell n	BV	139
	"Alm Conf Bus# Tamp"	An alarm was confirmed by a bus tamper	BV	139
	"Alarm Confirm"	Confirmed alarm	BV	139
	"Alarm Conf. =="	Confirmed alarm with tamper on expander n	BV	139
	"Alm Confirm SRN=="	Confirmed alarm with tamper on radio siren n	BV	139
	"Alarm Conf. =="	Confirmed alarm with tamper on keypad n	BV	139
	"Alarm Conf ==ER"	Alarm has been confirmed by a missing external prox reader on keypad n	BV	139
	"Alm Conf Panel Jam"	Alarm confirmed by panel jamming	BV	139
	"Alm Conf Panel Lid"	Confirmed alarm with tamper on control unit lid	BV	139
	"Alrm Conf REP=="	Confirmed alarm with tamper on Radio Repeater n	BV	139
	"Alarm Conf ==IS"	Confirmed alarm with tamper on Internal Radio Sounder n	BV	139
	"Alarm Conf. VKP"	Confirmed alarm with tamper on virtual keypad	BV	139
	"Alm Confirm WAM=="	Confirmed alarm with tamper on WAM n	BV	139
	"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	BV	139
	"Alarm Confirm Z=="	Confirmed alarm on zone	BV	139
	"Burg Z== Alarm"	Burglar alarm on zone n	BA	130

	"Burg Z== Restore"	Burglar alarm on zone n restored	BR	130
	"PRM Z=== Active"	Perimeter zone n active	UA	131
	"PRM Z=== Restore"	Perimeter zone n restored	UR	131
Technical Alarm	"Tech Z== Alarm"	Technical alarm on zone n	UA	150
	"Tech Z== Restore"	Technical alarm on zone n restored	UR	150
Masking	"Mask Z=="	Masking detected on zone n	BT	380
	"Mask Flt Z=="	Masking fault detected on zone n	BT	380
	"Mask Rstr Z=="	Masking restored on zone n	BJ	380
Tampers	"RKBS Tamp (==)"	Tamper at radio keypad base station n	ES	341
	"RKBS Tmp Rs(==)"	Tamper restored at radio keypad base station n	EJ	341
	"RK== Tamper"	Tamper on radio keypad n	TA	137
	"RK== Tamper Rstr"	Tamper on radio keypad n restored	TR	137
	"Aux # Tamper"	Control unit Aux Tamper	TA	137
	"Aux # Tamper Rstr"	Control unit Aux Tamper restored	TR	137
	"Bell # Tamper"	External wired siren n tamper	TA	137
	"Bell # Tamper Rstr"	External wired siren n tamper restored	TR	137
	"Bus # Tamper"	Bus n has been tampered (for example wires cut or disconnected)	TA	137
	"Bus # Tamper Rstr"	Bus n has been restored	TR	137
	"Duplicate =="	Duplicate expander n detected	ET	
	"Dup. == Restore"	Duplicate expander restored	ER	
	"Missing =="	Expander n missing from bus	EM	341
	"Missing == Rstr"	Missing expander n restored to bus	EN	341
	"Tamper =="	Tamper at expander n	ES	341
	"Tamper == Rstr"	Tamper at expander n restored	EJ	341
	"RSN== Tamper"	Tamper on External Radio Siren n	TA	137
	"RSN== Tamper Rstr"	Tamper Restore on External Radio Siren n	TR	137
	"IP Cam # Missing"	IP camera n is missing (camera supervision failed)	IA	
	"IP Cam # Miss Rstr"	Connection to IP cam n restored	IR	
	"Duplicate =="	Duplicate keypad n detected	ET	
	"Dup. == Restore"	Duplicate keypad restored	ER	
	"Missing ==ER"	An External prox Reader connected to keypad n has gone missing (possibly disconnected from the keypad)	TA	137
	"Missing ==ER Rs"	An External prox Reader connected to keypad n has been re-connected	TR	137
	"Tamper ==ER"	Tamper at external reader n	TA	137
	"Tamper ==ER Rst"	Tamper at external reader n restored	TR	137
	"Missing =="	Keypad n missing from bus	EM	137
	"Missing == Rstr"	Missing keypd n restored to bus	EN	137
	"Tamper =="	Tamper at keypad n	ES	137
	"Tamper == Rstr"	Tamper at keypad n restored	EJ	137
	"Panel lid open"	Control unit lid open	TA	137
	"Lid Tamper Restore"	Control unit lid closed	TR	137
	"REP== Tamper"	Tamper on Radio Repeater n	TA	137
	"REP== Tamper Rstr"	Tamper Restore on Radio Repeater n	TR	137
	"ISN== Tamper"	Tamper on Internal Radio Sounder n	TA	137
	"ISN== Tamper Rstr"	Tamper Restore on Internal Radio Sounder n	TR	137
	"Tamper Z=="	Zone n tamper	TA	137
	"Tamper Z== Restore"	Zone n tamper restored	TR	137
	"RK== Excess Keys"	Radio keypad n has been tampered by excess key presses	TA	137

	"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	TR	137
	"K== Excess Keys"	Excess keys tamper at keypad n	TA	137
	"Panel Excess Keys"	Exceeded number of maximum attempts to enter access code	TA	137
	"== Ex Keys Rstr"	Excess keys (code attempts) tamper restore	TR	137
	"VKP Excess Keys"	Excess keys (code attempts) tamper at virtual keypad	TA	137
	"VKP Ex Keys Rstr"	Excess keys tamper at virtual keypad restored	TR	137
	"Websvr Excess Keys"	Web server has caused a tampered by a user trying to log with the wrong password more than four times	JA	461
	"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	TR	137
	"WAM== Tamper"	WAM n tampered	TA	137
	"WAM== Tamper Rstr"	WAM n tamper restored	TR	137
Set/Unset	"U-- Ptn # Set"	User n set partition	CL	401
	"U-- System Set"	User n set system	CL	401
	"Auto Ptn # Set"	Partition n set by calendar setting	CA	403
	"Auto System Set"	The system was full set by calendar setting	CA	403
	"Auto Ptn # Unset"	Partition n unset by calendar setting	OA	403
	"Auto System Unset"	The system was unset by calendar setting	OA	403
	"Autoset Fail P#"	Calendar setting of partition failed	CI	455
	"Autoset Fail"	Calendar setting of system failed	CI	455
	"AS defer U-- P#"	User n defered calendar setting for partition n	CE	464
	"Autoset defer U--"	User defered calendar setting of system	CE	464
	"U-- Ptn # Unset"	User n unset partition	OP	401
	"U-- System Unset"	User n unset system	OP	401
	"Set Fail Z=="	Setting failed at zone	EA	457
	"Key Sw Ptn # Set"	Partition n set from keyswitch	CS	409
	"Key Sw System Set"	System set from keyswitch	CS	409
	"Key Sw Ptn # Unset"	Partition n unset from keyswitch	OS	409
	"Key Sw System Unset"	System unset from keyswitch	OS	409
	"U-- Ptn # Override"	User n overrode set fail at partition	CW	
	"U-- Set Override"	User n overrode set fail	CW	
	"Ptn # Remote Rst"	User reset partition n remotely	OR	305
	"Remote Reset"	User reset system remotely	OR	305
	"U-- Ptn # Reset"	User n reset partition	OR	305
	"U-- System Reset"	User n reset system	OR	305
	"Set Z=== Shunted"	The system was set with zone n shunted	CG	
	"Z=== Shunted"	Zone n is shunted	UB	575
	"Z=== UnShunted"	Zone n has been un-shunted	UU	575
Part Set	"Auto Ptn # PtSet"	Partition n was part set by calendar setting	CA	403
	"Auto Part Set #"	The system was part set by calendar setting	CA	403
	"Key Sw Ptn # PtSet"	Partition part set from keyswitch	CS	409
	"Key Sw System PtSet"	System part set from keyswitch	CS	409
	"U-- Ptn # PtSet"	User n part set partition	CL	401
	"U-- System PtSet #"	User n part set system	CL	401
Omit	"U--- Z=== HUA Omit"	User n omitted Hold Up Alarm zone n	PB	570
	"U--- Z=== Omit Rst"	User n included Hold Up Alarm zone n	PU	570
	"U-- Z== Omit"	User n omitted zone	BB	573
	"U--- Z=== Omit Rst"	User n included (restored) zone n	BU	573

RF Supervision*	"== Superv Fail"	Radio signal fail for 2 hours for device n	ET	381
	"== Superv Rstr"	Radio signal restored for device n	ER	381
	"RK== Superv Fail"	Radio keypad n failed supervision	ET	381
	"RK== Superv Rstr"	Radio keypad n supervision restored	ER	381
	"RSN== Superv Fail"	Radio signal fail for 2 hours for External Radio Siren n	YA	381
	"RSN== Superv Rstr"	Radio signal restored for External Radio Siren n	YH	381
	"REP== Superv Fail"	Radio signal fail for 2 hours for Radio Repeater n	ET	381
	"REP== Superv Rstr"	Radio signal restored for Radio Repeater n	ER	381
	"ISN== Superv Fail"	Radio signal fail for 2 hours for Internal Radio Sounder n	YA	381
	"ISN== Superv Rstr"	Radio signal restored for Internal Radio Sounder n	YH	381
	"WAM== Superv Fail"	WAM n has failed supervision	ET	381
	"WAM== Superv Rstr"	WAM n supervision restored	ER	381
	"Superv'n Fail Z=="	Supervision failed for radio detector at zone n	BT	381
	"Superv'n Rstr Z=="	Supervision restored for radio detector at zone n	BR	381
RF Jamming*	"RKBS Jam (==)"	Radio jamming detected at radio keypad base station n	XQ	344
	"RKBS Jam Rs(==)"	Radio jamming removed at radio keypad base station n	XH	344
	"Kpd == Jamming"	Radio jamming detected at radio keypad n	XQ	344
	"Kpd == JammingR"	Radio jamming removed at radio keypad n	XH	344
	"Jamming =="	Jamming detected	XQ	344
	"Jamming == Rstr"	Jamming ceased	XH	344
	"RSN== Jamming"	Jamming on External Radio Siren n	XQ	344
	"RSN== Jamming Rstr"	Jamming Restored on External Radio Siren n	XH	344
	"REP== Jamming"	Jamming on Radio Repeater n	XQ	344
	"REP== Jamming Rstr"	Jamming restored on Radio Repeater n	XH	344
	"ISN== Jamming"	Jamming on Internal Radio Sounder n	XQ	344
	"ISN== Jamming Rstr"	Jamming Restored on Internal Radio Sounder n	XH	344
	"RF Jamming"	Radio jamming detected	XQ	344
	"RF Jamming Restore"	Radio jamming removed	XH	344
	"Z== Jamming"	Jamming on Radio Detector n	XQ	344
	"Z== Jamming Rst"	Jamming restored on Radio Detector n	XH	344
RF Battery/PSU	"Kpd == Low Batt"	Low battery voltage at radio keypad n	XT	338
	"RK== Low Battery"	Radio keypad n has low battery	XT	338
	"RK== PSU Fail"	PSU failure on radio keypad n	YP	337
	"RK== PSU Restore"	PSU restored on radio keypad n	YQ	337
	"RSN== Low Battery"	Low battery on External Radio Siren n	XT	338
	"RSN== Battery Rstr"	Low battery Restored on Internal Radio Sounder n	XR	338
	"Social U-- Low Bat"	Social Care pendant assigned to User n has a low battery	XT	338
	"Medi U-- Low Bat"	Medical pendant assigned to user N has a low battery	XT	338
	"REP== Low Battery"	Low battery on Radio Repeater n	XT	338
	"REP== Battery Rstr"	Low battery Restored on Radio Repeater n	XR	338
	"REP== PSU Fault"	PSU fault on Radio Repeater n	XP	337
	"REP== PSU Flt Rstr"	PSU restored on Radio Repeater n	XR	337
	"ISN== Low Battery"	Low battery on Internal Radio Sounder n	YT	338
	"ISN== Battery Rstr"	Low battery Restored on Internal Radio Sounder n	YR	338
	"WAM== Low Battery"	WAM n has low battery	XT	338
	"WAM== Battery Rstr"	WAM n low battery restored	XR	338
	"WAM== PSU Fail"	WAM n has low power supply	YP	337
	"WAM== PSU Restore"	WAM n low power supply restored	YQ	337
	"Low Battery Z=="	Radio detector at zone n has low battery	XT	384
	"Low Batt Z== Rstr"	Radio detector at zone n has low battery restored	XR	384

Panel Battery	"Batt= Charger Rstr"	Control unit battery charger working again	YR	302
	"Batt = Load Fail"	Control unit battery failed load test	YT	309
	"Battery Load OK"	Control unit battery passed load test	YR	309
	"Batt = Low/Missing"	Control unit battery missing or low	YM	311
	"Batt= Charger Fail"	Control unit battery charger failed	YT	302
	"Batt = Fault Rst"	Control unit battery restored	YR	311
	"== Load 1 Fail"	Battery 1 failed load test	ET	330
	"== Load 1 OK"	Battery 1 passed load test	ER	330
	"== Load 2 Fail"	Battery 2 failed load test	ET	330
	"== Load 2 OK"	Battery 2 passed load test	ER	330
	"== Low Batt 1"	Battery 1 low	ET	338
	"== Batt 1 Rstr"	Battery 1 restored	ER	338
	"== Miss Batt 1"	Battery 1 missing	ET	330
	"== Batt 1 Rstr"	Battery 1 missing restored	ER	330
	"== Low Batt 2"	Battery 2 low	ET	338
	"== Batt 2 Rstr"	Battery 2 restored	ER	338
	"== Miss Batt 2"	Battery 2 missing	ET	330
	"== Batt 2 Rstr"	Battery 2 missing restored	ER	330
	"== Chargr 1 Flt"	Battery 1 charger fault	ET	330
	"== Chargr 2 Flt"	Battery 2 charger fault	ET	330
	"== Chargr 1 Rst"	Battery 1 charger fault restored	ER	330
	"== Chargr 2 Rst"	Battery 2 charger fault restored	ER	330
	"Low Battery ="	Control unit battery low	YT	302
	"Low Batt = Restore"	Control unit battery no longer low	YR	302
	"Ext Batt Fault Z=="	Zone n with type Batt Fault activated	YM	311
	"Ext Batt Rstr Z=="	Zone n with type Batt Fault restored	YR	311
Mains Fail	"Panel A/C Fail"	AC power failure at control unit	AT	301
	"Panel A/C Restore"	AC power restored at control unit	AR	301
	"== A/C Fail Flt"	AC mains fail	ET	342
	"== A/C Fail Rst	AC mains restored	ER	342
	"A/C Fail Ptn ##"	Control unit or EXP-PSU mains fail, or "zone of type "AC Fail" was triggered in partition n	AT	301
	"A/C Rstr Ptn ##"	Mains fail was restored in the partition n	AR	301
	"A/C Fail"	Control unit or EXP-PSU mains fail, or "zone of type "AC Fail" was triggered	AT	301
	"A/C Restore"	Mains fail was restored	AR	301
	"A/C Fail"	AC mains failed and was communicated	AT	301
	"A/C Restore"	AC mains was restored	AR	301
	"Ext A/C Fail Z=="	Zone n with type AC Fail activated	AT	342
	"Ext A/C Rstr Z=="	Zone n with type AC Fail restored	AR	342
Faults	"RKBS Low V (==)"	Low voltage at radio keypad base station n	YP	337
	"RKBS L V Rs(==)"	Low voltage restored at radio keypad base station n	YQ	337
	"ATE L.F. All"	All lines to alarm transmission equipment failed	YC	
	"ATE L.F. Restore"	Line to alarm transmission equipment restored	YK	
	"ATE L.F. Single"	Alarm transmission equipment has a single line fault	YS	
	"Auxiliary 12V Fail"	Control unit 12V Aux DC not working	YP	300
	"Wifi 12V Fail"	Control unit 12V Wi-Fi DC not working	YP	300
	"Auxiliary 12V Rstr"	Control unit 12V Aux DC restored	YQ	300
	"Wifi 12V Restore"	Control unit 12V Wi-Fi DC restored	YQ	300
	"Aux. 14V4 # Fail"	Control unit 14.4V supply failed	YP	300

	"Aux. 14V4 # Rstr"	Control unit 14.4V supply restored	YQ	300
	"Bell # 12V Fail"	12V DC supply to bell n failed	YP	300
	"Bell # 12V Restore"	12V DC supply to bell n restored	YQ	300
	"Bus # 12V Fail"	12V DC supply to Bus n failed	YP	300
	"Bus # 12V Restore"	12V DC supply to Bus n restored	YQ	300
	"Cloud Connected"	Connection to SecureConnect made	YK	
	"Cloud Disconnected"	SecureConnect disconnected	YC	
	"Mobile test Fail"	SecureConnect periodic Mobile/Cellular path test failed	YS	
	"Cloud push fail"	Push notifications to SecureConnect failed	YS	
	"Cloud push restore"	Push notifications to SecureConnect restored	YK	
	"All Comms Pths Flt"	All communications paths have a fault	LT	351
	"All Comms Pths Rst"	All communications path faults restored	LR	351
	"Comms 12V Fail"	DC power to comms module failed	YP	300
	"Comms 12V Restore"	DC power to comms module restored	YQ	300
	"Ethernet Line Flt"	Ethernet line fault (e.g no connection to router)	LT	351
	"Ethernet Line Rst"	Eithernet line restored	LR	351
	"GPRS/3G Signal Flt"	GPRS/3G module signal loss	LT	351
	GPRS/3G Signal Rst	GPRS/3G module signal restored	LR	351
	"GSM Signal Fault"	GSM module signal loss	LT	351
	"GSM Signal Restore"	GSM module signal restored	LR	351
	"$m Line Fault"	Communications line failed (ie line disconnected) Line Fail Response option must not be set to "Disabled"	LT	351
	"$m Line Restore"	Communications line restored Line Fail Response option must not be set to "Disabled"	LR	351
	"$m Modem Fault"	Modem failed	IA	
	"$m Modem Restore"	Modem restored	IR	
	"Pri Comms Path Flt"	Primary communications path has a fault	LT	351
	"Pri Comms Path Rst"	Primary communications path fault restored	LR	351
	"PSTN Line Fault"	PSTN line failt	LT	351
	"PSTN Line Restore"	PSTN line restored	LR	351
	"Sec Comms Path Flt"	Secondary communications path has a fault	LT	351
	"Sec Comms Path Rst"	Secondary communications path fault restored	LR	351
	"Wifi Signal Fault"	Wi-Fi signal lost	LT	351
	"Wifi Signal Rstr"	Wi-Fi signal restored	LR	351
	"== Aux Fuse Flt"	Aux fuse failed	ET	330
	"== Aux Fuse Rst"	Aux fuse restored	ER	330
	"== Aux1 O/P Flt"	Auxiliary output 1 fault	ET	337
	"== Aux1 O/P Rst"	Auxiliary output 1 fault restored	ER	337
	"== Aux2 O/P Flt"	Auxiliary output 2 fault	ET	337
	"== Aux2 O/P Rst"	Auxiliary output 2 fault restored	ER	337
	"== Bus O/P Flt"	Bus dc power output fault	ET	337
	"== Bus O/P Rst"	Bus dc power output restored	ER	337
	"== Coms O/P Flt"	Plug-by comms output fault	ET	337
	"== Coms O/P Rst"	Plug-by comms output fault restored	ER	337
	"== Low Voltage"	PSU reports low voltage	ET	337
	"== Voltage OK"	Voltage OK	ER	337
	"== Sys Volt Flt"	System voltage fault	ET	337
	"== Sys Volt Rst"	System voltage fault restored	ER	337
	"Panel Ext DC Fail"	External DC PSU failure	YP	300
	"Panel Ext DC Restore"	External DC PSU restored	YQ	300

	"RSN== Fault"	Fault on External Radio Siren n	YA	
	"RSN== Fault Rstr"	Fault restored on External Radio Siren n	YH	
	"4K4 Fault Z=="	Fault resistor active on zone n	IA	389
	"4K4 Rstr Z=="	Fault resistor restored on zone n	IR	389
	"Alarm Test Call"	Manual alarm test call made	RX	601
	"Ext DC Fail Ptn ##"	External DC supply has failed in partition n	YP	300
	"External DC Fail"	External DC supply has failed	YP	300
	"Ext DC Rstr Ptn ##"	External DC supply has restored in partition n	YQ	300
	"External DC Rstr"	External DC supply has restored	YQ	300
	"Alarm Test Call"	Periodic alarm test call made	RP	602
	"ISN== Fault"	Fault on Internal Radio Sounder n	YA	320
	"ISN== Fault Rstr"	Fault restored on Internal Radio Sounder n	YH	320
	"HUA U-- Low Batt"	Low battery on User radio device n	XT	338
	"Z== Smoke Flt"	Smoke detector at zone n has fault	FT	373
	"Z== Smoke Flt Rst"	Smoke detector at zone n has been restored	FJ	373
	"Z== Smoke PSU Flt"	Smoke detector at zone n has power supply fault	YP	337
	"Z== Smoke PSU Rst"	Smoke detector at zone n power supply fault restored	YQ	337
	"System 12V Fail"	Control unit 12V supply failed	YP	300
	"System 12V Restore"	Control unit 12V supply restored	YQ	300
	"System Error"	Control unit has fault in main processor	YW	300
	"Remote U-- Low Bat"	Remote control belonging to user has low battery	XT	338
	"Soak Fail Z== Alm"	Zone n on soak test failed	RY	
	"Soak Fail Z== Tmp"	Zone n on soak test tampered	RY	
	"Ext PSU Fault Z=="	Zone n with type Fault activated	YP	337
	"Ext PSU Rstr Z=="	Zone n with type Fault restored	YQ	337
	"Ext Low Volts Z=="	Zone n with type Low Volts activated	YT	338
	"Ext Volts Rstr Z=="	Zone n with type Low Volts restored	YR	338
	"Ext WD Fault Z==="	A warning device has reported a fault through zone n	YA	320
	"Ext WD Restr Z==="	The fault reported through zone n by a warning device has been restored	YH	320
	"HUD Fault Z==="	A hold up device reported a fault on zone n	PT	375
	"HUD Fault Rst Z==="	A hold up device fault reported on zone n was restored	PJ	375
Installer Mode	"VKP Disconnected"	Virtual keypad disconnected	RS	628
	"U-- Off-Site"	User n left Installer mode	LS	628
	"U-- Off-Site (Web)"	User n logged out of Installer Menu from web server	RS	628
	"U-- On-Site"	User n entered Installer mode	LB	627
	"U-- On-Site (Web)"	User n logged into Installer Menu from web server	RB	627
	"VKP Connected"	Virtual keypad connected	RB	627
User Code Change	"Codes Defaulted"	All access codes were returned to factory defaults	RH	
	"U-- Delete U=="	User n deleted another User n from system	JX	
	"U-- Change U=="	User n changed their password	JV	
Time/Date Reset	"U-- Time/Date"	User n changed time and/or date	JT	625
Zone Status*	"Z== Closed"	Zone n quiescent	ZC	
	"Z== Open"	Zone n activated	ZO	

*__Note:__ The control unit communicates Jamming, Supervision and Zone Status when the system is unset.

Appendix B: Log Messages

Introduction

This Appendix gives short explanations of the messages that may appear in the control unit's log. This appendix includes general i-on messages; depending on the panel model, a subset of the messages listed here can be produced.

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 "n". The characters "$m" stand in for the type of communications.

Log messages

Event Log Text (Scantronic)	Description
"$m Alarm Fail"	Communicator failed to send alarm No ACK received after 3 retries
"$m Alarm OK"	Alarm successfully sent to ARC and an acknowledgement was received
"$m Email Fail"	Control unit failed to send email
"$m Line Fault"	Communications line failed (ie line disconnected) Line Fail Response option must not be set to "Disabled"
"$m Line Restore"	Communications line restored Line Fail Response option must not be set to "Disabled"
"$m Modem Fault"	Modem failed
"$m Modem Restore"	Modem restored
"$m SMS Fail"	SMS call failed to get to destination
"$m Social Fail"	Communication to Social Care monitoring station failed
"$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 n
"== RF Warning"	Radio signal lost for 20 min for device n
"== Superv Fail"	Radio signal fail for 2 hours for device n
"== Superv Rstr"	Radio signal restored for device n

"== 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 n
"4K4 Rstr Z=="	Fault resistor restored on zone n
"A/C Fail Ptn ##"	Control unit or EXP-PSU mains fail, or "zone of type "AC Fail" was triggered in partition n
"A/C Fail"	Control unit or EXP-PSU mains fail, or "zone of type "AC Fail" was triggered
"A/C Fail"	AC mains failed and was communicated
"A/C Restore"	Mains fail was restored
"A/C Restore"	AC mains was restored
"A/C Rstr Ptn ##"	Mains fail was restored in the partition n
"Al. Conf ==RKBS"	Confirmed alarm with tamper on radio keypad n base station
"Alarm Abort U--"	Alarm aborted by user n
"Alarm Conf ==ER"	Alarm has been confirmed by a missing external prox reader on keypad n
"Alarm Conf ==IS"	Confirmed alarm with tamper on Internal Radio Sounder n
"Alarm Conf Aux #"	Confirmed alarm with tamper on Aux n
"Alarm Conf Bell #"	Confirmed alarm with tamper on Bell n
"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 expander n
"Alarm Conf. =="	Confirmed alarm with tamper on keypad n
"Alarm Conf. VKP"	Confirmed alarm with tamper on virtual keypad
"Alarm Confirm RK=="	Confirmed alarm with tamper on radio keypad n
"Alarm Confirm Z=="	Confirmed alarm on zone
"Alarm Confirm"	Confirmed alarm
"Alarm Test Call"	Manual alarm test call made
"Alarm Test Call"	Periodic 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
"Alrm Conf REP=="	Confirmed alarm with tamper on Radio Repeater n
"APP U--- HU Alarm"	Confirmed Hold Up Alarm from APP user
"APP U--- O/P === Off"	User defined output switched off by APP user
"APP U--- O/P === On"	User defined output switched on by APP user
"AS defer U-- P#"	User n defered calendar setting for 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"	Control unit Aux Tamper restored
"Aux # Tamper"	Control unit Aux Tamper
"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 n failed
"Bell # 12V Restore"	12V DC supply to bell n restored
"Bell # Tamper Rstr"	External wired siren n tamper restored
"Bell # Tamper"	External wired siren n tamper
"Burg Z== Alarm"	Burglar alarm on zone n

"Burg Z== Restore"	Burglar alarm on zone n restored
"Burg Z=== Alarm"	Burglar on First linked zone n in Beam Group
"Burg Z=== Restore"	Burglar on First linkedzone n in Beam Group restored
"Bus # 12V Fail"	12V DC supply to Bus n failed
"Bus # 12V Restore"	12V DC supply to Bus n restored
"Bus # Tamper Rstr"	Bus n has been restored
"Bus # Tamper"	Bus n has been tampered (for example wires cut or disconnected)
"Cloud Connected"	Connection to SecureConnect made
"Cloud Disconnected"	SecureConnect disconnected
"Cloud push fail"	Push notifications to SecureConnect failed
"Cloud push restore"	Push notifications to SecureConnect restored
"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 n disabled
"Disabled =="	Keypad n disabled
"Downloader Lockout"	Downloader locked out for 30 mins due to 10 consecutive authentication errors
"Dup. == Restore"	Duplicate expander restored
"Dup. == Restore"	Duplicate keypad restored
"Duplicate =="	Duplicate expander n detected
"Duplicate =="	Duplicate keypad n detected
"Email error ---"	Control unit email send error
"Email Test Call"	Email test call initiated by Installer
"Enabled =="	Expander n enabled
"Enabled =="	Keypad n enabled
"Entry Started Z=="	Entry started by zone n
"Entry Stray Z=="	Stray on entry alarm at zone n
"Ethernet Line Flt"	Ethernet line fault (e.g no connection to router)
"Ethernet Line Rst"	Eithernet line restored
"Exit Mode Changed"	Local setting mode applied (from Remote set)
"Exp. == deleted"	Expander n deleted from bus
"Expndr == added"	Radio expander n added to bus
"Expndr == added"	Wired expander n added to bus
"Expndr == found"	New radio expander n found on bus
"Expndr == found"	New wired 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 DC Fail Ptn ##"	External DC supply has failed in partition n
"Ext DC Rstr Ptn ##"	External DC supply has restored in partition n
"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 n by a warning device has been restored
"External DC Fail"	External DC supply has failed
"External DC Rstr"	External DC supply has restored
"Fire == Alarm"	Fire alarm at keypad n
"Fire Reset"	User reset system after fire alarm
"Fire Restore"	Fire alarm restored from radio keypad
"Fire Restore"	Fire alarm at keypad restored
"Fire Z== Alarm"	Fire alarm on zone n
"Fire Z== Restore"	Fire alarm on zone n restored
"GPRS/3G Signal Flt"	GPRS/3G module signal loss
"GSM CME Info --"	The GSM plug-on module has a problem
"GSM CMS Info --"	The GSM plug-on module has a problem
"GSM Signal Fault"	GSM module signal loss
"GSM Signal Restore"	GSM module signal restored
"HU == Alarm"	Hold Up alarm at keypad n
"HUA Cnf RF HD U---"	Hold Up Alarm confirmed by radio HUD belonging to user
"HUA Cnf RF MD U---"	Hold Up Alarm confirmed by radio Man Down transmitter belonging to user n
"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 n 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 Conf. REP=="	Hold Up Alarm confirmed by Radio Repeater lid tamper
"HUA Confirm =="	Hold Up Alarm confirmed on keypad HUA keys
"HUA Confirm Aux #"	Hold Up Alarm confirmed by control unit AUX tamper
"HUA Confirm Bell #"	Hold Up Alarm confirmed by control unit Tamper Return (TR)
"HUA Confirm RK=="	Hold Up Alarm confirmed by tamper on radio keypad n
"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 n
"HUA Confirm"	Hold Up Alarm confirmed on device
"HUA Restore P#"	Hold Up Alarm has been restored
"HUA Restore P#"	Hold Up Alarm has been restored
"HUA Restore P#"	Hold Up alarm at keypad restored for partition n
"HUA Restore P#"	Hold Up Alarm has been restored in partition n
"HUA Restore"	Hold Up Alarm has been restored
"HUA Restore"	Hold Up Alarm has been restored
"HUA Restore"	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
"HUA Z== Alarm"	Hold Up alarm on zone n
"HUA Z== Restore"	Hold Up alarm restored on zone 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
"Inv Login Attpt KP"	Invalid access code entered on keypad
"Inv Login Attpt PX"	Invalid prox tag presented to keypad
"Inv Login Attpt RM"	Invalid remote access attempt
"IP Cam # Err 404"	HTTP error 404 from IP camera n
"IP Cam # Err Auth"	Login details to IP camera n incorrect
"IP Cam # HTTP Err."	HTTP error at IP camera n
"IP Cam # Miss Rstr"	Connection to IP cam n restored
"IP Cam # Missing"	IP camera n is missing (camera supervision failed)
"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 n
"ISN== RF Warning"	Radio signal lost for 20 min for Internal Radio Sounder n
"ISN== Superv Fail"	Radio signal fail for 2 hours for Internal Radio Sounder n
"ISN== Superv Rstr"	Radio signal restored for Internal Radio Sounder n
"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 n set from keyswitch
"Key Sw Ptn # Unset"	Partition n 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 n added to system
"Keypad == found"	New keypad n 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"	Zone n with type "lock set" was closed (If Inverted attribute is set to "normal")
"Lockset Z=== Unset"	Zone n with type "lock set" was opened (If Inverted attribute is set to "normal")
"Login Keypad"	Valid access code entered on keypad
"Login Prox"	Valid prox tag presented to keypad

"Low Batt = Restore"	Control unit battery no longer low
"Low Batt Z== Rstr"	Radio detector at zone n has low battery restored
"Low Battery ="	Control unit battery low
"Low Battery Z=="	Radio detector at zone n has low battery
"Mask Flt Z=="	Masking fault detected on zone n
"Mask Rstr Z=="	Masking restored on zone n
"Mask Z=="	Masking detected on zone n
"Medi U-- Low Bat"	Medical pendant assigned to user N has a low battery
"Medical K== Alarm"	Medical alarm at keypad n
"Medical Restore P#"	Medical alert restored for radio keypad n
"Medical Restore P#"	Medical alarm at keypad restored
"Medical Restore"	Medical alarm in partition has been restored
"Medical Restore"	Medical alarm in partition has been restored
"Missing == Rstr"	Missing expander n restored to bus
"Missing == Rstr"	Missing keypd n restored to bus
"Missing =="	Expander n missing from bus
"Missing =="	Keypad n missing from bus
"Missing ==ER Rs"	An External prox Reader connected to keypad n has been re-connected
"Missing ==ER"	An External prox Reader connected to keypad n has gone missing (possibly disconnected from the keypad)
"Mobile app command"	Command actioned from Mobile APP
"Mobile test Fail"	SecureConnect periodic Mobile/Cellular path test failed
"Mobile test OK"	SecureConnect periodic Mobile/Cellular path ok
"Network SysErr =="	Network System Error n (should never happen)
"Occupancy Set P#"	Set but with Occupancy zone(s) open
"Offline (Ethernet)"	SecureConnect offline on Ethernet path
"Offline (Mobile)"	SecureConnect offline on Mobile/Cellular path
"Online (Ethernet)"	SecureConnect online on Ethernet path
"Online (Mobile)"	SecureConnect online on Mobile/Cellular path
"Panel A/C Fail"	AC power failure at control unit
"Panel A/C Restore"	AC power restored at control unit
"Panel Excess Keys"	Exceeded number of maximum attempts to enter access code
"Panel Ext DC Fail"	External DC PSU failure
"Panel Ext DC Restore"	External DC PSU restored
"Panel lid open"	Control unit lid open
"Partn # Rearmed"	Partition n was rearmed after an alarm by control unit
"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=== Active"	Burglar on First linked Perimeter zone n in Beam Group
"PRM Z=== Restore"	Perimeter zone n restored
"PRM Z=== Restore"	Burglar on First linked Perimeter zone n in Beam Group restored
"PSTN Line Fault"	PSTN line failt
"PSTN Line Restore"	PSTN line restored
"Ptn # Remote Rst"	User reset partition n 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
"REP== Battery Rstr"	Low battery Restored on Radio Repeater n
"REP== Jamming Rstr"	Jamming restored on Radio Repeater n
"REP== Jamming"	Jamming on Radio Repeater n
"REP== Low Battery"	Low battery on Radio Repeater n
"REP== PSU Fault"	PSU fault on Radio Repeater n
"REP== PSU Flt Rstr"	PSU restored on Radio Repeater n
"REP== RF OK"	Radio signal restored for Radio Repeater n
"REP== RF Warning"	Radio signal lost for 20 min for Radio Repeater n
"REP== Superv Fail"	Radio signal fail for 2 hours for Radio Repeater n
"REP== Superv Rstr"	Radio signal restored for Radio Repeater n
"REP== Tamper Rstr"	Tamper Restore on Radio Repeater n
"REP== Tamper"	Tamper on Radio Repeater n
"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## Soc. Emergency"	Social Care alert raised at radio keypad n
"RK== 4/6 Mismatch"	Incorrect code length entered at 1-way radio keypad n
"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== Medical"	Medical alert raised at radio keypad n

"RK== PSU Fail"	PSU failure on radio keypad n
"RK== PSU Restore"	PSU restored on radio keypad n
"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 n
"RSN== RF Warning"	Radio signal lost for 20 min for External Radio Siren n
"RSN== Superv Fail"	Radio signal fail for 2 hours for External Radio Siren n
"RSN== Superv Rstr"	Radio signal restored for External Radio Siren n
"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 n shunted
"Shunt Group ## OFF"	User n de-activated shunt group n
"Shunt Group ## ON"	User n 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 n on soak test failed
"Soak Fail Z== Tmp"	Zone n on soak test tampered
"Soc Emergency K=="	Social-care alert issued from keypad
"Social Inactive"	Social-care alert caused by inactivity at monitored zones
"Social Test Call"	Not used
"Social U-- Low Bat"	Social Care pendant assigned to User n has a low battery
"Software Changed"	New control unit software has been installed
"Software Changed"	Control unit sofware version X has been replaced with software version Y
"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
"Superv'n Fail Z=="	Supervision failed for radio detector at zone n
"Superv'n Rstr Z=="	Supervision restored for radio detector at zone n
"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 n restored
"Tamper == Rstr"	Tamper at keypad n restored
"Tamper =="	Tamper at expander n
"Tamper =="	Tamper at keypad n
"Tamper ==ER Rst"	Tamper at external reader n restored
"Tamper ==ER"	Tamper at external reader n
"Tamper Z== Restore"	Zone n tamper restored
"Tamper Z=="	Zone n tamper
"Tech Z== Alarm"	Technical alarm on zone n
"Tech Z== Restore"	Technical alarm on zone n restored
"Test Call Fail"	Test call failed
"Test Call OK"	Test call succeeded
"U-- Change U=="	User n changed their password
"U-- Config Change"	User n changed programming configuration
"U-- Delete U=="	User n deleted another User n from system
"U-- Download Fail"	Downloader session failed

"U--- Duress Restr"	User n keyed in a Duress code to unset the system (part setting system)
"U--- Duress"	User n keyed in a Duress code to set the system (part setting system)
"U-- Log On Remote"	Virtual keypad logon from user n
"U--- Medical Alm"	User n has triggered a medical alarm from pendant
"U--- O/P === Off"	User defined output swittched on by user n
"U--- O/P === On"	User defined output swittched off by user n
"U-- Off-Site (Web)"	User n logged out of Installer Menu from web server
"U-- Off-Site"	User n left Installer mode
"U-- On-Site (Web)"	User n logged into Installer Menu from web server
"U-- On-Site"	User n entered Installer mode
"U-- Ptn # Override"	User n overrode set fail at partition
"U-- Ptn # PtSet"	User n part set partition
"U-- Ptn # Reset"	User n reset partition
"U-- Ptn # Set"	User n set partition
"U-- Ptn # Unset"	User n unset partition
"U--- Ptn ## Dur Rs"	User n keyed in a Duress code to unset partition n
"U--- Ptn ## Duress"	User n keyed in a Duress code to set partition n
"U--- Ptn ## Exit"	User n started the exit process for full set on partition n
"U--- PtSet # Exit"	User n started the exit process for part set on partition n
"U-- Rem Download"	Downloader session completed successfully
"U-- Set Override"	User n overrode set fail
"U--- Shunt Code"	User n Shunt code used
"U-- Soc. Emergency"	User n has triggered a social-care alert from pendant
"U-- Spch Tel = Chg"	User changed speech dialler telephone number
"U--- System Exit"	User n started the exit process for full set on a part setting system
"U-- System PtSet #"	User n part set system
"U-- System Reset"	User n reset system
"U-- System Set"	User n set system
"U-- System Unset"	User n unset system
"U-- Time/Date"	User n changed time and/or date
"U-- Z== Omit"	User n omitted zone
"U--- Z=== HUA Omit"	User n omitted Hold Up Alarm zone n
"U--- Z=== Omit Rst"	User n included Hold Up Alarm zone n
"U--- Z=== Omit Rst"	User n included (restored) zone n
"Upgrade Aborted"	Control unit software upgrade has been aborted
"Upgrade Conn. Err."	Control unit unable to connect to software upgrade server
"Upgrade File Error"	Control unit software upgrade file error
"Upgrade Vrfy Fail"	Verification of control unit software file failed.
"Upgrade Write Err."	Failed to write new software to control unit
"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
"Walk Test Complete"	Detector walk test completed
"WAM== Battery Rstr"	WAM n low battery restored
"WAM== Low Battery"	WAM n has low battery
"WAM== PSU Fail"	WAM n has low power supply
"WAM== PSU Restore"	WAM n low power supply restored
"WAM== RF OK"	WAM n supervision OK
"WAM== RF Warning"	WAM n about to fail supervision
"WAM== Superv Fail"	WAM n has failed supervision
"WAM== Superv Rstr"	WAM n supervision restored
"WAM== Tamper Rstr"	WAM n tamper restored
"WAM== Tamper"	WAM n 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
"Wifi 12V Fail"	Control unit 12V Wi-Fi DC not working
"Wifi 12V Restore"	Control unit 12V Wi-Fi DC restored
"Wifi Signal Fault"	Wi-Fi signal lost
"Wifi Signal Rstr"	Wi-Fi signal restored
"WSN== Trouble Rstr"	Trouble message from wired siren n restored
"WSN== Trouble"	Trouble message from wired siren n input to control unit
"Z== Alarm Photos"	Photos from an IP camera are associated with a Zone n Alarm event
"Z== Closed"	Zone n quiescent
"Z== Follow Photos"	Photos from an IP camera are associated with a Zone n Folllow event
"Z== Jamming Rst"	Jamming restored on Radio Detector n
"Z== Jamming"	Jamming on Radio Detector n
"Z== Open"	Zone n activated
"Z== RF OK"	Radio zone n supervision OK
"Z== RF Warning"	Radio zone n about to fail supervision
"Z== Smoke Flt Rst"	Smoke detector at zone n has been restored
"Z== Smoke Flt"	Smoke detector at zone n has fault

"Z== Smoke PSU Flt"	Smoke detector at zone n has power supply fault
"Z== Smoke PSU Rst"	Smoke detector at zone n power supply fault restored
"Z=== Shunted"	Zone n is shunted
"Z=== UnShunted"	Zone n has been un-shunted
GPRS/3G Signal Rst	GPRS/3G module signal restored

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

Appendix C: Installer Menu Map

Important: The defaults listed below 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 available only if the relevant hardware is fitted, or for certain models of control unit.

MENU Option			Factory Default	Notes
1 Detectors/Devices				
Detectors	Add/Del Detectors	Panel		Available only for i-on30R+ and i-on40H+.
		Zone nnn...		
		Delete all		
		Exp. Rn-nn		Available only if a radio expander is fitted.
		Zone nnn...		
		Delete all		
		Delete all		
	Program Zones	Zone 000...		
		Name	"Zone nnn"	
		Type	Not used	
		Partitions	None	Available only in a partitioned system and when zones have a type other than "Not Used".
		Attributes	All "off", except Supervision	Available 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	Not available for i-on Compact.
Address Bus Device				Not available for i-on Compact.
Wired Expanders (Not available for i-on Compact)	Address Bus Device			
	Edit Expander	Expander Wn-01...		
		Name	"Exp. Wn-nn"	
		Partitions	Partition 1	Available only in a partitioned system.
		Wired zone type	FSL 2k2/4k7	
		Loudspeaker volume	Zero when expander first added to bus	
		Battery 2	Disabled	Available only for EXP-PSU and EXP-PSU-LM
	Delete Expander			
	Enable Expander		Yes	
	Replace Expander			

Radio Expanders (Not available for i-on Compact)	Address Bus Device			
	Edit Expander	Expander Rn-01...		
		Name	"Exp. Rn-nn"	
		Partitions	Partition 1	Available only in a partitioned system.
		Loudspeaker Volume		
	Delete Expander			
	Enable Expander		Yes (all expanders enabled).	
	Replace Expander			
Wired Keypads (Not available for i-on Compact)	Address Bus Device			
	Edit Keypad	Keypad Kn-51...		
		Name	"Keypad Kn-nn".	
		Partitions	Partition 1	Available only in a partitioned system.
		Key A	Name: "Key A" Action: Partition 1 Full Set OR Full Set in a Part Setting System	
		Key B	Name: "Key B" Action: Partition 2 Full Set OR Part Set B in a Part Setting System	
		Key C	Name: "Key C" Action: Partition 3 Full Set OR Part Set C in a Part Setting System	
		Key D	Name: "Key D" Action: Partition 4 Full Set OR Part Set D in a Part Setting System	
		Zones	Disabled	Available only when a suitable keypad is fitted.
		Wired Zone Type	2K2/4K7	
		Loudspeaker Volume		
		Buzzer Volume		
		Backlight		
		Internal Prox	Enabled	
		External Prox	Disabled	
		Virtual Kpd		
		Name		
		Partitions		
		Key A		
		Key B		
		Key C		
		Key D		
	Delete Keypad			
	Enable Keypad		Yes (all keypads enabled)	
	Replace Keypad			
On-board Keypad (i-on Compact only)	Key A	Name	Key A	
		Action	Set – Full Set	
	Key B	Name	Key B	
		Action	Set – Part Set B	
	Key C	Name	Key C	
		Action	Set – Part Set C	
	Key D	Name	Key D	
		Action	Set – Part Set D	
	ABCD Led		Enabled	
	Audible Keys		Enabled	
	Status fault		Enabled	
	Status OK		Enabled	
	Backlight	Mode	Timed	
		Brightness	Normal	
	Internal Prox		Enabled	
Radio	i-rk01			
	Add/Del Radio Keypad			

Keypads	Edit Keypads	Radio Kpd 01...		
		Name	"Radio Kpd 0n"	
		Partitions	Partition 1	Available only in a partitioned system.
		Key A	Name: "Key A" Action: Partition 1 Full Set OR Full Set in a Part Setting System	
		Key B	Name: "Key B" Action: Partition 2 Full Set OR Part Set B in a Part Setting System	
		Key C	Name: "Key C" Action: Partition 3 Full Set OR Part Set C in a Part Setting System	
		Key D	Name: "Key D" Action: Partition 4 Full Set OR Part Set D in a Part Setting System	
	KEY-RAS			
	Add/Del Radio Keypad			
	Edit Keypads	Radio Kpd 01...		
		Name	"Radio Kpd 0n"	
		Partitions	Partition 1	Available only in a partitioned system.
		Key A	Name: "Key A" Action: Partition 1 Full Set OR Full Set in a Part Setting System	
		Key B	Name: "Key B" Action: Partition 2 Full Set OR Part Set B in a Part Setting System	
		Key C	Name: "Key C" Action: Partition 3 Full Set OR Part Set C in a Part Setting System	
		Key D	Name: "Key D" Action: Partition 4 Full Set OR Part Set D in a Part Setting System	
		Sounder Volume		
		Battery Only	Yes	
	KEY-RKPZ			Not available for i-on Compact.
	Address Bus Device			
	Edit Keypad	Keypad Kn-51...		
		Name	"Keypad Kn-nn".	
		Partitions	Partition 1	Available only in a partitioned system.
		Key A	Name: "Key A" Action: Partition 1 Full Set OR Full Set in a Part Setting System	
		Key B	Name: "Key B" Action: Partition 2 Full Set OR Part Set B in a Part Setting System	
		Key C	Name: "Key C" Action: Partition 3 Full Set OR Part Set C in a Part Setting System	
		Key D	Name: "Key D" Action: Partition 4 Full Set OR Part Set D in a Part Setting System	
		Zones	Disabled	
		Internal Prox	Enabled	
		Wired Zone Type	2K2/4K7	
	Delete Keypad			
	Enable Keypad		Yes (all keypads enabled)	
	Replace Keypad			

External Sirens	Add/Del Siren			
	Edit Siren	Radio SRN 01...		
		Name		
		Partitions	Partition 01	Available only in a partitioned system.
		Supervision	Enabled	
Internal Sounders	Add/Del Sounder			
	Edit Sounder	Int. SNDR 01...		
		Name	"Int. SNDR nn"	
		Partitions	Partition 01	Available only in a partitioned system.
		Supervision	Enabled	
		Volume	0	
WAMs	Add/Del WAM			
	Edit WAM			
Cameras	IP Cam 1...	Camera Triggers	None	
		Zone Follow		
		Zone Alarm		
		Trigger Partitions	All Partitions	Available only in a partitioned system.
		IP Address		
		HTTP Port Internal	80	
2 Outputs				
Radio outputs	Add Outputs			
	Edit Outputs	Panel		Available only for i-on30R+ and i-on40H+.
		EDIT O/P PAN>01... or EDIT RADIO O/P n		
		Name	"O/P PAN>nn R"	
		Type	Not used	
		Pulsed	No	
		Partitions	Partition 1	Available only in a partitioned system.
		Delay	0 seconds	Available when Pulsed set to “Yes”.
		On Time	1 second	
		Zones	None	Available only for Zone Follow and Zone Alarm output types
		Exp. Rn-nn		Available only when a radio expander is fitted.
		EDIT O/P Rn>nn>nn		
		Name	"Rn>nn>nn"	
		Type	Not used	
		Pulsed	No	
		Partitions	Partition 1	Available only in a partitioned system.
		Delay	0 seconds	Available when Pulsed set to “Yes”.
		On Time	1 second	
		Zones	None	Available only for Zone Follow and Zone Alarm output types
Wired outputs (Not available for i-on Compact)	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	
		Latched	No	For User-Defined output type.
		Pulsed	No	Not available for dedicated siren and strobe outputs.
		Partitions	All outputs allocated to all Partitions	Available only in a partitioned system.
		Delay	0 seconds	Available when Pulsed set to “Yes”.
		On Time	1 second	

		Zones	None	Available only for Zone Follow and Zone Alarm output types.
	Exp. Wn-nn	EDIT *output*		Available only when a wired expander is fitted.
		Name		
		Type	Not used	
		Polarity	Normal	
		Latched	No	For User-Defined output type.
		Pulsed	No	
		Partitions	All outputs allocated to all Partitions	Available only in a partitioned system.
		Delay	0 seconds	Available when Pulsed set to “Yes”.
		On Time	1 second	
		Zones	None	Available only for Zone Follow and Zone Alarm output types.
	Keypad kn-nn	EDIT *output*		Available only when a suitable keypad is fitted.
		Name		
		Type	Not used	
		Polarity	Normal	
		Latched	No	For User-Defined output type.
		Pulsed	No	
		Partitions	All outputs allocated to all Partitions	Available only in a partitioned system.
		Delay	0 seconds	Available when Pulsed set to “Yes”.
		On Time	1 second	
		Zones	None	Available only for Zone Follow and Zone Alarm output types.
Plug-by outputs (Not available for i-on Compact)	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 O/P13: Ext PSU Low Volts O/P14: Ext PSU Fault O/P15: 24 Hour Alarm O/P16: RF Fault	The number of available plug-by outputs is dependent on the control unit model.
		Polarity	Normal	
		Latched	No	For User-Defined output type.
		Pulsed	No	
		Partitions	All outputs allocated to all Partitions.	Available only in a partitioned system.
		Delay	0 seconds	Available when Pulsed set to “Yes”.
		On Time	1 second	
		Zones	None	Available only for Zone Follow and Zone Alarm output types.
Custom Outputs (Not available for i-on Compact)	Custom Output 1...	Mode	Any (Or)	
		Inputs	None	
3 Partitions (only shown in a partitioned system)				
Partition 1...	Name		“Partition n”	
	Full Set Name		"Full Set"	
	Exit Mode		Timed Set (Partition 2 onwards defaults to the same as partition 1)	
	Settle Time		10 seconds	Available only if Exit Mode is “Final Door Set”, “Lock Set” or “Exit Terminate”.

	Confirm Set		On	Available only if Exit Mode is “Silent Set”.
	Exit Time		40 seconds	Available only if Exit Mode is “Timed Set” or “Silent Set”.
	Entry Time		40 seconds	
	Extended Entry Time		40 seconds	
	Linked Zone Time		10 seconds	Available only if there is a zone that has the "Linked Zone" attribute.
	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 B/C/D (available only if a zone has a Part Set attribute)	Name	“Part Set B/C/D”	
		Exit Mode	Instant Set	
		Settle Time	15 seconds	Available only if Part Set Exit Mode is “Final Door Set” , “Lock Set” or “Exit Terminate”.
		Confirm Time		Available only if Exit Mode is “Silent Set”.
		Confirm Set	On	Available only if Exit Mode is “Silent Set”.
		Exit Time	40 seconds	Available only if Part Set Exit Mode is “Timed Set” or “Silent Set”.
		Entry Time	40 seconds	
		Extended 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	
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 (Not available for i-on Compact)	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			
	Force Set		On	
3 Setting Options (only shown in a part-setting system)				
Full Set	Name		"Full Set"	
	Exit Mode		Timed Set	
	Settle Time		15 seconds	Available only if Exit Mode is "Final Door Set".
	Confirm Set		On	Available only if Exit Mode is "Silent Set".
	Exit Time		40 seconds	Available only if Exit Mode is "Timed Set" or "Silent Set".
	Entry Time		40 seconds	
	Extended 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 (available only if a zone has a Part Set attribute)	Name		"Part Set B/C/D"	
	Exit Mode		Instant Set	
	Settle Time		15 seconds	Available only if Exit Mode is "Final Door Set".
	Confirm Set		On	Available only if Exit Mode is "Silent Set".
	Exit Time		40 seconds	Available only if Exit Mode is "Timed Set" or "Silent Set".
	Entry Time		40 seconds	
	Extended Entry Time		40 seconds	
	Linked Zone Time		10 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 (Not available for i-on Compact)	Add Event	Event 01...		
		Event Time	00:00	
		Event Days	No for all days	
		Event Actions	Full Set	
		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	Full Set	
		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			
	Force Set		On	
4 System Options				
User Options	User Access	HUA keys active	No	
		Quick set	No	
		Quick omit	No	
		User code reqd	Yes	
		2 Way Replies	Yes	Available only when a FOB-2W-4B is assigned.
		2W Set Instant	Yes	
		Duress Enable	No	Not available for i-on Compact.
		Terminated Set	Yes	Used for KEY-EP.
		Tamper Omit	No	
		Silence Alerts	User Code	
		Wi-Fi Setup	No	Available only if a Wi-Fi module fitted.
	User Reset	Zone alarms	Yes	Available only if Confirmation Mode is "Basic".
		Zone tampers	Grade 2: Yes. Grade 3: No.	
		System tampers	Grade 2: Yes. Grade 3: No.	
		Code Tampers	Grade 2: Yes. Grade 3: No.	
		CSID Code	0000	
	Keypad Text		Model name	
Restore Defaults	Staged defaults	Users		
		User 001		
		Zones		
		Radio Devices		
		Outputs		
		Setting Info		
		System Options		
		Communications		
	Factory defaults			
	Part set mode/Partition mode			
Installer Options	Installer Name		"Installer"	
	Inst Tel Number			
	Installer Email			
	Inst Contract Num			
	Installer Code		Installer configured	
	Installer Remote Password		Installer configured	
	Installer Timeout		60 minutes	
	Service Date		01/01/1900	
	Service Banner		Disabled	
Confirmation	Confirmation Mode	DD243		These options are available only when the country version is the UK. For all other countries, Basic is used.
		BS8243	Default for UK systems	
		Basic		
	Confirmation Time		30 minutes	Available for BS8243 or DD243.
	Entry Alarm Delay		Yes	
	After Entry		1 zones	Available for BS8243 or DD243. Default changes to 2 zones when Confirmation Mode = DD243.

	Entry Keypad Lock		Off	Available for BS8243 or DD243.
	Sounder on		Unconfirmed	
	Siren on		Unconfirmed	
	Unconfirmed reset		User	Available for BS8243 or DD243.
	Confirmed reset		Installer	Available for BS8243 or DD243.
	HUA Response		Audible	Available only for part-setting systems.
	HUA Confirm Time		8 hours	Available for BS8243 only.
	Tamp as Tamp-Only		Enabled	Available for BS8243 only.
	Abort Time		120 seconds	
	Auto Rearm		Never	Available only in EU control units or when Confirmation Mode is “Basic”.
Hardware	Panel Name			
	Wired Zone Type	Panel Zones	2 Wire FSL 2k2/4k7	Available only if the control unit supports wired zones.
		All Zones	2 Wire FSL 2k2/4k7	Available only if a device connected to the bus supports wired zones.
	On-board Sounder (i-on Compact only)	Volume	4	
		Partitions		Available only in a partitioned system.
	Panel Loudspeaker	Partitions	All	Not available for i-on Compact. *Partitions* is available only in a partitioned system.
		Volume	4	
	A/C Fail Reporting		On	i-on Compact only.
	Mains Fail Delay		0 minutes	
	Ext DC Fail Reporting		Off	i-on Compact only.
	Ext DC Fail Delay		0 minutes	i-on Compact only.
	Comms Antenna		Internal/External	Available only if a module that supports mobile or WI-Fi communications is fitted.
	Panel Tamper Return		CC	Not available for i-on Compact.
	Reset Codes Pins		Enabled	
Radio Options	Supervision		Tamper	
	Jamming		Tamper	
	Remotes	Remote needs Entry	Disabled	Available only if the control unit has learnt a remote control.
		Remote Entry PrtSt	Disabled	
		Force Set	Off	
	Radio Keypads	RKP needs Entry	Disabled	Available only if the control unit has learnt an i-RK01 or KEY-RAS keypad.
		RKP Entry PrtSt	Disabled	
		Force Set	Off	
Masking Options	Masking		Grade 2: Off. Grade 3: On.	Not available for i-on Compact. *Mask Override* is available only when Masking is On.
	Mask Override		On	
Perimeter Options	PZ Unset Response		Silent	Available only for a part-setting system and if there is a zone of type “Perimeter”. The Partitions menu contains the equivalent options for a partitioned system.
	PZ Set Response		Silent	
	PZ Reset Time		0	
Shunt Groups	Shunt Group 1...			Not available for i-on Compact.
Date and Time	Set Date & Time			
	SNTP Time Sync	SNTP Enable	Off	
		Sync on Startup	Off	
		Sync Interval	Off	
		Manual Sync		
Updates	Language		English	
	Panel Upgrade			
	Level 4 Update		Disabled	
Backup/ Restore	Backup to SD Card			
	Restore from SD Card			
Social Care	Start Monitoring Hr		08:00	
	End Monitoring Hour		20:00	
	Monitoring Interval		4 hours	
	Social Alarm Response		Audible	
	Medical Alarm Response		Audible	

6 Communications				
Contacts	Recipient A...	Name	Recipient A	
		Tel No 1	Empty	
		Tel No 2	Empty	
		IP Address	Empty	
ARC Reporting	Call Mode		Single	
	Telecoms Priority	LAN	1	
	Recipients	Tel. Recipient 1	None	
		Tel. Recipient 2	None	
		IP Recipient 1	None	
		IP Recipient 2	None	
	Account Numbers		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	Available 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	Available only when Report Type is SIA or CID. Masking is not available for i-on Compact.
	Restorals		Enabled	
	Burg Comms Rearm		Enabled	Available only if Confirmation Mode is Basic and Report Type is Fast Format.
	21CN FF Ack time		800ms	Available only if Report Type is Fast Format and a COM-SD-PSTN or COM-SD-GSM module is fitted.
	Dynamic Test Call		Enabled	Available only if Static Test Call is disabled.
	Static Test Call		Disabled	Available only if Dynamic Test Call is disabled.
	Unset Comms		Enabled	
Speech Dialler	Call Mode		Disabled	Available only if a COM-SD-PSTN or COM-SD-GSM module is fitted.
	Messages		None	
	Triggers		None	
	Destinations			
	Call Acknowledge		Enabled	
SMS	Outgoing	Call Mode	Disabled	SMS is available only if a COM-SD-GSM or COM-SD-PSTN module is fitted.
		Messages	Blank	Available only if Call Mode is enabled. PSTN SMS is available only if a COM-SD-PSTN module is fitted.
		Triggers	None	
		Destinations		
		PSTN SMS		
	Incoming	Forwarding	None	Available only if a COM-SD-GSM module is fitted.
Line Fail	Panel Ethernet		Silent	
	Module:		Silent	Available only if a module is fitted.

Response	Plug-by		Silent	Not available for i-on Compact.
Line Fail Delay	Panel Ethernet		9s	
	Module:		9s	Available only if a module is fitted.
	Plug-by		9s	Not available for i-on Compact.
IP Options	Cloud Access	Enabled	No	
		Cloud Time Sync	Daily	
		Cloud Push Fail	Silent	
		Offline Response	Silent	
		Offline Delay	360 minutes	
	Module: 4G/3G/2G	Data Mode	Mobile as backup	Available only if a COM-DATA-4G module is fitted.
		Network Type	Auto	
		Network Selection	Auto	
		Provider	Other	
		Edit APN		
		Comms Antenna	Internal/External	
		Primary Path Rpt	Enabled	
		Secondary Path Rpt	Enabled	
	Module: Wi-Fi	Network		Available only if a Wi-Fi module is fitted. The IP Address, IP Subnet Mask, Gateway IP Address and DNS IP Address options are displayed only if DHCP is Disabled.
		WPS		
		DHCP	Enabled	
		IP Address		
		IP Subnet Mask		
		Gateway IP Address		
		DNS IP Address		
		Comms Antenna	Internal/External	
	Module: 4G/3G/2G-Wi-Fi	4G/3G/2G		
		Wi-Fi		
	Panel Ethernet	DHCP	Enabled	
		IP Address		Displayed only if DHCP is Disabled.
		IP Subnet Mask	Blank	
		Gateway IP Address	Blank	
		DNS IP Address	Blank	
	LAN	Web Server		
		Status	Disabled	
		Port	80	Displayed only if Status is Enabled.
		User Timeout	1 minute	Displayed only if Status is Enabled.
Send Tamp as Burg			Disabled	
7 Test				
Sirens & Sounders	Ext. Radio Sirens			Available only if a radio siren is used.
	On-board Sounder			i-on Compact only.
	Wired Sirens			Not available for i-on Compact.
	Loudspeakers			
	Wired Keypads			
	KEY-RKPZ			
	KEY-RAS			Available only if a KEY-RAS is used.
	Internal Sounders			Available only if an internal sounder is used.
Wired Keypad				Not available for i-on Compact.
On-board Keypad				i-on Compact only.
Radio Keypads	i-rk01			Available only if a radio keypad is used.
	KEY-RAS			
	KEY-RKPZ			
Expanders	Exp. W/ Rn-nn-...			Not available for i-on Compact.

Walk Test	Chime		Once	
	System			
	Partitions			Available only for a partitioned system.
	Expanders			Not available for i-on Compact.
	Zones			
Zone Resistances				Available only in systems that have wired zones.
Zone Status	Wired Zones			
	Radio Zones			
Signal Strengths	Detectors			The menu contains options only for those device types that have been added.
	Radio Keypads	i-rk01		
		KEY-RAS		
		KEY-RKPZ		
	External Sirens			
	WAMs			
	Internal Sounders			
Outputs	Radio Outputs			
	Wired Outputs			Not available for i-on Compact.
	Plug-by outputs			Not available for i-on Compact.
	Expander Outputs			Not available for i-on Compact.
Remotes				
Pendants				
User HUDs				
Prox Tags				
ARC Reporting				
Speech Dialler				
SMS				SMS is available only if a COM-SD-GSM or COM-SD-PSTN module is fitted.
PSU Current	Panel			Not available for i-on Compact.
	Exp. Wn-...			Available only if a remote power supply is fitted.
Panel PSU				i-on Compact and i-on20R only.
Battery(s)				
Locate Panel				Not available for i-on Compact.
Locate Bus Device				Not available for i-on Compact.
Network				
8 View Log				
All Events				
Mandatory Events				
Non-Mand. Events				
9 ABOUT				
Panel				
Installer				
Bus				Not available for i-on Compact.
Cloud				
Expanders				Not available for i-on Compact.
Keypads				Not available for i-on Compact.
Comms	Module			
	Panel Ethernet			
Zone Mapping	Zone Numbers			Not available for i-on Compact.
	Zone Addresses			

SecureConnect is a trademark of Eaton

www.myscantronic.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 14199581 Issue 3 24th January 2022