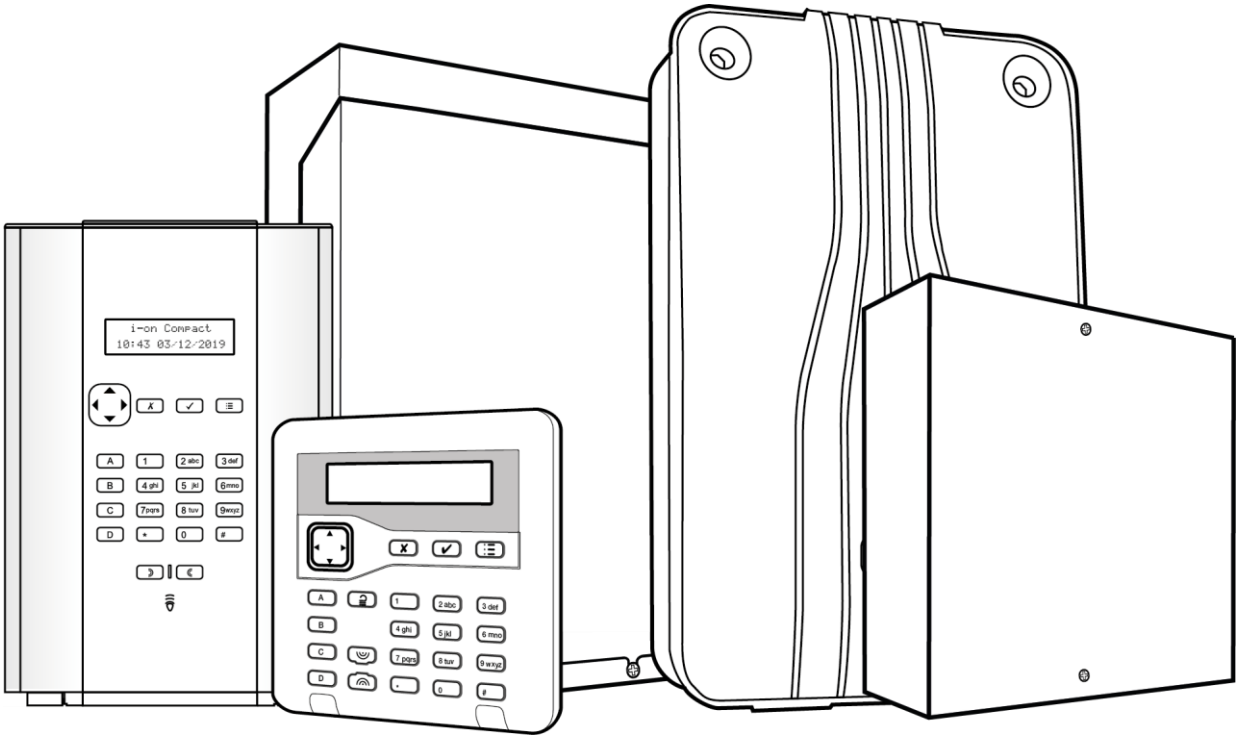
i-on Series
Security System

Installation Manual

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



Issue 1

Control unit software version 6.0.xx

Scantronic

About this Manual

This manual explains:

- The architecture and components of i-on alarm systems.
- System limits, such as the maximum number of zones and bus devices per control unit.
- How to plan the installation of an i-on alarm system.
- How to install an i-on control unit. **Note:** this information is also available in the installation instructions provided with each control unit.

This manual does **not** cover:

- The configuration (programming) of control units – this is covered in the *Configuration Guide*.
- How to install devices other than the control unit – this is covered in the installation instructions provided with each device.

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 Configuration Guide** – This gives full details of how to configure (program) i-on control units. It covers all options in the Installer menu.
- **SecureConnect™ Installer Guide** – This provides an overview of SecureConnect, explains how to set up the system and describes how to manage control units using the SecureConnect web portal.

Contents

Chapter 1: Introduction

About the i-on range of control units

The i-on range of control units have been designed to satisfy the most demanding requirements of alarm-systems professionals for domestic, commercial and industrial applications. The control units are flexible, easy to install and robust. The i-on range supports wired, wirefree or hybrid applications.

The modular approach of i-on alarm systems allows the design to match site requirements and maximise cost-efficiency.

Five different models of control unit are available for different sizes and types of application:

- **i-on Compact**. This is a radio (wire-free) solution for domestic applications. The i-on Compact has a built-in keypad and supports up to 20 radio zones (detectors).
- **i-on30R+**. This provides on-board support for 30 radio zones, and supports a system maximum of 60 zones. Any combination of radio and wired zones can be used. The i-on30R+ uses a plastic enclosure.
- **i-on40H+**. This provides on-board support for 30 radio zones and 10 wired zones, and supports a system maximum of 80 zones. The i-on40H+ uses a plastic enclosure.
- **i-onG2SM**. This provides on-board support for 10 wired zones, and supports a system maximum of 50 zones. The i-onG2SM is compliant with grade 2 (as are all control units in the range), and uses a Small Metal (SM) enclosure.
- **i-onG3MM**. This provides on-board support for 10 wired zones, and supports a system maximum of 200 zones. The i-onG3MM is grade compliant, and uses a Medium Metal (MM) enclosure.

Summary of features

The i-on range of control units feature:

- Grade 2 compliance for all control units; grade 3 compliance for the i-onG3MM.
- A bus for connection to devices such as wired keypads and expanders (not i-on Compact). Expanders provide additional zones up to the system maximum shown in Table 1.
- An on-board radio transceiver (not i-onG2SM and i-onG3MM), which has a range of up to 500m and supports devices such as radio detectors, Scantronic radio siren/strobe units and radio outputs.
- Sockets for an optional plug-on communicator (required for grade 2/3).
- Terminals for a plug-by communicator (depending on the control unit).
- Cloud access using the freely-available SecureConnect™ application. SecureConnect provides web access for installers to configure the system, allows users to operate the system remotely from a mobile app, and carries out background tasks such as to send alarm notifications by email or over the internet to an ARC.

- An Ethernet port for optional use of the web interface, network cameras and SecureConnect™.
- The ability to configure the system using:
  - A standard keypad on the bus (not i-on Compact).
  - A engineer keypad connected directly to the engineer keypad port (not i-on Compact).
  - The control unit's built-in web interface, optionally via SecureConnect.
- A micro-SD card for local mass storage of images from network cameras, and for updating system firmware.
- Support for multiple partitions (not i-on Compact).
- On-board outputs and wired zones (depending on the control unit).
- On-board connections for a wired siren/strobe unit (not i-on Compact).
- On-board connections for an external loudspeaker (not i-on Compact).

Table 1 specifies the features and system limits for each control unit.

Table 1: Overview of features

	Feature	i-on Compact	i-on30R+	i-on40H+	i-onG2SM	i-onG3MM
	EN 50131 security grade	2	2	2	2	3
Zones	Max on-board radio zones	20	30	30	0	0
	Max on-board wired zones (Note 6)	0	0	10	10	10
	Max zones on expanders, keypads, etc.	0	30	40	40	190
	Max wired and radio zones (system wide)	20	60	80	50	200
Bus	RS485 Buses	0	1	1	1	2
	Max bus devices (Note 8)	0	20	20	20	50
Outputs	Max on-board radio outputs	20	10	10	0	0
	On-board transistor outputs	0	2	2	1	2
	On-board relay outputs	0	0	2	0	2
	Max outputs on expanders, keypads, etc.	0	30	40	50	200
	On-board plug-by outputs	0	0	12	12	16
	On-board siren\strobe connections	No	Yes	Yes	Yes	Yes
	Max custom outputs	0	4	4	5	20
	Max outputs (system wide) (Note 5)	20	30	40	50	200
Ports	Ethernet port	Yes	Yes	Yes	Yes	Yes
	Plug-on module port	Yes	Yes	Yes	Yes	Yes
	USB port	Yes	No	No	No	No
	On-board loudspeaker connections	0	1	1	1	1
	Micro SD card slot	Yes	Yes	Yes	Yes	Yes
Devices	Max wired keypads (Note 2)	0	20	20	20	50
	Max i-rk01 and KEY-RAS radio keypads (Note 3)	2	4	4	5	20
	Max external radio siren\strobe units (Note 4)	2	4	4	5	20
	Max network cameras	2	4	4	5	20

	Max internal radio sounders (Note 4)	2	4	4	5	20
	Max Wireless Access Modules	2	4	4	5	20
Case	Control unit case	Plastic	Plastic	Plastic	Metal	Metal
	Battery (Note 7)	1 (2.2Ah)	1 (7Ah)	1 (7Ah)	1 (7Ah)	1 (17Ah)
	Power Supply Unit (PSU)	0.5A	1.0A	1.0A	1.0A	2.0A
	PSU current reserved for battery charging	100mA	180mA	180mA	180mA	750mA
	Back and lid tamper	Yes	Yes	Yes	Yes	Yes
Software	Users	20	30	50	50	200
	Part sets (including per partition in partitioned mode)	3	3	3	3	3
	Max partitions (see Note 1)	0	4	4	5	20
	Mandatory log events	250	750	750	750	1500
	Non-mandatory log events	50	250	250	750	1500
	Calendar set events	0	10	10	10	50
	Calendar set exceptions	0	30	30	30	30
	Max shunt groups	0	4	4	5	20
	Max simultaneous keypad sessions	1	4	4	5	10
	Web interface	Yes	Yes	Yes	Yes	Yes
	SecureConnect and web browser interface	Yes	Yes	Yes	Yes	Yes
	Firmware update via web interface, cloud auto update, or SD card	Yes	Yes	Yes	Yes	Yes
	Firmware update via USB port	Yes	No	No	No	No
	Multilanguage support (-EU variant)	Yes	Yes	Yes	Yes	Yes

Note 1: Each partition can have three part-set levels. Partitions are not available for i-on Compact.

Note 2: The maximum number of wired keypads is the same as the maximum number of bus devices, but decreases by one for each expander or KEY-RKPZ that is added. A KEY-RKPZ is a radio keypad that uses a KEY-RKBS base station wired to the bus. Up to two KEY-RKPZ keypads can connect to the same base station, but this feature cannot be used to increase the total number of keypads beyond the limit shown in Table 1.

Note 3: The maximum number of i-rk01 and KEY-RAS radio keypads is in addition to the maximum number of wired keypads.

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

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

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

Note 7: The maximum sizes of batteries are given. A battery is supplied only for i-on Compact.

Note 8: The i-onG3MM has two busses. The limit of 50 devices is the combined total of all devices on both busses. You cannot connect 50 devices to each bus.

System bus

All control units except the i-on Compact have a system bus to connect devices such as wired keypads, expanders, remote power supplies and base stations (for KEY-RKPZ keypads). The i-onG3MM has two busses. The bus architecture allows the system to be easily expanded to accommodate additional devices if the need arises.

Devices can connect to a bus using a "daisy chain" or star layout, as shown in Figure 1.

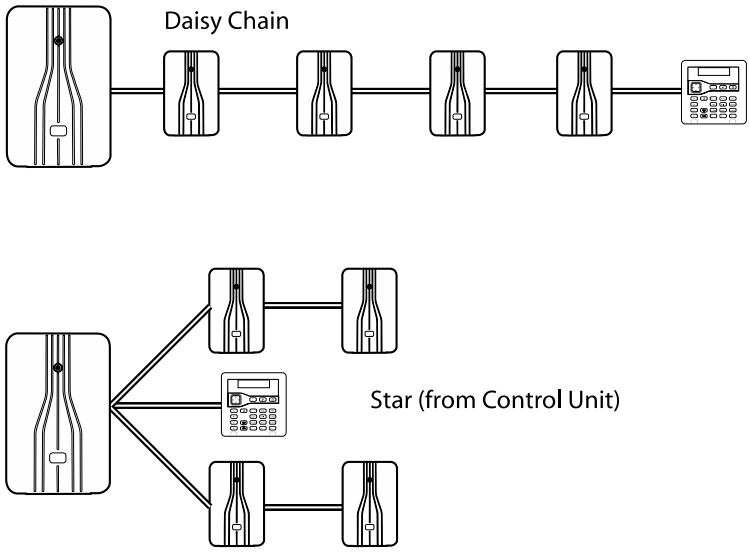


Figure 1. Daisy chain and star connections

Bus address

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

For the i-onG3MM, the address is unique across both busses, so unlike previous-generation i-on systems, the same address does not exist in both busses. The system As an installer, you have complete flexibility to add a device to either bus. A benefit of the two-bus i-onG3MM is that if there is a cable fault on one bus, it does not affect the other bus.

Part-setting and partitioned modes

All control units except i-on Compact offer part-setting and partitioned modes. The i-on Compact offers part-setting mode only.

Part-setting mode

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

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

Partitioned mode

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

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

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

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

Grade 2 or grade 3 compliance

All of the control units are suitable for use in systems conforming to security grade 2 requirements.

The i-onG3MM can be used in either security grade 2 or 3 alarm systems. During initial power up (and if you reset a system to factory defaults), you can choose grade 2 or 3, which automatically sets various system options for either grade 2 or grade 3 compliance.

- **Grade 2:** The system uses four-digit user codes, turns masking off, sets *System Options – User Options – User Reset – Zone Tampers* to Yes, and communicates tampers as alarms.

  If you install any radio devices, this will limit approval to grade 2 in the partition in which they are used. For a part-setting system, the whole system will be limited to grade 2.

  For grade 2, you must fit at least an ATS2 communicator (for example the COM-SD-PSTN).

- **Grade 3:** The system uses six-digit user codes, turns masking on, sets *System Options – User Options – User Reset – Zone Tampers* to No. The system communicates tampers as tampers.

  For grade 3, you must use the plug-by communicator outputs to connect the control unit to an ATS4 communicator. The communicator must be able to transmit a mains-fail condition.

  Note: If the system uses radio HUDs, and no other radio transmitters, the system can be approved as grade 3, provided the rest of the system meets grade 3 standards.

You can override any of the settings by selecting individual options in other parts of the Installer Menu. Note that if you do so, the system may no longer comply with the selected Grade.

Supported hardware devices

This section gives an overview of the purpose of each type of additional hardware device.

Keypads

Keypads are used by installers to configure the system, and by users to set or unset the system.

The i-on30R+, i-on40H+, i-onG2Sm and i-onG3MM can use radio keypads, or wired keypads connected to the system bus. The i-on Compact has a built-in keypad, and can also use radio keypads.

The various types of keypad are described in the following sections. Table 1 specifies the number of keypads supported by each control unit. Table 2 on page 12 shows the features supported by each type of keypad.

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

Wired keypads

Wired keypads (not available for i-on Compact) connect to the bus. There are several different models of wired keypads that offer different styling and features:

KEY-K01	A wired keypad only.
i-kp01	A wired keypad with built-in proximity reader.
KEY-KP01	A wired keypad, with a built-in proximity reader, and terminals for a KEY-EP external proximity reader.
KEY-KPZ01	A wired keypad, with built-in proximity reader, two on-board zones, one programmable output, and terminals for a KEY-EP external proximity reader.
KEY-FKPZ	A wired flush-mount keypad, with built-in proximity reader, two on-board zones, one programmable output, terminals for an external loudspeaker, and terminals for a KEY-EP external proximity reader. The keypad is available in a range of colours and finishes.

Radio keypads

i-RK01	A one-way battery-powered radio keypad for setting/unsetting, with a built-in proximity reader. This keypad communicates directly to a control unit that has built-in radio communications, or to a radio expander.
KEY-RKPZ	A two-way battery-powered radio keypad, with built-in proximity reader, LCD display and two on-board zones. This keypad communicates over a radio link to a base station connected to the bus, which acts as a communications bridge between the keypad and the control unit. You can use a KEY-RKPZ in the same way as a wired keypad to configure the system, set or unset the system, etc.
KEY-RAS	A two-way radio keypad that can be used to set/unset the system, display the current set/unset status, and to sound entry, exit and alarm tones. The keypad also features a built-in proximity reader, and can be powered by batteries or from an external DC supply. This keypad communicates directly to a control unit that has built-in radio communications, or to a radio expander.

Summary of keypad features

Table 2: Keypad features

Feature	KEY-K01	i-kp01	KEY-KP01	KEY-KPZ01	KEY-FKPZ	i-RK01	KEY-RKPZ	KEY-RAS	i-on Compact keypad
Wired keypad	Yes	Yes	Yes	Yes	Yes	No	No	No	-
Radio keypad	No	No	No	No	No	Yes	Yes	Yes	-
Built-in proximity reader	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
KEY-EP external proximity reader terminals	No	No	Yes	Yes	Yes	No	No	No	No
Zones	0	0	0	2	2	0	0	2	-
Outputs	0	0	0	1	1	0	0	0	-
Loudspeakers	0	0	0	0	1	0	0	0	-
Two-line by 20-character backlit LCD display	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Illuminated four-way switch (the “navigation key”), which is used to navigate through menus	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
LEDs behind the navigation key to show the fault status of the system	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Numeric keypad for entering access codes and keying in text	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dedicated A, B, C and D keys, which can be programmed to set individual partitions or part sets (as applicable), or allocated to control outputs.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Keys for “yes”, “no” functions	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Unset key	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hold-Up Alarm (HUA) keys	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
User menu key and an automatic timeout from the user menu	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Internal sounder to give setting tones, alarm sounds, etc	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Backlit keys	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Engineering keypad

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

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

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

KEY-EP external proximity tag reader

A KEY-EP external proximity tag reader can connect to a KEY-KP01, KEY-KPZ01 or KEY-FKPZ keypad to enable the system to be to set or unset externally.

Many keypads also include an internal proximity tag reader.

Detectors (zones)

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

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

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

Wired detectors

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

Please refer to page 22 for details of the different wiring methods you can use for wired detectors.

Note: If 4-wire CC wiring is used, this may reduce the available number of zones; see page 23.

All wired detectors with contacts that open and close are supported, as there is no protocol involved.

Radio detectors

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

The following radio detectors are supported:

DET-RDC	Slimline door contact
DET-REXT-PIR30	External perimeter PIR
DET-REXT-IR50/100	Barrier detectors
DET-RS	Shock or movement detector
XCELR	PIR
XCELRPT	Pet-tolerant PIR
DET-RDT	Combined microwave and PIR detector
720rEUR-00	Smoke detector
DET-RSMOKE	Smoke Detector
705REUR-00	Hand-held dual-channel transmitter
706rEUR-00	10mW tilt switch and personal attack transmitter.
710rEUR-00	Dual-button personal attack transmitter

713rEUR-00	Pet-tolerant PIR
714rEUR-00	PIR
726rEUR-50	Long-range hand-held personal attack transmitter
726rEUR-60	Short-range hand-held personal attack transmitter
734rEUR-00	CC door contact - white
734rEUR-01	FSL door contact - white
734rEUR-05	CC door contact - brown
734rEUR-06	FSL door contact - brown
738rEUR-00	Spyder shock sensor – white
738rEUR-04	Spyder shock sensor – brown
DET-RDCS	Spyder shock sensor and door contact combined
739rEUR-00	Sentrol glass-break without tamper
DET-RWATER	Flood detector
DET-RARB	Request-for-assistance button
703R	Universal transmitter

Expanders

Expanders provide additional connections for zones, outputs and loudspeakers, up to the limits specified in Table 1 (not available for i-on Compact).

Wired expanders

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

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

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

Radio expanders

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

- Two i-RK01 or KEY-RAS radio keypads.
- Two external radio sirens.
- Two internal radio sounders.
- Two Wireless Accessory Modules (WAMs).
- One wired loudspeaker.

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

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

Communicators

Plug-by (digital communicator)

All control units except i-on Compact and i-on30R+ include a built-in plug-by communicator, which allows the system to communicate externally to an alarms-receiving site using a separate digital communicator (purchased separately).

Table 1 shows the number of plug-by outputs available on each control unit. By default, the outputs are switched negative (from 12Vdc to 0V) when active. You can program these outputs to be switched positive (from 0V to 12Vdc) when active.

Note: SIA IP (SIA over the network) is available by connecting the control unit to the internet and configuring SIP IP communications in SecureConnect.

Plug-on modules

All control units can also communicate externally using a plug-on module. the following plug-on modules are supported:

COM-SD-PSTN	A speech dialler and PSTN (Public Switched Telephone Network) module. This allows control units to report alarm conditions over a wired telephone network using standard ARC protocols (FF, SIA or CID), recorded speech messages or SMS texts.
COM-SD-GSM	A speech dialler and GSM (Global System for Mobile communication) module. This allows control units to report alarm conditions over a 2G mobile phone network using standard ARC protocols (FF, SIA or CID), recorded speech messages or SMS texts. A SIM card is required. Preferably, a "pay-as-you-go" tariff should not be used. **Note:** The use of GSM for ARC communication is not recommended, as the networks often distort the audio tones, which can cause the communication to fail. If you use GSM and experience difficulties, try a different format (such as Contact ID). Alternatively, IP communications via an optional COM-DATA-4G plug-on module will provide a more robust and reliable solution.
COM-DATA-4G	The COM-DATA-4G module allows a control unit to access the SecureConnect service over the internet using LTE and GSM (4G and 2G) mobile phone networks. A SIM card is required that supports 4G and 2G data. A data allowance of 250MB per month should be sufficient to cover normal activity in a typical installation. Preferably, a "pay-as-you-go" tariff should not be used.

The COM-SD-GSM and COM-DATA-4G have a built-in antenna, which is suitable in most cases. If the location of the control unit has poor signal strength, an external antenna (COM-ANT-01) can be purchased, which must be fitted outside of the control unit.

Output devices

Devices such as indicators, lighting systems or third-party equipment can be switched on or off using "outputs" available from the i-on system. You can configure outputs in the Installer menu to control the external devices when, for example there is an alarm in a specified zone, mains is disconnected or a combination of specified conditions occur.

The following types of output are available:

- Wired outputs. These are available on some control units, keypads, expanders and remote power supplies, depending on the model used. Table 1 shows the number of wired outputs available on each control unit. There are two types of wired output:
    - Transistor (open collector) – By default, these are switched negative (from 12Vdc to 0V) when active; you can program them to be switched positive (from 0V to 12Vdc).
    - Relay – These provide voltage-free changeover contacts. You connect one side of the external device to the C (Common) terminal, and the other to either NO (Normally Open) or NC (Normally Closed) side of the relay, depending on the application.
- Radio outputs. These connect directly to a control unit that has built-in radio communications, or to a radio expander.
- Dedicated outputs on the control unit for a siren/strobe unit (not available for i-on Compact) – see the next section.
- Plug-by outputs (not available for i-on Compact or i-on30R+), used for communicating alarms to an Alarms Receiving Centre (ARC); see page 15.

Sounders

Sounders indicate alarms, entry tones, exit tones and other conditions. A sounder is built into the i-on Compact control unit and into all types of keypad except the i-RK01. There are various types of additional sounders, as described next.

External wired siren/strobe units

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

The following external wired siren/strobe units are supported:

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

External radio sirens/strobes

Radio siren/strobe units can communicate directly to control units that have built-in radio communications, or to radio expanders. Table 1 specifies the number of external radio siren/strobe units that each type of control unit can support.

The following external radio siren/strobe units are supported:

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

Internal radio sounders

SND-RINT internal radio sounders are intended for use in areas that are out of audio range of keypads, but where users need to hear system sounds.

Internal radio sounders can communicate directly to control units that have built-in radio communications, or to radio expanders. Table 1 specifies the number of internal radio sounders that each type of control unit can support.

Loudspeakers

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

Cameras

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

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

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

Remote power supplies

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

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

The EXP-PSU connects to the system bus (see page 26), and communicates with the control unit in the same way as a wired expander.

Remote controls

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

The following devices are supported:

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

WiFi module

An i-wifi01 module allows any i-on control unit to connect wirelessly to the network. The module is mounted inside the control unit and connects to the Ethernet port.

Other supported radio devices

The following radio devices are also supported:

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

About SecureConnect

Any i-on control unit can connect to the internet to access the SecureConnect service. The key features of SecureConnect include the following:

- SecureConnect enables installers to remotely configure, manage and monitor multiple control units using a web browser over the internet.
- Users can remotely operate their alarm system using the SecureConnect app.
- The SecureConnect service can keep the time at control units automatically updated, send emails (including camera images) automatically when events occur, and report alarms to an Alarms Receiving Centre (ARC) over the internet.

Updating 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 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.
- 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.

Chapter 2: Planning the Installation

Choosing the installation locations

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

Control unit

The control unit must be located:

- Within the protected area (but not in an entry or exit zone).
- Upright (battery at the bottom for all except i-on Compact) on a wall or other flat surface to discourage tamper attempts from the rear.
- Out of sight of potential intruders.
- Ideally, more than 2 metres from the floor.
- Where maximum cable distances will not be exceeded (see page 24).

Radio devices

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

Do not locate any radio device, control unit (with built-in radio capability), or radio expander:

- Near to any source of electromagnetic or radio interference.
- Within 1 metre of high-voltage cables, metal pipes, computers, photocopiers, or other electrical or electronic equipment.
- In a location where maximum radio range will be exceeded.
- In a metal enclosure or close to large metal structures.

Keypads and proximity readers

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

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

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

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

External sirens

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

Checking power availability

EN50131-1 or PD6662 Grade 2 requires the backup battery to be able to power the system for at least 12 hours. Grade 3 requires the backup battery to power the system for at least 30 hours. In both cases, the duration must including two 15-minute periods in alarm.

i-on Compact

For an i-on Compact, the backup battery (when fully charged) meets the requirements of EN50131-1 or PD6662 Grade 2.

Note: The 12Vdc output in an i-on Compact is not backed up by the battery. Therefore, a WiFi module powered by the 12Vdc output will not operate during a mains power failure.

i-on30R+, i-on40H+, i-onG2SM and i-onG3MM

For these control units, you must make sure that:

a) The control unit's power supply will have sufficient capacity to power all connected devices. The i-on30R+, i-on40H+, i-onG2SM have a 1.0A power supply, of which 180mA is reserved for battery charging. The i-onG3MM has a 2.0A power supply, of which 750mA is reserved for battery charging.

b) The backup battery can provide sufficient power in the event of a mains failure.

If there is insufficient power available from the control unit or backup battery, consider the use of remote power supplies (see pages 17 and 26).

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

Table 3 gives a summary of the current consumed by the i-on control unit PCBs and popular peripheral devices.

Table 3: Current Consumptions

Device	**Current Consumption (In Alarm)**
i-on30R+ PCB	Quiescent: 80mA In alarm: 90mA
i-on40H+ PCB	Quiescent: 90mA In alarm: 110mA
i-onG2SM PCB	Quiescent: 90mA In alarm: 110mA
i-onG3MM PCB	Quiescent: 100mA In alarm: 150mA
COM-SD-PSTN	Quiescent: 20mA In alarm: 30mA
COM-SD-GSM	Quiescent: 15 mA

	In alarm: 140mA
COM-DATA-4G	Quiescent: 15 mA In alarm: 240mA
Wired expander	20mA (no sounder connected)
Wired PIR	15mA
KEY-FKPZ keypad	Quiescent: 25mA In alarm: 65mA
i-kp01 keypad	Quiescent: 30/40/60mA (backlight off/on/bright respectively) In alarm: 45/45/65mA (backlight off/on/bright respectively)
KEY-KPZ01, KEY-KP01 or KEY-K01 keypad	Quiescent: 35mA (backlight off, no external proximity reader) In alarm: 65mA (backlight on, external proximity reader fitted)
KEY-RKBS two-way keypad base station	35mA (buzzer off)
SDR-WEXT external siren/strobe	Quiescent: 35mA In alarm: 225mA

Worked example

The following shows a simplified example of checking power availability.

Device (quiescent)	**Current**
Control unit PCB (i-on30R+)	80mA
COM-SD-PSTN	20mA
10 x PIRs at 15mA each	150mA
1 x wired expanders	20mA
2 x KEY_FKPZ at 25mA each (backlights off)	50mA
Siren	35mA
Total	355mA

During an alarm, the current consumptions are:

Device (in alarm)	**Current**
Control unit PCB (i-on30R+)	90mA
COM-SD-PSTN	30mA
10 x PIRs at 15mA each	150mA
1 x wired expanders	20mA
2 x KEY_FKPZ at 65mA each	130mA
Siren	225mA
Total	645mA

Since the control unit's power supply can provide 820mA (excluding battery charging), the above shows that the power supply is able to power the system during an alarm (645mA).

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

(0.355A x 11.5h) + (0.645A x 0.5h) = 4.41Ah

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

Detector (zone) wiring types

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

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

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

The wiring types are as follows.

Fully Supervised Loop (FSL)

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

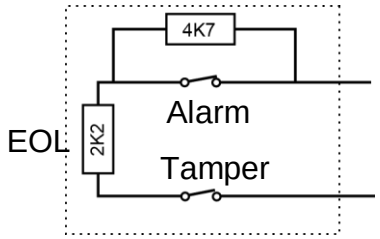


Figure 2. FSL connections (using 2k2 and 4k7 resistors)

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

Table 4: FSL Resistor Bands (without Masking)

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

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

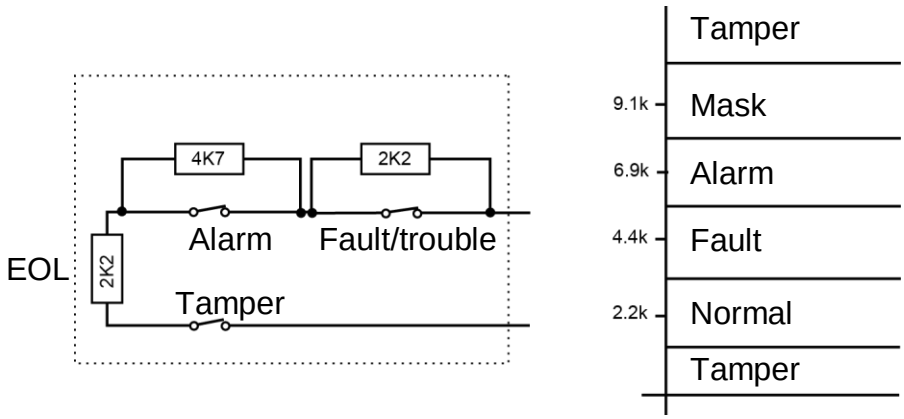


Figure 3. FSL connections with masking

4-wire CC

This uses a separate pair of wires for the alarm and tamper contacts. No end-of-line resistors are used. Selecting 4-wire CC may halve the maximum number of wired zones the device supports, as shown in Table 5.

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

Table 5: 4-Wire CC Zones

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

2-wire CC

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

Checking cable requirements

Standard cable type

Normally, the control unit requires standard 7/0.2 un-screened 4-core alarm cable for wiring to bus devices and wired siren/strobe units.

For bus cabling, use one pair for data lines A and B. Use the other pair for 12V and 0V.

Screened cable

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

If screened cable is required:

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

Cable segregation

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

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

Mains cable routing

Use separate cable-entry holes in the enclosure for mains and signal cables. Please refer to the figures in *Chapter 3: Installing i-on Control Units* for details of the holes to use for each type of cable.

Mains cable must be routed away from any aerials in the enclosure (i-on Compact and i-on30R+ only). For i-on Compact, please refer to Figure 7 on page 29. For i-on30R+, please refer to Figure 11 on page 32.

Cable length and configuration (star or daisy chain)

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

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

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

Bus termination

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

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

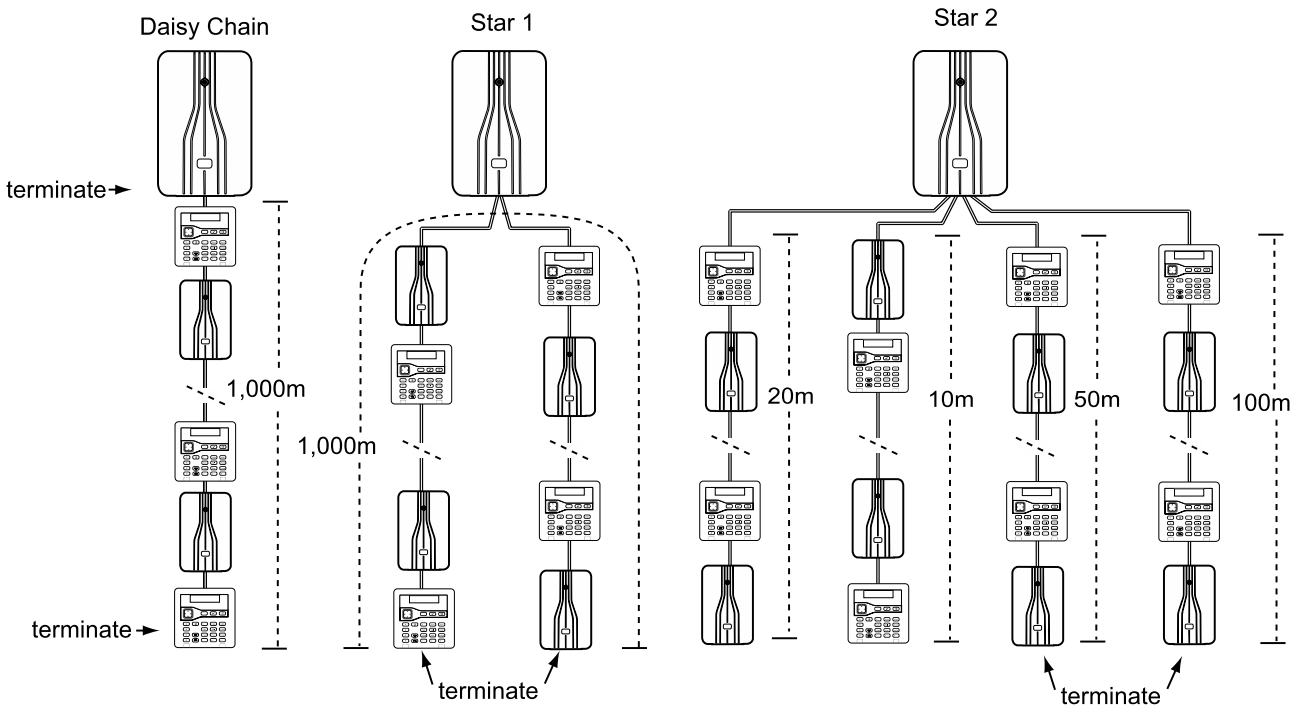


Figure 4. Bus termination

Voltage drop

In order for the system to work correctly, the voltage at each bus device must NOT drop below 10.5V (even when running on the standby battery), and preferably should stay above 12.0V to avoid unexpected behaviour. For a wired detector, the minimum voltage is generally 9.5V, but this depends on the detector type (see the detector instructions).

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

Table 6 shows the voltage drop against the current drawn and cable length. The shaded area shows where the voltage drop would cause the voltage to fall from 13.8V to below 12.0V when using a single core.

Table 6: Voltage drop along cable

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

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

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

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

Note that if detectors connect to expanders or other bus devices, the current along the bus is the total of the current drawn by the bus devices and detectors.

Using remote power supplies

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

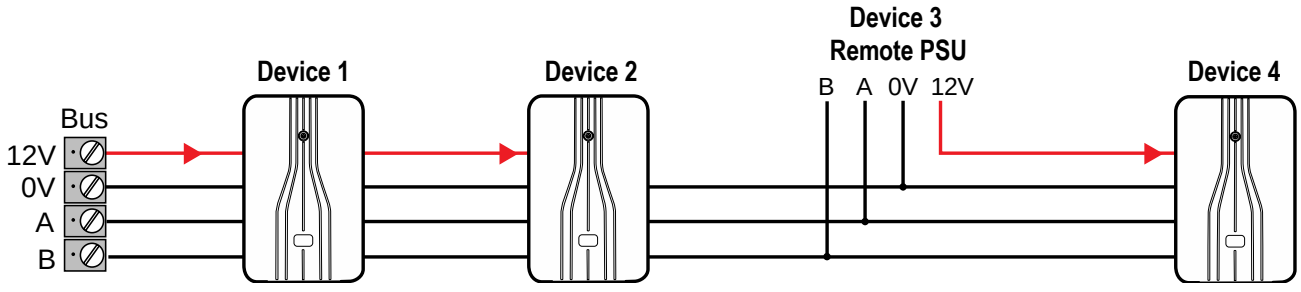


Figure 5. Connecting a remote power supply

Chapter 3: Installing i-on Control Units

This chapter explains how to install each type of control unit.

Note: The instructions in this chapter are the same as those to be found in the *Installation Instructions* enclosed provided with each control unit.

Safety Information

This product must be installed by qualified service personnel.

WARNING: BEFORE INSTALLING THIS EQUIPMENT, ENSURE THAT THE MAINS SUPPLY FOR THE CONTROL UNIT IS DISCONNECTED AND ISOLATED. All electrical connections must be carried out by a qualified electrician and comply with current local regulations.

WARNING: When connected to the mains with power applied, mains voltages are present on the shrouded heads of the terminal screws of the mains connector.

WARNING: The mains cable to the control unit must use a double-pole isolation device in accordance with EN 62368-1.

WARNING: Good practice requires that documentation is not stored within the enclosure.

Caution: If you need to handle the PCB in the control unit, take standard precautions to prevent damage by static electricity.

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

Pre-Installation Requirements

Before starting the installation, make sure that you have followed all the requirements specified in *Chapter 2: Planning the Installation*. This includes checking the power requirements, checking cable requirements and performing a radio survey (if applicable).

i-on Compact Installation Instructions

During installation, please refer to Figure 6 and to *Overview of PCB links, connectors and LEDs* on page 40.

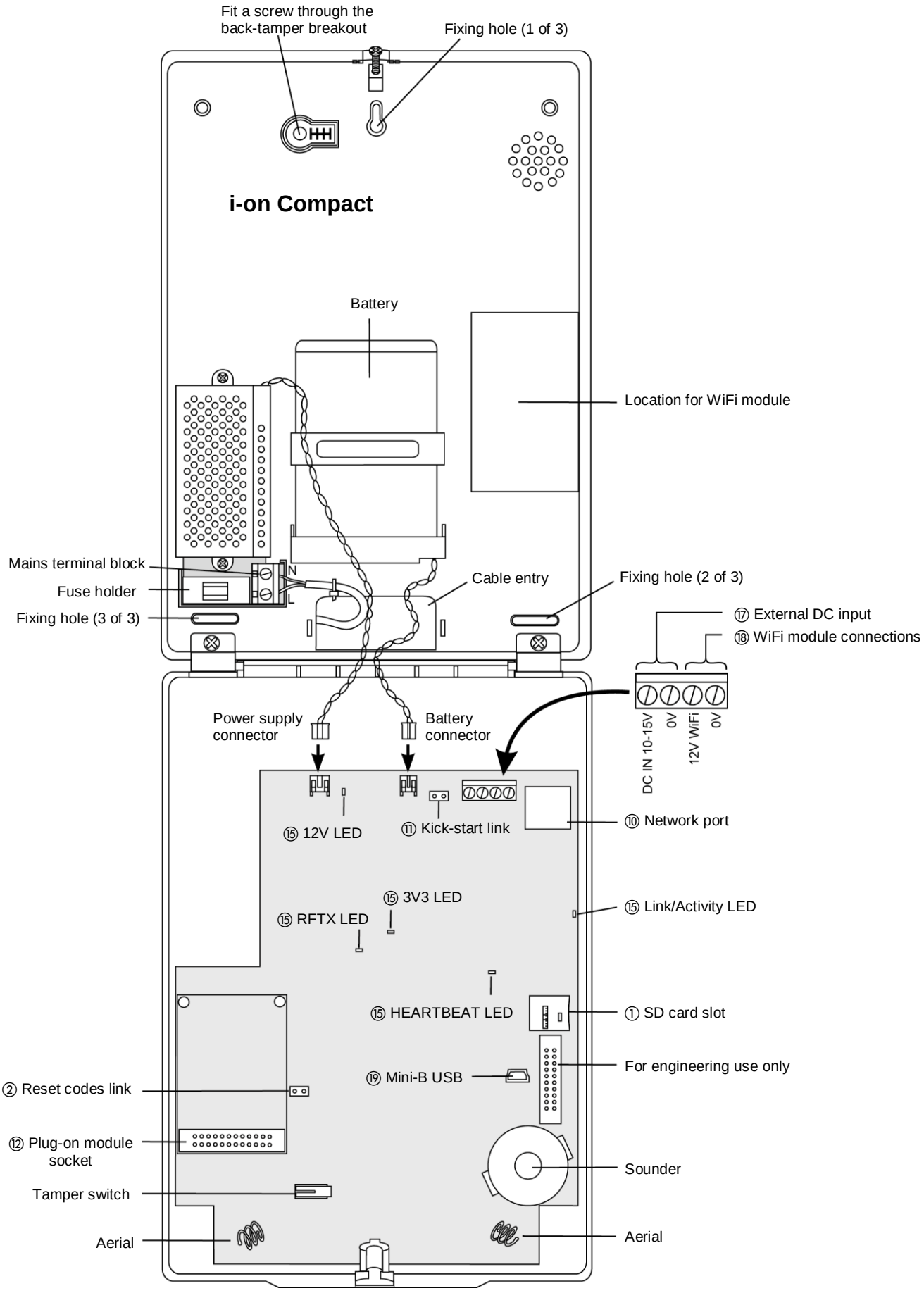


Figure 6. i-on Compact: Control unit Internals

Step 1: Install cables

Make sure mains cables are routed away from the internal aerials, as shown in Figure 7. Use only the dedicated cable-entry holes, as shown in Figure 6.

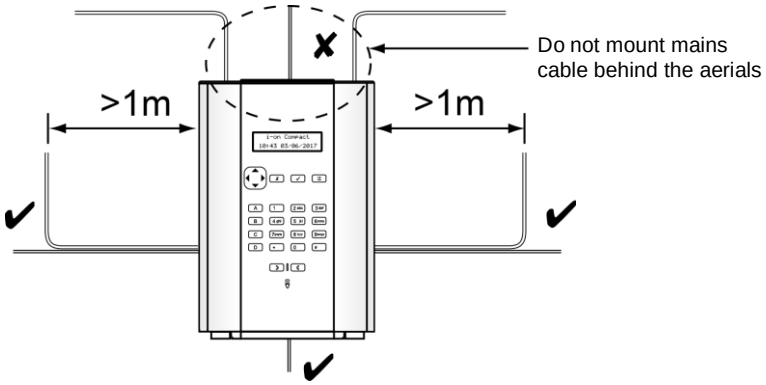


Figure 7. i-on Compact: Mains cable routing

Step 2: Open the control unit

1. Remove the screw located at the top of the lid.
2. Insert a small screwdriver into the screw recess and use it to lever open the lid, as shown in Figure 8 (the lid is hinged at the bottom).

   Note: When the control unit is firmly fixed to a wall, you should be able to open the lid without using a lever by releasing the screw and pulling the lid downwards.

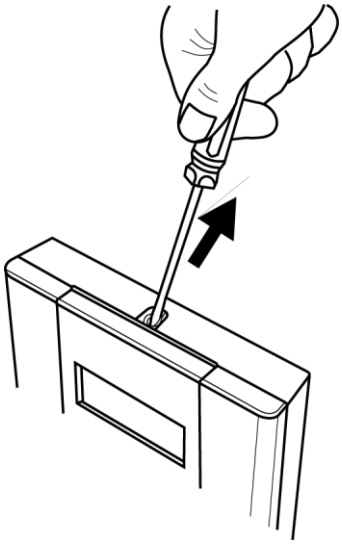


Figure 8. i-on Compact: Opening the lid

Step 3: Mount the control unit

Use minimum 36mm long No8/4mm screws through the three fixing holes and back-tamper breakout shown in Figure 6.

Important: Make sure you fit a screw through the back-tamper breakout. This enables the system to generate a tamper alarm in the event that the control unit is wrenched off the wall. Do not cut the webs on the breakout.

Step 4: Connect wiring and optional modules

WARNING: ENSURE THAT THE MAINS SUPPLY IS DISCONNECTED AND ISOLATED.

Connect a 2-core mains cable to the mains terminal block (Figure 6) and fit a strain-relief cable tie. Confirm the mains cable is routed as shown in Figure 7. Do not apply power until after the lid is closed (Step 6).

Fit any optional modules and other wiring to the main PCB as shown in Figure 6. DO NOT CONNECT THE BATTERY UNTIL STEP 5.

If you are using a plug-on module, connect the device as described in the module's installation instructions.

If you are using a WiFi module, mount the module in the location shown in Figure 6.

Step 5: Connect the battery

The battery pack provides at least 12 hours of operation in the event of a power fail.

Fit the battery and power supply connector to the PCB, as shown in Figure 6.

Step 6: Close the lid, switch on and configure the system

WARNING: An alarm tone may be generated when you apply power. If anyone is working near a siren, make sure that any sudden noise does not startle them and cause a fall, such as from a ladder.

Close the lid, refit the screw, then switch on the mains supply to the control unit.

Go through the initial configuration prompts and set up the system as described in the *Configuration Guide*. You are prompted to specify default master user and installer codes, and whether to enable Basic or Full configuration. Basic enables faster and simpler configuration and should be considered if connection to an Alarm Receiving Centre (ARC) is not required.

It is recommended that you connect the control unit to the internet and enable "Level 4 Update" in the installer and user menus. When you enter your installer code, the system can then check online whether later versions of the firmware or language file exist, and prompt you to install them. Please refer to the *Configuration Guide* for further details.

Step 7: Install additional devices

Install PIRs, door contacts, siren/strobe units, internal sounders and other required devices as described in the installation instructions provided with each device.

i-on30R+/40H+ Installation Instructions

During installation, please refer to Figure 9 and to *Overview of PCB links, connectors and LEDs* on page 40.

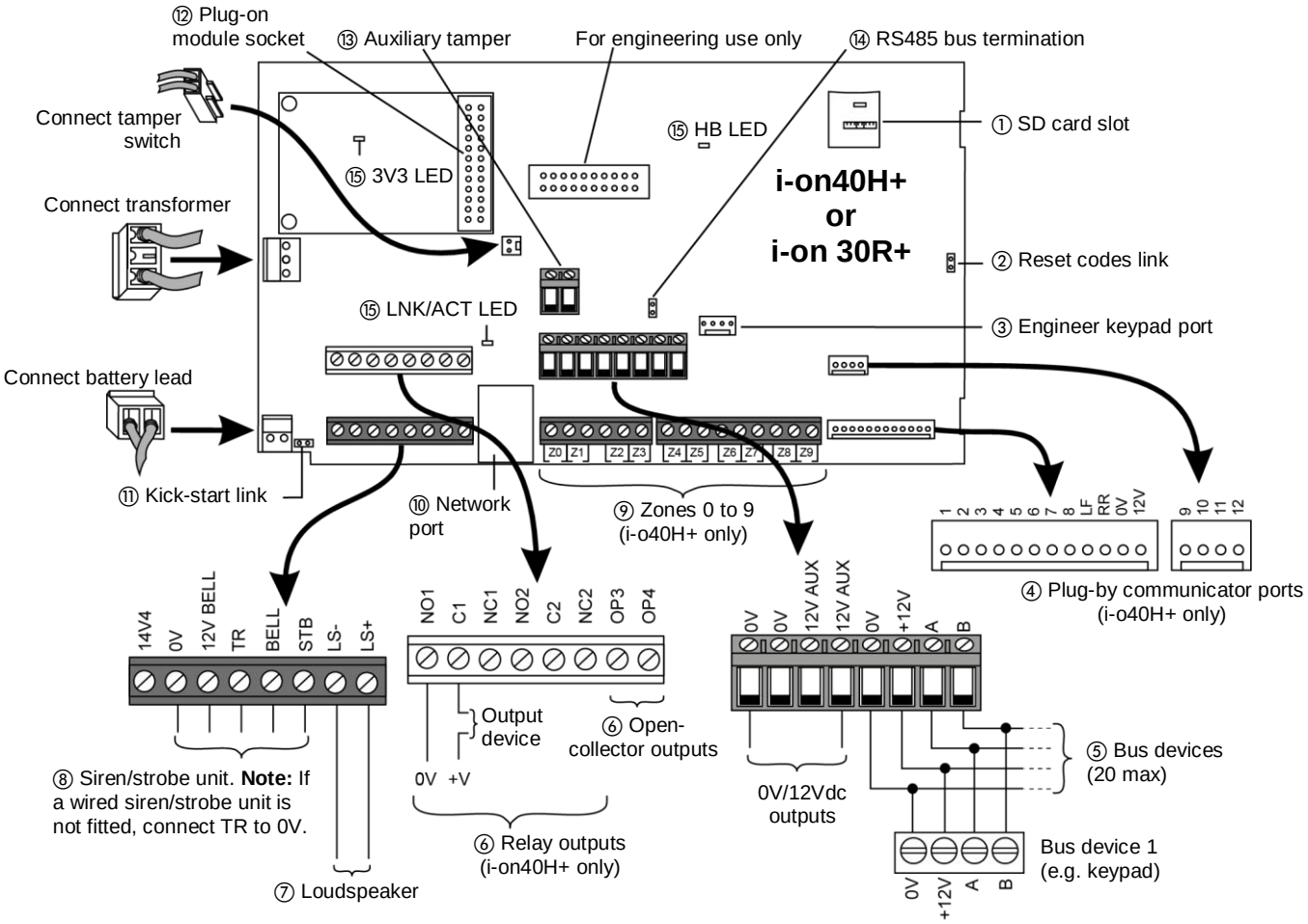


Figure 9. i-on30R+ and i-on40H+: Control unit PCB

Step 1: Install cables

Use only the dedicated cable-entry holes, as shown in Figure 10.

For an i-on30R+, make sure mains cables are routed away from the internal aerials, as shown in Figure 11.

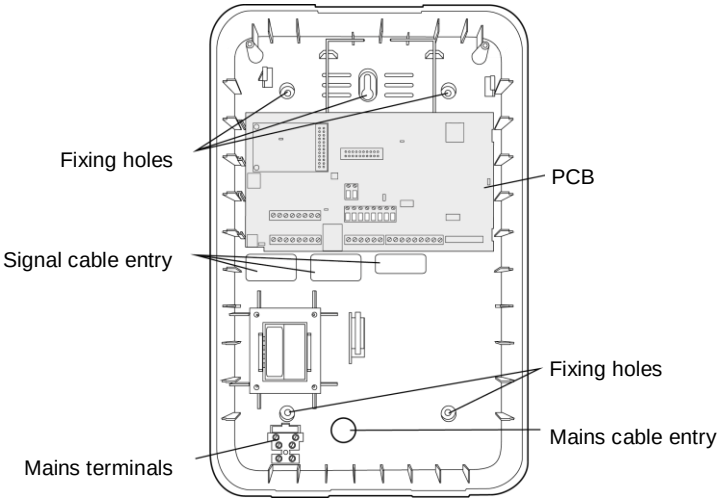


Figure 10. i-on30R+ and i-on40H+: Fixing holes and cable entries

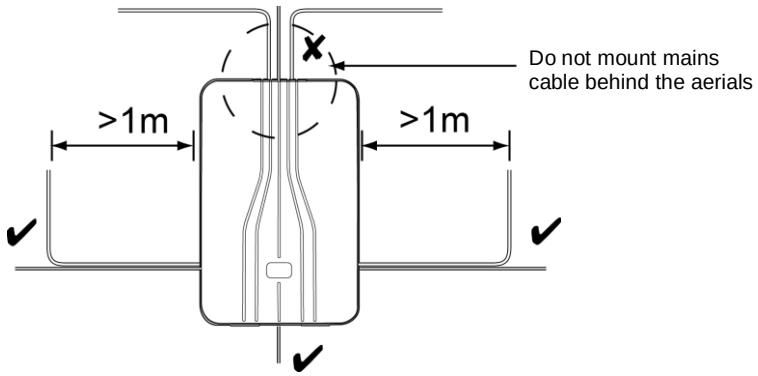


Figure 11. i-on30R+ and i-on40H+: Mains cable routing

Step 2: Remove the lid of the control unit

Release the two screws on the front of the lid, then lift it off.

Step 3: Fit the tamper switch and shroud

Fit the tamper switch assembly through the slot in the back of the case (Figure 12).

Also, for added security, fit the tamper shroud to the wall so that when you mount the control unit, the shroud will surround the arm of the tamper switch.

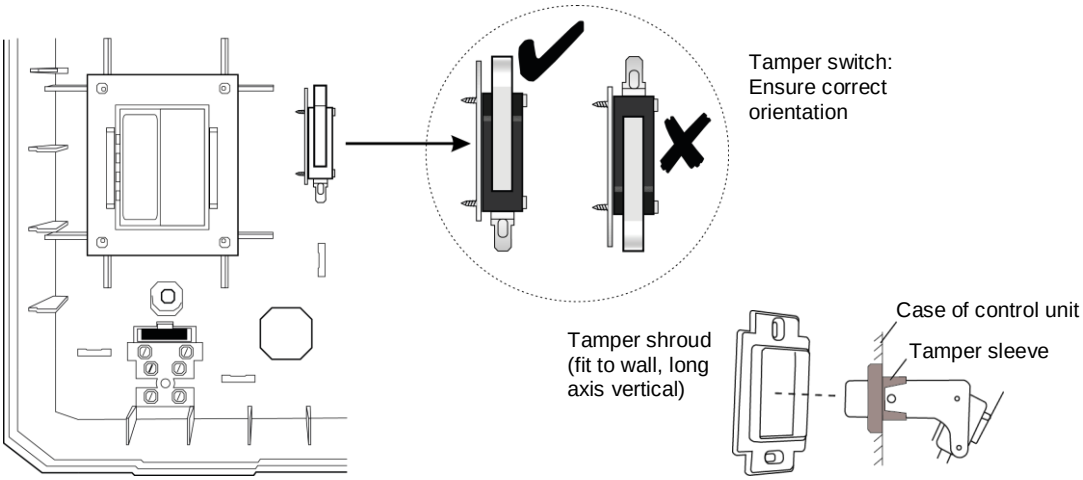


Figure 12. i-on30R+ and i-on40H+: Fitting the tamper switch and shroud

Step 4: Mount the control unit

Mount the control unit in the orientation shown in Figure 10 using at least 4 fixing holes and minimum 40mm long No10(5mm) screws. Use only the designated cable-entry holes.

Step 5: Connect all wired devices

Connect all wired devices except the battery, as shown in Figure 9.

If you are using a plug-on module, fit and connect the device as described in the module's installation instructions.

Step 6: Connect the battery

Note: Connecting the battery does not start the system.

Fit a 7Ah lead-acid battery in the bottom-right corner of the control unit and secure with a strap provided.

Connect the battery leads to the battery (red to positive and black to negative), and connect the other end to the PCB (Figure 9). Also connect the transformer lead to the PCB (Figure 9).

Step 7: Connect the mains cable

WARNING: ENSURE THAT THE MAINS SUPPLY IS DISCONNECTED AND ISOLATED.

Connect the mains cable to the terminal block (Figure13) and fit a strain-relief tie. Confirm the mains cable is routed as shown in Figure 11.

Do not apply power until after the lid is re-fitted.

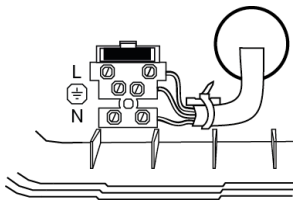


Figure 13. i-on30R+ and i-on40H+: Mains connections

Step 8: Re-fit the lid, switch on and configure the system

WARNING: During initial power-up, keypad sounders and any internal loudspeaker may give an alarm tone. If you are working at the top of a ladder, make sure that the sudden noise does not startle you and cause a fall.

Re-fit the lid, then switch on the mains supply to the control unit.

Go through the initial configuration prompts and set up the system as described in the *Configuration Guide*. You are prompted to specify installer and user codes during initial system configuration.

It is recommended that you connect the control unit to the internet and enable "Level 4 Update" in the installer and user menus. When you enter your installer code, the system can then check online whether later versions of the firmware or language file exist, and prompt you to install them. Please refer to the *Configuration Guide* for further details.

i-onG2SM Installation Instructions

During installation, please refer to Figure 14 and to *Overview of PCB links, connectors and LEDs* on page 40.

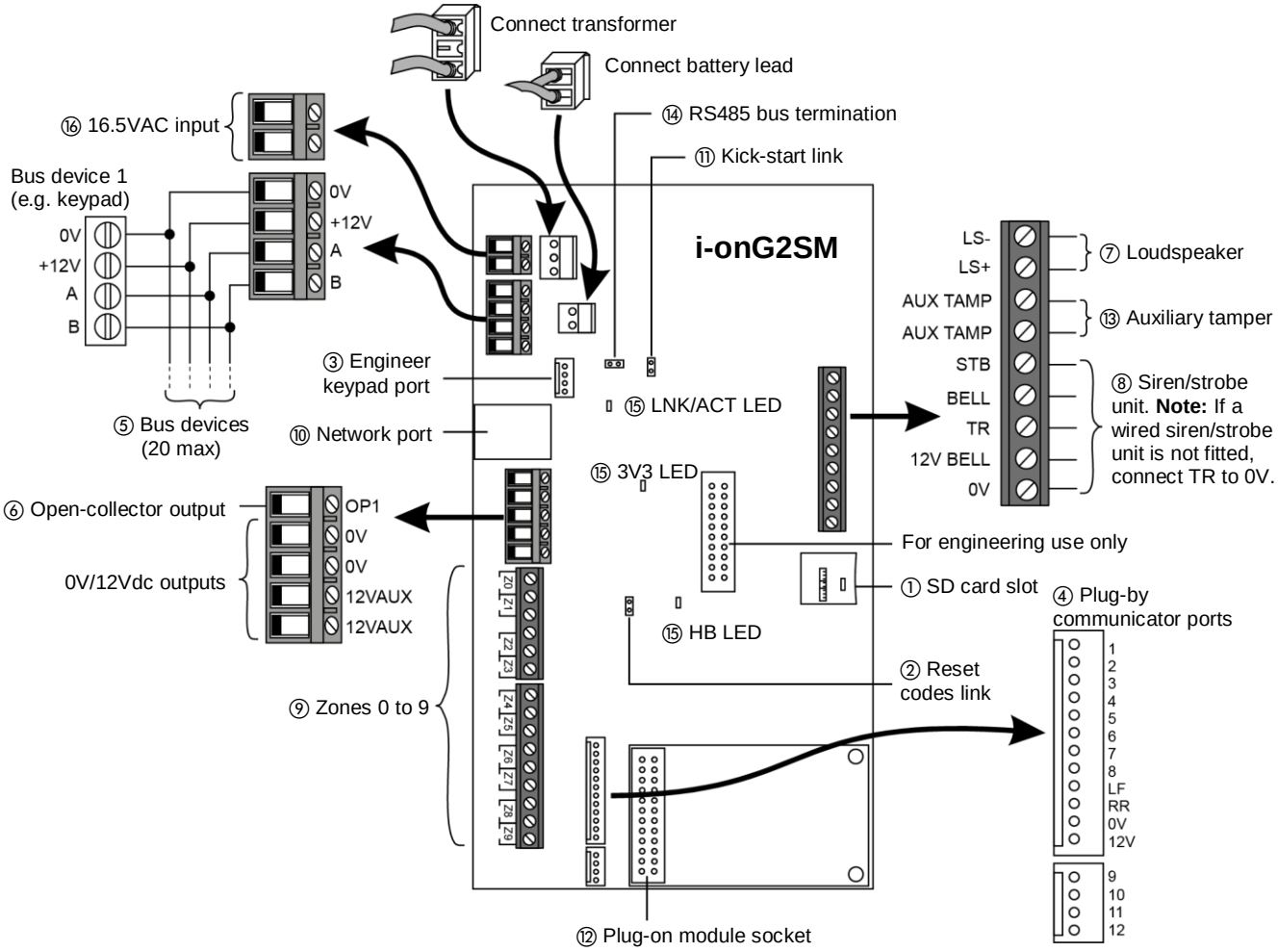


Figure 14. i-onG2SM: Control unit PCB

Step 1: Remove the lid of the control unit

Release the two screws on the front of the lid, then lift it off.

Step 2: Mount the control unit

Mount the control unit in the orientation shown in Figure 15 using the three fixing holes and minimum 40mm long No8 (4mm) screws. Use only the designated cable-entry holes.

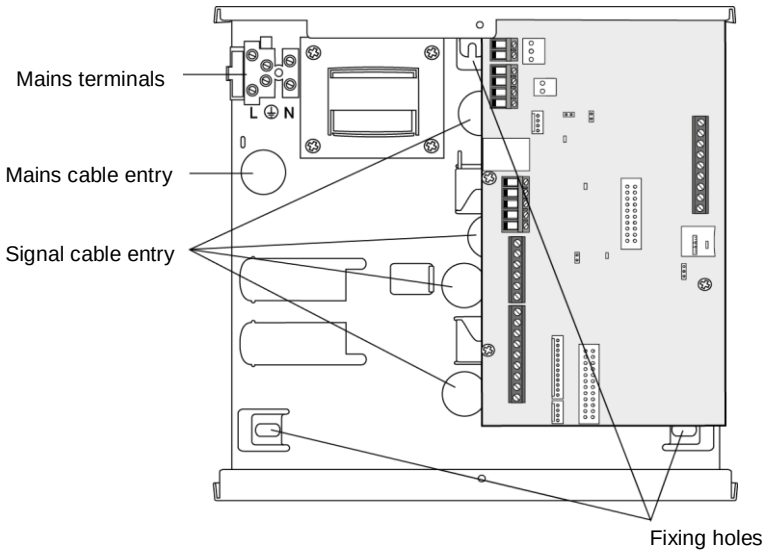


Figure 15. i-onG2SM: Fixing holes and cable entries

Step 3: Connect all wired devices

Connect all wired devices except the battery, as shown in Figure 14. If you are using a plug-on module, fit and connect the device as described in the module's installation instructions.

Step 4: Connect the battery

Note: Connecting the battery does not start the system.

Fit a 7Ah lead-acid battery in the bottom-left corner of the control unit.

Connect the battery leads to the battery (red to positive and black to negative), and connect the other end to the PCB (Figure 14). Also connect the transformer lead to the PCB (Figure 14).

Step 5: Connect the mains cable

WARNING: ENSURE THAT THE MAINS SUPPLY IS DISCONNECTED AND ISOLATED.

Connect the mains cable to the terminal block (Figure 16) and fit a strain-relief tie. Do not apply power until after the lid is re-fitted.

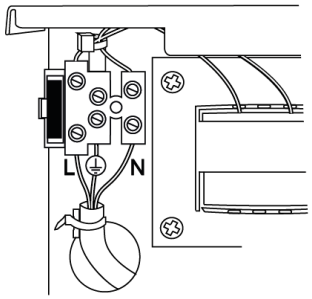


Figure 16. i-onG2SM: Mains connections

Step 6: Re-fit the lid, switch on and configure the system

WARNING: During initial power-up, keypad sounders and any internal loudspeaker may give an alarm tone. If you are working at the top of a ladder, make sure that the sudden noise does not startle you and cause a fall.

Re-fit the lid, then switch on the mains supply to the control unit.

Go through the initial configuration prompts and set up the system as described in the *Configuration Guide*. You are prompted to specify installer and user codes during initial system configuration.

It is recommended that you connect the control unit to the internet and enable “Level 4 Update” in the installer and user menus. When you enter your installer code, the system can then check online whether later versions of the firmware or language file exist, and prompt you to install them. Please refer to the *Configuration Guide* for further details.

i-onG3MM Installation Instructions

During installation, please refer to Figure 17 and to *Overview of PCB links, connectors and LEDs* on page 40.

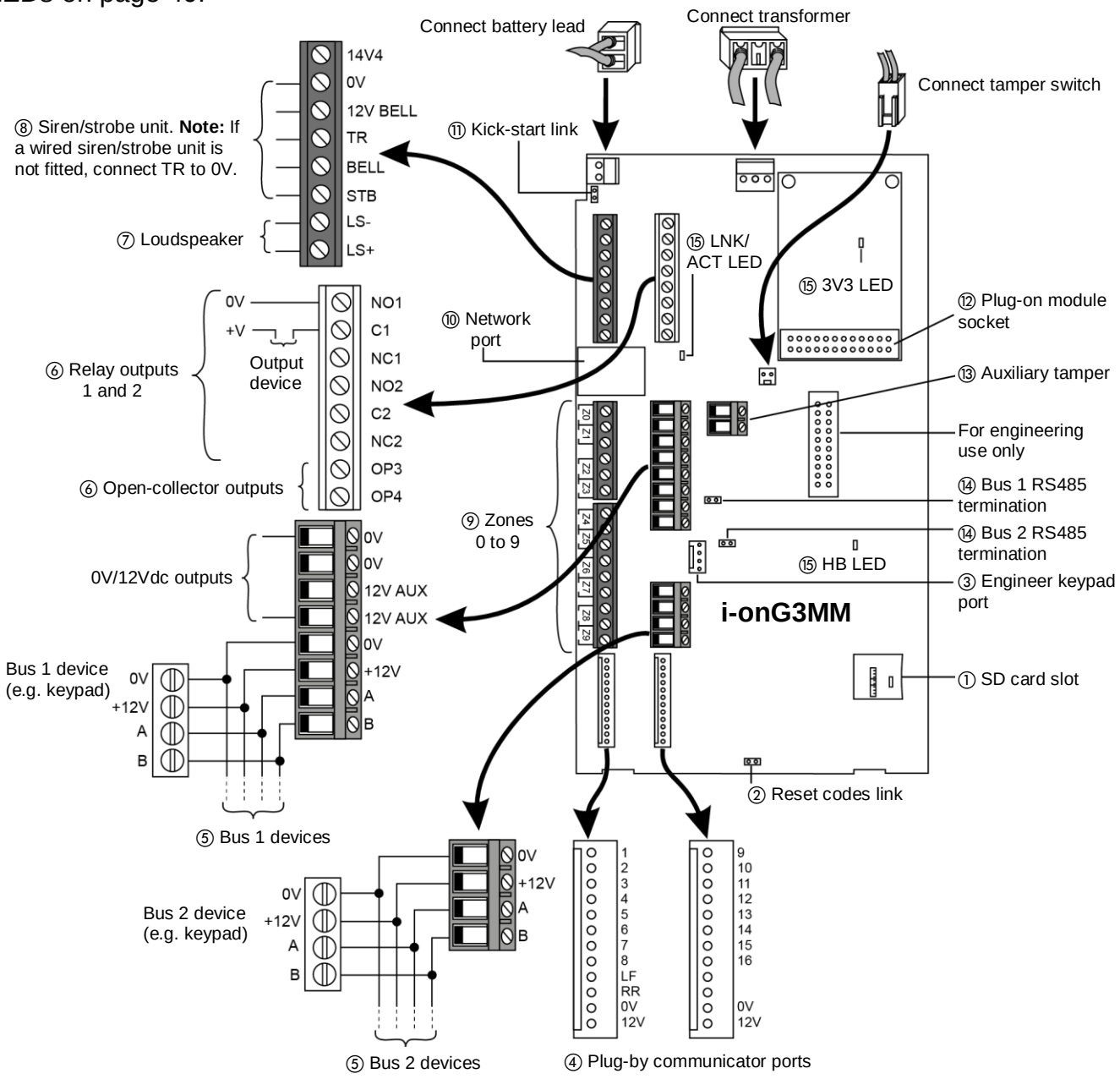


Figure 17. i-onG3MM: Control unit PCB

Step 1: Remove the lid of the control unit

Release the screw on the front of the lid, then lift it off.

Step 2: Fit the feet and tamper sleeve

Fit the supplied plastic feet and tamper sleeve to the bottom of the case, as shown in Figure 18.

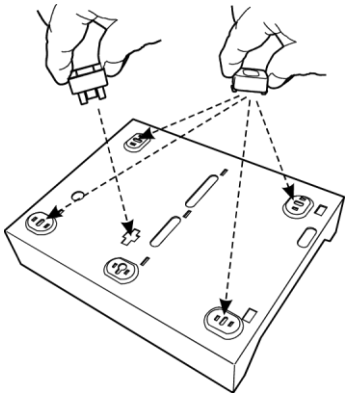


Figure 18. i-onG3MM: Fitting the feet and tamper sleeve

Step 3: Fit the tamper switch and shroud

Fit the tamper switch assembly through the slot in the case (Figure 19). Also, for added security, fit the tamper shroud to the wall so that when you mount the control unit, the shroud will surround the arm of the tamper switch.

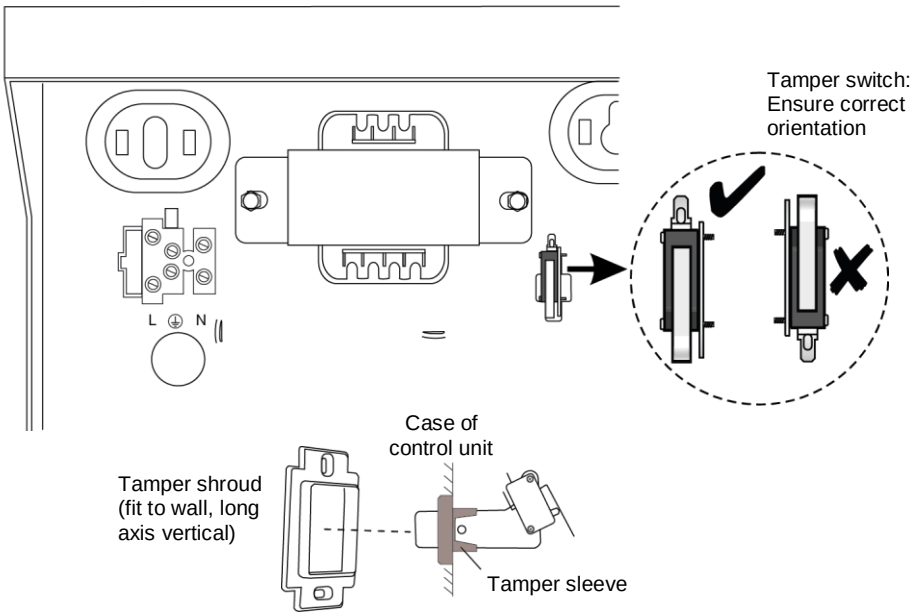


Figure 19. i-onG3MM: Fitting the tamper switch and shroud

Step 4: Mount the control unit

Mount the control unit in the orientation shown in Figure 20 using at least 4 fixing holes and minimum 50mm long No10(5mm) screws. Use only the designated cable-entry holes.

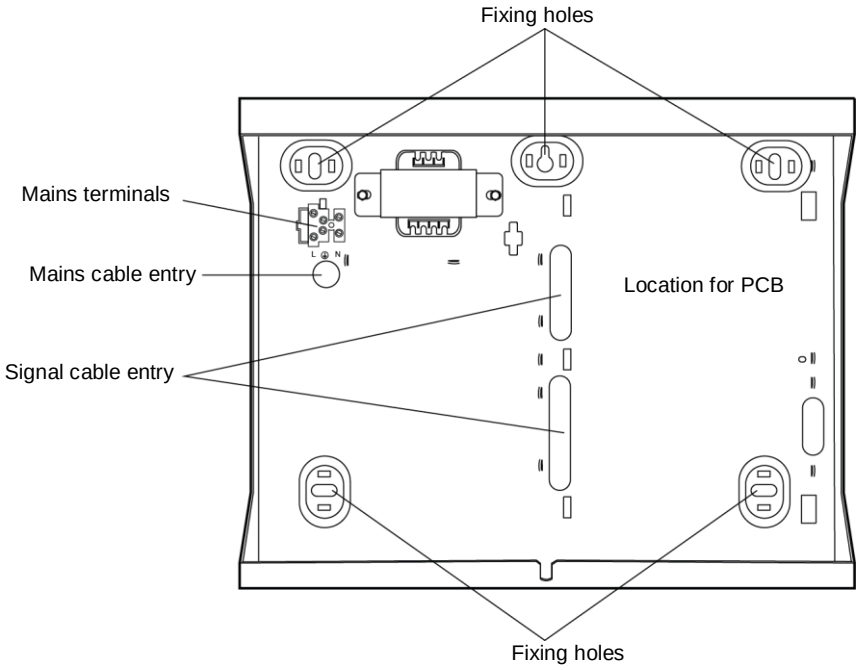


Figure 20. i-onG3MM: Mounting holes and cable entries

Step 5: Fit the PCB

Fit the PCB into the case as shown in Figure 21.

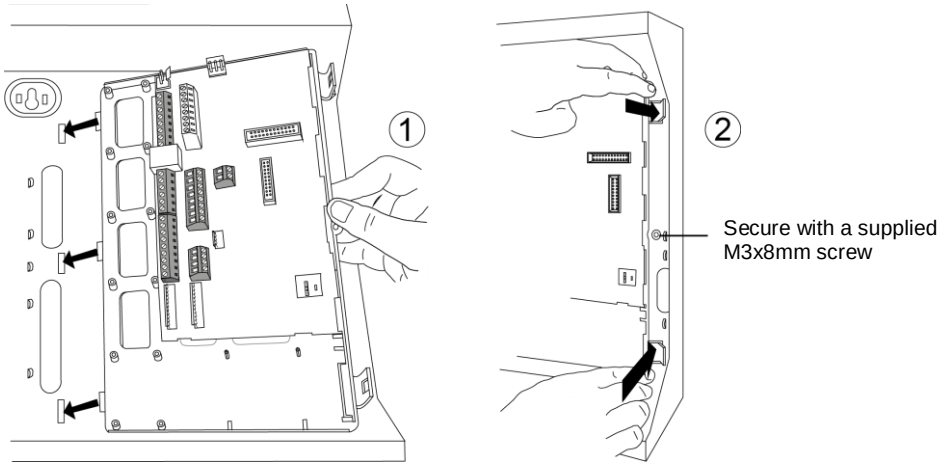


Figure 21. i-onG3MM: Fitting the PCB

Step 6: Connect all wired devices

Connect all wired devices except the battery, as shown in Figure 17.

If you are using a plug-on module, fit and connect the device as described in the module's installation instructions.

Step 7: Connect the battery

Note: Connecting the battery does not start the system.

Fit the lead-acid battery in the bottom-left corner of the control unit.

Connect the battery leads to the battery (red to positive and black to negative), and connect the other end to the PCB (Figure 17). Also connect the transformer lead to the PCB (Figure 17).

Step 8: Connect the mains cable

WARNING: ENSURE THAT THE MAINS SUPPLY IS DISCONNECTED AND ISOLATED.

Connect the mains cable to the terminal block (Figure 22) and fit a strain-relief tie.

Do not apply power until after the lid is re-fitted.

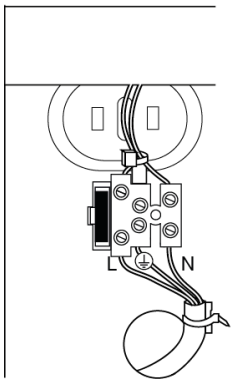


Figure 22. i-onG3MM: Mains connections

Step 9: Re-fit the lid, switch on and configure the system

WARNING: During initial power-up, keypad sounders and any internal loudspeaker may give an alarm tone. If you are working at the top of a ladder, make sure that the sudden noise does not startle you and cause a fall.

Re-fit the lid (Figure 23), then switch on the mains supply to the control unit.

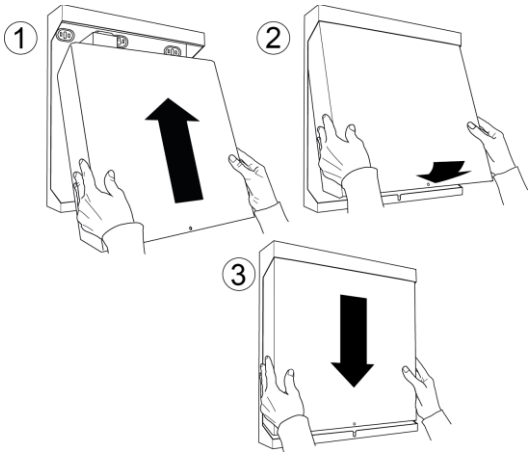


Figure 23. i-onG3MM: Re-fitting the lid

Go through the initial configuration prompts and set up the system as described in the *Configuration Guide*. You are prompted to specify installer and user codes during initial system configuration.

It is recommended that you connect the control unit to the internet and enable “Level 4 Update” in the installer and user menus. When you enter your installer code, the system can then check online whether later versions of the firmware or language file exist, and prompt you to install them. Please refer to the *Configuration Guide* for further details.

Overview of PCB links, connectors and LEDs

The following sections provide information about the links, connectors and LEDs shown in Figures 6 to 17.

① SD card slot

A micro-SD card can be used to store camera images from a compatible network camera, or to upgrade firmware or languages.

② Reset codes link

You can use this link to reset the installer and all user codes (e.g. in the event that codes have been forgotten). All proximity tags, hold-up devices and remote controls are also deleted. Please refer to the *Configuration Guide* for details of how to use this link.

③ Engineer keypad port

Note: Not available in i-on Compact.

You can use an engineer keypad to configure the system, rather than a keypad on the bus. An engineer keypad does not need an address.

④ Plug-by communicator ports

Note: Not available in i-on30R+ and i-on Compact.

You can connect a plug-by communicator to these ports using an optional MISC-COMPACK12 wiring harness (available separately).

By default, the outputs are 0V when active, and 12Vdc when inactive. Please refer to the *Configuration Guide* for the default output type used for each output and programming details.

Connect LF (Line Fail) to an output from the communicator that is 12Vdc when communicator detects that there is a communications fault to the ARC, and 0V when no fault is present.

If a dual-path (landline and mobile) communicator is used, such as a RedCARE STU, re-program one of the plug-by outputs to type ATS Test, and wire that to the ATS Test input of the communicator. Also connect Line Fail to the Line Fail output of the communicator, as above. This is needed to comply with BSIA Form No. 175, April 2005. The control unit generates an “ATE LF Single” alert if one network is unavailable, or “ATE LF All” if both are unavailable.

Connect RR (Remote Reset) to an output from the communicator that indicates to the control unit that a user can reset the system after a system tamper. The input must be 12Vdc for at least 100ms to indicate the reset, and 0v normally. For further details, see “Remote Reset (Redcare Reset)” in the *Configuration Guide*.

Note: During system commissioning, confirm with the ARC that the communicator is working correctly.

⑤ Bus devices

Note: Not available in i-on Compact.

Devices such as keypads and expanders can connect to the system bus. The installation instructions supplied with each device provide details of how to install and configure the device. The address of each device is set by the control unit.

Please refer to Table 1 on page 7 for details of the number of devices that can connect to the bus, and to page 23 for guidance about bus cabling. See also “RS485 bus termination link” and “Engineer keypad port” in this section.

⑥ Wired outputs

Note: Not available in i-on Compact.

Wired outputs can be used to switch external equipment on or off.

Relay outputs (if available) are voltage-free. Connect to the common terminal and to either the NC (Normally Closed) or NO (Normally Open) terminal, as required.

Open-collector (transistor) outputs are, by default, 12Vdc when inactive and 0V when active (this can be reversed from the Installer menu).

Note: Radio outputs can also be used if the control unit has built-in radio communications (i-on40H+, i-on30R+ and i-on Compact), or if a radio expander is used (not available for i-on Compact).

⑦ Loudspeaker connections

Note: Not available in i-on Compact.

If fitted, a loudspeaker mimics alarm tones and repeats setting and entry tones. The loudspeaker must be min 16 Ohms.

Note:

- A loudspeaker is not a warning device as described by EN50131-4.
- You can set the loudspeaker volume and partitions from the Installer menu.

⑧ Siren/strobe connections

Note: Not available in i-on Compact.

Please refer to the installation instructions provided with the siren/strobe unit for connection details.

Note: Scantronic radio siren/strobe units can be used instead of, or in addition to, a wired unit (requires a radio expander if the control unit does not have built-in radio communications).

⑨ Wired zone connections

Note: Not available in i-on30R+ and i-on Compact.

You can connect up to 10 wired detectors (0 to 9) using the Fully-Supervised Loop (FSL), 4-wire Closed Circuit (CC) or 2-wire CC wiring method (Figure 24). You must use the same method for all detectors connected to the control unit. If 4-wire CC is used, the number of zones is halved. To maintain ten 4-wire CC zones, fit an ADP-10CC board and configure the resistance setting of each zones as 2k2/4k7.

For any method, the total wiring and switch resistance must be less than 100 Ohms (EOL resistor shorted in the case of FSL).

By default, the system assumes normally-closed contacts. Detectors with normally-open contacts must be programmed with the “Inverted” attribute set.

Note: If you are using a detector with an anti-mask contact, use 2k2 EOL, 4k7 alarm, and 2k2 anti-mask resistors; see the *Configuration Guide*.

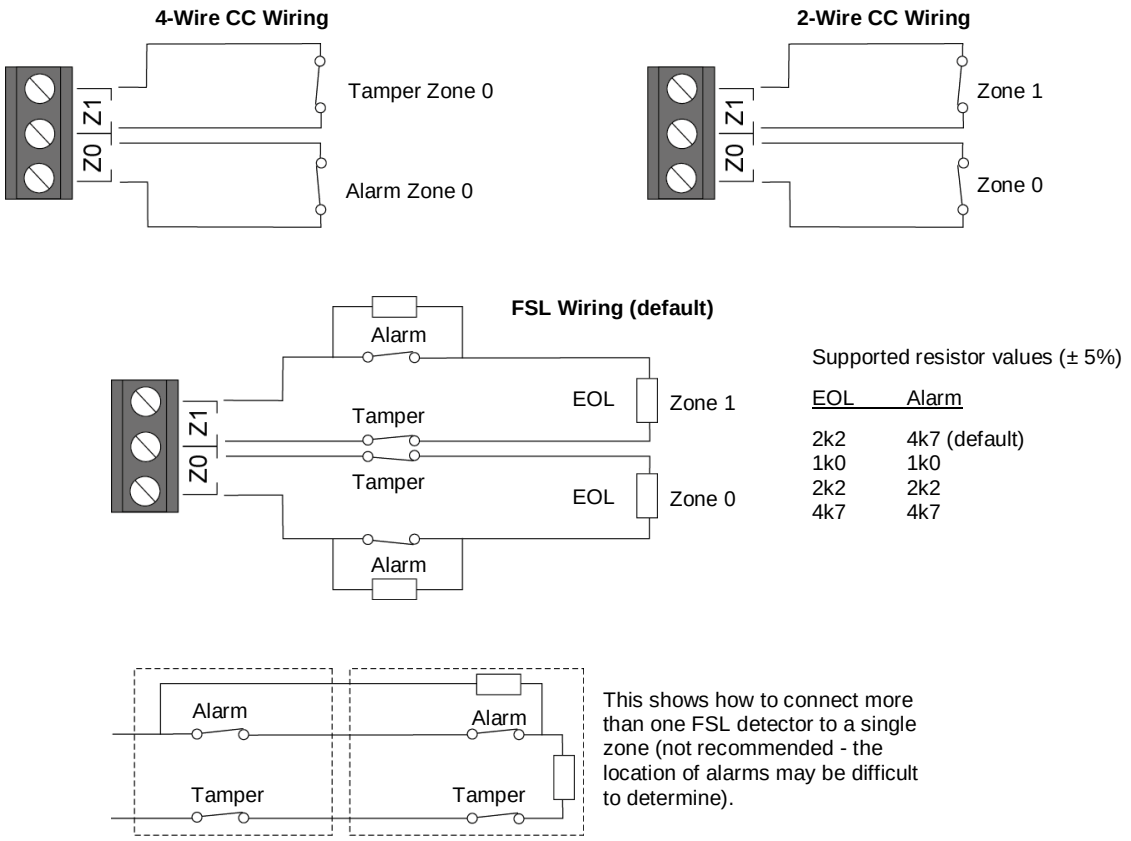


Figure 24. Zone wiring

⑩ Network port

Connecting to a network allows you to, for example, configure the control unit using the web interface, use network cameras to capture images when an alarm occurs, and use the SecureConnect application (e.g. for app cloud connectivity, or to send alarm notifications by email or to an ARC).

Note: The control unit's network settings are configured from the Installer menu.

⑪ Kick-start link

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, start the control unit by briefly shorting this link.

⑫ Plug-on module connector

COM-SD-PSTN, COM-SD-GSM and COM-DATA-4G plug-on modules enable the control unit to communicate over a landline or mobile network. This can be used to send alarm information to an ARC, direct speech/text alarm messages to an administrator, or to allow users to control the system using the SecureConnect mobile application.

Please refer to page 15 for further details about the modules.

⑬ Auxiliary tamper terminals

Note: Not available in i-on Compact.

These terminals can be used to monitor the tamper status of other equipment. Use a 2k2 End-of-Line (EOL) resistor in series with the tamper contact (Figure 25). Ensure that a 2k2 resistor is fitted across the auxiliary tamper terminals if they are not used.

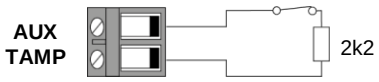


Figure 25. Auxiliary tamper wiring

⑭ RS485 bus termination link

Note: Not available in i-on Compact.

If a single daisy chain of devices is connected to the bus connector, and the control unit is at one end of the chain, fit a jumper across the bus termination link in the control unit and in the last device on the bus.

The i-onG3MM has one termination link for each bus connector.

RS485 termination can improve performance in electrically noisy environments.

Please refer to page 24 for further guidance.

⑮ LEDs

- **3V3** (and **12V** in i-on Compact): Lit when the internal power supply is functioning.
- **HB** (heartbeat): Flashes approximately once every two seconds to indicate normal operation.
- **LNK/ACT** (**LINK/ACTIVITY**): Flashes when the control unit is connected to the network and there is network activity.
- **RFTX** (i-on Compact only): Lit when there is radio transmission.

⑯ 16.5VAC input

Note: Available only in i-onG2SM.

This input can be used to instead of the standard 3-pin push-fit transformer connector to provide 16.5VAC power to the PCB. Typically, it is used when upgrading an i-on30EX to an i-onG2SM.

⑰ External DC input

Note: Available only in i-on Compact.

You can power the control unit using an external 10-15Vdc power supply connected to the DC IN and 0V terminals.

⑱ WiFi module power

Note: Available only in i-on Compact.

You can use these terminals to provide power to an optional WiFi module. You can mount the module in the space provided on the backplate (see Figure 6).

Note: The backup battery does not provide power to these terminals in the event of a mains failure.

⑲ Mini-B USB port

Note: Available only in i-on Compact.

You can connect a PC to this port and use the Update Utility to update the firmware.

Appendix A: Alarms Transmission System

This appendix documents the manufacturer's information requirements of EN 50136-2.

Overview

The control units incorporate an Alarms System (AS) and an integral Supervised Premises Transceiver (SPT). The SPT can be configured to use:

- PSTN or GSM, via an optional COM-SD-PSTN or COM-SD-GSM module. **Note:** Please refer to the important note on page 15 regarding the use of GSM for ARC communications
- Internet protocols, via the built-in Ethernet capability or an optional COM-DATA-4G plug-on module (which is also cabable of switching to 2G).

GSM and PSTN transmissions

Mode of operation

Alarms from the AS are transmitted, via the SPT, in a pass-through mode of operation by forwarding them directly to the alarm receiving centre via its Receiving Centre Transceiver (RCT). If an alarm transmission is unsuccessful, the following event is logged:

- "PSTN Alarm Fail" – for PSTN communications.
- "GSM Alarm Fail"– for GSM communications.

The SPT attempts to send unsuccessful alarm transmissions until the retry sequence has expired, and if still unsuccessful, the alarm transmissions are tagged for repeat transmission with the next alarm.

Acknowledgments of successful alarm transmissions received from the RCT are forwarded to the AS via the SPT.

Transmission monitoring

The Primary ATP can be either the PSTN or the GSM connection. Monitoring the integrity of the transmission system is performed in two stages:

1. The transmission network interface is monitored as follows:
    - PSTN – the local connection from the SPT to the PSTN network is verified by monitoring the line voltage.
    - GSM – the local connection from the SPT to the GSM network is verified by periodically checking the signal strength and registration to a service provider. **Note:** the SPT does not check the credit on PAYG SIMs, or the provider's contract validity.

If the transmission network interface connection fails, the following transaction are logged:

- PSTN – “PSTN Line Fault" (the keypad also changes status from green to red). When the connection is restored, another transaction is logged: "PSTN Line Restored".
- GSM – “GSM Line Fault" (the keypad also changes status from green to red). When the connection is restored, another transaction is logged: "GSM Line Restored".

2. The Alarm Transmission System (ATS) is monitored by making a test call to check the complete system. (The test call must be configured as either dynamic or static.) The following is the sequence of logged events for a successful test call:
   - "Alarm Test Call" (this logged event triggers the test call)
   - "Test call success"

   For an unsuccessful test call:
   - "Alarm Test Call"
   - "Test Call Fail"

Internet transmissions

Mode of operation

Alarms from the AS are transmitted, via the SPT, in a store-and-forward mode of operation.

For a SIA IP Direct connection:

- The SPT forwards the transmission directly to the SecureConnect servers.
- The SecureConnect servers store the transmission.
- The SecureConnect servers forward the stored transmission directly to the alarm receiving centre via its Receiving Centre Transceiver (RCT).

For a CSL DualCom connection:

- The SPT forwards the transmission directly to the SecureConnect servers.
- The SecureConnect servers store the transmission.
- The SecureConnect servers forward the transmission to the CSL DualCom Gemini Network, and CSL Dual Com passes the transmission onto the alarm receiving centre via its Receiving Centre Transceiver (RCT).

The SPT maintains a continuous connection to the SecureConnect servers and attempts to send unsuccessful alarm transmissions as follows:

- SPT to SecureConnect Servers – If an alarm transmission is unsuccessful from the SPT to the SecureConnect servers and the retry sequence has expired, the following event is logged at the SPT: “Cloud Push Fail". If the connection to the SecureConnect servers is not available at the time the transmission is due to be transmitted, the transmission is held at the SPT until a connection to the SecureConnect servers can be re-established. Acknowledgments of successful alarm transmissions received from the SecureConnect servers are forwarded to the AS via the SPT.

- SecureConnect Servers to Receiving Centre Transceiver (RCT) – If an alarm transmission is unsuccessful from the SecureConnect servers to the Receiving Centre Transceiver (RCT), no response is received at the end of the retry sequence. Acknowledgments of successful alarm transmissions received from the RCT are forwarded to the SecureConnect servers and logged.
- SecureConnect Servers to CSL Dual Com – If an alarm transmission is unsuccessful in transmitting from the SecureConnect servers to CSL Dual Com, the following event is logged at the SecureConnect Servers at the end of the retry sequence: “No response from CSL". Acknowledgments of successful alarm transmissions received from the RCT are forwarded to the SecureConnect servers and logged.

Transmission monitoring: single-path connection

The Primary ATP can be either the Ethernet connection or the 4G/2G mobile connection. For a single-path Ethernet connection, no COM-SD-GSM module must be fitted. For a single-path 4G/2G connection, the COM-SD-GSM module's "Data Mode" setting must be set to "Mobile Only".

Monitoring the integrity of the transmission system is performed in two stages:

1. The transmission network interface is monitored using the following methods:
   - Ethernet – the local connection from the SPT to the LAN is verified by monitoring the line voltage.
   - 4G/2G mobile data – the local connection from the SPT to the mobile data network is verified by periodically checking the signal strength and registration to a service provider. **Note:** the SPT does not check the credit on PAYG SIMs, or the provider's contract validity.

   If the transmission network interface connection fails, the following transactions are logged:
   - Ethernet – “Ethernet Line Fault" (the keypad also changes status from green to red). When the connection is restored, another transaction is logged: "Ethernet Line Restored".
   - 4G/2G – “GSM Line Fault" (the keypad also changes status from green to red). When the connection is restored, another transaction is logged: "GSM Line Restored".
2. The Alarm Transmission System (ATS) is monitored by the SPT maintaining a continuous connection to the SecureConnect servers. This connection is periodically polled to ensure the connection between the SPT and the SecureConnect servers is available.

   The following is logged for a loss in connection between the SPT and the SecureConnect servers:
   - "Offline (Ethernet)" – for an Ethernet connection.
   - "Offline (Mobile)"– for a 4G/2G connection.

   The following is the logged for a restoral of the connection between the SPT and the SecureConnect servers:
   - "Online (Ethernet)" – for an Ethernet connection.
   - "Online (Mobile)" – for a 4G/2G connection.

   The SecureConnect servers notify the alarm receiving centre via its Receiving Centre Transceiver (RCT) of both the loss and restore of a connection between the SPT and the SecureConnect servers at the required intervals.

Transmission monitoring: dual-path connection

The primary ATP will be the Ethernet connection. The alternative ATP will be the 4G/2G mobile data connection. The COM-SD-GSM module's "Data Mode" setting must be set to "Mobile as Backup".

Monitoring the integrity of the alternative ATP is performed in two stages:

1. The local connection from the SPT to the mobile data network is verified by periodically checking the signal strength and registration to a service provider. **Note:** the SPT does not check the credit on PAYG SIMs, or the provider's contract validity.

   If the transmission network interface connection fails, “GSM Line Fault" is logged (the keypad also changes status from green to red). When the connection is restored, another transaction is logged: "GSM Line Restored".
2. The alternative ATP is monitored by the SPT by performing a periodic connection to the SecureConnect servers.

   The following is the sequence of logged events for a periodic connection:

   - For an unsuccessful periodic connection "Mobile test Fail".
   - For a successful periodic connection: "Mobile test OK".

Appendix B: System Maintenance

Inspections

The system should be inspected once or twice per year. At each inspection:

- Check the control unit for obvious signs of damage to the case or its lid.
- Check the action of the tamper switch.
- Check, and if necessary, replace the standby battery.
- Check keypads and other devices for obvious signs of damage.
- Test the action of all buttons on all keypads.
- Clean the surface and display of each keypad using a clean, soft, dry cloth. Do not use water, solvents or any proprietary cleaning materials.
- Where applicable, check cabling for signs of damage or wear.
- Check the signal strength and battery condition of all detectors, radio keypads, remote controls, radio HUDs and radio sounders. Test each device. Replace batteries as recommended by the device instructions.
- Gently clean the lenses of any PIRs with a clean, soft dry cloth. Do not use water, solvents or any proprietary cleaning materials.
- Walk test all detectors.
- Test any external sounders and strobes.

Note: You can use *Test – Locate Bus Device* to find the location of a bus device (the device emits a continuous sound).

Replacing or removing devices

Note: Make sure that you remove all power from the system before physically disconnecting any device.

Removing a plug-on module

If you wish to remove a plug-on module, ensure that you disable communications first in the appropriate menus (such as in the *Communications – ARC Reporting*, *Communications – Speech Dialler* and *Communications – SMS* menus). Otherwise, the control unit will continually report a communications failure.

Removing a bus device permanently

Before physically disconnecting the device, enter the Installer menu, and use the appropriate *Delete* option. For example, to delete a keypad, use *Devices/Detectors – Wired Keypads – Delete Keypad*. This ensures that the system does not report a missing device and the device's internal address is erased (allowing it to be used on another system).

Replacing a bus device

Before physically disconnecting the device, enter the Installer menu, and use the appropriate *Replace* option. For example, to replace a keypad, use *Devices/Detectors – Wired Keypads – Replace Keypad*. The control unit disables the selected device, but retains the configuration of the old device (such as the zone configuration). You can then power down the system, disconnect the device from the bus, and reconnect a new device (of the same type) to the bus.

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

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

Note: If you are replacing a keypad on a single-keypad system, you will have to re-program the new keypad with all the functions of the old keypad, including any non-default ABCD key functions.

Using LEDs for diagnostics

You may notice an LED on the PCB of a device flashing unusually. Please refer to page 43 for the meaning of each LED.

Appendix C: Specifications

	i-on Compact	i-on30R+	i-on40H+	i-onG2SM	i-onG3MM
Standards and Compliance					
Grade	2	2	2	2	2 or 3
Environmental Class	II	II	II	II	II
Environ. protection	IP40 / IK06				
ATS category	DP2 / SP3				
Standards compliance - general	EN 50130-4:2011+A1:2014; EN 61000-6-3:2007+A1:2011; EN 62368-1:2018				
Standards compliance – intruder alarm	EN 50131-1:2007+A2:2017; EN 50131-3:2009; EN 50131-6:2017; EN 50131-10:2014; EN 50136-1:2012 BS8243:2010; PD6662:2017				
Standards compliance - radio	EN 300 220-2 V2.4.1; EN 301 489-1 V2.2.0; EN 301 489-3 V2.1.1; EN 50131-5-3:2017			n/a	
Certification body	Telefication	TBA	TBA	TBA	TBA
Certifications	INCERT T O31:2014 C-016-1367				
Security					
Radio detector combinations	16,777,214				
Radio supervision	Programmable				
Access codes - default	4-digit				6-digit (G3)
Access codes - option	6 -digit				4-digit (G2)
Combinations - default	10,000				1,000,000
Code blocking	Blocked for 90 secs after 4 incorrect codes in series				
Proximity tag differs	4,294,967,296				
General					
Relative humidity	0 to 93%, non-condensing				
Operating temp. range	-10°C to +55°C				

	i-on Compact	**i-on30R+**	**i-on40H+**	**i-onG2SM**	**i-onG3MM**
Height	238mm	384mm		239mm	320mm
Width	161mm	245mm		250mm	400mm
Depth	38mm	94mm		87mm	102mm
Weight	710g (with battery)	2kg (without battery)		2.8kg (without battery)	4.5kg (without battery)
Case material	ABS			Mild Steel	
Number of RS485 buses	1	1	1	1	2
Network port:	Ethernet 10/100Mbps SSL/TLS				
Radio					
Radio frequency	868.6625MHz			n/a	n/a
Type	Narrowband			n/a	n/a
Radio power	10mW max			n/a	n/a
Transmitter range (free space)	500m			n/a	n/a
Electrical					
Compliance	EN 50131-6 Type A				
Mains supply	85-250VAC 150-60mA 50/60Hz	230VAC +10%/-15% 130mA max 50Hz		230VAC +10%/-15% 200mA max 50Hz	230VAC +10%/-15% 240mA max 50Hz
Internal mains fuse	T1A	T250mA		T250mA	T500mA
Control Unit Power supply	12Vdc, 500mA	13.7Vdc 1.0A		13.7Vdc 1.0A	13.7Vdc 2.0A
Reserved for battery charging	100mA	180mA		180mA	750mA
Available for the system	400mA	820mA		820mA	1,250mA
Control Unit PCB current consumption: -					
• Quiescent	80mA	80mA	90mA	90mA	100mA
• With backlight	105mA	n/a	n/a	n/a	n/a
• Max. (in alarm) *	150mA	90mA	110mA	110mA	150mA
	*Excludes external devices, plug-on modules, and battery charging				
Standby battery for Grade 2/PD6662	7.2V, 2200mAh	12V 7Ah		12V 7Ah	12V 7Ah

	i-on Compact	**i-on30R+**	**i-on40H+**	**i-onG2SM**	**i-onG3MM**
Standby battery for Grade 3	n/a				12V 17Ah
Battery chemistry	NimH	Sealed lead acid			
Battery supplied	Yes	No		No	No
Minimum standby time	12 hrs	12 hrs		12 hrs	G3 30 hrs G2 12 hrs PD6662 12 h
Max time to recharge to 80% capacity	36 hrs	72 hrs		72 hrs	24 hrs
Low battery warning at	<7.2V	<12Vdc			
Battery deep discharge	6±0.5V	10±0.5V			
pk-to-pk ripple voltage	±0.5Vdc max				
12Vdc WiFi output for Eaton i-WiFi01 Note: not battery backed up	11 – 12.6Vdc 200mA max Fault: <9Vdc	n/a			
12Vdc external DC input	10-15Vdc Max 500mA	n/a			
DC supplies: -					
• 12Vdc Aux	n/a	600mA max			
• 12Vdc Bell	n/a	600mA max			
• 12Vdc Bus	n/a	400mA max per bus			
• 14.4V Aux	n/a	230mA max		n/a	230mA max
• 12Vdc to plug-by	n/a	400mA max			
		max = current before triggering over-current protection			
• 12Vdc range	n/a	9.5Vdc to 13.8Vdc			
• 14.4Vdc range	n/a	9.5Vdc to 14.7Vdc			
• Over-voltage protection	n/a	n/a		n/a	15.6Vdc ± 1Vdc
Aux power fault at		<9Vdc			
Output 1	n/a	n/a	Voltage-free relay: 1A@24Vdc max	Open-collector transistor, 500mA max	Voltage-free relay: 1A@24Vdc max

	i-on Compact	**i-on30R+**	**i-on40H+**	**i-onG2SM**	**i-onG3MM**
Output 2	n/a	n/a	Voltage- free relay: 1A@24Vdc max	n/a	Voltage-free relay: 1A@24Vdc max
Output 3&4	n/a	Open-collector transistor, 500mA max		n/a	Open-collector transistor, 500mA max
Number of plug-by outputs (50mA)	n/a	n/a	12	12	16
Loudspeaker	n/a	12Vdc, 280mA max. Min impedance 16 Ohm			
Siren interface for Bell+Strobe+TR	Yes				
Aux tamper input	No	Yes			

SIMPLIFIED EU DECLARATION OF CONFORMITY

Hereby, Eaton Electrical Products Ltd declares that radio equipment types i-on Compact, i-on30R+ and i-on40H+ are in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address: www.touchpoint-online.com

SecureConnect is a trademark of Eaton

www.touchpoint-online.com
Product Support (UK) Tel: +44 (0) 1594 541978
Available between:
08:30 to 17:00 Monday to Friday.
email: securitytechsupport@eaton.com
Part Number 13368865 Issue 1 1st October 2019