

FORCE

Advanced Security System



Installation Guide

System Version: Beta

PIMA
FOR BETTER PROTECTION
PIMA Electronic Systems Ltd.

Table of Contents

Chap. 1 Introduction	7
1.1 Main features	7
1.2 Technical specs.....	7
Chap. 2 Installation & Wiring	8
2.1 Location guidelines.....	8
2.2 Mounting the rack	8
2.3 The control panel	9
2.4 Connecting expanders and peripherals	10
2.5 The BUS	10
2.6 Zone connection	11
2.6.1 Zone doubling.....	11
2.7 Connecting phone line and set	11
2.8 Connecting sirens.....	12
2.9 Connecting zones and outputs expanders	12
2.9.1 Interfacing with the BUS.....	12
2.9.2 Local 8-zone expansion card, ZEL508	13
2.9.3 Remote 8-zone expansion card, ZEX508	13
2.9.4 Setting the expander's ID number.....	14
2.9.5 The LEDs.....	15
2.9.6 Location buzzer	15
2.9.7 Remote 16-zone expansion card, ZEX516.....	15
2.9.8 Remote 8-relay outputs expansion card, OEX508	16
2.10 Connecting radio transmitters, TRV/TRU-100	17
2.11 Connecting tamper switches	18
2.12 Connecting keypads	18
2.12.1 Keypads installation guidelines	18
2.12.2 LCD keypads, KLT/KLR500.....	18
2.12.3 Connect the KLT/KLR500 keypads.....	20
2.13 GSM add-on, GSM501.....	21
2.13.1 Main features.....	21
2.13.2 The LEDs.....	21
2.13.3 Add-on installation and how to replace the SIM card.....	22
Chap. 3 System Programming	23
3.1 Menus and codes	23
3.1.1 Code setting guidelines	23
3.1.2 Activation codes	23
3.2 Changing the default Master codes	23
3.2.1 Changing the Master user code.....	23
3.2.2 Changing the Master technician code.....	24
3.3 The technician menu	24
3.3.1 System Configuration.....	24
3.3.2 Tests & Diagnostics.....	24
Chap. 4 Installation Wizard	25
Chap. 5 Peripherals	26
5.1 Zone expanders.....	26
5.2 Tamper and EOLs	26
5.3 Keypad Settings.....	27
Chap. 6 Zones.....	28
6.1 Zone Settings.....	28
6.2 Zone Types Settings.....	29
6.2.1 Attributes	29
6.3 Copy Zones.....	30
6.3.1 Single to Multiple.....	30

6.4	Multiple to Multiple	30
6.5	Partitions Names.....	30
Chap. 7	Outputs	31
7.1	Onboard	31
7.2	Zone Expanders.....	32
7.3	Output Expander.....	32
Chap. 8	CMS & Communications	33
8.1	Monitoring Stations	33
8.1.1	CMS 1-2.....	33
8.1.2	Radio.....	34
8.1.3	Custom Zones Reports	35
8.2	PIMA Cloud	36
8.3	General Setting	36
8.4	Telephone Settings.....	36
8.5	Network Settings	37
8.6	GSM/GPRS Settings.....	37
Chap. 9	Faults	38
9.1	AC Fault	38
Chap. 10	Timers and Counters.....	39
10.1	Programmable Output Types.....	41
Chap. 11	General Settings	42
11.1	Arm Prevention - Faults	43
Chap. 12	Reset to Defaults	44
12.1	Resetting to factory defaults	44
Chap. 13	Tests & Diagnostics	45
13.1	Event Memory	45
13.2	Zone Test	45
13.3	Output Test.....	45
13.4	Power Diagnostics	46
13.5	Communication Tests	46
13.6	Communications Monitor.....	46

Table of Figures

Figure 1.	The control panel's rack	8
Figure 2.	The rack's cover	8
Figure 3.	The control panel	8
Figure 4.	Wiring diagram	9
Figure 5.	Normal zone	10
Figure 6.	EOL supervised zone.....	10
Figure 7.	Two EOLs supervised zone.....	10
Figure 8.	Phone line connection	10
Figure 9.	Sirens connection	11
Figure 10.	Dip-switch setting.....	12
Figure 11.	Connecting peripherals over the BUS (up to 500m)	12
Figure 12.	Local 8 zone expansion card	13
Figure 13.	Remote 8 zone expansion card.....	14
Figure 14.	Remote 16 zone expansion card.....	14
Figure 15.	8 relay output expansion card.....	15
Figure 16.	Connecting the TRV/TRU-100 radio transmitters.....	16

Figure 17. KBH500 connection diagram 19

Figure 18. GSM add-on front side 20

Figure 19. GSM add-on back side 20

Figure 20. The GSM add-on installed onboard 20

Safety Instructions. Read Carefully

The Force security system has been registered in accordance with EN60950 and its rules.

Among other things, EN60950 requires us to advise you the following information:

- Hazards of fire and electric shock exist in this alarm system. To reduce the risk of fire or electric shock, do not expose this alarm system to rain or moisture. Pay attention: Telephone cords could be a good conductor for lightings energy.
- Warning: this equipment has no mains On/Off switch. The plug of the direct plug-in power supply is intended to serve as the disconnecting device.
- Dangerous high voltages are present inside the control panel's enclosure. Refer servicing to qualified personnel only.
- This alarm system should be used with 230VAC/110VAC, 50/60Hz, protected by anti-electric shock breaker. Use only the power supply provided with this equipment. Use of unauthorized power supplies may cause damage.
- Do not spill liquid of any kind onto the unit. If liquid is accidentally spilled onto the unit, immediately consult a qualified service.
- Disposal of used batteries must be made in accordance with local waste recovery and recycling regulations.

Default Codes

Master: 5555

Installer: 1234

Signs in this guide



Warning



Note



Enter sub-menus, select/deselect, save selection



Menu with sub-menus



Options menu



Return/Esc, cancel (except in the *Keypad Settings* menu)



Select/deselect to enable/disable



Scroll between zones, partitions, users, etc.

Chap. 1 Introduction

This guide will introduce you with the new, highly reliable **FORCE** security system. With its 7-line LCD and clear menu-driven display, **FORCE** is an intuitive easy to install and program system.

The Technician and User subject menus make programming and navigating fast and easy. Help screens reduce the need to look in this guide on every servicing.

A special Tests & Diagnostics menu allows you to see various information about the current system status.

The PIMAlink 2.0 cloud service and smartphone application allow the end-users to control the **FORCE** from anywhere.

This Installation guide refers to the **FORCE** security system, version 0.8.X. The system is supplied with two guides:

- This guide that includes the system and peripherals installation and wiring instructions, as well as the technician-programming guide.
- The User guide that includes the user-programming guide and the system maintenance instructions.

1.1 Main features

- 8 zones, expandable to 144
- Up to 144 users, each with unique user code
- Up to 32 contacts, for receiving alarm and other notifications
- Up to 16 true partitions with separate keypads for each
- Expansion cards for 8 and 16 zones, with one or two relays on each
- Multi-channel, simultaneous communications: Ethernet, GSM, GPRS, landline telephone, and radio.
- Up to 2 CMSs (Central Monitoring Station) with password protection for each
- Remote operations via PIMAlink 2.0 cloud and application
- Graphic, LCD, 7-line keypad display, with various menus
- Detailed test and diagnostics menus
- Remote upload/download using the **FORCE** Manager software, via all media
- Remote firmware update

1.2 Technical specs

- AC power input: 11-18V
- Backup battery DC input: 13.8V
- Maximum output current: 13.8VDC, 1.1A
- Maximum idle output current (no expansions): 50mA
- EOL resistors: programmable
- Temperature: -10° to 50° Celsius
- AC Power supply: 16.5V
- Aux output: 7.2-13.8V, up to 1.1A
- Current consumption: up to 50mA

Chap. 2 Installation & Wiring

2.1 Location guidelines

To make installation and servicing easy and efficient, the **FORCE's** control panel, transformer and backup battery are mounted on a special rack. The rack is covered by a metal case.

Use the following list as a guide to find a suitable location to install the **FORCE** security system:

- Install this product on a protected location, where people cannot trip over any line or power cord.
- Select a location free from vibration and shock.
- Mount this product on a flat stable surface, near telephone and network sockets, and a power outlet.
- Do not select a location that exposes the control panel to direct sunlight, excessive heat, moisture, vapors, chemicals, or dust.
- Protect cords from damage or abrasion.
- Disconnect all sources of power supply prior to installation. Pay attention: do not install low voltage wires near any AC power wires. They should be installed separately.
- Do not install this product near water, e.g. bath tub, sink, wet basement.

2.2 Mounting the rack

The **FORCE's** control panel is installed on a designated rack. The rack is supplied with a metal cover. In addition to the control panel's circuit, the rack is designed to hold the transformer, backup battery, local zone expander, radio and GSM modules, and more.

The rack's sizes including the metal cover are L:30.3 H:27.2 W:7.7 cm.

To mount the rack, follow the next steps:

1. Use the next diagram or the rack itself, to position the two upper and one middle hanging holes.
2. Pass the wires of the zones and expanders from behind the rack, through the opening.
3. According to the designated surface, use appropriate wall plugs (if necessary) and screws and mount the rack.
4. When you finish connecting the wires, place the metal cover: tilt it upwards, insert the two tooth on the rack to the notches on the cover and place the cover on the rack.
5. Finally, fasten the screw at the bottom.

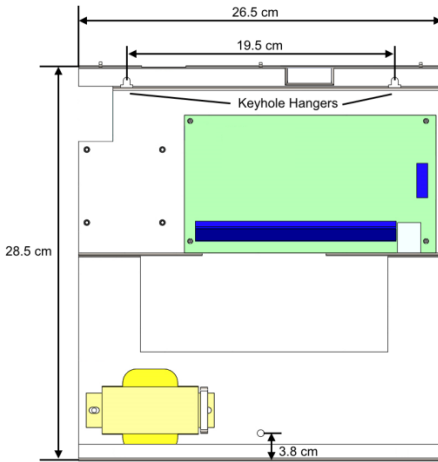


Figure 1. The control panel's rack

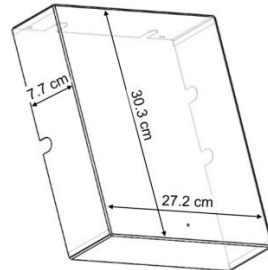


Figure 2. The rack's cover

2.3 The control panel

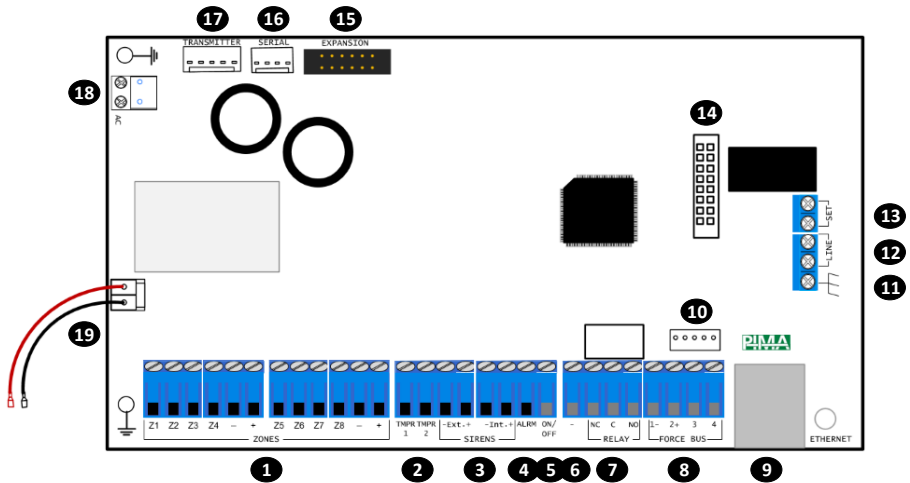


Figure 3. The control panel

Following is the list of the control panel's terminals:

1. Zone inputs Z1-Z8, detectors voltage (+)/(-)
2. Tamper switches 1-2 inputs
3. External/internal Sirens, (+)/(-)
4. ALRM output (by default, switched to (-) at alarm)
5. ON/OFF output: (by default, switched to (-) on arming)
6. GND (-)
7. Relay output: NC (Normally Close), C (Common), NO (Normally Open)

8. Force BUS. All expanders and keypads have the same 1-4 wire numbering.
9. Ethernet socket (RJ-45)
10. Technician keypad's connector
11. Earth ground - use only with non-PIMA non-metal cases!
12. Telephone line
13. Telephone set, fax, answering machine
14. GSM add-on socket
15. For future use
16. Serial RS-232 socket
17. Radio transmitter socket
18. 14-20 VAC input
19. Backup battery, Red (+)/Black (-)

2.4 Connecting expanders and peripherals

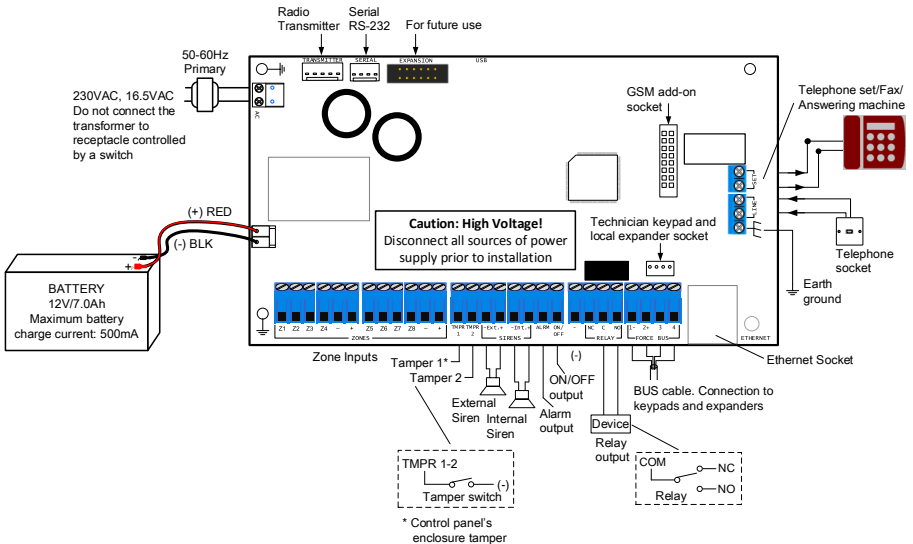


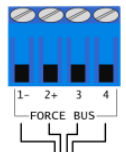
Figure 4. Wiring diagram

2.5 The BUS

The BUS is a serial communication channel, used for exchanging data between the control panel and the peripherals. The protocol in use by the BUS is ForceBUS (PIMA proprietary).

Use four 0.5mm (24 Gauge (AWG)) wires. The maximum BUS length is 500m, including all peripherals and keypads.

Connect the wires using the numbers 1-4, where terminal #1 on the control panel connects to the same terminal on the peripheral, and so on.



2.6 Zone connection

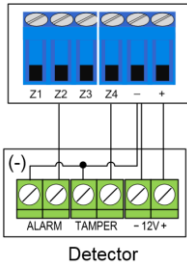


Figure 5. No EOL

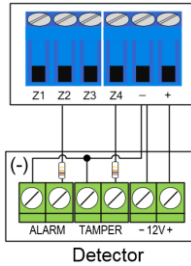


Figure 6. One EOL¹

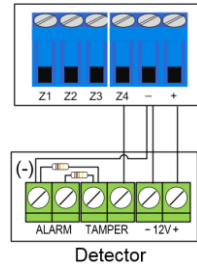


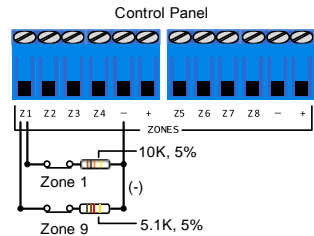
Figure 7. Two EOLs

2.6.1 Zone doubling

Zone Doubling allows you to double the eight onboard zones to 16. All doubled zones must be wired according to the diagram below.

Note that you cannot use zone expanders when you double zones.

On the diagram, the zone using the 10K resistor will be the first zone (lower number zone) and the zone using the 5.1K resistor will be the second zone (higher number zone). For example, Zone 1 input will serve Zone 1 (10K) and Zone 9 (5.1K), Zone 2 input will serve Zone 2 and 10, and so on.



2.7 Connecting phone line and set

The phone line is connected to the LINE terminals: connect the cord between the LINE terminals and the phone socket. If the line is used for ADSL modem, use an appropriate filter.

Connect phone sets, fax machines and answering machine to the SET terminals - this will enable the control panel to answer any incoming call.

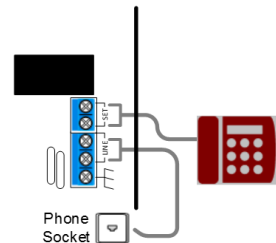


Figure 8. Phone line connection

¹ End Of Line resistor

2.8 Connecting sirens

The Sirens inputs are for DC sirens only.

1. Connect the external siren to the SIREN Ext. terminals
2. Connect the internal siren to the SIREN Int. terminals
3. For EOL loop supervision, connect a 2K resistor between the two siren wires, close or inside the siren's enclosure.

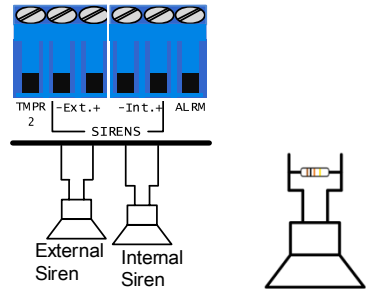


Figure 9. Sirens connection

2.9 Connecting zones and outputs expanders

PIMA's product line includes zone and output expanders. All expanders interface with the BUS. Following is the expander's list:

-
- ZEL508** Local 8-zone expander. The expander is installed beside the control panel and is connected using a special 4-wire cable.
-
- ZEX508** Remote 8-zone expander with one relay output
-
- ZEX516** Remote 16-zone expander with two relay outputs
-
- OEX508** Remote 8-relay outputs expander
-

2.9.1 Interfacing with the BUS

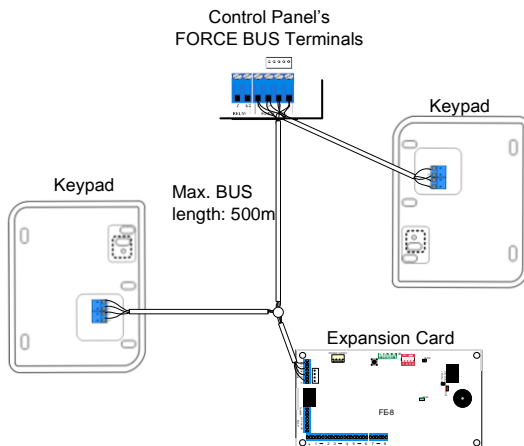


Figure 10. Connecting peripherals over the BUS

2.9.2 Local 8-zone expansion card, ZEL508

The ZEL508 allows adding eight zone inputs to the **FORCE** security system, locally. The card is installed on the control panel's rack, and interfaces with the BUS using the technician's fast connector on the control panel (see below), using a special cable (supplied).

Main features

- Eight zone inputs. The zones are automatically numbered 9-16
- Interfaces with the BUS
- Two indicative LEDs: communication and status (see details below)
- Two parallel connectors: one for the control panel cable and one for the technician keypad
- Sizes: 8.2 X 7.5cm
- Technical specs: 10-15V, 30mA in idle state, Fuse: 0.9A

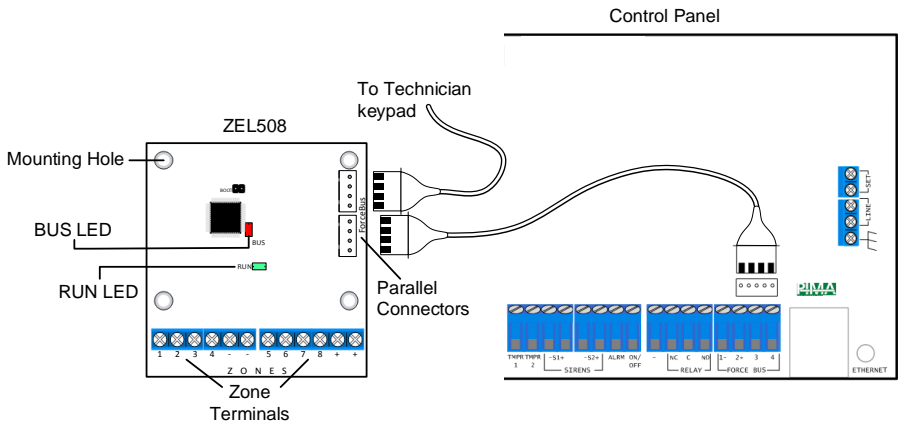


Figure 11. ZEL508 connection diagram

The LEDs

Green	Flashes once every one second	Card status OK
Red	Flashes	Communication in progress

2.9.3 Remote 8-zone expansion card, ZEX508

The ZEX508 allows adding 8 zone inputs to the **FORCE** security system, remotely. The card interfaces with the BUS.

Main features

- 8 zone inputs, one relay output.
- Interfaces with the BUS
- External tamper switch input
- Tamper bypass jumper
- Technician keypad fast connector
- PS-2 power supply socket
- ID number DIP switch

- Card location buzzer
- Supplied mounted in a standard plastic 19 X 13 cm box
- Size: 8.2 X 15cm
- Technical specs: 10-15V, 30mA in idle state, fuse: 0.9A

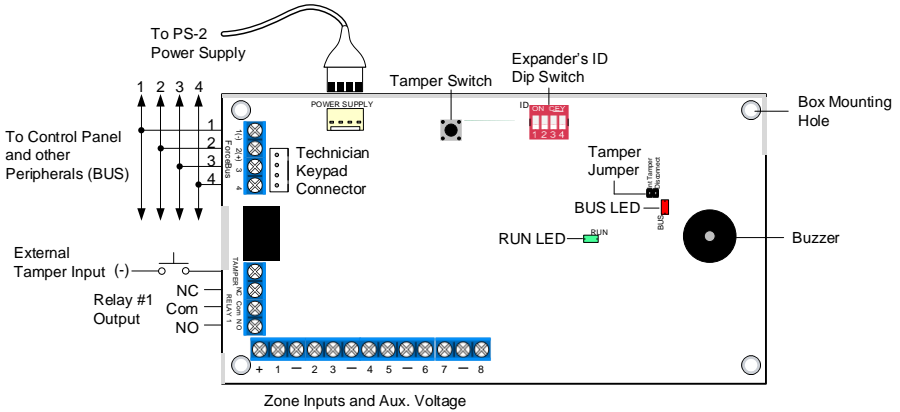


Figure 12. ZEX508 connection diagram

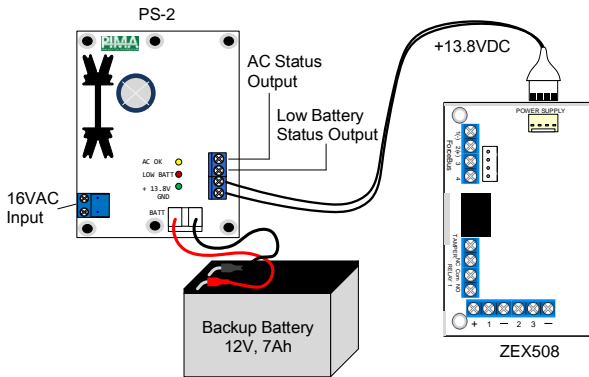


Figure 13. ZEX508 with PS-2 power supply (up to 1.2A)² connection diagram


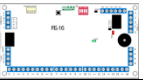

2.9.4 Setting the expander's ID number

Each remote expansion card must carry a unique ID number, between 1 & 16. The ID is set by a dip-switch. Numbering must follow the next rules:

- The number must be unique
- Numbers must be consecutive
- Each 16-zone expander (ZEX516) takes 2 consecutive numbers automatically. For example, expander with ID number 4 takes no's 4 & 5, so the next expander must carry the ID number of 6.

² The battery is for illustration purpose only.

ID numbering example:

			
Expander	ZEX508	ZEX516	ZEX508
ID no.	6	7 (& 8)	9

The next diagram shows the dip-switch number settings, with the ID number for each setting:

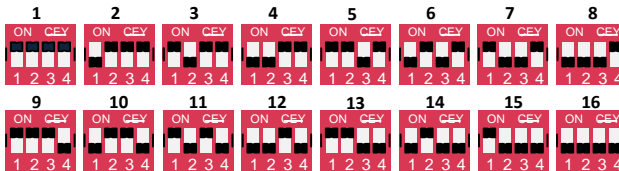


Figure 14. Dip-switch optional settings

2.9.5 The LEDs

LED	State	Description
RUN	Flashes	Card runs OK
Green	Off	Card fault
BUS	Flashes	BUS connection OK
Red	Off	Communication fault

2.9.6 Location buzzer

Each **FORCE** expansion card has a buzzer, which helps in locating the card on the premises. The buzzer is triggered together with the card's relay output, when performing an output test (see the *Test and Diagnostics* menu, on page 45).

2.9.7 Remote 16-zone expansion card, ZEX516³

The ZEX516 allows adding 16 zone inputs to the **FORCE** security system, remotely. The ZEX516 has the same features of the ZEX508, except the following:

- 16 zone inputs, 2 relay outputs
- Additional voltage and COM terminals

³ ZEP716 (P/N 8290013) is a ZEX516 expander with a 4.2A power supply, mounted in a metal case. See a separate guide, P/N 4410474.

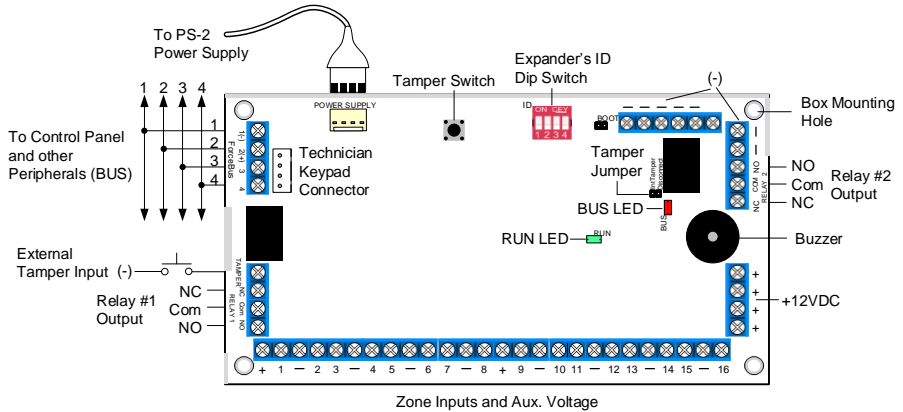


Figure 15. ZEX516 connection diagram

2.9.8 Remote 8-relay outputs expansion card, OEX508

The OEX508 has 8 relay outputs for connecting various peripherals and devices.

Main features

- 8 Normally Open/Normally Closed/COM relay outputs
- Multiple voltage and COM terminals
- Interfaces with the BUS
- External tamper switch input
- Tamper bypass jumper
- Technician keypad fast connector
- PS-2 power supply socket
- ID number DIP switch
- Card location buzzer
- Supplied mounted in a standard plastic 19 X 13cm box
- Size: 8.2 X 15cm
- Technical specs: 10-15V, 30mA in idle state, Fuse: 0.9A

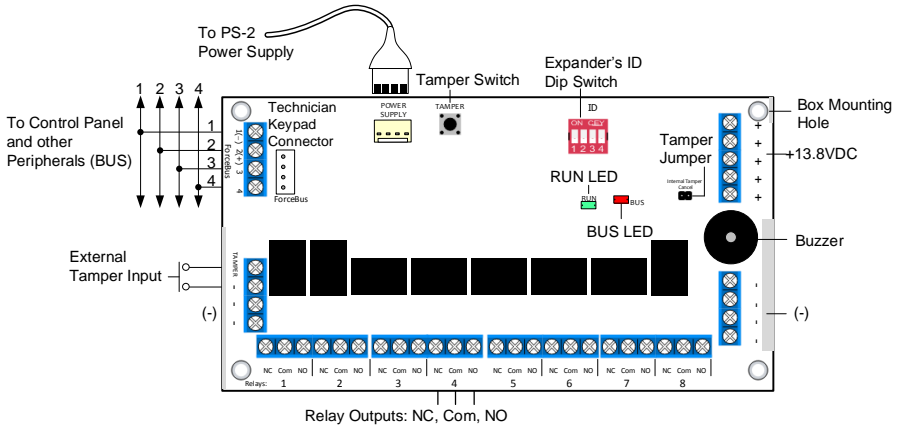


Figure 16. OEX508 connection diagram

2.10 Connecting radio transmitters, TRV/TRU-100

PIMA's TRV-100 (VHF) and TRU-100 (UHF) long-range radio transmitters are used as main or backup communication path to the monitoring station (CMS). Each model can use two different frequencies⁴ within its transmitting range.

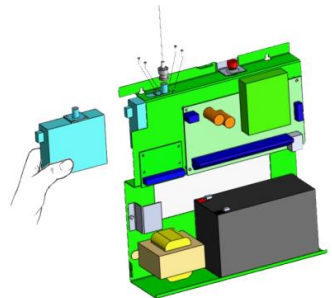
Only one transmitter can be connected per each control panel.



Disconnect AC power and battery before installation.

To connect the transmitters, do the steps that follow:

1. Mount the transmitter on the upper left side of the control panel's rack:
 - a. Hold it tight to the rack's back and insert its top side to the designated elliptic hole, upwards.
 - b. Fasten the transmitter to the rack with the supplied screws.
 - c. Make sure the screws are tighten, not to decrease the radio transmission.
2. Connect the antenna, by rotating it clockwise.
3. To Program the radio parameters, see section 8.1.2, on page 34.
4. Test the radio.



⁴ The frequencies are set using the *Comax* software (guide P/N 4410053).

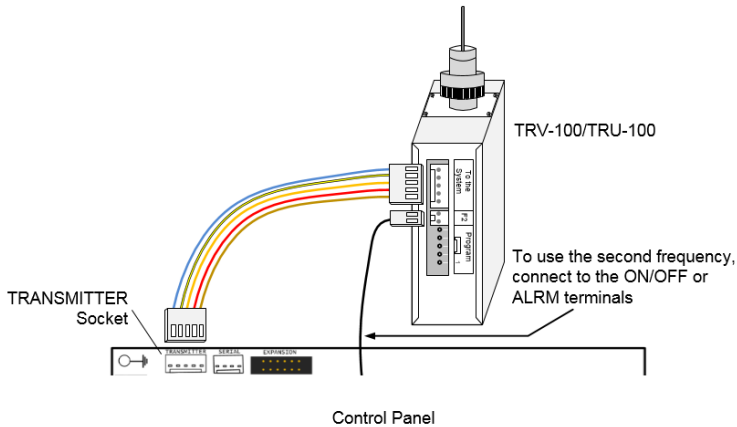


Figure 17. TRV/TRU-100 connection diagram

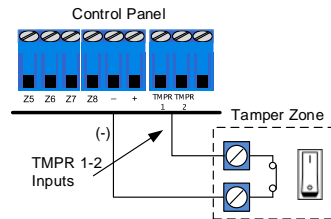
2.11 Connecting tamper switches

TMPR 1 & 2 serve as inputs for tamper switches in boxes, detectors, sirens, etc. The inputs are set in the *Peripherals* → *Tampers & EOLs* menu (see section 5.2, on page 26).

By default, the control panel's box tamper is connected to TMPR 1 input.

To connect tampers, follow the next steps:

1. Connect one wire to the TMPR 1 or 2 terminals.
2. Connect the other wire to a (-) input.
3. Set the tampers parameters.



2.12 Connecting keypads

2.12.1 Keypads installation guidelines

- 16 addressable keypads (max) numbered 1-16 (or un-addressable keypads with ID=0).
- The ID numbers must be consecutive.
- Keypad with ID=0 cannot be supervised, nor partitioned.
- The ID number is set in the *Expanders* → *Keypads Setting* menu (see section 5.3, on page 27).

2.12.2 LCD keypads, KLT/KLR500

Main features

- Touch/rubber keys, 7-line LCD screen, 128x64 pixels display
- 4 operational LEDs
- Interfaces with the BUS and uses PIMA proprietary protocol
- Tamper switch protection

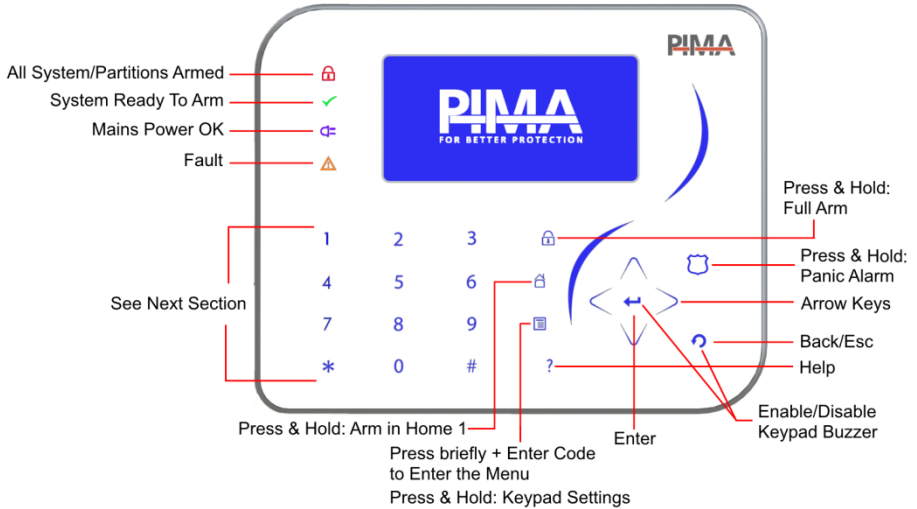
Technical specs





- Powered by 13.8VDC, nominal
- Operating Voltage Range: +9 to +14 VDC

Current consumption:

- Min.: 50mA (max.)
- Illuminating: 90mA

Quick guide



LED	Type	Status	Indicates
	Arming	Steady On	System armed Away/all partitions armed
		Off	System disarmed/all partitions disarmed
		Flashes once every second	Exit delay in progress (in all or some partitions)
		Flashes once every two seconds	One or more partitions are armed (where relevant)
	Ready To Arm	Steady On	System can be armed
		Off	One or more zones are open or a fault exist
	Fault	Flashes once every 0.5 second	One or more faults exist, system/partition is disarmed.
		Off	No fault exist (or the system is armed)
	Mains	Steady On	AC OK
		Off	AC loss

Action and alarm keys

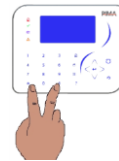
Pressing and holding some keys allows the following actions:

Key	Action
1-4	Arming to Home 1-4 modes
5	Display zone status
*	Turn on/off the keypad's buzzer for all the chime zones
0	Display the service provider, system name and cloud code


Keypad alarms

The users can trigger three different alarms - panic, fire, and medical - by pressing and holding key combinations on the keypad. When these alarms are triggered, **FORCE** activates the programmed responses for such alarms, including triggering the sirens and reporting the CMS (where relevant) and contacts.


Key Combination	Alarm	Response
4 + 6	Medical	The same as in <i>Medical</i> zone
7 + 9	Fire	The same as in <i>Fire</i> zone
* + #	Panic	The same as in <i>Panic</i> zone

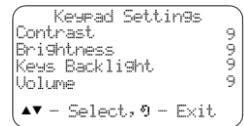


Keypad settings

Press and hold the keypad settings key  to enter the settings screen. In this screen you set the keypad's audio visual definitions: *contrast*, *brightness*, *keys backlight* and the buzzer's *volume*.

Each setting is scaled 0-9. Settings are per keypad.

Use the arrow keys to select a parameter, press Esc  to save and exit.

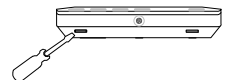


Warning: if you set the volume to 0, no alert will be sounded from the keypad buzzer, including from chime zones.

2.12.3 Connect the KLT/KLR500 keypads

Follow the next steps to connect the keypads⁵:

1. Insert a flathead screwdriver to the notches on the keypad's bottom, press and remove the backplate.
2. Pass the BUS wires through the opening at the backplate.
3. Mount the backplate on a flat surface.
4. Connect the BUS wires.
5. Attach the keypad to the mounted backplate, top side first.



⁵ The tamper reports over the BUS.

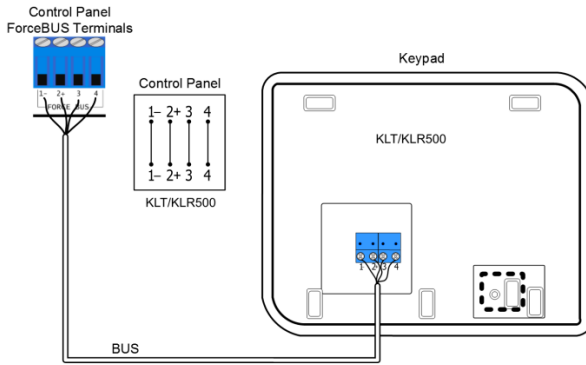


Figure 18. KLT/KLR500 connection diagram

2.13 GSM add-on, GSM501

The GSM add-on is used for transmitting reports and notifications from the **FORCE** to the CMS and the contacts, via cellular network. It is a Quad-band transceiver. An external antenna (long/short) can be used with the GSM501.

2.13.1 Main features

- 4 bands: 850/900/1800/1900 MHz
- Current consumption: 30mA in idle state, 200mA when broadcasting.
- Antenna connection type: SMA
- The GSM add-on requires a SIM card, which should be purchased separately.

2.13.2 The LEDs

The GSM module has 2 LEDs: network registration and voltage. The LEDs states are:

LED	State	Indication
Network Registration (Red)	Flashes rapidly	Initializing
	Flashes once every 3 sec.	SIM registered
	Flashes once every 1 sec.	SIM not registered
	Off	SIM missing or power loss
Modem Power (Green)	Illuminates	Power OK
	Off	Power loss

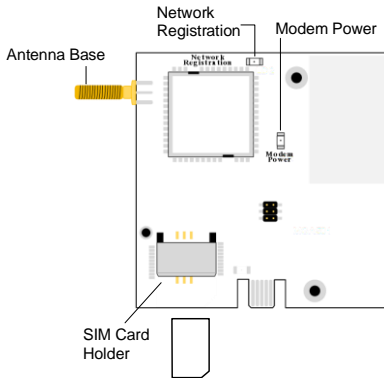


Figure 19. Add-on's front side

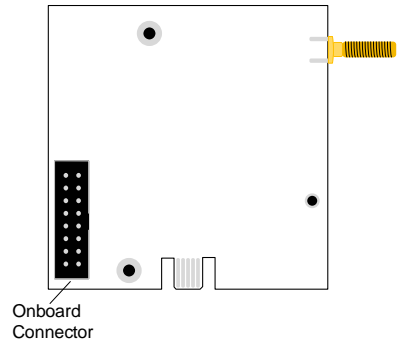


Figure 20. Add-on's back side

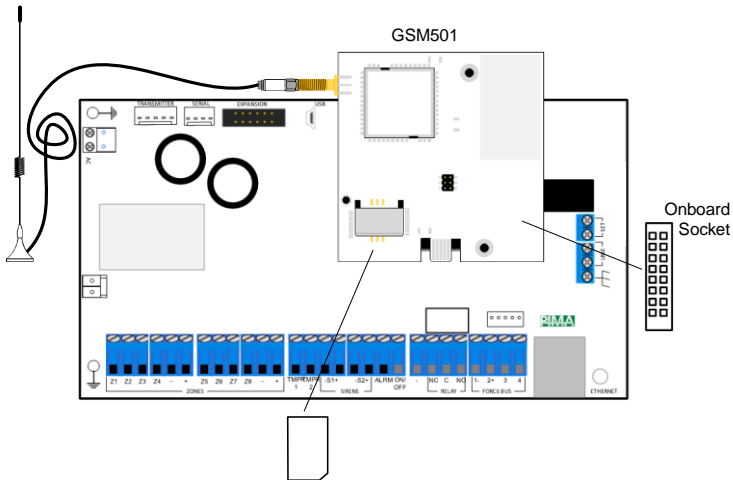


Figure 21. The GSM add-on installed onboard

2.13.3 Add-on installation and how to replace the SIM card



Disconnect AC and battery power before connecting the add-on.

1. Insert the SIM card to the SIM holder: hold the SIM card so that the metal contacts are facing down, and the notch is aligned correctly, as shown in Figure 19, above.
2. Connect the antenna to the add-on, by rotating its connector clockwise, and place the antenna where the cellular network signal is strong. The antenna's cable is 3 meters long.
3. Pressing gently, connect the add-on to the socket (J8).
4. Reconnect the control panel to power and set the add-on in the *Peripherals/Comm. Modules/GSM Module* menu (see page 37).
5. Test the add-on

Chap. 3 System Programming

3.1 Menus and codes

Like all PIMA alarm systems, **FORCE** has two menus: User and Technician, each accessed with its own Master code. However, the **FORCE** has a new feature, in which a Central Monitoring Station (CMS) can have a separate communication settings lock code.

- **Master technician code:** allows accessing all the technician menus, including all CMSs menus, as long as no CMS code was set; see next.
- **CMS lock code:** an optional code, for locking the CMS definitions from accessing it using the Master technician code. This code only allows the technician/CMS to set and access the CMS communication definitions, including the account ID no. and the communication paths.

3.1.1 Code setting guidelines

Note the following when setting codes in the **FORCE** security system:

- All codes, except the Quick Arm code are made of 4 to 6 digits
- The Quick Arm code (set by the users) is made of 2 digits
- Codes cannot start with the 2 digits of the Quick Arm code
- Every code is unique
- Codes 1234 and 5555 are reserved

3.1.2 Activation codes

Eight codes for activating devices (via relay outputs) by the system users - whether it's an electric gate or a floodlight, users can turn them on and off using these 8 codes. Triggering the relay outputs is done using the *Activation Codes 1-8* programmed output types (see Appendix C, on page 50).

Activation codes are subject to keypad and user partitioning (where relevant).




3.2 Changing the default Master codes

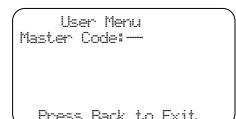
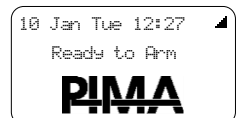
When entering the menus for the first time, the **FORCE**'s default technician and user Master codes must be changed. The default codes are:

- Master technician code: *1234* Master user code: *5555*

Follow the next steps to change the codes. This process cannot be avoided.

3.2.1 Changing the Master user code

1. After connecting the **FORCE** to power, the main screen is displayed.
2. Press 5555 - the Master User Code screen is displayed.
3. Press Enter  - the cursor moves to the right.
4. Enter a new 4-6 code and press Enter . Write the code down and advise the system owner to keep it in a safe place.
5. Press Esc  to return to the main screen.



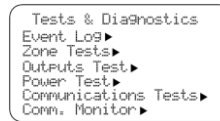
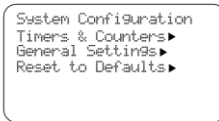
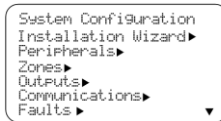
3.2.2 Changing the Master technician code

1. Enter the Master user code to enter the User menu.
2. Press the Down arrow to scroll to the *System Options* menu and press Enter ↵.
3. Scroll to *Technician Permit* and press Enter ↵ - the main screen is displayed. This step is mandatory and is time limited.
4. Press 1234 - the Master Technician Code screen is displayed.
5. Press Enter ↵ - the cursor moves to the right.
6. Enter a new 4-6 Master technician code. Write it down and keep it in a safe place.
7. Press Enter ↵ - the cursor moves back to the left.
8. Press Esc ↶ to return to the main screen.



3.3 The technician menu

The technician menu is divided into 2 sub-menus: System Configuration, and Tests & Diagnostics. See the menus below.



3.3.1 System Configuration

The *System Configuration* menu includes the sub-menus listed in the next table:

Menu	Parameters
↵ Installation Wizard	Step by step, quick setup parameters: account ID menu, CMS1 communication paths and radio report codes.
↵ Peripherals	Zone and output expanders, keypads, tamper switches, and EOL resistors.
↵ Zones	Zone and zone type definitions, copy zones.
↵ Outputs	Control panel and expansion cards' relay outputs.
↵ Communications	CMS 1-2 definitions, PIMA cloud, and radio report codes.
↵ Faults	System responses to faults and entering false code.
↵ General Settings	System name, service provider, Master technician code, and other parameters.
↵ Reset to Defaults	Partial or full system reset

3.3.2 Tests & Diagnostics

See Chap. 13, on page 45.

Chap. 4 Installation Wizard



Parameter	Description	Default	Range
Time and Date	The system time	-	-
Entry Delay 1	A period of time that should allow disarming and entering the premises through delayed zones, and disarming the control panel, without triggering the alarm.	30 sec	0-250
Exit Delay 1	A period of time that should allow arming and exiting the premises through delayed zones, without triggering the alarm.	60 sec	5-250
Ext. Siren	The <i>External Siren</i> programmed output type time	240 sec	0-9998
Int. Siren	The <i>Internal Siren</i> programmed output type time		
Remote Expanders	The no. of remote ZEX508/516 zone expanders.	0	0-16 ⁶
Keypads	The no. of addressable keypads (ID 1-16)	0	1-16
Tech. Code	The Master technician code	-	-
↵ CMS1	See section 8.1, on page 33.		
↵ Report Codes	See page 34.		

⁶ Depending on the overall zone number.

Chap. 5 Peripherals

The *Peripherals* menu includes the following sub-menus:

- 1) ↪ Zone Expanders: see below.
- 2) ↪ Tamper & EOLs: see below.
- 3) Keypads: set the no. of addressable keypads (ID 1-16). Keypad with ID no. 0 is not supervised, nor can it be partitioned.
- 4) Keypads: see section 5.3, on page 27.
- 5) Output Expanders: set the no. of the relay output expanders.

5.1 Zone expanders

System Configuration ► *Peripherals* ► *Zone Expanders*

The *Zone Expanders* menu includes the following sub-menus:

- 1) Remote Expanders: set the no. of 8/16 remote zone expanders.



Each 16-zone expander is programmed as two 8-zone expanders and occupies 2 consecutive ID numbers. For example, if expander #3 is a 16-zone one, it takes ID numbers 3 and 4 and so expander #4, the next expander will take ID number 5 (and not 4).

- 2) Local Zone Expander: select if the ZEL508 local zone expander is installed.
- 3) Zone Doubling: when selected the onboard zone 1-8 inputs can be used as inputs for 8 additional zones; see section 2.6.1, on page 11.

5.2 Tamper and EOLs

System Configuration ► *Peripherals* ► *Tampers and EOLs*

Parameter	Description
<input type="radio"/> Tamper 1	TMPR1 input is active.
<input type="radio"/> Tamper 1+EOL	TMPR1 input is EOL supervised, for detecting a short.
<input type="radio"/> Tamper 2	TMPR2 input is active.
<input type="radio"/> Tamper 2+EOL	TMPR2 input is EOL supervised, for detecting a short.
<input type="radio"/> External Siren+EOL	SIREN Ext. output is EOL supervised, for detecting cut and short.
<input type="radio"/> Internal Siren+EOL	SIREN Int. output is EOL supervised, for detecting cut and short.
<input type="radio"/> Double EOL	Two EOL resistors are used on ALL EOL supervised zone loops.
Resistor 1-2	Enter the resistors values in Ohm. The value entered is multiplied by 100. For example, when using a 2.2 kΩ resistor, set the value to 220.

5.3 Keypad Settings

System Configuration ► Peripherals ► Keypad Settings

Press * or # to select a keypad. Note that the *Keypad Settings* menu applies only for addressable keypads with ID no 1-16; keypad with ID=0 has no option for settings.

The *Keypads* menu includes the following sub-menus:

- 1) Name: user text, up to 16 characters.
- 2) ↵ Options (press * or # to select a keypad):

Parameter	Description
⊙ Illum. During Alarm	The keypad will illuminate during the alarm time.
⊙ Illum. During Delay	The keypad will illuminate during the exit/entry delay times.
3) ↵ Partitions:	select the keypad's partitions by pressing the desired partition/s. The selected partitions will stay on and not flash.

Chap. 6 Zones

The *Zones* menu includes the following sub-menus:

- 1) ↪ Zone Settings. See below.
- 2) ↪ Zone Type Settings. See section 6.2, on page 29.
- 3) ↪ Copy Zones. See section 6.3, on page 30.
- 4) ↪ Partitions Names. See section 6.4, on page 30.

6.1 Zone Settings

System Configuration ► Zones ► Zone Settings

Press * or # to select a zone.

- 1) Type: select the zone type from the list. See the list below.
- 2) Name: user text, up to 28 characters.
- 3) Delay/24H: select from the following options:

Parameter	Description
Instant	Opening this zone while the system is armed will trigger the alarm instantly
Entry Delay #1-2	Opening this zone while the system is armed will trigger the alarm only after this delay elapses, unless the system is meanwhile disarmed.
Delay Follower	Opening this zone while the system is armed will not trigger the alarm as long as the entry delay has not expired. If the delay elapses and the zone is still open, the alarm will be set off.
24 Hour	This zone is constantly armed, regardless of the system state of arming. In use mostly with smoke detectors and panic keys.

- 4) Attributes: select from the following list:

Parameter	Description
<input type="radio"/> Disabled	The zone is permanently inactive.
<input type="radio"/> Normally Open	<ul style="list-style-type: none"> • Selected: Normally Open zone • Unselected: Normally Close zone
<input type="radio"/> Allocated to Home 1-4	Select to which <i>Home</i> partial arming mode this zone will be allocated to. Multiple selection is allowed.
<input type="radio"/> EOL Supervision	Select if the zone will be supervised for cut and/or short ⁷ .
<input type="radio"/> Chime Zone	This zone will trigger the keypad buzzer, whenever it is opened while the system is disarmed. Also triggered is the <i>Chime Activation</i> programmed output type.
<input type="radio"/> Roller Blinds	Select to adjust the zone's sensitivity to roller blinds.

- 5) False Alarms: select from the list that follows (*Inactive* is also an option).

Parameter	Description
→ Double Knock	This zone will trigger the alarm only if two pulses are detected during the <i>Double Knock</i> time (see Chap. 10, on page 39).
Cross Zoning	This zone will trigger the alarm when opened, only if other cross zone is opened too, during the <i>Cross Zoning</i> time (see Chap. 10, on page 39).

⁷ Depending on the defined number of resistors. See Chap. 11, on page 42.

Parameter	Description
Partition Allocation	Select the zone's partitions. The selected numbers will stay on and not flash.
Soak Test Mode	Select to put the zone in test mode for up to one week. See Chap. 10, on page 39 for details.

6.2 Zone Types Settings

System Configuration ► Zones ► Zone Types Settings


Zone Type	Attributes
↵ Burglary, Panic, Silent Panic, Fire, Duress, Medical, Anti-Mask, Shock Sensor, Key Switch Modes, Custom Zone Types	1) → Sensitivity: set the zone sensitivity in milliseconds. Range: 1-3000, default: 800. Sensitivity is the time period between opening the zone (relay), and triggering the alarm. Closing the relay for one second resets the zone. 2) ↵ Attributes: see below. 3) → Audible Notification: select from the list: <ul style="list-style-type: none"> Alarm tone: when calling the contacts, hi-lo alarm will be sounded.
Key Switch Types	↵ Key Switch in Away/Home 1-4: select the key type and set its sensitivity (see above).
Custom Zone Types	4) Custom Zone Type 1-5: see the other zone types above, and in addition: <ol style="list-style-type: none"> 1) Trigger & Report: select a standard zone type (Burglary, Panic, Etc.) to be used for reporting the CMS and triggering outputs, or <i>Custom Type</i>. If you select <i>Custom Type</i> you can use it to trigger outputs to activate/deactivate special devices such as pumps and heaters). 2) Name: user text, up to 16 characters.

6.2.1 Attributes

System Configuration ► Zones ► Zone Types Settings ► Attributes

The zone type attributes are listed in the table below:

Attribute	When selected...
⊙ Trigger Sirens	The <i>External</i> and <i>Internal Siren</i> programmed output types will be triggered in alarm, and activate the sirens (by default. See Section 7.1, on page 31 for a warning).
⊙ Ext. Siren at Disarm	The <i>External Siren</i> programmed output type will be triggered in alarm, and activate the external siren, even while the FORCE is at disarm.
⊙ Reports at Disarm	Reports to the CMS will be sent, even while the FORCE is at disarm.
⊙ Auto-bypass	If this zone triggers the alarm 3 times while the system is armed, the zone is automatically bypassed (a <i>Zone Bypass</i> report is generated) until the system/partition is disarmed, or until the <i>Auto-bypass Limit</i> time elapses. See Chap. 10, on page 39.
⊙ Different Siren Tone	A different tone will be sounded when this zone triggers the alarm

Attribute	When selected...
<input type="radio"/> Alarm Re-triggering	<ul style="list-style-type: none"> Selected: if the zone is still open at the end of the alarm time, the zone will retrigger the alarm, continue to activate the sirens and will generate a new alarm report. Unselected: if the zone is still open when the alarm time elapses, it will NOT retrigger the alarm (unless it is closed and re-opened).
 Note	
<input type="radio"/> Activate Buzzer	The keypad's buzzer will sound beeps throughout the alarm time
<input type="radio"/> User Bypass	Users are allowed to bypass the zone temporarily (for the next arming session, or until the <i>Zone Bypass Limit</i> time elapses)

This attribute can only be used, if the Trigger Sirens attribute is selected too.

6.3 Copy Zones

System Configuration ► Zones ► Copy Zones

Select between copying a single zone's attributes, type, partitions, and name to one or more zones, and copying succeeding zones to a different location.

- 1) Single to Multiple: see below.
- 2) Multiple to Multiple: see below.

6.3.1 Single to Multiple

- 1) Select the zone to be copied and to which zone/s.
- 2) ↩ Copy Options:

Attribute	What will be copied
<input type="radio"/> Zone Attributes	The parameters from the zone attribute screen
<input type="radio"/> Zone Type	The zone type
<input type="radio"/> Zone Partitions	The partitions that the zone is allocated to
<input type="radio"/> Zone Name	The zone name

6.4 Multiple to Multiple

- 1) Define a group of consecutive zones to be copied.
- 2) Select a zone from which the zones will be copied to; for example, if you select to copy zones 21-34 (14 zones) and select zone 47, the 14 zones will be copied to zones 47-60.
- 3) ↩ Copy Options: see above.

6.5 Partitions Names

System Configuration ► Zones ► Partitions Names

Partitions can have unique names that will appear in the contacts reports and the event memory.

- 1) Use # or * to scroll and select the partition.
 - Name: user text, up to 16 characters.

Chap. 7 Outputs

The *Outputs* menu includes the following sub-menus:

- 1) ↪ Onboard Outputs: see below.
- 2) ↪ Zone Expanders: set the 8-zone and 16-zone expanders (ZEX508/516). There are up to 16 available outputs, depending on the overall number of expanders. See section 7.17.2.
- 3) ↪ Outputs Expander: up to 32 relay outputs can be set in outputs expanders (OEX508, 8 outputs per expander). See section 7.3.

7.1 Onboard

System Configuration ► *Outputs* ► *Onboard*

The *Onboard* menu includes the following sub-menus:

- 1) ↪ External Siren
- 2) ↪ Internal Siren
- 3) ↪ Relay
- 4) ↪ On/Off
- 5) ↪ Alarm

Both the external and internal siren outputs have the following features:

- They supply high current
- They can only trigger DC sirens
- They can be triggered separately



Warning: the sirens outputs will be triggered, only if you don't change the default sirens programmed output types that triggers them.

Each output screen has the following parameters:

Parameter	Details
Output Type	The programmed output type that will trigger the output. For example: <i>Burglary, Panic, Key in Away/Home 1-4</i> . For the complete list of the output types see Appendix C., on page 50.
⊙ Positive Polarity	Set the output's polarity: <u>ON/OFF, Alarm (Open Collector)</u> <ul style="list-style-type: none"> • <u>Selected</u>: the output is normally switched to ground; disconnected when activated. • <u>Unselected</u>: the output is normally disconnected; switched to ground when activated.
	<u>Relay</u> <ul style="list-style-type: none"> • <u>Selected</u>: the C and NC terminals are normally shorted; C and NO terminals are shorted when activated. • <u>Unselected</u>: the C and NO terminals are normally shorted; C and NC terminals are shorted when activated.

Parameter	Details
↵ Partitions	Set the physical output's allocation to partition/s - press the desired partition/s. The selected partitions will stay on and not flash. Press # or * to scroll between partitions.
→ Name	User text, up to 16 characters.

7.2 Zone Expanders

System Configuration ► Outputs ► Zone Expanders

The ZEX508/516 zone expander's parameters are the same as those of the onboard outputs, above.

Press # or * to scroll between expanders.

7.3 Output Expander

System Configuration ► Outputs ► Output Expander

The OEX508 output expander's parameters are the same as those of the onboard outputs, above.

Press # or * to scroll between expanders.

↵ Relay No.1-8: press the desired relay and set its parameters.

Chap. 8 CMS & Communications

The *CMS & Communications* menu includes the following sub-menus:

- 1) ↪ Monitoring Stations. See below.
- 2) ↪ PIMA Cloud. See section 8.2, on page 36.
- 3) ↪ General Settings. See section 8.1.3, on page 35.
- 4) ↪ Telephone Settings. See section 8.4, on page 36.
- 5) ↪ Network Settings. See section 8.5, on page 37.
- 6) ↪ GSM/GPRS Settings. See section 8.6, on page 37.

8.1 Monitoring Stations

System Configuration ► *CMS & Communications* ► *Monitoring Stations*

The *Monitoring Stations* menu includes the following sub-menus:

- 1) ↪ CMS⁸ 1-2. See below.
- 2) ↪ Radio. See section 8.1.2, on page 34.
- 3) ↪ Custom Zones Report. See section 8.1.3, on page 35.

8.1.1 CMS 1-2

System Configuration ► *CMS & Communications* ► *Monitoring Stations* ► *CMS 1-2*

The *CMS 1-2* menu includes the following sub-menus:

- 1) ↪ Comm. Paths. See below.
- 2) ↪ Event Reporting: see page 34.
- 3) → CMS Name: user text, up to 16 characters.
- 4) → CMS Lock Code: set a code to the definitions of this CMS. See Appendix D, on page 52.

Comm. Paths

System Configuration ► *CMS & Communications* ► *Monitoring Stations* ► *CMS 1-2* ► *Comm. Paths*

The *Communication Paths* menu includes the following sub-menus:

- 1) ↪ Telephone (PSTN). The parameters in this menu are:

Parameter	Details
↪ Account ID	For each defined partition, set an ID number. If you only set partition 1's number, it will serve all other partitions.
↪ Telephones	Set up to 4 numbers of the CMS.
→ Protocol	Select the CMS PSTN protocol from the list. The options are: ContactID, PID, SIA ⁹ , and NPAF.
System ID	A parameter required by the NPAF protocol only. Consult the CMS.
↪ ACKS	1) → Handshake Wait: how long the control panel will wait for a Handshake, before disconnecting the call and redialing. Change the default time only if necessary, for example if the Handshake signal for the selected protocol is not the first one sent by the CMS receiver. Range: 20-250 seconds.

⁸ Central Monitoring Station

⁹ Consult with PIMA support team regarding the functionality of the PID and SIA protocols

Parameter	Details
	2) → Kissoff Wait: how long to wait for a Kissoff message, before resending the report. Change only if necessary, for example if there are delays in the communication. Range: 1-5000 milliseconds.
	3) → ACK Frequency: select between Lo-Hi, 1400, 2300, and SIA.
Periodic Test	Set a time of the day to send a test report to the CMS. This report is sent in addition to the test report interval (next).
Test Interval	Set an interval in hours to send a test report to the CMS. This report is sent in addition to the periodic test report.
Number of Dials	Set the number of dials and redials that if fail (no ACK is received), a communication fault is reported.
☉ Primary Path	Select if the telephone is the primary path for reporting the CMS.
4) ↵ GSM-Voice:	see the Telephone (PSTN) menu above.
5) ↵ Network (Ethernet):	in addition to the above Telephone (PSTN) parameters, the network has the following:

Parameter	Details	Default	Range
↵ Network Addresses	<u>IP/URL 1-2</u> : enter up to two IP addresses of the CMS, or a URL (web address). <u>Port 1-2</u> : enter the port no.		
Supervision	Set supervision (test) report interval. The report is designated to the IP receiver at the CMS.	5 min	0 (not reporting)-59:59 mm:ss

6) ↵ GPRS-IP: see Network (Ethernet) above.

Event Reporting

System Configuration ► CMS & Communications ► Monitoring Stations ► CMS 1-2 ► Event Reporting

Select the events to report to the CMS (e.g. Burglary Alarm, Tamper Alarm, Invalid Code).

8.1.2 Radio

System Configuration ► CMS & Communications ► Monitoring Stations ► Radio

See section 8.1.1 above for details on the parameters, except those on the next table:

Parameter	Details	Default	Range
Format	Set the radio format. Obtain it from the CMS.		-
↵ Report Codes	See below.		-
Transmissions No.	Set the number of transmissions and retransmissions per report.	5	1-16
Frames Per Trans.	Set the number of frames per single transmission.	10	1-16

Reporting Codes

Set the radio reporting codes for alarms and other events, as well as the restore codes. Note the following:

- The codes apply only for some radio protocols. Consult the CMS before setting them.
- A zone is restored in the following conditions:
 - The alarm system/partition is disarmed (or the first partition, if the zone is allocated to more than one).

- b. A user un-bypass a zone
 - c. *Bypass Limit* time elapses
3. Following are several points regarding the *zone restore* reporting:
- o A *zone restore* report is generated when an alarmed zone is closed and rearms itself. When siren time elapses, the zone status is checked and if it has already been closed, the report is generated.
 - o If the zone is not set to trigger the sirens, the report is sent as soon as the zone is closed.
 - o If a zone had triggered the alarm and was meanwhile closed, the report will be generated as the alarm system is disarmed.
 - o In partitioned system, a *zone restore* report is generated, only when the partition it's allocated to, is disarmed.

The *Reporting Codes* menu includes the following sub-menus:

Parameter	Details
↵ Zones	For each zone, set codes for the following events: <i>Alarm+Restore</i> , <i>Fault+Restore</i> , <i>Bypass+Restore</i> . Press # or * to scroll between zones.
↵ Arm/Disarm-User	For each user, set event codes for <i>Arming</i> and <i>Disarming</i> . Press # or * to scroll between users.
↵ Arm/Disarm-Other	Set codes for <i>Arming</i> and <i>Disarming</i> events, in any way other than by users.
↵ Faults	Set event and restore codes for the following events: <ol style="list-style-type: none"> 1) Power: <i>AC Loss</i>, <i>Low Battery</i>, <i>Power Loss</i>, <i>Detector's Voltage Failure</i>, <i>Fuse</i>, <i>Peripheral's Power Fault</i>. 2) Communication: <i>Communication Fault</i>, <i>Telephone Line Fault</i>, <i>Cellular Fault</i>, <i>Network Fault</i>. 3) Sirens: <i>External Siren Fault</i>, <i>Internal Siren Fault</i>.
↵ Alarms and Others	Set event and restore codes for the following events: <ol style="list-style-type: none"> 1) <i>Panic</i> and <i>Fire</i> alarms, <i>Technician On-site</i>, <i>Invalid Code</i>, <i>Test</i>. 2) ↵ <i>Tampers: Tamper 1-2</i> and <i>Peripherals' Alarm</i> and Restore codes.

8.1.3 Custom Zones Reports

System Configuration ► *CMS & Communications* ► *Monitoring Stations* ► *Custom Zones Reports*

Set the ContactID (alarm and restore) codes, and SIA's alarm and restore codes for the custom zones. Custom zones are based on modified zone types that allow alarm reporting with any ContactID or SIA code (other than the original zone type - Burglary, Panic, etc.).

Below is a list of more frequently used ContactID and SIA events, which can be used with the custom zones.

Event	ContactID	SIA
Gas detected	151	GT
Refrigeration	152	ZA
Loss of heat	153	ZA
Water Leakage	154	WA
Low bottled gas level	157	GA
High temp	158	KA

Event	ContactID	SIA
Low temp	159	ZA
High Humidity	168	-
Low Humidity	169	-
Low water pressure	201	WT
Low water level	204	WT

8.2 PIMA Cloud

System Configuration ► CMS & Communications ► PIMA Cloud

Select the communication path to the cloud. The options are Network (Ethernet) and GPRS-IP. See section 8.1.1 above for details.

8.3 General Setting

System Configuration ► CMS & Communications ► General Setting

Parameter	Details
<input type="radio"/> Remote Up/Download	<ul style="list-style-type: none"> <u>Selected</u>: remote upload/download via the FORCE Command software without the need for user permission is enabled. <u>Not selected</u>: remote upload/download is enabled only with user permission (see the User guide [P/N 4410460] for how to details)
<input type="radio"/> Remote Disarm	Select to enable remote system disarm via the PIMALink app.

8.4 Telephone Settings

System Configuration ► CMS & Communications ► Telephone Settings

Parameter	Details
<input type="radio"/> Telephone Connected	Select if the control panel is connected to PSTN line.
External Line Access	Set an access number (up to seven digits) for private PBX.
Prefix	Set digit/s to be dialed before any of the PSTN telephone numbers.
Rings to Answer	Set the number of rings before the control panel answers a call.
<input type="radio"/> Check Dial Tone	<ul style="list-style-type: none"> <u>Selected</u>: dial tone will be checked before making a call <u>Not selected</u>: the control panel will dial without checking for dial tone
<input type="radio"/> Answering Machine	Answering or facsimile machine are connected to the telephone line. To connect to the control panel by phone remotely, do the following: <ol style="list-style-type: none"> 1) Call the FORCE. 2) Wait for 2 rings. 3) Hang off. 4) Wait a few seconds and redial.
<input type="radio"/> VoIP	The telephone line uses Voice over IP technology.
<input type="radio"/> Line Check at Arm	When the alarm system is armed away dial tone will be checked every 1 minute.

Parameter	Details
☉ Line Check at Disarm	When the alarm system is disarmed dial tone will be checked every 1 minute.
↵ Callback No.	Set a telephone number for the control panel, to call the computer running the Upload/Download software. This number is displayed in the user menu under <i>Remote Service</i> . See the User guide for details (P/N 4410460).

8.5 Network Settings

System Configuration ► CMS & Communications ► Network Settings

Parameter	Details
☉ Network Connection	The control panel is connected to Ethernet network.
☉ DHCP	The control panel is automatically assigned with an IP address by the router. If you don't select it, enter a static IP address (next).
Static IP	Enter a valid IP address of the control panel. When the IP address is set, the DHCP parameter is ignored (even if selected).
Netmask, DNS, Default Gateway	Set these parameters.
Callback Address, Port	Set an IP address and port no. for the control panel to return a session connection, in response to a request made by the FORCE Manager software, or by a user (from the User Menu.)

8.6 GSM/GPRS Settings

System Configuration ► CMS & Communications ► GSM/GPRS Settings

Parameter	Details
→ GSM Module	Select <i>Installed</i> , if the module is connected.
☉ Virtual Provider	Select if the SIM card's provider is virtual.
Callback Address, Port	Set an IP address and port no. for the control panel to send a connector request, in response to a request made by the FORCE Manager software.
↵ APN 1 Settings	<ol style="list-style-type: none"> 1) Name: user text, up to 16 characters. 2) Username, Password: obtain these from the service provider.

Chap. 9 Faults

The *Faults* menu includes the following sub-menus:

- 1) ↪ AC Fault. See below.
- 2) ↪ Low Battery. See *AC Loss* below.
- 3) ↪ Phone Line Fault. See *AC Loss* below.
- 4) ↪ Network Fault. See *AC Loss* below.
- 5) ↪ GSM Module Fault. See *AC Loss* below.
- 6) ↪ CMS Comm. Fault. See *AC Loss* below.
- 7) ↪ Tamper Open. See *AC Loss* below.
- 8) ↪ Invalid Code. See *AC Loss* below. This event is generated when a user exceeds the Code Keystrokes counter, without a valid code. See *Timers and Counters* on the next page.
- 9) ↪ Other Faults. See *AC Loss* below.

9.1 AC Fault

System Configuration ► Faults ► AC Fault

Parameter	Details
Attributes	See section 6.2.1, on page 29.
Notification Delay	Set time in minutes to delay notifications to the CMS and the contacts. The delay also applies to activating outputs and the keypad's buzzer. Range: 0-250.
Report Time Span	Set a time span in which the fault will be reported. This feature is useful when large scale faults, such as a wide outage occur, to prevent report overloading at the CMS.
Audible Notification	Select the notification when alerting the contacts by phone: <ul style="list-style-type: none"> • Alarm Tone: hi-lo sound

Chap. 10 Timers and Counters

The *Timers and Counters* menu includes the system timers' definitions. All times (except those otherwise mentioned) are in seconds.

Parameter	Description	Default	Range
Programmed Output Types	See next section.		
Entry Delay 1-2	A time period that allows entering the premises and disarming it (or a partition), without triggering an alarm.	30/60	
Exit Delay	A time period that allows exiting the premises after arming the alarm system (or a partition), without triggering an alarm.		
Double Knock	A time period during which only if a detector activates twice, it triggers an alarm.		
Cross Zoning	A time period during which only if two cross zones activate, an alarm is triggered. This timer starts running as soon as the first cross zone activates - if another cross zone also activates during this time, an alarm is triggered. If the other zone is activated after the timer elapsed, no alarm is triggered. If the first cross zone is still active when the timer elapses, whenever another cross zone activates, an alarm is triggered.	30	0-250
Soak Test	A time period (days) during which the zone is in test mode: if it activates it will not trigger an alarm (but the event will be recorded). After this timer elapses, the zone is automatically reinstated (at midnight).	3 days	1-7
Bypass Limit	A time limit before arming the alarm system (or a partition) during which a zone can be bypassed by a user. The zone is un-bypassed when the timer elapses or the alarm system/partition is disarmed, whichever comes first.	0 hr.	0-250
Auto Bypass Limit	A time period during which a zone that was automatically bypassed after triggering the alarm three times during one arming session is reinstated.		
Inactivity	A time period (days) during which if the alarm system has not been armed, ContactID event no. 654 is reported.	7 days	0-99
Code Keystrokes	The number of allowed keystrokes, when entering codes. Any more keystrokes will trigger an alarm and lock the keypad. See next. To reset the counter, wait 30 seconds.	24	10-250
Keypad Lockout	A time period during which the keypad is locked, due to illegal number of keystrokes (see above).	180	0-250

Parameter	Description	Default	Range
Siren beep	The arming/disarming indication beep length	300 mSec	0-1000
↩ Report Delay			
<ul style="list-style-type: none">• AC Fault• Phone Line Fault• GSM Fault• Network Fault	The delay time before transmitting a fault event.	120 min	0-250

10.1 Programmable Output Types

System Configuration ► Timers and Counters ► Programmable Output Types

See *Programmable Output Types*, on page 50, for details on all the programmable output types.



The default alarms and sirens programmable output types match the default zone types, and should not be changed in most installations.

Each Programmable output types' timer has 3 options:



Time (sec)	Description	Use example
0	The output type will activate the physical output until the alarm system is disarmed.	Turning a floodlight on
1-9998	The output type will activate for the set time.	Fire Alarm: escape door opening
9999	The output type will activate for as long as the source event exist.	AC Fault: flashlight indication

Programmable output type	Default	Programmable out type	Default
↔ Alarms		External Siren	240
Burglary		Internal Siren	
Panic		Zone Bypass	9999
Silent Panic		Smoke Reset	60
Fire		Chime	3
Medical	240	Output-Keyfob	5
Duress		Energy Saving ¹⁰	15 min
Anti-mask		Invalid Code	5
Tamper Alarm		↔ Operation Codes 1-8	
↔ Custom Zone Types 1-5			
↔ Faults			
Any Fault			
AC Fault			
Low Battery			
Phone line/Net	9999		
GSM Module			
Communication			
Tamper	240		

¹⁰ See the *Glossary*, on page 54.

Chap. 11 General Settings

Following is the parameters of the *General Settings* menu:

Parameter	Details
System Name	Appears in contacts' notifications. User text, up to 16 characters.
Service Provider	User text, up to 24 characters. The text is displayed when pressing and holding 0 (zero).
Contract Expiration	Date to display appropriate message onscreen
Technician Code	Change code, 4-6 digits.
⊙ One Key Arming	Arming with the Arm Away+Home1 keys ( , ), with no passwords is enabled.
⊙ Display Alarms at Arm	Alarm messages will be displayed when the control panel is armed.
⊙ Final Door Arming	Closing any delayed zone during the exit delay, terminates the delay.
↔ Home Modes-Instant	No exit delay when arming in Home 1-4 modes
⊙ Additional CMSs	<ul style="list-style-type: none"> • <u>Selected</u>: setting CMS 2 parameters + code is enabled • <u>Unselected</u>: setting CMS 2 parameters + code is enabled only by using the Master technician code.
⊙ Zone Bypass-Auto Arm	Open zones are automatically bypassed when auto-arming
⊙ Momentary Key	<ul style="list-style-type: none"> • <u>Selected</u>: momentary key switch • <u>Unselected</u>: toggle key switch
→ Beep on Arming	<ul style="list-style-type: none"> • Any Arming: the siren will sound a beep, whenever the alarm system is armed. • Key switch/Key fob: the siren will sound a beep, when the alarm system is armed by key switch or key fob. • Inactive
→ Beep on Disarming	<ul style="list-style-type: none"> • Any Disarming: the siren will sound 2 beeps, whenever the alarm system is disarmed. • Key switch/Key fob: the siren will sound 2 beeps, when the alarm system is armed by key switch or key fob. • Any+Alarm in Memory: the siren will sound 3 beeps, whenever the alarm system is disarmed, if the alarm was triggered when the system was armed. • Key Switch+Alarm Mem: the siren will sound 3 beeps, whenever the alarm system is disarmed using keyfob or key switch, if the alarm was triggered when the system was armed. • Inactive
↔ Arm Prevention - Faults	See below.

11.1 Arm Prevention - Faults

System Configuration ► General Settings ► Arm Prevention - Faults

You can prevent the users from arming the alarm system if some faults exist¹¹. Without fixing these faults the system cannot be armed.

⊙ The user will be allowed to override the selected faults in this menu.

The faults are: AC Loss, Low Battery, Tamper, Any Expander, Telephone Line, GSM module, and Network.

¹¹ In the user's menu *System Options/Fault Override-Arm* (user permission required)

Chap. 12 Reset to Defaults

The *Reset to Defaults* menu includes the following sub-menus:

- 1) ↪ Select Parameters: select the parameters to be reset, from the following list:
 - ⊙ Communication
 - ⊙ Zones
 - ⊙ Outputs
 - ⊙ User
 - ⊙ Full System Reset - includes all the above.
- 2) ↪ Reset to Defaults: press to reset the selected parameters.



Warning: this action cannot be undone!

12.1 Resetting to factory defaults

If the Master technician code is unavailable, the **FORCE** can be reset to its factory defaults.

To reset to the factory defaults, do the following:

1. Disconnect the alarm system from AC and battery power for 5 seconds.
2. Reconnect AC power.
3. Within 30 seconds from when the main screen is displayed, press 000000 (six zeros). The system reset screen is displayed.
4. Press on *Press and Wait*.
5. When the reset process is over, set new Master codes. See section 3.2, on page 23 for details.
6. Reconnect the battery.

Chap. 13 Tests & Diagnostics

In the main screen, press *Tests & Diagnostics*. This menu includes the sub-menus that follows.

- 1) ↵ Event Memory
- 2) ↵ Zone Test. See below.
- 3) ↵ Output Test
- 4) ↵ Power Diagnostics
- 5) ↵ Communication Tests
- 6) ↵ Comm. Monitor

13.1 Event Memory

Tests & Diagnostics ► *Event Memory*

The *Event Memory* stores up to 1,000 events. Each event is made of a time stamp, the event description, and the event source.

Scroll through the events using the up/down arrow keys.

13.2 Zone Test

Tests & Diagnostics ► *Zone Test*

The *Zone Test* menu includes the following sub-menus:

- 1) ↵ Single Zone: enter the desired zone number, trigger the detector and check the *Successfully Tested* field.
- 2) ↵ All Zones: walk through the entire premises, trigger the detectors and check the display:
 - 5) Tested: the number of tested zone, out of the overall defined zones.
 - 6) Last Tested (zone)
 - 7) ↵ Failed/Not Tested: a list of the zones that failed the test or were not tested.
- 3) Audible Indication: select from the following list:
 - ⊙ Keypad Buzzer
 - ⊙ Beep-External Siren
 - ⊙ Beep-Internal Siren

13.3 Output Test

Tests & Diagnostics ► *Output Test*

The *Output Test* menu includes the following sub-menus, for testing the physical outputs. If an output is not functioning properly, it helps defining whether it is a hardware or configuration based problem:

- 1) ↵ Onboard: select any of the control panel's outputs and *Activate/Deactivate* it. The available outputs are: *External/Internal Siren, Relay, On/Off, Alarm*.
- 2) ↵ Zone Expanders: select an expander (press # or *) and *Activate/Deactivate* the expander's relay output/s. To easily locate the expander, press *Activate Buzzer* and *Activate/Deactivate* the expander's buzzer.

- 3) ↵ Output Expanders: select an expander (press # or *) and an output, and *Activate/Deactivate* it. To easily locate the expander, press *Activate Buzzer* and *Activate/Deactivate* the expander's buzzer.
- 4) ↵ Keypad Buzzer: *Activate/Deactivate* the buzzer.

13.4 Power Diagnostics

Tests & Diagnostics ► *Power Diagnostics*

The *Power Diagnostics* menu includes the following sub-menus, for viewing the control panel and peripherals' voltage and current status.

- 1) ↵ Zone Expanders: select *Local* or *Remote Expanders* and view the card's voltage and current.
- 2) ↵ Keypads: select a keypad (press # or *) and see its current voltage and current.
- 3) ↵ Output Expanders: select an expander (press # or *) and see its voltage and current.
- 4) Battery Voltage: the backup battery's voltage status.
- 5) Panel Current: the control panel and the peripherals' current consumption. Note that *PS* on the display indicates that the peripheral is powered by a local power supply and so its current is not pulled from the control panel.

13.5 Communication Tests

The **FORCE** allows you to test each CMS defined communication path - telephone number, URL etc., by generating a Test report. During the test the display shows the online communication process - dialing, connecting, sending, etc.

13.6 Communications Monitor

Select any communication path and view the current data exchange.

Appendix A Implementing Partitions

FORCE allows defining up to 16 true partitions, whereby each can independently be in a different arming mode, i.e., Away, Home, or Disarmed.

A partition consists of several zones, and is normally a defined area, such as a building floor, a store or a compartment. Every partition can have its own subscriber ID no., user codes, keypads, peripherals, etc.

Partitions' event reporting is subject to the following:

Event	Reporting ID no.
Zone alarm	The ID no. of any partition that the zone is allocated to. If the zone is allocated to more than one partition, a separate report will be sent on each partition. If only partition's #1 ID no. is defined, any event will carry that no.
Arming/Disarming	The same as in zone alarm
Keypad alarm	The ID no. of any partition that the keypad is allocated to.
Non-zone Fault	Partition's #1

Zone, keypads, users, and contacts can be allocated to more than one partition. In such a case, the following will apply:

1. Arming a zone is subject to all the partitions that the zone is allocated to: it will only be armed when all its partitions are armed.
2. An armed zone becomes disarmed, as soon as one of the partitions it is allocated to is disarmed.
3. Arming and disarming via a keypad is subject to both the keypad and the user's partitioning. For example, if a user that is allocated to partitions 1, 3 & 5, enters its code in a keypad that is allocated to partitions 4, 5 & 7, only partition 5 will either be armed or disarmed.
4. A keypad can only display the status of and control the partitions it's allocated to. The *Armed* LED stays on only when ALL the keypad's partitions are armed, and flashes when only some partitions are armed.

Appendix B Remote Upload/Download

User Authorization

The parameter *Remote Up/Download* in the *Communication/General Settings* sets if connecting remotely via telephone/network requires a user approval (see page 35). See the **FORCE** User guide on how the user approves the connection¹².

Upload/Download is done using the Force Manager software. Connection is made possible only if the Up/download code matches and the communication module is not at fault.



Using the CMS lock code will always require the user to allow it by pressing on Technician permit.

B.1 Remote connection code

A 6-digit code that allows connecting and programming the **FORCE** (except CMS locked menus) remotely. You should change the default code on first connection using the Force Manager software (it cannot be done locally).

B.2 Connection options

Below are the options on the User menu *System Options/Communication Opt./Remote Service*:

Option	Description
Accept Phone Call	<p>The connection steps are as follows:</p> <ol style="list-style-type: none"> 1. The control panel enters <i>Standby Mode</i> (User Menu/System Options/Communication Opt./Remote Service/Accept Telephone Call). If <i>Remote Upload</i> is selected (under CMS & Communications/ Monitoring Stations/ <i>General Setting</i>), this step is not required. 2. The technician connects via the Force Manager and FORCE allows the connection 3. The technician enters the Master Technician Code and is granted access to the Technician menu. The Remote connection code must be changed on first connection. <p>If the technician does not have the Master Technician Code, it can define a new CMS (if not all were taken already) and set its parameters. When the Force Manager downloads data to the control panel, the CMS code becomes the Up/download code - on any future connection after entering this code the technician will be allowed to view and set the CMS menus (only).</p>

¹² Up to 5 minutes from approving the connection, the control panel picks up a call immediately, regardless of related parameter, such as number of rings.

Option	Description
Allow Cloud Service	<p>The connection steps are as follows:</p> <ol style="list-style-type: none"> 1. The control panel establishes a connection with PIMA cloud and the cloud assigns a one-time pairing code (the code will not be saved). 2. The control panel enters <i>Standby Mode</i> 3. The user submits the pairing code to the technician. The code is valid for a few minutes only. 4. The technician enters the code on the Force Manager and connects to the control panel
Connect by Phone/Network/GPRS	<p>The telephone number and IP address are set in the <i>Communication/Monitoring Stations/Telephone, Network, GSM/GPRS Settings</i> menus, in <i>Callback No./Callback Address</i> parameters.</p> <p>On all three matching User menus, the user can manually enter the number and address.</p>

Appendix C Programmable Output Types

Output Type	Activation	Deactivation ¹³	Timer			Partitioning	Default
			1-9998 (sec)	9999 (Follower)	0 (Latch) ¹⁴		
Alarms: Burglary, Panic, Silent panic, Fire, Medical, Duress, Anti-mask, Custom zone1-5	Alarm triggering	Time elapses or disarming	✓	⊘	✓	✓	240 sec
Faults: Any fault, AC, Low battery, Phone line/Network, GSM module, Communication, Tamper open	Fault occurrence	Time elapses or disarming	✓	✓	✓	⊘	9999
External siren	Siren triggered	Time elapses or disarming	✓	⊘	✓	✓	240 sec
Internal siren			✓	⊘	✓	✓	
Zone bypass ¹⁵	Bypassing any zone	Time elapses or disarming	✓	✓	✓	✓	9999
Smoke Detector Reset	Fire zone alarm or pressing and holding together the keys 7 & 9 on a keypad	Time elapses or pressing and holding the # key on a keypad	✓	⊘	⊘	✓	60 sec
Chime	Chime triggered	Time elapses	✓	⊘	⊘	✓	3 sec
Zone open	Opening (activating) any zone	Closing the last open zone	⊘	✓	⊘	✓	9999
Arming	Arming in any mode	Disarming					
Entering Technician code	Entering the code	Exiting Technician menu	⊘	✓	⊘	⊘	9999
Activation code1-8	Entering the code	Time elapses	✓	⊘	✓ ¹⁶	✓	5 sec

¹³ For non-follower timers

¹⁴ Latched, until system/partition disarming.

¹⁵ See more below the table.

¹⁶ Toggle mode

Output Type	Activation	Deactivation ¹³	Timer			Partitioning	Default
			1-9998 (sec)	9999 (Follower)	0 (Latch) ¹⁴		
Code keystrokes	<i>Code Keystrokes</i> counter exceeds limit	Time elapses	✓	⊖	✓	✓ ¹⁷	24 key-strokes

The *Zone Bypass* programmed output type timer has special triggering definitions, as follows:

1. 1-9998: the timer restarts each time a zone is bypassed
2. 9999: the output type is active, as long as there is a bypassed zone
3. 0: the output type is triggered when the first zone is bypassed and deactivates at disarm

¹⁷ Subject to the keypad's partitioning


Appendix D Technician and CMS codes

There are two technician codes in the **FORCE** security system: Master technician code, and CMS lock code, which allows limiting the access to the CMS menus by a password. Following is information on each code.

D.1 Master technician code

By default, and as long as no CMS lock code (see next) has been set, the Master technician code enables to access all the technician menus, including all the CMSs'.

To enter the technician menu for the first time, follow the next steps:

1. The user must grant you access by pressing on *Technician Permit (User menu/ Other Options)*.
2. Immediately enter the default Master technician code *1234*.
3. In the code menu, enter a new 4-6 digit Master technician code and press Enter .


D.2 CMS lock code

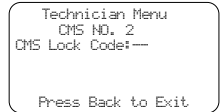
The CMS lock code ensures the CMS definitions from unauthorized access. Setting such a code prevents the Master technician code from accessing the locked CMS menus.



The CMS lock code is to be used, only when a technician needs to set the CMS definitions and doesn't have the Master technician code in hand.

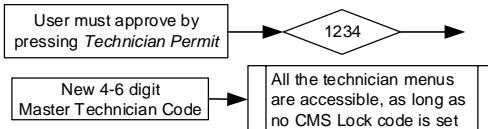
If you need to set the CMS definitions and you don't have the Master technician code, follow the next steps:

1. The user must grant you access via the *Technician Permit menu (User menu/Other Options)*.
2. Immediately enter the default Master technician code, *1234* - the next undefined CMS lock code screen is displayed¹⁸.
3. Enter a new 4-6 digit lock code.
4. Press the "Back"  button.

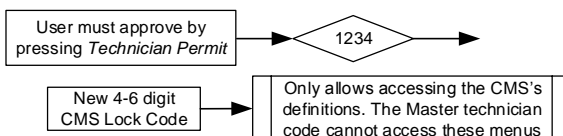


From now on, these CMS definitions are only accessed using the new lock code. Whenever there will be a need to change or view these CMS's definitions, the user will have to approve it, after pressing the *Technician Permit* menu. A technician that has the Master technician code, will not be able to view or change these definitions.

How to change the default Master Technician code:



How to set CMS Lock code:



¹⁸ Providing there is an available CMS menu

Appendix E Text and Characters

Text is entered like in a telephone set: each key is allocated with several characters; each keystroke presents a different character. For example, press 8 twice to type U.

The keystrokes and character table are described in the table and image that follow:

Key	Characters
1	1.,?!()/*:~+##@'
2	ABC/abc2
3	DEF/def3
4	GHI/ghi4
5	JKL/jkl5
6	MNO/mno6
7	PQRS/pqrs7
8	TUV/tuv8
9	WXYZ/wxyz9
0	Space, 0
#	Delete, return to default
*	Uppercase/lowercase/digits

1.,?!()/*:~+##@'	ABC2	DEF3
1	2	3
GHI4	JKL5	MNO6
4	5	6
PQRS7	TUV8	WXYZ9
7	8	9
Letter Case	Space, 0	
*	0	#

Appendix F CMS Event Reporting

Below is a table with a list of the events that are reported to the CMS and private users.

Event source/type	Reporting
Burglary zone	Alarm/Fault in <i>Burglary</i> or <i>Shock Sensor</i> zones
Panic zone	Alarm/Fault in <i>Panic/Silent Panic</i> zones or keypad <i>Panic</i> alarm
Fire zone	Alarm/Fault
Duress zone	Alarm/Fault
Medical zone	Alarm/Fault
Custom zone	Alarm/Fault
Tamper zones/switches, Anti-mask zone, External/Internal Siren, EOL supervised loops	Tamper Alarm
Restore report	Any zone that has alarmed
Zone Bypass report	Except zones that are not set to report on alarm
Faults	Fault+Restore: AC ¹⁹ , Voltage, Low Battery, Phone Line (low DC and dial tone), GSM add-on/GPRS+SIM, Fuse current, CMS communication.
Arming/Disarming	Appropriate report
Invalid code (after 24 keystrokes)	Appropriate report
Technician code	Appropriate report
Remote Testing	Appropriate report

¹⁹ When the report has a delay, if the fault doesn't exist by the time the delay elapses, no report is sent.

Appendix G Glossary

Cross Zones

A false alarm reduction feature: two cross zones will trigger the alarm (separately), only if both are activated during the *Cross Zones* time. If only one cross zone is activated no alarm will occur. If the second (or any other) cross zone is activated after the *Cross Zones* time expired, no alarm will occur.

Normally, cross zoning is used across nearby zones, especially zones on the exit/entry route.

Custom Zone Type

A zone type that can be fully or partly customized. Use these zones for special, non-standard zones such as flood or freeze ones.

Custom zones can report as any standard zone (Burglary, Panic, Medical, Etc.), but have different sensitivity and characteristics, or have custom reporting codes (set in *Custom Zones Report* menu).

Custom zone types with *Custom Type* reporting type can be utilized to trigger outputs for specific purposes, such as activating a pump.

Double Knock

A false alarm reduction feature: this zone will trigger the alarm, only if it activates twice during the *Double Knock* time. A *Double Knock* zone will also trigger the alarm if it's opened for the duration of the *Double Knock* time.

Energy Saving (Programmable Output Type)

The *Energy Saving* timer starts running when all the zones are closed and it runs as long as no movement is detected. It can be utilized (using a relay) to turn off lights and air-conditions, if the alarm system was armed but these appliances (or any other) were left on.

Roller Blinds

A special zone sensitivity, for use with roller blinds. This zone will trigger the alarm when it five times within two minutes, or activates once for five seconds. The zone restores after not being activated for five seconds.

Limited Warranty

PIMA Electronic Systems Ltd. does not represent that its Product may not be compromised and/or circumvented, or that the Product will prevent any death, personal and/or bodily injury and/or damage to property resulting from burglary, robbery, fire or otherwise, or that the Product will in all cases provide adequate warning or protection. The User understands that a properly installed and maintained equipment may only reduce the risk of events such as burglary, robbery, and fire without warning, but it is not insurance or a guarantee that such will not occur or that there will be no death, personal damage and/or damage to property as a result.

PIMA Electronic Systems Ltd. shall have no liability for any death, personal and/or bodily injury and/or damage to property or other loss whether direct, indirect, incidental, consequential or otherwise, based on a claim that the Product failed to function.

Please refer to a separate warranty statement found on PIMA website at: <http://www.pima-alarms.com/site/Content/t1.asp?pid=472&sid=57>

Warning: The user should follow the installation and operation instructions and among other things test the Product and the whole system at least once a week. For various reasons, including, but not limited to, changes in environment conditions, electric or electronic disruptions and tampering, the Product may not perform as expected. The user is advised to take all necessary precautions for his/her safety and the protection of his/her property.

This document may not be duplicated, circulated, altered, modified, translated, reduced to any form or otherwise changed unless PIMA's prior written consent is granted.

All efforts have been made to ensure that the content of this manual is accurate. Pima retains the right to modify this manual or any part thereof, from time to time, without serving any prior notice of such modification.

Please read this manual in its entirety before attempting to program or operate your system. Should you misunderstand any part of this guide, please contact the supplier or installer of this system.

Copyright © 2018 by PIMA Electronic Systems Ltd. All rights reserved. E&OE



Manufactured by:

PIMA Electronic Systems Ltd. **WWW.PIMA-ALARMS.COM**

5 Hatzoref Street, Holon 5885633, ISRAEL

Tel: +972.3.6506414 Fax: +972.3.5500442

Email: support@pima-alarms.com

P/N: 4410459



Revision: 01 (Beta), XX en, Jan 2018