PowerMaster-360R

Installer's Guide

V19.4

Table of Contents

1. Introduction

PowerMaster-360R is a regulated intrusion panel that combines Wi-Fi and Z-Wave radios for Smart Home automation applications. The PowerMaster-360R is a professional intrusion panel with battery backup for up to 12 hours. It also provides communication backup through a cellular 2G or 3G network. This backup provides protection even in the case of infrastructure failure. Property owners receive notifications of events by either email, SMS or both. It is based on the PowerG RF security technology with IP communication that is optimized for intrusion applications from an installation, security, robustness, and range perspective.

The PowerMaster-360R security system is fully controllable from a computer, and accessible to home and property owners through their mobile devices. Installers program and configure the system remotely through the computer and mobile application's keypad (see APPENDIX A and B).

This manual refers to PowerMaster-360R. The most updated manuals can be downloaded from the Visonic Web site at http://www.visonic.com.

The PowerMaster-360R control panel is supplied with 2 instruction manuals:

- **Installer's Guide** (this manual) – for use by the system installer during system installation and configuration
- **User's Guide** –for use by the system installer during system installation and configuration, and for the master user of the system, once installation is completed. Hand over this manual to the master user of the system.

1.1 System features

The following table lists the PowerMaster-360R features with a description of each feature and how to use it.

Feature	Description	How to configure and use
Visual alarm verification	When used with Next CAM PG2 PIR-camera detector, or TOWER CAM PG2, and GPRS or Ethernet communication, the PowerMaster-360R is able to provide the Monitoring Station with clips captured in alarm situations. The system sends the clips to the Monitoring Station automatically for burglary alarms and, depending on setup, also for fire and personal emergency alarms.	**1. Setup GPRS communication:** see GSM Module Installation (section 3.4). **2. Configure camera settings:** refer to the Next CAM PG2 Installation Instructions. **3. Enable fire and personal alarm verification:** see section 4.6.5 Configuring Motion Cameras for Video Alarm Verification.
On demand clips from cameras	The PowerMaster-360R can provide images from the Next CAM PG2 or TOWER CAM PG2 by demand from a remote PowerManage server. Pictures are taken based on a command from the monitoring station via the VisonicGo application. To protect customers' privacy, the system can be customized to enable the **On Demand View** only during specific system modes (i.e. Disarm, Home & Away) and also to a specific time window following an alarm event.	**1. Setup the On demand feature:** see section 4.6.5 Configuring Motion Cameras for Video Alarm Verification. **2. To request and view images:** refer to the PowerManage User's Guide, Chapter 5 Viewing and Handling Events.
Easy enrollment	PowerG devices are enrolled from the control panel's Virtual or Touch Keypad. Pre-enrollment can also be performed by entering the PowerG device ID number and then activating the device in the vicinity of the panel.	**To enroll or pre-enroll devices:** see section 4.4.2 Adding New Wireless Devices.
Device configuration	Device parameters and related system behavior can be configured from the control panel or from a remote location. Each PowerG device has its own settings which can be configured through the control panel by entering the DEVICE SETTINGS menu. ***Note:*** *The minimum configuration of the system includes one detector.*	**To configure devices from the control panel:** see Chapter 4 Programming and also the individual device's Installation Instructions. **To configure devices from a remote location:** refer to the PowerManage User's Guide Chapter 3 Working with Panels and to the Remote Programmer PC software User's Guide, Chapters 6 and 7.
Diagnostics of the control panel and peripherals	You can test the function of all wireless sensors deployed throughout the protected area, to collect information about the received signal strength from each transmitter and to review accumulated data after the test.	**To perform diagnostics and to obtain signal strength indication:** see section 4.9 Diagnostics.
Conducting periodic tests	The system should be tested at least once a week and after an alarm. The periodic test can be conducted locally or from a remote location (with the assistance from a non-technical person in the house).	**To conduct a walk test locally**: see Chapter 5 Periodic Test. **To conduct a walk test from remote location:** refer to the Remote Programmer PC software User's Guide, Chapter 6 Data Details Tables.

Partitions	The partitioning feature, when enabled, divides your alarm system into distinct areas each of which operates as an individual alarm system. Partitioning can be used in installations where shared security systems are more practical, such as a home office or warehouse building.	**1. Enable partitioning:** see section 4.12 Partitioning. **2. Setup partition association for each device:** see section 4.4.2 Adding New Wireless Devices. **To understand more about partitioning:** see APPENDIX E. Working with Partitions and APPENDIX B. in the User's Guide.
Device configuration templates	The default parameters with which a new device is enrolled into the system can be set before you enroll devices. This default template saves time on device configuration.	**1. Define enrollment defaults for devices:** see section 4.4.7 Defining Configuration Defaults for Device Settings. **2. Enroll or pre-enroll devices:** see section 4.4.2 Adding New Wireless Devices.
SirenNet - distributed siren using Smoke detectors	All PowerG smoke detectors are able to function as sirens, alerting on any of 4 types of alarm in the system: fire, gas, burglary and flood.	**Enable and configure SirenNet for each smoke detector:** refer to the SMD-426 PG2 / SMD-427 PG2 Installation Instructions.
Reporting to private users and/or monitoring station by SMS and IP communication	The PowerMaster-360R system can be programmed to send notifications of alarm and other events to 4 SMS cellular phone numbers and to report these events to the Monitoring Station by SMS or IP communication. Users can also receive notifications on the Visonic-Go application.	**To configure notifications to Private phones:** refer to the PowerMaster-360R User's Guide, Chapter 4, section B.12 Programming Email, MMS and SMS Reporting. **To configure reporting to the Monitoring Station:** see section 4.6.3 Configuring Events Reporting to Monitoring Stations.
Quick installation with link quality indication	With PowerG devices, there is no need to consult the control panel when mounting a wireless device, because PowerG devices include a built-in link quality indicator. Choosing the mounting location is a quick and easy process.	To choose the ideal location to mount a wireless device, see Chapter 2 Choosing the Installation Location.
Device locator	Helps you to easily identify the actual device displayed on the LCD display.	**To read more on the Device Locator:** refer to the PowerMaster-360R User's Guide, Chapter 2, Operating the PowerMaster-360R System. **To use the device locator when bypassing a zone or when clearing a bypassed zone:** refer to the PowerMaster-360R User's Guide, Chapter 4, section B.1 Setting the Zone Bypass Scheme. **To use the device locator when conducting the periodic test:** see Chapter 5 Periodic Test or refer to the PowerMaster-360R G2 User's Guide, Chapter 7 Testing the System.
Guard key-safe	PowerMaster is able to control a safe that holds site keys that are accessible only to the site's guard or Monitoring Station's guard in the event of an alarm. Operates with the magnetic contact device with auxiliary input only (MC-302E PG2)	**1. Configure the safe's zone type to Guard Zone:** see section 4.4.2 Adding New Wireless Devices. **2. Setup guard code:** see section 4.3 Setting Installer Codes.
Arming key	External system may control arming and disarming of the PowerMaster system.	Refer to the MC-302 PG2 / MC-302E PG2 / MC-302V PG2 Installation Instructions.

2. Choosing the installation location

To ensure the best mounting location for the PowerMaster-360 control panel, the following points should be observed when selecting a location:

- Place approximately in the center of the installation site between all the transmitters, preferably in a hidden location.
- Place in close proximity to an AC source.
- Place where there is good cellular coverage, if a cellular module is used.
- Place in close proximity to a home router wired Ethernet (LAN) connections.
- Place far from sources of wireless interference, such as the following:
  - Computers or other electronic devices, power conductors, cordless phones, light dimmers, etc.
  - Large metal objects (such as metal doors or refrigerators)

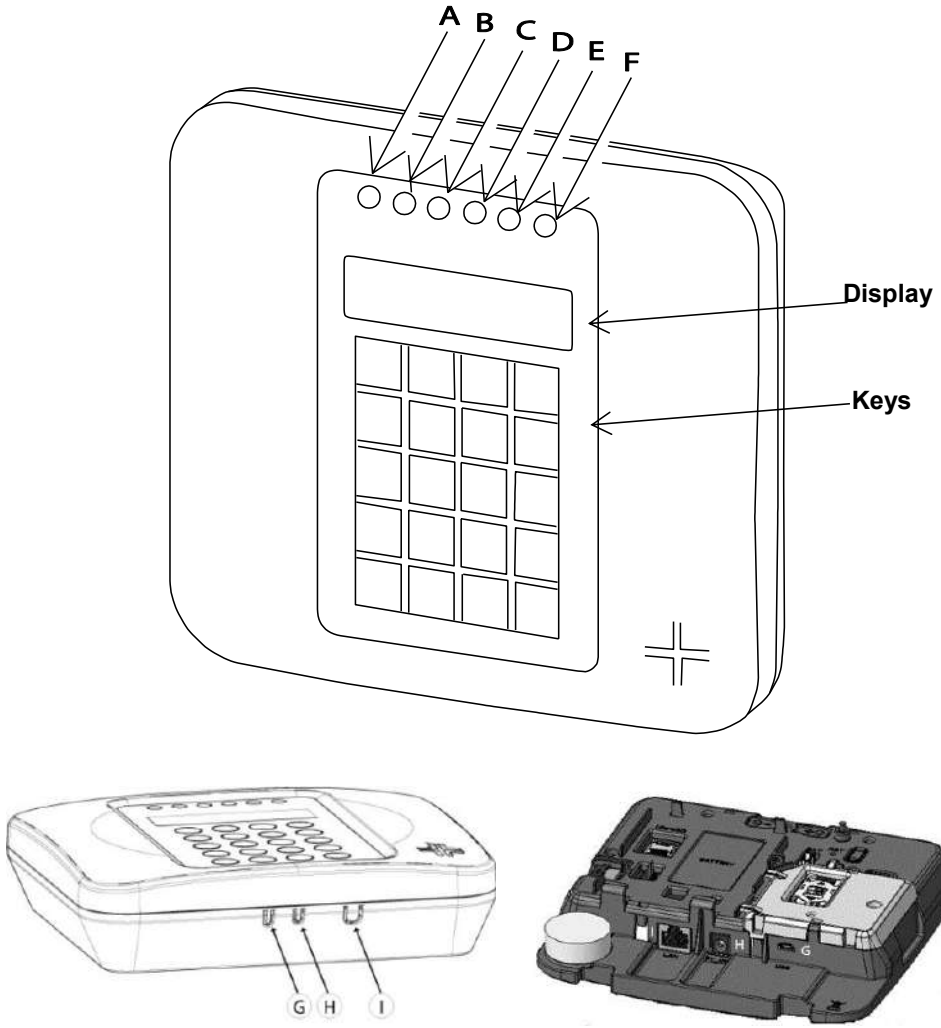
    Note: *A distance of at least 1 meter (3 ft.) is recommended.*

When mounting wireless devices, ensure that the following conditions are in place:

- Ensure the signal reception level for each device is either **Strong** or **Good**, but not **Poor**.
- Install wireless magnetic contacts in a vertical position and as high up the door or window as possible.
- Install wireless PIR detectors upright at the height specified in the relevant installation manual.
- Locate repeaters high on the wall mid-distance between the transmitters and the control panel.

3. Installation

3.1 LED indicators and connections



External view of cable outputs

Internal cable connections

A. Power indicator

B. Status indicator

C. Trouble condition (TRBL) indicator

D. Service server indicator

E. Smart Home Service Indicator

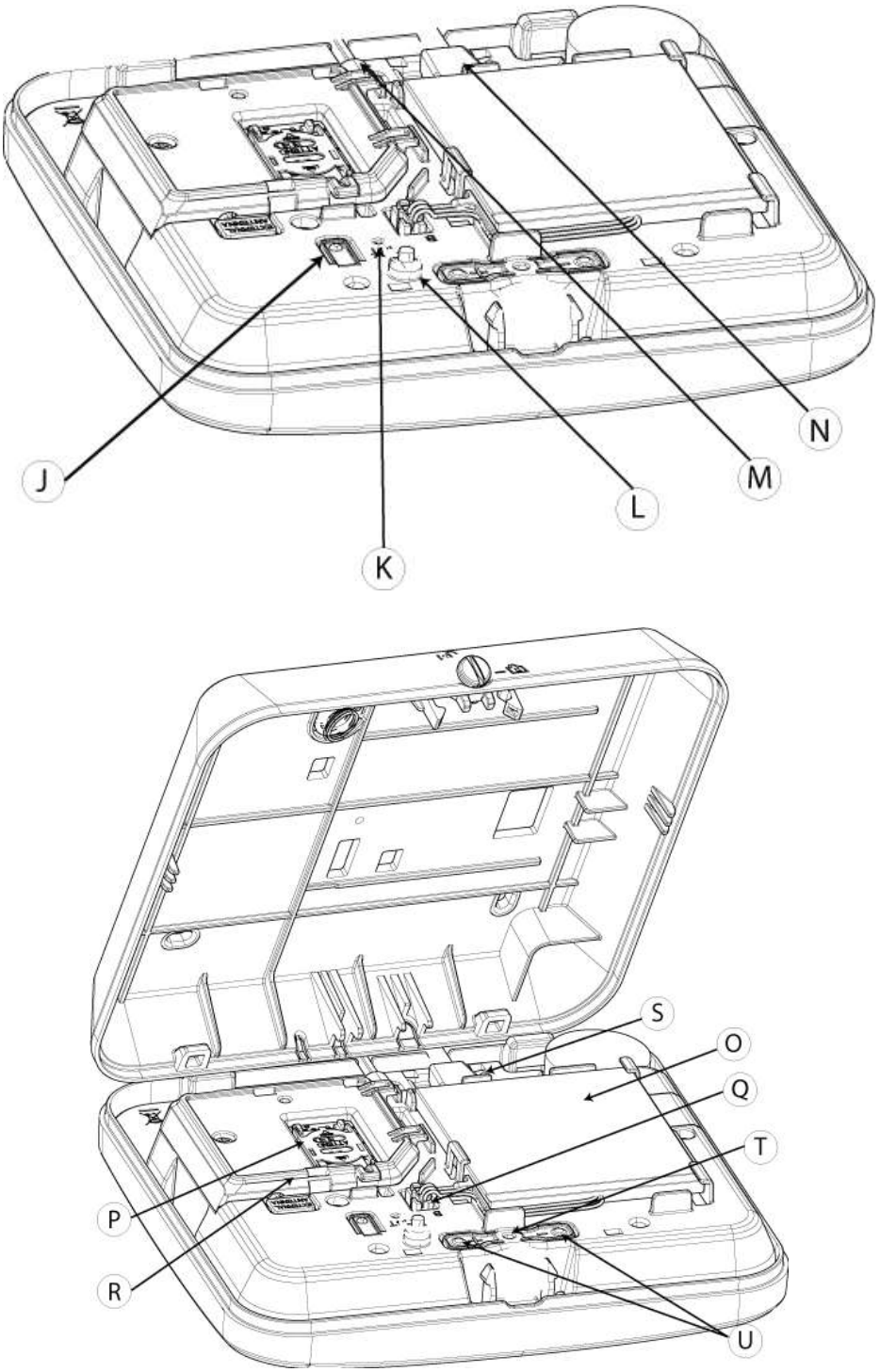
F. WiFi indicator

G. Micro USB connection

H. 5V DC power connection

I. LAN connection

Figure 3.1 a – LED indicators and connections



J. Restore to factory default settings. Press for 30 seconds to restore system parameters to preset factory defaults.

K. Opening for reset button

L. Tamper switch

M. Power cable

N. LAN cable

O. Rechargeable battery

P. SIM card holder

Q. Battery plug socket

R. GSM module

S. Electronic unit

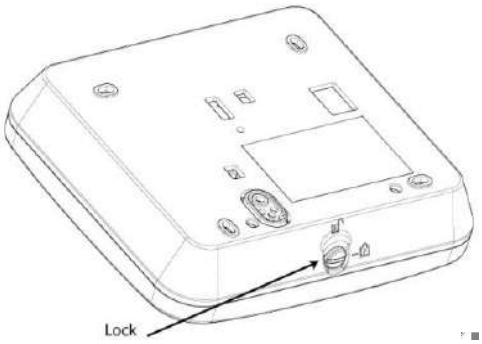
T. Enroll LED

U. (**+**) button Add Z-Wave devices

(**-**) button Delete Z-Wave devices

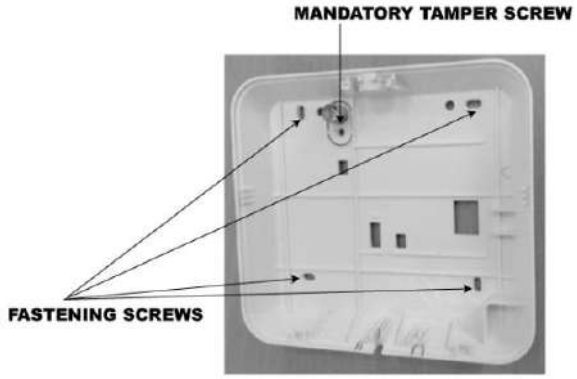
Figure 3.1 b – Internal panel view

3.2 Installing the PowerMaster-360R battery and cables



1) To open the panel, use a coin or 3 mm flathead screwdriver to rotate the lock by 90 degrees counter clockwise to the unlocked position.

2) Use minimal force to pull the panel from the base.



3) Use the screws and anchors provided to fasten the base to the wall.
Warning: *The tamper screw is mandatory; use the remaining screws to secure the base.*

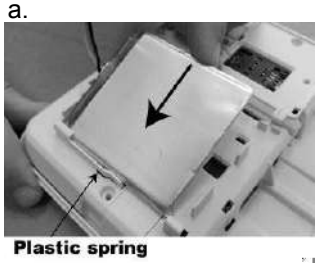
4) To install the battery in the panel, complete the following steps:

a) To prevent mechanical damage, insert the battery carefully into the slot in the direction of the arrow, see figure (a) for details.

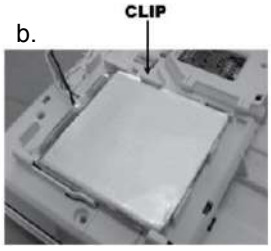
b) Press downwards and place under the clip, see figure (b) for details.

c) Run the wire along the channel and connect the battery cable plug into the battery socket, see figure (c) for details.

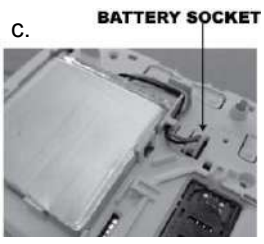
a.

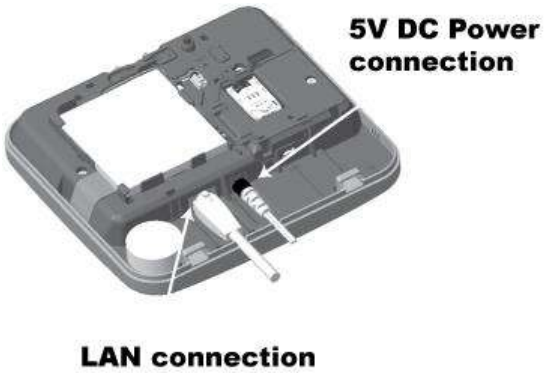


b.



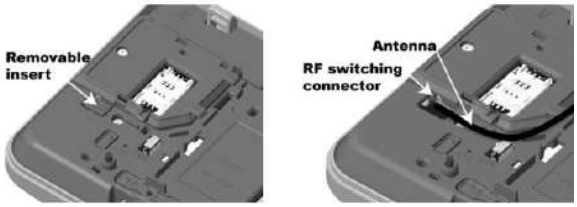
c.





5) Connect the AC/DC adapter cable to the panel.

6) Connect the IP LAN cable to the panel.

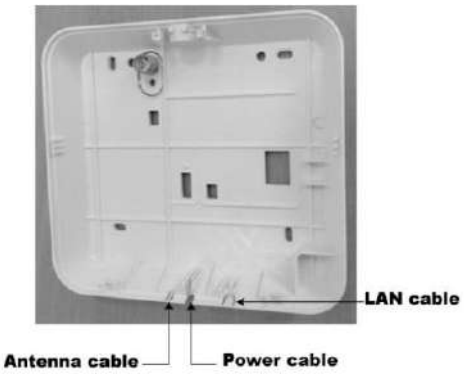


a. b.

7) Optional: To connect an external GSM antenna, complete the following steps:

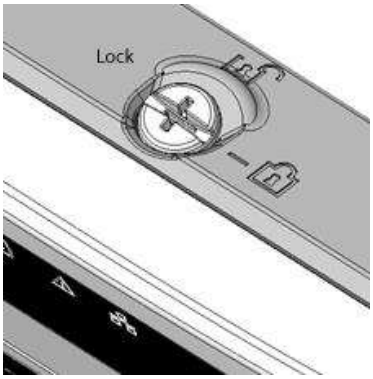
a) Push out the removable insert for the external antenna, see figure (a) for details.

b) Connect the external antenna to the RF switching connector, see figure (b) for details.



8) Push out the appropriate knockout for the cables that are connected to the panel.

9) To place the panel on the base, align the two tabs of the base with the slots on the panel.



10) Close and hold the panel to the base.

11) Rotate the lock by 90 degrees clockwise to the locked position.

3.4 PowerMaster-360R connections

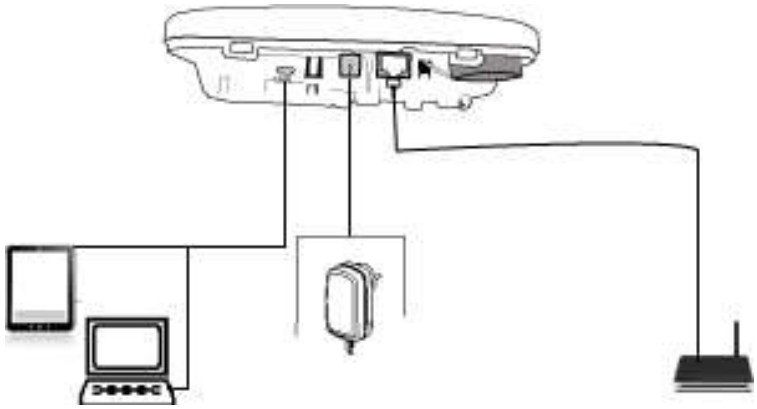


Figure 3.2 PowerMaster-360R connections

Note: *If there is a GSM module in your control panel, first connect the SIM card before performing the following procedure – see section 3.5 for details.*

1. *Rotate the lock anti-clockwise to the unlocked position with a coin or flathead screwdriver. Remove the panel from the base to access the ports – see section 3.2 step 1 for details.*
2. *Connect the IP cable from the LAN connection to the local home-router connection – see section 3.2 step 6 for details.*
3. *Connect the AC/DC adapter cable into the main electrical socket.*
4. *Optional: To use the software configurator, connect the micro USB cable from the micro USB connection to the PC, laptop, or tablet connection.*
   - *When the configurator setup is complete, disconnect the micro USB cable from the PowerMaster-360R.*
5. *Place the panel back on the base, align the two tabs on the base with the slots on the panel and return the screw to the locked position.*

Note: *For details about installing and configuring the virtual keypad software, see APPENDIX A PC configurator and APPENDIX B VisonicPRO.*

3.5 GSM connection and configuration

The GSM modem auto detection feature enables automatic enrollment of the GSM modem into the control panel memory. GSM modem auto detection is activated after reset that is after power-up or after exiting the Installer Mode menu. This action causes the PowerMaster-360R to automatically scan the GSM COM ports for the presence of a GSM modem.

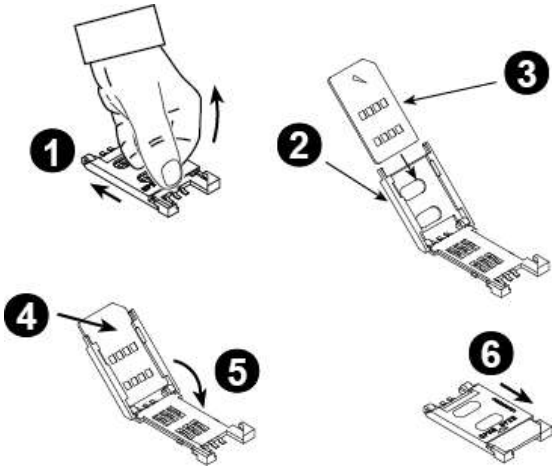
In the event that the GSM modem auto detection fails and the modem was previously enrolled in the control panel, the message **Cel Remvd Cnfrm** is displayed on the Configurator's Virtual or Touch Keypad. This message disappears from the display after you press **OK**. The modem is then considered as not enrolled and no GSM trouble messages are displayed.

Notes:

1) A message is displayed only when the alarm system is disarmed.

2) The GSM Alarm Transmission System is designed to comply with EN 50131-1 DP4.

3.6 SIM card insertion



The following procedure outlines how to insert SIM card into the GSM module, see Figure 3.1 (P):

1. Slide the top cover.
2. Open the cover.
3. Align the SIM card in the cover (note cover orientation).
4. Slide the SIM card into the cover.
5. Rotate the cover to close.
6. Lock the cover to close.

CAUTION! Do not insert or remove the SIM card when the control panel is powered by AC power or battery.

To configure the GSM modem, see section 4.6.2.

3.7 PowerMaster-360R Prerequisites

Connection to the PowerManage server requires the following ports to be open on the router to access the internet:

- TCP ports : 8080, 5001
- UDP port: 5001
- FTP port: 21

Note: *In a typical setup these ports on the router are open.*

The Configurator supports Windows 7 PC Operating System.

3.8 Enrolling and deleting a Z-Wave device

Enrolling a Z-Wave device

To enroll a device, complete the following steps:

1. Press and hold the (+) button (**U** in Figure 3.1) for 2 seconds. The red LED (**T** in Figure 3.1) blinks slowly.

2. Press the **Enroll** button on the device.

3. If Enroll is successful, the green LED blinks quickly, a success beep is heard, and the LED turns off.

Notes:

- *To cancel the enrollment, press and hold the (+) or (-) buttons for 2 seconds. The LED stops blinking.*
- *If enroll is not successful, the red LED lights constantly for 3 seconds and a failure beep is emitted.*
- *Long press on the **(+)** button, returns the panel to normal operation.*

Deleting a Z-Wave device

To delete an enrolled device, press and hold the (-) button (**U** in Figure 3.1) for 2 seconds. The red LED (**T** in Figure 3.1) blinks quickly, a success beep is emitted, and the LED turns off.

Notes:

- *To cancel the deletion, press and hold the (+) or (-) buttons for 2 seconds. The LED stops blinking.*
- *If the deletion is not successful, the red LED lights for 3 seconds and a failure beep is emitted.*
- *To return the panel to normal operation, long press on the (-) button.*

3.9 Panel reset

To reset the panel, use a blunt instrument to press the reset button (**K** in Figure 3.1), or, alternatively, exit the Installer Mode. The Orange LED (**T** in Figure 3.1) lights constantly until panel initialization is complete. When the PowerLink is reset, the Orange LED (**T**) turns off.

3.10 Factory default restore

To restore system parameters to the factory default parameters, complete the following steps:

Note: The panel must be disarmed before performing the reset.

1. Press the Back to Factory button (**J** in Figure 3.1) for 30 seconds.

Note: *During Back to Factory, the red LED (**T** in Figure 3.1) blinks.*

2. If Back to Factory is successful the green LED blinks 3 time, a success beep sounds, and the panel immediately initiates software reset.

Note: *If the Back to Factory procedure fails, the red LED lights constantly for 3 seconds and a failure beep sounds.*

4. Programming

4.1 General guidance

This chapter explains the installer programming configuration options of your PowerMaster-360R system and how to customize its operation to your particular needs and end user requirements.

Software configuration of the alarm system is performed using the Virtual or Touch Keypad, which contain the control keys, numerical keypad and display. The panel includes an intrusion sounder with a Piezo sounder.

The control panel includes a partition feature. Partitioning allows you to have up to three independently controllable areas with different user codes assigned to each partition. You can arm or disarm a partition regardless of the status of the other partitions within the system.

You can use the Soak Test feature to test selected zones for a pre-defined period of time. If you activate a zone in Soak Test mode, it does not initiate an alarm, siren or strobe. The zone activation is recorded in the event log and is not reported to the Monitoring Station. The zone remains in Soak Test mode until the pre-defined period of time for the Soak Test elapses without any alarm activation. The zone then automatically removes itself from Soak Test mode and returns to normal operating mode.

Software Upgrade allows you to upgrade the software of the control panel from the remote PowerManage server. During a software upgrade, **UPGRADING…** appears on the PowerMaster-360R keypad.

Note: *A software upgrade is delayed if the control panel is armed to* ***AWAY*** *or if an AC failure occurs. To continue with the upgrade either disarm the panel, restore the AC power or both.*

Tech Tip :

For your convenience, program the PowerMaster-360R on a work bench before the installation. You can obtain operating power from the backup battery or from the AC/DC adapter.

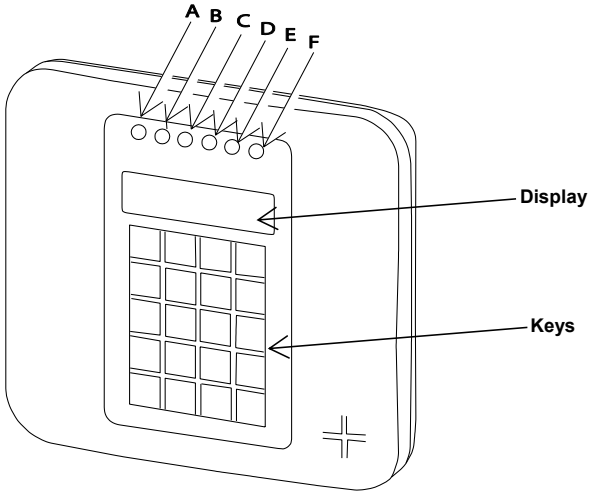
ATTENTION! FIRST SWITCH ON THE CONTROL PANEL and then INSERT BATTERIES INTO ACCESSORIES DEVICES.

The devices search for the control panel to which they are enrolled for a period of 24 hours only after you insert the battery.

Note: *If you switch on the control panel a long time after inserting batteries into the accessories devices you must open and then close the cover of the PowerMaster-360R to activate the tamper switch. Alternatively, remove and reinsert the battery into the device.*

4.1.1 PowerMaster-360R panel indicators and controls

LED indicators



No.	Function
Ⓐ	**Power** ⏻ **(Green)** indicates that your system is connected to the power outlet.
Ⓑ	**Arming Status** 🔒 **(Flashing Red / Static Red)** indicates HOME / AWAY.

No.	Function
Ⓒ	**Trouble condition (TRBL)** **(Orange)** lights when the system detects an abnormal condition caused by a fault, see Chapter 3 for details.
Ⓓ	**Service Server** **(Blue)** lights when the system is connected to the security server.
Ⓔ	**Smart Home Service** **(Blue)** lights when the system is connected to the smart home server.
Ⓕ	**WiFi** **(Green)** indicates if the WiFi module is enabled or disabled. The light blinks fast when activating or deactivating a WiFi access point and blinks slowly when the WiFi access point is active.

Control keys

When you program the panel you can use the keypad's buttons for navigation and configuration. The following table provides each key definition and its use:

Key	Definition	Navigation and use
	Next	Move forward to the next menu option.
	Back	Move backward to the previous menu option.
	OK	Select a menu option or confirm a setting or action.
	Fire alarm	Configure a fire alarm.
	Volume Up	Increase volume.
	Arm away	Arm building when empty.
	Volume down	Decrease volume.
	Arm home	Arm building when occupied.
	Chime	Turn on or off chime.
	OFF	Disarm system.
	Event log	Review the event log.
	Cancel entry delay	Cancel entry delay when system is armed to home or away.
	Partition	Select a partition.
	Emergency alarm	Configure an emergency alarm.
0 – 9	N/A	Enter numerical data, where applicable.

To review the options within the control panel menus and select an option, repeatedly press the Next or Back until the desired option displays (also designated as in this guide), then press the OK to select the desired option (also designated as OK in this guide). To return to the previous options, repeatedly press the Home . To exit the programming menu, press Away .

4.1.2 Feedback sounds

The panel or PC provides the following audible indicators when configuring the panel:

Sound	Definition
♩	Single beep indicates that a key is pressed.
♩ ♩	Double beep indicates a return to the normal operating mode after a timeout.
♩ ♩ ♩	Three beeps indicate an abnormal condition in the system due to a fault.
♫	**Success Tune** (- - - ——), indicates the successful completion of an operation.
♫	**Failure Tune** (———), indicates an incorrect option or the value that is not accepted.

4.2 Entering installer mode and selecting a menu option

All **installer mode** options are accessed from the **installer mode** menu option.

To enter and select an option from the Installer Mode menu, complete the following steps:

Step 1 ⓘ	Step 2 ⓘ	Step 3 ⓘ				Step 4
Select **Installer Mode** Option [1]	Enter Installer Code [2]	Select Installer Mode menu option [3]				
▶▶		▶▶	See	▶▶	See	
READY 00:00		**01:INSTALL CODES**	4.3	**08:USER SETTINGS**	4.10	
↓		**02:ZONES/DEVICES**	4.4	**09:FACTORY DEFLT**	4.11	
INSTALLER MODE OK	**ENTER CODE:■**	**03:CONTROL PANEL**	4.5	**10:SERIAL NUMBER**	4.12	
If the **Installer Mode** is not shown, refer to section 4.2.1		**04:COMMUNICATION**	4.6	**12:PARTITIONING**	4.13	OK Go to the indicated section of the selected option
		06:CUSTOM NAMES	4.8	**13:OPERATION MOD**	4.14	
		07:DIAGNOSTICS	4.9	**<OK> TO EXIT**		

ⓘ	ⓘ *- Entering the Installer Mode menu*
[1]	You can access the **Installer Mode** only when the system is disarmed. The process described refers to the case where a **User permit** is not required. If a **User permit** is required, select the **User Settings** option and ask the Master User to enter his code and then scroll to the **User Settings** menu and select the **Installer Mode** option (last option in the menu). Continue to Step 2.
[2]	If you have not already changed your Installer code number, use the default settings: 8888 for installer & 9999 for master installer. If you enter an invalid installer code 3 - 5 times, the keypad is automatically disabled for a pre-defined period of time and the message **WRONG PASSWORD** is displayed.
[3]	You have now entered the **Installer Mode menu**. Scroll and select the menu you require and see the relevant section in the guide, the section is indicated on the right side of each option.

4.2.1 Entering the installer mode when User Permit is enabled

In certain countries the regulations may require that the user grants permission to make changes to the panel configuration. To comply with these regulations, the **Installer Mode** option can be accesses only from the **User Settings** menu. The Master user must first enter the **User Settings** menu and scroll until the **Installer Mode** option is shown and then the installer can continue as shown in the above table (see also ⓘ [1] in Step 1 above).

To configure the panel to comply with **user permission** requirements - see option #91 **User Permit** in section 4.5.8.

4.2.2 Selecting options

ⓘ	ⓘ – *Selecting an option from a menu*
	Example: To Select an Option from the COMMUNICATION menu:
[1]	Enter the **Installer Mode menu** and select the **04.COMMUNICATION** option (see section 4.2).
[2]	Select the sub-menu option you need, for example: **3: C.S. REPORTING**.
[3]	Select the parameter you wish to configure for example: **11:RCVR 1 ACCOUNT**
[4]	To continue, go to the section of the selected sub-menu option, for example section 4.6.3 for the **3:C.S.REPORTING** menu. Then look for the sub-menu you wish to configure for example, **11:RCVR 1 ACCOUNT**. After configuring the selected parameter the display returns to step 3.
	To Change the Configuration of the Selected Option:
	When entering the selected option, the display shows the default (or the previously selected) **setting** marked with ■.
	To change the configuration, scroll ▶▶ the Options menu and select the setting you wish and press OK to confirm. When done, the display reverts to Step 3.

4.2.3 Exiting the installer mode

To exit the Installer Mode, proceed as follows:

Step 1	ⓘ	Step 2	ⓘ	Step 3	ⓘ
	[1]		[2]		[3]
Any screen	[⌂] or [🔓]	**<OK> TO EXIT**	OK	**READY 12:00**	

ⓘ	ⓘ – *Exiting the Installer Mode*
[1]	To exit **INSTALLER MODE**, move up the menu by pressing the [⌂] button repeatedly until the display reads **<OK> TO EXIT** or press the [🔓] button once which brings you immediately to the exit screen **<OK> TO EXIT**.
[2]	When the display reads **<OK> TO EXIT**, press [i OK].
[3]	The system exits the **INSTALLER MODE** menu and returns to the normal disarm state while showing the READY display.

4.3 Setting installer codes

The PowerMaster-360R system provides two installer permission levels with separate installer codes, as follows:

- **Master Installer:** The Master Installer is authorized to access all Installer Mode menu and sub-menu options. The default code is: 9999 (*).
- **Installer:** The Installer is authorized to access most but not all Installer Mode menu and sub-menu options. The default code is 8888 (*).
- **Guard Code:** Enables an authorized guard to only Arm Away / Disarm the control panel. The default code is 0000 (*).

The following actions require you to enter the **Master Installer code**:

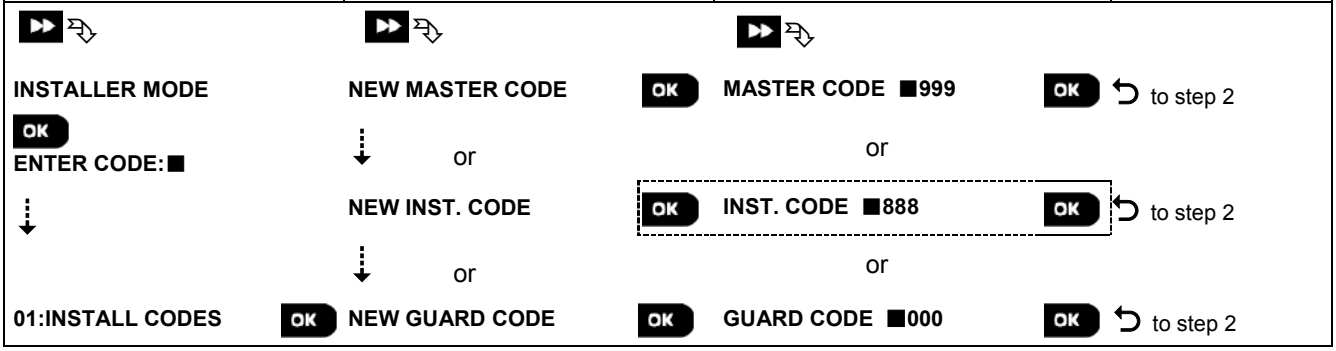
- Changing the Master Installer code.
- Defining specific communication parameters – see **3:C.S REPORTING** in section 4.6.2 and 4.6.3.
- Resetting the PowerMaster-360R parameters to the default parameters – see **09:FACTORY DEFLT** in section 4.11.

Note: *Not every system includes a* ***Master Installer code*** *feature. In such systems, the* ***Installer*** *can access all Installer Mode menu and sub-menu options identical to the Master Installer.*

(*) You are expected to use the default codes only once for gaining initial access, and replace it with a secret code known only to yourself.

To change your Master Installer or Installer Codes proceed as follows:

Step 1	ⓘ	Step 2	ⓘ	Step 3	ⓘ	Step 4
Select 01:INSTALL CODES Option	[1]	Select **Master Installer, Installer** code or **Guard** code	[2]	Enter NEW **Master Installer, Installer** code or **Guard** code	[3]	



ⓘ	ⓘ *– Setting Installer Codes*
[1]	Enter the **Installer Mode menu** and select the **01:INSTALL CODES** option (see section 4.2).
[2]	Select the **NEW MASTER CODE**, **NEW INST. CODE** or **NEW GUARD CODE**. Some panels may have only the Installer Code and New Guard Code option.
[3]	Enter the new 4-digit Code at the position of the blinking cursor and then press ⓘ | OK.

Notes:

1. *Code **0000** is not valid for Master Installer or installer.*
2. *Inserting **0000** for the Installer will delete the Installer Code.*
3. ***Warning!** Always use different codes for the Master Installer, for the Installer and for the Users. If the Master Installer Code is identical to the Installer code, the panel will not be able to recognize the Master Installer. In such a case, you must change the Installer code to a different code. This will re-validate the Master Installer code.*

4.3.1 Identical installer and master installer codes

In a 2-installer code system, the non-master installer may inadvertently change the Installer Code to that of the Master Installer Code. In this case, the panel will allow the change in order to prevent the non-master installer from realizing the discovery of the Master Installer's Code. The next time the Master Installer enters the Installer Mode, the Master Installer will be considered an Installer and not a Master Installer. In this case, the Master Installer should use one of the following solutions:

1. Access the panel using the Remote Programmer PC software application and change the Master Installer Code to a different code than the one programmed by the Installer.
2. Change the Installer Code to a temporary code exit the Installer Mode as follows:
   a. Enter the Installer Mode again using the Master Installer code (the Master Installer Code will now be accepted).
   b. Change the Master Installer code to a different code.
   c. Change the NON-Master Installer Code back again (that is, undo the change to the temporary code) so that the NON-Master Installer can still enter the system.

4.4 Zones and devices

4.4.1 General guidance & ZONES/DEVICES menu options

From the ZONES/DEVICES menu you can add, configure, and delete devices.

To select an option follow the instructions below. See section 4.2 for more information.

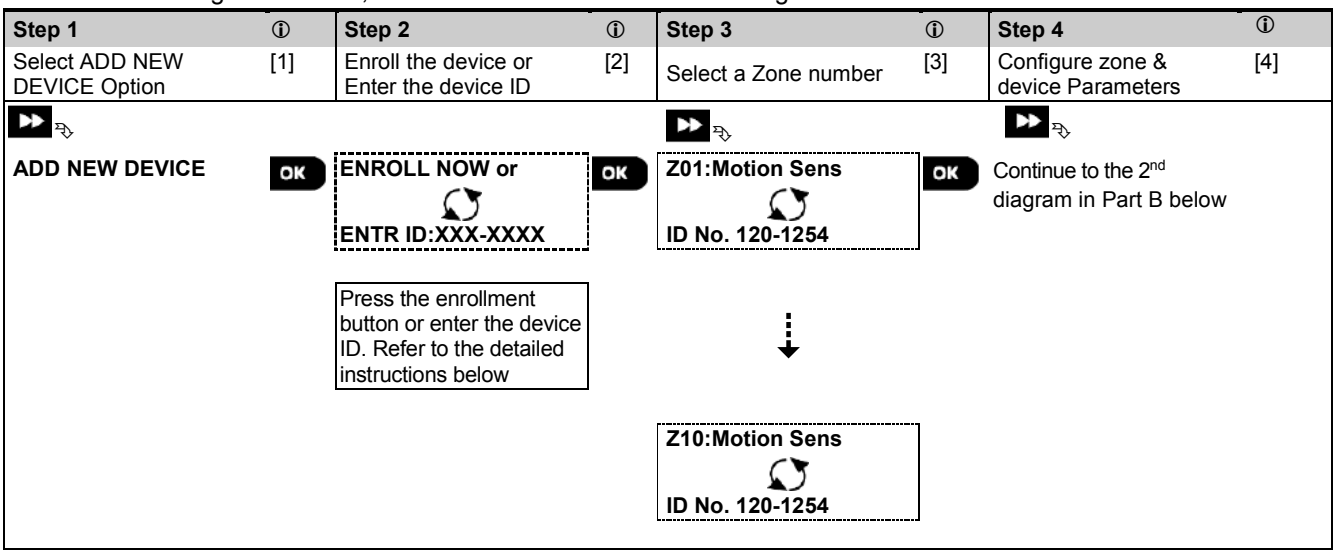
INSTALLER MODE ⇨ **02:ZONES/DEVICES** ⇨ **MENU**	⇨ indicates scroll ▶▶ and select OK

Option	Use	Section
ADD NEW DEVICES	To **enroll** and **configure** the device's operation according to your preference and in the case of sensors to also define their zone name (location), zone type and chime operation.	4.4.2
DELETE DEVICES	To **delete** devices from the system and to reset their configuration.	4.4.3
MODIFY DEVICES	To **review** and/or **change** the device's configuration.	4.4.4
REPLACE DEVICES	To **replace** faulty devices with automatic configuration of the new device.	4.4.5
ADD TO SOAK TEST	To **enable** the Soak Test for device zones.	4.4.6
DEFINE DEFAULTS	To **customize** the defaults of the device's parameters according to your personal preferences for each new device enrolled in the system.	4.4.7

4.4.2 Adding new wireless devices

Part A – Enrollment

To enroll and configure a device, follow the instructions in the following chart:



ⓘ	ⓘ *- Adding New Devices*
[1]	Enter **INSTALLER MODE**, select **02:ZONES DEVICES** (see section 4.2) . Select **ADD NEW DEVICE**. Because of encryption, PowerG devices (including Keyfobs) cannot be used on more than one system at one time. Remember to verify panel and device compatibility.
[2]	See enrollment by button or device ID below. If enrollment is successful, the display reads **DEVICE ENROLLED** (or **ID ACCEPTED**) and then shows the device details - see [3]. However, if the enrollment fails, the display will advise you the reason for failure, for example: **ALREADY ENROLLED** or **NO FREE LOCATION**. If the enrolled device is adapted to operate as another device that the panel recognizes, the display then reads **ADAPTED TO <OK>**.
[3]	The display shows the device details and the first available free Zone number for example: **Z01:Motion Sensor** > **ID No. 120-1254** (*or* **K01:Keyfob** / **S01:Siren** etc. depending on the type of the enrolled device). Detectors can be enrolled in any zone number. To change the zone number, click the ▶▶ button or type in the zone number, and then press ⓘ | OK to confirm.
[4]	Continue to Part B to configure the device – see diagram below

Checking panel to device compatibility

Each PowerG device bears a 7-character Customer ID printed on the device sticker in the format: FFF-M:DDD, (for example, 868-0:012) where FFF is the frequency band and M:DDD is the variant code.

For PowerG system devices compatibility, make sure the frequency band (FFF) and the variant code (M) of the devices match. The DDD can be ignored if the panel displays **ANY** for DDD.

Enrollment using device ID

The 7-digit Device ID can be used to register a device into the panel locally or from a remote location using the Remote Programmer PC software. The enrollment by device ID is a 2 stage procedure.

In the 1st stage you register the devices' ID numbers into the panel and complete the device configuration. This can be done from a remote location using the Remote Programmer PC software. Following the 1st stage, thePowerMaster-360R panel waits for the device to appear on the network in order to complete the enrollment.

In the 2nd stage, the enrollment is completed when the panel is in full working mode by inserting the battery into the device, or by pressing the tamper or enrollment button on the device. This procedure is very useful for adding devices to existing systems without the need to provide technicians with the Installer Code, or to allow access to the programming menus.

Notes:

1. *The system will display **NOT NETWORKD** until the 2nd stage of all registered devices is completed.*
2. *The Soak Test on pre-enrolled zones can be activated only when the zone is fully enrolled.*

Enrollment using the Enrollment button

The panel is set to the Enrollment mode (step #2 above) and the device is enrolled using the Enroll button (refer to the device information in the device Installation Instructions, then open the device and identify the **Enroll button**). For keyfobs and keypads, use the **AUX '✱'** button. For gas detectors, **insert the battery**.

Press the enroll button for 2-5 seconds until the LED lights steadily and then release the button. The LED will extinguish or may blink for a few more seconds until the enrollment is completed. If enrollment is successfully completed, the PowerMaster-360R sounds the Success Tune and the Virtual or Touch Keypad momentarily shows **DEVICE ENROLLED** and then displays the device details.

Enrolling a Wired Input

To enroll a wired input to the detector, complete the following process:

ⓘ	ⓘ *- Adding a Wired Input*
[1]	Enter **INSTALLER MODE**, and select **02:ZONES DEVICES** (see section 4.2) .
[2]	Select **ADD WIRED SENSOR**.
[3]	Select the required sensor group, for example Contact Sensors, Shock Sensors.
[4]	Select the required device.
[5]	Select the required PIN number from the HW INPUT PIN #. The input is enrolled as a zone**, for example:Z02: Wired Sensor** with ID number **053-XXXX**.
[6]	Scroll to select the required zone number, location, zone type, chime configuration, and device setting. The device settings for a wired input include the following **Wiring Type** options: - EOL– end of line - Normally open - Normally closed - Double EOL (not available for all devices – see device installation instructions)
[NOTE:]	Once a wired input is enrolled to a device, the menus **Input #1** (for MC-302 E) and **Aux Input** (for SD-304) are not available for further configuration in the device's **Device Settings**.
[NOTE:]	Deleting the device will automatically delete its wired input.

Enrolling a PGM Output

To enroll a PGM output to the detector, complete the following process:

ⓘ	ⓘ *- Adding a PGM Input*
[1]	Enter **INSTALLER MODE**, and select **02:ZONES DEVICES** (see section 4.2) .
[2]	Select **ADD PGM OUTPUT**.
[3]	Select the required sensor group (Contact Sensors).
[4]	Select the required device.
[5]	Select the required PIN number from the PGM OUTPUT PIN #.
[6]	Scroll to select the required location name.

Part B – Configuration

Step 1	ⓘ	**Step 2**	ⓘ	**Step 3**	ⓘ	**Step 4**	ⓘ
Enter Location Menu	[1]	Select Location *(see list below)*	[2]	Enter Zone Type	[3]	Select Zone Type *(see list below)*	[4]
▶▶ ⇨		▶▶ ⇦		▶▶ ⇨		▶▶ ⇦	
Z10:LOCATION	OK	**Dining room ■** ⇩ **Custom 5**	OK	**Z10:ZONE TYPE**	OK	**1:Exit/Entry1 ■** ⇩ **5. Interior**	OK

Step 5	ⓘ	**Step 6**	ⓘ	**Step 7**	ⓘ	**Step 8**	ⓘ
Enter Chime Menu	[5]	Select Chime option	[6]	Enter Partitions Menu	[7]	Select Partition options	[8]
▶▶ ⇨		▶▶ ⇦		▶▶ ⇨		▶▶ ⇦	
Z10:SET CHIME	OK	**chime OFF ■** ⇩ **melody-chime**	OK	**Z10:PARTITIONS**	OK	**Z10:P1■ P2 P3**	OK

Step 9	ⓘ	Step 10	ⓘ	Step 11
Enter Device Settings Menu	[9]	Configure Device Parameters	[10]	Continue or End
▶▶ ⇨		▶▶ ⇘		
Z10:DEV SETTINGS	OK	Refer to device datasheet in the device Installation Instructions for specific configuration instructions.		To continue – See ⓘ [11]

ⓘ	ⓘ - ***Configuring New Devices***
	Location (name) setting:
[1]	To review or change the **Location** (name) setting, press the i OK button, otherwise scroll to the next option.
[2]	To change the Location name, enter the menu and select the name from the **Location List** below. You can assign additional custom names using the **06.CUSTOM NAMES** option in the Installer Mode menu. See section 4.8. ***Note:*** *As a shortcut, press the 2 digit serial No. of the Custom Location, which takes you directly to its menu.*
	Zone Type setting:
[3]	To review or change the **Zone Type** setting, press the i OK button, otherwise scroll to the next option.
[4]	The zone type determines how the system handles signals sent from the device. Press i OK and select a suitable zone type. The list of available **Zone Types** and the explanation for each zone type is provided below. ***Note:*** *As a shortcut, press the 2 digit serial No. of the* ***Zone Type*** *shown in the Location List below, which takes you directly to its menu.*
	Chime setting:
[5]	All zones are set to **chime OFF** by default. To configure the device to cause the panel to sound (when disarmed) a **Chime** melody when tripped, press the i OK button, otherwise scroll to the next option.
[6]	Select between **Chime OFF**, **melody-chime** and **zone name-chime**. In melody chime the control panel sounds a chime melody when the sensor is tripped. In zone name-chime the control panel sounds the zone name when the sensor is tripped. The chime operates during the Disarm mode only.
	Partitions setting:
	Note: *The PARTITIONS menu appears only if Partitions is enabled in the control panel (see section 4.13).*
[7]	When entering the menu, the display shows the default Partition selection (marked with ■).
[8]	Use the keypad keys 1, 🔊, 2, 3, 💡 to assign partitions to the device.
	Device Configuration:
[9]	To review or change the **Device Configuration (settings)**, press the i OK button, otherwise scroll to the next option – see ⓘ [11].
[10]	To configure the device parameters, refer to its corresponding device datasheet in the device Installation Instructions. The defaults of the device parameters can be also configured as explained in section 4.4.7.
[11]	After completing the configuration of the device, the wizard brings you to the **Next Step** menu with the following 3 options: **NEXT Device** to enroll the next device. **MODIFY Same Dev.** reverts to Step 1 (**LOCATION**) to allow you to perform additional changes to the device, if needed. **EXIT Enrollment** exits the enrollment procedure and returns to Step 1 bringing you back to the **ADD NEW DEVICES** menu.

Location List

No.	Location Name	No.	Location Name	No.	Location Name	No.	Location Name
01	Attic	09	Dining Room	17	Hall	25	Utility Room*
02	Back door	10	Downstairs	18	Kitchen*	26	Yard
03	Basement	11	Emergency	19	Wired PSU*	27	Custom1*
04	Bathroom	12	Fire	20	Wired Siren*	28	Custom2*

No.	Location Name	No.	Location Name	No.	Location Name	No.	Location Name
05	Bedroom	13	Front Door	21	PSU RED CARE*	29	Custom3*
06	Child room	14	Garage	22	RED CARE	30	Custom4*
07	Closet	15	Garage Door	23	Office	31	Custom5*
08	Den	16	Guest Room	24	Upstairs		

* All location names can be customized by 06:CUSTOM NAMES menu (see section 4.8)

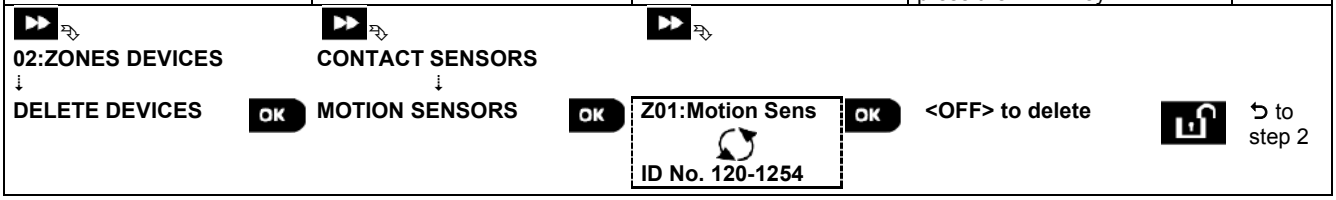
Zone type list

No.	Zone type	Description
1.	Exit/Entry 1	This Zone starts the exit time when the user arms the system or the entry time when the system is armed. To configure the Exit/Entry 1 time, see sections 4.5.1 & 4.5.2 - Installer Mode menu **03.CONTROL PANEL** options 01 and 03. (*)
2.	Exit/Entry 2	Same as Exit / Entry 1 but with a different delay time. Used sometimes for entrances closer to the panel. For configuring the Exit and Entry 2 delays, see sections 4.5.1 & 4.5.2 – **Installer Mode** menu **03.CONTROL PANEL** options 02 and 03. (*)
3.	Home Delay	Used for Door/Window Contacts and Motion sensors protecting entrance doors to interior living areas where you wish to move freely when the system is armed HOME. Functions as a **Delayed** zone when the system is armed **HOME** and as a **Perimeter Follower** zone when the system is armed **AWAY**.
4.	Inter-Follow	Similar to **Interior** zone but temporarily ignored by the alarm system during entry/exit delay periods. Usually used for sensors protecting the route between the entrance door and the panel.
5.	Interior	This zone type generates an alarm only when the system is armed **AWAY** but not when the system is armed **HOME**. Used for sensors, installed in interior areas of the premises, that must be protected when people are not present inside the premises.
6.	Interior-Delay	This zone type behaves as an **Interior** zone when the system is armed **HOME** and as a **Delayed** zone when the system is armed **AWAY**.
7.	Perimeter	This zone type generates an alarm when the system is armed both in **AWAY** and **HOME** modes. Used for all sensors protecting the perimeter of the premises.
8.	Perim–Follow	Similar to **Perimeter** zone, but is temporarily ignored by the alarm system during entry/exit delay periods. Usually used for sensors protecting the route between the entrance door and the control panel.
9.	24h silent	This zone type is active 24 hours, even when system is **DISARMED**. It is used to report alarm events from sensors or manually activated buttons to the Monitoring Station or private telephones (as programmed) without activating the sirens.
10.	24h audible	Similar to 24hr silent zone, but also provides an audible siren alarm. ***Note:*** *This zone type is used only for burglary applications.*
11.	Emergency	This zone type is active 24 hours, even when the system is **DISARMED**. It is used to report an emergency event and to initiate an **Emergency call** to the Monitoring Stations or private telephones (as programmed).
12.	Arming Key	An Arming key zone is used to control the arming and disarming of the system. ***Note:*** *Operates with the magnetic contact device, magnetic contact device with auxiliary input and vanishing magnetic contact device.*
13.	Non-Alarm	This zone does not create an alarm and is often used for non-alarm applications. For example, a detector used only for sounding a chime.
14.	Fire	A Fire zone is used for connecting the MC-302E (magnetic contact with hard-wired input) to a wired smoke detector.
17.	Guard keybox	A Guard keybox zone is usually connected to a metal safe containing the physical keys needed to enter the building. Following an alarm, the safe becomes available to a trusted Guard who can open the Guard keybox, obtain the keys and enter the secured premises. The Guard keybox zone acts just like a 24H audible zone. The Guard keybox zone also provides automatic audible internal and external siren alarm that is immediately reported to the Monitoring Station (and does not depend on the Abort Time). ***Notes:*** ***1.*** *Opening/closing the Guard keybox causes the PowerMaster-360R to signal the Monitoring Station.* ***2.*** *Operates with the magnetic contact device with auxiliary input.*

No.	Zone type	Description
18	Outdoor	A zone for outdoor areas where an activated alarm does not indicate intrusion into the house. This zone type generates an alarm when the system is armed both in AWAY and HOME modes. Events are sent to private phones and not to the Monitoring Station.
19	Int./Delay	This zone type behaves as an “Interior” zone when the system is armed ‘Home’ and as a “Delayed” zone when the system is armed ‘Away’.
20	Tamper	This is a 24 hour zone operating all of the time even when the system is disarmed. The tamper zone reports tamper alarm events from an external wired device. The behavior is the same as opening the tamper switch of a detector.
21	Line Fail	This is a 24 hour zone that operates all of the time even when the system is disarmed. The line fail zone reports phone line failures from an external wired receiver that is connected to a phone line.
22	PSU Fail	This is a 24 hour zone that operates all of the time even when the system is disarmed. The PSU fail zone reports power supply failures from an external wired device.
23	Panic	This is a 24 hour zone that operates all of the time even when the system is disarmed. The panic zone reports panic events from any panic device to the monitoring station or private telephone numbers. A panic event generates an audible siren alarm.
24	Freezer Trbl	This zone type is active 24 hours, even when the system is disarmed. It is used to report freezer trouble. The freezer trouble zone reports a trouble from an external (3rd party) temperature device if it detects a change in temperature. Freezer trouble beeps can also be produced by the siren if enabled. This zone type is often used with refrigerators with an external output temperature detector. If the temperature inside the refrigerator is above a defined value the refrigerator can trigger the output connected to the freezer trouble zone type, and the PowerMaster panel will trigger a freezer trouble alert.
(*)	*These Zone types are useful mainly when arming and disarming the system from inside the protected premises. If you arm and disarm the system from outside without tripping any sensor, such as using a keyfob, it is better to use the other Zone Types.*	

4.4.3 Deleting a device

Step 1	ⓘ	Step 2	ⓘ	Step 3	ⓘ	Step 4	ⓘ	Step 5
Select DELETE DEVICES Option	[1]	Select the respective device Group	[2]	Select exact device you wish to delete	[3]	To delete the device: press the 🔓 key	[4]	



ⓘ	ⓘ *– Deleting a Device*
[1]	Enter the **Installer Mode Menu**, select the **02.ZONES/DEVICES** option (see section 4.2) and then select the **DELETE DEVICES** option.
[2]	Select the respective group of the device you wish to delete. For example, **MOTION SENSORS**.
[3]	Scroll the Device Group, identify (by zone and/or ID number) the exact device you wish to replace, for example: **Z01: Motion Sensor** > **ID No. 120-1254** and press the ⓘ | OK button.
[4]	The display prompts you **<OFF> to delete**. To delete the device, press the 🔓 (OFF) button.

4.4.4 Modifying or reviewing a device

To **Modify** or **Review** the device parameters proceed as follows:

Step 1	ⓘ	Step 2	ⓘ	Step 3	ⓘ	Step 4	ⓘ	Step 5
Select MODIFY DEVICES Option	[1]	Select the respective device Group	[2]	Select exact device you wish to modify	[3]	Select the Parameter you wish to modify	[4]	Modify the Parameter
▶▶ 02:ZONES DEVICES ↓ MODIFY SENSORS	OK	▶▶ CONTACT SENSORS ↓ MOTION SENSORS	OK	Z10:Motion Camra ↻ ID No. 140-1737	OK	Z10:LOCATION Z10:ZONE TYPE Z10:SET CHIME Z10:PARTITIONS Z10:DEV SETTINGS	OK	See ⓘ [4] When done ⮌ to step 2

ⓘ	ⓘ *– Modifying or Reviewing a Device*
[1]	Enter the **Installer Mode menu**, select the **02:ZONES/DEVICES** option (see section 4.2) and then select the **MODIFY DEVICES** option.
[2]	Select the respective group of the device you wish to review or modify. For example, **MOTION SENSORS**.
[3]	Scroll the Device Group, identify (by zone and/or ID number) of the exact device you wish to modify or review, for example: **Z10:Motion Camra** > **ID No. 140-1737**.
[4]	From here on the process is same as the configuration process that follows the enrollment of that device. To continue, refer to Section 4.4.2 Adding a New Wireless Device Part B. When done, the display will show the next device of the same type (i.e. Motion camera).

4.4.5 Replacing a device

Use this option to replace a faulty device that is enrolled in the system with another device of the same type number (i.e. same first 3 digit of the ID number – see section 4.4.2.A) while keeping the same configuration of the original device. There is no need to delete the faulty device or to reconfigure the new device. Once enrolled, the new device will be configured automatically to the same configuration of the faulty (replaced) device.

To **Replace**, a device proceed as follows:

Step 1	ⓘ	Step 2	ⓘ	Step 3	ⓘ	Step 4	ⓘ	Step 5
Select REPLACE DEVICES Option	[1]	Select the respective device Group	[2]	Select exact device you wish to replace	[3]	Enroll the new device	[4]	
▶▶ 02:ZONES/DEVICES ↓ REPLACE DEVICES	OK	▶▶ CONTACT SENSORS ↓ KEYFOBS	OK	K03:Keyfob ↻ ID No. 300-0307	OK	ENROLL NOW or ↻ ENTR ID:300-XXXX	OK	See ⓘ [4].

ⓘ	ⓘ *– Replacing a Device*
[1]	Enter the **Installer Mode menu**, select the **02:ZONES/DEVICES** option (see section 4.2) and then select the **REPLACE DEVICES** option.
[2]	Select the respective group of the device you wish to replace. For example, **KEYFOBS**.
[3]	Scroll the Device Group, identify (by zone and/or ID number) the exact device you wish to replace, for example: **K03: Keyfob** > **ID No. 300-0307**. If you try enrolling a new device of a different type than the replaced device, the PowerMaster-360R will reject the new device and the Virtual or Touch Keypad display will read **WRONG DEV.TYPE**. When done, the Virtual or Touch Keypad display shows the device details of the new device.

4.4.6 Configuring soak test mode

This option enables you to enter device zones into Soak Test mode.
To **Enable** the Soak Test proceed as follows:

Step 1 ⓘ	**Step 2** ⓘ	**Step 3** ⓘ	**Step 4** ⓘ	**Step 5** ⓘ
Select ADD TO SOAK TEST Option [1]	Select the respective device Group [2]	Select device zone number [3]	Select to enable or disable the Soak Test [4]	[5]
▶▶ ⮆ **02:ZONES/DEVICES** ↓ **ADD TO SOAK TEST** OK	▶▶ ⮆ **CONTACT SENSORS** ↓ **MOTION SENSORS** OK	▶▶ ⮆ **Z09:Motion Sens** ↻ **ID No. 120-2468** OK	▶▶ ⮆ **Disable test** ■ **Enable test** OK	See ⓘ [5] ⮌ to Step 3

ⓘ	ⓘ ***– Enabling Soak Test mode***
[1]	Enter the **Installer Mode menu**, select the 02.ZONES/DEVICES option (see section 4.2) and then select the ADD TO SOAK TEST option.
[2]	Select the respective Group of the device you wish to add the Soak Test. For example, **MOTION SENSORS**.
[3]	Scroll to select the specific device zone number.
[4]	Select between **Disable test** (default) or **Enable test**.
[5]	If set to **Enable Test** you must set the duration of the Soak Test before the Soak Test will start (see section 4.5.8). You can stop the test for the relevant zone by changing the setting to **Disable test** at any time during the testing period. All Soak test zones will be reset to start a new test upon occurrence of one of the following: 1) Power up of the system; 2) Setup of Factory Default; 3) Change in system Soak Time.

4.4.7 Defining configuration defaults for device settings

PowerMaster-360R enables you to define the **default parameters** used during enrollment and to change them whenever you wish so that new devices enrolled into the system will be configured automatically with these default parameters without the need to modify the configuration of each new enrolled device. You can use a certain set of defaults for certain group of devices and then change the defaults for another group.

IMPORTANT: Devices that were already enrolled in the PowerMaster-360R system before the defaults have been changed will not be affected by the new default settings.

To **Define** the Default parameters of a device Group proceed as follows:

Step 1	ⓘ	**Step 2**	ⓘ	**Step 3**	ⓘ	**Step 4**	ⓘ	**Step 5** ⓘ
Select DEFINE DEFAULTS Option	[1]	Select the respective device Group	[2]	Select the Default Parameter	[3]	Select the new Default Setting	[4]	[5]
▶▶ **02:ZONES/DEVICES** ↓ **DEFINE DEFAULTS**	OK	▶▶ **CONTACT SENSORS** ↓ **MOTION SENSORS**	OK	▶▶ **Alarm LED** **Event Counter** **Disarm Activity** ↓	OK	▶▶ **Low** ■ **High**	OK	See ⓘ [5] ⮌ to Step 3

ⓘ	ⓘ ***– Changing Defaults***
[1]	Enter the **Installer Mode menu**, select the 02.ZONES/DEVICES option (see section 4.2) and then select the DEFINE DEFAULTS option.
[2]	Select the respective Group of the device you wish to define its defaults. For example, **MOTION SENSORS**.
[3]	Scroll the parameter list of the Device Group and select the Default Parameter you wish to change, for example: **Event Counter**. The list combines the parameters of all devices in the group, for example, the parameters of all types of Motion sensors.
[4]	In the example, the existing default setting of the Event Counter for enrolled motion sensors was Low Sensitivity (marked with ■) . To change it to **High**, scroll the menu until the display shows **High** and press the ⓘ OK button. The new default for the Event Counter parameter setting of Motion Sensors enrolled from now on will be **High**.
[5]	The new default does not affect motions sensors that were already enrolled before the change was made but only new motion sensors that will be enrolled in the PowerMaster-360R after the change is performed.

4.4.8 Updating devices after exiting installer mode

When exiting the **Installer mode**, the PowerMaster-360R panel communicates with all devices in the system and updates them with the changes that have been performed in their Device Settings configuration. During the updating period, the display indicates **DEV UPDATING 018** where the number (for example, 018) is a countdown of the remaining number of devices yet to be updated.

4.5 Control panel

4.5.1 General guidance – Control panel flow-chart & menu options

The **CONTROL PANEL** menu enables you to configure and customize the operation of the control panel. The **CONTROL PANEL** menu provides you with configurable parameters divided into several groups, each dealing with certain aspects of the system operations as follows (see detailed list in Step 2 of the chart below):

Group	Description of Group Features and Parameters	Section
Arming/Disarming and Exit/Entry Procedures	Contains configurable features and parameters related to Arming and Disarming of the system and the Exit and Entry procedures.	4.5.2
Zone Behavior	Contains configurable features and parameters related to the functionality of the Zones.	4.5.3
Alarms & Troubles	Contains configurable features and parameters related to initiating, canceling and reporting of Alarm and Trouble events.	4.5.4
Sirens	Contains configurable features and parameters common to all sirens in the system.	4.5.5
User Interface	Contains configurable features and parameters related to the functionality of the panel's audible and visual indications.	4.5.6
Jamming & Supervision	Contains configurable features and parameters related to detecting and reporting of RF Jamming and device Supervision (missing device) events.	4.5.7
Miscellaneous	Contains a variety of other configurable features and parameters related to the system.	4.5.8

To enter the **03.CONTROL PANEL** menu and to select and configure an option, proceed as follows:

Step 1	Step 2						Step 3
Select **CONTROL PANEL** option	Select the **Control Panel** Parameter you wish to configure						Configure option
⏩	⏩	See	⏩	See	⏩	See	
INSTALLER MODE ↓	**Arming & Disarming**	4.5.2	**Alarms & Troubles**	4.5.4	**User Interface**	4.5.6	
03.CONTROL PANEL OK	**01:ENTRY DELAY1**		**31:PANIC ALARM**		**51:PIEZO BEEPS**		
	02:ENTRY DELAY2		**32:DURESS ALARM**		**52:TROUBLE BEEPS**		
	03:EXIT DELAY		**33:INACTIVE ALRT**		**53:MEMORY PROMPT**		OK
	04:EXIT MODE		**34:TAMPER ALARM**		**54:LOW-BAT ACK**		Go to the indicated group section of the selected option
	05:QUICK ARM		**35:AC FAIL REPRT**		**55: BACKLIGHT**		
	06:BYPASS ARM		**36:CONFIRM ALARM**		**56:SCREEN SAVER**		
	07:LATCHKEY ARM		**37:ABORT TIME**				
	08:DISARM OPTION		**38:CANCEL ALARM**				
	09:ARMING KEY		**39:ALARM RESET**		**Jamming and Supervision**		
			40:ABORT FIRE T.		**61:JAM DETECT**		
	Zone Behavior	4.5.3	**Sirens**	4.5.5	**62:MISSING REPRT**	4.5.7	
	21:SWINGER STOP		**43:PANEL SIREN**		**63:NOT READY**		
	22:CROSS ZONING		**44:SIREN TIME**		**64:MISS/JAM ALRM**		OK When done ⮌ to Step 2
			45:STROBE TIME		**65:SMOK FAST MIS**		
			46:SIREN ONLINE		**Miscellaneous**		
					80: 3rd PARTY H.A		
					91:USER PERMIT	4.5.8	
					93:SOAK PERIOD		

4.5.2 Configuring arming/disarming and exit/entry procedures

The following table provides you with a detailed description of each option and its configuration settings. To select an option and change its configuration – refer to section 4.5.1.

Option	Configuration instructions
01:ENTRY DELAY1 **02:ENTRY DELAY2**	Two different entry delays allow the user to enter the protected site (while the system is in the armed state) via dedicated exit/entry doors and routes without causing an alarm. Following entry, the user must disarm the control panel before the entry delay expires. Slow-rate warning beeps start sounding via the Configuration device (PC or mobile) once the door is opened, until the last 10 seconds of the delay, during which the beeping rate increases. The **ENTRY DELAY 1** and **ENTRY DELAY 2** options allow you to program the time length of these delays. Options: **00 seconds**; **15 seconds** (default for entry delay 2); **30 seconds** (default for entry delay 1); **45 seconds**; **60 seconds**; **3 minutes** and **4 minutes**. ***Notes:*** *1. In some PowerMaster-360R variants, these menus are displayed in the Operation Mode only (see section 4.14).* *2. To comply with **EN** requirements, the entry delay must not exceed 45 sec.*
03:EXIT DELAY	This option allows programming the time length of the exit delay. An exit delay allows the user to arm the system and leave the protected site via specific routes and exit/entry doors without causing an alarm. Slow-rate warning beeps start sounding via the Configuration device (PC or mobile) once the arming command has been given, until the last 10 seconds of the delay, during which the beeping rate increases. Options: **30 seconds**; **60 seconds** (default); **90 seconds**; **120 seconds, 3 minutes** and **4 minutes**.
04:EXIT MODE	The **Exit Delay** time can be further adjusted according to your preferred exit route. The control panel provides you with the following **Exit Mode** options: **A: normal** - The exit delay is exactly as defined. **B: restrt+arm home** - Exit delay restarts when the door is reopened during exit delay. If no door was opened during exit delay AWAY, the control panel will be armed HOME. **C: restart>reentry** - The exit delay restarts when the door is reopened during exit delay. The restart occurs once only. Restarting the exit delay is helpful if the user re-enters immediately after going out to retrieve an item that he left behind. **D: end by exit** - The exit delay expires (ends) automatically when the exit door is closed even if the defined exit delay time was not completed. Options: **normal** (default); **restrt+arm home**; **restart>reentry** and **end by exit.** ***Note:*** *In some PowerMaster-360R variants, this menu is displayed in the Operation Mode only (see section 4.14).*
05:QUICK ARM	Define whether or not the user will be allowed to perform quick arming or not. Once quick arming is permitted, the control panel does not request a user code before it arms the system. Options: **OFF** (default) and **ON** (default in USA).
06:BYPASS ARM	Define whether or not the user will be allowed to manually **bypass** individual zones, or allow the system to perform automatic bypassing of open zones during the exit delay (i.e. **force arm**). If a zone is open and **forced arming** is not permitted, the system cannot be armed and **NOT READY** is displayed. If **no bypass** is selected, neither manual bypassing nor force arming is allowed which means that all zones must be secured before arming. Options: **no bypass** (default); **force arm** and **manual bypass** (default in USA). ***Notes:*** *1. To comply with **EN** requirements, **manual bypass** must be selected.* *2. The **option force** arm is not applicable in the **UK**.* *3. A zone in Soak Test mode that is configured as bypass will trigger a test fail event if the system detects a potential alarm event.* *4. There is no limit of reported events when a bypass zone is in Soak Test mode.*
07:LATCHKEY ARM	When **ON**, a **latchkey** message will be reported by SMS message to users (see Note) upon disarming by a **latchkey user** (users 5-8 or keyfob transmitters 5-8). This mode is useful when parents at work want to be informed of a child's return from school. Options: **OFF** (default) and **ON**. ***Note:*** *To enable the reporting, you must configure the system to report alrt events to Private users (Latchkey belongs to the alerts group of events). Refer to section 4.6.4 **REPORTED EVENTS** option in both **VOICE REPORT** & **SMS REPORT** menus.*

Option	Configuration instructions
08:DISARM OPTION	Certain regulations require that when the system is armed in AWAY mode, it may not be disarmed from the outside of the house (such as by keyfobs) before entering the protected premises and activating an Entry Delay zone. To answer this requirement, the PowerMaster-360R provides you with the following configurable options to disarm the system: **A:** At **any time** (default), the system can be disarmed at all times from all devices. **B:** During entry delay, the system can be disarmed only using keyfob or prox operated devices (**on entry wrless)**. **C:** During entry delay by code, the system can be disarmed only using the Configuration device (PC or mobile) (**entry + away kp.**). **D:** During entry delay, the system can be disarmed using keyfobs or by code using the Configuration device (PC or mobile) (**on entry all.**). ***Note:*** *In some PowerMaster-360R variants, this menu is displayed in the Operation Mode only (see section 4.14).*
09:ARMING KEY	Determine that, when activated, the Arming Key will arm AWAY or HOME. Options: **arm AWAY** (default) and **arm HOME**.

4.5.3 Configuring zones

The following table provides you with a detailed description of each option and its configuration settings. To select an option and change its configuration – refer to section 4.5.1.

Option	Configuration instructions
21:SWINGER STOP	Define the number of times a zone is allowed to initiate an alarm within a single arming/disarming period (including tamper & power failure events of detectors, etc.). If the number of alarms from a specific zone exceeds the programmed number, the control panel automatically bypasses the zone to prevent recurrent siren noise and excessive reporting to the Monitoring Station. The zone will be reactivated upon disarming, or 8 hours after having been bypassed (if the system remains armed). Options: **after 1 alarm** (default); **after 2 alarms** (default in USA); **after 3 alarms** and **no stop**. ***Note:*** *When a detector is in Soak Test[1] mode and also set to bypass, Swinger Stop will not prevent the sending of events. This may result in excessive reporting of Soak Fail events.*
22:CROSS ZONING	Define whether cross zoning will be active **ON** or inactive **OFF** (default). Cross zoning is a method used to counteract false alarms - an alarm will be initiated only when two adjacent zones (zone couples) are violated within a 30-second time window. This feature is active only when the system is armed AWAY and only with respect to the following zone couples: 18+19, 20+21, 22+23, 24+25, 26+27. ***Notes:*** *1. If one of the two crossed zones is bypassed (see Section 4.5.2), the remaining zone will function independently.* *2. It is recommended that crossed zones will be only zones used for detection of burglary i.e. Zone Types: Entry/ Exit, Interior, Perimeter and Perimeter follower.* *3. If a cross zone is in Soak Test mode, then each zone of this zone couple functions independently.* ***Important!*** *Do not define cross zoning to any other zone types such as Fire, Emergency, 24h audible, 24h silent etc.*

4.5.4 Configuring alarms and troubles

The following table provides you with a detailed description of each option and its configuration settings. To select an option and change its configuration – refer to section 4.5.1.

Option	Configuration instructions
31:PANIC ALARM	Define whether or not the user will be allowed to initiate a Panic Alarm from keypads (by simultaneous pressing the two Panic Buttons) or keyfobs (by simultaneous pressing the Away + Home buttons) and whether the alarm will be silent (i.e. only reporting of the event) or also audible (i.e. the sirens will also sound).
	Options: **audible** (default); **silent** and **disabled**.
32:DURESS ALARM (not applicable in UK)	A duress (ambush) alarm message can be sent to the Monitoring Station if the user is forced to disarm the system under violence or menace. To initiate a duress message, the user must disarm the system using a duress code (2580 by default).
	To change the code, enter the new 4-digit of the new Duress code at the position of the blinking cursor or enter 0000 to disable the duress function and then press OK.
	Notes: *The system does not allow programming a duress code identical to an existing user code.*
33:INACTIVE ALRT Previously known as NOT ACTIVE	If no sensor detects movement in interior zones at least once within the defined time window, an **inactive alert** event is initiated. Define the **time window** for monitoring the **lack of motion**.
	Options: **disabled** (default); **after**: **3/6/12/24/48/72 hours**
34:TAMPER ALARM	Define whether the Tamper switch protection of all zones and other peripheral devices (except the control panel) are **active** (default) or **not active**.
	Warning!: *If you select **not active**, be aware that no alarm or report will be initiated in case of tampering with any of the system peripheral devices.*
35:AC FAIL REPRT	To avoid nuisance reporting in case of short interruptions in the house of AC power, the system reports an AC Fail message only if the AC power does not resume within a pre-determined time delay.
	Options: **after 5 minute** (default)**, after 30 minute**, **after 60 minute** or **after 3 hours.**
	Note: *To comply with **EN** requirements, the time delay must not exceed 60 min.*
36:CONFIRM ALARM Previously known as CONFIRM TIME	If two successive alarm events occur within a specific time window, the system can be configured to report the second alarm event as a **confirmed alarm** (see section 4.6.3 option 61). You can activate this feature and set the respective time window.
	Options: **disable** (default in USA); **in 30/45/60** (default)/**90 minutes** ***Note:*** *In some PowerMaster-360R variants, this menu is displayed in the Operation Mode only (see section 4.14).*
37:ABORT TIME	The PowerMaster-360R can be configured to provide a delay before reporting an alarm to the Monitoring Station (not applicable to alarms from 24H SILENT and EMERGENCY zones). During this delay period, the siren sounds but the alarm is not reported. If the user disarms the system within the delay time, the alarm is aborted. You can activate the feature and select the Abort Time interval.
	Options: **in 00** (default in USA)/**15/30** (default)**/45/60 seconds**; **in 2/3/4 minutes**
	Note: *In some PowerMaster-360R variants, this menu is displayed in the Operation Mode only (see section 4.14).*
38:CANCEL ALARM Previously known as ALARM CANCEL	The PowerMaster-360R can be configured to provide a Cancel Alarm time window that starts upon reporting an alarm to the Monitoring Station. If the user disarms the system within that cancel alarm time, a cancel alarm message is sent to the Monitoring Station indicating that the alarm was canceled by the user.
	Options: **not active** (default in USA); **in 1/5** (default)/**15/60 minute(s)** and **in 4 hours**.

Option	Configuration instructions
	Notes: *1. In some PowerMaster-360R variants, this menu is displayed in the Operation Mode only (see section 4.14).* *2. Since the Soak Test zone does not report an alarm event to the Monitoring Station, the PowerMaster-360R will not send a cancel alarm message to the Monitoring Station even if disarmed within the Cancel Alarm period.*
39:ALARM RESET Previously known as RESET OPTION	The PowerMaster-360R provides you with the following configurable options for resetting the alarm condition and rearming the system: By the user as usual **- by user** (default). By the engineer (installer) by entering and exiting the Installer Mode, by entering and exiting the Event Log using the Installer Code or by accessing the system remotely via the PowerManage server using the Installer Code (**by engineer**). For accessing the system via the PowerManage server, see the PowerManage User's Guide.
	Note: *This feature is not applicable in the USA.*
40:ABORT FIRE T.	Select the length of time allowed by the system to abort a Fire alarm. The PowerMaster-360R is able to provide an abort interval that starts upon detection of a Fire event. During this interval, the buzzer sounds a warning but the siren remains inactive and the alarm is not reported. If the user disarms the system within the allowed abort interval, the alarm is aborted.
	Options: **in 00** (default)/**30**/**60**/**90 seconds**

4.5.5 Configuring siren functionality

The following table provides you with a detailed description of each option and its configuration settings. To select an option and change its configuration – refer to section 4.5.1.

Option	Configuration instructions
43:PANEL SIREN	Determines whether the control panel's built-in siren will sound alarms - "**ON**" (default) or remain silent – "**OFF**".
	Note: *Panel siren must be enabled unless an external sounder is connected to the product.*
44:SIREN TIME Previously known as BELL TIME	Define the period of time the sirens sounds when an alarm occurs.
	Options: **1**/**3**/**4** (default)/**8**/**10**/**15**/**20 minute(s)**.
	Notes: *1. To comply with **EN** requirements, the Siren Time must not exceed 15 minutes.* *2. For Canada, the Siren Time must be set to 8 minutes.*
45:STROBE TIME	Define the length of time the strobe light flashes when an alarm occurs.
	Options: **5**/**10**/**20** (default)/**40**/**60 minutes**.
46:SIREN ON LINE	Determine if the siren is activated when the phone line fails and the system is armed.
	Options: **disable on fail** (default) **or enable on fail.**

4.5.6 Configuring audible and visual user interface

The following table provides you with a detailed description of each option and its configuration settings. To select an option and change its configuration – refer to section 4.5.1.

Option	Configuration instructions
51:PIEZO BEEPS with partition disabled	Define whether or not the panel exit or entry warning beeps sound during exit and entry delays. An additional option is to mute the warning beeps only when the system is armed "HOME".
	Options: **ON** (default), **OFF when home** (default in USA) and **OFF**, and **OFF exit home**.
	Note: *When exit beeps are OFF, the happy (success) melody still sounds toward the end of an exit delay.* *The volume level of the exit or entry beeps can be modified by pressing the* 1 *button on the keypad to increase the volume, or by pressing the* 4 *button to decrease the volume.*

Option	Configuration instructions
51:PIEZO BEEPS with partition enabled	Define whether or not the panel exit or entry warning beeps sound during exit and entry delays. An additional option is to mute the warning beeps only when the system is armed “HOME”. The control panel’s display is: Def:P1■ P2□ P3□ Press the buttons 1, 2, or 3 to select the corresponding partitions. Pressing each button repeatedly toggles between the following options. Options: ■ (enable beeps), **H** (OFF when home), **h** (OFF exit home) and □ (disable beeps). ***Notes:*** *1. When exit beeps are OFF, the happy (success) melody still sounds toward the end of an exit delay.* *2. The volume level of the exit or entry beeps can be modified by pressing the 1 button on the keypad to increase the volume, or by pressing the 4 button to decrease the volume.*
52:TROUBLE BEEPS	Under trouble conditions, the panel sounder emits a series of 3 short reminder beeps once per minute. Define whether to enable or disable this reminder beeping or just disable it at night. The “night” hours are predefined factory settings but are usually from 8 PM (20:00) until 7:00 AM. Options: **ON** (default in USA only); **OFF at night** (default) and **OFF**.
53:MEMORY PROMPT	Define whether or not the user will receive Memory indication on the Virtual or Touch Keypad that an alarm has been activated. By pressing the i OK button in standby mode, you can view details of the alarm memory. Options: **ON** (default) and **OFF**.
54:LOW-BAT ACK	You can activate or deactivate the Low Battery Acknowledge requirement from the user whose keyfob's battery is low. For further information, see PowerMaster-360R User's Guide Chapter 6. Options: **OFF** (default) – acknowledge not needed; **ON** – acknowledge required.
55:BACK LIGHT	Define whether the panel's back lighting remains on at all times or turns on only when a key is pressed and turns off within 10 seconds if no further keystrokes are sensed. Options: **always ON** and **OFF after 10 sec** (default).
56:SCREEN SAVER with partition disabled	The Screen Saver option (when activated) replaces the status display on the Virtual or Touch Keypad with PowerMaster-360R display if no key is pressed during more than 30 seconds. You can activate the Screen Saver and determine whether the status display will resume following any key press (**refresh by Key**) or by entering a code (**refresh by Code**). If **refresh by Key** is selected, the first pressing of any key (except Fire and Emergency) will produce the status display and the second press will perform the key function. For further information, see the User's Guide, Chapter 1, Screen Saver Mode. Options: **OFF** (default); **refresh by Code** and **refresh by Key**. ***Notes:*** *1. To comply with **EN** requirements, refresh by code must be selected.* *2. For Fire and Emergency keys, the first key press will produce the status display and will also perform the Fire/Emergency function.*
56:SCREEN SAVER With Partition enabled	Certain regulations require that the system status display will not be exposed to unauthorized persons. The Screen Saver option (when activated) replaces the system status indication on the Virtual or Touch Keypad with idle text if no key is pressed during more than 30 seconds. You can activate the Screen Saver option and determine whether the status display will resume following any key press (**Text - by Key**) or by entering a code (**Text - by Code**). If **Text by Key** is selected, the first pressing of any key (except Fire and Emergency) will produce the status display and the second press will perform the key function. Regarding the Fire and Emergency keys, the first key press will produce the status display and will also

Option	Configuration instructions
	perform the Fire/Emergency function. You can also determine that if no key is pressed during more than 30 seconds the date and time will appear on the display. You can determine that normal display will return after pressing the  button followed by entering user code (**Clock - by Code**) or after pressing any key (**Clock - by Key**). For further information, see the User's Guide, Chapter 1, Screen Saver Mode.
	Options: **OFF** (default); **Text - by code**; **Text - by Key**; **Clock - by Code**; **Clock - by Key**.
	Note: *1. To comply with **EN** requirements, refresh by code must be selected.* *2. For Fire and Emergency keys, the first key press will produce the status display and will also perform the Fire/Emergency function.*

4.5.7 Configuring jamming and supervision (missing device)

The following table provides you with a detailed description of each option and its Options. To select an option and change its setting (configuration) – refer to section 4.5.1.

Option	Configuration instructions
61:JAM DETECT	Define whether jamming (continuous interfering transmissions on the radio network) will be detected and reported or not. If any of the jam detection options is selected, the system will not allow arming under jamming conditions. The PowerMaster-360R provides several jam detect and reporting options to comply with the following standards: ***Note:*** *Jamming is identified by the message system jammed displayed on the Virtual or Touch Keypad.*

Option	Standard	Detection and Reporting occurs when:
UL 20/20	USA	There is continuous 20 seconds of jamming
EN 30/60	Europe	There is an accumulated 30 seconds of jamming within 60 sec.
Class 6 (30/60)	British Standard	Like EN (30/60) but the event will be reported only if the jamming duration exceeds 5 minutes.
disabled	(default)	No jamming detection and reporting.
Notes:	*To comply with **EN** requirements, EN 30/60 must be selected.* *To comply with **UK** Class-6 requirements, class 6 (30/60) must be selected.*	

62:MISSING REPRT Previously known as SUPERVISION	Define the time window for reception of supervision (keep alive) signals from the various wireless peripheral devices. If any device does not report at least once within the selected time window, a MISSING alert is initiated.
	Options: **after 1/2/4/8/12** (default) **hour(s)**; and **disabled**.
	Note: *To comply with **EN** requirements, 1 hour or 2 hours must be selected.*
63:NOT READY	Define that in case of a supervision trouble (i.e. a device is missing - see 62: MISSING REPRT) whether the system will continue to operate as **normal** or the system status will become Not Ready (**upon missing**) for as long as the Missing trouble exists.
	Options: **normal** (default) and **if missing dev.**
64:MISS/JAM ALRM Previously known as BELL/REP.OPT	EN/UL standards require that if a supervision (missing) or jamming trouble occurs during AWAY arming, the siren will sound and the event will be reported as a tamper event. Define whether the system will behave according to **EN standard** or as **normal** (default).
	Note: *To comply with **EN** requirements EN standard must be selected.*
65:SMOK FAST MIS	Determine that If the smoke detector does not report at least once within a time window of 200 seconds, a MISSING alert is initiated.
	Options: **Disabled** (default) and **Enabled.**

4.5.8 Configuring miscellaneous features

The following table provides you with a detailed description of each option and its configuration settings. To select an option and change its configuration – refer to section 4.5.1.

Option	Configuration instructions
80:3 rd PARTY H.A	Determines if a third party home automation interface is connected or not. Options: **disable** (default) or **enable**
91:USER PERMIT	User Permission enables you to determine whether access to the INSTALLER MODE requires the user's permission or not. If you select **enabled**, the installer will be able to access the system only through the user menu after the user code has been entered (see section 4.2). Options: **disable** (default) or **enable** (default in UK). ***Note:*** *To comply with* ***EN*** *requirements, Enable must be selected.*
93:SOAK PERIOD	Define the period of time for the Soak Test. Options: **Disable** (default), **7 days**, **14 days** or **21 days**. ***Notes:*** *1. If set to one of the above pre-defined period of times, to be operational Soak Test mode must also be set to* ***Enable Test*** *from the 02:ZONES/DEVICES menu (see Section 4.4.6).* *2. If a change is made to the period of time of the Soak Test while the zone is currently being tested, this will restart the Soak Test.* *3. The start of the Soak Test period is defined in the factory from 9 AM (09:00).*

4.6 Communication

4.6.1 General guidance – Communication flow-chart & menu options

The COMMUNICATION menu enables you to configure and customize the communication and reporting of alarm, troubles and other system events for monitoring companies or private users according to your local requirements and personal preferences. PowerMaster-360R offers a variety of communication means including Cellular GSM, GPRS, EMAIL, MMS or SMS and IP via broadband internet connection.

The **04.COMMUNICATION** menu contains several sub-menu options, each covering a group of configurable features and parameters related to the communication and reporting as follows (see detailed list in Step 3 of the chart below):

Option	Description of features and parameters	Section
2:GSM/GPRS/SMS	Contains configurable features and parameters related to the Cellular connection of the PowerMaster-360R system.	4.6.2
3:C.S. REPORTING	Contains configurable features and parameters related to Reporting of event messages to Monitoring Stations via cellular or IP broadband communication.	4.6.3
4:PRIVATE REPORT	Contains configurable features and parameters related to Reporting event messages to Private Users via email, MMS or SMS.	4.6.4
5:MOTION CAMERA	Contains configurable features and parameters related to Motion Cameras for Video Alarm Verification.	4.6.5
6:UP/DOWNLOAD	Contains configurable connection information, access permission and security codes related to the Upload/Download procedures via GPRS.	4.6.6
7:BROADBAND[1]	Contains DHCP Client settings, enables to enter LAN parameters, to reset broadband module and to enter LAN parameters.	4.6.7
8:Wi-Fi	Contains configurable Wi-Fi connection parameters. Only in the event that a wired connection is not available is the Wi-Fi connection used. From V19.4 onwards PowerMaster-360-R has the ability to connect to an internet router by Wi-Fi to communicate and report alarms, troubles, and other system events. Wi-Fi client configuration is available through the VisonicGO application.	

To enter the **04.COMMUNICATION** menu and to select and configure an option, proceed as follows:

Step 1	Step 2	Step 3		Step 4
Select COMMUNICATION	Select Communication Sub-menu option	Select the **Communication** Parameter you wish to configure		
▶▶	▶▶	▶▶	▶▶	See
INSTALLER MODE ↓ **04.COMMUNICATION** OK	**2:GSM/GPRS/SMS** OK ↓	**SMS REPORT** **GPRS APN** **GPRS USERNAME** **SIM PIN CODE**	**GPRS PASSWORD** OK **NETWORK ROAMING** **REQUEST OPERATOR** **OP. BLACK LIST** **NETWORK TYPE** **GPRS ALWAYS ON** **GSM KEEP ALIVE** **TRANS. PROTOCOL**	4.6.2
	3:C.S. REPORTING OK ↓ (✳) These options are available only to the **Master Installer**	**01:REPORT EVENTS** ✳ **02:1st RPRT CHAN** **05:DUAL REPORT** **11:RCVR1 ACCOUNT** ✳ **12:RCVR2 ACCOUNT** ✳ **21:IP RCVR 1** ✳ **22:IP RCVR 2** ✳ **26:SMS RCVR 1** ✳ **27:SMS RCVR 2** ✳ **28 : RCVR 1 DNS** **29 : RCVR 2 DNS**	**47:GSM RETRIES** **48:BB IP RETRIES** **51: AUTO-TST LOOP** **52:AUTO-TST TIME** **53:COM.FAIL RPRT** **→GSM/GPRS FAIL** **→BROADBAND FAIL** **61:RPRT CNF ALRM** **62:RECENT CLOSE** ✳ **63:ZONE RESTORE** **64:SYST.INACTIVE** **66:24H ZONE RPRT**	OK 4.6.3

[1] The name of the product is PowerLink3 IP Communicator

Step 1	Step 2	Step 3			Step 4
Select COMMUNICATION	Select Communication Sub-menu option	Select the **Communication** Parameter you wish to configure			
▶▶ ↘	▶▶ ↘	▶▶ ↘	▶▶ ↘		See
	4:PRIVATE REPORT ↓	OK SMS REPORT	EMAIL BY SERVER	OK	4.6.4
		→REPORTED EVENTS	→1st E-MAIL		See also User's Guide Chap. 4 Section B.12
		→1st SMS tel#	→2nd E-MAIL		
		→2nd SMS tel#	→3rd E-MAIL		
		→3rd SMS tel#	→4th E-MAIL		
		→4th SMS tel#			
		→SMS Permission			
		SMS/MMS BY SRVR			
		→1st SMS/MMS			
		→2nd SMS/MMS			
		→3rd SMS/MMS			
		→4th SMS/MMS			
	5:MOTION CAMERA ↓	OK VIEW ON DEMAND		OK	4.6.5
		VIEW TIME WINDOW			
		VIEW OTHER ALARM			
		UPLOAD FILM			
		KIDS COME HOME			
	6:UP/DOWNLOAD ↓	OK UP/DWNLOAD PARAM	GPRS UP/DOWNLOAD	OK	4.6.6
		→Remote access	→Panel SIM Tel. #		
		→Mast. UL/DL code	→1st caller ID#		
		→Inst. UL/DL code	→2nd caller ID#		
		→UL/DL Modes			
	7:BROADBAND [1]	OK DHCP Client	RESET MODULE	OK	4.6.7
		Manual IP			
		PLNK curr.params			
		→Curr.IP address			
		→Curr.subnet mask			
		→Current Gateway			
		→Current path			
	8:WiFi	OK ACCESS-POINT		OK	4.6.8
		→A.POINT MODE			
		→START A.POINT			
		→STOP A.POINT			

4.6.2 Configuring GSM-GPRS (IP) - SMS cellular connection

The GSM/GPRS module is capable of communicating with the Monitoring station receiver by GPRS or SMS channels. The GPRS channel is always enabled. If the GPRS module is not able to communicate successfully, the message is sent by SMS.

04:COMMUNICATION OK ▶▶ ··· ▶▶ **2:GSM/GPRS/SMS** OK ▶▶ ··· ▶▶ **MENU item** OK

Enter **2:GSM/GPRS/SMS**, select the menu you wish to configure see guidance above and in section 4.6.1, then refer to the following table for an explanation and configuration instructions for each option.

Option	Configuration instructions
SMS REPORT	Define whether the system will report events to the Monitoring Stations' **SMS receivers** via the **SMS** Channel. For further information, see section 4.6.3 options 26 & 27.
	Options: **disable** (default); **enable.**

[1] The name of the product is PowerLink3 IP Communicator

GPRS APN	Enter the name of the **APN Access Point** used for the internet settings for the **GPRS** (up to 40 digits string). ***Note:*** *To enter the APN Access Point, use the* ***String Editor*** *in section 4.9.1.*
GPRS USERNAME	Enter the **Username** of the **APN** used for **GPRS** communications (up to 30 digits string). ***Note:*** *To enter the Username, use the* ***String Editor*** *in section 4.9.1.*
SIM PIN CODE	Enter the **PIN code** of the **SIM card** installed in the **GSM** module (up to 8 numerical digits). ***Note:*** *To enter the numerical PIN code, use the numerical keyboard.*
GPRS PASSWORD	Enter the **Password** of the **APN** used for **GPRS** communications (up to 16 digits string). ***Note:*** *To enter the Password, use the* ***String Editor*** *in section 4.9.1.*
NETWORK ROAMING	A new cellular roaming algorithm to support cases where the panel is successfully connected to a network but GPRS connection has timed-out. With the new roaming algorithm, in such cases the panel attempts to connect to a different network. ***Modem roam en:*** *when selected, the panel uses the internal Cellular modem's algorithm for roaming. (en) = enable* ***Roam disable:*** *when selected, roaming is not allowed. Only the 'Home' network can be accepted.* ***Manual roam en :*** *when selected, the panel uses its own algorithm to select the best cellular operator.(en) = enable* ***Lock network:*** *when selected, the panel uses the operator defined in 'Requested Network'. (en) = enable*
REQUEST OPERATOR	Specifies a preferred network for example Vodafone that the panel attempts to register with. The signal strength must be above the Minimum RSSI value. Where a Requested Operator is specified, the panel attempts to return to this network on subsequent attempts. ***Note:*** *Contains an editable line to enter up to 6 numbers MCC (Mobile country code) +MNC (Mobile network code)*
OP. BLACK LIST	Used to avoid certain networks, for example, when a high signal strength operator is unreliable or the device oscillates between networks (country borders). ***Note:*** *Contains an editable line to enter up to 6 numbers MCC (Mobile country code) +MNC (Mobile network code).*
NETWORK TYPE	Define whether to use a 2G or 3G network or whether to enable the panel to use a 3G network as first priority or a 2G network as second priority. Options: **automatic** (default); **3G**; **2G**.

GPRS ALWAYS ON	Define whether the control panel will stay continuously connected **enabled**, via GPRS communication, or disconnect **disabled** (default), after each report session.
GSM KEEP ALIVE	Some GSM Service providers tend to disconnect the GSM connection if the user has not initiated any outgoing telephone calls during the last 28 days. To prevent from disconnecting the GSM connection, you can configure the system to generate a **keep alive GSM** call **every 28 days** sending a test message either to the first SMS number (if exists) or alternatively first private telephone number. Options: **Disable** (default) or **Every 28 days.**
TRANS. PROTOCOL	Select the IP protocol used to transfer data over the internet/GPRS. Options: **TCP** (default); or **UDP.**

Plink GPRS	The GSM/GPRS module is capable of communicating with the monitoring station receiver by GPRS or SMS channels. The GPRS channel is always enabled. If it fails, the GPRS module will try to communicate via SMS. **Limited (default)** – Plink uses GPRS only when the wired Ethernet channel is not functional, and for event and film reports (keep-alive and NTP mechanism will not use the GPRS channel). **Unlimited** – Plink uses GPRS only when the wired Ethernet channel is not functional, and for any other purpose. **Disable** – Plink does not use GPRS for event reports, film reports, or the home automation app.

4.6.3 Configuring event reporting to monitoring stations

The PowerMaster-360R control panel is designed to report alarm, alerts, troubles and other events and messages to two Monitoring Stations C.S.1 and C.S.2 via Cellular i.e. GPRS (IP) & SMS or Broadband IP communications channels. In this section you configure and define all parameters and features required for the reporting of the event messages to Monitoring Stations such as:

- The events reported to each of the two Monitoring Stations C.S.1 and C.S.2 and corresponding backups.
- The communication means (channel) used for the reporting and the backup means (channel) in case of failure.
- The customer's (subscriber) account number(s) to be reported to each Monitoring Station.
- The IP addresses, SMS numbers and reporting formats of the corresponding alarm receivers at the two Monitoring Stations C.S.1 and C.S.2 and the number of reporting retry attempts in case of failure to report.
- The communication Auto Tests and communication Fail reports.
- The reporting of certain system function events such as Confirmed Alarm, Recent Close, Zone Restore and System Not-Used.

04:COMMUNICATION OK ▶▶ ··· ▶▶ **3:C.S.REPORTING** OK ▶▶ ··· ▶▶ **MENU item** OK

Enter **3:C.S.REPORTING**, select the menu you wish to configure (see guidance above and in section 4.6.1), then refer to the table below which provides you with detailed explanations and configuration instructions for each option.

Option	Configuration instructions
01:REPORT EVENTS	Define which events (i.e. **Alarms (alrm)**; **Open/close (o/c)**; **Alerts (alrt)**; **All events (all)**; **Maintenance** and **Troubles**) will be reported to the Monitoring Stations. The minus (-) symbol means less/except e.g. **all(-alrt)** means **all** events except **alerts**. The asterisk (✱) is a separator between events reported to **Monitoring Station 1** (C.S.1) and events reported to **Monitoring Station 2** (C.S.2). For detailed and more complete explanation see the **Event Reporting Chart** at the end of this section. Options: **all-o/c✱ backup** (default) **all-o/c✱o/c** **disable report** **all ✱all** **all(-alrt)✱alrt** **all ✱backup** **all-o/c✱all-o/c** **alrm✱all(-alrm)** ***Note:*** *Alarm events (**alrm**) have highest priority and Alert events (**alrt**) have lowest priority.*
02:1st RPRT CHAN	If the system is equipped also with Cellular communicators, you must define which of the communicating channels (i.e. Cellular or Broadband) the system will use as the main channel (i.e. 1st priority) for reporting event messages to Monitoring Stations. Enter the 1st RPRT CHAN; option and define which of the communication channels the system will use as the main reporting channel. Options: **broadband first** (default); **disable**; and **cellular first**. ***Important:*** *If the selected main reporting channel fails, the system will use the other communication channel to report event messages to Monitoring Stations. **If none is selected, the reporting to Monitoring Stations will be disabled**.*
05:DUAL REPORT	Define whether or not to report events using broadband and cellular communication channels. Options: **disable** (default); **broadbnd & cell**.
11:RCVR1 ACCOUNT	Enter the respective 1st Account (subscriber) number (11:RCVR 1 ACCOUNT) that will

Option	Configuration instructions
12:RCVR2 ACCOUNT Master Installer only	identify your specific alarm system to the 1st Monitoring Station (designated as RCVR1 or RCV1) and a 2nd Account (subscriber) number (12:RCVR 2 ACCOUNT) that will identify the system to the 2nd Monitoring Station (designated as RCVR2 or RCV2). Each of the Account numbers consists of 6 hexadecimal digits. To enter Hexadecimal digits, use the following table: **Entering Hexadecimal Digits** **Digit** 0…..9 A B C D E F **Keying** 0…..9 [#]→[0] [#]→[1] [#]→[2] [#]→[3] [#]→[4] [#]→[5]
21:IP RCVR 1 **22:IP RCVR 2** Master Installer only	The PowerMaster-360R can be programmed to report event messages defined in the Report Events option (option 01) to two IP Receivers (PowerManage servers). You can use a maximum of two IP receivers reporting through a GPRS (IP) channel or broadband IP channel using SIA IP format. Enter the IP addresses (000.000.000.000) of receiver one (21:IP RCVR 1) and the IP address of receiver two (22:IP RCVR 2). ***Note:*** *You must enter the IP address of the receiver, even if you enter the Domain Name System (DNS) server name where the receiver is installed. See option* ***28:RCVR 1 DNS and 29:RCVR 2 DNS*** *for details on how to enter the DNS name.*
26:SMS RCVR 1 **27:SMS RCVR 2** Master Installer only	If equipped with GSM module, the PowerMaster-360R can be programmed to report the event messages defined in Report Events option (option 01) to two SMS Receivers via the GSM SMS channel using a special SMS text format. For further details concerning the SMS text format please contact Visonic. Enter the two telephone numbers (including area code – maximum 16 digits).of the SMS Receiver 1 located at the 1st Monitoring Station (26:SMS RCVR 1) and SMS Receiver 2 located at the 2nd Monitoring Station (27:SMS RCVR 2). ***Note:*** *To enter the international prefix (+) at the 1st digit – key-in [#]→[1].*
28:RCVR 1 DNS **29:RCVR 2 DNS** Master Installer only	Specifies the DNS name of the servers where the IP receivers are installed. Enter the DNS name of the servers where receiver 1 and receiver 2 are installed, the name can contain a maximum of 32 characters. The DNS name one (28:RCVR 1 DNS) must be resolved to IP receiver one (21:IP RCVR1) and the DNS name two (29:RCVR 2 DNS) must be resolved to IP receiver two (22:IP RCVR2). ***Note:*** *If you enter the DNS name you must also enter the corresponding IP receiver address. See option* ***21:IP RCVR 1*** *and* ***22:IP RCVR 2*** *for details on how to enter the IP receiver's address.*
47:GSM RETRIES	Define the number of times the system will retry to report to the Monitoring Station in case of failure to report via the cellular connection - GPRS (IP) and SMS. Options: **2 attempts**; **4 attempts** (default); **8 attempts**; **12 attempts** and **16 attempts**.
48:BB IP RETRIES	Define the number of times the system will retry to report to the Monitoring Station in case of failure to report via the Broadband Module connection. Options: **2 attempts**; **4 attempts** (default); **8 attempts**; **12 attempts** and **16 attempts**.
51: AUTO-TST LOOP	To verify a proper communication channel, the PowerMaster-360R can be configured to send a test event to the Monitoring Station periodically. You can set the interval between the consecutive test events or disable the automatic sending of this event entirely. If the interval is set for every one day or more then the exact hour of reporting can be selected with option 52. Options: **test OFF** (default); **every 1/2/5/7/14/30 day(s)**; and **every 5 hours**.
52:AUTO TST TIME	Enter the exact time (**auto test time**) during the day at which the Auto Test message (if enabled in option 51) will be sent to the Monitoring Station. ***Note:*** *If the AM/PM format is used, you can set the AM digit with the*  *button and the PM digit with the*  *button.*

Option	Configuration instructions
53:COM.FAIL RPRT **→GSM/GPRS FAIL** (Return)	Determines whether a failure in the system communication channel i.e. GSM/GPRS will be reported or not and the time delay between detection of the failure and reporting of the failure event to the Monitoring Station. A trouble event (i.e. GSM line fail) will be respectively stored in the event log
→BROADBAND FAIL (Return)	Determines whether a failure in the broadband communication channel is reported or not. You can specify the time delay between the detection of the failure and reporting the event to the Monitoring Station. This event is stored in the event log.
Previously known as LINE FAIL REPORT	Options: **after 1/2/5/15/30 min, 1/3/6 hours** and **do not report** (default).
61:RPRT CNF ALRM	Define whether the system will report whenever 2 or more events (confirmed alarm) occur during a specific period or enable the report and bypass the detector.
	Options: **rprt disabled** (default), **rprt ena+bypass** and **rprt enabled** ***Note:*** *In some PowerMaster-360R variants, this menu is displayed in the Operation Mode only.*
62:RECENT CLOSE	False alarms may occur if users do not exit the premises within the exit delay period, resulting in a false alarm a short time later. In such cases, inform the Monitoring Station that the alarm occurred shortly after the system was armed (this event is known as Recent Close). The report enabled option sends a recent closing report to the Monitoring Station if an alarm occurs within 2 minutes from the end of the exit delay.
	Options: **report disabled** (default) and **report enabled**
63:ZONE RESTORE	Some Monitoring Stations require that following an alarm event from a specific zone, the system will also report when the alarming zone has restored to normal.
	Options: **report enabled** (default) and **report disabled**
64:SYST.INACTIVE	The PowerMaster-360R can report a System Inactive event message (CID event 654) to the Monitoring Station if the system is not used (i.e. armed) during a predefined time period.
	Options: **report disabled** (default); **after 7/14/30/90 days**.
66:24H ZONE RPRT Applicable in UK only	Define whether 24 hour (silent and audible) zones will function as normal 24 hour zones or as panic zones.
	Options: **audible as panic**; **silent as panic**; **both as panic**; and **both burglary** (default).

Event reporting chart

To simplify the configuration of reporting system events to Monitoring Stations, the event messages are divided into 4 Event Groups as described in the following table below: Due to lack of space in the display, the following abbreviations are used **alrm**, **alrt**, **o/c** and **all** (i.e. all events).

Event Group	Abbr.	Events Messages Reported
Alarms	**alrm**	Fire, CO, Burglary, Panic, Tamper
Open/close	**o/c**	Arming AWAY, Arming HOME, Disarming
Alerts	**alrt**	No-activity, Emergency, Latchkey
Trouble	-	All other Trouble events not indicated above, e.g. Missing, Jamming, Communication Fail, Low Battery, AC failure etc.
Note: Alarms *group has the highest priority and* ***Alerts*** *group has the lowest priority.*		

The PowerMaster-360R allows you also to select which event groups will be reported to each of the two Monitoring Stations. The table below describes the available reporting options. The minus (**-**) symbol means but/less/except e.g. **all(-alrt)** means **all** events except **alerts**. The asterisk (✱) is a separator between event messages reported to **Monitoring Station 1** (C.S.1) and event messages reported to **Monitoring Station 2** (C.S.2).

Available reporting options	Events reported to C.S. 1	Events reported to C.S. 2
all ✳ backup	All	All, only if C.S.1 does not respond
all-o/c ✳ backup	All but open/close	All but open/close, only if C.S. 1 does not respond
all ✳ all	All	All
all-o/c ✳ all-o/c	All but open/close	All but open/close
all–o/c ✳ o/c	All but open/close	Open/close
all(–alrt) ✳ alrt	All but alerts	Alerts
alrm ✳ all(–alrm)	Alarms	All but alarms
disable report	None	None
***Note: all** means that all 5 Groups are reported including Trouble messages - sensor / system low battery, sensor inactivity, power failure, jamming, communication failure etc.*		

4.6.4 Configuring event reporting to private users

The PowerMaster-360R system can be programmed to send various SMS event notifications such as alarm, arming or trouble events, if a GSM option is installed. The system can send the messages also to 4 emails, MMS and SMS telephone numbers via the server. These reports can be programmed either instead of or in addition to the reports transmitted to the monitoring company. In this section you configure:

- The specific events you wish the system to report.
- The 1st, 2nd, 3rd, and 4th SMS numbers of the private subscribers.
- Event notification messages to be sent to 1st, 2nd, 3rd, and 4th private emails and private MMS and SMS telephone numbers via the server.

SMS Permission defines if the panel accepts SMS commands from any number or only from known numbers. For a detailed description of this menu options, refer to the User's Guide Chapter 6, section B. 12.To select and configure an option follow the instructions below. Additional guidance is provided in section 4.6.1.

04:COMMUNICATION OK ▶▶ ··· ▶▶ **4:PRIVATE REPORT** OK ▶▶ ··· ▶▶ **MENU item** OK

The **4:PRIVATE REPORT** menus and sub-menus configuration is shown in the table in section 4.6.1. For a detailed description of the menus options, refer to the User's Guide Chapter 4, section B.12.

4.6.5 Configuring motion cameras for visual alarm verification

The PowerMaster-360R can communicate to Monitoring Stations (equipped with Visonic PowerManage server) with image clips captured by Motion Cameras (models Next CAM PG2, Next-K9 CAM PG2 and TOWER CAM PG2). The Monitoring Station can use the video clips for verification of Burglary alarms detected by the Motion Cameras. The system can be configured to capture image clips also upon occurrence of Non-Burglary alarms (i.e. Fire, Duress, Emergency and Panic). The server can then forward the images to the management computer of the Monitoring Station or to 4 private emails and/or 4 mobile phones by MMS images.

In addition, the Monitoring Station can log into the PowerManage server and request the system to provide image clips On Demand and to forward them as defined in the PowerManage application. To protect customers' privacy, the PowerMaster-360R can be customized to enable the On Demand View only during specific system modes (i.e. Disarm, Home and Away) and also to a specific time window following an alarm event.

04:COMMUNICATION OK ▶▶ ··· ▶▶ **5:MOTION CAMERAS** OK ▶▶ ··· ▶▶ **MENU item** OK

Enter **5:MOTION CAMERAS**, select the menu you wish to configure (see guidance above and in section 4.6.1), then refer to the table below which provides you with detailed configuration instructions.

Option	Configuration instructions
VIEW ON DEMAND	By enabling the On Demand View, you can determine during which arming modes (system states) the On Demand View will be permitted. In the next option VIEW TIME WINDOW you can determine when, during the permitted arming modes, the On Demand View will be enabled.
	Options: **disabled** (default); **in all modes**; **in AWAY only**; **in HOME only**; **in HOME & AWAY; DISARM & AWAY**; **DISARM & HOME**; and **in DISARM only**.
VIEW TIME WINDOW VIEW TIME WINDOW menu appears only if VIEW ON DEMAND was enabled	If the On Demand View is enabled in the previous option, you can further determine whether the On Demand View will be possible at any time during the selected arming modes (i.e. Always) or restricted only to a specific limited time window that follows an alarm event.
	Options: **Always** (default); **Alarm + 5 min.**; **Alarm + 15 min.**; **Alarm + 1 hour**
VIEW OTHER ALARM	Define whether the system will capture and forward image clips also upon occurrence of Non-Burglary alarms (i.e. Fire, Duress, Emergency and panic).
	Options: **Enable** (default)**; Disable.**
KIDS COME HOME	Define that upon PIR-camera detection, the system will send up to 4 images to a 3rd party server if the system is disarmed via keypad or proximity tag by latchkey users 5 to 8 and only when the system was in Entry Delay or the Abort Time was enabled.
	Options: **Enable**; **Disable** (default). ***Note:*** *At least one PIR camera must be defined as one of the following zone types: Perim-Follow / Inter-Follow / Exit/Entry 1 / Exit/Entry 2.*
UPLOAD FILM	Define whether to enable / disable the sending of images to the PowerManage server.
	Options: **Enable** (default)**; Disable**.

4.6.6 Configuring upload / download remote programming access permissions

Using a PC, the PowerMaster-360R can be configured (by upload/download) either locally or from remote via GPRS cellular communication.
Local programming can be performed by directly connecting the computer to the panel's USB port using the Remote Programmer PC Software.
Remote programming via GPRS is performed using a Visonic PowerManage server and related Remote Programmer PC software. The PowerManage server calls from a cellular modem to the Panel's SIM card number. The panel checks the caller ID and if identical with any of the two callers ID 1 or 2 programmed in the **GPRS UP/DOWNLOAD** menu (see table below), the panel initiates a GPRS connection with the respective IP Receiver 1 or 2 (as configured in section 4.6.3 options 21 & 22). When connection is established, the monitoring company can perform the upload/download procedure via the established secured GPRS connection. For further information refer to the PowerManage User's Guide.

In this section you can configure the access permissions (i.e. security codes and identification) and determine the functionality of the upload/download procedures via GPRS channel.

04:COMMUNICATION OK ▶▶ ··· ▶▶ **6:UP/DOWNLOAD** OK ▶▶ ··· ▶▶ **MENU item** OK

Enter **6:UP/DOWNLOAD**, select the menu to configure (see guidance above and in section 4.6.1), then refer to the table below for configuration instructions.

Option	Configuration instructions
UP/DWNLOAD PARAM	Configure the Upload/Download functionality. The functionality is determined through a sub-menu of the **UP/DOWNLOAD** option as shown below. To program: Press OK to enter the **UP/DOWNLOAD** sub menu and then select and configure each of the sub-menu options as shown below. When done, press ⌂ to return.
→Remote access	Enable or disable the **remote access** to the system. If disabled, the system cannot be **accessed** remotely thereby inhibiting the Upload/Download and the Remote Control via GSM analog communication channel (see Chapter 5 in the User's Guide).
	Options: **enabled** (default)**; disabled.**
→Mast. UL/DL code	Enter the 4-digit **password** (Master Installer download code) code that will allow the **Master Installer** to access the system remotely and upload/download data to the PowerMaster-360R panel.
	Note: *0000 is not a valid code and must not be used.*
→Inst. UL/DL code	Enter the 4-digit **password** (Installer download code) code that will allow the **Installer** to access the system from remote and upload or download data into the PowerMaster-360R panel.
	Notes: *1. 0000 is not a valid code and must not be used.* *2. The installer can configure via UL/DL only the options he is authorized to configure from the control panel.*
→UL/DL modes	Define whether the downloading/uploading can be performed in Disarm mode (state) only or in all modes (i.e. Away, Home & Disarm).
	Options: **in all modes** (default) or **in DISARM only**.
⌂ (Return)	
GPRS UP/DOWNLOAD	Configure the Upload/Download functionality via GPRS. The functionality is determined through a sub-menu of the **GPRS UP/DOWNLOAD** option as shown below. To program: Press OK to enter the **GPRS UP/DOWNLOAD** sub menu and then select and configure each of the sub-menu options as shown below. When done, press ⌂ to return.
→ Panel SIM Tel.# (Previously known as **My SIM Tel.#**)	Enter the PowerMaster-360R **SIM card** telephone number. The PowerManage server at the Monitoring Station sends an SMS or voice message to this number for the panel to call back the PowerManage server via GPRS for initiating the uploading / downloading process.

Option	Configuration instructions
	Enter the SIM card telephone number of the panel's GSM module.
→ **1st caller ID#** → **2nd caller ID#**	Enter the **Caller ID** (i.e. telephone number) from which **Monitoring Station #1** (C.S.1) / **Monitoring Station #2** (C.S.2) calls the control panel for initiating the Up/Download process. If the sender's Caller ID matches with the 1st caller ID# / 2nd caller ID#, the PowerMaster-360R will call back the PowerManage server using **IP RCVR 1** / **IP RCVR 2** address as configured in Section 4.6.3, options 21 and 22.
	Note: *Caller ID#1/ID#2 must contain at least 6 digits otherwise the process will not work.*

(Return)

4.6.7 Broadband[1]

In this section you can define how to obtain an IP address, enter LAN parameters and reset broadband module settings. In addition, the PLNK curr.params menu enables reading the current IP addresses of the PowerLink for support purposes only.

04:COMMUNICATION OK ▶▶ ··· ▶▶ **7:BROADBAND** OK ▶▶ ··· ▶▶ **MENU item** OK

Enter **7:BROADBAND**, select the menu to configure (see guidance above and in section 4.6.1), then refer to the table below for configuration instructions.

Option	Configuration instructions
DHCP Client	Define whether to obtain an IP address automatically using a DHCP server or to enter an IP address manually.
	Options: **disable; enable** (default)**.**
Manual IP	Manually enter LAN parameters.
	Note: *This menu will appear only if DHCP Client is disabled.*
PLNK curr.params	Displays the current IP addresses of the PowerLink.
→**Curr.IP address**	Displays the current PowerLink IP address.
→**Curr.subnet mask**	Displays the current PowerLink subnet mask.
→**Current Gateway**	Displays the current PowerLink default gateway.
→**Current path**	Displays the current PowerLink mode of communication.
	Options: **lan; cellular; none**
RESET MODULE	Determine whether to reset the broadband module (reboot).

4.6.8 WiFi

You can configure the panel remotely from the installer configurator application using a wireless device such as a mobile phone or tablet.

To connect a wireless network device to the panel, complete the following steps:

1. From the **8: WiFi** > **ACCESS-Point** > **A.POINT Mode** menu, select **Enable.** The installer must configure this option to activate WiFi access.
2. From the **ACCESS-Point** menu, select **START A.Point** to activate the access-point.
   The WiFi status indicator light on the panel blinks fast during the activation process and blinks slowly when the access-point is active.
   Note: When the system is armed or a USB cable is connected to the panel, you cannot activate the WiFi access-point.
3. Connect the wireless device to the panel's WiFi access-point. Enter the Panel ID when requested to enter the SSID (Panels Service Set Identifier) and enter the serial number of the panel when requested to enter the password. Both numbers are printed on a sticker on the panel. Alternatively, select the **INSTALLER** > **10: SERIAL NUMBER** menu to view this information.
4. When the wireless device is connected to the panel, start the configuration application.

[1] The name of the product is PowerLink3 IP Communicator

5. When the configuration is complete, from the **ACCESS-Point** menu, select **STOP A.Point** to close the access-point.
   Note: By default the total time for access-point activity is one hour. Five minutes before the access-point is deactivated, a message is sent to the installer. You can extend the time by activating the access-point again from the menu.

From the installer mode menu, select the following options:

04:COMMUNICATION OK ▶▶ .. ▶▶ **8:WiFi** OK ▶▶ . ▶▶ **ACCESS-POINT** OK

Option	Configuration instructions
8:WiFi > ACCESS-POINT	From the WiFi ACCESS-POINT menu you can enable, activate, and deactivate an access-point.
8:WiFi > ACCESS-POINT > A.POINT MODE	To enable WiFi access, from the **ACCESS-POINT** menu select **A.POINT MODE**. Select enable to activate or disable to deactivate wireless activity.
	Options: **Disable** (default)**; Enable.**
	Press [home] to return.
8:WiFi > ACCESS-POINT > START A.POINT	To activate an access-point channel for wireless access, from the **ACCESS-POINT** menu select **START A.POINT**.
	The panel shows the status when you open the access-point channel. For example, Please Wait, OK or FAIL.
	Press [home] to return.
8:WiFi > ACCESS-POINT > STOP A.POINT	To close the access-point channel, from the **ACCESS-POINT** menu, select **STOP A.POINT**.
	The panel shows the status when you close the access-point channel.
	Press [home] to return.

4.7 PGM Output

4.7.1 General Guidance

The "**05:OUTPUTS**" menu enables you to select events/conditions under which the PGM (programmable) output will function.

To configure a PGM output located on the WL-IOG general Inputs / Outputs wireless transceiver device, use the following menu path:

05:OUTPUS OK ▶▶ ... ▶▶ **PGM OUTPUTS** OK .. **PGM ON CONTACTS** OK ... **MENU you wish** OK

Enter "**PGM ON CONTACTS**", select the zone or device and the PGM PIN number you wish to configure, and then refer to the table in section 5.7.3 for PGM configuration instructions.

Note: *PGM is not to be enabled in UL Listed Products.*

4.7.2 PGM Output Configuration

Define which factors, including any combination of factors, will determine the PGM output.

Option	Configuration Instructions
PGM: BY ARM AWAY **PGM: BY ARM HOME**	Determine to activate the PGM output upon arming **Away / Home / Disarm**.
PGM: BY DISARM	Options: **disable** (default)**; turn ON; turn OFF; activate PULSE**.
PGM: BY MEMORY	Determine to activate the PGM output upon registration of an alarm in the memory. The output will restore to normal upon memory clearing.
	Options: **disable** (default)**; turn ON; turn OFF; activate PULSE**. ***Note:*** *In Soak Test[1] mode and when BY MEMORY is enabled, the PGM will not be activated.*

[1] Soak Test is not applicable for UL installations

PGM: BY DELAY	Determine to activate the PGM output during the **Exit and Entry** delays.
	Options: **disable** (default); **turn ON**; **turn OFF**; **activate PULSE**.
PGM: BY KEYFOB	Determine to activate the PGM output upon pressing the AUX (✱) button of keyfob transmitters configured to activate the PGM output. For further details, refer to the configuration instructions of the AUX (✱) button of the respective keyfobs' datasheets.
	Options: **disable** (default)**; turn ON; turn OFF; activate PULSE; toggle**
PGM: BY SENSOR **→ Zone A Z:_ _** **→ Zone B Z:_ _** **→ Zone C Z:_ _**	Determine to activate the PGM output upon activation of any one of up to 3 sensors (zones) in the systems irrespective of whether the system is armed or disarmed. To configure: Press OK to enter the "**PGM: BY SENSOR**" sub menu and then select the Zone you wish to program, for example **"Zone A**". If the zone was configured before, the display shows the current zone number "**(Z:xx)**" and if not, the zone number will be blank ("**Z:_ _**"). To configure the zone number, press OK. Enter the Zone number (2 digits) you wish to activate the PGM output and press OK to confirm. To add another sensor, select any of the other two options ("**Zone B**" and "**Zone C**") and repeat the above process. When done press ⌂ to return.
	Options: **disabled** (default); **turn ON**; **turn OFF**; **activate PULSE**; **toggle** ***Note:*** *If you select* ***toggle****, the PGM output will be turned on upon event occurrence in any of these zones and will be turned off upon next event occurrence, alternately*.
PGM:BY LINE FAIL	Determine to activate the PGM output following failure of the PSTN line
	Options: **by line fail NO** (default)**; by line fail YES.**
PGM: BY OTHER	Determine the PGM by one of the following options: Disable (default) **ON by Com Fail**: The PGM output is activated when the panel fails to report an event. **ON by Siren**: The PGM output is activated by an external wired siren. **ON by strobe**: The PGM output is activated by a strobe.
PGM:PULSE TIME	Determine the PGM output pulse time. This value is the same for all events (by ARM AWAY, by ARM HOME, by DISARM etc.) which were selected with "activate PULSE" option.
	Options: **pulse time 2s** (default); **pulse time 30s**; **pulse time 2m**; **pulse time 4m**.

4.7.3 Entering Daytime Limits

05:OUTPUS OK ▶▶ ··· ▶▶ **LOCKOUT TIME** OK …

Enter the "**LOCKOUT TIME**" menu and enter the daytime limits through which the PGM device will turn off, even when the associated sensors are triggered.

Step 1	Step 2	Step 3	Step 4	
Select "05:OUTPUTS" menu	Select "LOCKOUT TIME" menu	Press i OK	Enter the time at which you wish the lockout state to begin	
▶▶ **05:OUTPUTS** OK	▶▶ **LOCKOUT TIME** OK	**start- HH:MM** OK	**TIME 11:30**	OK
Step 5	**Step 6**	**Step 7**	**Step 8**	
Press ▶▶	Press i OK	Enter the time at which you wish the lockout state to end	Press ⌂ to return to "LOCKOUT TIME" or 🔓 to take you to "<OK> TO EXIT"	
▶▶ **start- HH:MM**	**stop- HH:MM** OK	**TIME 19:00** OK	**stop- HH:**	

4.8 Custom names

4.8.1 Custom zone names

During the device enrollment process you also define the Location name where the device is installed. The location name is selected from a Location List of Custom names - see Section 4.4.2, Part B, for Location List and instructions. Define the custom location names according to your specific needs and use them during device enrollment.

To define the Custom Location names, follow the instructions below. Additional guidance is provided in section 4.2.

06:CUSTOM NAMES OK ▶▶ ··· ▶▶ **CUST.ZONES NAME** OK

Enter **CUST.ZONES NAME** (see guidance above), then refer to the table below which provides you with detailed explanations and programming instructions to edit the desired custom location.

Note: *All 31 location names can be edited..*

Configuration instructions

Enter the Custom Location names you wish to edit.

To edit:

Press OK to enter the **CUST. ZONES NAME** sub menu and then press OK again to select the Location # you wish to edit, for example **TEXT LOC. #01** – the display alternates with the current Custom name, for example, **Master Bdrm**. To change the name, at the blinking cursor, enter the Location name you wish and at the end, press OK to confirm. When done, press ⌂ to return.

Note: *To enter the Location name use the String Editor below.*

IMPORTANT! *The editing of a custom zone name automatically deletes the original text.*

PowerMaster-360R String Editor

Key	String Editor Functionality
0	' ', '0'
1	'.', ',', '1'
2	'a', 'A', 'b', 'B', 'c', 'C', '2'
3	'd', 'D', 'e', 'E', 'f', 'F', '3'
4	'g', 'G', 'h', 'H', 'i', 'I', '4'
5	'j', 'J', 'k', 'K', 'l', 'L', '5'
6	'm', 'M', 'n', 'N', 'o', 'O', '6'
7	'p', 'P', 'q', 'Q', 'r', 'R', 's', 'S', '7'
8	't', 'T', 'u', 'U', 'v', 'V', '8'
9	'w', 'W', 'x', 'X', 'y', 'Y', 'z', 'Z', '9'
*	!, #, %, &, ', *, +, -, /, =, ^, @, _, , :
▶▶	Moves the digits cursor from **left to right**.
◀	Moves the digits cursor from **right to left**.
#	**Changes** between **lowercase** letters (a,b,c…z), **uppercase** letters (A,B,C…Z) and **numbers** (1,2,3).
0	**Clears a single digit** of the string by cursor.
🔓	**Clears a single digit** of the string to the left of cursor.
OK	**Confirms and saves** the edited string and reverts to previous menu.
	Exiting the edit screen and moves one level up to previous or top menu without saving the edit string.
🔒	**Exiting** the edit screen and moves to the <OK> TO EXIT exit screen without saving the edit string.

4.9 Diagnostics

4.9.1 General guidance – Diagnostic flow-chart & menu options

The DIAGNOSTICS menu enables you to test your system and to verify proper operation of your PowerMaster-360R panel, wireless devices attached to it and the communication (GSM/GPRS/SIM) modules.

IMPORTANT! *Reliable reception must be assured during the initial testing and also throughout subsequent system maintenance. A* ***device should not be installed in location where signal strength is poor.*** *If you get poor signal strength from a certain device, simply re-locate it and re-test until a good or strong signal strength is received. This principle should be followed throughout the diagnostic test procedure*.

The diagnostic test process is shown below.

The **07.DIAGNOSTICS** menu contains several sub-menu options, each covering a group of configurable features and parameters related to the communication and reporting as follows (see the list in Step 3 of the chart below):

Option	Description of features and parameters	Section
WL DEVICES	Describes how to test the devices attached to the PowerMaster-360R panel, review devices' status and RF signal status. You can test all devices, test single device, review devices status and review RF problems, in case of any.	4.9.2
GSM/GPRS	Describes how to test the GSM/GPRS communication module.	4.9.3
SIM NUMBER TEST	Tests the SIM number to ensure correct entry of the SIM number in the control panel.	4.9.4
BROADBAND MODULE [1]	Enables to test the communication of the Broadband Module with the PowerManage server.	4.9.5
WLAN	Tests the communication of the WLAN Module with the PowerManage server.	4.9.6

To enter the **07.DIAGNOSTICS** menu and to select and configure an option, proceed as follows:

Step 1	Step 2	Step 3			Step 4
Select 07.DIAGNOSTICS	Select sub-menu option	Select the diagnostics you want to perform			
▶▶	▶▶	▶▶		▶▶	See
INSTALLER MODE					
▶▶					
07.DIAGNOSTICS OK	**WL DEVICES** OK	**TEST ALL DEVICES** OK			4.8.2
		SHOW ALL DEVICES			
		SHOW RF PROBLEMS			
		TEST ONE DEVICE OK	**Contact sensors** OK		
			Motion sensors		
			▶▶		
			Repeaters		
	GSM/GPRS OK				4.8.3
	SIM NUMBER TEST[1] OK	**Tst by IP RCVR 1** OK	**SIM# verified**		4.8.4
		Tst by IP RCVR 2			
	BROADBAND MODULE[2] OK	**PLEASE WAIT…**	**Unit is OK**		4.8.5
	WLAN OK	**PLEASE WAIT…**	**Unit is OK**		4.9.6

4.9.2 Testing wireless devices

The PowerMaster-360R enables to test the wireless devices attached to the panel. You can test all devices, one device at a time, display devices' status and review RF problems, in case of any.

07:DIAGNOSTICS OK ▶▶ ··· ▶▶ **WL DEVICES** OK ▶▶ ··· ▶▶ **MENU item** OK

[1] The name of the product is PowerLink4 IP Communicator

Enter the **WL DEVICES** menu, select the type of test you wish to perform (see guidance above and in section 4.8.1), then refer to the table below which provides you with detailed explanations for each option.

Option	Instructions
TEST ALL DEVICES	You can test all wall-mounted devices automatically, one after the other, after which the installer tests the other devices in the following order: vanishing magnetic contact devices, keyfobs and then panic buttons. While in **TEST ALL DEVICES**, press OK to initiate the test. The following screen will appear: **TESTING Xxx NNN**, where Xxx indicates the type of device and NNN indicates the number of enrolled devices in the panel that have not been tested yet. This number automatically drops one count for every tested device. Pressing any key during the testing process will open the following options: 1. Press ▶▶ to jump to the next device group. For example, from wall-mounted devices to keyfobs. 2. Press OK to continue the testing process 3. Press 🔒 to exit the test process. When all wall-mounted devices have completed the test procedure, you can test vanishing magnetic contact devices. While in the vanishing test process, indicated by the corresponding display, for example, **TEST VANISH NNN**, momentarily open the door or window. When all vanishing magnetic contact devices have been tested, you can test keyfobs. While in the keyfobs test process, indicated by the corresponding display, for example, **TEST KEYFOBS NN**, press any key of the selected device to initiate the test. When all keyfobs have been tested, you can test panic buttons. While in the panic button test process, indicated by the corresponding display, for example, **TEST PANIC BT. NN**, press a button on the pendant. At the end of the test process, the panel will present the following: **SHOW ALL DEVICES**. Press OK to view devices' status. ***Note:*** *Refer to* ***SHOW ALL DEVICES*** *section below for further information on device status.*
TEST ONE DEVICE **→CONTACT SENSORS** **→MOTION SENSORS** **→GLASSBREAK SENS.** **→SHOCK SENSORS** **→SMOKE SENSORS** **→CO SENSORS** **→GAS SENSORS** **→FLOOD SENSORS** **→TEMPERATURE SENS.** **→KEYFOBS** **→PANIC BUTTONS** **→KEYPADS** **→SIRENS** **→REPEATERS**	You can select a specific device group you wish to test, for example, Motion Sensors. Press OK to enter the **TEST ONE DEVICE** sub menu and use ▶▶ to scroll through the device families. Press OK to enter the **<device family>** sub menu, for example: **MOTION SENSORS**. ***Note:*** *If there is no enrolled device,* ***NO EXISTING DEV.*** *will be displayed.* The following screens will then appear: **Xxx:<device name>** ⮌ <**location**> Where Xxx indicates the device number. You can now select a specific device. Press OK to test the selected device. The following screen will appear: **TESTING Xxx 001**. While in the keyfobs, panic button or vanishing magnetic contact test process, indicated by the corresponding display, for example, **Xxx ACTIVATE NOW**, press any key of the selected keyfob or panic button, or momentarily open the door or window to initiate the test. At the end of the test process, the panel will present the devices' status: **Xxx: 24hr: <status>**[1] ⮌ **Xxx: NOW: <status>**[1]. ***Note:*** *Refer to* ***SHOW ALL DEVICES*** *section for further information on device status.*
SHOW ALL DEVICES	You can view the devices status. ***Note:*** *This option is available only after testing process was done.* Press OK to view the devices' status.

[1] The signal strength indications are as follows: **STRONG**; **GOOD**; **POOR**; **1-WAY** (the device operates in 1-way mode or, the **NOW** communication test failed); **NOT TST** (results are shown without any performed test); **NOT NET** [device is not networked (not fully enrolled)]; **NONE** (keyfob 24Hr result); or **EARLY** (result of the last 24Hrs without statistics).

Option	Instructions
	The following screens will appear: **Xxx: 24hr: <status>**[1] ↺ **Xxx: NOW: <status>**[1] Use ▶▶ to scroll between the device's families. To view additional information of the selected device, press OK. The following screens will appear: **Xxx <device name>**[1] ↺ **<location>**[1]. If the control panel receives information via a repeater, it will be displayed as follows: **Xxx <device name>**[1] ↺ **<location>**[1] ↺ **RPx:Via Repeater** ↺
SHOW RF PROBLEMS	You can view only the devices which have RF problems. ***Note:*** *This option is available only after testing process was done.* Press OK to view the devices' status. The following screens will appear: **Xxx: 24hr: <status>**[1] ↺ **Xxx: NOW: <status>**[1] Use ▶▶ to scroll between the device's families. To view additional information of the selected device, press OK. The following screens will appear: **Xxx <device name>**[1] ↺ **<location>**[1]. If the control panel receives information via a repeater, it will be displayed as follows: **Xxx <device name>**[1] ↺ **<location>**[1] ↺ **RPx:Via Repeater** ↺
<OK> TO END	Select to terminate the diagnostics test.

4.9.3 Testing the GSM module

The PowerMaster-360R enables to test the panel's integrated GSM module.

07:DIAGNOSTICS OK ▶▶ ··· ▶▶ **GSM/GPRS** OK **Please wait…**

Enter the **GSM/GPRS** menu, and press OK to initiate the GSM diagnostic test. Upon test completion, the PowerMaster-360R will present the test result.

The following table presents the test result messages.

Message	Description
Unit is OK	GSM / GPRS is functioning correctly
GSM comm. loss	GSM/GPRS module does not communicate with the Panel
Pin code fail	Missing or wrong PIN code. (Only if SIM card PIN code is enabled.)
GSM net. fail	Unit failed with registration to local GSM network.
SIM card fail	SIM not installed or SIM card failure.
GSM not detected	GSM auto enroll failed to detect GSM/GPRS module.
No GPRS service	The SIM card does not have the GPRS service enabled.
GPRS conn. fail	Local GPRS network is not available or, wrong setting to GPRS APN, user and/or password.
Srvr unavailable	PowerManage receiver cannot be reached – Check the Server IP
IP not defined	Server IP #1 and #2 are not configured.
APN not defined	APN is not configured.
SIM card locked	After entering a wrong PIN code 3 consecutive times the SIM is locked. To unlock it enter a PUK number. The PUK number cannot be entered by the control panel.
Denied by server	PowerManage denies the connection request. Check that the panel is registered to PowerManage.

4.9.4 Testing the SIM number

You can test the SIM number to ensure that the SIM number was entered correctly in the control panel (see section 4.6.2) and to coordinate with the operator.

07:DIAGNOSTICS OK ▶▶ ··· ▶▶ **SIM NUMBER TEST** OK ···

Enter the **SIM NUMBER TEST** menu, select the IP server (out of two) used for the verification of the SIM and press OK. The server sends a test SMS to the panel.

If the panel receives the SMS, a **SIM# verified** message is displayed and the test ends successfully. If the SMS was not received for example there is a connection issue, a **SIM not verified** message is displayed.

During testing the following messages are displayed and can help troubleshoot problems:

Message	Description
SIM # verified	Test successful
SIM NOT verified	Test fails
SIM TEL. missing	Test fails because the panel SIM is not defined
GSM init	Test is in progress waiting for GSM modem to initialize
Connect srvr	Test is in progress waiting for connection to the server
Request SMS	Test is in progress requesting server to send sms
Wait for SMS	Test is in progress waiting to receive sms from server

4.9.5 Testing the broadband/PowerLink Module [1]

The Broadband diagnostic procedure enables a test of the communication of the Broadband Module (see section 4.6.7) with the PowerManage server and reports the diagnostic result. In case of communication failure, detailed information of the failure is reported.

07:DIAGNOSTICS OK ▶▶ ··· ▶▶ **BROADBAND MODULE** OK ··· **PLEASE WAIT…** **Unit is OK**

Notes:

1. *When the* OK *button is pressed, the test result may take up to 4 min. before it is displayed.*
2. *If the Broadband Module is not registered to the PowerMaster-360R, the menu BROADBAND MODULE will not be displayed.*

The following table presents the list of messages that may be reported:

Message	Description
Unit is ok	Broadband Module is functioning correctly.
Test aborted	The diagnostic test is aborted, as follows: • AC failure – Broadband Module is set to OFF mode. • Broadband Module has not completed the power-up procedure. In this case, the installer should wait a maximum of 30 seconds before re-testing.
Comm. loss	The RS-232 serial interface between the Broadband Module and the PowerMaster-360R failed.
Rcvr Ip missing	Receivers IP 1 and 2 settings are missing in the PowerMaster-360R.
Cable unplugged	The Ethernet cable is not connected to the Broadband Module.
Check lan config	This message appears in any of the following cases: • Incorrect Broadband Module IP has been entered. • Incorrect subnet mask has been entered. • Incorrect default gateway has been entered. • DHCP server failure.
Rcvr#1 UnReach. **Rcvr#2 UnReach.**	Receiver 1 or 2 is inaccessible, as follows: • Wrong receiver IP has been entered. • Receiver failure. • WAN Network failure.
Rcvr#1 UnReg. **Rcvr#2 UnReg.**	The PowerMaster-360R unit is not registered to IP receiver 1 or 2.
Timeout err.	Broadband Module does not respond to test result within 70 sec.
Invalid result	Broadband Module responds with a result code that is not recognized by the PowerMaster-360R.

[1] The name of the product is PowerLink4 IP Communicator

4.9.6 Testing the WLAN Module

The WLAN diagnostic procedure enables a test of the communication of the WLAN Module with the PowerManage server and reports the diagnostic result. In case of communication failure, detailed information of the failure is reported.

07:DIAGNOSTICS OK ▶▶ ··· ▶▶ **08: WLAN** OK ··· **PLEASE WAIT…** **Unit is OK**

The following table presents the list of messages that might be reported:

Message	Description
"Please wait…"	Test in progress
0 – "Success"	WLAN is ok
1 – "Wi-Fi disabled"	Wi-Fi client is not enabled
2 – "Router disconn."	No connection to router (no link, or wrong SSID or password)
3 – "DHCP failure"	Plink fail to gel IP from DHCP server (router)
4 – "Wrong password"	Wrong SSID or password
5 – "No WAN"	Plink fail to connect DNS or 8.8.8.8
6 – "Wi-Fi is OK", status of both servers. **"RCV1: OK RCV2: OK"** **"RCV1: OK RCV2: --"** **"RCV1: OK RCV2: ER"**	"ER" – No connection to server "--" – Empty IP Unreachable
7 –"Plink general err"	General Plink error
8 – "No Wi-Fi module"	No Wi-Fi module detected
9 – "Eth. connected"	Ethernet connection detected

4.10 User settings

This USER SETTINGS menu provides you with a gateway to the user settings through the regular user menus. Refer to the PowerMaster-360R User's Guide for detailed procedures.

4.11 Factory default

The FACTORY DEFLT menu enables you to reset the PowerMaster-360R parameters to the factory default parameters. To obtain the relevant parameters defaults, contact the PowerMaster-360R dealer. Reset factory default parameters as follows:

Step 1	Step 2	Step 3	Step 4	Step 5
Select 09:FACTORY DEFLT menu	Select <OK> to restore	Enter Installer Code	Resetting of factory default parameters is underway	

▶▶ ↬

09:FACTORY DEFLT OK **<OK> to restore** OK **ENTER CODE:** ■ OK **PLEASE WAIT…** ⮌ to Step 1

Notes:

1) For PowerMaster-360R with 2 installer codes, INSTALLER code and MASTER INSTALLER code, only the master installer code enables to perform the factory default function.

2) If the Soak Test is active, performing factory default will restart the Soak Test.

4.12 Serial number

The SERIAL NUMBER menu enables reading the system serial number and similar data for support purposes only. To read the system serial number and other relevant data proceed as follows:

Step 1	ⓘ	Step 2	ⓘ	Step 3
Select 10:SERIAL NUMBER menu	[1]	Click next repeatedly to view relevant data.	[2]	

▶▶ ↬ ▶▶ ↬

10:SERIAL NUMBER OK OK ⮌ to Step 1

	Definition
0907030000.	Control panel serial number
JS702766 R19.412	Control panel software version
PANEL ID: 18DD6	Control panel ID for PowerManage connectivity
J-702770 R19.412	Control panel default version
JS702767 R01.033	Control panel boot version
JS702768 R02.036	Control panel Remote Software Upgrade downloader version
PL8.0.92.3 raw	Displays the PowerLink software version
GE910 QUAD V3	Displays the cellular modem type, if installed.

4.13 Partitioning

4.13.1 General guidance – Partitioning menu

This menu allows you to enable/disable partitions in the system (for further details, see APPENDIX E).

4.13.2 Enabling and disabling partitions

To enable or disable the partition feature, proceed as follows:

Step 1	Step 2	Step 3	Step 4
Select 12:PARTITIONING menu	Select whether to Enable or Disable Partitions	Partitions are now enabled	

▶▶ ↬ ▶▶ ↬

12:PARTITIONING OK **Disable** ■ OK **Enable** ■ ⮌ to Step 1

⋮↓

Enable

4.14 Operation mode

Note: *The Operation Mode feature is applicable only in specific PowerMaster-360R variants.*

4.14.1 General guidance – Operation mode menu

This mode allows you to select an operation mode for the control panel according to specific compliance standards. Each operation mode has its own configuration.

4.14.2 Select setting

To select the desired operation mode, proceed as follows:

Step 1	Step 2	Step 3	Step 4
Select 13:OPERATION MOD menu	Enter 01:SELECT MODE	Select NORMAL, EN-50131, DD243, BS8243, INCERT or CP01	
▶▶ **13:OPERATION MOD** OK	▶▶ **01 SELECT MODE** OK	▶▶ **NORMAL** ■ OK	⮌ to Step 2

Note: *If **Normal / EN-50131 / INCERT** is selected, the control panel will operate according to OTHERS setup configuration (see section 4.13.6).*

4.14.3 BS8243 Setup

13:OPERATION MOD OK ▶▶ ··· ▶▶ **02:BS8243 SETUP** OK

Enter the **02:BS8243 SETUP** menu to configure its settings.

Option	Configuration instructions
01:DISARM OPTION	Define when it is possible to disarm the system: **entry/BS devs** (default) – By keypad after the entry delay has expired and if an alarm occurred in the system. By keyfob or KP-160 PG2 at all times. **entry/all devs** - During entry delay, when the system is armed AWAY, by all devices. When not in entry delay by keyfob or KP-160 PG2 only. **entry/DD devs** - During entry delay, when the system is armed AWAY, by using the keyfob or KP-160 PG2. Keypads cannot disarm at all. **anytime/all dev** – At any time and by all devices.
02:ENTRY ALARM	Define whether the system will report a confirmed alarm during an entry delay (see CONFIRM ALARM below). **BS8243** (default) – An alarm initiated by another detector during the entry delay is regarded as a confirmed alarm. An additional 30 seconds delay is added to the entry delay for reporting the event (does not affect the Abort Time, see section 4.5.4). **BS8243 no cnfrm** - The panel will not send any confirmed alarm once a delay zone has been activated, until the control panel is disarmed. **DD243** - An alarm initiated by another detector during the entry delay is not regarded as a confirmed alarm. **normal mode** - The control panel will report a confirmed alarm for the second alarm that is triggered from a different zone within the confirmation time. There are no alarm restrictions during entry delay or for the delay zone.
03:END EXIT MODE	Define how the exit delay is terminated or restarted according to the following options: **door/fob only** (default) - When the door is closed, or by pressing the AUX button on the keyfob[1], whichever first. **restart>reentry** - Exit delay restarts when the door is reopened during exit delay. The restart occurs once only. Restarting the exit delay is helpful if the user re-enters immediately after going out to retrieve an item that was left behind. **door/fob/timer** - When the door is closed, by pressing the AUX button on the keyfob[1], or when the exit delay has expired, whichever first. **fob/timer** - By pressing the AUX button on the keyfob[1], or when the exit delay has expired, whichever first.

[1] Applies only when the keyfob is defined as skip exit delay (for further details, see the keyfob's User's Guide)

Option	Configuration instructions
04:FOB/KP PANIC	Define the devices that cannot trigger a panic alarm. **BS8243** (default) – KF-234 PG2 and KF-235 PG2. **all** - All devices can trigger a panic alarm
05:CONFIRM ALARM	Define a specific time period that if 2 successive alarms occur, the second alarm will be considered as a **confirmed alarm**, (see RPT CNFM ALRM below). Options: **in 30** (default)/**45**/**60**/**90 minutes**
06:CONFIRM PANIC	A confirmed panic alarm is reported if one of the following occurs within the confirmation time: a) A second panic device is activated. b) A second panic alarm on the same device is activated. c) A tamper event is activated (not from the zone / device that initiated the panic alarm). Options: **in 4**/**8**/**12**/**20** (default)/**24 hours** and **disabled**
07:RPT CNFM ALRM	Define whether the system will report a confirmed alarm. **enable + bypass** (default) - The system will report a confirmed alarm and will bypass all alarmed open zones when the siren ends or when the confirmation timer expires. **disable** - The system will not report a confirmed alarm. **enable** - The system will report a confirmed alarm.
08:ENTRY DELAY 1 **09:ENTRY DELAY 2**	Two different entry delays allow the user to enter the protected site (while the system is in the armed state) via 2 specific doors and routes without causing an alarm. Following entry, the user must disarm the control panel before the entry delay expires. Slow-rate warning beeps start sounding once the door is opened, until the last 10 seconds of the delay, during which the beeping rate increases. Locations No. 1 (entry delay 1) and 2 (entry delay 2) allow you to program the length of these delays. Options: **10**/**15**/**30**(ENTRY DELAY 1 *default*)/**45**/**60**(ENTRY DELAY 2 *default*) **seconds**; **3**/**4 minutes**
10:ABORT TIME	The PowerMaster-360R can be configured to provide a delay before reporting an alarm to the Monitoring Station (not applicable to alarms from FIRE, 24H SILENT and EMERGENCY zones). During this delay period, the siren sounds but the alarm is not reported. If the user disarms the system within the delay time, the alarm is aborted. You can activate the feature and select the Abort Time interval. Options: **in 00** (default in USA)/**15**/**30** (default)**/45/60 seconds**; **in 2**/**3**/**4 minutes**
11:CANCEL ALARM	The PowerMaster-360R can be configured to provide a Cancel Alarm time window that starts upon reporting an alarm to the Monitoring Station. If the user disarms the system within that cancel alarm time, a cancel alarm message is sent to the Monitoring Station indicating that the alarm was canceled by the user. Options: **not active** (default in USA); **in 1**/**5** (default)/**15**/**60 minute(s)** and **in 4 hours**.

4.14.4 DD243 Setup

13:OPERATION MOD OK ▶▶ … ▶▶ **03:DD243 SETUP** OK

Enter the **03:DD243 SETUP** menu to configure its settings.

Option	Configuration instructions
01:DISARM OPTION	Define when it is possible to disarm the system: **entry/wl+awy kp** – By the control panel when the system is armed AWAY. By keyfob or KP-160 PG2 during entry delay only. **entry/all devs** - During entry delay, when the system is armed AWAY, by all devices. When not in entry delay by keyfob or KP-160 PG2 only. **entry/DD devs** (default) - During entry delay, when the system is armed AWAY, by using the keyfob or KP-160 PG2. Keypads cannot disarm at all. **anytime/all dev** – At any time and by all devices.

Option	Configuration instructions
02:ENTRY ALARM	Define whether the system will report a confirmed alarm during an entry delay (see CONFIRM ALARM below). **DD243** (default) - An alarm initiated by another detector during the entry delay is not regarded as a confirmed alarm. **normal mode** - The control panel will report a confirmed alarm for the second alarm that is triggered from a different zone within the confirmation time. There are no alarm restrictions during entry delay or for the delay zone.
03:END EXIT MODE	Define how the exit delay is terminated or restarted according to the following options: **door/fob only** - When the door is closed, or by pressing the AUX button on the keyfob[1], whichever first. **restart>reentry** - Exit delay restarts when the door is reopened during exit delay. The restart occurs once only. Restarting the exit delay is helpful if the user re-enters immediately after going out to retrieve an item that was left behind. **door/fob/timer** - When the door is closed, by pressing the AUX button on the keyfob[1], or when the exit delay has expired, whichever first. **fob/timer** (default) - By pressing the AUX button on the keyfob[1], or when the exit delay has expired, whichever first.
04:FOB/KP PANIC	Define the devices that cannot trigger a panic alarm. **DD243** (default) – KF-234 and KF-235 PG2. **all** - All devices can trigger a panic alarm
05:CONFIRM ALARM	Define a specific time period that if 2 successive alarms occur, the second alarm will be considered as a **confirmed alarm**, (see RPT CNFM ALRM below). Options: **in 30**/**45**/**60**(default)/**90 minutes**
06:CONFIRM PANIC	A confirmed panic alarm is reported if one of the following occurs within the confirmation time: a) A second panic device is activated. b) A second panic alarm on the same device is activated. c) A tamper event is activated (not from the zone / device that initiated the panic alarm). Options: **in 4**/**8**/**12**/**20**(default)/**24 hours** and **disabled**
07:RPT CNFM ALRM	Define whether the system will report a confirmed alarm. **enable + bypass** (default) - The system will report a confirmed alarm and will bypass all alarmed open zones when the siren ends or when the confirmation timer expires. **disable** - The system will not report a confirmed alarm. **enable** - The system will report a confirmed alarm.
08:ENTRY DELAY 1 **09:ENTRY DELAY 2**	Two different entry delays allow the user to enter the protected site (while the system is in the armed state) via 2 specific doors and routes without causing an alarm. Following entry, the user must disarm the control panel before the entry delay expires. Slow-rate warning beeps start sounding once the door is opened, until the last 10 seconds of the delay, during which the beeping rate increases. Locations No. 1 (entry delay 1) and 2 (entry delay 2) allow you to program the length of these delays. Options: **10**/**15**/**30**(ENTRY DELAY 1 *default*)/**45**/**60**(ENTRY DELAY 2 *default*) **seconds**; **3**/**4 minutes**
10:ABORT TIME	The PowerMaster-360R can be configured to provide a delay before reporting an alarm to the monitoring station (not applicable to alarms from FIRE, 24H SILENT and EMERGENCY zones). During this delay period, the siren sounds but the alarm is not reported. If the user disarms the system within the delay time, the alarm is aborted. You can activate the feature and select the Abort Time interval. Options: **in 00** (default in USA)/**15**/**30** (default)/**45/60 seconds**; **in 2/3/4 minutes**
11:CANCEL ALARM	The PowerMaster-360R can be configured to provide a Cancel Alarm time window that starts

[1] Applies only when the keyfob is defined as skip exit delay (for further details, see the keyfob's User's Guide)

Option	Configuration instructions
	upon reporting an alarm to the Monitoring Station. If the user disarms the system within that cancel alarm time, a cancel alarm message is sent to the Monitoring Station indicating that the alarm was canceled by the user.
	Options: **not active** (default in USA); **in 1/5** (default)/**15/60 minute(s)** and **in 4 hours**.

4.14.5 CP01 Setup

13:OPERATION MOD OK ▶▶ ··· ▶▶ **CP01 SETUP** OK

Enter the **04:CP01 SETUP** menu to configure its settings.

Option	Configuration instructions
01:DISARM OPTION	Certain regulations require that when the system is armed in AWAY mode, it may not be disarmed from the outside of the house (such as by keyfobs) before entering the protected premises and activating an Entry Delay zone. To answer this requirement, the PowerMaster-360R provides you with the following configurable options to disarm the system: **any time** (default) – the system can be disarmed at all times from all devices. **on entry wrless** – During entry delay, the system can be disarmed only using keyfob or prox operated devices. **entry + away kp.** – During entry delay by code, the system can be disarmed only using PowerMaster-360R Virtual or Touch Keypad . **on entry all.** – During entry delay, the system can be disarmed using keyfobs or by code using the PowerMaster-360R Virtual or Touch Keypad.
03:END EXIT MODE	Define how the exit delay is terminated or restarted according to the following options: **restart+arm home** (default) – During exit delay if the door was not opened, the alarm system will be armed HOME instead of armed AWAY. **restart>reentry** - Exit delay restarts when the door is reopened during exit delay. The restart occurs once only. Restarting the exit delay is helpful if the user re-enters immediately after going out to retrieve an item that was left behind. **door/fob/timer** - When the door is closed, by pressing the AUX button on the keyfob[1], or when the exit delay has expired, whichever first. **fob/timer** - By pressing the AUX button on the keyfob[1], or when the exit delay has expired, whichever first.
05:CONFIRM ALARM	Define a specific time period that if 2 successive alarms occur, the second alarm will be considered as a confirmed alarm, (see **RPT CNFM ALRM** below). Options: **disable** (default in USA); **in 30/45/60**(default)/**90 minutes**
07:RPT CNFM ALRM	Define whether the system will report a confirmed alarm. **report disabled** (default) - The system will not report a confirmed alarm. **report enabled** - The system will report a confirmed alarm.
08:ENTRY DELAY 1 **09:ENTRY DELAY 2**	Two different entry delays allow the user to enter the protected site (while the system is in the armed state) via 2 specific doors and routes without causing an alarm. Following entry, the user must disarm the control panel before the entry delay expires. Slow-rate warning beeps start sounding once the door is opened, until the last 10 seconds of the delay, during which the beeping rate increases. Locations No. 1 (entry delay 1) and 2 (entry delay 2) allow you to program the length of these delays. Options: **30** (default)/**45/60 seconds**; **3/4 minutes**
10:ABORT TIME	The PowerMaster-360R can be configured to provide a delay before reporting an alarm to the monitoring station (not applicable to alarms from FIRE, 24H SILENT, EMERGENCY, GAS FLOOD and TEMPERATURE zones). During this delay period, the external siren will not sound and the alarm is not reported. If the user disarms the system within the delay time, the alarm is aborted. Options: **in 15** (default)/**30/45 seconds**

[1] Applies only when the keyfob is defined as skip exit delay (for further details, see the keyfob's User's Guide)

Option	Configuration instructions
11:CANCEL ALARM	Define the cancel alarm period that starts upon reporting an alarm to the Monitoring Station. If the user disarms the system within that time period, a cancel alarm message is sent to the Monitoring Station.
	Options: **in 5** (default)**/15/60 minutes**; **in 4 hours**
12:CNCEL ANOUNCE	Define whether a special beep will sound when an alarm cancel event is sent to the monitoring station.
	enable (default) and **disable**
13:ABORT ANOUNCE	Define that when the user disarms the system within the allowed abort interval a special beep will sound to indicate no alarm transmission.
	enable (default) and **disable**

4.14.6 Other setup

13:OPERATION MOD OK ▶▶ ··· ▶▶ **05:OTHERS SETUP** OK

Enter the **05:OTHERS SETUP** menu to configure its settings.

Option	Configuration instructions
01:DISARM OPTION	Certain regulations require that when the system is armed in AWAY mode, it may not be disarmed from the outside of the house (such as by keyfobs) before entering the protected premises and activating an Entry Delay zone. To answer this requirement, the PowerMaster-360R provides you with the following configurable options to disarm the system: **any time** (default) – the system can be disarmed at all times from all devices. **on entry wrless** – During entry delay, the system can be disarmed only using keyfob or prox operated devices. **entry + away kp.** – During entry delay by code, the system can be disarmed only using PowerMaster-360R Virtual or Touch Keypad. **on entry all.** – During entry delay, the system can be disarmed using keyfobs or by code using the PowerMaster-360R Virtual or Touch Keypad.
03:END EXIT MODE	The Exit Delay time can be further adjusted according to your preferred exit route. The control panel provides you with the following **Exit Mode** options: **A: normal** (default) - The exit delay is exactly as defined. **B: restart>reentry** - The exit delay restarts when the door is reopened during exit delay. The restart occurs once only. Restarting the exit delay is helpful if the user re-enters immediately after going out to retrieve an item that he left behind. **C: end by exit** - The exit delay expires (ends) automatically when the exit door is closed even if the defined exit delay time was not completed.
	Options: **normal** (default); **restart>reentry** and **end by exit.**
05:CONFIRM ALARM	Define a specific time period that if 2 successive alarms occur, the second alarm will be considered as a confirmed alarm, (see **RPT CNFM ALRM** below).
	Options: **disable** (default in USA); **in 30/45/60** (default)/**90 minutes**
07:RPT CNFM ALRM	Define whether the system will report a confirmed alarm. **report disabled** (default) - The system will not report a confirmed alarm. **report enabled** - The system will report a confirmed alarm.
08:ENTRY DELAY 1 **09:ENTRY DELAY 2**	Two different entry delays allow the user to enter the protected site (while the system is in the armed state) via 2 specific doors and routes without causing an alarm. Following entry, the user must disarm the control panel before the entry delay expires. Slow-rate warning beeps start sounding once the door is opened, until the last 10 seconds of the delay, during which the beeping rate increases. Locations No. 1 (entry delay 1) and 2 (entry delay 2) allow you to program the length of these delays.
	Options : **00/15** (ENTRY DELAY 2 default)/**30** (ENTRY DELAY 1 default)/**45/60 seconds**; **3/4 minutes**

Option	Configuration instructions
10:ABORT TIME	The PowerMaster-360R can be configured to provide a delay before reporting an alarm to the monitoring station (not applicable to alarms from FIRE, 24H SILENT and EMERGENCY zones). During this delay period, the siren sounds but the alarm is not reported. If the user disarms the system within the delay time, the alarm is aborted. You can activate the feature and select the Abort Time interval.
	Options: **in 00** (default in USA)/**15**/**30**(default)**/45/60 seconds**; **in 2/3/4 minutes**
11:CANCEL ALARM	The PowerMaster-360R can be configured to provide a Cancel Alarm time window that starts upon reporting an alarm to the Monitoring Station. If the user disarms the system within that cancel alarm time, a cancel alarm message is sent to the Monitoring Station indicating that the alarm was canceled by the user.
	Options: **not active** (default in USA); **in 1**/**5** (default)/**15**/**60 minute(s)** and **in 4 hours**.

5. Periodic test

5.1 General guidance

This mode provides you with the means to conduct a periodic test of all system sirens, detectors, keyfobs, keypads, repeaters and other peripheral devices, via the **PERIODIC TEST** menu, at least once a week and after an alarm event.

When you are instructed to perform a periodic test, walk throughout the site to check the detectors / sensors (except for Temperature Sensors). When a detector/sensor is triggered into alarm, its name, number and the alarm reception level should be indicated (for example, **Bathroom**, **Z19 strong**) and the buzzer should sound according to the alarm reception level (1 of 3). Each device should be tested according to the device Installation Instructions.

To enter the **PERIODIC TEST** menu and to conduct a periodic test, proceed as follows:

Step 1	ⓘ	Step 2	ⓘ
READY	[1]	Select the test to be performed	[2]
▶▶ ↓			
PERIODIC TEST (enter installer / master code)	OK	**SIRENS TEST** **TEMP/LIGHT TEST** **TEST ALL DEVICES** **TEST ONE DEVICE**	OK

ⓘ	ⓘ ***– Periodic Test***
[1]	Not including Siren and Temperature Sensors
[2]	After reviewing all untested devices the control panel will read **<OK> TO END**. You can now do one of the following: press OK to abort the testing procedure; press ▶▶ to continue the testing procedure; or press 🔓 to exit the testing procedure.

5.2 Conducting a periodic test

The PowerMaster-360R enables you to conduct the periodic test in five parts:

Siren Test: Each siren of the system is automatically activated for 3 seconds (outdoor sirens with low volume).

Temp/Light Test: For devices with temperature sensing, the panel displays the temperature of each zone in Celsius or Fahrenheit. For devices that have both temperature and light sensing, the panel displays the temperature and light intensity of each zone.

Test all devices: All devices are tested.

Other Device Test: Each of the other devices in the system is activated by the installer and the display indicates which devices were not yet tested. The **it's me** indication helps to identify the untested devices if necessary. A counter also indicates the number of devices that remain untested.

Email Test: Generates an event to be sent to the predefined private email addresses.

READY OK ▶▶ ··· ▶▶ **PERIODIC TEST** OK ▶▶ ··· ▶▶ **MENU item** OK

To conduct a periodic test, make sure the system is disarmed and then enter the **PERIODIC TEST** menu using your installer code (8888 by default) or master installer code (9999 by default). Immediately after entering the **PERIODIC TEST** menu, all the LEDs on the panel will momentarily light (LED test).

Option	Instructions
SIRENS TEST	You can test wireless sirens and strobes and sirens of smoke sensors. To initiate the siren test, press ⓘ OK. The display now reads **SIREN N**. **N** indicates the zone location assigned to the siren that is currently being tested. The first siren enrolled in the panel sounds for 3 seconds after which the PowerMaster-360R system will automatically repeat the procedure for the next siren enrolled in the system until all sirens are tested. You should listen to the sirens sounds and make sure that all sirens sound. Once all the sirens have been tested, the control panel will now test the sirens of smoke sensors that are enrolled in the alarm system. The display now reads **Zxx: SMOKE SIREN**, where **Zxx** indicates the zone number of the smoke sensor, and alternates with **<OK> TO CONTINUE**. During this time, the siren of the tested smoke sensor will sound for up to one minute. Press ⓘ OK to test the siren of the next smoke sensor. When the sirens test is complete, the display reads **SIREN TESTS END**. Press the ⓘ OK

Option	Instructions
	or the ▶▶ button to confirm the test.
TEMP/LIGHT TEST	The control panel reads the temperature and light intensity of the zone. When testing, all previous temperature and light results from sensors are cleared. To display the temperature and light intensity of zones on the control panel, press OK. After 20 seconds the control panel reads the temperature of the zone. If there is no result the following message is displayed "Zxx TEMP: No TST". The control panel reads the light intensity of each zone. The light level indication is dynamic that is if a detector has only two light threshold defined the following is displayed on the panel: • For 100 % light: LIGHT (**) • For complete darkness: LIGHT () If there is no light result the following message is displayed "Zxx LIGHT: No TST" The display alternates between the temperature, light, sensor number and the sensor location, as in the following example: **Z01 24.5°C** > **Z01: LIGHT (**) > Z01: Sensor number** > R**oom location**. Repeatedly click the ▶▶ button to review the temperature and light intensity of each zone. When the temperature and light of all zones is reviewed, the display reads **DEVICE TESTS END**. Press the OK or the ▶▶ button to confirm the test and then move to the next step to test the other devices.
TEST ALL DEVICES	You can test all devices in one procedure. While in **TEST ALL DEVICES**, press OK to initiate the test. The control panel now reads **NOT TESTED NNN**. **N** indicates the number of enrolled devices in the control panel that have not been tested. This number automatically drops one count for every tested device. When the **NOT TESTED NNN** screen appears, walk throughout the site to test the detectors / sensors or press any key of the selected handheld device to initiate the test. After a device has been activated, the control panel reads **Zxx IS ACTIVATED** and the **N** indicator drops one count. Pressing OK during the testing process will display details of each device that has not yet been tested. The control panel reads the device number, followed by the device type (for example, Contact Sensor, Motion Sensor or Keyfob) and followed by the device location. At this stage, pressing any one of the following keys will open the following options: **1.** Press ▶▶ to view details of the next untested device. **2.** Press 🔒 to exit the test process. During testing, you can also check the signal strength indication of each device according to the number of LED blinks of the device, (for further details, refer to the device Installation Instructions). After all devices have been tested, the control panel reads **DEVICE TESTS END**.
TEST ONE DEVICE **→CONTACT SENSORS** **→MOTION SENSORS** **→GLASSBREAK SENS.** **→SHOCK SENSORS**	Select a specific device group you wish to test. For example, Motion Sensors. Press OK to enter the **TEST ONE DEVICE** sub menu and use ▶▶ to scroll through the device families. Press OK to enter the < device family > sub menu. For example: **MOTION SENSORS**. The following screens will appear: **Xxx:<device name>** ⮌ **<location>** Where **Xxx** indicates the device number. If there is no device, the following screen will appear: **NO EXISTING DEV.**. Press OK to test the selected device. The following screen will appear: **Z01 ACTIVATE NOW**. Walk throughout the site to test the detectors / sensors or press any key of the selected handheld device to initiate the test. During testing, you can also check the signal strength indication of each device, (for further details, refer to the device Installation Instructions). At the end of the test process the panel will revert to: **TEST ONE DEVICE**.

Option	Instructions
	To test the microwave range of the dual detector: **1.** Press OK to enter the **TEST ONE DEVICE** sub menu and use ▶▶ to navigate to **MOTION SENSORS**. **2.** Press OK; the following screens will appear: **Z01:Motion Sens** ⮌ **<location>**. **3.** Press ▶▶ continuously to select a different zone number. **4.** Press OK; If the selected device is Tower-32AM PG2, the following screens will appear: **<OK MW ADJUST>** ⮌ **<NEXT> TEST ONE**. To test the microwave range, go to step 5. To test a different microwave range, go to step 7. **5.** Press ▶▶; the following screen will appear: **ACTIVATE MW NOW**. **6.** Activate the device; the screen will return to **TEST ONE DEVICE**. You can now repeat the procedure for another dual detector. **7.** Press OK to select the sensitivity setting. **8.** Press ▶▶ continuously to select between **Minimum** (default), **Medium** or **Maximum** **9a**. Press OK; the panel will receive an acknowledge from the device that is indicated by a black box next to the selected setting. Thereafter, the screen momentarily changes to **ACTIVATE MW NOW** and then returns to the selected setting. **9b**. If you press ⌂, the adjustment procedure ends. **Important**: The procedure mentioned above is for testing purposes only and does not change the detector settings. The settings must be saved through the MODIFY DEVICES menu. **To test the shock detector:** **1.** Press OK to enter the **TEST ONE DEVICE** sub menu and use ▶▶ to navigate to **SHOCK SENSORS**. **2.** Press OK; the following screens will appear: **Zxx:Shk+AX+CntG3**[1] ⮌ **<location>**. **3.** Press ▶▶ continuously to select a different zone number. **4.** Press OK; the following screens will appear: **Zxx ACTIVATE NOW** ⮌ **SHOCK NOT ACTIV**. ⮌ **CNTACT NOT ACTIV** ⮌ **AUXIL. NOT ACTIV**. ***Note:*** *The above screens are the full range of screens that can appear and indicate the inputs that have not yet been activated. However, since there are various models of the shock detector, not all of these screens will appear on some models.* **5.** At this stage, activate each input of the shock detector in turn. **To test motion detector with integrated camera (Next CAM PG2 or TOWER CAM PG2):** **1.** Press OK to enter the **TEST ONE DEVICE** sub menu and use ▶▶ to navigate to **MOTION SENSORS**. **2.** Press OK; the following screens will appear: **Z01:Motion Sens** ⮌ **<location>**. **3.** Press ▶▶ continuously to select a different zone number. **4.** Press OK; the following screen will appear: **Zxx ACTIVATE NOW**. **5.** Activate the input of the detector; the following screens will appear: **<Zxx IS ACTIVATE>** ⮌ **<OK> SEND IMAGE**.
E-MAIL TEST	To test emails, proceed as follows: While in **E-MAIL TEST**, press OK to initiate the test. The following screen will appear: **Please wait…** and at the termination of the test will

[1] Depending on shock detector model, one of the following may appear instead: **Zxx:Shk+AX** / **Zxx:Shk+CntG3** / **Zxx:Shk+CntG2**.

Option	Instructions
	change to **<Pls chck MailBox>**. Check the private email inbox to view the sent email. ***Note:*** ***1.*** *For test success, the event must first reach the server before the server can send the email to the user's inbox.* ***2.*** *Since a Burglary alarm is sent, an alarm event must be configured for reporting events (see sections 4.6.3 Configuring Events Reporting to Monitoring Stations and 4.6.4 Configuring Events Reporting to Private Users).*

6. Maintenance

6.1 Handling system faults

Fault	What it means	Possible Solution
1-WAY	The control panel cannot configure or control the device. Battery consumption increases.	• Make sure the device is physically present. • Check the display for device faults, for example, low battery. • Use RF diagnostics to check the current signal strength and during the last 24 hours. • Open the device cover and replace the battery or press the tamper switch. • Install the device in a different location. • Replace the device.
AC FAILURE	There is no power to gas sensor	Make sure that the AC/DC adapter is connected properly
AC SUPPLY FAILURE	There is no power and the system is working on backup battery power	Make sure that the AC/DC adapter is connected properly
CLEAN ME	The fire detector must be cleaned	Use a vacuum cleaner to clean the detector air vents occasionally to keep them free of dust.
COMM. FAILURE	A message could not be sent to the monitoring station or to a private telephone or a message was sent but was not acknowledged	• Check telephone cable connection • Check that correct telephone number has been dialed. • Dial Monitoring Station to check whether or not events are received.
CPU LOW BATTERY	The backup battery within the control panel is weak and must be replaced. See section 6.2, Replacing the Backup Battery.	• Check that AC power is available to the Panel. • If the problem exists for more than 72 hours, replace the battery pack
CPU TAMPER OPEN	The control panel was physically tampered with or its cover was opened, or it was removed from wall.	The control panel is not closed properly. Open the control panel and then close it.
GAS TROUBLE	Gas detector failure	Gas detector: Disconnect and then put back the AC power supply connector CO Gas detector: Replace the detector
GSM NET FAIL	The GSM communicator is not able to connect to the cellular network.	• Move the Panel and GSM unit to another location. • Enter and exit the Installer Mode menu • Disconnect GSM unit and install it again

Fault	What it means	Possible Solution
		• Replace SIM card • Replace the GSM unit
JAMMING	A radio-frequency signal which is blocking communication channel of sensors and control panel is detected.	Locate the source of interference by switching off any wireless devices (cordless telephones, wireless ear plugs, etc.) in the house for 2 minutes then check if trouble continues. Use also RF diagnostics to check signal strength.
LOW BATTERY	The battery in a sensor, keyfob or wireless commander is near the end of its useful life.	• For AC powered devices, check that AC power is available and connected to the device. • Replace the device battery.
MISSING	A device or detector has not reported for some time to the control panel.	• Make sure the device is physically present. • Check the display for device faults, for example, low battery. • Use RF diagnostics to check the current signal strength and during the last 24 hours. • Replace the battery. • Replace the device.
NOT NETWORKED	A device was not installed or not installed correctly, or, cannot establish communication with the control panel after installation.	• Make sure the device is physically present. • Use RF diagnostics to check the current signal strength and during the last 24 hours. • Open the device cover and replace the battery or press the tamper switch. • Enroll the device again.
RSSI LOW	The GSM communicator has detected that GSM network signal is weak	Move the Panel and GSM unit to another location.
SIREN AC FAILURE	There is no power to the siren	Make sure that the AC/DC adapter is connected properly
TAMPER OPEN	The sensor has an open tamper	Close sensor tamper
TROUBLE	The sensor reports trouble	Replace the sensor
SOAK TEST FAIL	Detector alarms when in Soak Test mode	If you wish to continue the Soak Test, no further action should be taken. If you wish to abort the Soak Test, disable the Soak Test, see section 4.4.6 for details.

6.2 Replacing the backup battery

Replacement and first-time insertion of battery pack is similar, see Figure 3.1b.
Separate the panel from the base, see section 3.2 Installing the PowerMaster-360R battery and cables for details. After inserting the new battery pack correctly, return the panel to the base and place the screw in the locked position. The TROUBLE indicator is extinguished. However, the MEMORY message will now blink in the Virtual or Touch Keypad display. This message is caused by the tamper alarm that is triggered when you remove the panel from the base. Clear the message by arming the system and immediately disarming the system.

6.3 Replacing and relocating detectors

Whenever maintenance work involves replacement or re-location of detectors, always perform **a full diagnostic test according to section 4.8.**
Remember! A poor signal is not acceptable.

6.4 Annual system check

Note: *The PowerMaster-360R system must be checked by a qualified technician at least once every three (3) years (preferably every year).*

The annual system check is designed to ensure proper operation of the alarm system by performing the following checks:

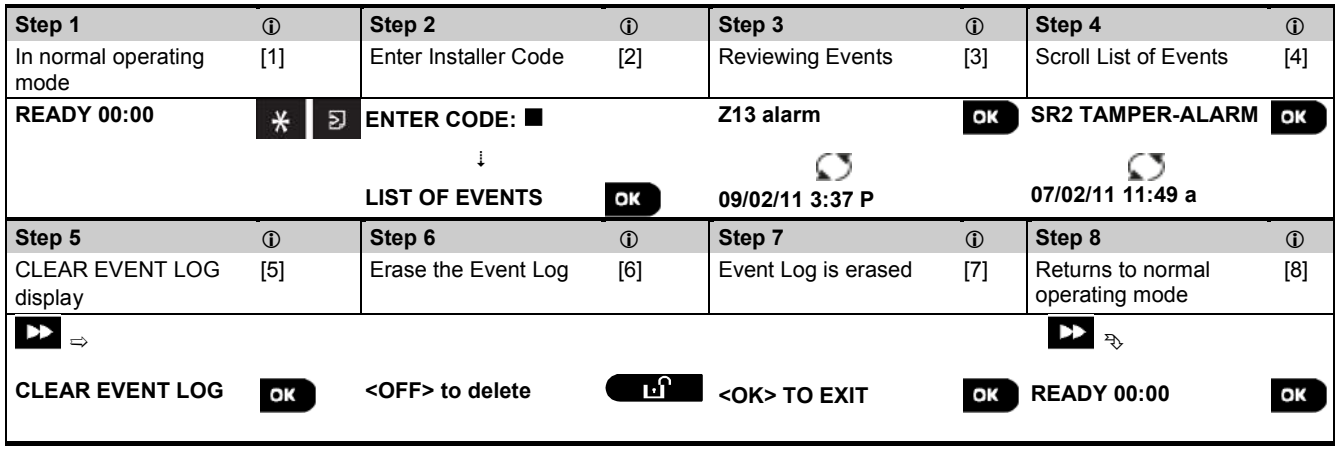
- Periodic test
- Arm/disarm function
- No trouble messages are displayed on the Virtual or Touch Keypad
- The clock displays the correct time
- Reporting: generating an event to be transmitted to the Monitoring Station and to the user.

7. Reading the event log

Up to 100 events are stored in the event log. You can access this log and review the events, one by one. If the event log fills up completely, the oldest event is deleted upon registration of each new event. The date and time of occurrence are stored for each event.

Note: *Up to 1000 events are stored in the event log that can be reviewed via the Remote Programmer PC software application or by the remote PowerManage server.*

When reading the event log, events are shown in chronological order - from the newest to the oldest. Access to the event log is provided by clicking the * button and not through the Installer Mode menu. The reading and erasing process of the event log is shown below.



ⓘ - *Reading Events*

[1] While the system is in the normal operating mode, press the * key.

Reading the Event Log

[2] Enter the current Installer Code and then press OK to enter **LIST OF EVENTS**.

[3] The latest event is shown.
The event is displayed in two parts, for example, **Z13 alarm** then **09/02/10 3:37 P**.
Note: *In Soak Test mode, the panel displays the alarmed zone and alternates with* ***Zxx:Soak T.Fail****.*

[4] Press OK repeatedly to scroll through the list of events.

Erasing and Exiting the Event Log:

[5] From anywhere within the event log, press the ▶▶ button and then press OK.

[6] At this stage in the procedure, clicking the 🏠 or 🔓 buttons will take you to **<OK> TO EXIT** without erasing the event log. Clicking the ▶▶ button will revert to **CLEAR EVENT LOG**.
Press the 🔓 button to erase the event log.

[7] The system erases the event log

[8] Press OK to revert to normal operating mode.

Clicking the 🏠 button repeatedly at any stage in the procedure takes you one level up with each click.
Clicking the 🔓 button will take you to **<OK> TO EXIT**.

APPENDIX A. LED icons and keys

LED icons show the status of the PowerMaster-360R. Use the control keys to move through the menu items of the panel and the arming keys to arm or disarm the system. Other keys are designated for certain tasks for example, to review event logs.

LED Icons

LED	Function
	Power.
	Armed away – LED lights steadily. Armed home – LED blinks.
	Trouble condition.
	Active service to the server.
	Smart home service.
	WiFi connection.

Control keys

Key	Function
	**OFF:** Delete a device.
	**NEXT:** Advance from item to item within a menu.
	**BACK**: Move one step back within a given menu.
	**UP:** Move one level up in the menu or to return to previous setting step.
	**OK:** Review status messages one by one and also to select an option.
	**ESC:** Cancel operation.

Arming Keys

Key	Function
	**AWAY:** Arming when nobody is at home.
	**HOME:** Arming when people remain at home.
	**INSTANT:** Canceling the entry delay upon arming (AWAY or HOME).
	**DISARM / OFF:** Disarming the system and stopping alarms.

Other Keys

Key	Function
	Chime ON/OFF
	Reviewing the event log
	Emergency
	Fire
	Panic

Note: *The key icons are used within this document.*

APPENDIX B. User mobile application with PowerMaster-360R

B1. Security Only Via PowerManage

After establishing connection with the PowerManage server, the PowerMaster-360R appears as an entry in the PowerManage Panel List. The WEB Name is retrieved from the PowerMaster-360R's Panel ID.

The home/property owner can access the PowerMaster-360R security system on a mobile device using the PowerManage Interactive app (for arming/disarming, viewing event details, etc.). The system's URL is ***https://[PowerManage server IP address]/[Panel's WEB Name]***.

For example: with a PowerManage on IP 100.101.102.103 using HTTPS communication and a panel with Panel_ID 140613. The link to this panel's web portal will be: ***https://100.101.102.103/140613.***

Note: *Only PowerManage DNS name can be set.*

B2. Security and Smart Home using 3rd Party application

The home or property owner can access the PowerMaster-360R security and smart home system on a mobile device using a 3rd Party application. From the application you can arm or disarm the system, switch on or off lights, A/C, etc.).

APPENDIX C. Specifications

C1. Functional

Zones Number	64 wireless zones
Installer and User Codes	• 1 master installer (9999 by default)* • 1 installer (8888 by default)* • 1 master user, no. 1 (1111 by default) • Users nos. 2 – 48 • Latchkey users 5 - 8 * Codes must not be identical
Note: The PowerMaster-360R system allows you to authorize up to 48 people to arm and disarm the system by providing each with a unique 4 digit personal security code (code 0000 is not allowed, maximum number of variations of PIN codes for each user – 10000 for logical keys), and assigning them with different security levels and functionalities.	
Control Facilities	Virtual or Touch Keypad, wireless keyfobs and keypads
Arming Modes	AWAY, HOME, AWAY-INSTANT, HOME-INSTANT, FORCED, BYPASS.
Alarm Types	Silent, personal panic/emergency, burglary, gas (CO), and fire.
External Siren (bell) Timeout	Programmable (4 min. by default)
Supervision	Programmable time frame for inactivity alert
Special Functions	- Chime zones - Diagnostic test and event log. - Local and Remote Programming over Broadband and GPRS IP connections. - Calling for help by using an emergency transmitter. - Tracking inactivity of people.
Data Retrieval	Alarm memory, trouble, event log
Real Time Clock (RTC)	The control panel keeps and displays time and date. This feature is also used for the log file by providing the date and time of each event
Battery Test	Once every 10 seconds
PowerG Receiver Range	160 ft. (50 m) internal, 6500 ft. (2000 m) external
Connectors	**External:** • DC Power Jack • RJ-45 Ethernet Connector • Micro USB Connector **Internal:** • SIM Card Slot (part of GPRS Module) • Battery Backup Connector

C2. Wireless

RF Network	PowerG – 2-way synchronized Frequency Hopping (TDMA / FHSS)		
Frequency bands (MHz)	433 – 434	868 - 869	912 – 919
Hopping frequencies	8	4	50
Region	Worldwide	Europe	North America and selected countries
Encryption	AES-128		
Maximum Tx Power	10 dBm @ 433 MHz, 14 dBm @ 868 MHz		
GSM (MHz)	2G Band		3G Band
	850, 900, 1800, 1900		850[1], 900[2], 1900[1], 2100[2]
Z-Wave (MHz) (optional)	868.4, 908.4, 921.4		
Wi-Fi - optional	2.4 GHz. Wi-Fi client for event reporting. Wi-Fi Access Point for IP camera support only.		

[1] [2] Bands are determined by the cellular modem type

C3. Electrical

External AC/DC adapter	**Input:** AC 100-240V, 50/60 Hz, 0.4A **Output:** 5.1V DC 1.96A
Nominal supply voltage	5.1 V DC - 5.3 V DC
Current Drain	~ 200 mA standby, 1500 mA peak at full load**.**
Low Battery Threshold	3.8 V
Backup Battery Pack	3.7 V, 3000 mAh LIPO, maximum charging voltage is 4.2 V.
Backup Battery Time	12 Hours
Time to Charge	~ 15 Hours (80 %)
Siren Sound Acoustic output	>84 dB
Siren Timeout	4 minutes by default; 20 minutes maximum value
Peak current consumption in alarm sounding state	1500 mA
Peak current consumption in non-alarm sounding state	1300 mA
Average current consumption and peak current consumption	PG2 - 40/120 mA Z-WAVE - 30/40 mA WiFi - 400 mA Cellular - 25 mA/2A

C4. Communication

Communication	IP, Ethernet 10/100 (primary mode), and GPRS (secondary mode)
Monitoring Station Report	2 via PowerManage on IP and/or GPRS and/or Wi-Fi
Private Notifications	4 emails, 4 SMS numbers
Local Management Protocol to Windows PC and Android Mobile	USB
Report Destinations	2 Monitoring Stations, 4 private SMS telephones via the server and 4 emails

C5. Physical Properties

Operating Temperature Range	32°F to 120°F (0°C to 50°C)
Storage Temperature Range	5°F to 140°F (-15°C to 60°C)
Humidity	93% relative humidity, @ 30°C (86°F)
Size	158x114.5x36.5 mm (6.22x4.5x1.43 in.)
Weight	225g (8 Oz)
Color	White
Mounting	Wall mount indoor

C6. Peripherals and Accessory Devices

Modules – factory default (SKU)	**Default:** • **Base** IP and PowerG • **GSM:** 2G or 2G/3G **Optional:** • **WiFi:** 2.4 GHz • **Z-Wave:** 500 Series
Number of wireless devices	Accommodates more than 120 wireless devices: • Up to 64 zones • Up to 15 PIR cameras, 32 keypads, 32 keyfobs, 8 sirens, 4 repeaters
Wireless Devices and peripherals	**Pendants:** PB-101 PG2, PB-102 PG2 **Magnetic Contact:** MC-302 PG2, MC-302E PG2, MC-302EL PG2, MC-302V PG2 **Motion Detectors:** Next PG2; Next K9 PG2, TOWER-20 PG2, TOWER-32AM PG2, TOWER-32AM K9 PG2, TOWER-30AM PG2, TOWER-30AM K9 PG2, CLIP PG2, TOWER CAM PG2 **PIR Camera Detectors:** Next CAM PG2; Next CAM-K9 PG2 Note: A maximum of 15 PIR cameras are supported, but the panel will communicate to the Visonic PowerManage server only the first 10 clips received from the cameras. **Smoke Detector:** SMD-426 PG2, SMD-427 PG2 **Keyfob:** KF-234 PG2, KF-235 PG2 **Keypad:** KP-140 PG2/KP-141 PG2 (with proximity tag), KP-160 PG2 **Indoor Siren:** SR-720 PG2, SR-720B PG2 **Outdoor Sirens:** SR-730 PG2, SR-740 PG2, SR-740 HEX PG2 **Repeater:** RP-600 PG2 **Gas:** GSD-441 PG2, GSD-442 PG2 (CO detector) **Glass-break:** GB-501 PG2 **Temperature:** TMD-560 PG2 **Flood:** FLD-550 PG2, FLD-551 PG2 **Shock:** SD-304 PG2

APPENDIX D. Working with Partitions

Your alarm system is equipped with an integrated partitioning feature that can divide your alarm system into three distinct areas identified as Partition 1 through 3. A partition can be armed or disarmed regardless of the status of the other partitions within the system. Partitioning can be used in installations where shared security systems are more practical, such as a home office or warehouse building. When partitioned, each zone, each user code and many of your system's features can be assigned to Partition 1 to 3. Each user code is assigned with the list of partitions it is allowed to control in order to limit access of users to certain partitions.

When partitioning is enabled, menu displays are changed to incorporate the partition feature and also each device, user, and proximity tag has additional partitions menu, where it is assigned to certain partitions and excluded from others.

Note: *When Partition Mode is disabled, all zones, user codes, and features of the control panel will operate as in a regular unit. When partition mode is enabled, all zones, user codes, and features of the control panel are automatically assigned to Partition 1.*

D1. User Interface and Operation

Refer to the control panel User's Guide APPENDIX B. PARTITIONING for a detailed description of the user interface (Arming/Disarming, siren behavior, show function, etc.), and APPENDIX A for keyfobs and keypads operation in Partition Mode.

D2. Common Areas

Common areas are areas used as walkthrough zones to areas of 2 or more partitions. There may be more than one common area in an installation depending on the layout of the property. A common area is not the same as a partition; it cannot be armed / disarmed directly. Common areas are created when you assign a zone or zones to 2 or 3 partitions. Table A1 summarizes the behavior of the different zone types in a common area.

Table A1 – Common Area Definitions

Common area zone types	Definition
Perimeter	• Acts as defined only after the last assigned partition is armed AWAY or HOME. • In case that one of the partitions is disarmed, an alarm initiated from this zone is ignored for all assigned partitions.
Delay zones	• Delay zones will not trigger an entry delay unless all assigned partitions are armed. It is, therefore, not recommended to define delay zones as common areas.
Perimeter follower	• Act as defined only after the last assigned partition is armed AWAY or HOME. • In case that one of the partitions is disarmed, an alarm initiated from this zone is ignored for all assigned partitions. • In case that one of the common area assigned partitions is in a delay state (and the other partitions are armed), the alarm will behave as a perimeter follower for this partition only. The event will be ignored for other assigned armed partitions.
Interior	• Acts as defined only after the last assigned partition is armed AWAY. • In case that one of the partitions is disarmed or armed HOME, an alarm initiated from this zone is ignored for all assigned partitions.
Interior follower	• Acts as defined only after the last assigned partition is armed AWAY. • In case that one of the partitions is disarmed or armed HOME, an alarm initiated from this zone is ignored for all assigned partitions. • In case that one of the common area assigned partitions is in a delay state (and the other partitions are armed), the alarm will behave as an interior follower for this partition only. The event will be ignored for other assigned armed partitions.
Home / Delay	• Acts as a Perimeter-Follower type when all assigned partitions are armed AWAY. • Acts as a Delay type when at least one of the assigned partitions is armed HOME. • Will be ignored when at least one of the assigned partitions is disarmed.
Emergency; Fire; Flood; Gas; Temperature; 24-hour silent; 24-hour audible; Non-alarm	• Always armed.

Note: *A Soak Test of Common areas cannot be initiated when one of its partitions is armed. When Soak Test of a Common area is active, an alarm event is ignored unless all the partitions that are assigned to the zone are armed.*

APPENDIX E. Detector Deployment & Transmitter Assignments

E1. Detector Deployment Plan

Zone No.	Zone Type		Location		Chime (melody Location) or Off (*)	Sensor Type	Holder
	Default	Programmed	Default	Programmed			
1	Exit/Entry 1		Front Door				
2	Inter-Follow		Living Room				
3	Exit/Entry 2		Attic				
4	Perimeter		Back Door				
5	Perimeter		Child Room				
6	Inter-Follow		Office				
7	Inter-Follow		Dining Room				
8	Perimeter		Dining Room				
9	Perimeter		Kitchen				
10	Perimeter		Living Room				
11	Inter-Follow		Living Room				
12	Inter-Follow		Bedroom				
13	Perimeter		Bedroom				
14	Perimeter		Guest Room				
15	Inter-Follow		Master Bedroom				
16	Perimeter		Master Bedroom				

Zone Types: *1 = Exit / Entry 1 ✳ 2 = Exit / Entry 2 ✳ 3 = Home Delay ✳ 4 = Interior Follower ✳ 5 = Interior ✳ 6 = Perimeter ✳ 7 = Perimeter Follower ✳ 8 = 24hr Silent ✳ 9 = 24hr Audible ✳ 10 = Emergency ✳ 11 = Arming Key ✳ 12 = Non-Alarm ✳ 17 = Guard ✳ 18 = Outdoor.*

Zone Locations: *Note down the intended location for each detector. When programming, you may select one of 31 custom locations – see 02:ZONES/DEVICES menu).*

Notes:

All zones are chime off by default. Enter your own choice in the last column and program accordingly.

E2. Keyfob Transmitter List

Transmitter Data						AUX button Assignments
No.	Type	Holder	No.	Type	Holder	Skip exit delay or Arming instant
1			17			Indicate the desired function (if any)
2			18			
3			19			
4			20			
5			21			
6			22			
7			23			
8			24			
9			25			
10			26			
11			27			
12			28			
13			29			
14			30			
15			31			Skip exit delay ☐
16			32			Arming instant ☐

E3. Emergency Transmitter List

Tx #	Transmitter Type	Enrolled to Zone	Name of holder
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

E4. Non-Alarm Transmitter List

Tx #	Transmitter Type	Enrolled to Zone	Name of holder	Assignment
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

APPENDIX F. Event Codes

F1. Contact ID Event Codes

Code	Definition
101	Emergency
110	Fire
114	Heat
120	Panic
121	Duress
122	Silent
123	Audible
129	Confirm panic
131	Perimeter
132	Interior
133	24 Hour (Safe)
134	Entry/Exit
137	Tamper/CP
139	Burglary verified
140	General alarm
151	Gas alarm
152	Freezer alert
153	Freeze alert
154	Flood alarm
158	High temperature
159	Low temperature
180	Gas trouble
220	Guard sensor alarmed
301	AC loss
302	Low system battery
311	Battery disconnect
313	Engineer reset
321	Fuse
333	Expansion modem failure
344	RF receiver jam detect

Code	Definition
351	Telco fault
373	Fire detector trouble
374	Exit error alarm (zone)
350	Communication trouble
380	Sensor trouble
381	Inactive event
383	Sensor tamper
384	RF low battery
389	Sensor self-test failure
391	Sensor Watch trouble
393	Fire detector clean me
401	O/C by user
403	Auto arm
406	Cancel
408	Quick arm
412	Successful download/access
426	Door open event
441	Armed home
454	Fail to arm
455	Autoarm failed
456	Partial arm
459	Recent close event
570	Bypass
602	Periodic test report
607	Walk test mode
625	Time/Date change
627	Program mode entry
628	Program mode exit
641	Senior watch trouble

F2. SIA Event Codes

Code	Definition
AR	AC Restore
AT	AC Trouble
BA	Burglary Alarm
BB	Burglary Bypass
BC	Burglary Cancel
BJ	Burglary Trouble Restore
BR	Burglary Restore
BT	Burglary Trouble / Jamming
BV	Burglary Verified
BX	Burglary test
BZ	Inactive event
CF	Forced Closing
CG	Armed home
CI	Fail to Close
CL	Armed Away
CP	Auto Arm
CR	Recent Close
EA	Door Open
FA	Fire Alarm
FJ	Fire detector trouble
FR	Fire Restore
FT	Fire Detector Clean

Code	Definition
LT	Phone Line Trouble
LX	Local Programming Ended
OP	Opening Report
OT	Fail to Arm
PA	Panic Alarm
PR	Panic Restore
QA	Emergency Alarm
RN	Engineer Reset
RP	Automatic Test
RS	Remote Program Success
RX	Manual Test
RY	Exit from Manual Test
TA	Tamper Alarm
TE	Communicator restored to operation
TR	Tamper Restore
TS	Communicator taken out of operation
UJ	Detector mask restore
UT	Detector mask
WA	Flood alarm
WR	Flood alarm restore
XR	Sensor Battery Restore
XT	Sensor Battery Trouble

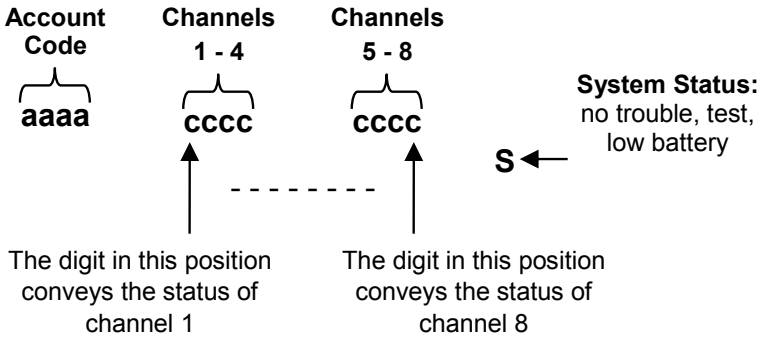
APPENDIX F. Event Codes

Code	Definition
FX	Fire test
GA	Gas alarm
GJ	Gas trouble restore
GR	Gas alarm restore
GT	Gas trouble
GX	Gas test
HA	Holdup Alarm (duress)
JT	Time Changed
KA	Heat alarm
KH	Heat alarm restore
KJ	Heat trouble restore
KT	Heat trouble
LB	Local Program
LR	Phone Line Restore

Code	Definition
YA	Fuse Fault
YH	Bell Restored
YI	Overcurrent Trouble
YM	System battery disconnect
YR	System Battery Restore
YT	System Battery Trouble / Disconnection
YX	Service Required
YZ	Service Completed
ZA	Freeze alert
ZH	Freeze alert restore
ZJ	Freezer alert restore
ZT	Freezer alert

F3. Understanding the Scancom Reporting Protocol Data Format

The SCANCOM data format consists of 13 decimal digits divided into 4 groups, from left to right, as shown on the right.
Each channel is associated with a specific event as follows:
1st C: Fire
2nd C: Personal attack
3rd C: Intruder
4th C: Open/close
5th C: Alarm cancel
6th C: Emergency
7th C: Second alarm
8th C: Trouble messages



Scancom Data Format

F4. SIA over IP - Offset for Device User

Type	Number Range In decimal	Example	Remarks
System reports	00	System tamper would report as 000	
Normal Zones/Detectors	1-499	Zone 5 would report as 005	
Keyfobs / Users /Tags	501-649	Keyfob/User number 101 would report 601	
Pendants	651-699	Pendant number 1 would report 651	
Keypads/ASU	701-799	Keypad number 8 would report 708	
Sirens	801-825	Siren number 9 would report 809	
Repeaters	831-850	Repeater number 4 would report 834	
Expanders/Bus devices	851-875	Device number 2 would report 852	
Troubles for: GSM BBA Plink Guard	 876 877 878 879	 GSM module network fail 876 BBA bus trouble 877	
	901- 999		For future use

APPENDIX G. Sabbath mode

G1. General guidance

The Sabbath Mode allows you to use the alarm system without violating the Sabbath. The basic feature of this alarm system is that the PIR sensors are not activated during Disarm mode.

The method of installation, as illustrated in the drawing below, is used in order to prevent transmission from the magnetic contact device. The MC-302E device is used only as a transmitting device to report the status of the door to the control panel. A wired magnetic contact is connected to the input of the MC-302E device and an open/close switch is connected in parallel to the MC-302E input.

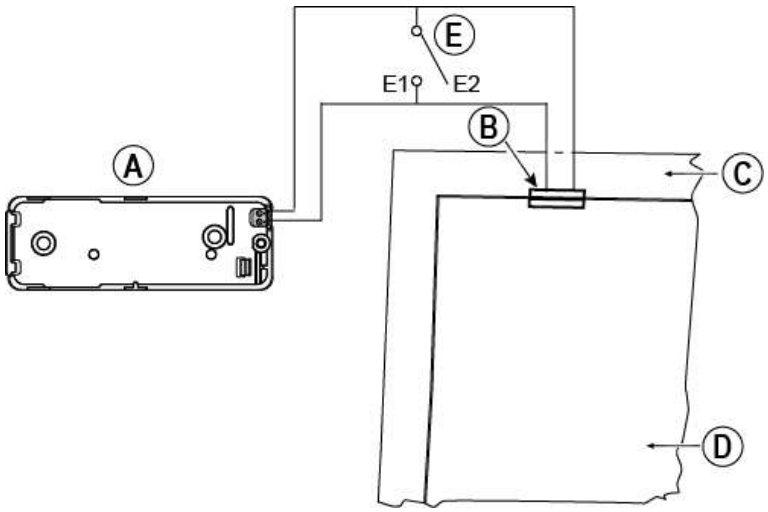
Note: *Before the Sabbath, closing the circuit neutralizes the detector's magnet. You can use the front door without violating the Sabbath. On the Sabbath day itself, you can open the switch to allow the door to be protected. This operation is permitted on the Sabbath and also when the control panel is armed.*

G2. Connection

1. Enroll an MC-302E to the PowerMaster-360R control panel (see section 4.4.2).
2. Configure the Input #1 setting option of the MC-302E to Normally Closed (refer to the MC-302E Installation Instructions, section 2.3).
3. Connect to the MC-302E a wired magnetic contact to be installed on the door and that is operated by opening/closing the door (see drawing below).
4. An open/close switch must be connected in parallel to the input of the MC-302E.

Wiring Setup

A. MC-302E device
B. Wired magnetic contact
C. Fixed frame
D. Moving part
E. Open/close switch
E1. Closed
E2. Open



G3. Arming the system by sabbath clock

1. Enroll an MC-302E to the PowerMaster-360R control panel (see section 4.4.2).
2. Configure the Zone Type to 11.Arming Key (see section 4.4.2)
3. Configure the Input #1 setting option of the MC-302E to Normally Open (refer to the MC-302E Installation Instructions, section 2.3).
4. From the 03:CONTROL PANEL menu, configure the 09:ARMING KEY setting option to arm HOME (see section 4.5.2).

Note: *When the alarm system is armed at night by a Sabbath clock, the open / close switch must be opened when the door is closed.*

APPENDIX H. Glossary

Abort Period: When an alarm is initiated, the internal sounder is activated first for a limited period of time which is the abort period set by the installer. If you cause an alarm accidentally, you can disarm the system within the abort period before the real sirens start and before the alarm is reported to the *remote responders.*

Alarm: There are 2 kinds of alarms:
Loud alarm - the external siren blares out constantly and the control panel reports the event.
Silent alarm - the sirens remain silent, but the control panel reports the event.

A state of alarm is caused by:
- Motion detected by a *motion detector* (when the system is in the Armed state)
- Change of state detected by a *magnetic contact detector* - a closed window or door is opened
- Detection of smoke by a *smoke detector,* detection of gas by a *gas detector* and detection of water based fluids by a *flood detector* (when in any state).
- *Tampering* with any one of the detectors

Arming: Arming the alarm system prepares the system to sound an alarm if a zone is violated. For example when motion is detected or a window or door is opened. The control panel may be armed in various modes (see *AWAY*, *HOME, INSTANT* and *LATCHKEY*).

Assigned: Refers to zones.

Associated: Refers to devices.

AWAY: This type of arming is used when the protected site is vacated entirely. All zones, *interior* and *perimeter* alike, are protected.

Chime Zones: Allow you to keep track of activity in the protected area while the alarm system is in the disarmed state. Whenever a chime zone is opened, the buzzer beeps twice via the Configuration device (PC or mobile). The buzzer does not beep, however, upon closing the zone (return to normal). Residences can use this feature to annunciate visitors or look after children. Businesses can use it to signal when customers enter the premises or when personnel enter restricted areas.
Note: *Your installer will never designate a 24-hour zone or a fire zone as a chime zone, because both zone types actuate an alarm if disturbed while the system is in the disarmed state.*

Although one zone or more are designated as chime zones, you can still enable or disable the chime function.

Communicators: Refers to communication channel, for example, GSM.

Control Panel: The control panel is a cabinet that incorporates the electronic circuitry and microprocessor that control the alarm system. It collects information from various sensors, processes it and responds in various ways. It also includes the user-interface - control keys, numerical keypad, display, sounder and loudspeaker.

Default Settings: Settings applicable to a specific device group.

Detector: The device (apparatus) that sends an alarm, that communicates with the control panel (for example, Next PG2 is a motion detector; SMD-426 PG2 is a smoke detector).

Disarming: The opposite of arming - an action that restores the control panel to the normal standby state. In this state, only *fire and 24-hour zones* will sound an alarm if violated, but a *panic alarm* may also be initiated.

Disturbed Zone: A zone in a state of alarm (this may be caused by an open window or door or by motion in the field of view of a motion detector). A disturbed zone is considered not secured.

Forced Arming: The alarm system cannot be armed when any one of the system zones is *disturbed* (open). To solve the problem eliminate the cause for zone disturbance for example closing doors and windows. Alternatively, impose **forced arming** that is automatic de-activation of zones that are still *disturbed* after termination of the exit delay. Bypassed zones are not protected throughout the arming period. Even if restored to normal (closed), bypassed zones remain unprotected until the system is disarmed.
Permission to force arm is given or denied by the installer while programming the system.

HOME: This type of arming is used when people are present within the protected site. A classic example is night-time at home, when the family is about to retire to bed. With HOME arming, perimeter zones are protected but interior zones are not. Consequently, motion within interior zones will be ignored by the control panel, but disturbance of a perimeter zone will cause an alarm.

Instant: You can arm the system AWAY-INSTANT or HOME-INSTANT, thereby canceling the entry delay for all delay zones for the duration of one arming period.
For example, you may arm the control panel in the HOME-INSTANT mode and remain within the protected area. Only perimeter protection is active, and if you do not expect somebody to drop in while the system is armed, alarm upon entry via the main door is an advantage.
To disarm the system without causing an alarm, use your control keypad (which is normally accessible without disturbing a perimeter zone) or use a keyfob transmitter.

Latchkey: The Latchkey mode is a special arming mode in which designated latchkey users will trigger a latchkey message to be sent to a telephone when they disarm the system.

For example, if a parent wants to be sure that their child has returned from school and disarmed the system. Latchkey arming is only possible when the system is armed in the AWAY mode.

Location: Assigning a named location to a device (for example, Garage, Front Door etc.)

Magnetic Contact Detector, Wireless: A Magnet- controlled switch and a wireless PowerG transmitter in a shared housing. The detector is mounted on doors and windows to detect changes in state (from closed to open and vice versa). Upon sensing that a door or window is open, the detector transmits its unique identification code accompanied by an alarm signal and various other status signals to the control panel.
The control panel, if not armed at that time, will consider the alarm system as not ready for arming until it receives a restored signal from the same detector.

Motion Detector, Wireless: A passive Infrared motion sensor and a wireless PowerG transmitter in a shared housing. Upon sensing motion, the detector transmits its unique identification code, accompanied by an alarm signal and various other status signals to the control panel. After transmission, it stands by to sense further motion.

Non-Alarm Zone: Your installer can designate a zone for roles other than alarm. For instance, a motion detector installed in a dark stairway may be used to switch on lights automatically when someone crosses the dark area. Another example is a wireless transmitter linked to a zone that controls a gate opening mechanism.

Quick Arming: Arming without a user code. The control panel does not request your user code when you press one of the arming buttons. Permission to use this arming method is given or denied by the installer while programming the system.

Remote Responder: A responder can be either a professional service provider to which the home or business owner subscribes (*a Monitoring Station*) or a family relation/friend who agrees to look after the protected site during absence of its occupants. The *control panel* reports events by telephone to both kinds of responders.

Restore: When a detector reverts from the state of alarm to the normal standby state, it is said to have been restored. A *motion detector* restores automatically after detection of movement, and becomes ready to detect again. This kind of restore is not reported to the remote *responders*.
A *magnetic contact detector* restores only upon closure of the protected door or window. This kind of restore is reported to the remote *responders*.

Sensor: The sensing element: pyroelectric sensor, photo-diode, microphone, smoke optical sensor etc.

Signal Strength: The quality link communication between the system components and the control panel.

Smoke Detector, Wireless: A regular smoke detector and a wireless PowerG transmitter in a shared housing. Upon detection of smoke, the detector transmits its unique identification code accompanied by an alarm signal and various status signals to the *control panel*. Since the smoke detector is linked to a special *fire zone*, a fire alarm is initiated.

State: AWAY, HOME, AWAY-INSTANT, HOME-INSTANT, LATCHKEY, FORCED, BYPASS.

Status: AC fail, low battery, trouble, etc.

User Codes: The PowerMaster-360R is designed to obey your commands, provided that they are preceded by a valid security access code.
Unauthorized people do not know this code, so any attempt on their part to *disarm* or defeat the system is bound to fail. Some operations, however, can be carried out without a user code as they do not degrade the security level of the alarm system.

Virtual or Touch Keypad: Contains the user-interface - control keys, numerical keypad and display.

Zone: A zone is an area within the protected site under supervision of a specific detector. During programming, the installer allows the *control panel* to learn the detector's identity code and links it to the desired zone. Since the zone is distinguished by number and name, the control panel can report the zone status to the user and register in its memory all the events reported by the zone detector. Instant and delay zones are on watch only when the control panel is armed, and other (*24-hour*) *zones* are on watch regardless of whether the system is armed or not.

Zone Type: The zone type determines how the system handles alarms and other signals sent from the device.

APPENDIX I. Compliance with standards

Compliance with standards

CE

European Standards: EN 300220, EN 300328, EN 301489, EN 50130-4, EN 60950-1, EN 50130-5, EN 50131-3, EN 50131-4, EN 50131-6, EN 50136-1,2, EN 50131-10

According to the European standard EN50131-1 and EN 50131-3, the PowerMaster 360R security grading is 2 - "low to medium risk" and environmental classification is II – "indoor general". The power supply type is A according to EN 50131-6, built-in siren -type Z warning device according to EN50131-4, and ATS Category is DP4, when IP module primary path and GPRS secondary, according to EN50136-1, EN50136-2 (pass through Operation Mode) and according to EN 50131-10 – Supervised Premises Transceiver (SPT).

Certified by Applica T&C in accordance with

EN 50131-1, EN 50131-3, EN 50131-4, EN 50131-6,EN 50131-5-3, EN 50130-5,

EN 50130-4, EN 50131-10, EN 50136-1, EN 50136-2

Applica T&C has certified only the 868MHz variant of this product.

UK: The PowerMaster-360R is suitable for use in systems installed to conform to PD6662:2010 at Grade 2 and environmental CLASS II. DD243 and BS8243

Hereby, Visonic Ltd. declares that the radio equipment type **PM-360R** is in compliance with Directive 2014/53/EU.
The full text of the EU declaration of conformity is available at the following internet address:
http://www.visonic.com/download-center.

U.S Standards: (FCC) CFR 47 part 15

WARNING! *Changes or modifications to this unit not expressly approved by the party responsible for compliance (Visonic Ltd.) could void the user's authority to operate the equipment.*

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

WARNING! *To comply with FCC RF exposure compliance requirements, the device should be located at a distance of at least 20 cm from all persons during normal operation. The antennas used for this product must not be co-located or operated in conjunction with any other antenna or transmitter.*

WARRANTY

Visonic Limited (the "**Manufacturer**") warrants this product only (the "**Product**") to the original purchaser only (the "Purchaser") against defective workmanship and materials under normal use of the Product for a period of twelve (12) months from the date of shipment by the Manufacturer.

This Warranty is absolutely conditional upon the Product having been properly installed, maintained and operated under conditions of normal use in accordance with the Manufacturers recommended installation and operation instructions. Products which have become defective for any other reason, according to the Manufacturers discretion, such as improper installation, failure to follow recommended installation and operational instructions, neglect, willful damage, misuse or vandalism, accidental damage, alteration or tampering, or repair by anyone other than the manufacturer, are not covered by this Warranty.

There is absolutely no warranty on software, and all software products are sold as a user license under the terms of the software license agreement included with such Product."

The Manufacturer does not represent that this Product may not be compromised and/or circumvented or that the Product will prevent any death and/or personal 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 Product, properly installed and maintained, only reduces the risk of such events without warning and it is not a guarantee or insurance that such events will not occur.

Conditions to Void Warranty:

This warranty applies only to defects in parts and workmanship relating to normal use of the Products. It does not cover:

- damage incurred in shipping or handling;
- damage caused by disaster such as fire, flood, wind, earthquake or lightning;
- damage due to causes beyond the control of the Seller such as excessive voltage, mechanical shock or water damage;
- damage caused by unauthorized attachment, alterations, modifications or foreign objects being used with or in conjunction with the Products;
- damage caused by peripherals (unless such peripherals were supplied by the Seller;
- defects caused by failure to provide a suitable installation environment for the products;
- damage caused by use of the Products for purposes other than those for which they were designed;
- damage from improper maintenance;
- damage arising out of any other abuse, mishandling or improper application of the Products.

Items Not Covered by Warranty:

In addition to the items which void the Warranty, the following items shall not be covered by Warranty: (i) freight cost to the repair centre; (ii) customs fees, taxes, or VAT that may be due; (iii) Products which are not identified with the Seller's product label and lot number or serial number; (iv) Products disassembled or repaired in such a manner as to adversely affect performance or prevent adequate inspection or testing to verify any warranty claim. Access cards or tags returned for replacement under warranty will be credited or replaced at the Seller's option.

THIS WARRANTY IS EXCLUSIVE AND EXPRESSLY IN LIEU OF ALL OTHER WARRANTIES, OBLIGATIONS OR LIABILITIES, WHETHER WRITTEN, ORAL, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR OTHERWISE. IN NO CASE SHALL THE MANUFACTURER BE LIABLE TO ANYONE FOR ANY CONSEQUENTIAL OR INCIDENTAL DAMAGES FOR BREACH OF THIS WARRANTY OR ANY OTHER WARRANTIES WHATSOEVER, AS AFORESAID.

THE MANUFACTURER SHALL IN NO EVENT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OR FOR LOSS, DAMAGE, OR EXPENSE, INCLUDING LOSS OF USE, PROFITS, REVENUE, OR GOODWILL, DIRECTLY OR INDIRECTLY ARISING FROM PURCHASER'S USE OR INABILITY TO USE THE PRODUCT, OR FOR LOSS OR DESTRUCTION OF OTHER PROPERTY OR FROM ANY OTHER CAUSE, EVEN IF MANUFACTURER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE MANUFACTURER 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. HOWEVER, IF THE MANUFACTURER IS HELD LIABLE, WHETHER DIRECTLY OR INDIRECTLY, FOR ANY LOSS OR DAMAGE ARISING UNDER THIS LIMITED WARRANTY, **THE MANUFACTURER'S MAXIMUM LIABILITY (IF ANY) SHALL NOT IN ANY CASE EXCEED THE PURCHASE PRICE OF THE PRODUCT INVOLVED,** WHICH SHALL BE FIXED AS LIQUIDATED DAMAGES AND NOT AS A PENALTY, AND SHALL BE THE COMPLETE AND EXCLUSIVE REMEDY AGAINST THE MANUFACTURER.

When accepting the delivery of the Product, the Purchaser agrees to the said conditions of sale and warranty and he recognizes having been informed of.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so these limitations may not apply under certain circumstances.

The Manufacturer shall be under no liability whatsoever arising out of the corruption and/or malfunctioning of any telecommunication or electronic equipment or any programs.

The Manufacturers obligations under this Warranty are limited solely to repair and/or replace at the Manufacturer's discretion any Product or part thereof that may prove defective. Any repair and/or replacement shall not extend the original Warranty period. The Manufacturer shall not be responsible for dismantling and/or reinstallation costs. To exercise this Warranty the Product must be returned to the Manufacturer freight pre-paid and insured. All freight and insurance costs are the responsibility of the Purchaser and are not included in this Warranty.

For sales in Israel only:

The Purchaser shall comply with the provisions of the Israeli Consumer Protection Law – 1981("Consumer Protection Law") related regulations, including the Israeli Consumer Protection Regulations (Warranty Sticker), 5772-2012) ("Regulations"), including, without limitation (i) providing its customers with at least the minimum warranty required by the Consumer Protection Law, and (ii) ensuring that a warranty certificate and a warranty sticker (as defined in the Regulations) ("Warranty Sticker") shall be attached to any sold Products and the date of the sale of the Product to the consumer or the end-user shall be added in a readable manner on the Warranty Sticker.

In no event shall the Purchser's compliance with the Consumer Protection Law and Regulations expand any of the Manufacturer's warranty obligations under this warranty, and the Purchaser shall be responsible for any warranty that it provides with respect to the Products which exceeds or is different from this warranty.

This warranty shall not be modified, varied or extended, and the Manufacturer does not authorize any person to act on its behalf in the modification, variation or extension of this warranty. This warranty shall apply to the Product only. All products, accessories or attachments of others used in conjunction with the Product, including batteries, shall be covered solely by their own warranty, if any. The Manufacturer shall not be liable for any damage or loss whatsoever, whether directly, indirectly, incidentally, consequentially or otherwise, caused by the malfunction of the Product due to products, accessories, or attachments of others, including batteries, used in conjunction with the Products. This Warranty is exclusive to the original Purchaser and is not assignable.

This Warranty is in addition to and does not affect your legal rights. Any provision in this warranty which is contrary to the Law in the state or country were the Product is supplied shall not apply.

Governing Law*:*

This disclaimer of warranties and limited warranty are governed by the domestic laws of Israel.

Warning

The user must follow the Manufacturer's installation and operational instructions including testing the Product and its whole system at least once a week and to take all necessary precautions for his/her safety and the protection of his/her property.

* In case of a conflict, contradiction or interpretation between the English version of the warranty and other versions, the English version shall prevail.

EMAIL: info@visonic.com
INTERNET: www.visonic.com

PowerMaster-360R Installer's Guide D-307083 Rev 0 (10/17)

D-307083

PowerMaster-360R Quick user guide

Arming and disarming the system

Step		Operation	User Actions	Notes
Optional	1	Press the Partition Selection button and then select a PARTITION (if Partition is enabled) – used to divide the alarm system into three independently controllable areas	# followed by any combination of 1, 2, or 3	A warning beep will be heard when selecting a partition to which no sensors / peripherals were enrolled.
	2	Arm AWAY - used to arm the system when the protected site is vacated entirely.	+ [ ] or enter code	**ARM indicator** lights steadily during the armed state. **ARM indicator** extinguishes during the disarmed state. Disarming the system also stops the siren alarm, irrespective of whether the alarm was initiated during the armed or the disarmed state.
		Arm HOME – used to arm the system when people are present within the protected site.	+ [ ] or enter code	
		Disarm (OFF) – used to restore the control panel to the normal standby state	+ [ ] or enter code	
Optional		Quick arm AWAY (If Quick Arm is enabled) – used to arm in the AWAY state without a user code		
Optional		Quick arm HOME (If Quick Arm is enabled) – used to arm in the HOME state without a user code		
Optional		Forced arming AWAY (system not ready) – used to arm the alarm system in the AWAY state when any of the system zones is disturbed	+ [ ] or enter code to silence the warning buzzer	
Optional		Forced arming HOME (system not ready) – used to arm the alarm system in the HOME state when any of the system zones is disturbed	+ [ ] or enter code to silence the warning buzzer	
Optional	3	INSTANT – used to arm in the Instant mode, without an entry delay.	(After arming HOME/AWAY) 0	
Optional		LATCHKEY – used for keyfob transmitters 5 through 8		

Note: *The factory default master user code is 1111. The code is not required if quick arming has been permitted by the installer. Change the factory default code to a secret code without delay (see section Chapter 4, section B.4 of the PowerMaster-360R User's Guide).*

Initiating Alarms

Alarms	Actions	Notes
Emergency alarm	+ (≈ 2 sec.)	To stop the alarm, press and then key in your valid user code.
Fire alarm	(≈ 2 sec.)	
Panic alarm	+ + (≈ 2 sec.)	

Preparing to Arm

Before arming, make sure that READY is displayed.

HH:MM READY

This indicates that all zones are secured and you may arm the system as desired.

If at least one zone is open (disturbed) the display will read:

HH:MM NOT READY

This indicates that the system is not ready for arming and in most cases that one or more zones are not secured. However, it can also mean that an unresolved condition exists such as certain trouble conditions, jamming etc., depending on system configuration.

To review the open zones click i|OK. The details and location of the first open zone detector (usually an open door or window sensor) will be displayed. To fix the open zone, locate the sensor and secure it (close the door or window) – see device locator below. Each click of i|OK will display another open zone or trouble indication. It is highly recommended to fix the open zone(s), thus restoring the system to the state of ready to arm. If you do not know how to do this, consult your installer.

Note: *To quit at any stage and to revert to the READY display, click* ←.

Device Locator: The PowerMaster-360R system has a device locator that helps you to identify open or troubled devices indicated on the LCD display. While the LCD displays an open or faulty device, the LED on the respective device flashes indicating **it's me**. The **it's me** indication will appear on the device within a maximum 16 seconds and will last for as long as the LCD displays the device.

Zone Bypass Scheme

Bypassing permits arming only part of the system and at the same time allowing free movement of people within certain zones when the system is armed. It is also used to temporarily remove from service faulty zones that require repair work or to deactivate a sensor if, for example, you are decorating a room.

You can set the Zone Bypass Scheme i.e. to scroll through the list of registered (enrolled) sensors to your PowerMaster-360R system and to Bypass (deactivate) faulty or disturbed sensors (either READY or NOT-READY) or to Clear (reactivate) BYPASSED zones (sensors).

Once you have set a Bypass Scheme you can use the following 3 options:

- To quickly clear a bypassed zone i.e. to reactivate the bypassed zone – refer to Chapter 4, section B.1 of the PowerMaster-360R User's Guide.
- To quickly review the bypassed zones – refer to Chapter 4, section B.2 of the PowerMaster-360R User's Guide.
- To repeat (recall) the last used zone bypassing scheme – refer to Chapter 4, section B.3 of the PowerMaster-360R User's Guide.