

ALARM SYSTEM AND DIALLER PRODUCTS



USER GUIDE



You have just bought a DAITEM security system, designed to cover all your protection needs. We would like to thank you for your confidence.

Precautions

- The installation of your system should be carried out according to applicable national standards. If your system is to be powered by 230 VAC mains power the connection must be carried out by a certified electrician.
- Your security system is simple to use. We advise you to switch it on (arm it) every time you leave your home.
- Do not leave your remote control in view.
- Keep a back-up remote control in a secret place.
- If one of the devices in your system is lost, stolen or sabotaged, call your installer right away.
- Keep the access codes to your control keypads secret.
- Switch your security system to partial protection mode to protect unoccupied rooms.

When you leave home

- Close all the protected doors and windows.
- Switch on (arm) your security system.
- If necessary, check for any fault indications or entrances left open.

When you're going to be away for a while

- Check that all doors and windows are closed.
- Check your security system is operating properly by performing a real test on the system.
- Switch on (arm) your system.

Important

Installing a dialler unit on the control panel (which does not have one when delivered) or installing a separate dialler in your home can provide your installer with remote access to your alarm system. This will allow your installer to:

- perform maintenance operations,
- modify parameter settings,
- download data via the internet according to the conditions described in the dialler product user manual. It is up to your installer to define with you the specific contractual conditions for accessing your system.

Warning

DAITEM shall in no way be held responsible for the consequences of the temporary or permanent unavailability of the SPTN switched public telephone network, the GSM/GPRS mobile network or the Ethernet (ADSL) network. Some features are only available with control panel versions 2.0.0 or later.

Enter # # # on your control panel keypad to check!
master code
(factory: 0000)

We would appreciate your suggestions

If you have any comments about how we might improve our guides and our products, we would be grateful if you could send them in writing to: Daitem - Service consommateur
rue du Pré de l'Orme - F-38926 CROLLES cedex


PRODUCT APPLICATION

The equipment marketed by DAITEM is designed to contribute to the protection and comfort of homes and some professional premises or to contribute to the protection and wellbeing of persons, according to the technical limits and environments described in the documentation supplied by DAITEM and recommended by the retailer.

CE MARKING AND REGULATIONS

The products marketed by DAITEM comply with the essential requirements of the applicable European directives. CE marking certifies that the products comply with these directives and the standards that define the technical specifications to be applied.

Your retailer will provide you with the conditions under which the manufacturer's guarantee and after-sales service apply.

 **Disposing of waste electrical and electronic devices at the end of their service life** (Applicable in European Union countries and other European countries with a waste collection system). This symbol on products or product packaging indicates that the product must not be thrown out with normal household waste. It must be taken to an appropriate collection point for recycling waste electrical and electronic equipment. By disposing of such products in the appropriate manner, you are helping to prevent any harmful effects they may have on the environment and human health. For further information about recycling this product, you should consult your local authorities, waste collection centre or the shop where you bought the product.

Contents

ALARM SYSTEM USER GUIDE

1. Operating your security system	4
1.1 Arming or disarming the system.....	4
1.2 Deactivating the exit time delay when the last exit is closed.....	4
1.3 Disarming the system under duress (this feature is only available with a remote monitoring service).....	4
1.4 Arming or disarming one or several groups.....	5
1.5 Partially arming the system.....	5
1.6 Arming the system in presence mode.....	6
1.7 Arming the system when a door or window is open.....	6
1.8 Automatic timed Arm/Disarm	7
1.9 System reactivation.....	7
2. The keypads transfer information about the control panel status	8
3. Configuring the system locally using the keypad built into the control panel	9
3.1 Modifying the language.....	9
3.2 Modifying the date and time.....	9
3.3 Modifying your master code.....	9
3.4 Modifying the user codes	10
3.5 Disabling or enabling the user codes.....	10
4. Restricting access to commands	10
4.1 Restricting access using the user codes	10
4.2 Restricting access using the tags.....	11
4.3 Disabling or enabling a tag	11
5. Testing the devices	12
6. Performing a real test on the system	13
7. The control panel indicates alarms	14
8. The control panel indicates faults	15
9. Consulting the events log	16
10. Additional keypad functions	17
10.1 Querying the status of your system	17
10.2 Triggering an alarm (if keypad button has been reprogrammed).....	17
10.3 Triggering a silent alarm (if keypad button has been reprogrammed).....	17

DIALLER PRODUCT USER GUIDE

Foreword	18
1. Introduction	19
1.1 Operation for outgoing calls	20
1.2 Operation for incoming calls.....	20
2. Configuring a dialler locally using the built-in keypad	21
2.1 Modifying the language.....	21
2.2 Modifying the date and time.....	21
2.3 Modifying your master code.....	21
2.4 Modifying your video code (GSM/GPRS - Ethernet ADSL)	22
2.5 Enabling or disabling remote access via the Internet (mains-powered GPRS - Ethernet ADSL)	22
2.6 Recording or modifying the personalised welcome message for vocal transmissions (PSTN-GSM)	23
2.7 Modifying the numbers of individual correspondents (PSTN - GSM)	23
3. Outgoing calls	24
3.1 Dialler call cycle procedure	24
3.2 Procedure for voice calls to individuals (PSTN - GSM).....	25
3.3 List of commands possible during listen-in period	25
3.4 List of voice messages and SMS transmitted to an individual correspondent according to the type of event (PSTN - GSM).....	26
3.5 Procedure for calls to a remote monitoring centre (PSTN-GSM/GPRS - Ethernet ADSL).....	27
4. Incoming calls	28
4.1 Voice remote operation over the telephone via the PSTN or GSM network (mains-powered).....	28
4.2 Configuring and operating the dialler from a PC connected via Internet (mains-powered GPRS - Ethernet ADSL).	30
4.3 Remote operation over SMS via the GSM network (mains-powered)	31
5. Testing calls to your correspondents (PSTN-GSM/GPRS- Ethernet ADSL)	32
6. Instructions sheet (to be completed and given to your correspondents)	33
DAITEM GUARANTEE AND EXTENSION CONDITIONS	35

ALARM SYSTEM USER GUIDE

1. Operating your security system

The control panel can operate up to 8 intrusion protection groups (depending on the type of control panel) either individually or at the same time.

Example: 4 intrusion protection groups



1.1 Arming or disarming the system

• Using a remote control:



ON or OFF

• Using a control keypad:

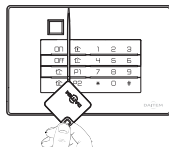


□ □ □ □ + ON or OFF
master code

Using a vocal keypad with tag reader and proximity detector



ON or OFF and



The LED indicating the reading zone flashes. Hold the tag against the pictogram ().

“bip, Armed”
or
“bip, Off”



Armed: all groups armed



Off: All groups disarmed

□ Group disarmed

■ Group armed

1.2 Deactivating the exit time delay when the last exit is closed

The exit time delay can be deactivated when one of the entrances with a detector programmed for this function is closed. Deactivation of this time delay can be automatically programmed by determining a door or window detector in charge of arming one, several or all groups.

1.3 Disarming the system under duress (this feature is only available with a remote monitoring service)

IMPORTANT: if a telephone transmission unit card has been installed.

This function allows users to quietly alert a correspondent when they are forced to disarm their alarm system by an intruder. The system behaves as if it is being disarmed but sends a specific silent alarm message via the telephone line to the remote monitoring centre.

Using a keypad:

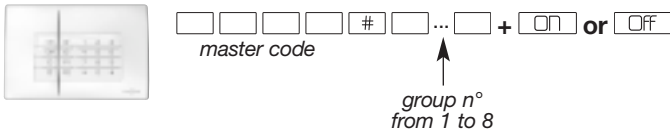


□ □ □ □ □ OFF
master code

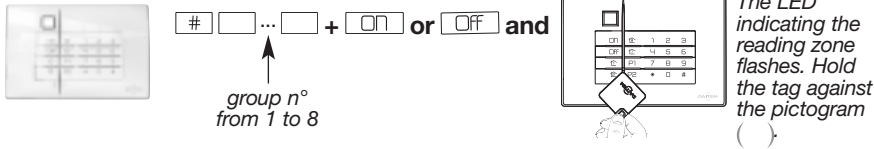
Users must check that this specific alert message can be processed by their remote monitoring centre.

1.4 Arming or disarming one or several groups

• Using a remote keypad:



• Using a vocal keypad with tag reader:



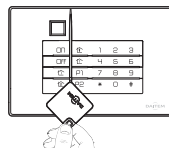
Example using a control keypad:

• Arming groups 3 + 4

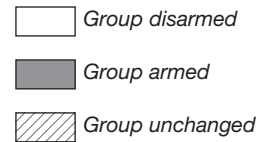
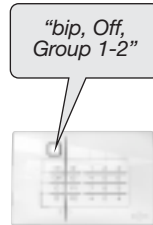


Example using a vocal keypad with tag reader:

• Disarming groups 1 + 2



The LED indicating the reading zone flashes. Hold the tag against the pictogram ()



1.5 Partially arming the system

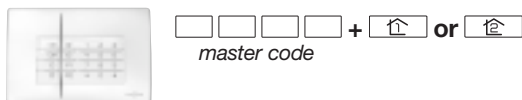
• Using a remote control:



P1 or P2

For P2, your installer must reprogramme the key.

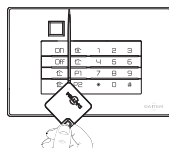
• Using a control keypad:



• Using a vocal keypad with tag reader:



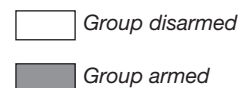
↑ or ↓ and



The LED indicating the reading zone flashes. Hold the tag against the pictogram ()



"bip, Armed Partial 1" or "bip, Armed Partial 2"



1.6 Arming the system in presence mode

The control panel allows for partial protection and quiet system responses in the event of intrusion: **Armed Presence**.

IMPORTANT: there is no exit time delay or entry time delay in armed presence mode.

• Using a control keypad:

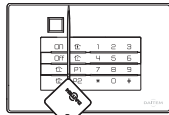


□ □ □ □ +
 master code

• Using a vocal keypad with tag reader::



and



The LED indicating the reading zone flashes. Hold the tag against the pictogram ().



"bip, Armed Presence"



"bip, Armed Presence"



Armed Presence: Group 1 only armed

Group disarmed

Group armed

ENTRY TIME DELAY

The entry time delay is the time allowed to disarm the system from inside the premises (e.g. using the keypad) without triggering the alerts and deterrents. Users can decide on the most suitable time delay for them with their installer.

A vocal warning "BIP, BIP, BIP, BIP, PROTECTION_ACTIVE" tells users to disarm the system.

EXIT TIME DELAY

The exit time delay is the time allowed to leave the premises without triggering the alarm system. Users can decide on the most suitable time delay for them with their installer. The end of this time delay is indicated by the control panel as it repeats the voice message that the system is armed.

1.7 Arming the system when a door or window is open

The control panel is factory programmed to prevent system arming in case a door or window (with a protection device installed on it) has been left open.

This factory programming can be modified by the installer.

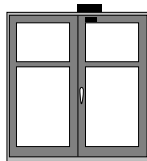
Example: arming with exit 2 open

You arm the system

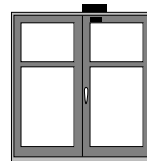


"bip, exit 2 opened"
The control panel does not arm the system

You close exit 2

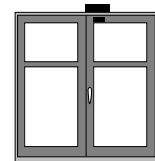


You arm the system



"bip, armed"

End of exit time delay



"bip, armed"

1.8 Automatic timed Arm/Disarm

This function makes it possible to send automatically Arm/Disarm commands to the alarm control panel at times programmed by your installer, via the TwinLoad® software.

You can activate or de-activate these timed automatic ON/OFF commands at the Control panel keypad .In factory default, this function is not activated.

Using the Control Panel keypad:



* 5 1 1 * * *

master code

↑
0: disabled
1: enabled

1.9 System reactivation

Factory default , this function is not active.

This command authorizes the resetting of the Control Panel after an alarm activation, intrusion alarm or fault (radio, loss of power... etc.).

This command is accessible locally from a separate/remote keypad or the built-in keypad of the Control Panel while programming:

2 0 #

master code

WARNING: this configuration is possible with control panel versions 2.1.0 or later (enter # 5 0 3 # # to check the version).






















2. The keypads transfer information about the control panel status

The keypads can be used to:

- operate your system,
- check the status of your system.


IMPORTANT

- Only commands sent from control and information keypads light up the LEDs.
- Only commands issued from a vocal keypad trigger voice messages indicating possible alarms, faults and the status of exits.

Commands sent to:	Command	Indications & messages at the information & command keypad		Message issued by vocal keypad with tag reader
		LED status	Buzzer	
A control panel	Disarm	 keyfob 1.5 s	long beep	"Bip, Off" or "Bip, Fault System"
	OFF/Disarm with alarm memory	  	3 short beeps	
	Arm	 keyfob 1.5 s	long beep	"Bip, Armed"
	ON/Arm with fault	 keyfob 1.5 s	3 short beeps	
	Armed partial 1	 keyfob 1.5 s	long beep	"Bip, Armed Partial 1"
	Armed partial 2	 keyfob 1.5 s	long beep	"Bip, Armed Partial 2"
	ON Partial 1, with a fault	 keyfob 1.5 s	3 short beeps	
	ON Partial 2, with a fault	 keyfob 1.5 s	3 short beeps	
	Arm group X	 keyfob 1.5 s	long beep	"Bip, Armed Group X"
	ON Group X with an anomaly	 keyfob 1.5 s	3 short beeps	
	ON blocked (1)	  	3 short beeps	
	Disarm group X	 keyfob 1.5 s	long beep	"Bip, Off Group X"
	OFF group X with alarm memory	  	3 short beeps	
	Arm in presence mode			"Bip, Armed Presence"
	Alarms memorised			"Bip, Off, Alarm System"
	Faults memorised			"Bip, Armed, Fault System" or "Bip, Off, Fault System"
Exits open	 keyfob 1.5 s	3 short beeps	"Bip, Armed, Exit Opened"	
Switching receiver, remote control unit	Transmit a home automation command (light, relay, etc.)	 keyfob 1.5 s		
	Switch to test mode			"Bip, Test mode"
	Switch to installation mode			"Bip, Installation mode"
	Switch to user mode			"Bip, Off"
System status query				"Bip, system status, Armed"
				"Bip, System_status, Armed Partial 1 or 2"
				"Bip, System_status, Off"
				"Bip, System_status, Armed Group X"
				"Bip, System_status, Armed Presence"
				"Bip, System_status,...Fault System"
				"Bip, System_status,...Exit Opened"
			"Bip, System_status,...Exit Inhibited"	

(1) A stopped ON/Arming operation means the system has been unable to complete Arming due to a system fault.

X: group 1 to 8 depending on type of control panel

 : green LED

 : red LED

3. Configuring the system locally using the keypad built into the control panel

Your installer will have already configured your control panel but you can modify some of the programming at any time.

If 5 wrong access codes are entered on the keypad in less than 5 minutes this will block the keypad for 5 minutes and the control panel will be informed.

3.1 Modifying the language

You can replace the original language with another language.

To modify the language, enter:

* * * *

master code

- 0: French
- 1: Italian
- 2: German
- 3: Spanish
- 4: Dutch
- 5: English

"bip + chosen language"



Factory setting: English

3.2 Modifying the date and time

The events memorised by the control panel are date and time stamped.

To **programme the date and time manually**, proceed as follows:

• Date

To modify the date, enter:

* * * * * *

master code

Day

Month

Year
(e.g. for 2012,
enter 12)

"bip + date announced"



• Time

To modify the time, enter:

* * * * *

master code

Hour

Minutes

"bip + time announced"



3.3 Modifying your master code

Do not lose your codes as you will need them in order to programme new codes. However, if you do lose your codes, contact your installer who will put the system back into its factory configuration and programme the codes again. Your master code allows you to configure the control panel and access all the system commands using the built-in keypad.

IMPORTANT

- To keep your codes confidential, we recommend you change the keypad access codes often and regularly clean the keys.
- To prevent unwanted calls to correspondents, do not end the master code with a "0".

To modify the master code, enter:

... * * ... * ... * *

old
master code

new
master code

new master
code repeated

IMPORTANT: all access codes must differ from each other.

Factory master code: 0000

Example:

To replace the factory master code "0000" with the new code "1423", enter:

* * * * *

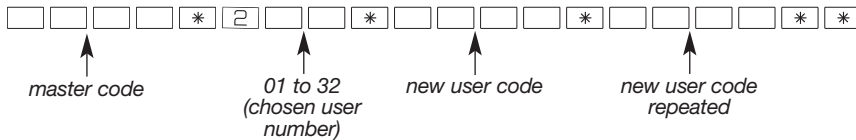
"beep"



3.4 Modifying the user codes

The user codes limit access to certain commands. They are meant for occasional users.

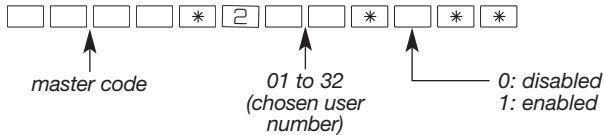
Using the keypad, enter:



3.5 Disabling or enabling the user codes

The following procedure can be followed to enable or disable user codes without modifying their programming.

Using the keypad, enter:



IMPORTANT: a programmed user code is automatically enabled.

4. Restricting access to commands

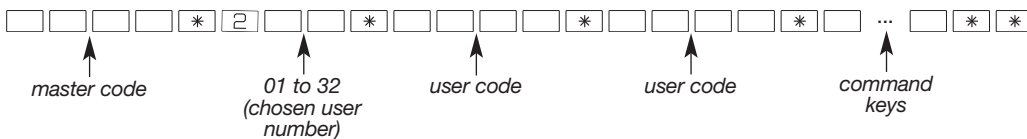
4.1 Restricting access to user codes

The user codes can have separate and limited access to:

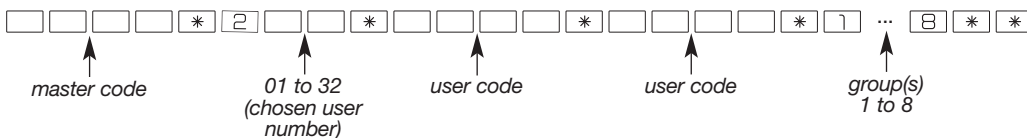
- specific keypad control keys,
- specific groups.

Only the command keys or groups selected during programming can be accessed when the user code is entered.

To **restrict** a user code to (a) **specific command key(s)**, use the keypad to enter:



To **restrict** a user code to (a) **specific group(s)**, use the keypad to enter:



Example, after entering the **master code** (1234), to restrict **user code 1** (1213) to **Group 1** and **Group 2**, enter:



In this case, user code 1 can only disarm and arm Group 1 and Group 2.

Example, arming groups 1 and 2:



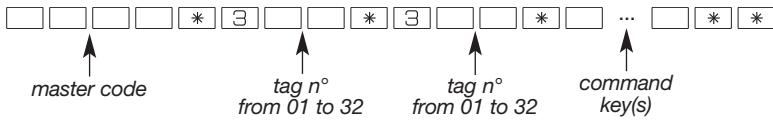
WARNING: the 32 user codes are only available with control panel keypad versions 2.1.0 or later.

Enter [] [] [] [] # 5 0 3 # # to check the version.
master code

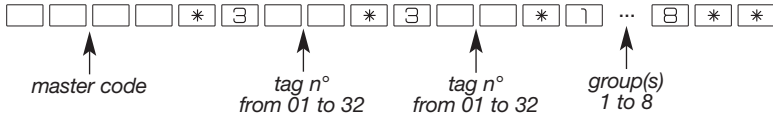
4.2 Restricting access using the tags

The tags can have separate and limited access to specific command keys and specific groups. Only the command keys or groups selected during programming can be accessed using the tag.

To **restrict** a tag to (a) **specific command key(s)**, use the keypad to enter:



To **restrict** a tag to (a) **specific group(s)**, use the keypad to enter:



• To **cancel a tag's restricted access**, use the keypad to enter:

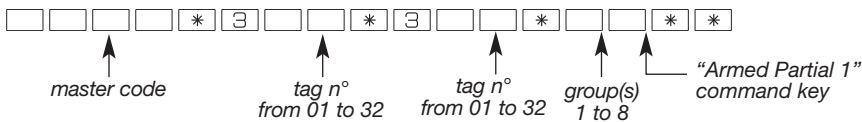


Example: to **cancel the restrictions linked to tag 02**, use the keypad to enter:



The access restrictions linked to tag 02 will be cancelled.

• To **restrict access to a command key and a group**, use the keypad to enter:



Example: to **restrict tag 01 to Armed/Off Group 1 and Armed Partial 1** commands, use the keypad to enter:



Only the commands for Off and Armed Group 1 and Armed Partial One are accessible using tag 01.

WARNING: the 32 tags are only available with control panel keypad versions 2.1.0 or later.
 Enter [] [] [] [] # [5] [0] [3] # # to check the version.
 master code

4.3 Disabling or enabling a tag

A registered tag is automatically enabled.

To disable or enable a tag, use the keypad to enter:



Examples:

• to **disable tag 01**, enter:



• to **enable tag 02**, enter:



WARNING: the 32 tags are only available with control panel keypad versions 2.1.0 or later.
 Enter [] [] [] [] # [5] [0] [3] # # to check the version.
 master code

IMPORTANT: once a year or before going away for a long period, we advise you to test your security system. The **TEST MODE** allows you to test each device in the system without triggering the sirens.

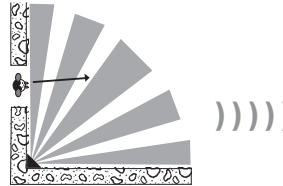
1. Switch the control panel to test mode

□ □ □ □ # 2 # #
master code



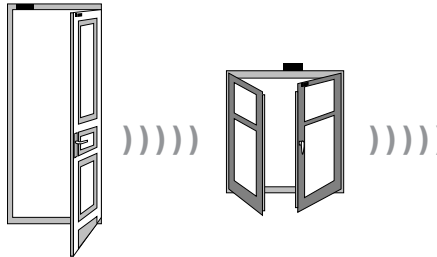
2. Test each detector

- Move in front of each motion detector.
- Check the message issued by the control panel.



IMPORTANT: before moving in front of an infrared detector, wait for 90 seconds in an unprotected area.

- Open then close all exits protected by a door/window or multicontact detector.
- Check the message issued by the control panel.



3. Test each remote control unit

- Press the Off key on each remote control unit.
- or**
- Enter your master code and press the Off key on each keypad.



4. Switch the control panel to user mode

□ □ □ □ # 1 # #
master code



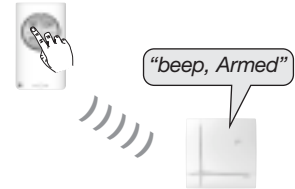
IMPORTANT

- You are now going to perform a real test on your security system. This test will trigger the alarm units and transmit a message to your correspondents by phone. We recommend you warn your correspondents beforehand (if a dialler unit has been installed in the control panel or a separate dialler has been installed).
- The sounding level of the sirens can cause hearing disorders. The necessary precautions must therefore be taken before carrying out the tests.

1. Close all the exits and leave the protected areas for at least 90 seconds.

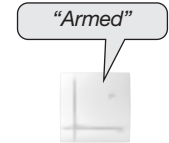
2. Arm the system

↪ when it receives the Arm command, the control panel responds: *"beep, Armed"*



3. Wait until the end of the Exit time delay

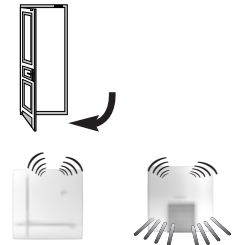
↪ the control panel announces: *"Armed"*



4. Enter a protected room

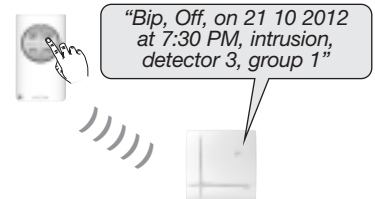
↪

- the control panel and sirens are triggered,
- the telephone dialler calls the programmed correspondents depending on the type of events transmitted. (1) (2)



5. Let the sirens sound for 30 seconds and then disarm the system (3)

↪ on receipt of the **"Off"** command, the sirens stop and the control panel responds. For example: *"Bip, Off, on 21 10 2012 at 7:30 PM, intrusion, detector 3, group 1"*.



6. Check transmission of the alarm (and any alarm images or films) to your programmed correspondents. (1) (2)

- (1) If a dialler unit or separate dialler have been installed.
 (2) Intrusions alarms which appear during an entry delay, are transmitted only 60 seconds after termination of the "Entry beeps" and provided that during this entry period no system "OFF" command is received.
 (3) For voice calls only, the transmission of the call to correspondents is stopped when the system is disarmed.

7. The control panel indicates alarms

- Alarms (intrusion, personal, technical, tamper or fire) are indicated:
 - on receipt of an Off order,
 - when the system is operated remotely.

- Voice indications specify:
 - the date and time at which the alarm occurred,
 - the type of alarm,
 - the identity of the device having triggered the alarm.

Intrusion protection

Control panel voice message	Events
"bip, date, time, intrusion, detector n°, group n°"	Intrusion on premises.
"bip, date, time, intrusion confirmed, detector n°, group n°"	Movement of the intruder on the premises.

Technical protection

Control panel voice message	Events
24/24 "bip, bip, bip, bip, Technical Alarm, Technical Detector n°" Message repeated every 10 seconds for 3 minutes (except in Total Arm mode)	Technical protection triggered by a sensor associated with a universal transmitter.

Fire protection

Control panel voice message	Events
24/24 "bip, date, time, Fire Alarm, Detector n°"	Fire protection triggered by a detector.
"bip, date, time, Fire Alarm, Remote Control_Unit n°"	Fire protection triggered by a remote control unit.

Protection against system tampering

Control panel voice message	Events
24/24 "bip, date, time, Tamper, Remote Control Unit n°"	Attempt to open or remove a keypad.
"bip, date, time, Tamper, Control Panel"	Attempt to remove or open the control panel.
"bip, date, time, Tamper, Siren n°" or "Tamper, relay n°"	Attempt to remove a siren or radio repeater relay.
"bip, date, time, Tamper, Detector n°, Group n°"	Attempt to open or remove a detector.
"bip, date, time, Tamper, Radio"	Detection of radio scrambling.

* Requires the installation of a dialler unit in the control panel or the installation of a separate dialler.

IMPORTANT: the alarm memory is automatically deleted the next time the system is armed.

8. The control panel indicates faults

- The control panel permanently monitors the state of devices:
 - power supply,
 - tamper system,
 - telephone line availability*,
 - radio link.

- The control panel indicates faults:
 - on receipt of an Off or Arm order,
 - when the system status is queried or consulted remotely.

Device power supply faults

Control panel voice message	Events
<i>"bip, Fault, Voltage, Control_panel"</i>	Control panel battery low
<i>"bip, Fault, Voltage, Battery, Control panel"</i>	The control panel does not have a Li-Ion back-up battery
<i>"bip, Fault, Voltage, Detector n°"</i>	Detector battery low
<i>"bip, Fault, Voltage, Siren n°"</i>	Siren battery low
<i>"bip, Fault, Voltage, Relay n°"</i>	Radio relay battery low
<i>"bip, Fault, Voltage, Remote Control Unit n°"</i>	Keypad or keyfob Low battery power

Device tamper faults

Control panel voice message	Events
<i>"bip, Fault, Tamper, Control panel"</i>	Control panel tamper fault
<i>"bip, Fault, Tamper, Detector n°, Group n°"</i>	Detector tamper fault
<i>"bip, Fault, Tamper, Siren n° or Tamper, Relay n°"</i>	Siren or radio repeater relay tamper fault
<i>"bip, Fault, Tamper, Remote Control Unit n°"</i>	Keypad tamper fault

Device radio link faults

Control panel voice message	Events
<i>"bip, Fault, Radio_link, Detector n°, Group n°"</i>	Loss of radio link between a detector and the control panel
<i>"bip, Fault, Radio_link, Siren n° or Tamper, Relay n°"</i>	Loss of radio link with a siren or radio repeater relay
<i>"bip, Fault, Radio_link, Remote Control Unit n°"</i>	Loss of radio link between a keypad and the control panel

* Requires the installation of a dialler unit in the control panel or the installation of a separate dialler.

9. Consulting the events log

The events log contains the **last 1,000** date and time stamped event to have occurred in the system. It makes it possible to keep track of all system operation and maintenance activities.

The complete events log can be **consulted** locally using the control panel keypad.

The events log records:

- intrusion protection status changes,
- automatic inhibitions of exits left open,
- alarms,
- faults,
- system mode changes.

To access the events log,

enter: # 1 0 # #
 master code

then press: 1 for the next event

↩ 2 to repeat the event

↩ 3 for previous

↩ 4 to fast forward (10 events by 10 events)

↩ 0 to end consultation

After 30 seconds without the keypad being pressed, the control panel automatically exits the events log.

Each event in the log is displayed with the following information:

- date and time,
- event name,
- identity of devices having triggered the event,
- detection zone (for intrusion and fire alarms).

Example:

*"bip, on 25/02/2012 at 3 PM,
Intrusion, Detector 3, Group 1"*
*"bip, on 13/01/2012 at 12 PM,
Tamper, Siren 1"*



10. Additional keypad functions

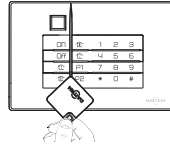
10.1 Querying the status of your system


- Control keypad:

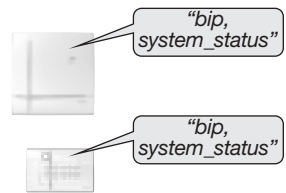
□ □ □ □ # 4 # # or □ □ □ □ 
master code master code

- Vocal keypad with tag reader:

4 # # or  or □ □ □ □ 
master code



The LED indicating the reading zone flashes. Hold the tag against the pictogram ().



10.2 Triggering an alarm (if a keypad button has been reprogrammed)

IMPORTANT: the sounding level of the sirens can cause hearing disorders. The necessary precautions must therefore be taken before carrying out the tests.

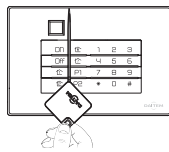
- Control keypad:


□ □ □ □ # 2 2 # # or □
master code Alarm
Press and hold longer than 2 s



- Vocal keypad with tag reader:

2 2 # # or □
Alarm
Press and hold longer than 2 s



The LED indicating the reading zone flashes. Hold the tag against the pictogram ().

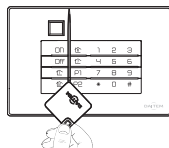
10.3 Triggering a silent alarm (if a keypad button has been reprogrammed)


- Control keypad:

□ □ □ □ # 2 4 # # or □
master code Silent alarm
Press and hold longer than 2 s

- Vocal keypad with tag reader:

2 4 # # or □
Silent alarm
Press and hold longer than 2 s



The LED indicating the reading zone flashes. Hold the tag against the pictogram ().

DIALLER PRODUCT USER GUIDE

Foreword

KEY:



→ only concerns dialler units using the media stipulated
(**present example:** GSM/GPRS and/or Ethernet ADSL)

ONLY WITH THE USE OF IMAGE TRANSMISSION DETECTORS

→ Only concerns an alarm system fitted with one or several image transmission detector(s).

ONLY WITH COMPATIBLE IP CAMERAS

→ Only concerns an alarm system fitted with one or several compatible IP video cameras

USER INFORMATION

ONLY FOR VIDEOS

The dialler is designed to protect homes and some business premises. This alarm transmission device triggers a remote alarm in the event of a break-in but is also able to remotely transmit films and videos of the monitored site in real time.

It should be noted that the installation of a video monitoring system in a public building is subject to regulations. Employees and members of the public entering the building must be clearly and constantly informed of the presence of the video monitoring system in compliance with legal requirements.

The installation of a video monitoring system on private premises is authorised, on condition that the cameras cannot see beyond the premises.

Furthermore, individuals who are filmed on a private property must be duly informed of this.

The installer is responsible for the installation of such a video monitoring system while the user is responsible for its use and compliance with associated legal specifications.

Exclusion of liability and communication networks (unavailability):

DAITEM shall not be held liable for use of the equipment described herein that does not comply with contractual stipulations.

DAITEM reminds users that its systems operate via telecommunications networks such as switched public telephone, radio, GSM, IP, GPRS, WIFI networks, etc.

As DAITEM is not responsible for managing such networks, it has no control over them. Their availability can only be guaranteed by their operator.

DAITEM also draws users' attention to the fact that should these networks become unavailable, its own systems may also become unavailable.

If such a situation should arise, independent of the will of DAITEM, the company informs users that neither it nor the manufacturer shall be held liable for the damaging consequences that such a situation may result in.

1. Introduction

A dialler unit can either be factory-mounted in a **separate dialler** or integrated into a **control panel with siren and keypad** transforming the device into a **control panel with siren, keypad and dialler**.

In what follows all of the products cited above shall be referred to as diallers.

The different control panels with siren and keypad: each control panel can be fitted with one of the dialler units listed opposite hence transforming the product into a control panel with dialler.



Control panel reference	Choice of dialler	Transmission media		
		PSTN	GSM/GPRS	Ethernet (ADSL)
SH320AU SH340AU SH380AU	SH501AX	PSTN	-	Ethernet (ADSL)
	SH502AX	-	GSM/GPRS	
	SH503AX	PSTN	GSM/GPRS	
	SH504AX	-	-	

The different separate diallers:



Separate dialler reference	Transmission media		
	PSTN	GSM/GPRS	Ethernet (ADSL)
SH511AX	PSTN	-	Ethernet (ADSL)
SH512AX	-	GSM/GPRS	
SH513AX	PSTN	GSM/GPRS	
SH514AX	-	-	

Dialler unit and transmission media:

Depending on its reference, the dialler unit has different transmission media (see tables above). To describe the use of the product, it is assumed that the dialler has three transmission media: PSTN, GSM/GPRS and ADSL.

Dialler

4 customisable control buttons:

- armed
- off
- armed partial 1
- armed partial 2

LED indications

LEDs	Colours	LED status	Indication
Three-colour LED	red	steady	button pressed or line occupied (incoming/outgoing call)
		continuous rapid flashing	operation blocked when powered (power supply, radio, transmission module link or keypad)
		12 s maximum rapid flashing	connection test, date and reference
		1 flash every 5 s	permanent indication of test mode
		2 flashes every 10 s	permanent indication of installation mode
		3 rapid flashes	error
	green	steady for 10 seconds	valid access code
		steady	recording of 10 s maximum voice message
	orange	rapid flashing	memory zone transfer
		1 flash every 20 s (1)	system fault (voltage fault, media fault or loss of system product radio link)
Blue light	modulated indication of renewed control panel transmissions	mode change: installation, test and use	
		arming or disarming	
		system status command	
		one of the 4 customisable keys pressed (arm, disarm, arm partial 1 and 2)	

(1) Only concerns a control panel with siren, keypad and dialler when the system is disarmed in user mode.

1.1 Operation for outgoing calls

Via its different communication networks, the dialler remotely alerts correspondents of intrusion or other events arising on the protected site.

- The dialler alerts individual correspondents or a remote monitoring centre in case of:
 - intrusion,
 - technical alarm,
 - fire alarm,
 - tamper alarm,
 - system device fault.
- In the event of intrusion, the dialler provides the following remote functions:
 - listen-in and speak-out/talk-back,
 - visual alarm confirmation via the transmission of images or films from image transmission detectors and/or compatible IP cameras installed on the protected site.

Transmission des événements

Separate dialler reference	Dialler unit reference	For transmission of an alarm to an INDIVIDUAL	For transmission of an alarm to a REMOTE MONITORING CENTRE
SH511AX	SH501AX	voice via PSTN network	via PSTN and ADSL network
SH512AX	SH502AX	voice and SMS via GSM network	via GSM and (ADSL or GPRS) network
SH513AX	SH503AX	voice via PSTN network or voice and SMS via GSM network	via (PSTN or GSM) network and (ADSL or GRS)
SH514AX	SH504AX	with remote monitoring service contract (ADSL)	via ADSL network

Transmission of alarm images and films

Separate dialler reference	Dialler unit reference	For transmission of images from image transmission motion detectors or IP cameras to an INDIVIDUAL	For transmission of alarm films from image transmission motion detectors or IP cameras to a REMOTE MONITORING CENTRE
SH511AX	SH501AX	with remote monitoring service contract (ADSL)	via ADSL network
SH512AX	SH502AX	MMS via GSM with MMS option (to n° 9)	via ADSL or GPRS network
SH513AX	SH503AX	MMS via GSM with MMS option (to n° 9)	via ADSL or GPRS network
SH514AX	SH504AX	with remote monitoring service contract (ADSL)	via ADSL network

1.2 Operation for incoming calls

- **The remote control function via the phone** (landline and/or mobile) using a dialler fitted with a PSTN or GSM module (mains-powered) makes it possible to:
 - remotely operate the alarm system (disarm, arm the system),
 - start a listen-in period (repeatable) to remotely listen in to background sounds,
 - speak out to a person on the premises where the alarm has been triggered by remotely activating the loudspeaker,
 - operate comfort applications (e.g. lighting) using external receivers,
 - modify correspondent telephone numbers (for calls to individuals).
- When no event has been triggered, the secure **Internet Portal**, which can be accessed from a computer via the DAITEM web site, makes it possible to connect up to a dialler linked to the Ethernet (ADSL) or GPRS (mains-powered) network in order to:
 - check the system status (installation, armed, disarmed, etc.), faults, access points, etc.)
 - perform a simple system configuration operation (change telephone numbers for calls, etc.),
 - operate the system (change the system status, operate receivers, etc.),
 - consult and save the system events log,

ONLY WITH THE USE OF IMAGE TRANSMISSION DETECTORS

- change the video code,
- consult archived alarm films from image transmission detectors,
- ask an image transmission detector to film the protected site.

GSM/
GPRS ETHERNET
(ADSL)

ONLY WITH COMPATIBLE IP CAMERAS

- change the video code,
- consult archived alarm films from IP cameras,
- view live video from IP cameras (only possible with Ethernet/ADSL media via Internet).

GSM/
GPRS ETHERNET
(ADSL)

2. Configuring a dialler locally using the built-in keypad

Your installer will have already configured your dialler but you can modify some of the programming at any time.

If 5 wrong access codes are entered on the keypad in less than 5 minutes this will block the keypad for 5 minutes and the control panel will be informed.

2.1 Modifying the language

You can replace the original language with another language.

To modify the language, enter:

□ □ □ □ * 1 7 * □ * *

master code

0: French 3: Spanish
1: Italian 4: Dutch
2: German 5: English

"bip + chosen language"



Factory setting: French

2.2 Modifying the date and time

The events memorised by the dialler are date and time stamped.

To programme the date and time manually, proceed as follows:

• Date

To consult the date, enter: □ □ □ □ * 7 0 * # * *

master code

To modify the date, enter: □ □ □ □ * 7 0 * □ □ * □ □ * □ □ * *

master code

Day
(1 to 31)

Month
(1 to 12)

Year
(e.g. for 2012,
enter 12)

"bip + date announced"



• Time

To consult the time, enter: □ □ □ □ * 7 1 * # * *

master code

To modify the time, enter: □ □ □ □ * 7 1 * □ □ * □ □ * *

master code

Hour
(0 to 24)

Minutes
(0 to 59)

"bip + time announced"



2.3 Modifying your master code

Do not lose your codes as you will need them in order to programme new codes. However, if you do lose your codes, contact your installer who will put the system back into its factory configuration and programme the codes again. Your master code allows you to configure the dialler and access all the system commands using the built-in keypad. Your master code can also be used to access your device remotely (using a telephone or a computer connected to the dialler via the secure Internet Portal):

IMPORTANT

- To keep your codes confidential, we recommend you change the keypad access codes often and regularly clean the keys.
- To prevent unwanted calls to correspondents, do not end the master code with a "0".

To modify the master code, enter:

□ ... □ * 5 0 * □ ... □ * □ ... □ * *

old master code

new master code

new master code

IMPORTANT: access codes must all be different.

Factory master code: 0000

Example:

To replace the factory master code "0000" with the new code "1423", enter:

0 0 0 0 * 5 0 * 1 4 2 3 * 1 4 2 3 * *

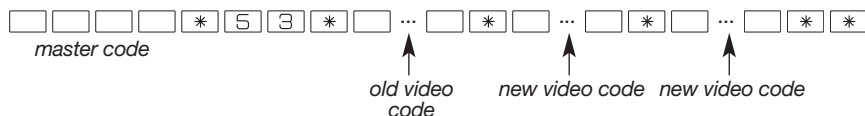
"beep"



IMPORTANT

- To ensure privacy, videos can only be accessed via the secure Internet Portal using a video access code specific to the user.
- Precautions when choosing the code:
 - do not use 1234, 7654 or 2468 type sequences,
 - do not choose the same code as the master code,
 - do not make a note of your codes anywhere.
- These parameters can be modified via the Daitem secure Internet Portal.

To modify the video code, enter



Factory video code: 4444

2.5 Enabling or disabling remote access via the Internet (mains-powered GPRS – Ethernet ADSL)

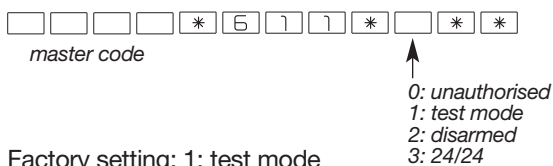
Accessing the dialler remotely using a computer connected via Internet (mains-powered GPRS or Ethernet media)

- The installer (or remote monitoring centre) will call you to switch the system to **test mode**. Using a computer and TwinLoad® configuration and maintenance software, your installer or centre can perform remote maintenance operations in **(factory) test mode**.
- You can authorise your installer to remotely access your dialler in installation or user mode **(only when the system is disarmed or 24/24 = system armed or disarmed)**.

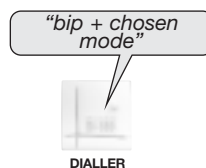
Whatever the case, video (if there is any video) can only be accessed using your personal video code during the identification phase following remote access to your dialler from a computer connected via the secure Internet Portal.

Your dialler's factory configuration does not allow access to your installer (or remote monitoring centre) in installation or user mode but you can modify this access at any time. Your installer will help you to define the best procedure for you.

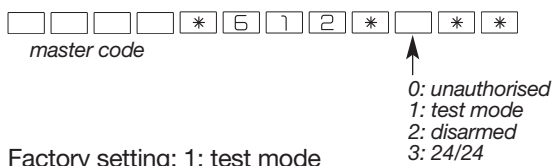
A. To modify the installer's authorisation to access the system remotely using a computer equipped with TwinLoad® configuration and maintenance software, enter:



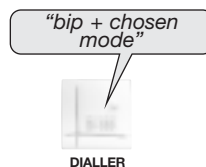
Factory setting: 1: test mode



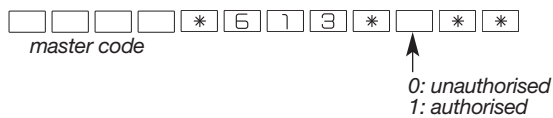
B. To modify the remote monitoring centre's authorisation to access the system remotely using a computer equipped with TwinLoad® configuration and maintenance software, enter:



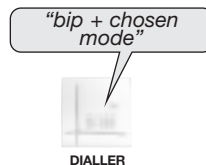
Factory setting: 1: test mode



C. To modify the user's authorisation to access the system remotely via the Daitem secure Internet Portal, enter:



Factory setting: 1: authorised



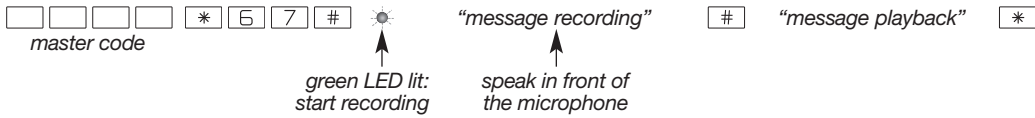
2.6 Recording or modifying the personalised welcome message for vocal transmissions

PSTN GSM

IMPORTANT: it is advisable to speak in front of the microphone.

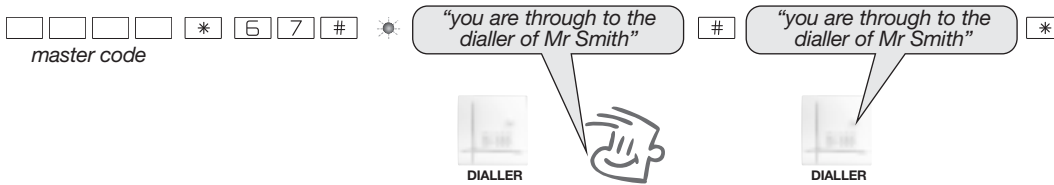
The personalised voice message (lasting 10 seconds maximum) allows correspondents to identify the dialler having triggered the call.

To record the message, enter:



Example of personalised voice message

• Enter:



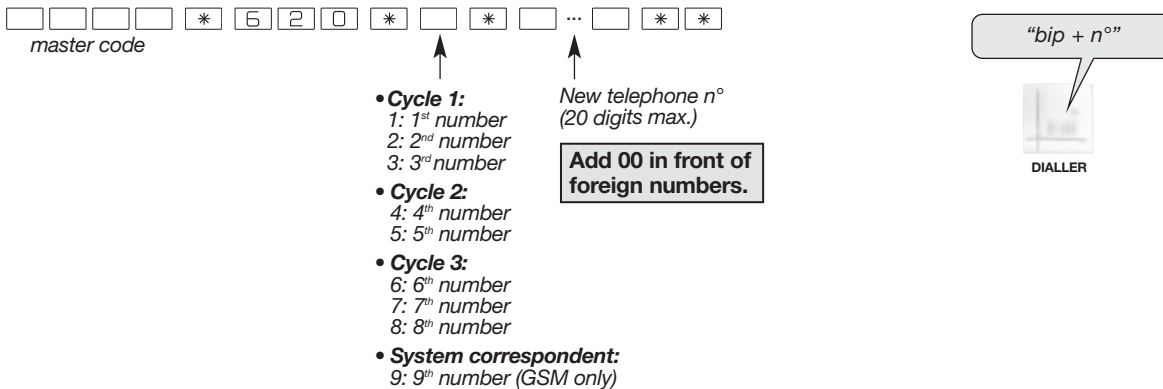
2.7 Modifying the numbers of your individual correspondents (PSTN-GSM)

PSTN GSM

Your installer will have already programmed for you the telephone numbers of your correspondents for calls to individuals. This programming only allows numbers that have already been programmed for calls to individuals to be **modified** in user mode. It is not possible to check or delete them.

IMPORTANT: this operation does not allow you to completely programme telephone numbers for calls to individuals and a remote monitoring centre (SMS/PSTN protocol, listen-in, etc.). Contact your installer for this if necessary.

To modify the correspondent number programmed for calls to individuals, enter:



3. Outgoing calls

The dialler remotely alerts correspondents of intrusion or other events occurring on the protected site.

3.1 Dialler call cycle procedure

If your first correspondent does not answer the call, is already engaged or has not terminated the call cycle properly:

- the dialler calls the number recorded in the next memory,
- if none of the correspondents acknowledge or terminate the call cycle or they are all engaged or not answering, the dialler goes through the complete call cycle.

Example: call cycle with 3 different types of cycle (intrusion, fire, fault):

		Procedure	Acknowledgement and termination
Cycle 1:	number 1 number 2 number 3		For each cycle, if the first calls are not acknowledged and terminated, the dialler continues on to the next numbers in the same cycle. When one of the calls in the cycle is acknowledged, the dialler stops transmission.
Cycle 2:	number 4 number 5		
Cycle 3:	number 6 number 7 number 8		

IMPORTANT

• If the alarm control panel issues a disarm order during the cycle:

- for calls to individuals: the dialler issues the voice message “Off, Control_ panel” and immediately puts an end to communication,
- for calls to a remote monitoring centre: the dialler terminates the call underway and transmits the “Off” order if the call is answered.

• Your installer can be directly warned of any fault with the system, regardless of alarm transmissions.

System correspondent

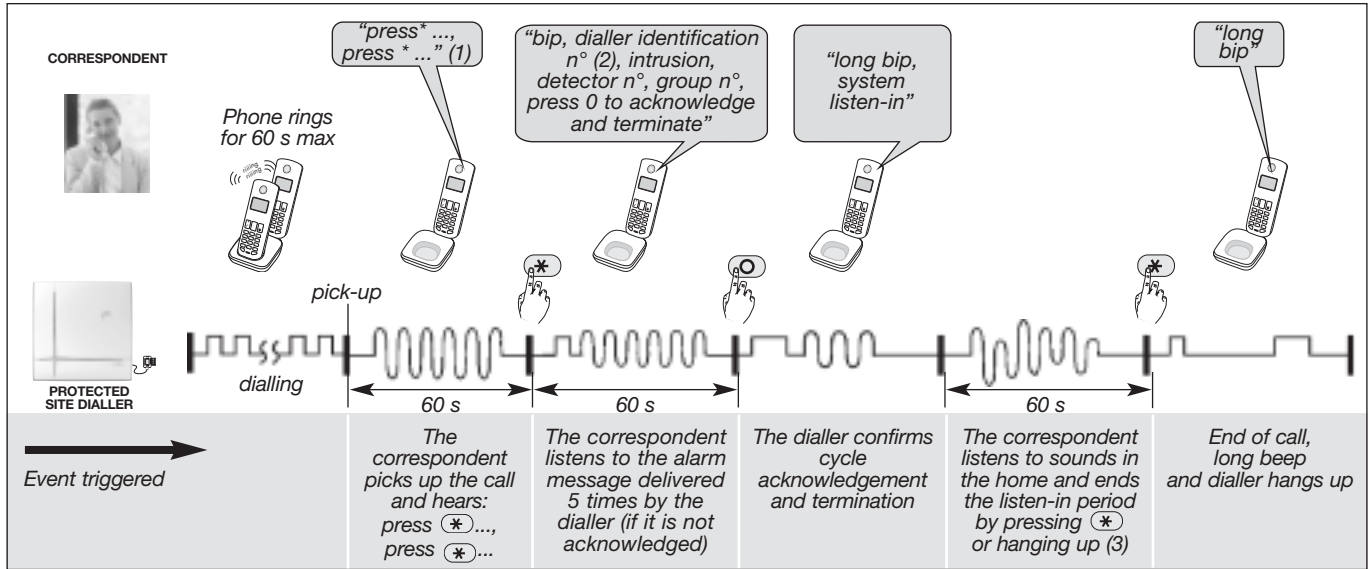
GSM/GPRS

A 9th number is programmed to be the “system correspondent” number for receiving:

- SMS messages for the “credit monitoring” function (if activated),
- the list of SMS (every 3 days if the system correspondent has been programmed),
- MMS images from IP cameras or detectors recognised by the control panel and the dialler (MMS parameters set),
- the date the validity of the SIM card ends (if card activated).

3.2 Procedure for voice calls to individuals

PSTN GSM



N.B. for calls to an individual using SMS and MMS digital protocol:

- each correspondent, from n° 1 to 8, can receive SMS alarm calls via the GSM network. The numbers programmed for SMS cannot acknowledge and terminate the call cycle underway.
- the individual system correspondent, n° 9, can receive up to 5 MMS alarm images via the GSM network with the MMS option.

- (1) Voice call to an individual with automatic listen-in if this has been programmed (for GSM voice calls there is no message inviting the correspondent to "press *").
- (2) For vocal transmissions, this identification message can be replaced with a voice message (see Configuring the dialler locally using the built-in keypad/Recording or modifying the personalised welcome message for vocal transmissions).
- (3) Telephone transmission can be followed by a listen-in period during which the correspondent can listen in to what is happening on the protected premises in order to confirm the alarm and issue telephone commands.

: press (*) on the telephone handset during the listen-in period when you want to stop listen-in and end the call.

3.3 List of possible commands during the listen-in period

Depending on the alarm transmitted and the parameters set on the dialler by the installer, a listen-in and speak-out/talk-back period can be activated. During this period, commands can be sent to the system using the telephone handset keys.

Command description	Command n°
Disarm command relay 1	11
relay 2	12
relay 3 for comfort type applications using	13
relay 4 the Daitem receiver (lighting, etc.)	14
Arm command relay 1	21
relay 2	22
relay 3	23
relay 4	24
Stop siren	30
Activate siren	31
Repeat listen-in period for 60 s (5 times max.)	#
Stop listen-in and hang up dialler	*
Allow speak-out/talk-back	7
Allow listen-in	8
Allow speak-out/talk-back and listen-in (1)	9

(1) Function only available with GSM media

List of events enabling listen-in period:

- Intrusion
- Intrusion confirmed
- Tamper
- Alarm
- Silent alarm
- Test call

3.4 List of messages and SMS transmitted according to the type of event (PSTN-GSM)

Events	"message"	Type of transmission	
		Voice PSTN GSM	SMS GSM
Intrusion	"Intrusion detector N° , group N° "	X	X
Intrusion confirmed	"Intrusion confirmed detector N° , group N° "	X	X
Fire alarm	"Fire Alarm PER N° "	X	X
Prealarm	"Prealarm, detector N° , group N° "	X	X
Prealarm confirmed	"Prealarm confirmed, detector N° , group N° "	X	X
Deterrence	"Deterrence, detector N° , group N° "	X	X
Deterrence confirmed	"Deterrence confirmed, detector N° , group N° "	X	X
Tamper	"Tamper PER N° "	X	X
Main battery fault	"Fault battery voltage PER N° "	X	X
Back-up battery fault	"Fault accumulator voltage PER N° "	X	X
Radio link fault	"Fault Radio link PER N° "	X	X
Radio tamper	"Radio Tamper PER N° "	X	X
Telephone line tamper	"Telephone line Tamper N° "	X	X
GSM scrambling tamper	"GSM Interference tamper"	X	X
Alarm and silent alarm	"Alert PER N° "	X	X
Test call	"Test call"	X	X
Mains connected	"Mains connected PER N° "	X	X
Mains disconnected	"Mains disconnected PER N° "	X	X
General technical alarm	"Technical alarm PER N° "	X	X
SIM credit monitoring	"Text operator"		X
MMS transfer (GSM with MMS option)	"Alarm video"		X
Test cycle call	"Test cycle call"		X
Totally arm	"Total armed"		X
Arm group	"Armed Group N° "		X
Partially arm 1	"Armed partial 1"		X
Partially arm 2	"Armed partial 2"		X
Totally disarm	"Off"		X
Disarm group	"Off group N° "		X

Format of messages transmitted: dialler, identification, "message":

• identification:

- for **voice** type messages: corresponds to the identification of the number programmed for voice calls or to the personalised welcome message recorded for vocal transmissions only,
- for **SMS** type messages: corresponds to the identification of the number programmed for **SMS**.

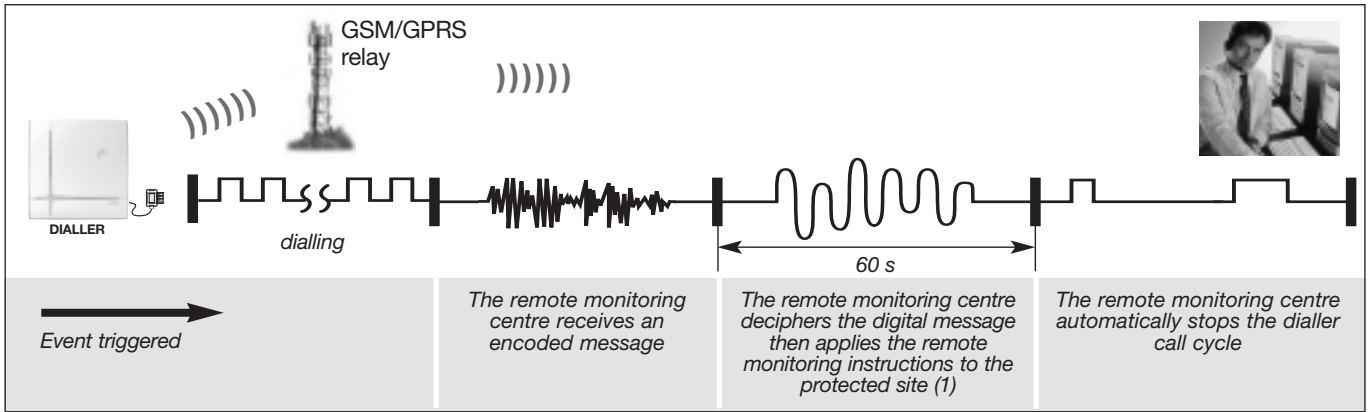
• "message":

- **PER**: corresponds to the name of the peripheral (control panel, control panel with dialler, detector, remote control unit, siren, dialler, device, alarm device, radio repeater relay),
- **N°**: number of peripheral, of group, etc.

3.5 Procedure for calls to a remote monitoring centre

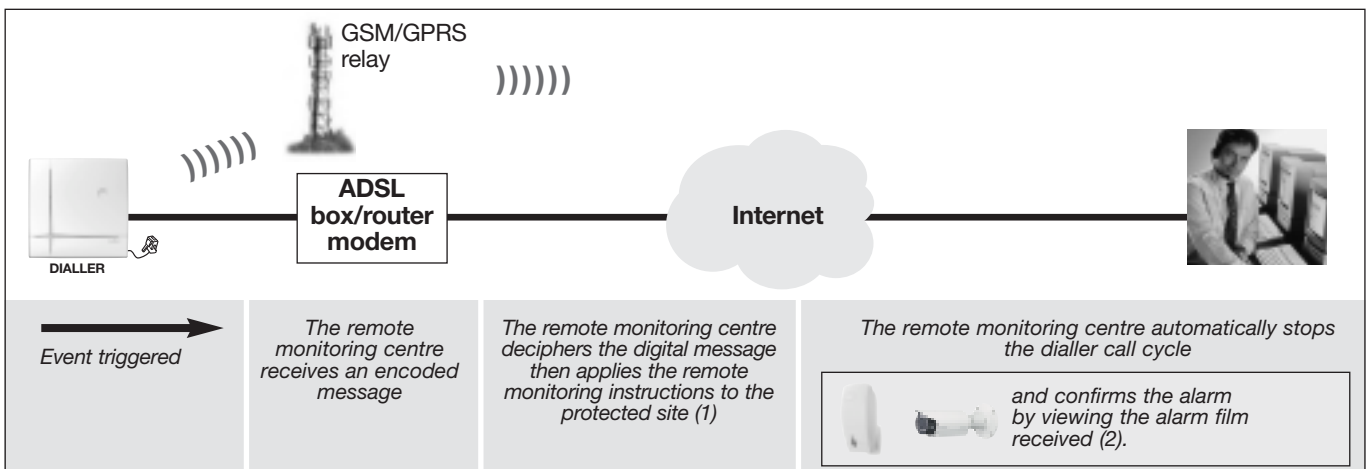
PSTN GSM/GPRS ETHERNET (ADSL)

- Procedure for calls to a remote monitoring centre via the PSTN network (Contact ID or FSK200 analogical digital protocol) or GSM network (Contact ID protocol)



(1) The telephone transmission can be followed by a listen-in period during which the remote monitoring centre can listen in to what is happening on the protected premises in order to confirm the alarm and issue telephone commands.

- Procedure for calls to a remote monitoring centre via the Ethernet (ADSL) or GPRS network (ViewCom IP digital protocol)



(1) The alarm transmission via the Ethernet (ADSL) network can be followed by a listen-in period for the remote monitoring centre.

(2) The remote monitoring centre can also view the video in real time (live) but only when compatible IP cameras managed by the dialler unit are used.

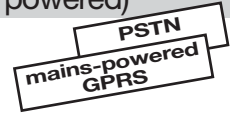
4. Incoming calls

The dialler can be operated remotely either using a telephone (PSTN or GSM) or a computer via the Internet (as well as via applications dedicated to Smartphones and touch-screen tablets).

4.1 Voice remote operation over the telephone via the PSTN or GSM network (mains powered)

4.1.1 Summary table of command codes for remote operation over the phone

Below is a list of commands that can be sent remotely over the phone

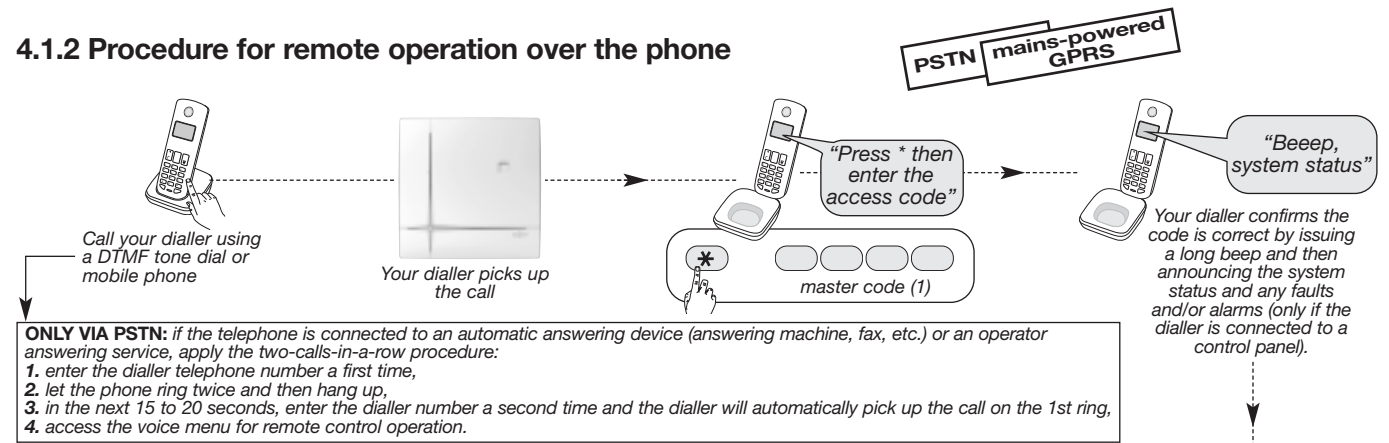


Command N°	Command description	Command N°	Command description	Command N°	Command description
4	System status query	82	Off relay 3 (2)	149	Off group 2 4
21	Totally disarm	84	On relay 3 (2)	151	Off group 1 2 4
23	Totally arm	86	Toggle switch relay 3 (2)	153	Off group 3 4
25	Partially arm 1	88	Timer relay 3 (2)	155	Off group 1 3 4
27	Partially arm 2	90	Pulse relay 4 (1)	157	Off group 2 3 4
33	Arm presence	92	Off relay 4 (2)	159	Off group 1 2 3 4
50	Pulse light (1)	94	On relay 4 (2)	163	Arm group 1
52	Light OFF (2)	96	Toggle switch relay 4 (2)	165	Arm group 2
54	Light ON (2)	98	Timer relay 4 (2)	167	Arm group 1 2
56	Light toggle switch (2)	112	Off control panel relay 1	169	Arm group 3
58	Light timer (2)	114	On control panel relay 1	171	Arm group 1 3
60	Pulse relay 1 (1)	122	Off control panel relay 2	173	Arm group 2 3
62	Off relay 1 (2)	124	On control panel relay 2	175	Arm group 1 2 3
64	On relay 1 (2)	131	Off group 1	177	Arm group 4
66	Toggle switch relay 1 (2)	133	Off group 2	179	Arm group 1 4
68	Timer relay 1 (2)	135	Off group 1 2	181	Arm group 2 4
70	Pulse relay 2 (1)	137	Off group 3	183	Arm group 1 2 4
72	Off relay 1 (2)	139	Off group 1 3	185	Arm group 3 4
74	On relay 2 (2)	141	Off group 2 3	187	Arm group 1 3 4
76	Toggle switch relay 2 (2)	143	Off group 1 2 3	189	Arm group 2 3 4
78	Timer relay 2 (2)	145	Off group 4	191	Arm group 1 2 3 4
80	Pulse relay 3 (1)	147	Off group 1 4		

(1) Control receiver command possible (via control panel).

(2) Control receiver or remote-controlled socket command possible (via control panel).

4.1.2 Procedure for remote operation over the phone



What to press on handset unit keypad	Result
<p>“Voice menu proposed”</p> <p>“To consult system status press ”</p>	<p>› system status announced</p>
<p>“To modify system status press ”</p> <p>“To disarm press ” (2)</p> <p>“To arm press ” (2)</p> <p>“For menu press ” (2)</p>	<p>› control panel disarmed</p> <p>› control panel armed</p> <p>› return to main menu</p>
<p>“To modify call number press ”</p> <p>“Press n° then ”</p> <p>“To consult press ”</p> <p>“To modify press ” (3)</p> <p>“For menu press ”</p>	<p>› recorded n° announced</p> <p>› new number recorded announced</p> <p>› return to main menu</p>
<p>“For system command press ”</p> <p>“Enter command”</p> <p> command n°</p>	<p>› command sent (see summary table of remote control command codes on previous page)</p>
<p>“To listen in press ”</p> <p>Options during Listen-in:</p> <p> speak-out/talk-back activated</p> <p> listen-in activated</p> <p> intercom activated</p> <p> intercom stopped and return to main menu</p>	<p>› Listen-in is active</p>
<p>“For menu press ”</p>	<p>› return to main menu</p>

- If the user does not press a key during any of the menus listed above, the dialler repeats the menu every 5 s (5 times max) before automatically hanging up.
- Press on your telephone handset unit keypad to return to the initial voice menu at any time.

(1) If 5 wrong master codes are entered in less than 5 minutes, the dialler hangs up and remote control operation is disabled for 5 minutes.
 (2) If the control panel does not respond, you will hear the message “Bip, Radio Fault”.
 (3) Only numbers can be remotely modified and not the protocols (voice, SMS) and associated options.
 (4) Function only available with GSM media.

4.2 Configuring and operating the dialler from a PC connected via the Internet

mains-powered
GPRS
ETHERNET
(ADSL)

You can connect up to your alarm system via the Internet using a PC in order to configure and operate the system. Access is possible in user mode if the dialler is connected to the Ethernet (ADSL) network or GPRS network (mains-powered dialler) and subject to the rights controlled by the user during programming of parameter 613 (factory setting: access authorised, see chapter on **Configuring the dialler locally using the built-in keypad/Enabling or disabling remote access via the Internet**).

4.2.1 General

This paragraph describes the implementation and use of the secure Internet Portal accessible via the DAITEM site. It does not explain how Vista MS-Windows or the web browser works. For more information about these environments, refer to the corresponding manuals.

The Daitem Internet Portal can be accessed from a PC fitted with Internet Explorer, Firefox or Chrome (as well as using applications dedicated to Smartphones and touch-screen tablets: iPhone/iPad and Android).

4.2.2 How the Daitem secure Internet Portal works

The Daitem Internet Portal is designed to operate the system. It has the following functionalities:

- connection to a dialler via the Internet (using Ethernet (ADSL) or mains-powered GPRS media),
- provision of information about the system (installation, arming, disarming, etc.), faults and access,
- simple system configuration (changing telephone numbers for calls),
- operating the system (changing the system status, issuing receiver commands, etc.),
- consulting and saving the system events log,

ONLY WITH THE USE OF IMAGE TRANSMISSION DETECTORS

- change the video code,
- consult archived alarm films from image transmission detectors,
- ask an image transmission detector to film the protected site,

GSM/
GPRS
ETHERNET
(ADSL)

ONLY WITH COMPATIBLE IP CAMERAS

- change the video code,
- consult archived alarm films shot by IP cameras,
- instantly view (real time) video shot by IP cameras (only possible with Ethernet/ADSL media via Internet).

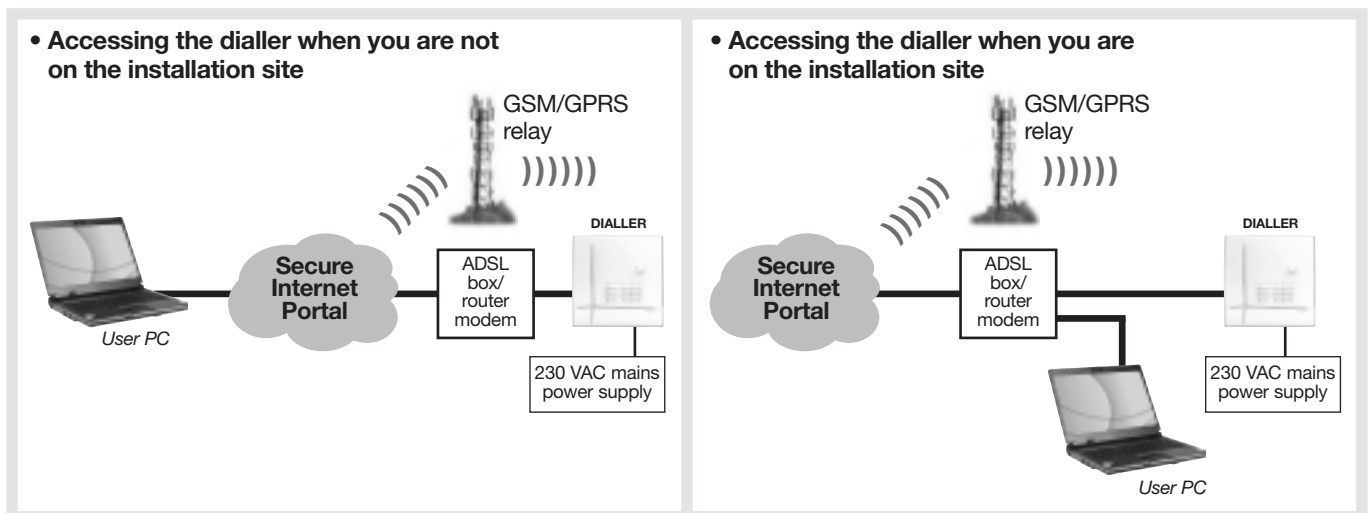
GSM/
GPRS
ETHERNET
(ADSL)

4.2.3 Warning

In case of video use only: the first “live video” consultation may require the installation of an additional ActiveX, Plugin or Applet java module.

4.2.4 Accessing the alarm system via the secure Internet Portal

A. BLOCK DIAGRAMS




B. ACCESSING THE PORTAL

1. Open your web browser on your PC (Internet Explorer, Firefox).
2. Go to the Daitem web site and click on the link which gives access to the dedicated portal.
3. Follow the instructions in the different menus

4.3 Remote operation over SMS via the GSM network (mains-powered)

mains-powered
GSM

To operate your system by SMS, send an SMS message to the Control/communicator using a mobile phone with the following syntax: **master code # command number # #**.



Command N°	Command description
21	Totally disarm
23	Totally arm
25	Partially arm 1
27	Partially arm 2
33	Arm presence

NB: if the transmission of the ON/OFF command is successful, the user can receive confirmation messages of ON total /OFF total of the system.

5. Testing calls to your correspondents

PSTN

GSM/
GPRS

ETHERNET
(ADSL)

All programmed numbers can be tested separately. The test procedure is identical whatever the transmission media. For voice calls and SMS, the message transmitted is "Dialler identification n°, test call". For calls to a remote monitoring centre, the message transmitted is encoded according to FSK200 Bauds, Contact ID and ViewCom IP protocols and the media used.

- First let your correspondents know you are going to perform a test call.
- We advise you to systematically perform a test call every time you record a new number.

1. Put the dialler in test mode:

□ □ □ □ # 2 # #
master code

2. To trigger a test call, enter:

□ □ □ □ # 5 8 □ # #

master code

↑

1: 1 st number	} Cycle 1	6: 1 st number	} Cycle 3
2: 2 nd number		7: 2 nd number	
3: 3 rd number		8: 3 rd number	
4: 1 st number	} Cycle 2	9: system correspondent number	
5: 2 nd number		(GSM/GPRS only)	



DIALLER

3. Wait until the end of the test call and then check the alarm has been telephone transmitted to the programmed correspondents.

4. Switch the dialler to user mode:

□ □ □ □ # 7 # #
master code

6. Instructions sheet (to be filled in and given to your correspondents)

PSTN GSM/GPRS

- The correspondent can acknowledge and terminate the dialler call cycle: yes no

When you pick up the phone you will hear:

- a voice message repeated several times specifying the event having triggered the call,
- a request to acknowledge the dialler: "Press 0 to acknowledge".

- If you are not supposed to acknowledge and terminate the dialler's call cycle, hang up.
- If you are supposed to acknowledge and terminate the dialler's call cycle, press 0 on the your telephone handset and you will hear a long confirmation beep.

- The correspondent can listen in to what is happening on the protected premises: yes no

Correspondents whose number has been programmed with the listen-in option can listen in to what is happening on the protected premises for 60 seconds (once the message has been delivered). This period can be repeated 4 times by pressing on the telephone handset # key.

Command description	Command n°
Disarm command relay 1	11
relay 2	12
relay 3 <i>for comfort type</i>	13
relay 4 <i>applications using</i>	14
Arm command relay 1 <i>the Daitem receiver</i>	21
relay 2 <i>(lighting, etc.)</i>	22
relay 3	23
relay 4	24
Stop siren	30
Activate siren	31
Repeat listen-in period for 60 s (5 times max.)	#
Stop listen-in and hang up dialler	*
Allow speak-out/talk-back	7
Allow listen-in	8
Allow speak-out/talk-back and listen-in (1)	9

(1) Function only available with GSM media

• General information about the caller:

Name: _____ Tel.: _____

Address: _____

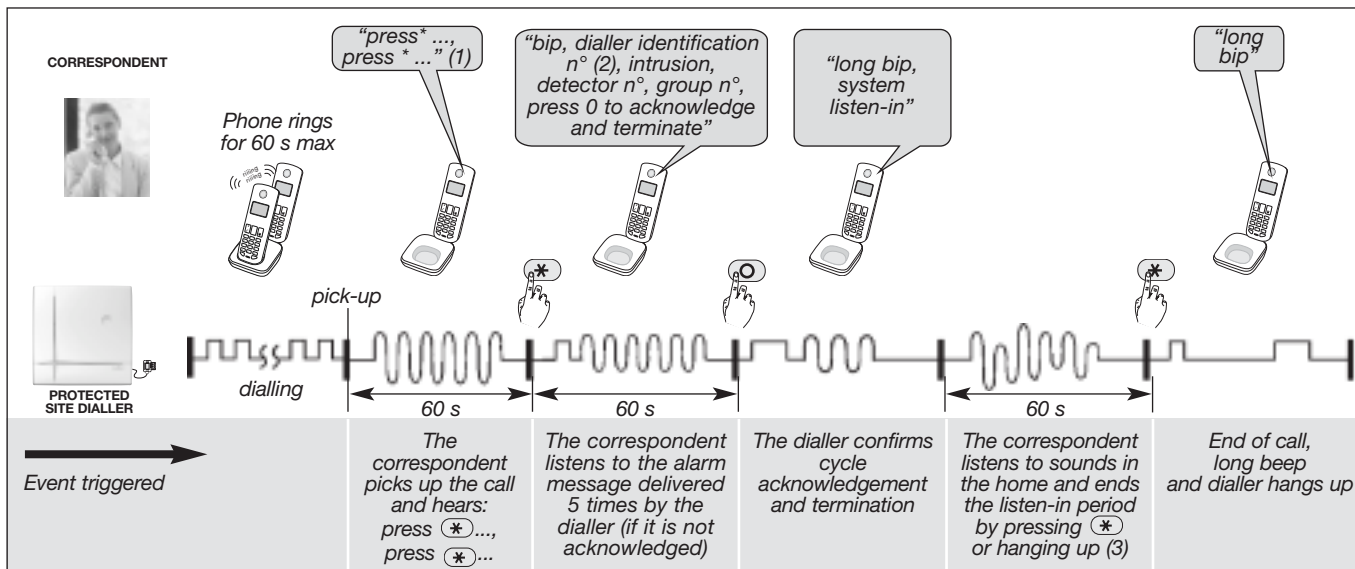
Identification n°: _____

Welcome message (if a message has been recorded this replaces the identification number): _____

• Instructions:

Make a note of the instructions to be followed if the dialler calls.

• Telephone call procedure



N.B. for calls to an individual using SMS and MMS digital protocol:

- each correspondent, from n° 1 to 8, can receive SMS alarm calls via the GSM network. The numbers programmed for SMS cannot acknowledge and terminate the call cycle underway.
- the individual system correspondent, n° 9, can receive up to 5 MMS alarm images via the GSM network with the MMS option.

- (1) Voice call to an individual with automatic listen-in if this has been programmed (for GSM voice calls there is no message inviting the correspondent to “press *”).
- (2) For vocal transmissions, this identification message can be replaced with a voice message (see Configuring the dialler locally using the built-in keypad/Recording or modifying the personalised welcome message for vocal transmissions).
- (3) Telephone transmission can be followed by a listen-in period during which the correspondent can listen in to what is happening on the protected premises in order to confirm the alarm and issue telephone commands.

• Meaning of the messages received

Your dialler delivers a message corresponding to the event having triggered the call. You must tell your correspondents what they are supposed to do depending on the message they receive (go to your home, contact a public service, etc.).

IMPORTANT: if a welcome message has been recorded this replaces the identification number.

Events	“message”	Acknowledgement	
		Yes	NO
Intrusion	“Intrusion detector N°, group N°”		
Intrusion confirmed	“Intrusion confirmed detector N°, group N°”		
Fire alarm	“Fire Alarm PER N°”		
Prealarm	“Prealarm, detector N°, group N°”		
Prealarm confirmed	“Prealarm confirmed, detector N°, group N°”		
Deterrence	“Deterrence, detector N°, group N°”		
Deterrence confirmed	“Deterrence confirmed, detector N°, group N°”		
Tamper	“Tamper PER N°”		
Main battery fault	“Fault battery voltage PER N°”		
Back-up battery fault	“Fault accumulator voltage PER N°”		
Radio link fault	“Fault Radio link PER N°”		
Radio tamper	“Radio Tamper PER N°”		
Telephone line tamper	“Telephone line Tamper N°”		
GSM scrambling tamper	“GSM Interference tamper”		
Alarm and silent alarm	“Alert PER N°”		
Test call	“Test call”		
Mains connected	“Mains connected PER N°”		
Mains disconnected	“Mains disconnected PER N°”		
General technical alarm	“Technical alarm PER N°”		

Format of messages transmitted: dialler, identification, “voice message”:

- identification for **voice** type messages: corresponds to the identification of the number programmed for voice calls or to the personalised welcome message recorded for vocal transmissions only,
- **“voice message”:**
 - **PER:** corresponds to the name of the peripheral (control panel, control panel with dialler, detector, remote control unit, siren, dialler, device, alarm device, radio repeater relay),
 - **N°:** number of peripheral, of group, etc.

ATRAL SYSTEM guarantees its DAITEM products for 2 years commencing from date of purchase by the initial user.

IMPORTANT: this guarantee is automatically extended to 5 YEARS if the guarantee extension request form opposite is correctly completed (including the installer's stamp, purchase date, the guarantee label for the system plus the guarantee labels of the other products making up the installation) and is returned to ATRAL SYSTEM within 10 days of purchase.

Where subsequent add-on accessories are concerned, you simply need to return the guarantee extension form for the additional products in order that they may also be included.

Any possible unavailability occurring on the networks – the availability of telecommunications networks (public telephone network, GSM...) cannot be 100% guaranteed – may result in the unavailability of our own systems, without engaging the liability of ATRAL SYSTEM.

In addition, this guarantee cannot be applied in cases of:

- Incorrect usage
- Installation not in conformity to ATRAL SYSTEM specifications
- Interference with the electronics
- Breakage through fall or impact
- Mechanical or electronic alteration of the product
- Use of supplies other than those recommended by ATRAL SYSTEM
- Natural disaster, atmospheric phenomena or vandalism.

Products suspected of being faulty must be returned to ATRAL SYSTEM by the installer in accordance with the instructions provided by DAITEM technical support, accompanied by the duplicate of the purchase order. Products are transported at the sender's expense and risk, and carriage forward returns will be refused by the ATRAL SYSTEM goods inwards department. All products that are the object of an exchange become the property of ATRAL SYSTEM.

It is recommended that all invoices relating to products be carefully conserved, as you may be required to produce them for application of the guarantee.

In the interest of improving its products, ATRAL SYSTEM reserves the right to modify them without prior notice.

DAITEM offers a technical telephone helpline. For all technical questions, or before returning any product, contact DAITEM technical support, who will inform you of the best procedure to follow for the particular case.

The DAITEM guarantee covers the products only, not including batteries.

Furthermore, the installation and any possible maintenance operations are the responsibility of the installer and are not covered by this guarantee (apart from errors in the assembly instructions).

As a general rule, the DAITEM guarantee entitles customers to the exchange of products recognised as faulty by ATRAL SYSTEM.

In exceptional circumstances, ATRAL SYSTEM reserves the right to choose to carry out repairs to products.

ATRAL SYSTEM shall undertake to replace defective products with an identical or equivalent product within the guarantee period.

All products exchanged under guarantee benefit from the remaining guarantee period of the original product.

**GM Techtronics Ltd.
Unit 17 Paxcroft Farm
Hilperton - Trowbridge - Wiltshire
BA14 6JB England**



DAITEM ***Guarantee extension form***

Section to be returned

We recommend that you complete the system guarantee extension form now.

Stick the guarantee label for each product in the appropriate space. If you have just bought several products (even with different references), only return this guarantee extension form for all the products.

Mr Mrs Miss Comp. Surname First name

Address

Postcode Town Tel.

E-mail

System	Tick the appropriate box:
Guarantee label	<input type="checkbox"/> Purchase <input type="checkbox"/> Replacement outside guarantee <input type="checkbox"/> Replacement within guarantee

Product(s) purchased on:

Telephone transmitter	Tick the appropriate box:
Guarantee label	<input type="checkbox"/> Purchase <input type="checkbox"/> Replacement outside guarantee <input type="checkbox"/> Replacement within guarantee

— Installer's stamp —

Other products

Guarantee label

— Area reserved for DAITEM —


Received on:



Product(s) purchased on:

Installer's stamp

GM Techtronics Ltd.
Unit 17 Paxcroft Farm
Hilperton - Trowbridge - Wiltshire
BA14 6JB England

 **Waste processing of electrical and electronic devices at the end of their service life** (Applicable in European Union countries and other European countries with a waste collection system). Used on products or product packaging, this symbol indicates that the product must not be thrown out with household waste. It must be taken to a waste collection point for electrical and electronic product recycling. When you make sure that this product is disposed of in the most appropriate manner, you are helping to protect the environment and human health. If you would like additional information concerning the recycling of this product, please contact your town/city council, nearest waste collection centre or the shop where you bought the product.

Daitem undertakes to treat this information in its entirety as strictly confidential.

<p>What are the protected premises used for?</p> <p>Main home <input type="checkbox"/></p> <p>Second home <input type="checkbox"/></p> <p>Business premises <input type="checkbox"/></p> <p>What type are the protected premises?</p> <p>Individual house <input type="checkbox"/></p> <p>Flat <input type="checkbox"/></p> <p>Shop <input type="checkbox"/></p> <p>Offices <input type="checkbox"/></p> <p>Stores and warehouses <input type="checkbox"/></p> <p>Factory <input type="checkbox"/></p> <p>Other <input type="checkbox"/></p> <p>Are you...?</p> <p>An owner <input type="checkbox"/></p> <p>A tenant <input type="checkbox"/></p> <p>How did you hear about Daitem?</p> <p>Advertising <input type="checkbox"/></p> <p>Professional recommendation <input type="checkbox"/></p> <p>Friend's advice <input type="checkbox"/></p> <p>On the Internet <input type="checkbox"/></p> <p>At a trade fair <input type="checkbox"/></p> <p>Other <input type="checkbox"/></p> <p>Do you have an alarm system already?</p> <p>Yes, to protect these premises <input type="checkbox"/></p> <p>Yes, to protect other premises <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>	<p>Is the user guide clear?</p> <p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p> <p>Please tick the 3 main reasons for your purchase:</p> <p>Ease of use <input type="checkbox"/></p> <p>Ease of installation <input type="checkbox"/></p> <p>Efficiency of system <input type="checkbox"/></p> <p>Independence from 230V mains power <input type="checkbox"/></p> <p>Reputation of brand <input type="checkbox"/></p> <p>Product aesthetics <input type="checkbox"/></p> <p>Upgradeable nature of system <input type="checkbox"/></p> <p>Did the 100% wire free technology play a part in your choice?</p> <p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p> <p>Did the quality/price ratio appear to you to be:</p> <p>Good <input type="checkbox"/></p> <p>Quite good <input type="checkbox"/></p> <p>Quite poor <input type="checkbox"/></p> <p>Poor <input type="checkbox"/></p>	<p>If you live in an individual house, which of the following is your accommodation equipped with?</p> <p>Door with access code <input type="checkbox"/></p> <p>Intercom system <input type="checkbox"/></p> <p>Videophone <input type="checkbox"/></p> <p>Doorbell only <input type="checkbox"/></p> <p>Automated gate <input type="checkbox"/></p> <p>Non-automated gate <input type="checkbox"/></p> <p>Automated garage door <input type="checkbox"/></p> <p>Non-automated garage door <input type="checkbox"/></p> <p>A garden or yard <input type="checkbox"/></p> <p>Do you own a personal computer?</p> <p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p> <p>Do you have access to the Internet?</p> <p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p> <p>Profession of head of household (or your profession where business premises are concerned)</p> <p>Farmer <input type="checkbox"/></p> <p>Shopkeeper, craftsperson, company owner <input type="checkbox"/></p> <p>Executive <input type="checkbox"/></p> <p>Middle management, technician, supervisor <input type="checkbox"/></p> <p>Employee <input type="checkbox"/></p> <p>Worker <input type="checkbox"/></p> <p>Retired <input type="checkbox"/></p> <p>Inactive for other reasons <input type="checkbox"/></p>	<p>Age of head of household (or your age where business premises are concerned)</p> <p>Less than 30 <input type="checkbox"/></p> <p>Between 30 and 39 <input type="checkbox"/></p> <p>Between 40 and 49 <input type="checkbox"/></p> <p>Between 50 and 59 <input type="checkbox"/></p> <p>Between 60 and 69 <input type="checkbox"/></p> <p>Over 70 <input type="checkbox"/></p> <p>Composition of household (only if the protected premises are used for residential purposes)</p> <p>1 person <input type="checkbox"/></p> <p>2 persons <input type="checkbox"/></p> <p>3 persons <input type="checkbox"/></p> <p>4 persons <input type="checkbox"/></p> <p>5 persons or more <input type="checkbox"/></p>
---	--	--	--



Lined writing area consisting of 28 horizontal lines for text entry.

ALARM CONTROL PANEL
Standard: EN 50130-4 and 5 versions 2011
EN 50131-3
EN 50131-6
EN 50131-4
EN 50131-5-3

**ELECTRONIC INTRUSION
DETECTION EQUIPMENT
PRODUCT SAFETY
EMC AND ENVIRONMENTAL
COMPATIBILITY
NF&A2P GRADE 2**

CNPP Cert.
Route de la Chappelle Réanville
BP 2265
F-27950 Saint-Marcel
www.cnpp.com

AFNOR Certification
11 rue Francis de Pressensé
F-93571 La Plaine Saint Denis
Cedex
http://www.marque-nf.com

NF&A2P Grade 2 - According to certificate NF324-H58

TRADE MARK: **Daitem**
PRODUC REFERENCES: **SH320AU / SH340AU / SH380AU**
CERTIFICATION No.: **1201300012**

