GB

On the website www.elkron.com, you may find updated information relating to the documentation provided with the product.

DS80MP5L-013H **LBT80898**

MP500/4N - MP500/8 MP500/16

Remote controllable alarm control panels

Programming Manual

ELKRON

DIRECTIVE 2012/19/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 July 2012 on waste electrical and electronic equipment (WEEE)

The symbol of the crossed-out wheeled bin on the product or on its packaging indicates that this product must not be disposed of with your other household waste.
Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product

ELKRON

Tel. +39 011.3986711 - Fax +39 011.3986703
www.elkron.com - mail to: info@elkron.it

TABLE OF CONTENTS

FIGURES

TABLES

INTRODUCTION

ORGANISATION OF THE MANUAL

The manual is divided into chapters and the various topics are arranged in sequence to provide step-by-step instructions for **programming** and **configuring** the system.

Information for system **design, installation** and **maintenance** are contained in the ***Installation Manual*.**
The Installation Manual also contains the **device acquisition procedure.**

Instructions for system use by the end user are contained in the ***User Manual*.**

CONVENTIONS USED

The following conventions are used in the manual for the sake of simplicity:

EVENT LOG TOTAL	This is the LCD with the displayed message. Unless otherwise specified, the same message is shown on the touchscreen keypad.
▲, ▼, ESC, OK, MENU …	This is the equivalent key to be pressed on the keypad.
<Master code> **<User code>** **<Installer code>** **<Technical Manager code>**	This indicates the code to be entered using the keypad.
<Master / User code>	This means that either code may be entered on the keypad indifferently.
H24	This means that the described function or service is always active.

Pay attention to the following symbols:

This symbol indicates an important warning.

This symbol indicates advice.

This symbol indicates EN50131 grade 3 compliance.
The compliance of the system as a whole is equal to the minimum certification of the installed devices and of the enabled functions.

This symbol indicates EN50131 grade 2 compliance.
The compliance of the system as a whole is equal to the minimum certification of the installed devices and of the enabled functions.

This symbol indicates that EN50131 compliance may depend on other functions enabled in the system.

The symbol means that the function or device is not EN50131 certified.

This symbol means that the function or device will cancel EN50131 certification.

1 - CONTROL DEVICES

This chapter contains a description of the devices which allow to access the alarm system locally, to arm or disarm the system, to program and to interact with it.
The function of the various keys and the information supplied by the LEDs and on the display are explained for keypads.
The information supplied by the LEDs is provided for readers.

1.1 KP500D/N - KP500DV/N KEYPAD DISPLAY

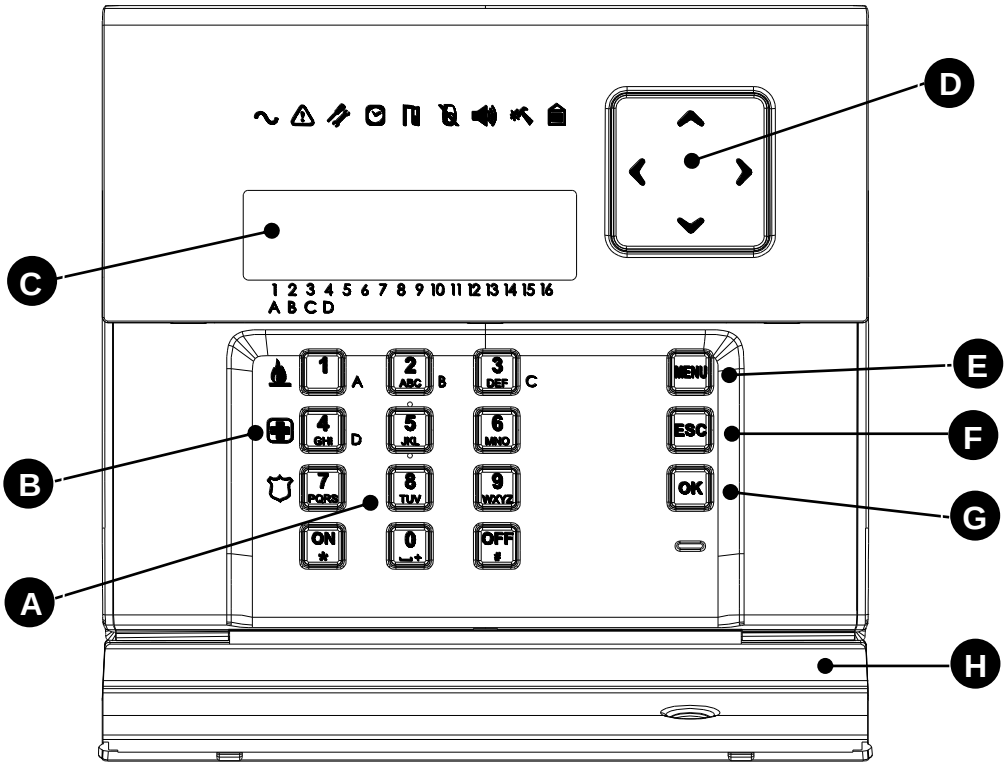


Figure 1 - KP500D/N and KP500DV/N keypads

Ref.	Description	Use or indications provided
A	Alphanumeric keys	For entering the access code, arming or disarming the system, programming the system.
B	Function keys	For activating fire, emergency and silent panic indications.
C	LCD 2 x 16 characters	Date and time or detailed information on system status is shown in stand-by mode*****. Menus and system parameters and information are shown during system programming or querying.
D	Navigation keys	These are used to go from one menu item to another. They change the value of some parameters.
E	**MENU** key	To access the menu.
F	**ESC** key	To go back to the upper menu level.
G	**OK** key	To confirm the access code and other entered data. To confirm the chosen menu and go to the submenu.
H	Lid	To protect the alphanumeric keys.

***** Displaying information other than date and time in stand-by mode declasses EN50131 certification from grade 3 to grade 2.

Table 1 - KP500D/N and KP500DV/N keypad elements

1.1.1 Function keys

Symbol	KP500D/N and KP500DV/N	Associated function
	1	Fire indication
	4 GHI	Emergency indication
	7 PQRS	Silent panic indication

Table 2 - KP500D/N and KP500DV/N keypad function keys

1.1.2 LEDs and status icons

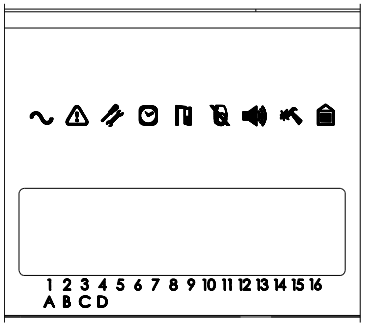


Figure 2 - Display and status LEDs on KP500D/N and KP500DV/N keypads

The LEDs on the keypads indicate system status and alarms. Available information is shown in *Table 3 - LEDs and icon indication of KP500D/N and KP500DV/N* keypads.

The amount of displayed information depends on system status level (armed or disarmed), the EN50131 grade set during programming and the access level (see paragraph *2.1 System access codes*). Paragraph *1.1.2.1 Use of LEDs with EN50131 grade 3* lists the information available in the various cases.

Symbol	Description	Indicator	Supplied indications
	Power	Green LED	**On** = mains power present **Blinking** = no mains power, battery power present
	Failure or notice [1]	Yellow LED	**Off** = normal operation **On**= failure or notice present **Blinking** = see details of current failures
	Maintenance	Yellow LED	**Off** = normal operation **On**= system maintenance in progress
	Timed programmer	Green LED	**Off** = no command **On** = commands present for the current day **Blinking** = control activation warning
	Open inputs	Yellow LED	**Off** = no open input **On** = open input **Blinking** = see details of current open inputs
	Inhibited or isolated inputs	Yellow LED	**Off** = no inhibited or isolated input **On** = inhibited or isolated input **Blinking** = see details of current inhibited or isolated inputs
	Alarm [2]	Red LED	**Off** = no alarm condition present **On** = at least one alarm condition present **Blinking** = see details of current alarms
	Tamper [3]	Red LED	**Off** = no tamper condition present **On** = at least one tamper condition present **Blinking** = see details of current tampering
	System status [4]	Green LED	**Off** = all partitions associated to the keypad are disarmed **On** = all partitions associated to the keypad are armed **Blinking** = some partitions associated to the keypad are armed

1) The indicated failures and warnings are: PSTN line, power overvoltage, power low voltage, battery (inefficient or low battery), system bus communication (devices not interfacing with control panel), control panel input and expansion +V voltage, control panel condition (burglar, input inhibition or isolation, tampering).
2) The indicated alarm conditions are burglar and warning. Technological indications are also provided (emergency, fire, technological 1, technological 2, technological 3).
3) The indicated tampering conditions are: control panel tamper, control panel SAB input, expansion SAB input, tamper input, imbalance of one of the inputs specialised as balanced or double balance, attempt to use a wrong access code or key (repeated 21 times).
4) Information is limited to the partitions associated to the keypad only. The status of any configured partitions which are not associated to the keypad cannot be determined.

Table 3 - LEDs and icon indication of KP500D/N and KP500DV/N keypads

1.1.2.1 Use of LEDs with EN50131 grade 3

The keypad LED indications which are visible without needing to enter a valid code depend on the EN50131 grade (Mode 3, Mode 2 or Mode 0) set during programming.

IMPORTANT ! By setting Mode 0 the system will lose EN50131 compliance it potentially had before.

Behaviour in Mode 2 is two-fold: all LED indications are visible when the alarm system is disarmed, while only the power, timed programmer and system status indications appear when the system is armed (the other LED indications may be viewed by entering a valid code). This mode is EN50131 grade 2 compliant.

The alarm system is EN50131 grade 3 compliant in Mode 3. LED indications are not always visible and depend on system status (armed or disarmed) and whether a valid access code is entered. The indications shown refer to the partitions associated to the keypad only.

IMPORTANT ! Mode 3 is not available for the MP500/4N control panel because this device is EN50131 grade 2, and not grade 3, compliant.

Table 4 - LED indication visibility of KP500D/N and KP500DV/N keypads complying with EN50131 grade 3 shows how the LEDs behave on the keypad in Mode 3.

Enter a valid code to see details on the indications.

All indications can be deleted using the Installer or Technical Manager codes. Only burglar, power failure and communication failure indications can be deleted with the Master or User codes.

Alarm system status	**Armed**			**Disarmed**		
Access code used	**No code**	**Master / User**	**Installer / Technical Manager**	**No code**	**Master / User**	**Installer / Technical Manager**
Power LED	■	■	■	■	■	■
Failure or warning LED		□	□	■	■	■
Maintenance LED		□	□	■	■	■
Timed programmer LED	■	■	■	■	■	■
Open inputs LED		□	□	■	■	■
Inhibited or isolated input LED		□	□		□	□
Alarm LED		□	□		□	□
Tamper LED		□	□		□	□
System status LED		□	□		□	□

■ = The LED indication is always visible even without entering an access code.

□ = The LED indication is only visible after having entered a valid access code.

Table 4 - LED indication visibility of KP500D/N and KP500DV/N keypads complying with EN50131 grade 3

1.1.3 Partition indications

The partition status is shown on the display in graphic mode.

The graphic symbols corresponding to digits 1 to 16 appear on the second line of the screen.

```
SYSTEM STATUS
□□□□□□. . . . . .
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
```

The meanings are:

Symbol	During normal use	During programming
□	partition disarmed	partition not associated to the function
■	partition armed	partition associated to the function
0	partition disarmed with one or more open inputs	-
.	partition does not exist	partition does not exist

Example for MP500/16

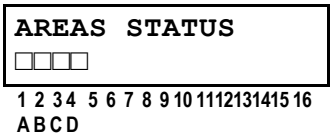
Partition 4 is armed, partitions 1, 2, 5 and 6 are disarmed, partition 3 is disarmed with one or more open inputs, partitions from 7 to 16 do not exist.

```
SYSTEM STATUS
□□0■□□. . . . . .
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
```

1.1.4 Area indications

The area status is shown on the display in graphic mode.

The graphic symbols corresponding to letters A, B, C, D appear on the second line of the screen.

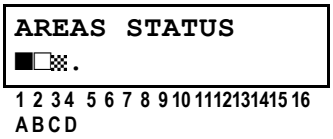


IMPORTANT! The MP500/4N control panel has only two areas and graphic symbols appear next to the letters A, B only.

The meanings are:

Symbol	During normal use	During programming
□	area disarmed	area not associated to the function
■	area armed	area associated to the function
▩	area partially armed	
.	area does not exist	area does not exist

Example:
Area A is armed, area B is disarmed, area C is partially active, area D does not exist.



1.2 KP500DP/N TOUCHSCREEN KEYPAD – KP500D/ST

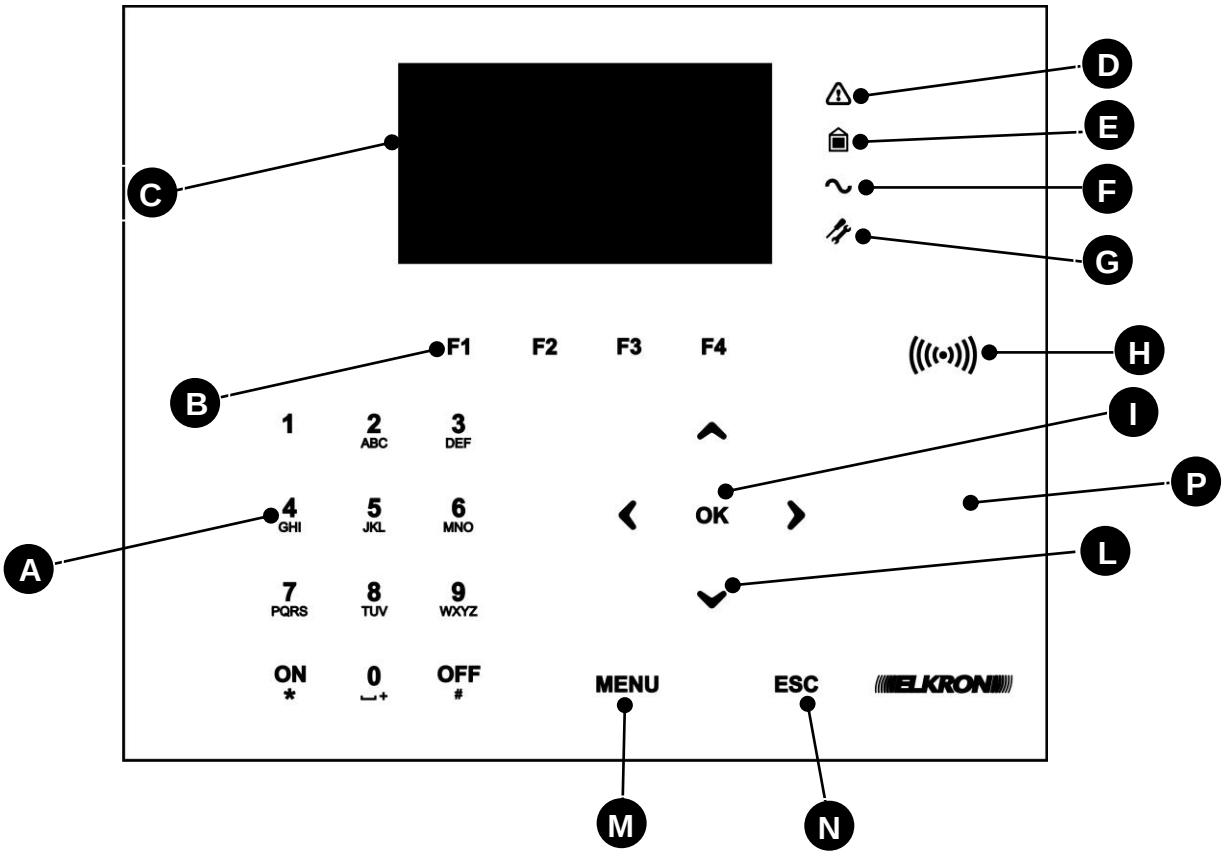


Figure 3 - KP500DP/N - KP500D/ST keypad

Ref.	Description	Use or indications provided
A	Alphanumeric keys	Used to enter the access code, select some functions and program the control panel
B	Function keys	Used to activate the additional system functions
C	Graphic OLED display	In stand-by, shows date and time, detailed system status information, event log and programming menus
D	Yellow LED Notices	**Off** = normal operation **On**= failure, fault, alarm or tampering
E	Green LED System status	**Off** = system disarmed **On**= system all armed **Blinking** = system partially armed
F	Green LED Mains voltage	**On** = mains power present **Blinking** = no mains power, battery power present See Installation Manual.
G	Yellow LED Maintenance	**Off** = normal operation **On**= system maintenance in progress
H	Proximity key reader	DK30 proximity key sensor (Not present in the KP500D/ST)
I	**OK** key	Confirm access code and other entered data; confirm chosen menu item and go to the submenu
L	Arrow keys	To scroll menu items and edit the value of some parameters
M	**MENU** key	To access the menu
N	**ESC** key	To go back to the upper menu level
P	Approach sensor	Approach the hand to activate the keypad

***** Displaying information other than date and time in stand-by mode declasses EN50131 certification from grade 3 to grade 2 (KP500DP/N).

Table 5 - KP500DP/N - KP500D/ST keypad elements

1.2.1 Function keys

Symbol	KP500DP/N - KP500D/ST key	Associated function
	F1	Silent panic indication
	F2	Emergency indication
	F3	Fire indication
	F4	Clean glass

Table 6 - KP500DP/N – KP500D/ST keypad function keys

1.2.2 Status icons

Figure 4 - KP500DP/N – KP500D/ST keypad display and status icons

The LEDs and icons on the keypads indicate system status and alarms. Available information is shown in *Table 7 - LED and icon indications of KP500DP/N – KP500D/ST keypad* .

The amount of displayed information depends on the system status level (armed or disarmed), the EN50131 grade set during programming and the access level (see paragraph *2.1 System access codes*). Paragraph *1.2.2.1 Use of LEDs and icons with EN50131 grade 3* lists the information available in the various cases.

Symbol	Description	Supplied indications
	Power	**Present** = no mains power **Highlighted** = see electric mains failures details
	Failure	**Present** = failures present **Highlighted** = see details of current failures
	Timed programmer	**Present** = commands present for the current day **Highlighted** = control activation warning
	Open inputs	**Present** = open input **Highlighted** = see details of current open inputs
	Inhibited or isolated inputs	**Present** = inhibited or isolated input **Highlighted** = see details of current inhibited or isolated inputs
	Alarm	**Present** = at least one alarm condition present **Highlighted** = see details of current alarms
	Tamper	**Present** = at least one tamper condition present **Highlighted** = see details of current tampering

Table 7 - LED and icon indications of KP500DP/N – KP500D/ST keypad

1.2.2.1 Use of LEDs and icons with EN50131 grade 3

The visibility of the keypad LED and icon indications without needing to enter a valid code depends on the EN50131 grade (Mode 3, Mode 2) set during programming.

IMPORTANT! By setting Mode 0 the system will lose EN50131 compliance it potentially had before.

Behaviour in Mode 2 is two-fold: all LED and icon indications are visible when the alarm system is disarmed, while only the power, timed programmer and system status indications appear when the system is armed (the other LED and icon indications may be viewed by entering a valid code). This use mode is EN50131 grade 2 compliant.
The alarm system is EN50131 grade 3 compliant in Mode 3. LED and icon indications are not always visible and depend on system status (armed or disarmed) and whether a valid access code is entered. The indications shown refer to the partitions associated to the keypad only.

IMPORTANT! Mode 3 is not available for the MP500/4N control panel because this device is EN50131 grade 2, and not grade 3, compliant.

Table 8 - LED indication visibility of EN50131 grade 3 compliant KP500DP/N – KP500D/ST keypad shows how the LEDs behave on the keypad in Mode 3.

Enter a valid code to see details on the indications.

All indications can be deleted using the Installer or Technical Manager codes. Only burglar, power failure and communication failure indications can be deleted with the Master or User codes.

Alarm system status	**Armed**			**Disarmed**		
Access code used	**No code**	**Master / User**	**Installer / Technical Manager**	**No code**	**Master / User**	**Installer / Technical Manager**
Power LED / icon	■	■	■	■	■	■
Failure or warning LED / icon		□	□	■	■	■
Maintenance LED		□	□	■	■	■
Timed programmer icon	■	■	■	■	■	■
Open inputs icon		□	□		□	□
Inhibited or isolated inputs icon		□	□		□	□
Alarm icon		□	□		□	□
Tamper icon		□	□		□	□
System status LED		□	□		□	□

■ = The LED / icon indication is always visible even without entering an access code.

□ = The LED / icon indication is only visible after having entered an access code.

Table 8 - LED indication visibility of EN50131 grade 3 compliant KP500DP/N – KP500D/ST keypad

1.2.3 Partition indications

The partition status is shown on the displays in graphic mode. The partitions appear on two lines.

The meanings are:

Symbol	During normal use	During programming
02	partition disarmed	partition not associated to the function
01	partition armed	partition associated to the function
12	partition disarmed with one or more open inputs	-
	partition does not exist	partition does not exist

In the example above, partitions 1 and 5 are armed, partition 12 has one or more open inputs and partition 16 does not exist. The remaining partitions are disarmed.

1.2.4 Area indications

The areas status is shown on the displays in graphic mode. The areas status is shown on the last line.

The meanings are:

Symbol	During normal use	During programming
C	area disarmed	area not associated to the function
A	area armed	area associated to the function
B	area partially armed	
▪	area does not exist	area does not exist

In the example above, area A is armed, area B is partially armed, area C is disarmed and area D does not exist.

1.3 DK500M-E ELECTRONIC KEY READERS

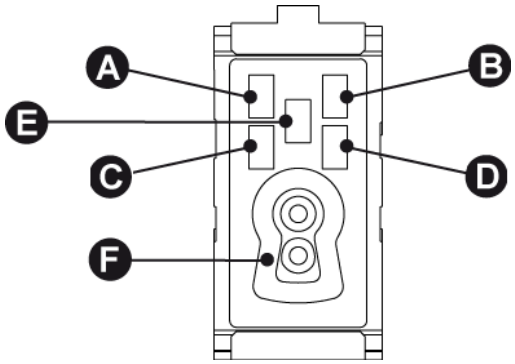


Figure 5 - DK500M-E electronic key readers

Ref.	Description	Use or indications provided	
		Operating mode = Mode 3	**Operating mode = Mode 2**
A B C D	LED (green) associated partition status	• **Off** * = all partitions associated to the LED are disarmed • **On*** = all partitions associated to the LED are armed • **Blinking** * = at least one partition associated to the LED is armed	• **Off** = all partitions associated to the LED are disarmed • **On**= all partitions associated to the LED are armed • **Blinking** = at least one partition associated to the LED is armed
E	LED (red) alarms and indications	• **Off** = no indications for the partitions associated to the reader • **On** = alarm indication stored for the partitions associated to the reader or tamper or system failure (the indication only appears when the system is disarmed) • **Blinking** = presence of at least one open input in the partitions associated to the reader. The indication only appears when the system is disarmed. The LED will light up fixed if there are alarms, or failures and open inputs at the same time. This LED lights up to indicate the need to check indication details on the keypad.	• **Off** = no indications for the partitions associated to the reader • **On** = alarm indication stored for the partitions associated to the reader or tamper or system failure (the indication only appears when the system is disarmed) • **Blinking** = presence of at least one open input in the partitions associated to the reader. The LED will light up fixed if there are alarms, or failures and open inputs at the same time. This LED lights up to indicate the need to check indication details on the keypad.
F	Electronic keyhole	Shaped hole for inserting the DK50 electronic key	

Mode 3 is EN50131 grade 3 compliant.

IMPORTANT! Mode 3 is not available for the MP500/4N control panel because this device is EN50131 grade 2, and not grade 3, compliant.

Mode 2 is EN50131 grade 2 compliant.

*****) The LED will remain off in a EN50131 grade 3 compliant system even if an indication is present. Insert the key and remove it to check system status: the LEDs associated to active partitions will light up for a few seconds (fixed or blinking).

1.4 DK500M-P AND DK510M-P PROXIMITY KEY READER

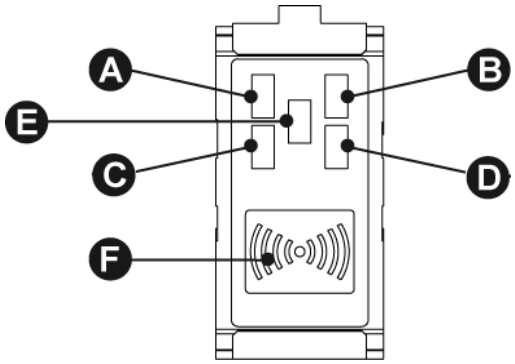


Figure 6 - DK500M-P and DK510M-P proximity key reader

Ref.	Description	Use or indications provided	
		Operating mode = Mode 3	**Operating mode = Mode 2**
A B C D	LED (green) associated partition status	• **Off** * = all partitions associated to the LED are disarmed • **On*** = all partitions associated to the LED are armed • **Blinking** * = at least one partition associated to the LED is armed	• **Off** = all partitions associated to the LED are disarmed • **On**= all partitions associated to the LED are armed • **Blinking** = at least one partition associated to the LED is armed
E	LED (red) alarms and indications	• **Off** = no indications for the partitions associated to the reader • **On** = alarm indication stored for the partitions associated to the reader or tamper or system failure (the indication only appears when the system is disarmed) • **Blinking** = presence of at least one open input in the partitions associated to the reader. The indication only appears when the system is disarmed. The LED will light up fixed if there are alarms, or failures and open inputs at the same time. This LED lights up to indicate the need to check indication details on the keypad.	• **Off** = no indications for the partitions associated to the reader • **On** = alarm indication stored for the partitions associated to the reader or tamper or system failure (the indication only appears when the system is disarmed) • **Blinking** = presence of at least one open input in the partitions associated to the reader. The LED will light up fixed if there are alarms, or failures and open inputs at the same time. This LED lights up to indicate the need to check indication details on the keypad.
F	Transponder	DK30 proximity key sensor for DK500M-P and DK70 proximity key for DK510M-P	

Mode 3 is compliant with EN50131 grade 3.

IMPORTANT! Mode 3 is not available for the MP500/4N control panel because this device is EN50131 grade 2, and not grade 3, compliant.

Mode 2 is EN50131 grade 2 compliant.

*) The LED is off in a EN50131 grade 3 compliant system even if an indication is present. Insert the key and remove it to check system status: the LEDs associated to active partitions will light up for a few seconds (fixed or blinking).

1.5 RC500 REMOTE CONTROL

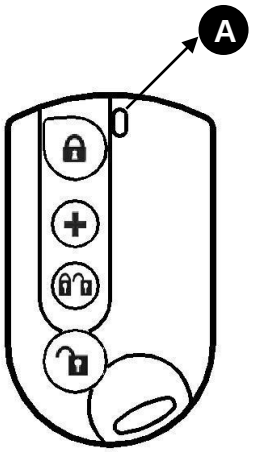


Figure 7 - RC500 remote control

Ref.	Description	Use or indications provided
A	Two-colour red/green LED	• **Red blinking** = any key was pressed (the remote control will beep if the control unit has received the control). • **Green fixed** = any key was pressed and the low battery status of the remote control is indicated. Both indications disappear after short while.
	Key 1 Arm	Arms all associated partitions.
	Key 2 Programmable according to control unit	This key can only be used to arm/disarm OUTPUT devices or to generate four different alarm types: silent panic, panic, emergency, fire.
	Key 3 Toggle arm/disarm	Arms/disarms the associated partitions using toggle function.
	Key 4 Disarm	Disarms all associated partitions.

Note: *The ER500 radio expansion must be installed to use the remote control.*

2 - SYSTEM ACCESS

This chapter contains a description of the available system access codes, functions and programming.

2.1 SYSTEM ACCESS CODES

Access to given system functions is permitted according to the access code type (Master, User, Installer or Technical Manager). The available codes are:

- **Master code**. This code is always enabled and is the only code authorised to enable other users, keys, timed programming and remote access. It can be used to reset all the other access codes to the factory default (useful if the changed access code is forgotten).
- **Installer code**. This code must be enabled each time by the Master code and is automatically deactivated when a new valid code is entered or a valid key is used. This is to program the system and for maintenance. This code is used by the installer. It can be used to reset all the other access codes to the factory default (useful if the changed access code is forgotten).

  IMPORTANT! The installer code will be automatically deactivated if any users enter their code while the installer code is enabled. The same will occur if an electronic or proximity key is used.

- **User code**. This code must be enabled by the Master code and will remain valid until it is deactivated by the Master code by a timed programmed control. This code is used by users for normal operations: arming and disarming the system, displaying system status, reading event log and changing the access code.
- **Technical Manager code**. This code must be enabled by the Master code and is automatically deactivated when a new valid code is entered or a valid key is used. It allows to access a limited number of system configuration functions. It can be used to reset all the other access codes to the factory default (useful if the changed access code is forgotten).

IMPORTANT! The Technical Manager code will be automatically deactivated if any user enters their code while the Technical Manager code is enabled. The same will occur if an electronic or proximity key is used.

Each access code is freely programmable with a variable length from a minimum of four to a maximum of six digits. Each user can change their access code at will.

IMPORTANT! Trough the use of the web server only 6-digit codes are allowed.

IMPORTANT! Any access code shorter than six digits will cancel the EN50131 grade 3 compliance of the entire burglar alarm system.
If there are no other limiting factors, five or six digit access codes allow EN50131 grade 2 compliance.
Four digit codes will cancel EN50131 compliance.

ADVICE: All users, including the Master and Installer, should change their code before commissioning the system.

Always press OK to confirm the entered access code to access menus or functions.

On MP500/4N, MP500/8 and MP500/16 control panels, starting from control panel SW version 1.01 and starting from keypad SW version 1.03, if the hold-up function has been enabled (see paragraph 2.1.4 *How to enable the hold-up function*), when user code is modified automaticaly, the system will also assing a code for the hold-up function which is the same as the chosen one + 1 (for example, if 789456 has been chosen, the hold-up code will be 789457).

IMPORTANT! Enabling the hold-up function will cancel EN50131 compliance.

2.1.1 Default access codes

The MP500/4N, MP500/8 and MP500/16 control panels are provided with default codes when they leave the factory.

The Installer and Technical Manager codes are enabled at the factory and automatically deactivated when a valid Master or User code is entered for the first time.

Code type	Level	Default code	Associated partitions	Enabled when leaving the factory	Enable time (once enabled)
Installer	3	000000	All	Yes	Temporary session
Master	2	111111	All	Yes	Permanent
User (2÷14)	2	000020-000140	Partition 1	No	Until expressly disabled
Technical Manager	3	222222	All	Yes	Temporary session

Table 9 - Default access codes for MP500/4N

Code type	Level	Default code	Associated partitions	Enabled when leaving the factory	Enable time (once enabled)
Installer	3	000000	All	Yes	Temporary session
Master	2	111111	All	Yes	Permanent
User (2 ÷31)	2	000020-000310	Partition 1	No	Until expressly disabled
Technical Manager	3	222222	All	Yes	Temporary session

Table 10 - Default access codes for MP500/8

Code type	Level	Default code	Associated partitions	Enabled when leaving the factory	Enable time (once enabled)
Installer	3	000000	All	Yes	Temporary session
Master	2	111111	All	Yes	Permanent
User (2 ÷62)	2	000020-000620	Partition 1	No	Until expressly disabled
Technical Manager	3	222222	All	Yes	Temporary session

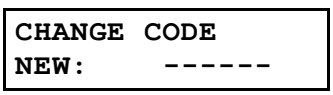
Table 11 - Default access codes for MP500/16

2.1.2 Code change

Each user can change their access code freely.

Proceed as follows to change the code:

1) Enter <Master / User / Installer / Technical Manager code>, press [OK] and then [MENU].
2) Press [▼] repeatedly until SETTINGS appears.
3) Press [OK] and then [▼] several times until CHANGE CODE appears.
4) Press [OK].
5) Enter the new code, from four to six digits, and press [OK].



IMPORTANT! Trough the use of the web server only 6-digit codes are allowed.

IMPORTANT! Any access code shorter than six digits will cancel EN50131 grade 3 compliance of the entire burglar alarm system.
If there are no other limiting factors, five or six digit access codes allow EN50131 grade 2 compliance.
Four digit codes will cancel EN50131 compliance.

6) Enter the new code and press OK to confirm.

```
CHANGE CODE
CONFIRM: ------
```

7) Press ESC repeatedly to exit from the menu.

```
    MP500/16
12/01/2014 10:10
```

2.1.3 How to reset an access code

An access code can be reset to its default value if a user forgets it.

Proceed as follows to reset a code to its default value.

1) Enter <Master / Installer / Technical Manager code>, press OK and then MENU.

```
UT01:MASTER
SYSTEM STATUS
```

2) Press ▼ repeatedly until SETTINGS appears.

```
UT01:MASTER
SETTINGS
```

3) Press OK and then ▼ several times until USERS appears.

```
SETTINGS
USERS
```

4) Press OK and then ▼ several times until DEFAULT CODE appears.

```
USERS
DEFAULT CODE
```

5) Press OK.

```
DEFAULT CODE
UT00:INSTALLER
```

6) Use ▲ and ▼ to select the user whose code you want to reset. Press OK to confirm.

```
UTxx:...
ARE YOU SURE?
```

7) Press OK to confirm the operation (UTxx is the selected user).

```
USERS
DEFAULT CODE
```

8) Press ESC repeatedly to exit from the menu.

```
    MP500/16
12/01/2014 10:10
```

2.1.4 How to enable the hold-up function

On MP500/4N, MP500/8 and MP500/16 control panels, starting from control panel SW version 1.01 and starting from keypad SW version 1.03, has been added the option to enable or disable the hold-up function for all the user codes already enabled or that will be enabled later.

Proceed as follows to set the hold-up function:

1) Enter <Installer code >, press OK and then MENU.

2) Press ▼ repeatedly until SETTINGS appears.

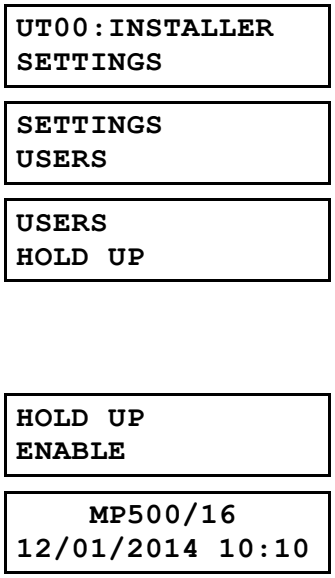
3) Press OK and then ▼ several times until USERS appears.

4) Press OK and then ▼ several times until HOLD UP appears.

5) Press OK.

6) Use ▲ and ▼ to select enable or disable. Press OK to confirm.

7) Press ESC repeatedly to exit from the menu.



IMPORTANT! Enabling the hold-up function will cancel EN50131 compliance.

2.1.5 Entering an invalid code or using an invalid key

An attempt to enter an invalid access code 21 consecutive times or use an invalid key 21 consecutive times will interpreted by the control panel as a sabotage attempt. The control panel will consequently generate a tamper alarm and activate the programmed alarm outputs and the telephone call dialler.

The incorrect code count will be reset as soon as a correct code or valid key is used.

IMPORTANT! Readers and keypads in the entire system will be blocked for 90 seconds after the tenth attempt to enter an invalid access code or an invalid key.

The message “WAIT please” and the time remaining before the end of the block will appear on the keypads.

No code or key can be entered during this time.
The system will allow to enter codes or keys again at the end of the block. The control panel will interpret other ten consecutive attempts to enter an invalid code (and will block the system for other 90 seconds) as a sabotage attempt and will generate a tamper alarm.

3 - MENU

This chapter describes the structure of the various menus of the MP500/4N, MP500/8 and MP500/16 control panels, how to access them and how to navigate them.
Clear graphics are provided to identify the entire path to be followed to access the various functions at a glance.

3.1 HOW TO ACCESS MENUS

The menus can be accessed in two ways:

1. By entering an access code (Master, Installer, User or Technical Manager), then [OK] and finally [MENU]. The displayed menu will reflect the privileges of the access code used.
2. Alternatively, press [MENU] directly. The free access below described above will be opened.

3.2 HOW TO NAVIGATE THE MENUS

The menus are organised in a tree structure, i.e. with reciprocally nested submenus, each consisting of one more items.

The submenu items differ according to the access code used and the system configuration. For example, if the respective menu items will not appear if the radio devices interface is not installed. Similarly, the ENABLE menu item (users, keys etc.) only appears in the Master menu and not in all the others.

The LCD typically shows the current menu on the first line and the submenu on the second line.

```
EVENT LOG
TOTAL
```

In the example shown, the EVENT LOG is the current menu and TOTAL is one of the possible submenus. The OLED display is different but the information is displayed according to the same criteria.

The various keys used to navigate the menus are shown in the following table.

[MENU]	To access the menu
[OK]	Confirms the entered access code, accesses the displayed submenu or confirms the selection made
[ESC]	Goes back to the previous page or menu level
[^]	Scrolls the menu items
[v]	Scrolls the menu items

For example, after having logged in as Master, in the following menu item:

```
ENABLE
INSTALLER
```

the following will occur when the various keys are press.

- Press [^] and [v] to scroll the submenus of the ENABLE menu, i.e. INSTALLER, TECH. MANAGER, USER, KEY, TIMED COMMANDS, VOCAL MESSAGES, ADVANCED. The submenu items appear in cycle, i.e. the first of the list appears after the last item (in this case, INSTALLER will appear again after ADVANCED).
- Press [OK] to access the INSTALLER submenu, which has two submenus: ENABLE AND DISABLE.
- Press [ESC] to go back to the main menu of the Master user (UT01:MASTER), in which ENABLE is one of the submenus.
- Press [ESC] repeatedly to exit from the menu.

The system will automatically exit from the menu after a minute if no key is pressed.

A brief *beep* will be heard each time a key is pressed.

A *beep-beep* will be heard to confirm that the entered parameter is correct, i.e. when a correct access code is entered.

A long *beep* will be heard if an incorrect parameter is entered, i.e. if an incorrect user code is entered.

3.3 FREE ACCESS MENU

Press MENU directly to access the following menu items:

- **SERVICE MESSAGE.** This is used to play, record and delete audio service messages. A valid code must be entered to access the functions. The menu is only available with voice keypads (KP500DV/N) and the optional SV500N board must be installed in the control panel. See *User Manual* for more details.
- **LCD INFO**. This is used to select what to display when the system is in stand-by: date and time, area status or partition status. Enter a valid access code to make the selection. See *4.7 LCD Info* for more details.

  IMPORTANT! The display of any information other than date and time will cancel the EN50131 grade 3 compliance of the entire burglar alarm system.

- **SET BUZZER**. This is used to adjust the volume of the sound indications of the keypad. See *User Manual* for more details.
- **SET CONTRAST**. This is used to adjust the contrast of the display. See *User Manual* for more details.
- **SET BACKLIGHT**. This is used to adjust the backlighting intensity of the display. See *User Manual* for more details.

3.4 MAIN MENU

The main menu is the first menu to be accessed after having logged in. All the various submenus can be accessed from this menu.

M T U R	SYSTEM STATUS		→	Submenu...	This shows the system status and can be used to change the partition status.
M T U R #	EVENT LOG		→	Submenu...	This is used to read the list of events stored in the control panel, except for the specifically technical ones.
R	DIAGNOSE LOG.		→	Submenu …	This is used to read the list of all events stored in the control panel.
M T U R #	SETTINGS		→	Submenu...	This is used to isolate inputs, set the current date and time, configure the users or reset codes to default value, acquire, configure and detect electronic keys and transponders and configure the timed programmer. In grade 3 compliant systems, inputs can only be isolated by the installer and the technical manager. In grade 2 compliant systems this can also be performed by the master and the users.
M #	ENABLE		→	Submenu...	This is used to enable and disable users, electronic keys, timed programmer and remote access.
M T #	TEST		→	Submenu...	This is used to carry out specific tests to check perfect operation of the system. It is possible to test the control panel inputs and the other devices connected to the bus, the GSM signal and the telephone call dialler separately.
T #	PROGRAMMING		→	Submenu...	This is used to set the number of system partitions, to configure them, to set the number of areas in the system and to configure them, to configure the various inputs of the control panel and of the other bus peripheral devices, to configure the control panel and expansion unit outputs and to configure keypads and readers.
T #	PARAMETERS		→	Submenu...	This is used to set the various system timers.
M T #	TELEPHONE DIALER		→	Submenu...	This is used to store the telephone numbers to be dialled to send alarms and indications, record the voice message, associate specific alarms to each telephone number and to specify the sending method, to set the PSTN and GSM network parameters, edit text messages, enable and configure other telephone functions.
T #	MAINTENANCE		→	Submenu...	This is used to carry out maintenance operations on the system, such as changing the languages, acquiring devices, deleting devices, upgrading the device firmware, resetting and saving the programmed settings.

#: accessible with the system disarmed only.

4 - SYSTEM COMMISSIONING

This chapter describes the programming needed to commission the burglar alarm system at the end of installation and to connect the various devices.

Programming may be carried out by means of a system keypad, a service keypad (see *Installation Manual* for more information on connections) or a PC provided with Hi-Connect software and connected to the control panel by means of a USB cable and optional interface (see *Installation manual* for more information on connections).

The control panel may be programmed at a workshop and the programming may later transferred on site using a USB flash drive and optional interface.

This chapter describes the programming procedures for keypads with LCD. The programming procedure on the KP500DP/N or KP500D/ST touchscreen keypad is the same but the information shown on the OLED may be slightly different.

4.1 CONVENTIONS USED IN PROGRAMMING PROCEDURES

Programming is carried out using the keys and reading the messages and information which appear on the display.

The main functions associated to the keys are:

MENU	To access the menu
OK	Confirms the entered parameter, accesses the displayed submenu or confirms the selection made
ESC	Goes back to the previous page or menu level
^	Scrolls the menu items, edits a value
v	Scrolls the menu items, edits a value
<	Moves the cursor along the writing line
>	Moves the cursor along the writing line

The following step-by-step programming and configuration procedures show the keys to be pressed and what appears on the display. Text is limited to the essential minimum. The concerned function, the parameters to be configured, what the parameters are for and the possible values are described before each procedure.

<Master code>
<User code>
<Technician code>
<Technical Manager code>
This indicates the code to be entered using the keypad.

<Master / User / Installer / Technical Manager code>
This means that either code may be entered on the keypad indifferently.

It is indicated whether each procedure is EN50131 grade 3 compliant or not.

The indication is hierarchic: this means that an indication provided in a parameter applies to the parameter below it unless otherwise indicated.

4.2 HOW TO ENTER ALPHANUMERIC CHARACTERS

The keypad can be used to enter alphanumeric characters to store descriptive names for users, partitions, areas, outputs etc. Each name can by up to 24 characters long. Press the keys to select several characters cyclically as shown on the following table. A cursor will blink on the display at the entry point of the new character.

To write a name:

- press the key associated to the required character until it appears
- press [>] and [<] to go to the previous or next position (use [0 ␣+] to delete characters in excess)
- finally, press [OK] to store the name or [ESC] to exit from the procedure without saving it.

Key	Character
1	. / : ; ! ? 1
2	A B C a b c 2
3	D E F d e f 3
4	G H I g h i 4
5	J K L j k l 5

Key	Character
6	M N O m n o 6
7	P Q R S p q r s 7
8	T U V t u v 8
9	W X Y Z w x y z 9
0	[space] 0 + -

4.3 VOCAL NAME

EN50131 NOT RELATED

MP500/4N, MP500/8 and MP500/16 allow to assign a vocal name to partitions, inputs and outputs. This identification will be used in the vocal messages sent by the control panel, including alarm messages. In order to use this function the MP500/4N, MP500/8 or MP500/16 control panel must be equipped with a vocal synthesis board (SV500N). See the *Installation Manual* for more information on connections and configurations of this device.

The playing, recording and deleting functions are available in the partition, input, output and radio device programming menu. Each vocal name is four seconds long.

The headset with microphone supplied with the vocal synthesis board or alternatively a vocal keypad (KP500DV/N) can be used to record and play. The delete command must be used to clear a memory position to record another vocal message.

IMPORTANT! Speak at a distance of approximately 20cm from the microphone for good quality of the recorded audio. Do not hold the vocal keypad, if this method is used, during recording.

4.4 HOW TO ENABLE THE INSTALLER

The Installer must have been previously enabled to work on the system. For safety reasons, Installer enabling is cancelled whenever a User or Master code is entered or when an electronic or proximity key is used.

IMPORTANT! The Installer is automatically enabled each time the system is turned on.

Proceed as follows to enable the Installer:

1) Enter **<Master code>**, press [OK], then [MENU] and finally press [v] repeatedly until ENABLE appears.

```
UT01:MASTER
ENABLE
```

2) Press [OK].

```
ENABLE
INSTALLER
```

3) Press [OK]. If, necessary, press [v] to make ENABLE appear.

```
INSTALLER
ENABLE
```

4) Press [OK] to enable the installer.

```
ENABLE
INSTALLER
```

5) Press [ESC] repeatedly to exit from the menu.

```
    MP500/16
12/01/2014 10:10
```

4.5 HOW TO ENABLE THE TECHNICAL MANAGER CODE

The Technical Manager must have been previously enabled to work on the system. For safety reasons, Technical Manager enabling is cancelled whenever a User or Master code is entered or when an electronic or proximity key is used.

IMPORTANT! The Technical Manager is automatically enabled each time the system is turned on.

Proceed as follows to enable the Technical Manager:

1) Enter **<Master code>**, press [OK], then [MENU] and finally press [▼] repeatedly until ENABLE appears.

```
UT01:MASTER
ENABLE
```

2) Press [OK] and then [▼] several times until TECHNICAL MANAGER appears.

```
ENABLE
TECH. MANAGER
```

3) Press [OK]. If, necessary, press [▼] to make ENABLE appear.

```
TECH. MANAGER
ENABLE
```

4) Press [OK] to enable the Technical Manager.

```
ENABLE
TECH. MANAGER
```

5) Press [ESC] repeatedly to exit from the menu.

```
    MP500/16
12/01/2014 10:10
```

4.6 HOW TO SELECT THE LANGUAGE

The first configuration is to select the language used to show the menu item messages on the display.

The default language is Italian but various available languages can be selected (English, Français, Deutsch, Español, Portoguese, Suomi, Polski, Slonensko).

Proceed as follows to access the language selection function:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally press [▼] repeatedly until MAINTENANCE appears.

```
UT00:INSTALLER
MAINTENANCE
```

2) Press [OK].

```
MAINTENANCE
LINGUA-LANGUAGE
```

3) Press [OK]. If there are various keypads, select the keypad on which you want to change the language, press [▼] and press [OK] to confirm the selection.

```
LINGUA-LANGUAGE
KP01:KP 01
```

4) Press [▼] repeatedly until the required language appears on the display.

```
KP01:KP 01
ENGLISH
```

5) Press [OK] to confirm. The message will appear on the keypad which is being used and on the keypad which is being updated. The keypad will beep repeatedly during the operation.

```
DOWNLOAD
IN PROGRESS  15%
```

6) This will appear at the end.

```
DOWNLOAD      OK
END CHANGE LANG.
```

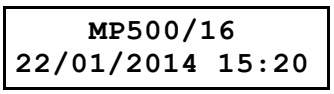
7) Press [ESC] repeatedly to exit from the menu.

```
    MP500/16
12/01/2014 10:10
```

4.7 LCD INFO

The keypad can display the following information when the system is in stand-by:

- date and time



- system partition status

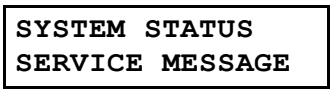
- system area status

The viewing mode may be independently elected for each keypad in the system.

IMPORTANT! The entire system will lose EN50131 grade 3 compliance if only one keypad in the system permanently displays information other than date and time.

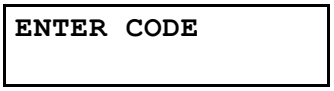
To change the display view in stand-by:

1) Press MENU.



2) Press ▼.

3) Press OK.



4) Enter **<User code>** and then OK.

5) Use ▼ and ▲ to select the information to be displayed: date and time, areas synoptic, synoptic (partitions). Press OK to confirm.
6) Press ESC repeatedly to exit from the menu.

4.8 HOW TO SET DATE AND TIME

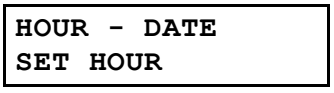
In addition to being shown on the keypad in stand-by viewing mode (see *4.7 LCD Info*), date and time information is used to record events on the Event Log and on the Diagnose Log and for the timed programmer functions. So, the timed programmer will not work properly if the date and time are not correct and the Event and Diagnose Log time references will not be correct.

Proceed as follows to modify the date and time shown on the display:

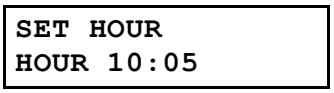
1) Enter **<Master / Installer code>**, press OK, then MENU and finally press ▼ repeatedly until SETTINGS appears.

2) Press OK.

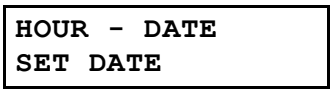
3) Press OK.



4) Press OK.
5) Enter the time in hh:mm (24 hour) format directly using the number keys using an initial 0 if needed. If you make a mistake press ESC and access the SET HOUR menu.



6) Press OK to confirm the entered time then ▼.



7) Press [OK].
8) Enter the date dd/mm/yy format directly using the number keys using an initial 0 if needed. If you make a mistake, press [ESC] and access the SET DATE menu.
9) Press [OK] to confirm the entered date then [▼].
10) Press [OK]. You can now choose to automatically update summer time/standard time. In the European Union, summer time starts on the last Sunday of March and ends on the last Sunday of October. To change automatically, press [▼] repeatedly until ENABLE appears.
11) Press [OK] to confirm the entered setting then [▼].
12) Press [OK]. Enter the month for shifting from summer time to standard time (10 = October for the European Union). Enter the month directly using the number keys.
13) Press [OK] to confirm the month then [▼].
14) Press [OK]. Enter the month for shifting from standard time to summer time (3 = March for the European Union). Enter the month directly using the number keys.
15) Press [OK] to confirm the month then [▼].
16) Press [OK]. Select the Sunday (LAST SUNDAY or FIRST SUNDAY) with the [▼] and [▲] on when to shift time (the last Sunday of the month in the European Union) and press [OK] to confirm the selection.
17) Press [ESC] repeatedly to exit from the menu.

```
SET DATE
DATE 12/01/14
```

```
HOUR - DATE
SUMMER TIME
```

```
SUMMER TIME
ENABLE
```

```
HOUR - DATE
LEGAL T. MONTH
```

```
LEGAL T. MONTH
        10
```

```
HOUR - DATE
SUMMER T. MONTH
```

```
SUMMER T. MONTH
         3
```

```
HOUR - DATE
SUNDAY
```

```
SUNDAY
LAST SUNDAY
```

```
    MP500/16
12/01/2014 10:10
```

4.9 PARTITION PROGRAMMING

The MP500/4N control panel can manage up to four partitions, the MP500/8 control panel up to eight and the MP500/16 control panel can manage up to 16 partitions. The actual number of partitions is established during the programming procedure. Each system must have at least one partition.
System inputs, outputs, keypads and readers can be freely assigned and belong to more than one partition.

The arming mode can be programmed for each partition so that some burglar inputs remain open when the system is armed:

EN50131 GRADO 3

EN50131 GRADO 2

Sys arm block: a partition programmed in this way cannot be armed if any assigned inputs are open.

EN50131

Standard: an alarm is generated if any assigned inputs are open when the partition is armed.

EN50131

Self Inhibition: the burglar inputs assigned to the partition which can be isolated and are open when the partition is armed will be automatically isolated (no more than 70% of the inputs assigned to the partition will be isolated; any inputs in excess will remain open and generate an alarm). The isolated inputs will automatically end insulation if they are closed again.

In other words, the system can be armed if there are open inputs in a standard partition, it cannot be armed if there are open inputs in a Sys Arm Block partition and it can always be armed if there are open inputs in a Self Inhibition partition but an alarm will be tripped if there are too many open inputs.

Proceed as follows to program the partitions:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until PROGRAMMING appears.

```
UT00:INSTALLER
PROGRAMMING
```

2) Press [OK].

```
PROGRAMMING
PARTITIONS
```

3) Press [OK].

```
PARTITIONS
PARTITIONS NO.
```

4) Press [OK].

```
PARTITIONS NO.
PART.N: 1
```

5) Press [OK].

```
PARTITIONS
PARTITIONS NO.
```

6) Press [▼] and [▲] to change the number of enabled partitions. Press [OK] to confirm.

```
PARTITIONS NO.
PART.N.: 1
```

IMPORTANT! To decrease the number of partitions, disassociate everything assigned to the partition you want to eliminate (users, detectors etc.) before deleting it.

7) Press [▼].

```
PARTITIONS
CONFIG. PARTIT.
```

8) Press [OK].

```
CONFIG. PARTIT.
SE01:...
```

9) Press [▼] and [▲] to select the required partition. Press [OK] to confirm.

```
SE01:...
ACTIVATION MODE
```

10) Press [▼] and [▲] to select the activation mode which will condition the behaviour of the partition when the system is armed. Possible options are STANDARD, SELF INHIBITION and SYSTEM ARM BLOCK. These are explained in detail at the beginning of the paragraph.

```
ACTIVATION MODE
SYS ARM BLOCK
```

11) Confirm the choice by pressing [OK] and press [▼].

```
SE01:...
DELAY TIMES
```

12) Press [OK].

```
DELAY TIMES
ROUTE ENTRY
```

13) Press [OK].

14) Press [▼] and [▲] to select the delay time. The possible values are: DISABLED, 5 s, 10 s, 15 s, 20 s, 30 s, 45 s, 1 min, 1 min 30 s, 5 min.

```
DELAY TIMES
30s
```

IMPORTANT! The delay cannot be longer than 45 second to remain EN50131 compliant. An arming delay time must be set and this cannot be longer than 45 second to be EN50131 compliant. So, DISABLED, 1 min, 1 min 30 s, 5 min cannot be selected.

15) Confirm the choice by pressing [OK], press [ESC] and then [▼].

```
SE01:...
NAME
```

16) Press [OK].

```
NAME
SE01:...
```

17) Enter a descriptive name for the partition using the keypad (see paragraph *4.2 How to enter alphanumeric characters*). The name can be up to 24 characters long.

18) Confirm the choice by pressing [OK] and press [▼].

```
SE01:...
VOCAL NAME
```

19) Press [OK].

```
VOCAL NAME
PLAY
```

20) Press [OK] to play the vocal name.

21) Press ⌄.

22) To record, press OK (see paragraph *4.3 VOCAL name* for more information).

23) Press ⌄.

24) Press OK to delete the vocal message of the partition (see paragraph *4.3 VOCAL name* for more information).

25) Press ESC ESC to program the other partitions repeating the procedure from step 9 or press ESC repeatedly to exit the menu.

```
VOCAL NAME
RECORD
```

```
VOCAL NAME
DELETE
```

4.10 AREAS PROGRAMMING

IMPORTANT! An areas must have at least one assigned partition. The system automatically distributes the first available partition to each area when they are created.

See the *Installation Manual* and for a detailed description of the concept of area and possible uses.

Proceed as follows to program the areas:

1) Enter **<Installer code>**, press OK, then MENU and finally ⌄ repeatedly until PROGRAMMING appears.

2) Press OK and then ⌄.

3) Press OK.

4) Press OK.

5) Press ⌄ and ⌃ to change the number of areas. Possible values are 0, 2 for MP500/4N, and 0, 2, 3, 4 for MP500/8 and MP500/16. Press OK to confirm.

6) Press OK to confirm the number of areas, otherwise press ESC.

7) Press ⌄.

8) Press OK.

9) Press ⌄ and ⌃ to select the required area.

10) Press OK to confirm.

11) Press OK. Enter a descriptive name for the area using the keypad (see paragraph *4.2 How to enter alphanumeric characters*). The name can be up to 24 characters long.

12) Confirm the choice by pressing OK and press ⌄.

13) Press OK. Press ‹ and › to select the partition to be assigned. Press ⌄ and ⌃ to assign the partition (the square will turn black) or to disassociate it (the square will appear empty). Partitions which cannot be assigned (e.g. because they are already associated to another partition) are represented by a dot. Repeat the procedure for all partitions to be assigned to the area. Press OK at the end.

14) Press ESC ESC to program the other areas repeating the procedure from step 9 or press ESC repeatedly to exit the menu.

```
UT00:INSTALLER
PROGRAMMING
```

```
PROGRAMMING
AREAS
```

```
AREAS
NUMBER OF AREAS
```

```
NUMBER OF AREAS
N      :  0
```

```
ARE YOU SURE?
PRESS OK or ESC
```

```
AREAS
CONFIGURE AREAS
```

```
CONFIGURE AREAS
AR A:…
```

```
AR A:…
NAME AREA
```

```
NAME AREA
AR A:...
```

```
AR A:…
ASSIGN
```

```
SE02:…
□■□□□□□□
```

4.11 WIRED INPUT PROGRAMMING

Detectors and other devices capable of triggering an alarm are connected to the wired inputs.

The MP500/4N system can manage up to 32 general purpose inputs, the MP500/8 system can manage up to 64 and the MP500/16 system can manage up to 128.

The SAB tamper inputs of the control panel and the EP500 expansion modules cannot be programmed.
See the *Installation Manual* for more information and for connections.

It is advisable to read the description of the various parameters which must be configured before starting programming operations.

4.11.1 Wired input encoding

Each input has two addresses: a physical address and a logical address. The two addresses are displayed as follows:

physical address → logical address

and in detail

ddXX In**Y:** → In**ZZZ**

where:

- **dd** is the bus device type or control panel (UC, EP, KP, DK)
- **XX** is the sequential number of the bus devices containing the inputs
- **Y** is the input number in the line device X
- **ZZZ** is the three-digit logical address of the input that the control panel assigns sequentially as the bus devices are assigned.

The physical address is useful for installers during system installation and maintenance. The physical location is shown on the display (UC=control panel, EP=expansion module, KP=keypad, DK=reader).
The logical address can be changed at any time by the installer.
The system identifies the inputs on the display by showing physical address, logical address and name. Vocal and number alarms, on the other hand, are identified by means of logical address and customised message (if any) only.
When acquiring EP500 expansion modules, the control panel automatically assigns a sequential logical address to all eight inputs (the first eight or four inputs of the system are those of the control panel itself), while the inputs of the keypads and the input 2 of the readers are not considered because they are set to NOT USED by default and consequently must be enabled and numbered manually, if needed.

4.11.2 Input types

The input type determines the way the control panel will interpret the electric circuit signals (detector + connection wires) connected to the input itself.
See *Installation Manual* for more details and application circuits.
The physical features of all inputs may be changed by programming, except for the SAB input which can only be of the balanced type and to which the tamper alarm is assigned.

Possible alarm input types are:

- **Not Used**: electric signal variations (including opening and tamper) of the input are ignored. Programming an input as "Not Used" additionally means avoiding to need to close the unused inputs with a jumper.

  IMPORTANT Remember that the MP500/16 can manage up to 128 inputs (MP500/4N up to 32 and MP500/8 up to 64). All control panel and expansion unit inputs are programmed by default, while the auxiliary inputs of keypads and input 2 of the readers are NOT USED by default. Input 1 of the readers is configured as tamper by default.
  So, if the maximum number of EP500 expansion modules are installed and you want to use some auxiliary inputs, you will need to deactivate an equal number of inputs to avoid exceeding the maximum number of inputs.

- **N.C**. (normally closed): the electric circuit connected to the input must be closed in stand-by mode. Its opening will trip the associated event. This is not EN50131 compliant.
- **N.O.** (normally open): the electric circuit connected to the input must be open in stand-by mode. Its closing will trip the associated event. This is not EN50131 compliant.
- **Balanced**: this determines two voltage thresholds for recognising stand-by state, alarm indication and tamper indication implemented by short-circuiting the wires. EN50131 grade 2 compliant.
- **Double balance**: this determines three voltage thresholds for recognising stand-by state, alarm indication and tamper indication implemented by short-circuiting or cutting the wires. EN50131 grade 3 and grade 2 compliant.
- **Shock**: an alarm indication is tripped when the electric circuit remains open for a time equal to programmed sensitivity. This is not EN50131 compliant.
- **Roller**: this causes an alarm indication to trip when the electric circuit is opened and closed for the number of times equal to the programmed sensitivity in a given time. This is not EN50131 compliant.

4.11.3 Wired input customisation

Alarm input customisation determines how, when and what alarm type to generate. The control panel will activate the respective devices (outputs, sirens and telephone dialler) according to the generated alarm type.
The possible input customisations are described below.

The customisations listed below are all EN50131 compliant:

IMMEDIATE
The opening of the input generates the burglar alarm when:
- the input has an AND type association and the partitions to which it belongs are all active,
- the input has an OR type association and at least one of the partitions to which it belongs is active.

See the *Installation Manual* for more information.

DELAYED
This is typically used for detectors which could be triggered by the users themselves when arming and disarming the system (for example, the magnetic contact on the entrance door).
It is advisable to use the First Entry, Last Exit, First Entry/Last Exit and Way customisations if there are more than two detectors with this feature.
A Delayed customised input behaves as an Immediate input, but the burglar alarm will only be generated after its Delay time has elapsed.
The Delay time can be defined separately for each single input (in input programming).
If there is only one delayed input in a partition, the Delay time determines both the “Entry Time” and the “Exit Time” (which are equal to each other).

The system will behave as follows if there are several delayed inputs in a partition with different Delay times:
- when the partition is armed, the "Exit Time" corresponds to the highest delay time
- when the partition is armed, the “Entry Time” is the one assigned to the first delayed input which is opened.

The “Entry Time”, and consequently alarm generation, may be interrupted by:
- deactivating all partitions with OR type association to which the input belongs or
- deactivating at least one of the partitions with AND type association to which the input belongs.

The control panel buzzer is activated by default during the “Entry Time” and during the “Exit Time” (see paragraph *4.13 Keypad programming*). The indication may be deactivated.

IMPORTANT! EN50131 compliance will be cancelled if the buzzer is deactivated.

If the control device (keypad or reader) used to arm and disarm the system is located inside a protected area, it is advisable to use the First Entry, Last Exit, First Entry/Last Exit and Way customisations for all the sensors interposed between the control device and the access doors.

ADVICE: Using Way customisation (instead of Delayed) for volumetric detectors in the home has the advantage that the detectors will behave as Immediate if the door is not opened.

ADVICE: Using the First Entry/Last Exit or Last Exit customisation (instead of Delayed) has the advantage that the Exit Time is interrupted when leaving the home when the door is closed.

ADVICE: A “Entry Way Time” different from the “Exit Way Time" can be set using the Way customisation.

IMPORTANT! Do not use inputs with Delayed customisation and with First Entry, Last Exit, First Entry/Last Exit and Way customisations in the same partition.

FIRST ENTRY - WAY - LAST EXIT - 1ST ENT/LST EXIT
See the *Installation Manual* for more information on how to use these customisations.

KEY
The opening of the input arms or disarms all the partitions assigned to it by reversing the respective state (the partitions will be disarmed if they are not, and vice versa). All partitions will be disarmed if some are armed and some are disarmed.

TAMPER
The opening of the input generates the Tamper event regardless of the partition arming status. The input is active H24.

FAILURE
The opening of the input generates the Failure event regardless of the partition arming status.
The input is active H24.

INPUT OF TEST
The opening and the closing of the input generates log and status display events without activating any alarm. Operation is independent from the partition arming status and is always active (H24). If may be used to test a sensor without generating false alarms.

JAMMING
The opening of the input generates the Jamming alarm. The Jamming output of motion detectors must be connected to the input.

DETECTOR FAILURE
The opening of the input generates the Detector Failure event. The failure output of detectors must be connected to the input.

SIREN FAILURE
The opening of the input generates the Siren Failure event. The failure output of siren must be connected to the input.

COM. FAULT
The opening of the input generates the Communicator Fault event. The customised failure output of the ATS4 external communicator must be connected to the input.
The input is active H24.

The customisations listed below are not EN50131 compliant:

FIRE ALARM
The opening of the input generates the Fire Alarm indication regardless of the partition arming status. The input is active H24.

IMPORTANT! This customisation of the input offers a further advantage for users but is not EN50131 compliant because it is not described in the standard.

TECHNOLOGICAL TYPE 1
The opening of the input generates a technological type 1 event regardless of the partition arming status.
The input is active H24.

Note: Technological type 1 inputs must be assigned (by means of the partitions) to at least one technological type 1 output.

TECHNOLOGICAL TYPE 2
The opening of the input generates a technological type 2 event regardless of the partition arming status.
The input is active H24.

Note: Technological type 2 inputs must be assigned (by means of the partitions) to at least one technological type 2 output.

TECHNOLOGICAL TYPE 3
The opening of the input generates a technological type 3 event regardless of the partition arming status.
The input is active H24.

Note: Technological type 3 inputs must be assigned (by means of the partitions) to at least one technological type 3 output.

PRE-ALARM
The opening of the input generates the burglar pre-alarm when:
- the partitions to which it belongs have an AND type association and are all active, or
- the partitions to which it belongs have an OR type association and at least one of them is active.

PANIC
The opening of the input generates the panic indication regardless of the partition arming status.
The input is active H24.

SILENT PANIC
The opening of the input generates the silent panic indication regardless of the partition arming status.
The input is H24.

HOLD-UP
The opening of the input generates the hold-up indication regardless of the partition arming status.
The input is active H24

RESET FIRE ALARM
The opening of the input switches the assigned reset fire alarm outputs for 1 second and resets the fire indications, regardless of the partition arming status.
The input is active H24.

EMERGENCY
The opening of the input generates the emergency indication regardless of the partition arming status.
The input is active H24.

IMPORTANT! This customisation of the input offers a further advantage for users but is not EN50131 compliant because it is not described in the standard.

4.11.4 Isolable

EN50131 GRADO 2 EN50131 GRADO 3

An input set as “isolable” will be subject to manual and automatic isolations.
See *9.1 Input isolation and end of isolation* for more details.

IMPORTANT! The input partition mode must be SYS ARM BLOCK to be EN50131 compliant.

IMPORTANT! Inputs programmed as “Delayed”, “First Entry”, “Way”, “Last Exit” and “First Entry/Last Exit” must not be programmed as “isolable”. Failure to respect this requirement may cause anomalous behaviour in the system.

4.11.5 Ancillary functions (Gong, Courtesy Light, Door Opener, Absence of Move)

Ancillary functions which can be used when the system is disarmed can be associated to the burglar inputs.
The ancillary functions only work if all the partitions assigned to the input are disarmed.
See *Installation Manual* for more details on the single functions.
These functions are not EN50131 compliant because they are not described in the standard.
Only one of the following ancillary function options may be selected for each input: None, Absence of Move, Gong, Courtesy Light, Door Opener.

4.11.6 Burglar input attributes (Release Type, AND / OR partitions)

This function is EN50131 compliant.
The operation of the burglar inputs may be customised further by setting the attributes.
The **Release Type** determines when the alarm signal is generated. Possible settings:

- **Single release**: the alarm is generated as soon as the input is open.
- **Double release**: the alarm is generated at the end of the second event only if this occurs within 120 seconds from the first one.

IMPORTANT! The input partition mode must be SYS ARM BLOCK to be EN50131 compliant.

Common input this determines what happens to an input which belongs to more than one partition. Possible settings:

- **AND Partitions**: this creates a logical connection between the partitions to which the input belongs and the alarm is generated only if all partitions are armed.
- **OR Partitions**: this creates a logical connection between the partitions to which the input belongs and the alarm is generated if at least one partitions is armed.

4.11.7 AND inputs

This function is EN50131 compliant.
This creates a logical connection between two burglar inputs with the same customisation. The alarm is generated only if both are kept open within 5 minutes from one another (the first input to be opened may be closed again in the meantime). The five minute interval cannot be edited.
See the *Installation Manual* for more information.

4.11.8 Programming procedure

IMPORTANT! Changes to the default customisations of the control panel inputs could cancel EN50131 compliance.

Proceed as follows to program the inputs:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until PROGRAMMING appears.
2) Press [OK] and then press [▼] several times until INPUTS appears.
3) Press [OK].
4) Press [OK].
5) Press [▼] and [▲] to select the required input. Press [OK] to confirm.

```
UT00:INSTALLER
PROGRAMMING
```

```
PROGRAMMING
INPUTS
```

```
INPUTS
CONTROL PANEL
```

```
CONTROL PANEL
UC.In1:    In001
```

```
UC.In1:    In001
LOGIC NUMBER
```

6) Press [OK].

7) Change the logical address using keys [<] [>] and the numeric keypad. Press [OK] to confirm.

```
LOGIC NUMBER
IN001:...
```

IMPORTANT! There cannot be two inputs with the same logical address.

8) Press [v].

```
UC.In1:   In001
INPUT TYPE
```

9) Press [OK].

10) Press [v] and [^] to select the required input type. Press [OK] to confirm.

```
INPUT TYPE
N.C. DOUBLE BAL.
```

11) Press [v].

```
UC.In1:   In001
ASSIGN
```

12) Press [OK]. Press [v] and [^] to assign the input to the SYSTEM (all partitions) or only to some PARTITIONS. Press [OK] to confirm.

```
ASSIGN
SYSTEM
```

13) If SYSTEM is selected, press [v] and [^] to select SYSTEM ASSIGN or SYSTEM DO NOT ASSIGN and press [OK] to confirm. Then [ESC] [ESC].

14) A representation of the partitions will appear if PARTITIONS is selected. The empty boxes represent partitions which are not assigned to the input and the black boxes the partitions which have already been assigned. Press [<] and [>] to select the partition to be associated. Press [v] and [^] to assign the partition (the square will turn black) or to disassociate it (the square will appear empty). Repeat the procedure for all partitions to be associated to the input.

```
SE##:
□□□□□■□
```

15) After having assigned the partitions, press [OK], then [ESC] and [v].

```
UC.In1:   In001
CUSTOMIZE
```

16) Press [OK]. Press [v] and [^] to customise the input customisation. The delay (5 s, 10 s, 20 s, 30 s, 1 min, 1 min 30 s, 5 min) can be selected if DELAY is selected.

```
CUSTOMIZE
1ST ENT/LST EXIT
```

IMPORTANT! The delay cannot be longer than 45 second to maintain EN50131 compliance. An arming delay time must be set and this cannot be longer than 45 second to be EN50131 compliant. So, DISABLED, 1 min, 1 min 30 s, 5 min cannot be selected.

17) Confirm the choice by pressing [OK] and press [ESC].

```
UC.In1:   In001
ISOLABLE
```

18) Press [OK]. Press [v] and [^] to enable or disable the input as isolable. Press [OK] to confirm.

```
ISOLABLE
ENABLE
```

19) Press [v] and then [OK]. Press [v] and [^] to select the ancillary function (none, absence of move, gong, courtesy light, door opener). Press [OK] to confirm.

```
UC.In1:   In001
ANCILLARY FUNCT
```

20) Press [v].

```
UC.In1:   In001
ATTRIBUTES
```

21) Press [OK]. Press [v] and [^] to select whether to release the alarm after the first or the second opening of the input (single, double). Press [OK] to confirm.

```
ATTRIBUTES
RELEASE TYPE
```

22) Press [v].

```
ATTRIBUTES
COMMON INPUT
```

23) Press [OK]. Press [v] and [^] to select how the status of the partitions which have the input in common must be considered for alarm purposes. Press [OK] to confirm.

```
COMMON INPUT
AND PARTITIONS
```

24) Press ESC and then ▼.

```
UC.In1:    In001
AND INPUTS
```

25) Press OK. Press ▼ and ▲ to select:

```
AND INPUTS
DISPLAY AND
```

- DISPLAY AND to view the input combined to the input being programmed
- DISABLE AND to cancel the combination with the other input
- SELECT AND to select the input (first the device and then the input) to be combined to the input being programmed.

Press OK to confirm the selection and follow the menu items show below.

26) Press ESC and then ▼.

```
UC.In1:    In001
NAME
```

27) Press OK. Enter a descriptive name for the input using the keypad (see paragraph *4.2 How to enter alphanumeric characters*). The name can be up to 24 characters long. Press OK to confirm.

```
NAME
Inxxx:...
```

28) Press ▼.

```
UC.In1:    In001
VOCAL NAME
```

29) Press OK. Press OK again to play the vocal name of the input.

```
VOCAL NAME
PLAY
```

30) Press ▼. To record, press OK (see paragraph *4.3 VOCAL name* for more information).

```
VOCAL NAME
RECORD
```

31) Press ▼. Press OK to cancel the vocal message of the input.

```
VOCAL NAME
DELETE
```

32) Press ESC ESC to program the other inputs of the same device, repeating the procedure from step 5; press ESC again to program the inputs of another device (expansion modules, keypads, readers), repeating the procedure from step 3. Use ▼ and ▲ to select another device.

33) Press ESC repeatedly to exit from the menu.

IMPORTANT! Program all inputs used in the system.

4.12 WIRED INPUT PROGRAMMING

The MP500/4N, MP500/8 and MP500/16 systems can manage up to 11, 27 and 51 general purpose outputs.
See the *Installation Manual* for more information and for connections.

4.12.1 Output encoding

Each output has two addresses: a physical address and a logical address. The two addresses are displayed as follows:

physical address → logical address

and in detail

ddXX UY: → UZZ

where:

- **dd** is the bus device type or the control panel (UC, EP, AS)
- **XX** is the sequential numbering of the bus devices containing the outputs
- **Y** is the number of the output of the bus device XX
- **ZZ** is the two-digit logical address of the output that the control panel assigns sequentially as the bus devices are assigned.

The physical address is useful for installers during system installation and maintenance. It may appear in a different manner on the display (UC=control panel, EP=expansion module, AS=power supply).

The logical address can be changed at any time by the installer.

The system identifies the outputs on the display by showing physical address, logical address and name. Vocal and number alarms, on the other hand, are identified by means of the logical address and the customised message (if any) only.

The control panel automatically assigns a sequential logical address in sequence to the outputs of the control panel itself during EP500 expansion module acquisition.

4.12.2 Output types

The physical features of the outputs can be changed during programming.

Possible output types are:
- **Not used**: this disables the output.
- **Output N.L.**: (in stand-by) if this is a relay output it will be de-energised, if this is an electric output it will be open (without potential).
- **Output N.H.**: (stand-by) if the output is a relay it will be energised; if the output is a positive reference electric output it will be set to 12 V level; if the output is negative reference output, it will be set to level 0 V.

See the *Instruction Manual* for a detailed analysis of relay and electric outputs when set to N.L. or N.H.

WARNING! For the correct functioning of the system, it is recommended **not to modify** the default programming (N.H.) for the control panel outputs (UC.U1, UC.U2, etc ...).

4.12.3 Output assignment

Each output may be assigned to the entire system, i.e. to all partitions, or only to some partitions.
The output is activated only by events or inputs which concern the assigned partitions.

4.12.4 Output customisations

The control panel and expansion outputs (both electric and relay) may be programmed to be activated after given events.

The table in paragraph *10.4 Detail of events and management* shows when and how an output is activated.

How to use TC outputs
The TC (Trigger Control) output is used to control detectors, sirens and other indicator devices, putting them in stand-by, for example, and is conditioned by the partition state.
The AND TC input means that all assigned partitions must be armed for the output to be activated.
For an OR TC it is sufficient for one of the assigned partitions to be armed for the output to be activated.

IMPORTANT! The TC output is set to N.H. and with polarisation jumper set to "**+**" by default. A high level is provided in stand-by in this manner (+12 V).

The possible customisations for EN50131 compliant outputs are described below.

O BURGLAR ALARM
The burglar alarm output is activated if a burglar event is generated.

O PRE-ALARM
The pre-alarm output is activated if a pre-alarm event is generated.

O RESET BURGL.AL
The reset burglar alarm output is activated in pulse mode for approximately 1 second when the partitions are armed.

O TAMPER
The tamper output is activated if a tamper event, or a wrong code event or a radio jamming event or a no radio supervision event occurs.

O SYSTEM FAILURE
The system failure output is activated when a system failure alarm is generated (siren failure, external communicator error, no interface on bus).

O TEL. FAILURE
The telephone failure alarm output is activated if a telephone fault event is generated.

O LOW BATTERY
The low battery output is activated when a no battery or inefficient battery event is detected.

O LACK OF POWER
The blackout output is activated if a "lack of power" event is generated.

O BUZZER
The buzzer output beeps slowly during the Exit Time and beeps rapidly during the Entry Time to partitions assigned to it.

O PARTIT. STATUS
The partition status output is activated when all the partitions assigned to it are armed.

O AND TC
The AND TC output is activated when all the partitions assigned to it are armed.

O OR TC
The OR TC output is activated when at least one of the partition associated to it is armed.

O ARM WARNING
The arm warning output is activated when the programmed warning time for executing a partition arming command by the timed programmer starts.

O FAILURE
The failure output is activated if a input failure event is generated.

O BURGL/TAMPER
The burglar/tamper output is activated when a burglar or tamper or wrong code event is generated.

O DETECT.FAILURE
The detector failure output is activated if an event is generated by a detector failure input or a jamming failure input.

The following customisations are not EN50131 compliant because they are not described in this standard.

O SILENT PANIC
The silent panic output is activated if a silent panic fault event is generated.

O AUDIBLE PANIC
The audible panic output is activated if a panic event is generated.

O HOLD-UP
The hold-up output is activated if a hold-up event is generated.

O EMERGENCY
The emergency output is activated if an emergency event is generated.

O TECHNOL.TYPE 1
The technological type 1 output is activated if a technological type 1 event is generated.

O TECHNOL.TYPE 2
The technological type 2 output is activated if a technological type 2 event is generated.

O TECHNOL.TYPE 3
The technological type 3 output is activated if a technological type 3 event is generated.

O FIRE ALARM
The fire alarm output is activated if a fire event is generated.

O RESET FIRE AL
The reset fire alarm output is activated if a reset fire alarm is opened.

O GONG
The gong output is activated if an input to which the ancillary gong function is assigned is opened.

O OPEN INPUT
The open input output is activated when at least one of the inputs which belong to the partitions assigned to it or a test input is activated.

IMPORTANT! The open input output is used to notify the state of the input and cancels EN50131 grade 3 compliance.

O INPUT ISOLATED
The input isolated output is activated when at least one of the inputs belonging to the partitions associated to it is isolated in any manner or for any reason.

IMPORTANT! The input isolated output is used to notify the state of the input and cancels EN50131 grade 3 compliance.

O COMMANDABLE
The commandable output is EN50131 compliant when:
- it is activated by a timed programmer output activation command.
- it is deactivated by a timed programmer output deactivation comand.

The commandable output may be activated but cancels EN50131 compliance when:
- it is activated/deactivated via SMS text message
- it is activated/deactivated remotely by dialling an appropriate DTMF sequence
- the control panel is called on the GSM network from the telephone number to which the zero-cost call function is associated
- the "**+**" key on the remote control is pressed.

O DOOR OPENER
The door opener output is activated when a door opener event is generated.

O COURTESY LIGHT
The courtesy light output is activated when a courtesy light event is generated.

O PULSED COMM.
Pulsed output is activated for approximately 1 second.
The pulsed commandable output is EN50131 compliant when:
- it is activated by a timed programmer output activation command.

The pulsed commandable output may be activated but cancels EN50131 compliance when:
- it is activated via SMS text message
- it is activated remotely by dialling an appropriate DTMF sequence
- the control panel is called on the GSM network from the telephone number to which the zero-cost call function is associated
- the "**+**" key on the remote control is pressed.

4.12.5 Programming procedure

IMPORTANT! Changes to the default customisations of the control panel outputs could cancel EN50131 compliance.

Proceed as follows to program the outputs:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until PROGRAMMING appears.

```
UT00:INSTALLER
PROGRAMMING
```

2) Press [OK] and then [▼] several times until OUTPUTS appears.

```
PROGRAMMING
OUTPUTS
```

3) Press [OK].

```
OUTPUTS
CONTROL PANEL
```

4) Press [▼] and [▲] to select the required device. Press [OK] to confirm.

```
CONTROL PANEL
UC.U!:        U01
```

5) Press [▼] and [▲] to select the required output. Press [OK] to confirm.

```
UC.U1:        U01
LOGIC NUMBER
```

6) Press [OK]. Change the logical address using keys [◄] [►] and the numeric keypad. Press [OK] to confirm.

```
LOGIC NUMBER
Uo1:...
```

IMPORTANT! There cannot be two outputs with the same logical address.

IMPORTANT! Commandable outputs must have a logical addresses comprised between 01 and 10.

7) Press [▼].

```
UC.U1:        U01
OUTPUT TYPE
```

8) Press [▼] and [▲] to select the output type. Press [OK] to confirm.

```
OUTPUT TYPE
OUTPUT N.H.
```

9) Press [▼].

```
UC.U1:        U01
ASSIGN
```

10) Press OK. Press ▼ and ▲ to assign the output to the SYSTEM (all partitions) or only to some PARTITIONS. Press OK to confirm.

```
ASSIGN
SYSTEM
```

11) If SYSTEM is selected, press ▼ and ▲ to select SYSTEM ASSIGN or SYSTEM DO NOT ASSIGN and press OK to confirm. Then ESC.

12) The screen page shown here by the side will appear if PARTITIONS is selected. The empty boxes represent partitions which are not assigned to the output and the black boxes the partitions which have already been assigned. Press ◄ and ► to select the partition to be associated. Press ▼ and ▲ to assign the partition (the square will turn black) or to disassociate it (the square will appear empty). Repeat the procedure for all partitions to be assigned to the output. Press OK at the end. Then ESC.

```
SE##:
□□□□□■□
```

13) Press ▼.

```
UC.U1:          U01
CUSTOMIZE
```

14) Press OK. Press ▼ and ▲ to select the output customisation and press OK to confirm.

```
CUSTOMIZE
BURGLAR
```

15) Press ▼.

```
UC.U1:          U01
NAME
```

16) Press OK. Enter a descriptive name for the output using the keypad (see paragraph *4.2 How to enter alphanumeric characters*). The name can be up to 24 characters long. Press OK to confirm.

```
NAME
U01:...
```

17) Press ▼.

```
UC.U1:          U01
VOCAL NAME
```

IMPORTANT! The vocal name can only be used for "commandable" customised outputs.

18) Press OK. Press ▼ and ▲ to select whether the output message must be activated (on) or deactivated (off). Press OK to confirm.

```
VOCAL NAME
MSG OUTPUT ON
```

19) Press OK to play the vocal message of the output.

```
MSG OUTPUT ON
PLAY
```

20) Press ▼. To record, press OK (see paragraph *4.3 VOCAL name* for more information).

```
MSG OUTPUT ON
RECORD
```

21) Press ▼. Press OK to delete the vocal message of the output.

```
MSG OUTPUT ON
DELETE
```

22) Press ESC three times to program the other outputs of the same device repeating the procedure from step 5. Press ESC again to program the outputs of another device (expansion modules, keypads, readers), repeating the procedure from step 4.

23) Press ESC repeatedly to exit from the menu.

IMPORTANT! Program all the outputs used by the system.

4.13 KEYPAD PROGRAMMING

The keypad programming procedure is described below. It is important to note that some functions are only available on vocal keypads KP500DV/N.

4.13.1 Functions to be configured

Gong function: audible buzz indication from the keypad when an input with ancillary gong function enabled is opened when the system is disarmed.

Sound time entry: auditory indication provided by the keypad buzzer of the elapsing entry time when the system is disarmed.

Sound time exit: auditory indication provided by the keypad buzzer of the elapsing exit time when the system is armed.

Masking: this hides system status (armed or disarmed) when it is enabled. The specific LED is off and nothing appears on the keypad display. System status may be checked when the masking function is enabled by entering a valid code on the keypad.

IMPORTANT! Do not enable masking to maintain EN50131 compliance. The LEDs are managed directly by the control panel.

Function keys: this is used to enable or disable the “Fire”, “Silent Panic” and “Emergency” keys on the keypad. By holding these keys pressed for at least three seconds, the control panel generates the respective alarm without needing to enter any code.

4.13.2 Emergency indication

In case of emergency indication (from emergency input, key or "lack of move"), the system will automatically activate the environmental listening function on the vocal keypad after having sent the pre-recorded vocal message.
The called user can listen to the voices and noises in the keypad surroundings.
DTMF controls (see paragraph *6.5 List of VOCAL answer machine DTMF controls* and following) can be used to alternate listening and talking or to listen to the environmental noises in the surroundings of other vocal keypads.

IMPORTANT! The automatic listening function can only be activated on the preferred keypad if there are several keypads.

The automatic listening function at end of call is activated directly on a vocal keypad on which the emergency key was pressed if the emergency indication was activated in this manner (the “ENVIR. LISTENING” programming is ignored).
The automatic listening function at end of call is activated directly by the keypad on which “ENVIR. LISTENING” is enabled (the programming is respected) if the emergency indication was activated by pressing the emergency key of a keypad without vocal functions.

4.13.3 Programming procedure

Proceed as follows to program the emergency indication:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until PROGRAMMING appears.

```
UT00:INSTALLER
PROGRAMMING
```

2) Press [OK] and then [▼] several times until KEYPADS appears.

```
PROGRAMMING
KEYPADS
```

3) Press [OK].

```
KEYPADS
KP01:KP 01
```

4) Press [▼] and [▲] to select the required keypad. Press [OK] to confirm.

```
KP01:KP 01
ASSIGN
```

5) Press [OK]. Press [▼] and [▲] to assign the keypad to the SYSTEM (all partitions) or only to some PARTITIONS. Press [OK] to confirm.

```
ASSIGN
SYSTEM
```

6) If SYSTEM is selected, press [▼] and [▲] to select SYSTEM ASSIGN or SYSTEM DO NOT ASSIGN and press [OK] to confirm. Then [ESC].
7) The screen page shown here by the side will appear if PARTITIONS is selected. The empty boxes represent partitions which are not assigned to the keypad and the black boxes the partitions which have already been assigned. Press [◄] and [►] to select the partition to be associated. Press [▼] and [▲] to assign the partition (the square will turn black) or to disassociate it (the square will appear empty). Repeat the procedure for all partitions to be associated to the keypad. Press [OK] at the end. Then [ESC].

```
SE##:
□□□□□■□
```

8) Press ▼.

```
KP01:KP 01
GONG FUNCTION
```

9) Press OK. Press ▼ and ▲ to enable or disable the keypad gong function. Press OK to confirm.

```
GONG FUNCTION
DISABLE
```

10) Press ▼.

```
KP01:KP 01
SOUND TIME ENTRY
```

11) Press OK. Press ▼ and ▲ to enable or disable the entry time sound. Press OK to confirm.

IMPORTANT! The Entry Time sound indication is mandatory for EN50131 grade 3 compliance.

12) Press ▼.

```
KP01:KP 01
SOUND TIME EXIT
```

13) Press OK. Press ▼ and ▲ to enable or disable the exit time sound. Press OK to confirm.

IMPORTANT! The Exit Time sound indication is mandatory for EN50131 grade 3 compliance.

14) Press ▼.

```
KP01:KP 01
MASKING
```

15) Press OK. Press ▼ and ▲ to enable or disable masking. Press OK to confirm.

IMPORTANT! Do not enable masking to maintain EN50131 compliance. The LEDs are managed directly by the control panel.

16) Press ▼.

```
KP01:KP 01
NAME
```

17) Press OK. Enter a descriptive name for the keypad using the keypad (see paragraph *4.2 How to enter alphanumeric characters*). The name can be up to 24 characters long. Press OK to confirm.

```
NAME
KP01:KP 01
```

18) Press ▼.

```
KP01:KP 01
FUNCTION KEYS
```

19) Press OK. Press ▼ and ▲ to select the concerned function. Press OK to confirm.

```
FUNCTION KEYS
FIRE ALARM
```

20) Press ▼ and ▲ to enable or disable the function key. Press OK to confirm.

21) Repeat the procedure from step 19 to enable the other function keys.

22) Press ESC to program the other keypads repeating the procedure from step 3.

23) Press ESC repeatedly to exit from the menu.

IMPORTANT! Program all the keypads used by the system.

4.14 READER PROGRAMMING

4.14.1 LED management

The reader LEDs may be freely assigned to one or more system partitions.
Different associations may be implemented for each reader but it is not possible to associate a same partition to several LEDs of the same reader.

The green LEDs display the associated partition status.
The red LED shows anomalies (open inputs, alarms).

The masking function hides system status (armed or disarmed) when it is enabled. The reader LEDs will be off. System status may be checked when the masking function is enabled by inserting a valid key.

EN50131

IMPORTANT! Do not enable masking to maintain EN50131 compliance. The LEDs are managed directly by the control panel.

4.14.2 Programming procedure

Proceed as follows to program the readers:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until PROGRAMMING appears.

```
UT00:INSTALLER
PROGRAMMING
```

2) Press [OK] and then [▼].

```
PROGRAMMING
READERS
```

3) Press [OK].

```
READERS
DK01:DK 01
```

4) Press [▼] and [▲] to select the required reader. Press [OK] to confirm the selection.

```
DK01:DK 01
ASSIGN
```

5) Press [OK]. Press [▼] and [▲] to select the concerned LED. Press [OK] to confirm.

```
ASSIGN
LED 1   |▲ |
```

6) The screen page shown here by the side will appear. The empty boxes represent partitions which are not assigned to the LED and the black boxes the partitions which have already been assigned. The partitions already assigned to another LED of the reader will not be displayed. Press [◄] and [►] to select the partition to be associated. Press [▼] and [▲] to assign the partition (the square will turn black) or to disassociate it (the square will appear empty). Repeat the procedure for all partitions to be assigned to the output. Press [OK] at the end.

```
SE01:
□□□□□■□
```

7) Repeat the procedure from step 5 for the other LEDs, if necessary (it is not necessary to assign all LEDs to partitions).

```
ASSIGN
LED 1   |▲ |
```

8) Press [ESC] and then [▼].

```
DK01:DK 01
MASKING
```

9) Press [OK]. Press [▼] and [▲] to enable or disable masking. Press [OK] to confirm.

IMPORTANT! Do not enable masking to maintain EN50131 compliance. The LEDs are managed directly by the control panel.

10) Press [▼].

```
DK01:DK 01
NAME
```

11) Press [OK]. Enter a descriptive name for the reader using the keypad (see paragraph *4.2 How to enter alphanumeric characters*). The name can be up to 24 characters long. Press [OK] to confirm.

```
NAME
DK01:DK 01
```

12) Press [ESC] to program the other readers repeating the procedure from step 3.

13) Press [ESC] repeatedly to exit from the menu.

IMPORTANT! Program all readers used in the system.

4.15 KEYS

The MP500/4N, MP500/8 and MP500/16 systems can manage up to 16, 32 or 64 electronic and proximity keys respectively. The key must be acquired, i.e. the control panel must read and store its univocal code, before configuring it.

4.15.1 Key acquisition

Proceed as follows to acquire an electronic or proximity key:

1) Enter **< Installer / Technical Manager code>**, press [OK], then [MENU] and finally [▼] repeatedly until SETTINGS appears.

```
UT00:INSTALLER
SETTINGS
```

2) Press [OK] and then [▼] several times until KEYS appears.

```
SETTINGS
KEYS
```

3) Press [OK].

```
KEYS
ACQUIRE KEY
```

4) Press [OK].

```
KEYS
ACQUIRE KEY
```

5) Press [OK]. Press [▼] and [▲] to acquire the key using a reader or touchscreen keypad. Press [OK] to confirm.

```
ACQUIRE KEY
READERS
```

6) The screen page shown here by the side will appear if reader is selected. Press [▼] and [▲] to select the reader to be used to acquire the key. Press [OK] to confirm.

```
READERS
DK01:DK01
```

7) The four LEDs on the front of the reader will start blinking to indicate that it is ready to receive a key to be stored.

```
READERS
IN PROGRESS...
```

8) Insert the electronic key or approach the proximity key (with transponder reader and touchscreen keypad). The LEDs of the reader will stop blinking and will light up green fixed. The address assigned to the key will appear on the keypad display.

```
READERS
KE01:...
```

9) Remove the acquired key or move it away.

10) To acquire other keys, either insert or approach time, according to the type, and wait for a new address to appear on the display.

11) Press [ESC] repeatedly to exit from the menu at the end of the acquisitions.

4.15.2 Delete Key

Proceed as follows to delete an electronic or proximity key from the system:

1) Enter **< Installer / Technical Manager code>**, press [OK], then [MENU] and finally [▼] repeatedly until SETTINGS appears.

```
UT00:INSTALLER
SETTINGS
```

2) Press [OK] and then [▼] several times until KEYS appears.

```
SETTINGS
KEYS
```

3) Press [OK].

```
KEYS
ACQUIRE KEY
```

4) Press [▼].

```
KEYS
DELETE KEY
```

5) Press [OK]. Press [▼] and [▲] to select the keys to be deleted. Press [OK] to confirm.

```
DELETE KEY
KE01:…
```

6) Press [OK] to confirm deletion [ESC] to cancel the operation.

```
KE01:…
ARE YOU SURE?
```

7) Press [ESC] repeatedly to exit from the menu at the end of the deleting procedure.

```
DELETE
IN PROGRESS...
```

4.15.3 Key configuration

The following parameters can be defined for each key:

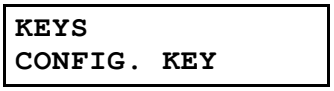
- **Key type**, i.e. what the key controls. The possible options are:
  - **Accesses**: the key switches the door opener output and this is stored on the event log.
  - **Partitions**: the key is enabled for the normal monitoring functions of the burglar alarm system (arming/disarming).
  - **Partitions + Accesses**: the key is enabled for both functions.
- **Partitions**, i.e. the partitions which are assigned to the key.
- **Name**, i.e. a descriptive name to easily identify the key on the event log and in messages.

Proceed as follows to configure an electronic or proximity key:

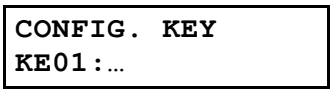
1) Enter **< Installer / Technical Manager code>**, press [OK], then [MENU] and finally [▼] repeatedly until SETTINGS appears.

2) Press [OK] and then [▼] several times until KEYS appears.

3) Press [OK] and then [▼] several times until CONFIG. KEY appears.



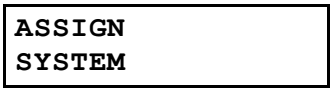
4) Press [OK]. Press [▼] and [▲] to select the keys to be configured. Press [OK] to confirm.



5) Press [OK]. Press [▼] and [▲] to select partition control, access control or partition-access control. Press [OK] to confirm.

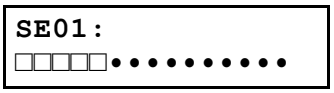
6) Press [▼].

7) Press [OK]. Press [▼] and [▲] to assign the key to the entire system or to specific partitions. Press [OK] to confirm.

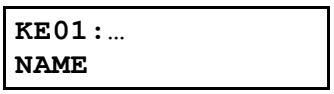


8) The screen page shown here by the side will appear if SYSTEM is selected. Press [▼] and [▲] to assign the key to the entire system or not. Press [OK] to confirm.

9) The screen page shown here by the side will appear if PARTITIONS is selected. Press [◄] and [►] to go from one partition to the other. Press [▼] and [▲] to select or deselect the partition (*empty square* = not assigned, *full square* = assigned). Press [OK] to confirm the selection.



10) Press [▼].



11) Press [OK]. Give a descriptive name (up to 24 characters long) to the key and press [OK] to confirm. See paragraph *4.2 How to enter alphanumeric characters* for insertion.

12) Press [ESC] repeatedly to exit from the menu.

4.16 ADVANCED PROGRAMMING

4.16.1 Remote control system code

The code which identifies the system must be set in the MP500/4N, MP500/8 or MP500/16 control panel in order to control it remotely using the Hi-Connect software.

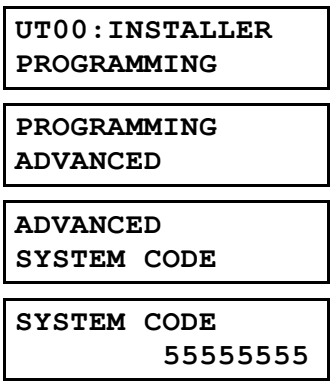
The code may be selected as required by the installer and must be eight digits long.

IMPORTANT! The code must be univocal for all systems managed by the installer, regardless of the type of installed control panel.

4.16.2 Programming procedure

Proceed as follows to program the remote control system code:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until PROGRAMMING appears.
2) Press [OK] and then press [▼] several times until ADVANCED appears.
3) Press [OK].
4) Press [OK]. Change the code using keys [◄] [►] and the numeric keypad. Press [OK] to confirm the new code or press [ESC] to cancel.
5) Press [ESC] repeatedly to exit from the menu.



4.17 GENERAL SYSTEM PARAMETERS (TIMINGS)

The general system parameters are used to manage alarms and indications. Some of these parameters may be configured.

IMPORTANT! Specific minimum and maximum values must be respected to ensure EN50131 compliance for the following parameters.
However, these requirements may be ignored, while maintaining EN50131 compliance, in presence of local police regulations which require other settings.

- **T BURGLAR ALARM**: This is the alarm output activation time (e.g. the time for which the sirens sound) for burglar alarms. Selectable times: 30 / 60 / 90 / 180 seconds and 9 / 15 minutes.

  IMPORTANT! The minimum alarm time for an EN50131 compliant system is 90 seconds.

- **T PRE-ALARM**: This is the pre-alarm output activation time (e.g. the time for which the sirens sound). Selectable times: 30 / 60 / 90 / 180 seconds and 9 / 15 minutes.

  IMPORTANT! The minimum alarm time for an EN50131 compliant system is 90 seconds.

- **T EMERGENCY ALAR**: This is the output activation time (e.g. the time for which the sirens sound) for the emergency alarms. Selectable times: 30 / 60 / 90 / 180 seconds and 9 / 15 minutes.

- **ALARM COUNT**: This is the number of permitted alarm repetitions also in case of new alarms. DISABLED means that the alarm indications will be generated at each new event. Selectable values: DISABLED, 2 / 4 / 6 / 8 / 10.

  IMPORTANT! The alarm count must be enabled to ensure EN50131 compliance.

  The alarm count is reset at each alarm system activation cycle and at 10:00 every day.

- **T LACK OF POWER**: this is the time of a mains blackout before generating the no power event. Selectable times: 10 / 30 minutes, 1 hour.

  IMPORTANT! The maximum no power time before generating an alarm must be 1 hour in an EN50131 compliant system.

4.17.1 Programming procedure

Proceed as follows to program the timings:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until PARAMETERS appears.

```
UT00:INSTALLER
PARAMETERS
```

2) Press [OK].

```
PARAMETERS
T BURGLAR ALARM
```

3) Press [OK]. Press [▼] and [▲] to select the required time. Press [OK] to confirm.

```
T BURGLAR ALARM
15min
```

4) Press [▼].

```
PARAMETERS
T PRE-ALARM
```

5) Press [OK]. Press [▼] and [▲] to select the required time. Press [OK] to confirm.

```
PRE-ALARM
15min
```

6) Press [▼].

```
PARAMETERS
T EMERGENCY ALAR
```

7) Press [OK]. Press [▼] and [▲] to select the required time. Press [OK] to confirm.

```
T EMERGENCY ALAR
180s
```

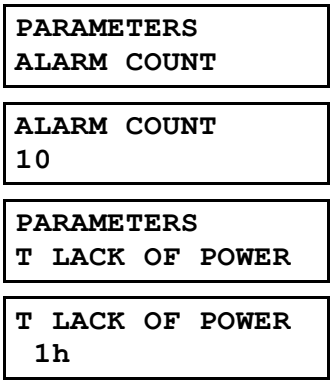
8) Press [▼].

9) Press [OK]. Press [▼] and [▲] to select the required time. Press [OK] to confirm.

10) Press [▼].

11) Press [OK]. Press [▼] and [▲] to select the required time. Press [OK] to confirm.

12) Press [ESC] repeatedly to exit from the menu.



4.18 TELEPHONE DIALER

IMPORTANT! The MP500/4N, MP500/8 or MP500/16 control panel must be connected to at least one telephone network PSTN or GSM. See the *Installation Manual* for more information on telephone connections.

IMPORTANT! The control panel connection type determines EN50131 compliance.

A MP500/8 or MP500/16 control panel connected via the ILT500-N interface to an ATS4 external communicator, connected in turn to a modem/router with ADSL line, is EN50131 grade 3 compliant.

A MP500/4N, MP500/8 or MP500/16 control panel connected directly to a PSTN line via the ILT500-N interface which uses numeric protocols for alarm communications is EN50131 grade 2 compliant.

All other telephone connections, including use of the GSM network via the IMG500/N interface, are not EN50131 compliant.

4.18.1 Telephone numbers

The dialler of the MP500/4N, MP500/8 and MP500/16 panels may store up to 12,12,12 telephone numbers, respectively. Each number may contain up to 28 digits or pauses in any combination.

Each pause lasts for 2 seconds. Simply queue pauses to obtain a longer pause. The pauses are inserted by pressing the [▼] key and are indicated on the display by a "**P**".
The stored telephone numbers may be associated to the entire system (the telephone number will be used for any event) or to specific partitions (the telephone number will be used only for the events concerning these partitions).
It is possible to select which telephone network (channel) the transmitter will use to connect with the outside: the traditional telephone landline (PSTN) or the mobile phone network (GSM). The choice will only be possible if both networks are available (PSTN line connected, GSM module inserted).

IMPORTANT! The GSM network cannot be used in an EN50131 compliant system.

ADVICE: By enabling the GSM answering machine the GSM module will always be active and calls will be sent faster.

4.18.1.1 Storing, editing and deleting a telephone number

The respective procedure are described in the *User Manual*.

4.18.2 Vocal messages

EN50131
NOT RELATED

IMPORTANT! The SV500N vocal synthesis board must be installed in MP500/4N, MP500/8 or MP500/16 control panels to be able to send vocal messages.

Vocal messages are created automatically by the dialler as they are sent. The message may be more or less detailed according to the event type to be communicated and the choice made during programming.

Four sending more, from the most simple (1) to the most complete (3) are available for MP500/4N, MP500/8 and MP500/16 control panels. Mode 4 allows to customise vocal messages completely. The messages are created by stringing together customised messages, pre-recorded messages and vocal names assigned to partitions and inputs during programming.

The elements of the message are:

- **Base message**: This is a 10 second long customisable message. It tells where the event occurred.
  Example: “Alarm system, John Smith's home, 10 Main Street, York”.
- **Event**: This pre-recorded message specifies the occurred event. Some event messages may be customised when Sending Mode 4 is selected.
- **Partition N**: This pre-recorded message identifies the partition(s) associated to the input which generated the event. The form is *“Partition n”*, where “n” is the number of the partition.
- **Input N**: This pre-recorded message specifies the input occurred by the event. The form is *“Input n”*, where “n” is the logical number of the input.
- **Partition name**: This is the recorded name of the partition ("vocal name") assigned during partition programming. It is played only if it is set.
- **Input name**: This is the recorded name of the input ("vocal name") assigned during input programming. It is played only if it is set

The table *10.1 VOCAL alarm messages* shows all the pre-recorded messages required for the various events.

The messages are formed as follows:

- **Mode 1**: Basic message + Event
- **Mode 2**: Basic message + Event + Partition number + Partition name.
- **Mode 3**: Basic message + Event + Partition number + Partition name + Input number + Input name.
- **Mode 4**: Basic message + Event + Partition name + Input name.

EXAMPLE
Someone has attempted to break into John Smith's home through the bathroom window. The bathroom window detector is connected to logical input 14 (vocal name: “Bathroom window”), which belongs to partition 1 (vocal name: “Perimeter”).

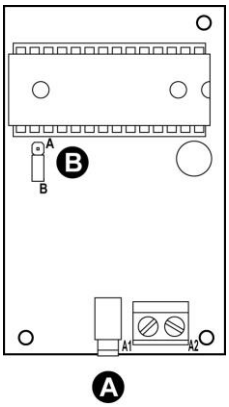
The message will be sent as follows in the four modes:

- **Mode 1**: “Alarm system, John Smith's home, 10 Main Street, York. Burglar alarm".
- **Mode 2**: “Alarm system, John Smith's home, 10 Main Street, York. Burglar alarm. Partition 1. Perimeter”.
- **Mode 3**: “Alarm system, John Smith's home, 10 Main Street, York. Burglar alarm. Partition 1. Perimeter. Input 14. Bathroom window”.
- **Mode 4**: “Alarm system, John Smith's home, 10 Main Street, York. Burglar alarm. Perimeter. Bathroom window”.

4.18.2.1 How to play and record vocal messages

IMPORTANT! On MP500/4N, MP500/8 and MP500/16 control panels, use a vocal keypad (KP500DV/N) or headset with microphone to be plugged into the vocal synthesis board directly (installer only) to play and record vocal messages.
It is advisable not to hold the KP500DV/N keypad in your hand for better audio quality.

On SV500N boards, you can select to record using the headset with microphone or vocal keypad and setting the jumper **B** on the vocal synthesis board appropriately.



Recording using vocal keypad.

Recording using headset plugged into jack **A**.

Figure 8 - Vocal synthesis board jumper and jack

4.18.2.2 Vocal message configuration

Proceed as follows to configure the vocal messages:

1) Enter **<Master / Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALER appears.

```
UT00:INSTALLER
TELEPHONE DIALER
```

2) Press [OK] and then [▼].

```
TELEPHONE DIALER
VOCAL MESSAGES
```

3) Press [OK].

```
VOCAL MESSAGES
MESSAGE LIST
```

4) Press [OK].

```
MESSAGE LIST
BASE MESSAGE
```

5) Press [▼] and [▲] to select the desired message. Press [OK] to confirm.

```
BASE MESSAGE
PLAY
```

6) Press [▼] and [▲] to select whether to play or record the message. Press [OK] to confirm. The maximum length of a message is 4 seconds. The message “RECORDING IN PROGRESS...” appears once the recording has started. The recording will stop automatically after the maximum time (which cannot be shortened).

   IMPORTANT! The original messages will be lost and can no longer be restored after they have been written over.

7) Press [ESC] to configure the other vocal messages repeating the procedure from step 5.

   IMPORTANT! The basic message is the only one which must always be recorded during the first installation.

8) Press [ESC] repeatedly to exit from the menu.

4.18.2.3 Vocal message sending mode

Proceed as follows to configure vocal message sending mode:

1) Enter **<Master / Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALER appears.

```
UT00:INSTALLER
TELEPHONE DIALER
```

2) Press [OK] and then [▼].

```
TELEPHONE DIALER
VOCAL MESSAGES
```

3) Press [OK].

```
VOCAL MESSAGES
MESSAGE LIST
```

4) Press [▼].

```
VOCAL MESSAGES
VOCAL SEND.MODE
```

5) Press [OK]. Press [▼] and [▲] to select the sending mode. The sending mode applies to <u>all</u> vocal messages. Press [OK] to confirm.

```
VOCAL SEND.MODE
MODE 1
```

6) Press [ESC] repeatedly to exit from the menu.

4.18.3 SMS text messages

The procedures for text messages are contained in the *User Manual*.

4.18.4 Alarm sending types

EN50131

IMPORTANT! Numeric codes with IDP protocol using an ATS4 external communicator is the only EN50131 grade 3 compliant sending type. EN50131 grade 2 compliance may be obtained without ATS4.
All other sending types cancel EN50131 compliance.
However, the grade 2 alarm sending types which are <u>added to the IDP sending mode (main mode)</u> do not prevent or cancel compliance.

The telephone dialler may interface with the outside world in various manners:

- **IDP**: the dialler sends alarms in form of numeric codes. This is only mode used for connecting to Alarm Receiving Centres. See table *10.3 IDP message structure* for details on IDP message structure.
- **ADF**: same as IDP, with different protocol.
- **Modem**: the dialler exchanges information (sending and receiving) with a PC provided with Hi-Connect software.
- **SMS**: the dialler sends alarms in form of SMS text messages. These alarms can only be sent on the GSM network.
- **C200B**: same as IDP, with different protocol.
- **C200B P-P**: same as IDP, with different protocol.
- **Vocal**: the dialler sends alarms in form of vocal messages. See paragraph *4.18.2 Vocal messages* for more details.

IMPORTANT! Respect the Alarm Receiving Centre requirements for sending using numeric codes (IDP, ADF, C200B, C200B P-P).

One or more sending modes can be selected according to the alarm type to be sent.
The various possibilities are shown in the table in paragraph *10.2 Alarm sending types*.
Multiple, simultaneous alarms will be send in order of priority (0 = maximum priority, 8 = minimum priority - see table).

You can decide what alarm messages to send and the mode to be used for each telephone number. For example, burglar alarms can be sent as a vocal message and Partition status can be sent in a text message to a mobile phone.
Furthermore, the same message can be sent in multiple manner, e.g. by sending the burglar alarm to the same mobile phone as vocal message and as text message. To do this, program the same telephone number in two different memory positions, one in vocal sending mode and the other in text sending mode.

IMPORTANT! The choice also depends on the associated channel (PSTN or GSM): the GSM network must be used for sending text messages.

IMPORTANT! Precise delivery times are not guaranteed for text messages and for this reason this mode should only be used for alarms and messages which are not very important (low priority).

4.18.4.1 Programming procedure

Proceed as follows to send the alarms:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALER appears.

```
UT00:INSTALLER
TELEPHONE DIALER
```

2) Press [OK] and then [▼] several times until SENDING MODE appears.

```
TELEPHONE DIALER
SENDING MODE
```

3) Press [OK].

```
SENDING MODE
T01:
```

4) Press [▼] and [▲] to select the telephone line (T01…T12) to be used to send the messages. Press [OK] to confirm.

5) Press [▼] and [▲] to select the mode to be used to send the messages. Press [OK] to confirm.

```
T01:
IDP
```

6) Press [▼] and [▲] to select the event type. Press [OK] to confirm.

```
EVENTS IDP
BURGLAR
```

7) Press [▼] and [▲] to select whether to send the alarm message related to the event to the telephone number according to the chosen mode or not. Press [OK] to confirm.

```
BURGLAR
DO NOT SEND
```

8) Repeat procedure from step 6 for all alarm messages which must be sent to the same telephone number with the same mode.

9) To send messages in different mode to the same telephone number, press [ESC] and repeat the procedure from step 5.

10) Finally, to program the other telephone numbers, press [ESC] repeatedly until SENDING MODE appears, press [OK] and repeat the procedure from step 4.

```
TELEPHONE DIALER
SENDING MODE
```

11) Press [ESC] repeatedly to exit from the menu.

4.18.5 Alarm message and call block sending mode

On MP500/4N, MP500/8 and MP500/16 control panels, starting from control panel SW version 1.01 and starting from keypad SW version 1.03, has been added the option to select between two alarm message sending modes:

- **Mode 1** (available on SW versions prior to 1.01 and compliant with EN50131 grade 2 and grade 3)
- **Mode 2** (not compliant with EN50131 grade 2 and grade 3)

Proceed as follows to program the alarm message sending mode:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALER appears.

```
UT00:INSTALLER
TELEPHONE DIALER
```

2) Press [OK] and then [▼] several times until ADVANCED appears.

```
TELEPHONE DIALER
ADVANCED
```

3) Press [OK] and finally [▼] repeatedly until SENDING MODE appears.

```
ADVANCED
SENDING MODE
```

4) Press [OK].

5) Press [▼] and [▲] to select the alarm sending Mode. Press [OK] to confirm.

```
SENDING MODE
MODE 1
```

6) Press [ESC] repeatedly to exit from the menu.

```
    MP500/16
12/01/2014 10:10
```

On control panels with SW version prior to 1.01, the sending Mode selection menu is not available, Mode 1 is only available.

Mode 1

When one or several alarm events occur, the dialer:

1) Main goal is to call as soon as possible all the configured numbers considering the priorities of the events and managing first the numbers in the low memory position.
2) Calls the telephone number or numbers configured for that alarm event, starting from the one at low memory position (e.g.: T02 is called before T05)
3) For each telephone number and sending mode, the dialer will make up to 3 calling attempts.
4) When several telephone numbers have been programmed, a sequence is generated in which calls are routed altenately to the various numbers, always respecting the priority order of events. The sequence of numbers called is dynamic and depends, from time to time, on the involved events and on the concerned telephone numbers.

The vocal call cycle can be stopped by dialling “12” on the telephone which received the call after hearing the message and receiving the call block beep.

For emergency vocal calls, "12" can be dialled after having closed the environmental listening session at the end of the emergency vocal message repetition.

Vocal calls and text messages following burglar events may be interrupted also by entering a code or a key having partitions in common with the telephone numbers programmed for the event. This function may be useful in case of false alarms, for instance.
It is important to note that a call cannot be stopped once it has started and will continue until the end of the 3 attempts. No other calls will be made to the next numbers for the burglar event.

In the event of text messages, delivery time depends on the GSM network company.

Example 1:

Managing burglar alarm sending to 5 telephone numbers:

Programming the 5 telephone numbers:

Number 1: Burglar alarm in vocal mode.
Number 2: Burglar alarm in vocal mode.
Number 3: Burglar alarm in vocal mode.
Number 4: Burglar alarm in vocal mode.
Number 5: Burglar alarm in vocal mode.

Sending via PSTN line- No tone line check– No answer control

1. Burglar alarm.
2. Call cycle:

a) First burglar alarm calling attempt to number 1
b) First burglar alarm calling attempt to number 2
c) Second burglar alarm calling attempt to number 1
d) Second burglar alarm calling attempt to number 2
e) Third burglar alarm calling attempt to number 1
f) Third burglar alarm calling attempt to number 2

g) First burglar alarm calling attempt to number 3
h) First burglar alarm calling attempt to number 4
i) Second burglar alarm calling attempt to number 3
j) Second burglar alarm calling attempt to number 4
k) Third burglar alarm calling attempt to number 3
l) Third burglar alarm calling attempt to number 4

m) First burglar alarm calling attempt to number 5
n) Second burglar alarm calling attempt to number 5
o) Third burglar alarm calling attempt to number 5

Mode 2

IMPORTANT! Use of Mode 2 will cancel EN50131 compliance.

This mode allows to send alarms and/or events in sequence starting from the telephone number at the low memory position (e.g. T02 is called before T05) till the 12th memory position, if stored telephone numbers are available, considering of max priority only the hold-up event, whereas all the other events are considered of equal priority.

Mode 2 sequence management rule is always valid and independent of:

- Network associated to the telephone number (PSTN, GSM, GPRS, LAN)
- Type of sending selected for individual number (Vocal, IDP, IDP-IP, Ademco Fast, C200B, SMS, Modem)
- BackUp
- Delayed sending programming

If during the sending to a certain number a new event arrives that shall be sent to that number, then it will be immediately queued. This typeof operation allows to optimize the total number of calls.

If during the burglar alarm call cycle for vocal calls and text messages, a valid user code is entered on the keypad, the control panel will stop call sensing to those numbers which have at least one partition in common with the entered user code, except for the started call, if any.

To better explain the above management operations, find below three sending examples:

Example 1:

Activation and next burglar alarm.

Programming three numbers:

Number 1: sending burglar alarms + partition status vocal messages
Number 2: sending Burglar alarm in vocal mode
Number 3: sending partition status vocal messages

Sending via PSTN line- No tone line check– No answer control

1. User activates system partitions.
2. Control panel generates partition activation event
3. Call cycle:
   a. First attempt to call number 1
   b. First attempt to call number 3
   c. Second attempt to call number 1
   d. Second attempt to call number 3
   e. Third attempt to call number 1
   f. Third attempt to call number 3

Burglar alarm

1. Control panel generates burglar alarm event
2. Call cycle:
   a. First attempt to call number 1
   b. First attempt to call number 2
   c. Second attempt to call number 1
   d. Second attempt to call number 2
   e. Third attempt to call number 1
   f. Third attempt to call number 2

Example 2:

Disarm partitions with hold-up code:

Programming three numbers:

Number 1: burglar alarms + partition status vocal messages.
Number 2: hold-up vocal messages
Number 3: partition status vocal messages

Sending via PSTN line- No tone line check– No answer control

A) User disarm system partitions with hold-up code.
B) Control panel generates hold-up and disarm partitions events
C) Call cycle:
   a) First hold-up call attempt to number 2
   b) First disarm partitions call attempt to number 1
   c) First disarm partitions call attempt to number 3
   d) Second hold-up call attempt to number 2
   e) Second disarm partitions call attempt to number 1
   f) Second disarm partitions call attempt to number 3
   g) Third hold-up call attempt to number 2
   h) Third disarm partitions call attempt to number 1
   i) Third disarm partitions call attempt to number 3

Example 3:

Managing burglar alarm sending to 5 telephone numbers:

Programming the 5 telephone numbers:

Number 1: Burglar alarm in vocal mode.
Number 2: Burglar alarm in vocal mode.
Number 3: Burglar alarm in vocal mode.
Number 4: Burglar alarm in vocal mode.
Number 5: Burglar alarm in vocal mode.

Sending via PSTN line- No tone line check– No answer control

1. Burglar alarm
2. Call cycle:

a) First burglar alarm calling attempt to number 1
b) First burglar alarm calling attempt to number 2
c) First burglar alarm calling attempt to number 3
d) First burglar alarm calling attempt to number 4
e) First burglar alarm calling attempt to number 5
f) Second burglar alarm calling attempt to number 1
g) Second burglar alarm calling attempt to number 2
h) Second burglar alarm calling attempt to number 3
i) Second burglar alarm calling attempt to number 4
j) Second burglar alarm calling attempt to number 5
k) Third burglar alarm calling attempt to number 1
l) Third burglar alarm calling attempt to number 2
m) Third burglar alarm calling attempt to number 3
n) Third burglar alarm calling attempt to number 4
o) Third burglar alarm calling attempt to number 5

4.18.5.1 Answering machines and call cycles

It is important to understand what will happen if an answering machine picks up the call.

If the “answer control” function is enabled in PSTN line parameters, the dialler may interpret the reply as a correctly delivered alarm message and stop other calling attempts.

In this case, if the alarm sending mode is vocal only to a single telephone number, the recipient may not receive the message or listen to it when it is too late (the same situation could occur if several telephone numbers are programmed each of which provided with an answering machine, although this is less likely). In this case, it is advisable to deactivate "answer control".

4.18.6 PSTN parameters

The following parameters can be used for configuring the PSTN connection:

- **Nation**: select the country where the system is installed to automatically set the technical PSTN telephone line connection parameters. Available countries are: Italy, France, Germany, Czech Republic, Poland, Spain, Portugal, Greece, UK.
- **PABX connection**: if the dialler is connected through a switchboard (PABX) and not directly to the external telephone line, the number (from 0 to 9) that the dialler must dial to engage the telephone line can be programmed.

> **IMPORTANT!** Remember to deactivate the PSTN Line Test function if "PABX Connection" is selected (see *4.18.10 PSTN Line Test*).

- **Tone Line Check**: this is used to determine whether the dialler will wait for the dial tone (Tone Line Check enabled) or not (Tone Line Check disabled) before dialling.
- **Answer control**: this is used to determine whether the dialler must wait for the called number to answer or not. The possible options are:
  - **Enabled**: the vocal message only starts after the called number has answered. The vocal telephone number which replied is not called back.
  - **Disabled**: the vocal message is sent immediately after having dialled the telephone number without waiting for the called number to answer. The alarm message is repeated three times. In this condition, the control panel will repeat the vocal message three times for each number regardless of whether the number answers or not. The call cycle can still be stopped by dialling code “12”, as described in *4.18.5 Alarm message and call block sending* .

> **IMPORTANT!** Read paragraph *4.18.5.1 Answering machines and call cycles* before enabling or disabling the "Answer Control" function.

4.18.6.1 Programming procedure

Proceed as follows to program the PSTN parameters:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALER appears.

```
UT00:INSTALLER
TELEPHONE DIALER
```

2) Press [OK] and then [▼] several times until PSTN PARAMETERS appears.

```
TELEPHONE DIALER
PSTN PARAMETERS
```

3) Press [OK].

```
PSTN PARAMETERS
NATION
```

4) Press [OK]. Press [▼] and [▲] to select the country. Press [OK] to confirm.

```
NATION
ITALY
```

5) Press [▼].

```
PSTN PARAMETERS
PABX CONNECTION
```

6) Press [OK]. Press [▼] and [▲] to disable the function (DISABLE, i.e. the dialler does not connect to a switchboard) or a number to be dialled to engage the line (DIGIT: 9 … DIGIT: 2). Press [OK] to confirm.

```
PABX CONNECTION
DISABLE
```

7) Press [▼].

```
PSTN PARAMETERS
TONE LINE CHECK
```

8) Press [OK]. Press [▼] and [▲] to enable or disable the dialling tone check function. Press [OK] to confirm.

```
TONE LINE CHECK
DISABLE
```

9) Press [▼].

```
PSTN PARAMETERS
ANSWER CONTROL
```

10) Press [OK]. Press [▼] and [▲] to enable or disable the answer check function. Press [OK] to confirm.

```
ANSWER CONTROL
DISABLE
```

11) Press [ESC] repeatedly to exit from the menu.

4.18.7 GSM parameters

The following parameters can be configured if the GSM module interface is installed:

- **SIM PIN**: this is used to store the SIM Card PIN code (if required). The code may be from 4 to 6 digits long. The PIN code is supplied by the GSM network company.

  IMPORTANT! The programming procedure is used to store the SIM PIN on the control panel but not to program it on the SIM Card itself. To program the SIM PIN on the SIM Card, insert the SIM Card in a normal mobile phone, program it using the functions of the mobile phone and then insert it in the GSM interface of the control panel.

- **SIM Card Expiry**: this is used to store the prepaid SIM Card expiry month and year. The MP500/16 (or MP500/8) control panel will send a notice message to the vocal numbers and text numbers configured for the event on the first day of the stored month at 10 a.m. It is advisable to set the month before the actual expiry date (for example, set "March" if the SIM Card expires in the month of April). Reset the new expiry date to be notified after having recharged the SIM Card credit.
- **Incoming SMS**: this is used to enable text message reception for managing controllable outputs.

4.18.7.1 Programming procedure

Proceed as follows to program the GSM parameters:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALER appears.

```
UT00:INSTALLER
TELEPHONE DIALER
```

2) Press [OK] and then [▼] several times until GSM PARAMETERS appears.

```
TELEPHONE DIALER
GSM PARAMETERS
```

3) Press [OK].

```
GSM PARAMETERS
SIM PIN
```

4) Press [OK]. Enter the PIN on the keypad. Press [OK] to confirm. To delete a PIN code if it is not required by the SIM Card, press [ESC] followed by [OK]. Dashes will appear instead of the digits in this manner, meaning “PIN not programmed”.

```
SIM PIN
          ------
```

5) Press [▼]

```
GSM PARAMETERS
SIM CARD EXPIRY
```

6) Press [OK]. Enter month and year using the keypad. Press [OK] to confirm.

```
SIM CARD EXPIRY
DATE 01/12/22
```

IMPORTANT! The day cannot be changed.

7) Press [▼].

```
GSM PARAMETERS
INCOMING SMS
```

8) Press [OK]. Press [▼] and [▲] to select whether to disable or enable incoming SMS text message reception. Press [OK] to confirm.

```
INCOMING SMS
DISABLE
```

9) Press [ESC] repeatedly to exit from the menu.

4.18.8 GPRS parameters

The following parameters can be configured if the GPRS module interface is installed:

- **APN**: Access Point Name, alphanumeric field, max. 25 characters, containing the server web name of the GPRS access provider.
- **User**: alphanumeric field, max. 25 characters for programming the user ID needed to access the network.
- **Password**: alphanumeric field, max. 25 characters for programming the password needed to access the network.
- **DNS1**: IP address of Domain Name Server 1.
- **DNS2**: IP address of Domain Name Server 2.
- **ACCESS NUMBER**: telephone number needed to access the GPRS network. This is the number provided by the GPRS access provider.

The value of all parameters does not need to be known for GPRS configuration because they may be provider-specific. The only mandatory value is APN.

4.18.8.1 Programming procedure

Proceed as follows to program the GPRS parameters:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALER appears.

```
UT00:INSTALLER
TELEPHONE DIALER
```

2) Press [OK] and then [▼] several times until GPRS PARAMETERS appears.

```
TELEPHONE DIALER
GPRS PARAMETERS
```

3) Press [OK].

```
GPRS PARAMETERS
APN
```

4) Press [OK]. Enter the APN parameter setting on the keypad and press [OK] to confirm.

5) Press [▼].

```
GPRS PARAMETERS
USER
```

6) Press [OK]. Enter the User setting on the keypad and press [OK] to confirm.

7) Press [▼].

```
GPRS PARAMETERS
PASSWORD
```

8) Press [OK]. Enter the password setting on the keypad and press [OK] to confirm.

9) Press [▼].

```
GPRS PARAMETERS
DNS1
```

10) Press [OK]. Enter the DNS1 setting on the keypad and press [OK] to confirm.

11) Press [▼].

```
GPRS PARAMETERS
DNS2
```

12) Press [OK]. Enter the DNS2 setting on the keypad and press [OK] to confirm.

13) Press [▼].

```
GPRS PARAMETERS
ACCESS NUMBER
```

14) Press [OK]. Enter the ACCESS NUMBER setting on the keypad and press [OK] to confirm.

15) Press [ESC] repeatedly to exit from the menu.

4.18.9 IDP/IP parameters

The following parameters can be set to send alarms in IDP mode over IP, i.e. using the GPRS telephone interface or the IT500WEB web server:

- **REM.CTRL CODE:** numeric field, max. 16 characters (min. 3 characters) containing the code which must be registered at the alarm receiving centre.
- **CODE RECEIVER:** numeric field, max. 6 characters (min. 1 character) containing the ID code of the alarm receiving centre (optional).
- **SYSTEM CODE**: numeric field, max. 6 characters (min. 1 character) containing a further system ID code which must be registered at the alarm receiving centre (optional).
- **ENABLE ENCRYPT.:** parameter for enabling encrypted transmission. Select the encryption key length if encryption is enabled.
- **ENCRYPTION KEY:** hexadecimal field (from 0-9 and A-B-C-D-E-F) with number of characters which depends on the selected encryption length.
- **TIME STAMP:** parameter for enabling alarm transmission complete with transmission date and time.

4.18.9.1 Programming procedure

Proceed as follows to program the IDP/IP parameters:

1. Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALLER appears.
2. Press [OK] and then [▼] several times until IDP/IP PARAM. appears.
3. Press [OK].
4. Press [OK]. Enter the REM.CTRL CODE setting on the keypad and press [OK] to confirm.
5. Press [▼].
6. Press [OK]. Enter the CODE RECEIVER parameter setting on the keypad and press [OK] to confirm.
7. Press [▼].
8. Press [OK]. Enter the SYSTEM CODE setting on the keypad and press [OK] to confirm.
9. Press [▼].
10. Press [OK]. Enter the ENABLE ENCRYPT. parameter setting on the keypad and press [OK] to confirm.
11. Press [▼].
12. Press [OK]. Enter the ENCRYPTION KEY setting on the keypad and press [OK] to confirm.
13. Press [▼].
14. Press [OK]. Enter the TIME STAMP setting on the keypad and press [OK] to confirm.
15. Press [ESC] repeatedly to exit from the menu.

```
UT00: INSTALLER
TELEPHONE DIALER
```

```
TELEPHONE DIALER
IDP/IP PARAM.
```

```
IDP/IP PARAM.
REM.CTRL CODE
```

```
IDP/IP PARAM.
CODE RECEIVER
```

```
IDP/IP PARAM.
SYSTEM CODE
```

```
PARAMETRI IDP/IP
ENABLE ENCRYPT.
```

```
IDP/IP PARAM.
ENCRYPTION KEY
```

```
IDP/IP PARAM.
TIME STAMP
```

4.18.10 PSTN Line Test

EN50131 GRADO 3

The MP500/xx control panels can be programmed to check for the dial tone and ensure that the connection is working perfectly. A "Telephone fault" event is generated if it is not. This event is generated after three consecutive unsuccessful tests.

Note: *It is advisable to enable the Tone Line Check function as well if the PSTN Line Test function is enabled.*

IMPORTANT! If the control panel is the first device on the telephone line, as recommended, the line test will interrupt any telephone calls in progress. This is because the control panel engages the line for a few seconds for each test.

Possible PSTN line test settings are:

- **Disable**: the dial tone is not checked (this choice is only recommended if the control panel is connected to a PABX extension line).
- **24h**: the dial tone is checked every 15 minutes even if the system is disarmed. This function is EN50131 grade 2 compliant.
- **System ON**: the dial tone is checked every 15 minutes only if all configured partitions are armed.
- **ATS4**: (function available but not necessary on MP500/4N control panel) the connection between the ILT500-N interface and the ATS4 external communicator is checked. A telephone fault event is generated within no longer than 90 seconds if there is no connection. Having an ATS4 communicator connected and working is mandatory for EN50131 grade 3 compliance. The dial tone is checked by the ATS4 communicator. This function is EN50131 grade 3 compliant.

4.18.10.1 Programming procedure

Proceed as follows to program the PSTN line test:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALER appears.

```
UT00:INSTALLER
TELEPHONE DIALER
```

2) Press [OK] and then [▼] several times until PSTN LINE TEST appears.

```
TELEPHONE DIALER
PSTN LINE TEST
```

3) Press [OK]. Press [▼] and [▲] to select DISABLE, 24 H, SYSTEM ON or ATS4. Press [OK] to confirm.

```
PSTN LINE TEST
24 H
```

4) Press [ESC] repeatedly to exit from the menu.

4.18.11 Period Comm Test

MP500/xx control panels can automatically call the alarm receiving or remote control centres at predetermined intervals of time if periodical confirmation of correct system operation is required.
This test function is not mandatory but strongly recommended.

The possible alternatives are:

- **Disable**: no calls are made.
- **24h**: the check is carried out even when the system is disarmed at the chosen interval of time starting from the set time. The call is made to the associated telephone number. Possible intervals of time are 1, 4, 8, 12, 24, 48, 72, 96, 120, 144, 168 hours.
- **System ON**: the check is carried out only if all the configured partitions are armed at the chosen interval of time starting from the set time. The call is made to the associated telephone number. Possible intervals of time are 1, 4, 8, 12, 24, 48, 72, 96, 120, 144, 168 hours.

IMPORTANT! The "Period Comm Test" function does not need to be enabled for EN50131 grade 3 compliance because this function must be managed by the external communicator (ATS4) which must be connected.
If the control panel must be EN50131 grade 2 compliant (e.g. if the ATS4 external communicator is not installed), the "Period Comm Test" function must be set to 24h with a frequency of less than 24 hours.

4.18.11.1 Programming procedure

Proceed as follows to program the Period Comm Test function:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALER appears.

```
UT00:INSTALLER
TELEPHONE DIALER
```

2) Press [OK] and then [▼] several times until PERIOD COMM TEST appears.

```
TELEPHONE DIALER
PERIOD COMM TEST
```

3) Press [OK]. Press [▼] and [▲] to select DISABLE, 24 H or SYSTEM ON. Press [OK] to confirm.

```
PERIOD COMM TEST
DISABLE
```

4) The screen page shown here by the side will appear if 24H or SYSTEM ON is selected.

```
24H
ASSIGN TEL N.
```

5) Press [OK]. Press [▼] and [▲] to select the telephone number of the alarm receiving centre. Press [OK] to confirm.

```
ASSIGN TEL N.
T01:...
```

6) Press [▼].

```
24H
SET HOUR
```

7) Press [OK]. Enter the time in hh:mm (24 hour) format directly using the number keys using an initial 0 if needed. If you make a mistake press [ESC] and access the SET HOUR menu. Press [OK] to confirm the entered time.

```
24H
HOUR 10:24
```

8) Press [▼].

```
24H
INTERVAL
```

9) Press [OK]. Press [▼] and [▲] to select the interval of time between calls. Press [OK] to confirm.

```
INTERVAL
 1h
```

10) Press [ESC] repeatedly to exit from the menu.

4.18.12 Rem Ctrl Backup

The "Rem Ctrl Backup" function is used to manage calls to the telephone numbers programmed for numeric codes (IDP, ADF, C200B, C200B P-P) and modems.

If the function is enabled, calls to other telephone numbers programmed for numeric codes and modems for the same event will be blocked as soon as the first numeric code or modem call is successfully established.
A call is considered successfully established once acknowledgement is received from the alarm receiving centre.
If the first call is not successful, the control panel will call the next number and so on until the event to be transmitted is correctly sent/received or until the attempts are finished, if the calls are not successful.

If the "Rem Ctrl Backup" function is disabled, the dialler will call all the numbers programmed for numeric codes and modems, regardless of the received replies.

4.18.12.1 Programming procedure

Proceed as follows to program the Rem Ctrl Backup function:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALER appears.

```
UT00:INSTALLER
TELEPHONE DIALER
```

2) Press [OK] and then [▼] several times until REM CTRL BACKUP appears.

```
TELEPHONE DIALER
REM CTRL BACKUP
```

3) Press [OK]. Press [▼] and [▲] to select whether to enable or disable the Rem Ctrl Backup function. Press [OK] to confirm.

```
REM CTRL BACKUP
DISABLE
```

4) Press [ESC] repeatedly to exit from the menu.

4.18.13 Answer Machine

EN50131

The control panel will answer incoming telephone calls if the answering machine function is enabled.

The function must be enabled separately for the PSTN line and the GSM networks. Therefore, the control panel can be programmed to answer GSM calls and not PSTN calls, and vice versa.

When enabling the answering machine function on the PSTN line, you can specify after how many calls the dialler must answer, compatibly with other devices (e.g. other answering machines).

The GSM module answers after five rings.

Note: *The GSM module will remain normally off and only turned on for calling if the GSM answering machine function is disabled.*

IMPORTANT! The answering machine function is not guaranteed if the call is "anonymous", i.e. caller's ID is hidden (this applies to calls from landlines or mobile phones).
The relevant function on the landline or mobile phone may be "Show ID", "Show my number to", "Show personal number" or the like.
If you cannot establish a communication with the control panel, check the settings of the telephone in use and try again.

4.18.13.1 Programming procedure

Proceed as follows to program the Answer Machine function:

1) Enter **<Installer code>**, press OK, then MENU and finally ▼ repeatedly until TELEPHONE DIALER appears.
2) Press OK and then ▼ several times until ADVANCED appears.
3) Press OK.
4) Press OK.
5) Press OK. Press ▼ and ▲ to select whether to deactivate the Answer Machine function for the PSTN line or whether to answer incoming calls after 2, 4 or 8 rings (2 RING, 4 RING or 8 RING). Press OK to confirm.
6) Press ▼.
7) Press OK. Press ▼ and ▲ to select whether to disable or enable the Answer Machine function for the GSM network. Press OK to confirm.
8) Press ESC repeatedly to exit from the menu.

```
UT00:INSTALLER
TELEPHONE DIALER
```

```
TELEPHONE DIALER
ADVANCED
```

```
ADVANCED
ANSWER MACHINE
```

```
ANSWER MACHINE
PSTN
```

```
PSTN
DISABLED
```

```
ANSWER MACHINE
GSM
```

```
GSM
ENABLE
```

4.18.14 Rem.Ctrl Code

The control panel must communicate the remote control code supplied by the alarm receiving centre in order to connect to the centre.

The remote control code function is used to store the code on the control panel.

4.18.14.1 Programming procedure

Proceed as follows to program the remote control code:

1) Enter **<Installer code>**, press OK, then MENU and finally ▼ repeatedly until TELEPHONE DIALER appears.
2) Press OK and then ▼ several times until ADVANCED appears.
3) Press OK.
4) Press ▼.
5) Press OK. Enter the remote control code on the keypad and press ◄ ►. Press ESC to delete. Press OK to confirm the entered code.
6) Press ESC repeatedly to exit from the menu.

```
UT00:INSTALLER
TELEPHONE DIALER
```

```
TELEPHONE DIALER
ADVANCED
```

```
ADVANCED
ANSWER MACHINE
```

```
ADVANCED
REM.CTRL CODE
```

```
REM.CTRL CODE
        66666666
```

4.18.15 Return Call

The installer can enable the Return Call function for remote control operations. In this manner, it will be possible to connect to the system from a remote location using a PC running Hi-Connect software, call the control panel and be called back immediately and automatically.
In this manner, the cost of the telephone call will be charged to the control panel user.

Return Call options are:

- **Ret.Call Disable**: the control panel will continue the connection procedure to Hi-Connect after having received the call. The cost of the telephone call will be charged to the installer or to the remote control centre.
- **Ret.Call Type A**: after answering, the control panel will hang up and call back the first stored Modem type number. The cost of the call will be charged to the owner of the control panel.
- **Ret.Call Type B**: after answering, the control panel will hang up and call the specific telephone number sent by Hi-Connect during the previous connection. The cost of the call will be charged to the owner of the control panel.

IMPORTANT! The "Ret.Call Type A" setting is safer because the connection can only be established with a previously programmed telephone number.

4.18.15.1 Special cases: Rechargeable or voice only SIM Card

The system can still be controlled remotely using Hi-Connect if the SIM Card used in the control panel is "voice only", i.e. without a specific data call number (no M2M and/or incoming fax/data).

The necessary conditions for enabling remote control in this case are:

1. At least one modem type number must be programmed on the control panel
2. Ret.Call Type A function must be enabled
3. Remote control for the installer must be enabled on the Master user menu.

See the Hi-Connect application manual for more details.

4.18.15.2 Programming procedure

Proceed as follows to program Return call:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALER appears.

```
UT00:INSTALLER
TELEPHONE DIALER
```

2) Press [OK] and then [▼] several times until ADVANCED appears.

```
TELEPHONE DIALER
ADVANCED
```

3) Press [OK].

```
ADVANCED
ANSWER MACHINE
```

4) Press [ESC] repeatedly repeatedly until RETURN CALL appears.

```
ADVANCED
RETURN CALL
```

5) Press [OK]. Press [▼] and [▲] to disable the call back function or enable it at type A or type B. Press [OK] to confirm.

```
RETURN CALL
RET.CALL DISABLE
```

6) Press [ESC] repeatedly to exit from the menu.

4.18.16 Telephone line enabling

IMPORTANT! The telephone lines used must be enabled to be able to make or receive calls in addition to having installed the specific PSTN and GSM modules.

Each telephone line can be enabled separately, i.e. it is possible to enable only the PSTN line or the GSM network or both.
Any function configured for the line will not useable if the telephone line is not enabled.

If both telephone lines are enabled, the automatic back-up procedure can be used on the secondary line if the main network (i.e. the one associated to each single telephone number) is not available. See paragraph *4.18.1 Telephone numbers* for more details.

4.18.16.1 Programming procedure

Proceed as follows to enable telephone networks:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until TELEPHONE DIALER appears.

```
UT00:INSTALLER
TELEPHONE DIALER
```

2) Press [OK] and then [▼] several times until ADVANCED appears.

```
TELEPHONE DIALER
ADVANCED
```

3) Press [OK].

```
ADVANCED
ANSWER MACHINE
```

4) Press [▼] repeatedly until the screen page shown here by the side appears.

```
ADVANCED
PHONE LINE ENABL
```

5) Press [OK].

```
PHONE LINE ENABL
PSTN LINE
```

6) Press [OK]. Press [▼] and [▲] to enable or disable the PSTN line. Press [OK] to confirm.

```
PSTN LINE
ENABLE
```

7) Press [▼].

```
PHONE LINE ENABL
GSM LINE
```

8) Press [OK]. Press [▼] and [▲] to enable or disable the GSM network. Press [OK] to confirm.

```
GSM LINE
ENABLE
```

9) Press [▼].

```
PHONE LINE ENABL
LAN LINE
```

10) Press [OK]. Press [▼] and [▲] to enable or disable the LAN network. Press [OK] to confirm.

```
LAN LINE
ENABLE
```

11) Press [▼].

```
PHONE LINE ENABL
GPRS LINE
```

12) Press [OK]. Press [▼] and [▲] to enable or disable the GPRS network. Press [OK] to confirm.

```
GPRS LINE
DISABLE
```

13) Press [ESC] repeatedly to exit from the menu.

4.19 TIMED PROGRAMMER

4.19.1 Operating principles

The timed programmer can be used to automate repetitive operations, such as arming or disarming a partition or a commandable output. Programming is on a weekly basis, i.e. the commands are repeated in the same way every week.

Every day of the week can be classified as working day, pre-holiday or holiday as required and eight commands can be freely created by the user for each type. Multiple commands can be programmed for the same time.

The automatic partition arming command is indicated in advance on the keypads (buzzer sounding the timed programmer LED blinking) and activation of the timed programmers as notice that the command is about to be implemented. The advance is programmed under the “Warning Time” parameter.

System arming can be postponed following the procedure described in the *User Manual*.

The available timed programmer commands are:

Command	Description	Notes and examples
Arm partitions	Arms the partition or partitions	
Disarm partitions	Disarms the partition or partitions	
Activate commandable output	Activates the commandable output	This output can be controlled remotely.
Deactivate commandable output	Deactivates the commandable output	
Activate pulsed commandable output	Activates the pulsed commandable output for approx. 1 second	This pulsed output can be controlled remotely.
Enable key or user code	Enables a key or a code	Cleaning services: by combining the two commands it is possible to allow cleaning personnel to enter and work indoors only on given days and at given times.
Disable key or user code	Disables a key or a code	

IMPORTANT! The timed programmer cannot manage festivities occurring during the week (such as Christmas, bank holidays etc.) which will be treated as the day of the week on which they occur.

The control panel stores the timed programmer events permanently. The timed programmer can be enabled or disabled without deleting the stored events as shown in the *User Manual*.

The hourly programming state (enabled or disable) is shown on the keypad by the timed programmer LED.
The timed programmer commands remain active until the opposite command is imparted (by the timed programmer itself or by a user using the keypad or a reader): the programmer sends commands but does not check system or output status.

Example of operation
An office is open from Monday to Friday from 9 a.m. to 6 p.m. Days from Monday to Friday are set as working days. Saturdays and Sundays are set as holidays. The first command for working days is to disarm the burglar alarm system at 8:55 a.m. and the last command is to arm the system at 6:05 every day. There are no commands for holidays.

In practice, with the timed programmer, the burglar alarm system will be armed automatically at the end of each working day and will be disarmed on the morning of the following day. After having been armed on Friday evening, it will not be disarmed until Monday morning, because there are no disarming commands on Saturday and Sunday.

To access protected areas, if needed, a user can disarm the system manually with the keypad or reader also on Saturdays and Sundays. The user must remember to rearm the system when leaving because otherwise the areas will remain unprotected.

4.19.2 Programming

ADVICE: Fill in the respective tables before starting to program the timed programmer (see *10.6 Timed programmer configuration*): your work will be enormously simplified.

IMPORTANT! The time and date must be right for correct operation of the timed programmer (see paragraph *4.8 How to set date and time*).

The following parameters must be configured during programming:

- **Day Type**: set whether each day of the week (Monday, Tuesday… Sunday) must be considered as a working day, a pre-holiday or a holiday.
- **Command Type**: up to eight commands can be set for each day type (working day, pre-holiday or holiday).
- **Command N**: the time and action type is defined for each command.
- **Action**: there are three possibilities: no action, arm (enable) and disarm (disable). The actions can be applied to partitions, outputs, users and keys.
- **Warning Time**: this determines how many minutes of warning must be given before the command is implemented. The warning time allows to leave the area or to interrupt the automatic implementation of the command. The possible values are: no warning, 5 min, 10 min, 15 min, 20 min.

4.19.2.1 Programming procedure

Proceed as follows to program the timed programmer:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until SETTINGS appears.

2) Press [OK] and then [▼] several times until P.O. appears.

3) Press [OK].

4) Press [OK].

5) Press [▼] and [▲] to select the concerned day. Press [OK] to confirm.

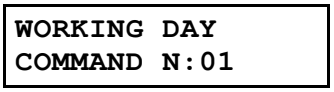
6) Press [OK]. Press [▼] and [▲] to select the type (working day, pre-holiday, holiday). Press [OK] to confirm.

7) Repeat from step 5 to define the type of all days.

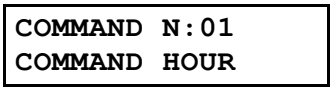
8) Press [ESC] and then [▼].

9) Press [OK]. Press [▼] and [▲] to select the concerned day type. Press [OK] to confirm.

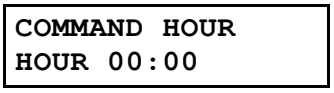
10) Press [▼] and [▲] to select the concerned command number. Press [OK] to confirm.



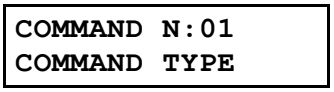
11) Press [OK].



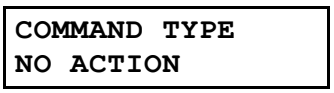
12) Enter the time on which to implement the command using the keypad. Press [OK] to confirm.



13) Press [▼].



14) Press [OK]. Press [▼] and [▲] to select the concerned command type (no action, arm, disarm). Press [OK] to confirm. If arm (or disarm) is chosen, you can choose whether to apply the action to partitions, outputs, users or keys and other details within each category. The selection procedures are user-friendly.



15) Repeat from step 11 for the other commands of the day, if needed [ESC].

16) Repeat from step 10 to configure the other day types.

17) Press [ESC].

```
P.O.
COMMANDS TYPE
```

18) Press [▼].

```
P.O.
WARNING TIME
```

19) Press [▼] and [▲] to select the warning time. Press [OK] to confirm.

```
WARNING TIME
WARNING 10m
```

20) Press [ESC] repeatedly to exit from the menu.

4.19.3 Deleting a command

To delete a command, follow the programming procedure and select "NO ACTION" for the command.
To block the entire programming, disable it without deleting it (see *User Manual*).

4.20 SYSTEM TEST

Check correct operation of the system as a whole after having installed and configured the devices.
The main tests are:

- Input test
- Output test
- Control panel battery test
- Vocal call test
- Alarm receiving centre test (if present)
- GSM test (if present)
- Radio device test (For more information see dedicated manual)
- Environmental listening test

4.20.1 Input test

Proceed as follows to test that the inputs work perfectly:

1) Enter **< Master / Installer code >**, press [OK] and then [MENU].

```
UT00:INSTALLER
TEST
```

2) Press [▼] repeatedly until TEST appears.

```
UT01:MASTER
TEST
```

3) Press [OK].

```
TEST
TEST INPUTS
```

4) Press [OK].

```
TEST INPUTS
IN PROGRESS...
```

5) Trip all system detectors (e.g. by passing in front of the volumetric detectors and opening doors with magnetic contacts). The input LED on the keypad will be activated whenever a detector is activated. Press [OK] at the end.

```
TEST INPUTS
TEST RESULT
```

6) Press [OK].

7) Press [OK] to view the list of all the inputs which were tripped during the test.

```
TEST RESULT
TEST INPUT OK
```

8) Press [ESC] and then [▼].

9) Press [OK] to view the list of all inputs which did not change. The list should be empty if all inputs were tripped during the test and they all opened and closed again correctly. Otherwise, the list will contain the inputs which were either not tripped or did not respond correctly.

```
TEST RESULT
TEST INPUT KO
```

10) Press [ESC] repeatedly to exit from the menu.

4.20.2 Output test

Proceed as follows to test that the outputs work perfectly:

1) Enter **< Master / Installer code >**, press OK and then MENU.
2) Press ▼ repeatedly until TEST appears.
3) Press OK and press ▼ repeatedly until TEST OUTPUTS appears.
4) Press OK.
5) Press ▼ and ▲ to select the device the outputs of which you want to test. Press OK to confirm.
6) Press ▼ and ▲ to select the output to test. Press OK to confirm.
7) The output will switch from ARM to DISARM every time OK is pressed. Check that the output behaves as expected, e.g. that a siren sounds (if the output is connected to a siren) or that an indicator lights up (if the output is connected to an indicator or blinker). Press ESC to proceed if the test was successful.
8) Repeat from step 6 to test the other outputs of the device.
9) After having tested all the outputs of the device, press ESC and repeat from step 5 to test the outputs of another device.
10) Press ESC repeatedly to exit from the menu. The outputs will be returned to the correct state.

```
UT00:INSTALLER
TEST
```

```
UT01:MASTER
TEST
```

```
TEST
TEST OUTPUTS
```

```
TEST OUTPUTS
CONTROL PANEL
```

```
CONTROL PANEL
UC.U1         U01
```

```
UC.U1         U01
ARM
```

4.20.3 Battery test

Proceed as follows to check the condition of the batteries:

1) Enter **< Master / Installer code >**, press OK and then MENU.
2) Press ▼ repeatedly until TEST appears.
3) Press OK and press ▼ repeatedly until TEST BATTERY appears.
4) Press OK.
5) The battery test will last for approximately 30 seconds during which the keypad will beep. The battery status information provided by the LEDs and on the event log will be updated at the end of the test (if there are changes). Any auxiliary power units will also run the battery test and communicate the result to the control panel at the end. The failure LED will indicate flat batteries.
6) Press ESC repeatedly to exit from the menu.

```
UT00:INSTALLER
TEST
```

```
UT01:MASTER
TEST
```

```
TEST
TEST BATTERY
```

```
TEST BATTERY
IN PROGRESS...
```

4.20.4 Vocal call test

Proceed as follows to test that the vocal calls work perfectly:

1) Enter **< Master / Installer code >**, press [OK] and then [MENU].
2) Press [▼] repeatedly until TEST appears.
3) Press [OK] and press [▼] repeatedly until ADVANCED TESTS appears.
4) Press [OK].
5) Press [OK].
6) Press [▼] and [▲] to select the programmed vocal telephone number to be called. Press [OK] to confirm.
7) The dialler will call the selected telephone number on the programmed channel and will repeat the basic message three times.
8) Repeat from step 6 for the other telephone numbers to be tested.
9) Press [ESC] repeatedly to exit from the menu.

```
UT01:MASTER
SYSTEM STATUS
```

```
UT01:MASTER
TEST
```

```
TEST
ADVANCED TESTS
```

```
ADVANCED
VOCAL CALL
```

```
VOCAL CALL
T01:xxxxxxxx
```

4.20.5 Alarm receiving centre call test

Proceed as follows to test that the numeric protocol calls work perfectly:

1) Enter **< Master / Installer code >**, press [OK] and then [MENU].
2) Press [▼] repeatedly until TEST appears.
3) Press [OK] and press [▼] repeatedly until ADVANCED TESTS appears.
4) Press [OK] and press [▼] repeatedly until PROTOCOL CALL appears.
5) Press [OK].
6) Press [▼] and [▲] to select the programmed telephone number for numeric code or modem calls to be called. Press [OK] to confirm.
7) The dialler will call the alarm receiving centre and send the parameter corresponding to the test call for correctly identifying the event.
8) Repeat from step 6 for the other telephone numbers to be tested.
9) Press [ESC] repeatedly to exit from the menu.

```
UT01:MASTER
SYSTEM STATUS
```

```
UT01:MASTER
TEST
```

```
TEST
ADVANCED TESTS
```

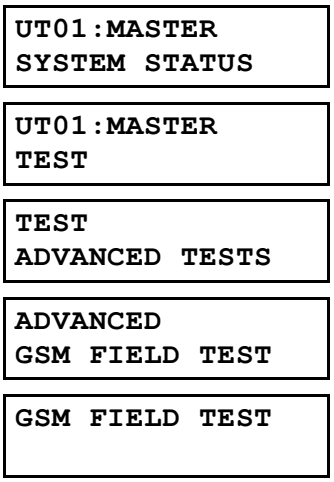
```
ADVANCED
PROTOCOL CALL
```

```
PROTOCOL CALL
T01:xxxxxxxx
```

4.20.6 GSM Field Test

Proceed as follows to test the GSM network signal level:

1) Enter **< Master / Installer code >**, press [OK] and then [MENU].
2) Press [▼] repeatedly until TEST appears.
3) Press [OK] and press [▼] repeatedly until ADVANCED TESTS appears.
4) Press [OK] and press [▼] repeatedly until GSM FIELD TEST appears.
5) Press [OK].
6) The keypad will beep during the GSM signal level test. The level of the GSM signal will appear in graphic form at the end of the test.
7) Press [ESC] repeatedly to exit from the menu.



4.20.7 Environmental listening test

It is advisable to test that this function works correctly if a KP500DV/N vocal keypad is installed in the system.
To do so, call from a telephone located outside the monitored area and follow the procedure described in paragraph *6.4 Remote control with guided voice menu* and following.

After having activated the function, check that the signal level is good in the entire area to be monitored. Otherwise, it may be necessary to install other vocal keypads to cover the areas in which the signal is not sufficient.

4.20.8 Final tests

Carry out the following checks in addition to the tests listed above:

- Arm and disarm (total and partial) the system from the keypads using all the programmed user codes.
- Arm and disarm the system using readers and/or KP500DP/N keypads, if present, using all the available keys.
- Test the remote functions of the system (if a dialler is installed) from a landline, a mobile phone or via modem (external assistance may be needed).

4.21 USER TRAINING

After having ascertained that the burglar alarm system is working perfectly, you can demonstrate the operations to be carried out on the system to the end users.

Proceed as follows to obtain the best training results:

- Directly involve all the people who will be using the system, if possible: training only one person is not a good idea because this person could forget something or may not be able to convey the information correctly to others.
- Perform an operation (e.g. arm and disarm the system) and then invite everyone to repeat the procedure personally while you are watching. You will be able to help if needed in this way.
- Prompt everyone to ask any questions: the fewer doubts users have, the more easily they will be able to operate the system.

The main instructions to be provided to users are:

- How to arm and disarm the system totally
- How to arm and disarm the system partially
- How to recognise the various indications: burglar, tamper attempt, flat battery etc. (on display and auditory indications)
- How to read the events stored on the control panel (events log)
- How to enable remote control (if applicable)
- How to test the system periodically.

Delete the Diagnose Log at the end of the test to hand over a clean system. See paragraph *9.9.3 How to delete the Diagnose Log* for instructions on how to delete.

5 - SYSTEM COMMISSIONING

This chapter illustrates how to arm and disarm the system totally or partially using the keypads and the electronic and proximity keys.

It also illustrates how to clear alarm indications and how to use the direct function keys (fire, emergency, silent panic).

IMPORTANT! Users and keys must have been previously acquired, configured and enabled as explained in the applicable paragraphs of this manual and in the *User Manual* to arm and disarm the system and to clear the alarms.

5.1 ARMING PROCEDURE

The alarm system has various arming modes, some of which are not EN50131 compliant.

EN50131 compliant modes are: arming from keypad, arming with electronic or proximity key, arming by timed programmer or arming from a specialised input using a mechanical key.

The following modes are not EN50131 compliant: remote arming, arming using GSM and DTMF commands, arming using a remote control.

The authorisation codes which must be used with keypads are described in paragraph *2.1 System access codes*.

It is possible to arm the entire system, only some partitions or one or more areas, if the latter are programmed. Areas allow operating on a subset of partitions at the same time without needing to select them each time.

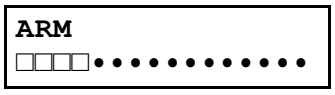
The user or key must have been assigned to the partition or area during programming in order to operate it.

5.2 ARMING FROM KP500D/N AND KP500DV/N KEYPADS

5.2.1 Total arming (system with partitions only)

Proceed as follows to arm the entire alarm system if no areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code >** and press [ON *].



2) The keypad will beep. Press [ESC] to exit without arming. The status LED will light up after 5 seconds (fixed if all partitions are armed, blinking if some partitions are not armed). Press [ON *] again if you do not want to wait for 5 seconds.

3) If programmed or if the system is EN50131 grade 3 compliant, the keypad will sound long beeps initially followed by short beeps for the last 10 seconds.
4) The display will go back to standard view automatically after one minute. Press [ESC] to go to standard display immediately.

IMPORTANT! The user will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.2.2 Total arming (system with areas and partitions)

Proceed as follows to arm the entire alarm system if areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code >** and press [ON *].

2) Enter [1] or [2 ABC] on the keypad. The procedure will continue as for partitions only if you press [2 ABC]. If you press [1]:

3) The keypad will beep. Press [ESC] to exit without arming. The status LED will light up after 5 seconds (fixed if all partitions or areas are armed, blinking if some partitions or areas are not armed) and all the areas will appear on the display. Press [ON *] again if you do not want to wait for 5 seconds.

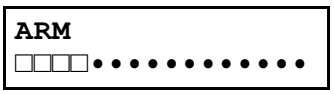
4) If programmed or if the system is EN50131 compliant, the keypad will sound long beeps initially followed by short beeps for the last 10 seconds.
5) The display will go back to standard view automatically after one minute. Press [ESC] to go to standard display immediately.

IMPORTANT! The user will arm only the assigned areas and not necessarily all the areas even with this procedure.

5.2.3 Partial arming (system with partitions only)

Proceed as follows to arm the alarm system partially if no areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code >** and press [ON *].



2) The keypad will beep. Press [ESC] to exit without arming.
3) Enter the number of the partitions to be armed on the keypad: the respective squares will turn black.

IMPORTANT! Simply enter the number directly if nine or fewer partitions have been programmed. If more than nine partitions have been programmed, always enter two digits to select the partitions, including for numbers from 1 to 9 (1 = 01, 2 = 02 etc.).

4) The status LED will light up after 5 seconds (fixed if all partitions are armed, blinking if some partitions are not armed). Press [ON *] again if you do not want to wait for 5 seconds.
5) If programmed or if the system is EN50131 compliant, the keypad will sound long beeps initially followed by short beeps for the last 10 seconds.
6) The display will go back to standard view automatically after one minute. Press [ESC] to go to standard display immediately.

IMPORTANT! The user will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.2.4 Partial arming (system with areas and partitions)

Proceed as follows to arm the entire alarm system if areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code >** and press [ON *].

2) Enter [1] or [2 ABC] on the keypad. The procedure will continue as for partitions only if you press [2 ABC]. If you press [1]:

3) The keypad will beep. Press [ESC] to exit without arming.
4) Enter the number of the partitions to be armed on the keypad: the respective squares will turn black.
5) The status LED will light up after 5 seconds (fixed if all areas are armed, blinking if some areas are not armed) and all the areas will appear on the display. Press [ON *] again if you do not want to wait for 5 seconds.
6) If programmed or if the system is EN50131 compliant, the keypad will sound long beeps initially followed by short beeps for the last 10 seconds.
7) The display will go back to standard view automatically after one minute. Press [ESC] to go to standard display immediately.

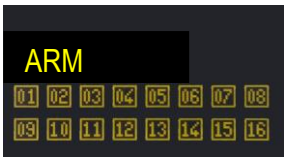
IMPORTANT! The user will arm only the assigned areas and not necessarily all the areas even with this procedure.

5.3 ARMING FROM KP500DP/N KEYPAD – KP500D/ST

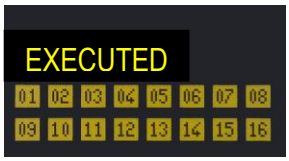
5.3.1 Total arming (system with partitions only)

Proceed as follows to arm the entire alarm system if no areas are defined:

1) Enter < Master / User code > and press ON



2) The keypad will beep. Press ESC to exit without arming. The status LED will light up after 5 seconds (fixed if all partitions are armed, blinking if only some partitions are armed). The square will appear full indicating the partitions which have been armed. The following will appear on the display:



3) Press ON again if you do not want to wait for 5 seconds.

4) The display will go back to standard view automatically after one minute. Press ESC to go to standard display immediately.

5) If programmed or if the system is EN50131 compliant, the keypad will sound long beeps initially followed by short beeps for the last 10 seconds.

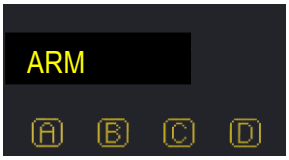
IMPORTANT! The user will arm only the assigned areas and not necessarily all the areas even with this procedure.

5.3.2 Total arming (system with areas and partitions)

Proceed as follows to arm the entire alarm system if areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code >** and press ON.

2) Press **F1** for areas or **F4** for partitions. Press **F1** (i.e. areas) on the display. An empty square will appear for each programmed area which is not armed assigned to the keypad and code. Full squares indicate that the area is armed. Half-full squares indicate that the area is only partially armed.

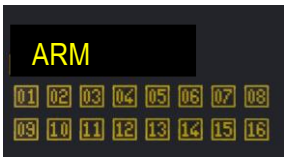


3) The keypad will beep. Press ESC to exit without arming. The status LED will light up after 5 seconds (fixed if all areas are armed, blinking if some areas are not armed). The squares will appear full indicating the areas which are not armed. The following will appear on the display:

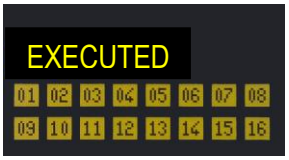
4) Press ON again if you do not want to wait for 5 seconds.

IMPORTANT! The user will arm only the assigned areas and not necessarily all the areas even with this procedure.

5) If **F4** (i.e. partitions) was pressed instead, an empty square will appear on the display for each programmed partition which is not armed assigned to keypad and code. Full squares indicate that the partition is armed. Octagons (e.g. 12) indicate that the partition is disarmed and some inputs are open.



6) The keypad will beep. Press ESC to exit without arming. The status LED will light up after 5 seconds (fixed if all partitions are armed, blinking if only some partitions are armed). The square will appear full indicating the partitions which have been armed. The following will appear on the display:



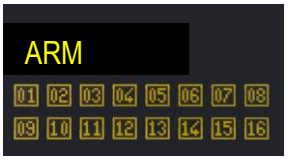
7) The display will go back to standard view automatically after one minute after arming both areas and partitions. Press ESC to go to standard display immediately.

8) For arming both areas and partitions, if programmed or if the system is EN50131 compliant, the keypad will sound long beeps initially followed by short beeps for the last 10 seconds.

5.3.3 Partial arming (system with partitions only)

Proceed as follows to arm the entire alarm system partially if no areas are defined:

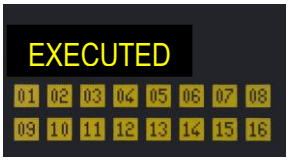
1) Enter **<Master / User / Installer / Technical Manager code >** and press ON *.



2) The keypad will beep. Press ESC to exit without arming.
3) Enter the number of the partitions to be armed on the keypad: the respective squares will become full.

IMPORTANT! Simply enter the number directly if nine or fewer partitions have been programmed. If more than nine partitions have been programmed, always enter two digits including for numbers from 1 to 9 (1 = 01, 2 = 02 etc.).

4) The status LED will light up after 5 seconds (fixed if all partitions are armed, blinking if only some partitions are armed). The square will appear full indicating the partitions which have been armed. The following will appear on the display:



IMPORTANT! The user will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

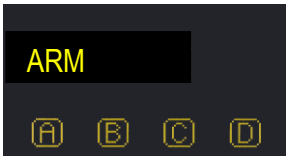
5) The display will go back to standard view automatically after one minute. Press ESC to go to standard display immediately.
6) If programmed or if the system is EN50131 compliant, the keypad will sound long beeps initially followed by short beeps for the last 10 seconds.

5.3.4 Partial arming (system with areas and partitions)

Proceed as follows to arm the entire alarm system partially if areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code >** and press ON *.

2) Press **F1** for areas or **F4** for partitions. Press **F1** (i.e. areas) on the display. An empty square will appear for each programmed area which is not armed assigned to the keypad and code. Full squares indicate that the area is armed. Half-full squares indicate that the area is only partially armed.

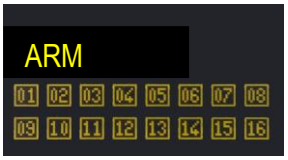


3) The keypad will beep. Press ESC to exit without arming.
4) Press the function keys (**F1**, **F2**, **F3** and **F4**) positioned under the areas to be armed: the respective squares of the areas will become full.
5) The status LED will light up after 5 seconds (fixed if all areas are armed, blinking if some areas are not armed). The following will appear on the display:

6) Press ON * again if you do not want to wait for 5 seconds.

IMPORTANT! The user will arm only the assigned areas and not necessarily all the areas even with this procedure.

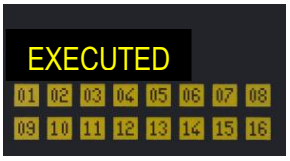
7) If **F4** (i.e. partitions) was pressed at the beginning of the procedure, an empty square will appear on the display for each programmed partition assigned to keypad and code which is not armed. Full squares indicate that the partition is armed. Circles indicate that the partition is disarmed and has open inputs.



8) The keypad will beep. Press ESC to exit without arming.
9) Enter the number of the partitions to be armed on the keypad: the respective squares will become full.

IMPORTANT! Simply enter the number directly if nine or fewer partitions have been programmed. If more than nine partitions have been programmed, always enter two digits including for numbers from 1 to 9 (1 = 01, 2 = 02 etc.).

10) The status LED will light up after 5 seconds (fixed if all partitions are armed, blinking if only some partitions are armed). The square will appear full indicating the partitions which have been armed. The following will appear on the display:



IMPORTANT! The user will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

11) The display will go back to standard view automatically after one minute after arming both areas and partitions. Press ESC to go to standard display immediately.

12) For arming both areas and partitions, if programmed or if the system is EN50131 grade 3 compliant, the keypad will sound long beeps initially followed by short beeps for the last 10 seconds.

5.4 ARMING WITH ELECTRONIC OR PROXIMITY KEY

5.4.1 Total arming from electronic key reader

IMPORTANT! This procedure can only be used if all partitions are disarmed.

5.4.1.1 System in use mode = Mode 3 (EN50131 grade 3 compliant)

Proceed as follows to arm all partitions assigned to the reader and to the key using the electronic key:

1. Insert the electronic key in the reader. The red LED will blink to indicate that the key is being read and the green LED will light up after a few instants to indicate that the key was recognised. All the green LEDs will blink rapidly if the key is not recognised.
2. The green LEDs corresponding to the armed partitions, if any, will appear if the key is recognised. The red LED will keep blinking.
3. Extract the key.
4. Insert the electronic key again when the red LED switches off.
5. Extract the electronic key when the red LED starts blinking.
6. The green LEDs will blink for a few seconds and the partitions associated to the reader and to the key will be armed.

IMPORTANT! The key will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.4.1.2 System in use mode = Mode 2 or Mode 0

Proceed as follows to arm all partitions assigned to the reader and to the key using the electronic key:

1. Insert the electronic key in the reader when all the green LEDs are off (the procedure will disarm the partitions if any LEDs are green). The red LED will blink to indicate that the key is being read. All the green LEDs will blink rapidly if the key is not recognised.
2. Extract the electronic key when the red LED starts blinking.
3. The green LEDs indicate the status of the partitions assigned to the reader. *LED on fixed* = partition armed, *LED off* = the key is not assigned to the partition and cannot arm it.

IMPORTANT! The key will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.4.2 Total arming from proximity key reader

IMPORTANT! This procedure can only be used if all partitions are disarmed.

5.4.2.1 System in use mode = Mode 3 (EN50131 grade 3 compliant)

Proceed as follows to arm all partitions assigned to the reader and to the key using the proximity key:

1. Approach the proximity key to the transponder. The red LED will blink to indicate that the key is being read and the green LED will light up after a few instants to indicate that the key was recognised. All the green LEDs will blink rapidly if the key is not recognised.
2. The green LEDs corresponding to the armed partitions, if any, will appear if the key is recognised. The red LED will keep blinking.
3. Move the key away.
4. Approach the proximity key again when the red LED switches off.
5. Move away the proximity key when the red LED starts blinking.
6. The green LEDs will blink for a few seconds and the partitions associated to the reader and to the key will be armed.

IMPORTANT! The key will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.4.2.2 System in use mode = Mode 2 or Mode 0

Proceed as follows to arm all partitions assigned to the reader and to the key using the proximity key:

1. Approach the proximity key in the reader when all the green LEDs are off (the procedure will disarm the partitions if any LEDs are green). The red LED will blink to indicate that the key is being read. All the green LEDs will blink rapidly if the key is not recognised.
2. Move away the proximity key when the red LED starts blinking.
3. The green LEDs indicate the status of the partitions assigned to the reader. *LED on fixed* = partition armed, *LED off* = the key is not assigned to the partition and cannot arm it.

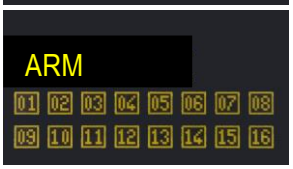
IMPORTANT! The key will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.4.3 Total arming from KP500DP/N keypad

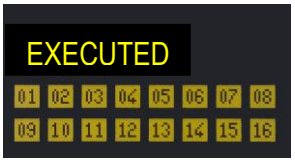
Proceed as follows to arm all partitions using the proximity key on a KP500DP/N keypad:

1) Approach the proximity key to the keypad transponder.

2) The keypad will beep. Press ESC to exit without arming.



3) The status LED will light up after 5 seconds (fixed if all partitions are armed, blinking if only some partitions are armed). The square will appear full indicating the partitions which have been armed. The following will appear on the display:



4) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

IMPORTANT! The key will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

IMPORTANT! The LED **H** (see *Figure 3 - KP500DP/N - KP500D*/ST keypad) will light up and the buzzer will sound to indicate an error (long beep) if a key which can be not been acquired (the key is not recognised) or which has not been enabled is used.

5.4.4 Partial arming from electronic key reader

5.4.4.1 System in use mode = Mode 3 (EN50131 grade 3 compliant)

Proceed as follows to arm only the partitions assigned to the reader and to the key using the electronic key:

1. Insert the electronic key in the reader. The red LED will blink to indicate that the key is being read and the green LED will light up after a few instants to indicate that the key was recognised. All the green LEDs will blink rapidly if the key is not recognised.
2. The green LEDs corresponding to the armed partitions, if any, will appear if the key is recognised. The red LED will keep blinking.
3. Extract the key.
4. Insert the electronic key again when the red LED switches off.
5. The red LED will blink and after a few seconds a cycle will start during which the green LEDs blink for a few seconds showing the various combinations of partitions in sequence.
6. Extract the electronic key when the combination of partitions to be armed is displayed by the LEDs. The possibility of arming each partition depends on the programming of the reader and on the key used.
7. The chosen partitions will be armed and the green LEDs will indicate the status of the partitions assigned to the reader for a few seconds.

IMPORTANT! The key will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.4.4.2 System in use mode = Mode 2 or Mode 0

Proceed as follows to arm only the partitions assigned to the reader and to the key using the electronic key:

1. Insert the electronic key in the reader when all the green LEDs are off (the procedure will arm the partitions if any LEDs are green during the first cycle). The red LED will blink to indicate that the key is being read. All the green LEDs will blink rapidly if the key is not recognised.
2. The red LED will blink and after a few seconds a cycle will start during which the green LEDs blink for a few seconds showing the various combinations in sequence.
3. Extract the electronic key when the combination of partitions to be armed is displayed by the LEDs. The possibility of arming each partition depends on the programming of the reader and on the key used.
4. The green LEDs indicate the status of the partitions assigned to the reader. *LED on fixed* = partition(s) armed, *LED off* = partition disarmed.

IMPORTANT! The key will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.4.5 Partial arming from proximity key reader

5.4.5.1 System in use mode = Mode 3 (EN50131 grade 3 compliant)

Proceed as follows to arm only the partitions assigned to the reader and to the key using the proximity key:

1. Approach the proximity key to the transponder. The red LED will blink to indicate that the key is being read and the green LED will light up after a few instants to indicate that the key was recognised. All the green LEDs will blink rapidly if the key is not recognised.
2. The green LEDs corresponding to the armed partitions, if any, will appear if the key is recognised. The red LED will keep blinking.
3. Move the proximity key away.
4. Approach the proximity key again when the red LED switches off.
5. The red LED will blink and after a few seconds a cycle will start during which the green LEDs blink for a few seconds showing the various combinations of partitions in sequence.
6. Move the proximity key away when the combination of partitions to be armed is displayed by the LEDs. The possibility of arming each partition depends on the programming of the reader and on the key used.
7. The chosen partitions will be armed and the green LEDs will indicate the status of the partitions assigned to the reader for a few seconds.

IMPORTANT! The key will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.4.5.2 System in use mode = Mode 2

Proceed as follows to arm only the partitions assigned to the reader and to the key using the proximity key:

1. Approach the proximity key to the transponder and hold it close for at least three seconds. The red LED will blink to indicate that the key is being read. Move it away when the four green LEDs blink.
2. A cycle will be started during which the green LEDs blink for a few seconds showing the various combinations in sequence. The possibility of arming each partition depends on the programming of the reader and on the key used.
3. When the combination of partitions to be armed is displayed by the LEDs, approach the proximity key to the transponder again, wait for an instant and then move it away.
4. The green LEDs will indicate the status of the partitions assigned to the reader for a few seconds: *LED on fixed* = partition(s) armed, *LED off* = partition disarmed.

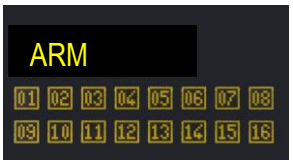
IMPORTANT! The key will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.4.6 Partial arming from KP500DP/N keypad

Proceed as follows to arm the partitions partially using the proximity key on a KP500DP/N keypad:

1) Approach the proximity key to the keypad transponder.

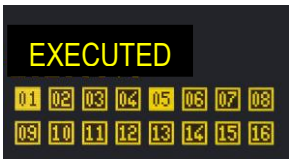
2) The keypad will beep. Press **F4** within 5 seconds. Press ESC to exit without arming.



3) Enter the number of the partitions to be armed on the keypad: the respective squares will become full.

IMPORTANT! Simply enter the number directly if nine or fewer partitions have been programmed. If more than nine partitions have been programmed, always enter two digits to select the partitions, including for numbers from 1 to 9 (1 = 01, 2 = 02 etc.).

4) The status LED will light up after 5 seconds. The following will appear on the display:



IMPORTANT! The user will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

5) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

IMPORTANT! The key will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

IMPORTANT! The LED **H** (see *Figure 3 - KP500DP/N - KP500D/ST keypad*)) will light up and the buzzer will sound to indicate an error (long beep) if a key which can be not been acquired (the key is not recognised) or which has not been enabled is used.

5.5 ARMING USING RC500 REMOTE CONTROL

EN50131

5.5.1 Total arming

The remote control must have been duly programmed for all partitions to arm all the partitions in the system.

Press the on the remote control to arm all partitions. The remote control buzzer will beep if the control panel acknowledges the command.

Note: The system can be armed/disarmed also by using the (toggle) key. Importantly, this key works as follows:

1. Pressing the key will cause the system status to switch from disarmed to armed and vice versa (toggle).
2. If the system is partially armed (partial arming), pressing the key will cause the system to be armed completely: any partitions which are disarmed will be armed.
3. Pressing the key again will cause the system to be totally disarmed (the entire system, not only the armed partitions).

5.5.2 Partial arming

The partial arming of only some partitions in the system is possible only if the remote control is duly programmed to do so.

Press on the remote control to arm the partitions to which the remote control is assigned. The remote control buzzer will beep if the control panel acknowledges the command.

Note: The some partitions assigned to the remote control can be armed/disarmed also by using the (toggle) key. Importantly, this key works as follows:

1. Pressing the key will cause the partition status to switch from disarmed to armed and vice versa (toggle).
2. If the partitions assigned to the remote control are partially armed (partial arming), pressing the key will arm all partitions: any partitions which are disarmed will be armed.
3. Pressing the key again will cause the partitions to be totally disarmed (not only the previously armed partitions).

5.6 DISARMING PROCEDURE

The arm system may be disarmed in various manners, some of which are not EN50131 compliant.

EN50131 compliant modes are: disarming from keypad, disarming with electronic or proximity key, disarming by timed programmer or disarming from a specialised input using a mechanical key.

Remote disarming, disarming by GSM and DTMF commands and disarming by remote control are not EN50131 compliant.

The authorisation codes which must be used with keypads are described in paragraph *2.1 System access codes*.

It is possible to disarm the entire system, only some partitions or one or more areas, if these are programmed. Areas allow operating on a subset of partitions at the same time without needing to select them each time.

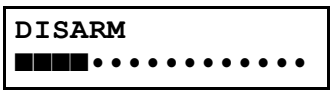
The user or key must have been assigned to the partition or area during programming in order to operate it.

5.7 DISARMING FROM KP500D/N AND KP500DV/N KEYPADS

5.7.1 Total disarming (system with partitions only)

Proceed as follows to disarm the entire alarm system if no areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code>** OFF.



2) The keypad will beep. Press ESC to exit without disarming. The status LED will switch off after 5 seconds and the following will appear on the display

3) Press OFF again if you do not want to wait for 5 seconds.
4) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

IMPORTANT! The user will disarm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.7.2 Total disarming (system with areas and partitions)

Proceed as follows to disarm the entire alarm system if areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code>** OFF.

2) Enter 1 or 2 ABC on the keypad. The procedure will continue as for partitions only if you press 2 ABC.
   If you press 1:

3) The keypad will beep. Press ESC to exit without disarming. The status LED will switch off after 5 seconds and the following will appear on the display

4) Press OFF again if you do not want to wait for 5 seconds.
5) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

IMPORTANT! The user will disarm only the assigned areas and not necessarily all the areas even with this procedure.

5.7.3 Partial disarming (system with partitions only)

Proceed as follows to disarm the alarm system partially if no areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code>** OFF.

2) The keypad will beep. Press ESC to exit without disarming.
3) Enter the number of the partitions to be disarmed on the keypad: the respective squares will appear empty.

IMPORTANT! Simply enter the number directly if nine or fewer partitions have been programmed. If more than nine partitions have been programmed, always enter two digits to select the partitions, including for numbers from 1 to 9 (1 = 01, 2 = 02 etc.).

4) The status LED will switch off after 5 seconds and the following will appear on the display

5) Press OFF if you do not want to wait for 5 seconds.
6) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

IMPORTANT! The user will disarm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.7.4 Partial disarming (system with areas and partitions)

Proceed as follows to disarm the alarm system partially if areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code>** OFF.

2) Enter 1 or 2 ABC on the keypad. The procedure will continue as for partitions only if you press 2 ABC.
   If you press 1:

3) The keypad will beep. Press ESC to exit without disarming.
4) Enter the number of the areas to be disarmed on the keypad: the respective squares will appear empty.
5) The status LED will switch off after 5 seconds and the following will appear on the display.

6) Press OFF if you do not want to wait for 5 seconds.
7) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

IMPORTANT! The user will disarm only the assigned areas and not necessarily all the areas even with this procedure.

5.7.5 Disarming from keypad under hol-up

On MP500/4N, MP500/8 and MP500/16 control panels, starting from control panel SW version 1.01, if the hold-up function has been enabled (see paragraph 2.1.4 *How to enable the hold-up function*) and you are threatened and forced by a criminal with the risk of life then, you can disarm the burglar system while arming the hold-up alarm simultaneously which will make the dialer sending the programmed alarm messages without activating the siren sound.

To disarm the system when your are under coercion, just increase your user code of one digit. For example if your user code is 000021 you need only to enter 000022; if user code is 29 enter 30, if it is 39 enter 40, etc.

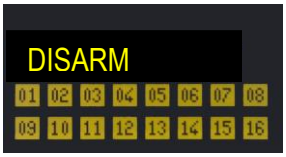
IMPORTANT! Enabling the hold-up function will cancel EN50131 compliance.

5.8 DISARMING FROM KP500DP/N - KP500D/ST KEYPAD

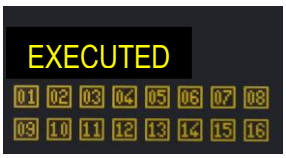
5.8.1 Total disarming (system with partitions only)

Proceed as follows to disarm the entire alarm system if no areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code >** and press OFF.



2) The keypad will beep. Press ESC to exit without disarming. After 5 seconds, the status LED will switch off and the squares will become empty indicating that the partitions have been disarmed. The following will appear on the display:



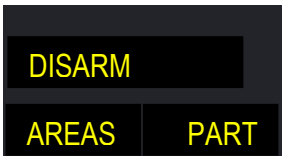
3) Press OFF again if you do not want to wait for 5 seconds.

4) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

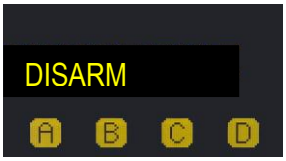
5.8.2 Total disarming (system with areas and partitions)

Proceed as follows to arm the entire alarm system if areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code >** and press OFF.



2) Press **F1** for areas or **F4** for partitions. Press **F1** (i.e. areas) on the display. An empty square will appear for each programmed area which is not armed assigned to the keypad and code. Full squares indicate that the area is armed. Half-full squares indicate that the area is only partially armed.

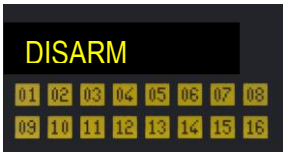


3) The keypad will beep. Press ESC to exit without disarming. After 5 seconds, the status LED will switch off and the squares will become empty indicating that the areas have been disarmed. Any half-full squares indicate that the area is partially armed. The following will appear on the display:

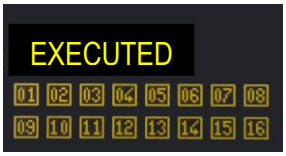
4) Press OFF if you do not want to wait for 5 seconds.

IMPORTANT! The user will disarm only the assigned areas and not necessarily all the areas even with this procedure.

5) If **F4** (i.e. partitions) was pressed instead, the following will appear on the display:



6) The keypad will beep. Press ESC to exit without disarming. After 5 seconds, the status LED will switch off and the squares will become empty indicating that the partitions have been disarmed. The following will appear on the display:



7) Press OFF # again if you do not want to wait for 5 seconds.

8) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

5.8.3 Partial disarming (system with partitions only)

Proceed as follows to arm the entire alarm system partially if no areas are defined:

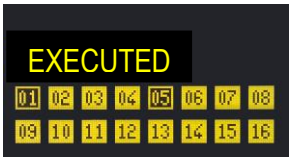
1) Enter **<Master / User / Installer / Technical Manager code >** and press OFF #.

2) The keypad will beep. Press ESC to exit without disarming. The following will appear on the display:

3) Enter the number of the partitions to be disarmed on the keypad: the respective squares will become empty.

IMPORTANT! Simply enter the number directly if nine or fewer partitions have been programmed. If more than nine partitions have been programmed, always enter two digits to select the partitions, including for numbers from 1 to 9 (1 = 01, 2 = 02 etc.).

4) After 5 seconds, the LED will switch off and the squares will become empty indicating that the partitions have been disarmed. The following will appear on the display:



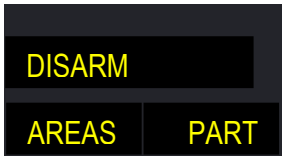
5) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

IMPORTANT! The user will disarm only the assigned partitions and not necessarily all the partitions even with this procedure.

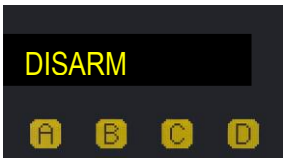
5.8.4 Partial disarming (system with areas and partitions)

Proceed as follows to arm the entire alarm system if areas are defined:

1) Enter **<Master / User / Installer / Technical Manager code >** and press OFF.

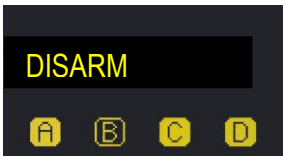


2) Press **F1** for areas or **F4** for partitions. Press **F1** (i.e. areas) on the display. An empty square will appear for each programmed area which is not armed assigned to the keypad and code. Full squares indicate that the area is armed. Half-full squares indicate that the area is only partially armed.



3) The keypad will beep. Press ESC to exit without disarming.

4) Press the function keys (**F1**, **F2**, **F3** and **F4**) positioned under the areas to be disarmed:

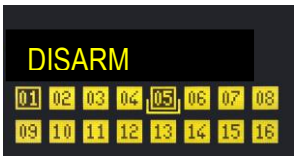


5) After 5 seconds, the status LED will switch off and the squares will become empty indicating that the areas have been disarmed. The following will appear on the display:

6) Press OFF if you do not want to wait for 5 seconds.

IMPORTANT! The user will disarm only the assigned areas and not necessarily all the areas even with this procedure.

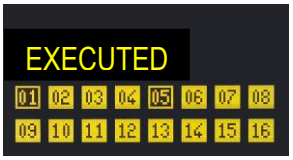
7) If **F4** was pressed, the following will appear on the display:



8) Enter the number of the partitions to be disarmed on the keypad: the respective squares will become empty.

IMPORTANT! Simply enter the number directly if nine or fewer partitions have been programmed. If more than nine partitions have been programmed, always enter two digits to select the partitions, including for numbers from 1 to 9 (1 = 01, 2 = 02 etc.).

9) After 5 seconds, the status LED will switch off and the squares will become empty indicating that the partitions have been disarmed. The following will appear on the display:



10) Press OFF if you do not want to wait for 5 seconds.

11) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

IMPORTANT! The user will disarm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.8.5 Disarming from keypad under hold-up

On MP500/4N, MP500/8 and MP500/16 control panels, starting from control panel SW version 1.01, if the hold-up function has been enabled (see paragraph 2.1.4 *How to enable the hold-up function*) and you are threatened and forced by a criminal with the risk of life then, you can disarm the burglar system while arming the hold-up alarm simultaneously which will make the dialer sending the programmed alarm messages without activating the siren sound.

To disarm the system when your are under coercion, just increase your user code of one digit. For example if your user code is 000021 you need only to enter 000022; if user code is 29 enter 30, if it is 39 enter 40, etc.

IMPORTANT! Enabling the hold-up function will cancel EN50131 compliance.

5.9 DISARMING WITH ELECTRONIC OR PROXIMITY KEY

5.9.1 Total disarming from electronic key reader

5.9.1.1 System in use mode = Mode 3 (EN50131 grade 3 compliant)

Proceed as follows to disarm all partitions assigned to the reader and to the key using the electronic key:

1. Insert the electronic key in the reader. The red LED will blink to indicate that the key is being read and the green LED will light up after a few instants to indicate that the key was recognised. All the green LEDs will blink rapidly if the key is not recognised.
2. The green LEDs corresponding to the armed partitions, if any, will appear if the key is recognised. The red LED will keep blinking.
3. Extract the key.
4. Insert the electronic key again after a few instants.
5. Extract the electronic key when the red LED starts blinking.
6. The green LEDs will go out. A LED will stay on to indicate that the key is not assigned to the partition. The possibility of disarming each partition depends on the programming of the reader and on the key used.

IMPORTANT! The key will disarm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.9.1.2 System in use mode = Mode 2 or Mode 0

Proceed as follows to disarm all partitions assigned to the reader and to the key using the electronic key:

1. Insert the electronic key in the reader. The red LED will blink to indicate that the key is being read. All the green LEDs will blink rapidly if the key is not recognised.
2. Extract the electronic key when the red LED starts blinking.
3. The green LEDs indicate the status of the partitions assigned to the reader. *LED off* = partition disarmed, *LED on* = key not assigned to the partition. The possibility of disarming each partition depends on the programming of the reader and on the key used.

IMPORTANT! The key will disarm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.9.2 Total disarming from proximity key reader

5.9.2.1 System in use mode = Mode 3 (EN50131 grade 3 compliant)

Proceed as follows to disarm all partitions assigned to the reader and to the key using the proximity key:

1. Approach the proximity key to the transponder. The red LED will blink to indicate that the key is being read and the green LED will light up after a few instants to indicate that the key was recognised. All the green LEDs will blink rapidly if the key is not recognised.
2. The green LEDs corresponding to any armed partitions will light up if the key is recognised (the procedure will disarm the partitions if any green LEDs are on). The red LED will keep blinking.
3. Move the key away.
4. Approach the proximity key again when the red LED switches off.
5. Move away the proximity key when the red LED starts blinking.
6. The green LEDs will indicate the status of the partitions assigned to the reader for a few seconds: *LED off* = partition disarmed, *LED on* = key not assigned to the partition. The possibility of disarming each partition depends on the programming of the reader and on the key used.

IMPORTANT! The key will disarm only the assigned areas and not necessarily all the areas even with this procedure.

5.9.2.2 System in use mode = Mode 2

Proceed as follows to disarm all partitions assigned to the reader and to the key using the proximity key:

1. Approach the proximity key to the transponder. The red LED will blink to indicate that the key is being read. All the green LEDs will blink rapidly if the key is not recognised.
2. Move away the proximity key from the transponder when the red LED starts blinking.
3. The green LEDs indicate the status of the partitions assigned to the reader. *LED off* = partition disarmed, *LED on* = key not assigned to the partition. The possibility of disarming each partition depends on the programming of the reader and on the key used.

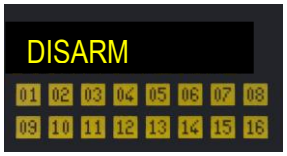
IMPORTANT! The key will disarm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.9.3 Total disarming from KP500DP/N keypad

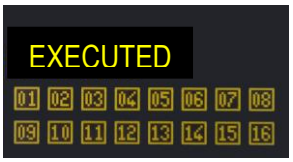
Proceed as follows to disarm all partitions using the proximity key on a KP500DP/N keypad:

1) Approach the proximity key to the proximity key reader.

2) The keypad will beep. Press ESC to exit without disarming.



3) After 5 seconds, the status LED will switch off and the squares will become empty indicating that the partitions have been disarmed. The following will appear on the display:



IMPORTANT! The key will disarm only the assigned partitions and not necessarily all the partitions even with this procedure.

IMPORTANT! The LED **H** (see *Figure 3 - KP500DP/N - KP500D*/ST keypad) will light up and the buzzer will sound to indicate an error (long beep) if a key which can be not been acquired (the key is not recognised) or which has not been enabled is used.

5.9.4 Partial disarming from electronic key reader

Follow the same procedure used for partial arming from electronic key reader to partially disarm the system from an electronic key reader.

5.9.5 Partial disarming from proximity key reader

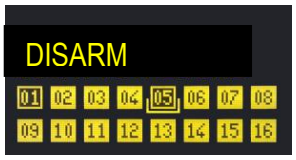
Follow the same procedure used for partial disarming from proximity key reader to partially disarm the system with a proximity key reader.

5.9.6 Partial disarming from KP500DP/N keypad

Proceed as follows to disarm some partitions using the proximity key on a KP500DP/N keypad:

1) Approach the proximity key to the keypad.

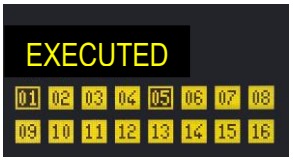
2) The keypad will beep. Press ESC to exit without disarming.



3) Enter the number of the partitions to be disarmed on the keypad.

IMPORTANT! Simply enter the number directly if nine or fewer partitions have been programmed. If more than nine partitions have been programmed, always enter two digits to select the partitions, including for numbers from 1 to 9 (1 = 01, 2 = 02 etc.).

4) After 5 seconds, the status LED will switch off and the squares will become empty indicating that the partitions have been disarmed. The following will appear on the display:



5) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

IMPORTANT! The key will disarm only the assigned partitions and not necessarily all the partitions even with this procedure.

IMPORTANT! The LED **H** (see *Figure 3 - KP500DP/N - KP500D*/ST keypad) will light up and the buzzer will sound to indicate an error (long beep) if a key which can be not been acquired (the key is not recognised) or which has not been enabled is used.

5.10 DISARMING USING RC500 REMOTE CONTROL

EN50131

5.10.1 Total system disarming

The remote control must have been duly programmed to disarm all the partitions in the system (see Programming Manual).

Press to disarm the entire system using the remote control. The remote control buzzer will beep if the control panel acknowledges the command.

5.10.2 Partial disarming with remote control

The remote control must have been duly programmed to partially disarm some the partitions in the system (see Programming Manual).

Press on the remote control to disarm the partitions to which the remote control is assigned. The remote control buzzer will beep if the control panel acknowledges the command.

5.11 SPLITTING

A splitting procedure which is carried out by means of the keypad can be used to arm and disarm the burglar alarm system partitions in addition to the procedures described above.

A particularity of the splitting method is that it allows to arm and disarm the partitions in the same way without needing to use two different procedures.

Proceed as follows to change the status of one or more partitions in the system:

1) Enter **<Master / User / Installer / Technical Manager code>**, press [OK] and then [MENU].
2) Press [OK]. The empty squares indicate a disarmed partition, the full squares indicate an armed partition.
3) Press [<] and [>] to point to the concerned partition. The selected partition will appear on the first line of the display.
4) Press [^] and [v] to change the partition status.
5) After having made the selections, press [OK] to confirm or press [ESC] to cancel.
6) The display will go back to standard view automatically after one minute. Press [ESC] to switch the view sooner.

```
UT02:...
SYSTEM STATUS
```

```
SE01:
□■□□□••••••••••••
```

IMPORTANT! The user will arm and disarm only the assigned partitions and not necessarily all the partitions even with this procedure.

5.12 DIRECT ACCESS FUNCTION KEYS

EN50131 NOT RELATED

Three pre-programmed keys are provided on the keypads for directly activating the fire, emergency and silent panic indications.

Their position and shape are keypad-specific but the icons are the same:

= fire = emergency = silent panic

5.12.1 KP500D/N and KP500DV/N keypads

Hold [1] (fire), [4 GHI] (emergency) or [7 PQRS] (silent panic) pressed for at least three seconds: the control panel will generate the respective event without needing to enter any code. Each key must be enabled.

The environmental listening function can be activated automatically at the end of the emergency call on KP500DV/N keypads if they are duly programmed to do so.

5.12.2 KP500DP/N - KP500D/ST keypad

Hold **F1** (silent panic), **F2** (emergency) or **F3** (fire) pressed for at least three seconds: the control panel will generate the respective event without needing to enter any code. Each key must be enabled.

5.12.3 RC500 remote control programming key

EN50131

During programming, the "**+**" key on the remote control may be configured to activate or deactivate a specific output to access one of the following technological functions (fire, emergency, panic, silent panic) directly. Hold the "**+**" key pressed for at least five seconds to generate the respective event.

5.13 HOW TO STOP ALARMS IN PROGRESS

The procedure for stopping an alarm is shown in detail in paragraph 7.2 *Description of ALARMS AND indications*.

It is important to remember that:

- Entering a valid code on a keypad will stop most alarms.
- The vocal alarm call cycle can be stopped by dialling “12” on the telephone which received the call after hearing the message and the beep (a DTMF tone keypad is needed for this).
- For emergency vocal calls, "12" can be dialled after having closed the environmental listening session at the end of the emergency vocal message repetition.
- The vocal alarm call cycle can also be stopped by entering a valid code on the system keypad within the first 30 seconds if the call delay function is enabled.

IMPORTANT! The system will not be EN50131 compliant if vocal only alarm calls are enabled.

IMPORTANT! Alarms calls made using numeric protocol and on ATS4 cannot be stopped.

IMPORTANT! The system will not be EN50131 compliant if alarm calling delay is enabled.

Vocal calls and text messages following burglar events may be interrupted also by disarming the partitions assigned to the telephone numbers programmed for the event. This function may be useful in case of false alarms, for instance.

It is important to note that a call to the first available telephone number cannot be stopped once it has started and will continue until the end of the attempts. No other calls will be made to the next numbers.

5.14 SYSTEM STATUS INFORMATION

Masking system status information is a mandatory requirement to be EN50131 grade 3 compliant.

Consequently, when Mode 3 (EN50131 grade 3 compliancy) is configured, system status (armed or disarmed) is not indicated directly by the LEDs, the keypad display or the electronic key and transponder reader LEDs. The system status may be checked by entering a valid code on the keypad or by using a valid electronic or proximity key (see the paragraphs on how to arm and disarm the system using a key for more information).

The system status masking method may be different on each keypad and single reader but it will suffice for one of these devices not to be masked to cancel compliance of the entire system.

This function is not available on MP500/4N control panel because these devices are EN50131 grade 2 compliant.

See chapter *1 - Control devices* for more information on system status visibility.

5.14.1 How to view system status

The system status is display by the LEDs provided on keypads and readers.

Each user can view the system status detail for the part assigned to them (only the partitions on which the user is authorised to operate will appear).

To view the system status:

1) Enter **<Master / User / Installer / Technical Manager code>**, press [OK] and then [MENU].

```
UT01:MASTER
SYSTEM STATUS
```

2) Press [OK]. The graphic systems corresponding to digits 1 to 16 appear on the second line of the screen. The meanings are:
   □ = the partition is disarmed
   0 = the partition is disarmed with one or more open inputs
   ■ = the partition is armed
   . = the partition was not programmed

```
SE01:...
□□0□■...
```

3) Press [<] and [>] to go from one partition to the next. The partition name will appear on the first line.
4) Press [ESC] repeatedly to exit the menu after examining the status.

```
    MP500/16
12/01/2014 10:10
```

IMPORTANT! Partition status can be displayed permanently instead of date and time, but this setting is not EN50131 grade 3 compliant and will declass the system.

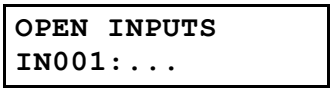
5.14.2 How to view open inputs

The presence of one or more open inputs is indicated by the specific LED on the keypad and by the reader LED (see chapter *1 - Control devices*). These LEDs also indicate the opening of isolated inputs.

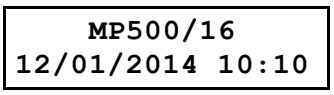
To view input addresses:

1) Enter **<Master / User / Installer / Technical Manager code>**, press OK twice and then press ▼ repeatedly until OPEN INPUTS appears.

2) Press OK. The inputs are identified as "<Logical address>:<Name>" on the second line. For example, an input to which the kitchen detector is connected with logical address "3" and named "Kitchen" will be identified as "In003:Kitchen".



3) Use ▼ and ▲ to scroll the list of open inputs.
4) Press ◄ and ► to see the input customisation.
5) Press ESC repeatedly to exit from the menu after examining the list.



5.14.3 How to view isolated or inhibited inputs

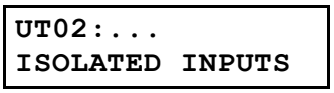
The presence of one or more isolated or inhibited inputs is indicated by the specific LED on the keypad and by the reader LED (see chapter *1 - Control devices*).

An input can only be isolated if it has been programmed as such.

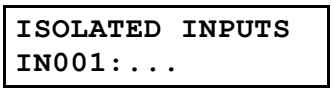
An input may be manually isolated by the installer or technical manager.

To view addresses of isolated inputs:

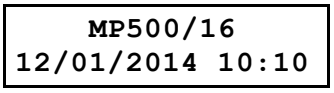
1) Enter **<Master / User / Installer / Technical Manager code>**, press OK twice and then press ▼ repeatedly until ISOLATED INPUTS appears.



2) Press OK. The inputs are identified as "<Logical address>:<Name>" on the second line. For example, an input to which the kitchen detector is connected with logical address "3" and named "Kitchen" will be identified as "In003:Kitchen".



3) Use ▼ and ▲ to scroll the list of open inputs.
4) Press ◄ and ► to see the input customisation.
5) Press ESC repeatedly to exit from the menu after examining the list.



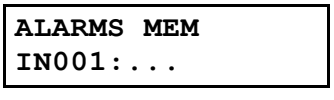
5.14.4 How to examine the Alarms Memory

Alarm events are indicated by the specific LEDs (on keypad and readers) and stored by the control panel. Details on the events can then be viewed on the keypad display.

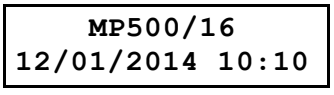
Proceed as follows to view details:

1) Enter **<Master / User / Installer / Technical Manager code>**, press OK twice and then press ▼ repeatedly until ALARMS MEM appears.

2) Press OK. The alarm LED will blink. The inputs are identified as "<Logical address>:<Name>" on the second line. For example, an input to which the kitchen detector is connected with logical address "3" and named "Kitchen" will be identified as "In003:Kitchen".



3) Use ▼ and ▲ to scroll the list of inputs which caused the alarm.
4) Press ◄ and ► to see the input customisation.
5) Press ESC repeatedly to exit from the menu after examining the list.

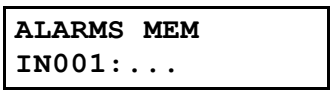


5.14.5 How to delete the Alarms Memory

Proceed as follows to delete the Alarms Memory:

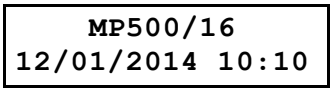
1) Enter **<Master / User / Installer / Technical Manager code>**, press OK twice and then press ▼ repeatedly until ALARMS MEM appears.

2) Press OK. The alarm LED will blink.



3) Use ▼ and ▲ to scroll the list of inputs which caused the alarm.
4) The following after examining the list:

5) Press OK to delete the Alarms Memory.
6) Press ESC repeatedly to exit from the menu.



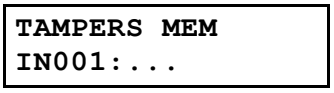
5.14.6 How to examine the Tampers Memory

Tamper events are indicated by the specific LEDs (on keypad and readers) and stored by the control panel. Details on the events can then be viewed on the keypad display.

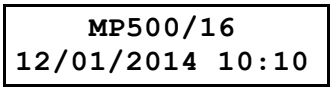
Proceed as follows to view details:

1) Enter **<Master / User / Installer / Technical Manager code>**, press OK twice and then press ▼ repeatedly until TAMPERS MEM appears.

2) Press OK. The tamper LED will blink. The inputs are identified as "<Logical address>:<Name>" on the second line. For example, an input to which the kitchen detector is connected with logical address "3" and named "Kitchen" will be identified as "In003:Kitchen".



3) Use ▼ and ▲ to scroll the list of inputs which triggered the tamper event.
4) Press ◄ and ► to see the input customisation.
5) Press ESC repeatedly to exit from the menu after examining the list.



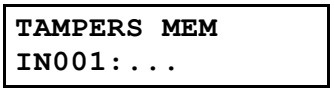
5.14.7 How to delete the Tampers Memory

The Tampers Memory must be deleted only by the Installer or by the Technical Manager.

Proceed as follows to delete the Tampers Memory:

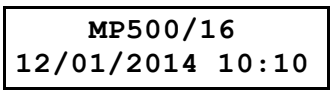
1) Enter **<Installer / Technical Manager code>**, press OK twice and then press ▼ repeatedly until TAMPERS MEM appears.

2) Press OK. The tamper LED will blink.



3) Use ▼ and ▲ to scroll the list of inputs which caused the alarm.
4) The following after examining the list:

5) Press OK to delete the Tampers Memory.
6) Press ESC repeatedly to exit from the menu.



IMPORTANT! A tamper event which is still present cannot be deleted.

5.14.8 How to examine the fault and anomaly memory

A fault, failure or anomaly (e.g. low or inefficient battery, telephone line fault, detector or siren fault) will be indicated by the specific LED on the keypad and the reader LED (see chapter *1 - Control devices*).

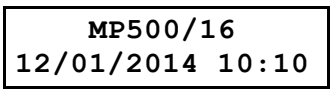
To examine the detected faults:

1) Enter **<Master / User / Installer / Technical Manager code>**, press OK twice.

2) Press OK. The fault LED will blink.

3) Use ▼ and ▲ to scroll the list of detected faults and anomalies.

4) Press ESC repeatedly to exit from the menu after examining the list.

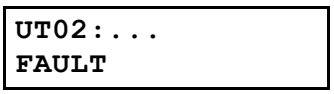


5.14.9 How to delete the fault memory

The fault memory deletion procedure is selective, i.e. depends on the entered access code because different codes have different resetting possibilities (Installer and Technical Manager can delete all memories, Master and User can only delete some memories).

How to delete the fault memory:

1) Enter **<Master / User / Installer / Technical Manager code>**, press OK twice.



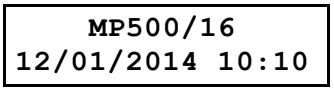
2) Press OK. The fault LED will blink.

3) Use ▼ and ▲ to scroll the list of faults.

4) The following after examining the list:

5) Press OK to delete the Tampers Memory.

6) Press ESC repeatedly to exit from the menu after examining the list.



6 - USER REMOTE CONTROL

6.1 HOW TO SKIP A TELEPHONE ANSWERING MACHINE

EN50131 NOT RELATED

The answering machine or fax must be set to pick up after at least two rings in order to be able to call the control panel for remote management on the PSTN line. The Answer Machine function of the control panel must be set to pick up after more rings that the answering machine.

The control panel can then be called for remote control as follows:

- Call the control panel and hang up after the first ring. The control panel will detect the incoming call without picking up because the number of rings is lower than the set number.
- Call the control panel back within 30 seconds.
- The control panel will immediately engage the line after the first ring without counting the number of programmed rings. In this manner, the telephone answering machine or fax will receive only one ring and will engage the line instead of the control panel.

This procedure is implemented automatically also by Remote Control Centres with Hi-Connect software and enabled function.

6.2 REMOTE CONTROL WITH TEXT MESSAGES

EN50131

Outputs programmed as “commandable” can be activated remotely by sending an SMS text message. The GSM answer machine and the "Incoming SMS" GSM parameter must be enabled to use this function. Furthermore, the text message must come from a known telephone number, i.e. one of the 12 telephone numbers stored on the control panel.

IMPORTANT! This number does not need to be associated to an event.

The text message to be sent to the telephone number of the SIM Card of the control panel must have the following syntax:

2nns.

where:

- **nn** is the logical number from 01 to 10 of the commandable output or commandable pulse to be switched
- **s** is a digit which represents the status that the output must assume: **1** (arm) or **0** (disarm). In case of pulsed commandable output only **1** (arm) can be used;
- **.** (full stop) is the end of the message.

Several controls can be queued in the same text message and separated by a comma. The text message must end with a full stop (“.”).

Any spaces will be ignored, but characters other than digits, spaces, commas and full stops will be considered errors. The text message will be rejected.

EXAMPLES

Text message	Description
2031.	Correct: this message will activate logical output 03
2 03 1.	Correct: this message will activate logical output 03
2031, 2050.	Correct: this message will activate logical output 03 and deactivate logical output 05
2031	Wrong: no full stop at the end of the message
2 3 1.	Wrong: the output number is not written using two digits
2031. 2050.	Partially correct: the first command will be executed, the second one will be rejected

The control panel will send a reply text message containing exclamation marks **“!!!”** followed by the received message to confirm command reception.

6.3 HOW TO ACTIVATE COMMANDABLE OUTPUTS AT NO COST

EN50131

Remote activations at no cost are possible if the control panel is provided with GSM module with a valid SIM Card and the GSM answer machine function is enabled.

This function uses the Caller ID of the calling telephones to activate programmable commandable outputs rapidly. During programming, a commandable output is assigned to a mobile telephone number stored on the control panel (one of those which are used to send alarms or other functions).

IMPORTANT! One telephone number may control multiple outputs. One output may be controlled by multiple telephone numbers.

The operating principle is:

1. Call the GSM number of the control panel from a registered telephone number.
2. Hang up within three rings to avoid charges.
3. All the assigned commandable outputs will be activated: the pulse outputs will be operated for approximately one second (e.g. to open the gate), the switchable or toggle commands will change state and remain active until they are deactivated by sending a command in a text message.
4. To confirm reception of the command, the control panel will call back the number which made the call for a few seconds. Do not reply to avoid changing the cost to the SIM Card of the control panel.

6.4 REMOTE CONTROL WITH GUIDED VOICE MENU

EN50131
NOT RELATED

The remote control call can be made from a landline with tone keypad (DTMF) or a mobile phone. The PSTN or GSM answer machine and remote disarming functions must be enabled to uses all functions (see *User Manual*).

IMPORTANT! Check that the telephone in use does not make anonymous calls because the control panel must be able to recognise the caller. Using a mobile phone, the function will allows to enable anonymous calls can be enabled in a specific menu. The menu is telephone-specific. The most common names are: *"Show ID"*, "*Show my number to"*, *"Show personal number"*. Check the settings in case of problems and try again.

Remote controls can be used to: arm partitions, disarm partitions, switch commandable outputs, activate environmental listening, isolate and include inputs, query system status.

The system status summary sends vocal messages related to: armed partitions, generic events present in the Event Log, no power indication, inefficient battery indication, SIM Card expiry.

No vocal message is generated if all partitions are disarmed and no event is present.

Wrong code or excluded input events are not managed even if stored in memory.

Proceed as follows for remote control:

1. Call the telephone number of the control panel from a landline or mobile phone.
2. Enter the Master code within 10 seconds on the keypad at the prompt. Enter a digit and wait for the confirmation beep before entering the next one. Enter "#" at the end of the digits.
3. You will hear a welcome message if the entered message is correct. Otherwise, try to enter the code again (up to three attempts).
4. After having been recognised you have a few seconds to enter the menu number (see*Table 12 - List of DTMF commands*) and access the required menu directly. Otherwise, follow the voice menu instructions to access and use the various functions.
5. Press " ***** " repeatedly to exit remote control.

IMPORTANT! In remote control mode, the ***** (asterisk) will go back to the previous menu.

6.5 LIST OF VOCAL ANSWER MACHINE DTMF CONTROLS

EN50131 NOT RELATED

Function	No. menu	Accepted digits	Action	Vocal messages
Arm Partitions	0	01 …16 followed by #	Arm all selected partitions	• List of partitions indicated in the command. • Arming result: ▭ EXECUTED ▭ NOT EXECUTED
		#	Arm all configured partitions (total arming)	
Disarm partitions	1	01 …16 followed by #	Disarm all selected partitions	• List of partitions indicated in the command. • Disarming result: ▭ DISARMED
		#	Disarm all configured partitions (total disarming)	
Remote controls Outputs Commandable	2	"01"-"10"	Select output on which to apply the remote control	• Current status output message • Output command result
		0 - 1	Output command (0 = disarm, 1 = arm)	
		1	Pulsed output command (1 = arm)	
Environment listening from vocal keypads	3	1 – 8 (configured keypad address)	Activate environmental listening on selected vocal keypad.	No message
		0	Switch between: "environmental listening" and "Vocal action"	
Exclude Include Inputs	4	"001"-"128"	Select the logical input number to be excluded/included (inputs which can be excluded only)	• Exclusion result • Inclusion result
		1	Exclude input	
		0	Include input	
GSM return call (GSM only)	5			Goodbye message and end of communication. The control panel will call the number in modem mode if type A return call is enabled and at least one GSM modem number is programmed.
System status summary	9		List: Partition status, stored events/notices, faults present	• Currently armed partition messages • Stored event type/notice messages • Present fault messages

Table 12 - List of DTMF commands

Examples

Key sequences	Result
0 #	Total system arming
1 0 2 0 5 0 7 #	Disarm partitions 2, 5 and 7
0 0 3 * 2 0 6 1 #	Arm partition 3 and activate commandable output 6

6.6 ENVIRONMENTAL LISTENING

EN50131 NOT RELATED

You can listen to environmental noises in the place where the vocal keypad is installed on a telephone. If there are several vocal keypads in the alarm system you can select which one to listen from each time.

The environmental listening function will remain active for approximately one minute and a half and will then be automatically interrupted. Press " ***** " to interrupt listening in advance.

Furthermore, you can speak through the keypad speaker. Communication is one-way (you can either speak or listen), but you can switch between speaking and listening whenever you want by pressing the "0" key on the telephone.

7 - ALARMS, EVENTS AND INDICATIONS

This chapter contains a detailed description of the alarms, events and indications managed by MP500/xx control panels.

7.1 ALARM AND EVENT INDICATIONS

The following table contains a summary of the various indications (LEDs, outputs, messages, memory records) which are activated in case of alarm or when an event occurs. The following paragraphs contain a detailed description of what an alarm or event implies.

7.1.1 How to use the table

The control panel may record and indicate an occurrence (i.e. an alarm, an indication or an event) in many ways. The indication or message is provided to allow to determine the causes.

Proceed as follows in case of indication on the keypad LED or the red LED of the key reader or if a telephone message is received:

1) Search for the indication or message in the corresponding columns of the table.
2) Read the reason for the indication or message in the "Cause" column on the same line. An indication or message may sometimes have several causes. In the latter case, it could be useful to read the description shown in the Event Log or in the Diagnose Log.

The following abbreviations may be used in the Event Log and in the Diagnose Log:

- **In** or **IN** identifies an input
- **KP** identifies a keypad
- **DD** identifies another type of device.

The supplementary auxiliary indications can set up during system installation by connecting indicating devices (warning lights, blinkers, bells, buzzers etc.) to outputs specifically programmed to be activated when a given event occurs.

7.1.1.1 Example of how to interpret the table

The LED ⚠ may light up for several different reasons. Read the Event Log or Diagnose Log (see paragraphs *9.8 Event Log* and *9.9 Diagnose Log*) to determine the cause of the indication more in detail.

For example, the message LOW BATTERY CONTROL PANEL means that the control panel battery is not completely flat.

Then, go to section *7.2 Description of ALARMS AND indications* and paragraph 7.2.18 *Control panel and other device low battery alarm* which contains a detailed explanation of what happened and what could happen.

The "Description of the event" column shows the message which appears on the first screen page on the first line and the message which appears on the second screen page on the second line.

Cause	LED		Log	Memory	Description of the event (Event Log and Diagnose Log)	Auxiliary indication (controlled output)	Telephone message EN50131 NOT RELATED
	Keypad	Reader					
Burglar alarm (immediate, delayed, delayed way, last exit)	🔊	■	■	■	Inxxx:name IN customisation	Burglar	Burglar alarm
Burglar pre-alarm	🔊	■	■	■	Inxxx:name IN customisation	Burglar	Burglar alarm
Panic indication from input / function key / remote control	🔊	■	■	■	“KP xx”	Panic	Panic
Fire indication from input / function key / remote control	🔊	■	■	■	“KP xx”	Fire	Fire alarm
Emergency indication from input / function key / remote control	🔊	■	■	■	“KP xx”	Emergency	Emergency request
Silent panic indication from input / function key / remote control			■	■	“KP xx”	Silent panic	Panic
Technological input / output 1 activation		■	■	■	Inxxx:name TECHNOL. TYPE 1	Technological 1	Technological service 1
Technological input / output 2 activation		■	■	■	Inxxx:name TECHNOL. TYPE 2	Technological 2	Technological service 2
Technological input / output 3 activation		■	■	■	Inxxx:name TECHNOL. TYPE 3	Technological 3	Technological service 3
Low battery	⚠				LOW BATTERY Control panel or device	Low battery	Battery fault/restored

Cause	LED		Log	Memory	Description of the event (Event Log and Diagnose Log)	Auxiliary indication (controlled output)	Telephone message EN50131 NOT RELATED
	Keypad	Reader					
Detector fault input alarm				■	Inxxx:name DETECTOR FAILURE	Detector fault	Anomaly
Siren failure input alarm		■		■	Inxxx:name SIREN FAILURE	System failure	Anomaly
Fault input alarm		■		■	Inxxx:name FAILURE	Failure	Anomaly
Jamming fault input alarm		■		■	Inxxx:name JAMMING	Detector fault	Anomaly
External communicator fault input alarm		■		■	Inxxx:name COM. FAULT	Telephone fault	Anomaly
Other faults				■		System failure	Failure
No communication with device on bus		■		■	BUS COMM.FAILURE BUS device (DDxx:name)	Sys fault	System tamper
Isolated inputs			■		Inxxx:name	Isolated inputs	Excluded input
Inhibited inputs (temporarily during arming)			■		INHIBIT	Isolated inputs	Excluded input
After having entered 21 wrong codes			■	■	WRONG CODE device (DDxx:name)	Tamper	
Tamper or SAB input indicating tampering		■		■	device (DDxx:name)	Tamper	System tamper
Balanced input imbalance		■		■	Inxxx:name IN customisation	Tamper	System tamper
Radio jamming		■		■	JAMMING device (DDxx:name)	Tamper	Radio tamper
No wireless device supervision		■		■	SUPERVISION device (DDxx:name)	Tamper	Radio tamper
Enter menu with installer code			■				
Open input		■			Inxxx:name IN customisation	Open input	
Test input opening			■	■	Inxxx:name INPUT OF TEST	Open input	
PO warning / arm partitions / enable-disable user or key / enable-disable output			■			PO warning	
Instantaneous lack of power	*				POWER INSTANT. (START/END)		
"Lack of power" after programmed timeout	*			■	POWER (START/END)	Lack of power	Power mains fault/restored
Arm/disarm partitions			■		EXECUTED or PARTIALLY DONE	Partition status	Armed Partition xx Disarmed partition xx
Override partition arming			■		SETT. OVERRIDDEN	Partition status	
System block, no mains power, battery not OK					ARREST SYSTEM		
Enter valid code on KPxx keypad			■		VALID CODE		
Edit date-time on KPxx keypad			■		Date Time + KPxx: name		
Enable/disable code			■		Start user enabling + KPxx: name		
Arm partition command not executed			■		NOT EXECUTED		Arming not executed
Hold-up alarm			■		ALARM HOLD-UP	Hold-up	Attack in progress
Inhibit tamper input					INHIB. TAMPER IN TAMPER IN		
IDP call from PSTN module (with positive result)					IDP-OK		
IDP call from PSTN module (with negative result)					IDP-KO		

* The LED will go from fixed to blinking in case of “Instantaneous lack of power” and will continue to blink until the power is restored in case of “Lack of power after programmed timeout”.

Table 13 - Indication overview

7.2 DESCRIPTION OF ALARMS AND INDICATIONS

7.2.1 Burglar alarm

This alarm is generated in case of burglar attempts. The control panels can manage one burglar alarm per partition, to which output actuators, such as sirens, can correspond.

The burglar inputs generate an alarm when the programmed conditions are respected: break-in detected by one or more devices, one or more detections, according to a given route etc.

The "Alarm Count" function determines a maximum number of alarms which can be caused by a detector during one day and as long as the respective partition is armed.

IMPORTANT! On MP500/8 and MP500/16 control panels the “Alarm Count” function is activated and configured to comply with EN50131 grade 3 requirements by default. Changing this configuration may cancel EN50131 grade 3 compliance of the system.

This is generated when...	• A burglar input is opened and at least one partition associated to it with OR function is armed. • A burglar input is opened and all partitions associated to it with AND function are armed.
It activates...	• The programmed burglar outputs which have at least one partition in common with the input which generated the event. • The dialler to send the respective burglar alarm message (if programmed) in form of numeric code, vocal call, text message or modem communication.
It is stored...	• In the Event Log and the Diagnose Log. • In the Alarms Memory.
It is indicated...	• On keypads which have at least one partition in common with the input. • On readers which have at least one partition in common with the input.
It lasts	• For the burglar/tamper/panic alarm time.
It is stopped by...	• Entering a valid code on the keypad which has at least one partition in common with the input which generated the event. • Inserting a valid key which has at least one partition in common with the input which generated the event. • Imparting a disarm partition command from key input which has at least one partition in common with the input which generated the event. • Imparting a disarm partition command from vocal menu. • Imparting a disarm command from remote control which has at least one partition in common with the input which generated the event.

7.2.2 Burglar pre-alarm

The burglar pre-alarm function can be used in the system, for example, to sound a buzzer whenever the detectors of an external area, e.g. a yard, detect the presence of a person.

This is generated when...	• A pre-alarm input is opened and at least one partition associated to it with OR function is armed. • A pre-alarm input is opened and all partitions associated to it with AND function are armed.
It activates...	• The programmed pre-alarm outputs which have at least one partition in common with the input which generated the event. • The dialler to send the respective pre-alarm message (if programmed) in form of numeric code, vocal call, text message or modem communication.
It is stored...	• In the Event Log and the Diagnose Log. • In the temporary Alarms Memory.
It is indicated...	• On keypads which have at least one partition in common with the input. • On readers which have at least one partition in common with the input.
It lasts...	• For the pre-alarm time.
It is stopped by...	• Entering a valid code on the keypad which has at least one partition in common with the input which generated the event. • Inserting a valid key which has at least one partition in common with the input which generated the event. • Imparting a disarm partition command from key input which has at least one partition in common with the input which generated the event. • Imparting a disarm command from remote control which has at least one partition in common with the input which generated the event.

7.2.3 Tamper alarm

This alarm is generated if someone attempts to tamper with the system. It is always active (H24), but can be temporarily deactivated by setting the system to maintenance status. See Installation Manual for how to connect a siren, if needed.

This is generated when...	• A tamper input is opened (control panel, keypad or wireless devices, such as DC, IR, sirens). • The SAB line of the control panel or expansion modules is opened or imbalanced. • A double balance input is imbalanced (short-circuit or wire cutting). • A programmed tamper input is opened. • A wireless device does not reply to its expansion module for longer than a pre-selected configuration time (monitoring function). • A wireless device outside the system either occupies or interferes with the radio bandwidth of the expansion module (jamming). The alarm is generated regardless of partition status (H24).
It activates...	• The programmed tamper outputs which have at least one armed partition in common (in case of double balanced inputs). In the other cases, it switches the tamper outputs of the armed partitions. • The dialler to send the respective tamper alarm message (if programmed) in form of numeric code, vocal call, text message or modem communication.
It is stored...	• In the Diagnose Log. • In the Tampers Memory.
It is indicated...	• On keypads. • On readers.
It lasts...	• For the burglar/tamper/panic alarm time.
It is stopped by...	• Entering a valid code on a keypad. • Inserting a valid key. • Imparting a disarm partition command from the key input. • Imparting a disarm command from a remote control which has at least one partition in common with the input which generated the event.

7.2.4 Wrong code alarm

This alarm is generated in case of trial-and-error attempts to identify a valid code for disarming the system. It is always active (H24), but can be temporarily deactivated by setting the system to maintenance status.

This is generated when...	• A wrong code is entered 21 consecutive times (the counter is reset when a valid code is entered). The alarm is generated regardless of partition status (H24).
It activates...	• The programmed tamper outputs which have at least one armed partition in common with the keypad where the wrong code was entered. • The dialler to send the respective wrong code alarm message (if programmed) in form of numeric code or modem communication.
It is stored...	• In the Diagnose Log. • In the Tampers Memory.
It is indicated...	• On keypads which have at least one partition in common with the one where the wrong code was entered. • On readers which have at least one partition in common with the one where the wrong code was entered.
It is stopped by...	• Entering a valid code on a keypad. • Inserting a valid key. • Imparting a disarm partition command from the key input. • Imparting a disarm command from a remote control which has at least one partition in common with the input which generated the event.

7.2.5 Panic indication

This indication can be triggered by the user in case of danger. It is always active (H24), but can be temporarily deactivated by setting the system to maintenance status.

This is generated when...	• A panic input is opened. • The "**+**" function key on the remote control is held pressed for at least 5 seconds (if programmed). The alarm is generated regardless of partition status (H24).
It activates...	• The programmed panic outputs which have at least one partition in common with the input which generated the event. • The dialler to send the respective panic alarm message (if programmed) in form of numeric code, vocal call or modem communication.
It is stored...	• In the Event Log and the Diagnose Log. • In the Alarms Memory.
It is indicated...	• On keypads which have at least one partition in common with the input. • On readers which have at least one partition in common with the input.
It lasts...	• For the burglar/tamper/panic alarm time.
It is stopped by...	• Entering a valid code on a keypad. • Inserting a valid key. • Imparting a disarm partition command from the key input. • Imparting a disarm command from a remote control which has at least one partition in common with the input which generated the event.

7.2.6 Silent panic indication

This indication can be triggered by the user in case of danger if the user does not want to attract the attention of the assailant. It is always active (H24), but can be temporarily deactivated by setting the system to maintenance status.

This is generated when...	• A silent panic input is opened. • The silent panic function key is held pressed for at least three seconds. • The "**+**" function key on the remote control is held pressed for at least 5 seconds (if programmed). The alarm is generated regardless of partition status (H24).
It activates...	• The programmed silent panic outputs with at least one partition in common with the input which generated the event or with the keypad on which the dedicated key was pressed. • The dialler to send the respective panic alarm message (if programmed) in form of numeric code, vocal call or modem communication.
It is stored...	• In the Event Log and the Diagnose Log. • In the Alarms Memory.
It lasts...	• For the burglar/tamper/panic alarm time.
It is stopped by...	• Entering a valid code on a keypad. • Inserting a valid key. • Imparting a disarm partition command from the key input. • Imparting a disarm command from a remote control which has at least one partition in common with the input which generated the event.

7.2.7 Hold-up indication

This is an indication that the user can trip when forced by an assailant to disarm the system. It is always active (H24), but can be temporarily deactivated by setting the system to maintenance status.

This is generated when...	• A hold-up input is opened. • hold-up user code is entered The alarm is generated regardless of partition status (H24).
It activates...	• The programmed hold-up outputs which have at least one partition in common with the input or with the entered access code. • The dialler to send the respective hold-up in progress alarm message (if programmed) in form of numeric code, vocal call or modem communication.
It is stored...	• In the Event Log and the Diagnose Log.
It lasts...	• For a fixed time of 30 seconds.
It is stopped by...	• Entering a valid code on a keypad which has at least one partition in common. • Inserting a valid key which has at least one partition in common. • Imparting a disarm partition command from the key input. • Imparting a disarm command from remote control which has at least one partition in common.

7.2.8 Emergency indication

The MP500/8 and MP500/16 control panels offer an auxiliary function (not compliant with standards in force) which can be used to generate requests for help.

IMPORTANT! A remote control system compliant with the standards in force must be provided to use the emergency call function.

This is generated when...	• An emergency input is opened. • An "absence of move" input is not opened meaning that no motion was detected for a given time (at least one opening every 12 hours). • The key associated to the emergency function is held pressed on the keypad for longer than three seconds. • The "**+**" function key on the remote control is held pressed for at least 5 seconds (if programmed). The alarm is generated regardless of partition status (H24).
It activates...	• The programmed emergency outputs with at least one partition in common with the input which generated the event or with the keypad on which the dedicated key was pressed. • The dialler to send the respective emergency message (if programmed) in form of numeric code, vocal call or modem communication. Environmental listening is activated automatically at the end of the vocal message.
It is stored...	• In the Event Log and the Diagnose Log. • In the Alarms Memory.
It is indicated...	• On keypads which have at least one partition in common with the input or keypad which generated the event. • On readers which have at least one partition in common with the input or keypad which generated the event.
It lasts...	• For the emergency alarm time.
It is stopped by...	• Entering a valid code on a keypad which has at least one partition in common. • Inserting a valid key which has at least one partition in common. • Imparting a disarm command from key input which has at least one partition in common. • Imparting a disarm command from a remote control which has at least one partition in common with the input which generated the event.

7.2.9 Fire indication

The control panels offer an auxiliary function (not compliant with standards in force) which can be used to manage fire detectors (smoke detectors, buttons etc.) and connect them to appropriately programmed inputs to generate "fire alarm" type indications.

IMPORTANT! See the Elkron general catalogue, Fire Alarm section, to make a system which fully complies with standards in force.

This is generated when...	• A fire input is opened. • The key associated to the fire alarm function is held pressed on the keypad for longer than three seconds. • The "**+**" function key on the remote control is held pressed for at least 5 seconds (if programmed). The alarm is generated regardless of partition status (H24).
It activates...	• The programmed fire alarm outputs with at least one partition in common with the input which generated the event or with the keypad on which the dedicated key was pressed. • The dialler to send the respective fire alarm message (if programmed) in form of numeric code, vocal call, text message or modem communication.
It is stored...	• In the Event Log and the Diagnose Log. • In the Alarms Memory.
It is indicated...	• On keypads which have at least one partition in common with the input or keypad which generated the event. • On readers which have at least one partition in common with the input or keypad which generated the event.
It lasts...	• For until a reset fire alarm input is opened which has at least one partition in common with the fire input which was triggered or using the keypad which generated the alarm.

7.2.10 Detector jamming alarm

Monitoring of devices provided with fault output can be implemented in combination on control panels.

This is generated when...	• If one or more customised jamming inputs are open.
It activates...	• The programmed detector fault outputs which have at least one partition in common with the input which generated the event (with partition armed). • The dialler to send the respective alarm message (if programmed) in form of numeric code, vocal call or modem communication.
It is stored...	• In the Diagnose Log and in the fault and anomaly memory.
It is indicated...	• On fault LED of keypads which have at least one partition in common with the input which generated the event. • On readers which have at least one partition in common with the input which generated the event.
After having solved the problem, the control panel...	• Stores end of fault in the Diagnose Log. • Deactivates the programmed fault detector outputs.

7.2.11 Detector fault alarm

Monitoring of devices provided with fault output can be implemented in combination on control panels.

This is generated when...	• If one or more customised detector fault inputs are open.
It activates...	• The programmed detector fault outputs which have at least one partition in common with the input which generated the event (with partition armed). • The dialler to send the respective alarm message (if programmed) in form of numeric code, vocal call or modem communication.
It is stored...	• In the Diagnose Log and in the fault and anomaly memory.
It is indicated...	• On fault LED of keypads which have at least one partition in common with the input which generated the event. • On readers which have at least one partition in common with the input which generated the event.
After having solved the problem, the control panel...	• Stores end of fault in the Diagnose Log. • Deactivates the programmed fault detector outputs.

7.2.12 Faulty siren alarm

Monitoring of devices provided with fault output can be implemented in combination on control panels.

This is generated when...	• One or more customised siren fault inputs are open.
It activates...	• The programmed system fault outputs which have at least one partition in common with the input which generated the event. • The dialler to send the respective alarm message (if programmed) in form of numeric code, vocal call or modem communication.
It is stored...	• In the Diagnose Log and in the fault and anomaly memory.
It is indicated...	• On fault LED of keypads which have at least one partition in common with the input which generated the event. • On readers which have at least one partition in common with the input which generated the event.
After having solved the problem, the control panel...	• Stores end of fault in the Diagnose Log. • Deactivates the programmed failure outputs.

7.2.13 Failure alarm from failure input

Monitoring of devices provided with fault output can be implemented in combination on control panels.

This is generated when...	• A programmed failure input is opened. The alarm is generated regardless of partition status (H24).
It activates...	• The programmed failure outputs which have at least one partition in common with the input which generated the event. • The dialler to send the respective alarm message (if programmed) in form of numeric code, vocal call, text message or modem communication.
It is stored...	• In the Event Log and the Diagnose Log. • In the faults and anomalies list.
It is indicated...	• On fault LED of keypads which have at least one partition in common with the input which generated the event. • On readers which have at least one partition in common with the input which generated the event.
It is stopped by...	• Closing the programmed failure input again.
After having solved the problem, the control panel...	• Activates the dialler to send the respective failure alarm message (if programmed) in form of numeric code, vocal call, text message or modem communication. • Stores the end of failure in the Event Log and in the Diagnose Log. • Deactivates the programmed failure outputs.

7.2.14 System failure alarm

This is generated when...	• An anomaly concerning the system power occurs. • An anomaly concerning the battery charging circuit occurs. • An anomaly concerning the sirens occurs. • An anomaly concerning the supplementary power supply occurs. The alarm is generated regardless of partition status (H24).
It activates...	• The programmed system failure outputs. • The dialler to send the respective alarm message (if programmed) in form of numeric code, vocal call or modem communication.
It is stored...	• In the Diagnose Log and in the fault and anomaly memory.
It is indicated...	• On The yellow fault LED on the keypads.
It is stopped by...	• Solving the problem.
After having solved the problem, the control panel...	• Stores end of fault in the Diagnose Log. • Activates the dialler to send the respective end of failure alarm message (if programmed) in form of numeric code, vocal call or modem communication. • Deactivates the programmed system failure outputs.

7.2.15 External communicator failure alarm

This is generated when...	• An external communicator failure input is opened. The alarm is generated regardless of partition status (H24).
It activates...	• The programmed communicator failure outputs. • The dialler to send the respective alarm message (if programmed) in form of numeric code, vocal call or modem communication.
It is stored...	• In the Diagnose Log and in the fault and anomaly memory.
It is indicated...	• On The yellow fault LED on the keypads. • On The red LED of the readers.
It is stopped by...	• Solving the problem.
After having solved the problem, the control panel...	• Stores end of fault in the Diagnose Log. • Activates the dialler to send the respective end of failure alarm message (if programmed) in form of numeric code, vocal call or modem communication. • Deactivates the programmed tel. failure outputs.

7.2.16 No Bus communication alarm

This is generated when...	• One or more bus devices are not communicating. The alarm is generated regardless of partition status (H24).
It activates...	• The programmed Tamper outputs. • The dialler to send the respective alarm message (if programmed) in form of numeric code, vocal call or modem communication.
It is stored...	• In the Diagnose Log and in the In the Diagnose Log and in the Tampers memory.
It is indicated...	• On the red tampers LED on the keypads. • On the red LED of the readers.
It is stopped by...	• Solving the problem.
After having solved the problem, the control panel...	• Stores end anomaly/tamper in the Diagnose Log. • Activates the dialler to send the respective end of anomaly/tamper alarm message (if programmed) in form of numeric code, vocal call or modem communication. • Deactivates the programmed Tamper outputs.

7.2.17 Protracted no mains power alarm

This is generated when...	• There is no mains power for a time equal to or higher than the programmed “Lack of power time”. The alarm is generated regardless of partition status (H24).
It activates...	• The programmed "lack of power" outputs. • The dialler to send the respective "lack of power" alarm message (if programmed) in form of numeric code, vocal call or modem communication.
It is stored...	• In the Diagnose Log.
It is indicated...	• On The green LED on keypads. • On The red LED on readers.
It is stopped by...	• Mains power being restored for at least 5 consecutive minutes.
Five minutes after mains power is re-established, the control panel...	• Stores end of no power event in the Diagnose Log. • Activates the dialler to send the respective burglar alarm message (if programmed) in form of numeric code, vocal call or modem communication. • Deactivates the programmed "lack of power" outputs.

7.2.18 Control panel and other device low battery alarm

This is generated when...	• The battery of the control panel or other devices is recognised as inefficient or missing. The alarm is generated regardless of partition status (H24).
It activates...	• The programmed low battery outputs. • The dialler to send the respective low battery alarm message (if programmed) in form of numeric code, vocal call or modem communication.
It is stored...	• In the Diagnose Log and in the fault and anomaly memory.
It is indicated...	• On The yellow failure LED on the keypads. • On The red LED on the readers.
When the battery charge is restored, the control panel...	• Stores end of low battery event in the Diagnose Log. • Deactivates the programmed low battery outputs. • Activates the dialler to send the respective burglar alarm message (if programmed) in form of numeric code, vocal call or modem communication.

7.3 DESCRIPTION OF EVENTS

An event is a voluntary or involuntary occurrence managed by control panels to send indications, store conditions or control implementations.

The indication of an event may precede an alarm indication, like a no mains power event.

The event types and their distinctive features are illustrated below.

7.3.1 Reset fire alarm event

This is generated when...	• A reset fire alarm input is opened.
It activates...	• The programmed reset fire alarm outputs which have at least one partition in common with the input which generated the event for one second.
It is stored...	• In the Diagnose Log.
In addition…	• Ends the respective fire indication. • Resets the fire alarm indication in the temporary memory. • Switches off the LED on the keypads and on the readers on which the alarm was indicated.

IMPORTANT! In case of fire alarm indication and manual resetting, restore the environmental conditions in the room where the alarm occurred and check that the detector is armed again to be able to detect a new danger situation.

7.3.2 Technological type 1 event

The MP500/4N, MP500/8 and MP500/16 control panels allow to manage some home automation functions (turning on the heating, managing the garden sprinkler system etc.) using technological events (type 1, 2 and 3), the door opener event and the courtesy light event.

The technological events are always active (H24), while the door opener event is only active when the partitions are disarmed.

This is generated when...	• A technological type 1 input is opened.
It activates...	• The programmed technological type 1 outputs which have at least one partition in common with the input which generated the event. • The dialler to send the respective technological alarm message (if programmed) in form of numeric code, vocal call, text message or modem communication.
It is stored...	• In the Event Log and the Diagnose Log.
It lasts...	• For Until at least one of the programmed technological type 1 input with at least one partition in common with the output remains open.

7.3.3 Technological type 2 event

This is generated when...	• A technological type 2 input is opened.
It activates...	• The programmed technological type 2 outputs which have at least one partition in common with the input which generated the event. • The dialler to send the respective technological alarm message (if programmed) in form of numeric code, vocal call, text message or modem communication.
It is stored...	• In the Event Log and the Diagnose Log.
It lasts...	• For 1 second

7.3.4 Technological type 3 event

This is generated when...	• A technological type 3 input is opened.
It activates...	• The programmed technological type 3 outputs which have at least one partition in common with the input which generated the event. • The dialler to send the respective technological alarm message (if programmed) in form of numeric code, vocal call, text message or modem communication.
It is stored...	• In the Event Log and the Diagnose Log.
It lasts...	• For Until a valid code is entered on the keypad and all the inputs programmed as technological type 3 which have at least one partition in common have returned to rest condition.

7.3.5 Door opener event

This is generated when...	• A burglar input belonging to one or more partitions on which the ancillary door opener function was enabled is opened. All partitions assigned to the input must be disarmed. • A key programmed as “access control” associated to one or more partitions is inserted. All partitions assigned to the key must be disarmed.
It activates...	• The programmed door opener outputs associated to at least one partition by the input or the key.
It is stored...	• In the Event Log and in the Diagnose Log only in case of actuation caused by a key.
It lasts...	• For Approximately 2 seconds.

7.3.6 Courtesy light event

This is generated when...	• A burglar input belonging to one or more partitions on which the ancillary courtesy light function was enabled is opened.
It activates...	• The programmed courtesy light outputs associated to at least one partition of the input.
It lasts...	• For Approximately 3 minutes.

7.3.7 Instantaneous no mains power event

This is generated when...	• There is no mains power for a time shorter than the programmed “Lack of power time”. The event is generated regardless of partition status (H24).
It is stored...	• In the Event Log and the Diagnose Log.
It is indicated...	• On By the green power LED blinking on the keypads. • When the power LED on the control panel board switches off.
It is stopped by...	• Mains power being re-established.
After mains power is re-established, the control panel...	• Switches on the green power LED on the keypads again. • Switches on the power LED on the control panel board. • Stores the end of no mains power event in the Event Log and in the Diagnose Log.

See the *Installation Manual* for more information.

7.3.8 Maintenance event

This is generated when...	• The menu is accessed using the Installer code.
It activates...	• The dialler to send the respective maintenance message (if programmed) in form of numeric code or modem communication.
It is indicated...	• On The yellow maintenance LED on the keypads.
It inhibits...	• Alarm outputs. • The dialler to send the alarm messages in form of numeric code, vocal call or modem communication.
It is stored...	• In the Event Log (start of maintenance).
It lasts...	• For Until end of maintenance.

See the *Installation Manual* for more information.

7.3.9 Inhibit inputs event

This is generated when...	• The user manually inhibits inputs when arming partitions (arming override). • The system automatically inhibits inputs open when the system was armed (if programmed). • If the system inhibits inputs because the "alarm count" was exceeded (if programmed).
It activates...	• The programmed isolated input outputs which have at least one partition in common with the inhibited input. • The dialler to send the isolated inputs message in form of numeric code (if programmed).
It is indicated...	• On The yellow isolated inputs LEDs on the keypads which have at least one partition in common with the inhibited input.
It is stored...	• In the Event Log and the Diagnose Log. • In the inhibited input list.
It lasts...	• For Until the partitions which were armed by inhibiting these inputs in case of arming override are disarmed.

IMPORTANT! Automatic input inhibition is not EN50131 compliant.

IMPORTANT! The “Alarm Count” function is activated and configured to comply with EN50131 by default on control panels. Deactivating the function will cancel EN50131 compliance of the system.

7.3.10 Isolated input event

This is generated when...	• The inputs are isolated manually.
It activates...	• The programmed isolated input outputs which have at least one partition in common with the isolated input. • The dialler to send the isolated inputs message in form of numeric code (if programmed).
It is indicated...	• On The yellow isolated inputs LEDs on the keypads which have at least one partition in common with the isolated input.
It is stored...	• In the Event Log and the Diagnose Log. • In the isolated input list.
At the end of input isolation, the control panel...	• Stores the end of input isolation event in the Event Log and in the Diagnose Log. • Deactivates the programmed isolated input outputs associated to the partitions which have no more isolated inputs. • Switches off the yellow isolated inputs LEDs on keypads associated to the partitions which have no more isolated inputs.

7.3.11 Arm/disarm partitions event

This is generated when...	• One or more partitions are armed. • One or more partitions are disarmed.
It activates...	• The programmed partition status outputs and at least one partition armed by overriding, the TC AND outputs and the TC OR outputs. • The dialler to send the partition armed and disarmed message (if programmed) in form of numeric code, vocal call or text message.
It is indicated...	• On Status LED on keypads associated to at least one concerned partition.
It is stored...	• In the Event Log and the Diagnose Log.

7.3.12 Arm/disarm partitions override event

This is generated when...	• The arming of one or more partitions is overridden (e.g. because there are open inputs).
It activates...	• The programmed partition status outputs and at least one partition armed by overriding, the TC AND outputs and the TC OR outputs. • The dialler to send the arming override message in form of numeric code (if programmed).
It is stored...	• In the Event Log and the Diagnose Log.

7.3.13 Open input event

This is generated when...	• An input is opened.
It activates...	• The programmed open input outputs associated to the partition to which the input belongs.
It is indicated...	• On The open input LED of the keypads associated to the input. • On The red LED blinking on the readers if no alarms or failures/faults are being indicated.

7.3.14 Open input test event

This is generated when...	• A customised test input is opened.
It activates...	• The programmed open input outputs associated to the partition to which the input belongs.
It is indicated...	• On The open input LED of the keypads associated to the input. • On The red LED blinking on the reader if it is not already on fixed to indicate faults/failures or alarms.
It is stored...	• In the Event Log. • In the Diagnose Log.

7.3.15 Arrest system event

This is generated when...	• There is no mains power and the battery is not sufficiently charged (≤ 10.5 V)
It is indicated...	• On Power LED off.
It is stored...	• In the Diagnose Log (if the battery is not yet completely flat).

7.3.16 Valid code entered by user on keypad event

This is generated when...	• A valid access code is entered.
It is stored...	• In the Event Log and the Diagnose Log.

7.3.17 Edit date-time on keypad event

This is generated when...	• The date and time is edited.
It is stored...	• In the Event Log and the Diagnose Log.

7.3.18 User code enable/disable event

This is generated when...	• An access code is enabled or disabled.
It is stored...	• In the Event Log and the Diagnose Log.

7.3.19 Key enable/disable event

This is generated when...	• An electronic or proximity key is enabled or disabled.
It is stored...	• In the Event Log and the Diagnose Log.

7.3.20 Key acquisition/deletion event

This is generated when...	• An electronic or proximity key is acquired or deleted.
It is stored...	• In the Event Log and the Diagnose Log.

7.3.21 Timed programmer warning event

This is generated when...	• The timed programmer will arm the partitions soon.
It activates...	• The programmed PO warning outputs (only if the control concerns the partition status). • The enabled and associated keypads (buzzer).
It is indicated...	• On Timed programmer LED (only if the command concerns partition status).

7.3.22 Arming block event

This is generated when...	• Arming is blocked, e.g. because inputs are open.
It is stored...	• In the Event Log and the Diagnose Log.

7.3.23 Arming not executed event

This is generated when...	• If one or more partitions are not armed because of severe system anomalies.
It activates...	• The dialler to send the incomplete partition arming message in form of numeric code (if programmed).
It is stored...	• In the Event Log and the Diagnose Log.

7.4 DESCRIPTION OF ACOUSTIC INDICATIONS

If appropriately programmed, the keypads can emit auditory indications following given events.

7.4.1 Entry/exit time indication

This is generated when...	• One or more partitions associated to the keypads on which this function is enabled are armed (exit time). • One or more areas with one or more associated partitions with this function enabled are armed (exit time). • An input is opened (e.g. a customised first entry input) (entry time).
It lasts...	• For the partition entry/exit time or the delayed input delay time.
It is activated on...	• Enabled and associated keypads. • The programmed buzzer outputs which have at least one partition in common with the arming input.

IMPORTANT! The entry/exit acoustic indication function is activated and configured to comply with EN50131 by default on control panels. Changing this mandatory configuration will cancel EN50131 compliance of the system.

7.4.2 Arming warning

This is generated when...	• The programmed warning time for executing a partition arming command by the timed programmer is elapsing.
It lasts...	• For until the partitions are armed or a postpone command is imparted.
It is activated on...	• Enabled and associated keypads with one beep per minute. • The programmed arming warning outputs which have at least one partition in common with the arming input.

7.4.3 Gong

This is generated when...	• An input on which the ancillary gong function was enabled is opened and all the partitions to which it is associated are disarmed.
It is activated on...	• Enabled and associated keypads with two consecutive beeps. • On programmed gong outputs which have at least one partition in common for one second.

7.4.4 System status by means of wireless sirens

EN50131

Some sirens can indicate the system status, i.e. arming and disarming by means of the remote control or other means, either local or remote. The behaviour is comparable to that of car anti-theft systems which indicate arming and disarming by beeping and flashing the indicators.

This is generated when...	• One or more partitions or the entire system is armed/disarmed (if appropriately programmed).
It is activated on...	• Sirens inside and outside the system.
It is indicated on...	• Sirens by means of auditory only or auditory-visual indication: • HP500 arming = 1 beep + 1 blink; disarming = 2 beeps + 1 sequential blink • IS500 arming = 1 beep; disarming = 2 beeps

7.5 DESCRIPTION OF VOCAL INDICATIONS

EN50131
NOT RELATED

The vocal indications are available only on KP500DV/N keypads. The control panel must be equipped with a vocal module.

7.5.1 Arming/disarming message

This is generated when...	• One or more partitions are armed or disarmed by means of a vocal keypad. • One or more areas are armed or disarmed by means of a vocal keypad.
It is activated on...	• Keypads enabled for this service.
The following sentence is listened...	**For arming:** • *"Arming executed"* followed by the vocal names recorded for the single armed partitions. **For disarming:** • *"Disarmed"* followed by the vocal names recorded for the single disarmed partitions. **If arming fails in one or more partitions:** • *"Activation not done",* followed by the vocal names recorded for the single partitions which were not armed because one or more inputs are open. • *"Warning: open input".* **In case of arming with automatic inhibition of the open inputs:** • *"Arming executed"* followed by the vocal names recorded for the single armed partitions. • *"Warning: open excluded".*
It is stopped by...	• Pressing ESC

IMPORTANT! The automatic inhibition function is not EN50131 compliant. The function cancels EN50131 compliance of the entire system.

8 - PROGRAMMING VIA COMPUTER

This chapter illustrates how to program the system using a computer running Hi-Connect.

IMPORTANT! Some programming procedures via computer are not EN50131 compliant.

8.1 PROGRAMMING METHODS

The control panel can be programmed via computer in three ways:

- **Local:** The PC is connected to the control panel via a USB port.
- **Remote:** The PC is connected to the control panel via a model with telephone line. This type of connection can also be used for maintenance and remote system maintenance.

EN50131

- **Postponed:** The system is programmed at the workshop and stored on a USB key to transfer it to the control panel.

8.2 PREREQUISITES

8.2.1 Hardware prerequisites for data transfer

Appropriate interfaces or supplementary devices are needed for connecting the PC to the control panel or for simply transferring data. The following table lists the necessary equipment according to the required connection.

Connection or transfer type	Programming			Material needed
	Local	Remote	Postponed	
Via USB port	■			Control panel: IT-USB kit (complete with USB cable)
Via PSTN telephone line		■		Control panel: PSTN interface PC: Modem
Via GSM line		■		Control panel: IMG500/N module PC: Modem
Data from USB flash drive			■	Control panel: Interface for USB flash drive - IT USB/KEY PC: USB flash drive

See the *Installation Manual* for more information.

8.2.2 Personal computer requirements

Personal computer minimum configuration:

- Pentium IV processor
- 256 MB Ram minimum
- 1,8 Ghz CPU
- 80 GB Hard Disk
- Windows 2000 /XP Service Pack 2 / Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10
- CD ROM reader
- available serial port or USB port

8.2.3 Software requirements

Hi-Connect - rev. 3.50 or higher.

8.2.4 Enabling requirements

Access via PC does not need to be enabled in advance for programming via USB interface.
Access via computer must be enabled (see *User Manual*) only in case of remote programming.

8.3 HOW TO SAVE AND RESTORE DATA ON USB FLASH DRIVE

The IT USB/KEY interface can be used to save the programming on a USB flash drive. See *Installation Manual* for how to connect the control panel interface.

8.3.1 Files

Various files can be saved:

- programming and configuration of the entire system;
- codes and keys;
- event Log.

The data is stored on the flash drive in the “MP500_4N”, “MP500_8” or “MP500_16” folder according to the control panel type.
The folders will be automatically created by the control panel if they are not already present on the flash drive.
All file names are the system number. The file extensions differ according to content.

Example:
The following files will be stored on the flash drive for a MP500/16 control panel having system code “12345678”:

MP500_16\12345678.cfg
MP500_16\12345678.cod
MP500_16\12345678.sto

8.3.2 File types

The file types are identified by the extension. The type determines how data are recorded and the possible use.

Extension	Contents	Read and/or write?	Use
.cfg	Programming, configuration and releases of control panel and various device software.	The file can be read and edited on PC with Hi-Connect software. It can be retrieved from the control panel.	• To restore the configuration of a control panel. • To copy the configuration from one control panel to another. • To transfer the configuration prepared in advance in a workshop to a control panel.
.cod	Code and key data (encrypted)	No	• To restore previously saved codes and keys on a control panel at any time. • To copy codes and keys from one control panel to another.
.sto	Event Log data	The file can be read on PC with Hi-Connect software.	To transfer and browse the events stored by a control panel on a PC.

8.3.3 How to save data on USB flash drive

Proceed as follows to save data on a USB flash drive:

1) Insert the USB flash drive in the USB - IT USB/KEY interface.

2) Enter **<Installer code>**, press OK, then MENU and finally ▼ repeatedly until MAINTENANCE appears.

```
UT00:INSTALLER
MAINTENANCE
```

3) Press OK and then ▼ several times until DATA TRANSFER appears.

```
MAINTENANCE
DATA TRANSFER
```

4) Press OK. Press ▼ and ▲ to select SAVE SETTINGS. Press OK to confirm.

```
DATA TRANSFER
SAVE SETTINGS
```

5) Press ▼ and ▲ to select the data to be saved: CONFIGURATIONS, CODES/KEYS, DIAGNOSE LOG. Press OK to confirm. The folders will be automatically created by the control panel if they are not already present on the flash drive.

```
SAVE SETTINGS
CONFIGURATIONS
```

6) A password will be required to save codes/keys. Enter the **< Master code>**.

7) The saving operation may take several minutes. The keypad will beep during the saving process and the message “WAIT PLEASE” will be gradually replaced by “>”. At the end, the message “CONFIGURATIONS OK” will appear if the operation is successful. Otherwise, “KO” will appear (other references may appear if other data are saved).

```
CONFIGURATIONS
  WAIT PLEASE
```

IMPORTANT! Never remove the key or disconnect power from the control panel while the yellow LED of the USB/KEY interface blinking.

8) Press ESC.

9) Repeat from step 5 to save other data types.

10) Press ESC repeatedly to exit from the menu.

8.3.4 How to restore data on the control panel

Proceed as follows to restore data stored on the USB flash drive on the control panel:

1) Insert the USB flash drive in the USB - IT USB/KEY interface.
2) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until MAINTENANCE appears.
3) Press [OK] and then [▼] several times until DATA TRANSFER appears.
4) Press [OK]. Press [▼] and [▲] to select RESTORE SETTINGS. Press [OK] to confirm.
5) Press [▼] and [▲] to select the data to be restored: CONFIGURATIONS, CODES/KEYS, DIAGNOSE LOG. Press [OK] to confirm.
6) Two passwords are required to restore codes/keys. Enter the **<Master code>** and then the **<Installer code>**.
7) Press [OK] to confirm [ESC] to cancel the operation.
8) The restoring operation may take several minutes. The keypad will beep during the restoring process and the message “WAIT PLEASE” will be gradually replaced by “>”. At the end, the message “CONFIGURATIONS OK” will appear if the operation is successful. Otherwise, “KO” will appear (other references may appear if other data are restored).
9) Press [ESC].
10) Repeat from step 5 to save other data types.

IMPORTANT Never remove the key or disconnect power from the control panel while the yellow LED of the USB/KEY interface blinking.

11) Press [ESC] repeatedly to exit from the menu.

```
UT00:INSTALLER
MAINTENANCE
```

```
MAINTENANCE
DATA TRANSFER
```

```
DATA TRANSFER
RESTORE SETTINGS
```

```
RESTORE SETTINGS
CONFIGURATIONS
```

```
CONFIGURATIONS
ARE YOU SURE?
```

```
CONFIGURATIONS
WAIT PLEASE
```

9 - MAINTENANCE

The maintenance operations requiring physical management of the system are described in the *Installation Manual*.
The maintenance operations which do not require to operate physically on the system are described here.

9.1 INPUT ISOLATION AND END OF ISOLATION

It may be necessary to isolate an input in the system temporarily, e.g. to run a test or because the connected detector is faulty and is causing false alarms thus preventing the system from being armed. Isolating an input may reduce the security of the system.

Isolating a double balanced input will inhibit both the burglar and the tamper alarm. Its opening will be indicated by the open input LED on the associated keypads.

IMPORTANT! Only the inputs which are programmed as “ISOLABLE” can be isolated.

9.1.1 How to isolate an input

Proceed as follows to isolate the inputs:

1) Enter **< Installer / Technical Manager code>**, for GRADE 3 systems or enter **<User / Installer / Technical Manager >** for GRADE 2 systems**,** press [OK], then [MENU] and finally [▼] repeatedly until SETTINGS appears.

```
UT00:INSTALLER
SETTINGS
```

2) Press [OK].

```
SETTINGS
ISOLATION
```

3) Press [OK]. Press [▼] and [▲] to select the input to be isolated. Press [OK] to confirm.

```
ISOLATION
In001:
```

4) Press [OK] to confirm insulation or [ESC] to cancel the operation. The isolated inputs LED will light up on the keypads.

```
In001:…
ISOLATE    OK?
```

5) Press [ESC] repeatedly to exit from the menu.

9.1.2 How to end isolate an input

Proceed as follows to include an input:

Proceed as follows to exclude the inputs:

1) Enter **<Installer / Technical Manager code>**, for GRADE 3 systems or enter **<User / Installer / Technical Manager >** for GRADE 2 systems**,** press [OK], then [MENU] and finally [▼] repeatedly until SETTINGS appears.

```
UT00:INSTALLER
SETTINGS
```

2) Press [OK].

```
SETTINGS
ISOLATION
```

3) Press [OK]. Press [▼] and [▲] to select the input to be included again. Press [OK] to confirm.

```
ISOLATION
In001:
```

4) Press [OK] to confirm inclusion or [ESC] to cancel the operation. The isolated inputs LED will be switched off on the keypads if there are no other isolated inputs.

```
In001:…
INCLUDE    OK?
```

5) Press [ESC] repeatedly to exit from the menu.

9.2 HOW TO VIEW DEVICE ADDRESSES

Proceed as follows to check the address of a given bus device in the system:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until MAINTENANCE appears.

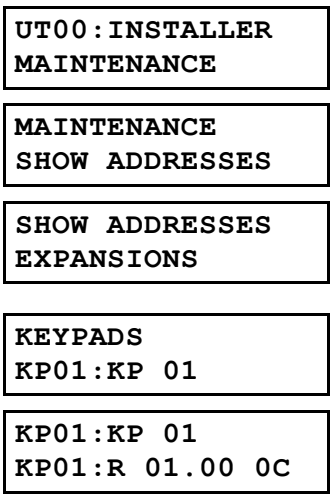
2) Press [OK] and then [▼] several times until SHOW ADDRESSES appears.

3) Press [OK]. Press [▼] and [▲] to select the concerned device type (EXPANSIONS, KEYPADS, READERS). Press [OK] to confirm.

4) Press [▼] and [▲] to select the concerned device. Press [OK] to confirm.

5) The address and name of the device will appear on the upper line and the installed firmware version will appear on the lower line.

6) Press [ESC] repeatedly to exit from the menu.



9.3 HOW TO VIEW THE FIRMWARE RELEASE OF DEVICES

Proceed as follows to read the firmware release of a bus device of the system or of the control panel itself:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until MAINTENANCE appears.

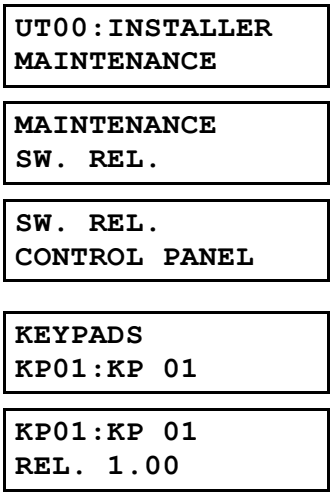
2) Press [OK] and then [▼] several times until SW. REL. appears.

3) Press [OK]. Press [▼] and [▲] to select the concerned device type (CONTROL PANEL, EXPANSIONS, KEYPADS, READERS). Press [OK] to confirm.

4) Press [▼] and [▲] to select the concerned device. Press [OK] to confirm.

5) The firmware release of the device will appear on the second line of the display.

6) Press [ESC] repeatedly to exit from the menu.



9.4 HOW TO UPGRADE BUS DEVICE FIRMWARE FROM MENU

The firmware of bus devices can be upgraded from the control panels without needing to disconnect the devices or switch the system off.

The firmware is upgraded by connecting them to the bus.

IMPORTANT! Firmware can only be upgraded if the Elkron Customer Care Centre has provided the necessary files and the accompanying technical notes.

9.4.1 Necessary conditions

The upgrade procedure will only be started in the following conditions:

- devices are acquired and correctly operating in the system
- Devices are equipped with software release which can be upgraded (see table).
- The files ("filename".BIN) reside in the "MP500_4N\UPG", "MP500_8\UPG" or "MP500_16\UPG" folder (only for device files; the control panel file must reside in the root of the USB flash drive).
- The firmware release of the upgrade file is different from the release residing in the device.
- The IT USB/KEY interface is connected to the control panel.

IMPORTANT! The IT-USB/KEY interface must be connected to the control panel when the latter is not powered (mains power and battery disconnected).

Device	Upgradeable FW release	Device type	File name
KP500DV/N	V 1.00	LCD vocal keypad	KP500DVN.bin
KP500D/N	V 1.00	LCD keypad with inputs	KP500DVN.bin
KP500DP/N	V 1.00	Soft touch keypad	KP500DPN.bin
KP500D/ST	V 1.00	Soft touch keypad	KP500DPN.bin
AS500/RPT	V 1.00	Supplementary power supply unit	AS500.bin
EP508	V 3.00	Wired expansion module	EP500.bin

IMPORTANT! Devices with FW releases lower than those shown in the table cannot be upgraded.

IMPORTANT! The electronic and proximity key readers cannot be upgraded.

9.4.2 Upgrade file

The upgrade files have extension ".bin".
The filename is equal to the name of the device to be upgraded.

Example for MP500/16 control panels:

KP500DV/N device upgrade file: KP500DVN.bin

The files of the devices must be copied to the **MP500_16\UPG** folder specifically created on the USB memory stick (USB flash drive etc.).
The control panel file must be copied directly to the root of the USB memory stick (USB flash drive etc.).

Example:

Device	File path on USB memory stick
KP500DV/N	MP500_16\UPG\KP500DVN.bin

IMPORTANT! Do not change name or path of the file: the control panel only recognises the set terminology. The file will not be recognised if the file is renamed or the position is changed on the USB memory stick and the upgrading procedure will not be started. Several files related to different device types or other files non-Elkron files may coexist on the same USB memory stick.

9.4.3 Preliminary operations

Check the firmware version of the devices to be upgraded.
Download the files related to the devices to be upgraded from the installer area on the Elkron website (www.elkron.com).
Save the downloaded files on a USB memory stick in the subfolders created as shown in paragraph *9.4.2 Upgrade file*.

ADVICE: Before upgrading the devices connected to the bus, it is advisable to save programming and configuration data of the entire system (.cfg) and the code and key file (.cod). The procedure is shown in paragraph *8.3.3 How to save data on USB flash drive*.

IMPORTANT! The "*.bin" files are supplied by Elkron only. Do not edit or open the files for any reason: they are encrypted in a proprietary binary format and protected by check fields and CRC to preserve content.
Do not download binary files from website other than the Elkron official website (www.elkron.com).

9.4.4 How to upgrade bus devices

Proceed as follows to upgrade the firmware of bus devices:

1) Plug the IT USB/KEY interface into the J11 connector of the control panel.

2) Insert the USB memory stick (e.g. USB flash drive) with upgrade files in the IT USB/KEY interface.

3) Enter **<Installer code>**, press OK, then MENU and finally ⌄ repeatedly until MAINTENANCE appears.

4) Press OK and then ⌄ several times until FIRMWARE UPDATE appears.

5) Press OK. Press ⌄ and ⌃ to select whether to upgrade the entire system (ALL THE DEVICES) or upgrade only a specific device type (expansions, keypads, readers). Press OK to confirm.

6) Press OK again when the confirmation prompt appears.

```
UT00:INSTALLER
MAINTENANCE
```

```
MAINTENANCE
FIRMWARE UPDATE
```

```
FIRMWARE UPDATE
ALL THE DEVICES
```

IMPORTANT! The devices which have already been upgraded to the firmware release of the files on the USB memory stick will not be concerned by the upgrade procedure.

The advancement will appear on the keypad display and on the run LED of the control panel after starting the upgrade procedure. The result will appear at the end of the procedure.

IMPORTANT! The advancement state will only appear if the keypad is not being upgraded. In this case, the keypad will not show any until upgrading is finished).

The upgrade procedure may take several minutes, indicatively approximately 4 minutes for the keypad only, less for other devices individually. It will take longer if several device types are upgraded at the same time. The control panel will light up the run LED according to the "Running" sequence (blinking for 1.6 seconds - off for 0.5 seconds).

IMPORTANT! Do not remove the flash drive until the upgrade procedure is completed.

Upgrade results are:

- **Positive result**. The procedure was successful. The run LED will light up on the control panel according to the "Successful Update" sequence (off for 2 seconds - blinking for 2 seconds).
- **Negative result**. The procedure was interrupted or is not OK. The run LED will light up on the control panel according to the "Update was not successful" sequence (on for 2 seconds - blinking for 2 seconds). The message "END DOWNLOAD KO" will appear on the keypad.

Details on the firmware upgrading procedure will be saved in the Event Log in both cases at the end of the operation.

9.5 FIRMWARE UPGRADE AT POWER ON

The firmware of the control panel and of all bus devices of the system can be upgraded automatically when the control panel is turned on. The necessary conditions, upgrade files and preliminary operations are the same as the firmware upgrading procedure from menu.

9.5.1 Device FW upgrade procedure at power on

The procedure is shown below:

1) Remove all power from the control panel (remove main power and disconnect the back-up battery).
2) Insert a jumper between the pins 5 and 6 of the “SERVICE” connector on the motherboard of the control panel.
3) Plug the IT USB/KEY interface into the J11 connector of the control panel.
4) Insert the USB memory stick, onto which the upgrade files were previously copied (.bin), into the USB port of the IT USB/KEY interface.
5) Power the control panel again (mains power and back-up battery).

Note: Implement the appropriate actions to block the fail-safe siren commands or otherwise disconnect the power by removing the internal back-up batteries.

When power is restored, the control panel will check:

- presence of the jumper JP on the “SERVICE” connector
- presence of the interface
- presence of the USB memory stick.

Upgrading may not be successful if only one of these conditions is not respected.

If the check was successful:

- The control panel will automatically start the upgrade procedure towards the system devices (the devices which can be upgraded are set to "BOOT" status).
- The control panel will upgrade the devices of the same type in parallel (keypads, expansion modules etc.) checking the result and repeating the procedure automatically in case of errors.
- During the entire upgrade procedure, the run LED lights up on the control panel according to the “Running” sequence (blinking for 1.6 seconds - off for 0.5 seconds).

After upgrading, one of the following indications will appear according to the result type.

- **Positive result.** The procedure was successful.
  The run LED will light up on the control panel according to the “Successful Update” sequence (off for 2 seconds - blinking for 2 seconds).

  IMPORTANT! This indication will appear even if the procedure never started. No device can be upgraded or the devices have the same upgrade file release (“filename”.BIN).

- **Negative result**. The procedure was interrupted or is not OK.
  The run LED will light up on the control panel according to the “Update was not successful” sequence (on for 2 seconds - blinking for 2 seconds).

  IMPORTANT! This indication will also appear if one of the following errors occurs:

  - The USB memory stick does not respond.
  - The files (.bin) are not in the dedicated folder (UPG).
  - Despite the automatic upgrade attempts all or some devices have not completed the procedure: communication interrupted, incorrect download (CRC KO), flash writing KO.
  - The devices which do not complete programming successfully will remain in "BOOT" state and will not be used in the system until they are reprogrammed.

The control panel will maintain one of the two indication sequences until the control panel power off.

To make the upgrade definitive and return the system to operating conditions:

1. Remove all power from the control panel (remove main power and disconnect the back-up battery).
2. Remove the jumper between the pins 5 and 6 of the “SERVICE” connector on the motherboard of the control panel.
3. Unplug the IT USB/KEY interface from the J11 connector of the control panel.
4. Power the control panel again (mains power and back-up battery).

9.5.2 Control panel upgrade procedure at power on

Proceed as follows to upgrade the control panel:

1. Remove all power from the control panel (remove main power and disconnect the back-up battery).
2. Plug the IT USB/KEY interface into the J11 connector of the control panel.
3. Insert the USB memory stick, onto which the upgrade file was previously copied (.bin), into the USB port of the IT USB/KEY interface.
4. Power the control panel again (mains power and back-up battery).

Note: Implement the appropriate actions to block any fail-safe siren commands or otherwise disconnect the power by removing the internal back-up batteries.

The control panel will be upgraded at power on and the new firmware will be downloaded. The upgrade procedure may last for a few minutes.

IMPORTANT! Do not remove the flash drive until the upgrade procedure is completed.

After upgrading, one of the following indications will appear according to the result type.

- **Positive result.** The procedure was successful.
  The run LED will light up on the control panel according to the “Successful Update” sequence (off for 2 seconds - blinking for 2 seconds).

  IMPORTANT! This indication will appear even if the procedure never started.
  No device can be upgraded or the devices have the same upgrade file release (“filename”.BIN).

- **Negative result**. The procedure was interrupted or is not OK.
  The run LED will light up on the control panel according to the “Update was not successful” sequence (on for 2 seconds - blinking for 2 seconds).

  IMPORTANT! This indication will also appear if one of the following errors occurs:

  - The USB memory stick does not respond.
  - The file (.bin) is not in the root of the USB memory stick.

The control panel will maintain one of the two indication sequences until the control panel power off.

To make the upgrade definitive and return the system to operating conditions:
1. Remove all power from the control panel (remove main power and disconnect the back-up battery).
2. Unplug the IT USB/KEY interface from the J11 connector of the control panel.
3. Power the control panel again (mains power and back-up battery).

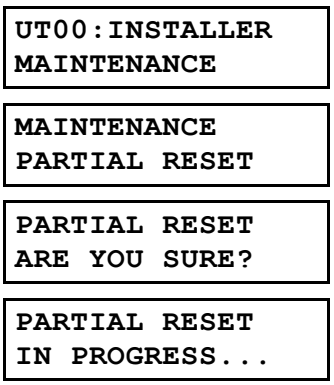
Details on the firmware upgrading procedure will be saved in the Event Log in both cases at the end of the operation.

9.6 PARTIAL RESET

The partial reset procedure returns the factory settings of all devices in the system, including the control panel, to default.
The codes, keys and logs are not deleted.

Proceed as follows to carry out the partial reset:

1) Enter **<Installer code>**, press OK, then MENU and finally ▼ repeatedly until MAINTENANCE appears.
2) Press OK and then ▼ several times until PARTIAL RESET appears.
3) Press OK.
4) Press OK to confirm the operation. Press ESC to cancel the operation. The keypad buzzer will sound during the operation.
5) The first page of the maintenance menu will appear at the end. Press ESC repeatedly to exit from the menu.

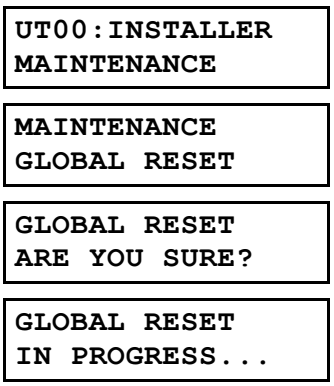


9.7 GLOBAL RESET

Global reset restores the control panel to factory settings (inputs, outputs, times, partitions, timed programmer, PSTN/GSM parameters) and eliminates all previously acquired devices. The respective configurations are restored to factory settings and the addresses are deleted.

Proceed as follows to carry out the global reset:

1) Enter **<Installer code>**, press OK, then MENU and finally ▼ repeatedly until MAINTENANCE appears.
2) Press OK and then ▼ several times until GLOBAL RESET appears.
3) Press OK.
4) Press OK to confirm the operation. Press ESC to cancel the operation. The keypad buzzer will sound during the operation.
5) A row of dots will appear on the control panels at the end of the operation. Switch the system off, switch it back on, reacquire the devices and reprogram the entire system.



9.8 EVENT LOG

The Event Log filters the events which are relevant for the user from the Diagnose Log (arming, disarming, inhibitions, no mains power etc.).

The events are displayed from the most recent to the oldest, i.e. the most recent event is the one with the lowest identification number. The stored events move down by one position as a new event is added.

The Event Log may be examined by the Master user and by the other users but may only be deleted by the Installer.

IMPORTANT! The Event Log may be viewed for the entire system or only for a specific area, if areas are created.

IMPORTANT! Regardless of the choice (areas or total), a user can only see the events related to the pertinent partitions, i.e. the assigned partitions.
The Master user is permanently assigned to all partitions and can always see all stored events.

9.8.1 How to interpret viewed data

Stored event information is displayed in the Event Log as follows:

```
xxxx hh:mm dd/MM
<<Text>>
```

where:

- **xxxx** is the sequential number of the event (0001 is the most recent event, 1000 is the oldest)
- **hh:mm** hours and minutes when the event occurred
- **dd/MM** day and month when the event occurred
- **<< Text >>** textual description of the event.

Additional information may be available according to the event type. Press [OK] once or more times to display the information cyclically.

9.8.2 How to browse the Event Log

Proceed as follows to browse the Event Log:

1) Enter **< Master / User / Installer / Technical Manager code>**, press [OK], then [MENU] and finally [▼] repeatedly until EVENT LOG appears.

```
UT01:MASTER
EVENT LOG
```

2) Press [OK].

```
EVENT LOG
TOTAL
```

3) Press [▼] and [▲] to select whether to view the entire log (TOTAL) or the log for the areas only (AREAS). Press [OK] to confirm.

```
EVENT LOG
AREAS
```

4) The last stored event will appear if TOTAL is chosen. Press [OK] repeatedly to view more information on the displayed event, if any.

```
0001 10:31 12/01
VALID CODE
```

5) Press [▼] and [▲] to scroll the various stored events.

6) If AREAS is chosen, press [▼] and [▲] to select the concerned area.

```
AREAS
AR A:…
```

7) Press [OK] to confirm.

```
AR A:…
READ EVENT LOG
```

8) Press [OK] to see the last stored event for the area. Press [▼] and [▲] to scroll the various stored events.

9) Press [ESC] repeatedly to exit from the menu.

```
    MP500/16
12/01/2014 10:40
```

9.9 DIAGNOSE LOG

The Diagnose Log stores the last 1000 events (arming, disarming, alarm, tamper etc.) which concerned the system.
The events are stored from the most recent to the oldest, i.e. the most recent event is the one with the lowest identification number.
The stored events move down by one position as a new event is added.
When the Diagnose Log reaches the maximum size (1000 events), each new event will be written over the oldest stored event.
The Diagnose Log can only be examined by the Technical Manager and the Installer, but deleted only by the Installer.

WARNING: The Diagnose Log also contains the Event Log. More specifically, the Event Log is extracted from the Diagnose Log. Viewing the Event Log simply means filtering all the stored events and ignoring those which are more specifically technical.

IMPORTANT! If areas are created, the Diagnose Log may be viewed by area or by system.

9.9.1 How to interpret viewed data

See paragraph *9.8.1 How to interpret viewed data* for how to interpret viewed information.

9.9.2 How to browse the Diagnose Log

Proceed as follows to browse the Diagnose Log:

1) Enter **<Installer code / Technical Manager >**, press [OK], then [MENU] and finally [▼] repeatedly until MAINTENANCE appears.

```
UT00:INSTALLER
MAINTENANCE
```

2) Press [OK] and then [▼] several times until DIAGNOSE LOG appears.

```
MAINTENANCE
DIAGNOSE LOG.
```

3) Press [OK]. Press [▼] and [▲] to select whether to view the entire log (TOTAL) or the log for the areas only (AREAS). The selection only appears if the system has areas. Press [OK] to confirm.

4) If TOTAL is selected:

```
TOTAL
READ EVENT LOG
```

5) Press [OK]. The last stored event will appear. Press [▼] and [▲] to scroll the various stored events. Press [OK] repeatedly to view more information on the displayed event, if any.

```
0001 10:31 15/03
VALID CODE
```

6) Select the concerned area if AREAS is selected. Press [▼] and [▲] to select the area. Press [OK] to confirm.

```
AREAS
AR A:…
```

7) Press [OK] to see the last stored event for the area. Press [▼] and [▲] to scroll the various stored events. Press [OK] repeatedly to view more information on the displayed event, if any.

```
AR A:…
READ EVENT LOG
```

8) Press [ESC] repeatedly to exit from the menu.

9.9.3 How to delete the Diagnose Log

IMPORTANT! The deletion operation cannot be undone.

IMPORTANT! The operation will also delete all information from the Event Log.

Proceed as follows to delete the Diagnose Log:

1) Enter **<Installer code>**, press [OK], then [MENU] and finally [▼] repeatedly until MAINTENANCE appears.

```
UT00:INSTALLER
MAINTENANCE
```

2) Press [OK] and then [▼] several times until DIAGNOSE LOG appears.

```
MAINTENANCE
DIAGNOSE LOG.
```

3) Press [OK]. Press [▼] and [▲] to select whether to view the entire log (TOTAL) if the system includes areas. Press [OK] to confirm.

```
TOTAL
READ EVENT LOG
```

4) Press [▼].

```
TOTAL
ERASE EVENT LOG
```

5) Press [OK].

```
ERASE EVENT LOG
ARE YOU SURE?
```

6) Press [OK] to confirm [ESC] to cancel the operation.

7) Press [ESC] repeatedly to exit from the menu.

9.10 EN50131 DEGREE COMPLIANCE

By factory setting, the behaviour of MP500/8 and MP500/16 systems is EN50131 grade 3 compliant, and that of MP500/4N system is EN50131 grade 2 compliant.

Some settings may be changed individually during programming. Others, such as system status visibility, indications and methods of use of readers, may be varied as a whole by selecting the relevant “Use mode”.

Mode 3 is the only one to be EN50131 grade 3 compliant. Mode 2 is EN50131 grade 2 compliant.

Mode 0 is not compliant to any standard. Mode 3 is not available for MP500/4N control panel.

Some differences of behaviour in Mode 3 and in Mode 2 are described in paragraphs *1.2.2.1 Use of LEDs and icons with EN50131 grade 3*, *5.4.1.1 System in use mode = Mode 3 (EN50131 grade 3 compliant)* and following, *5.4.4.1 System in use mode = Mode 3 (EN50131 grade 3 compliant)* and following.

IMPORTANT! The settings of the alarm system are not changed if the mode is changed.

For example, if the mode of a fully EN50131 grade 3 compliant systems is changed from Mode 3 to Mode 2, compliance will be lost. Simply set Mode 3 again to regain compliance.

On the other hand, if the alarm system settings and its hardware configuration are not EN50131 grade 3 compliant it will not be enough to set Mode 3 to make the alarm system EN50131 grade 3 compliant.

To change the use mode of the system:

1) Enter **<Installer code>**, press OK, then MENU and finally ▼ repeatedly until MAINTENANCE appears.

2) Press OK and then ▼ several times until USE MODE appears.

3) Press OK. Press ▼ and ▲ to select the mode. Press OK to confirm.

IMPORTANT! By setting Mode 2 or Mode 0 the system will lose EN50131 grade 3 compliance.

IMPORTANT! The Operation Mode 0 is only available starting from control panels with SW version 1.01 and starting from keypad SW version 1.03.

4) Press ESC repeatedly to exit from the menu.

```
UT00:INSTALLER
MAINTENANCE
```

```
MAINTENANCE
USE MODE
```

```
USE MODE
MODE 3
```

9.11 HOW TO ACQUIRE BUS DEVICES

The procedure for acquiring a bus device (expansion module, keypad, reader) is contained in the *Installation Manua*l.

9.12 HOW TO DELETE BUS DEVICES

The procedure for deleting a bus device (expansion module, keypad, reader) is contained in the *Installation Manual*.

10 - TABLES

10.1 VOCAL ALARM MESSAGES

The following tables show all the vocal messages (both pre-recorded and not) for the possible events and show which messages can be customised by recording a personal message over it. Further details are provided for each message type with indication of how to listen to it.
The basic message must be recorded. It is in common to all events and alarms and it is 10 seconds long.
The maximum length of all other messages is 4 seconds.

Event/alarm	Message	Customisable Mode 4	Generated for	More details in Mode:
Burglar alarm	*Burglar alarm*	■	Opening of a burglar alarm input	2, 3, 4
Tamper alarm	*System tamper*	■	Device tampering (tamper, SAB or no communication)	
			Input imbalance	2, 3, 4
Panic	*Panic*		Opening of a panic alarm input	2, 3, 4
Silent panic			Opening of a silent panic alarm input	2, 3, 4
			Pressing a function key on the keypad	
			Pressing key 2 on the remote control (if programmed)	
Hold-up alarm	*Attack in progress*	■	Entering a hold-up code	2, 3, 4
			Opening of a hold-up alarm input	
Fire alarm	*Fire alarm*	■	Opening of a fire alarm input	2, 3, 4
			Pressing a function key on the keypad	
			Pressing key 2 on the remote control (if programmed)	
Emergency alarm	*Help needed*	■	Opening of an emergency input or no movement detected	2, 3, 4
			Pressing a function key on the keypad	
			Pressing key 2 on the remote control (if programmed)	
Technological event type 1 - 2 - 3	*Technological service*	■	Opening of a technological input 1 - 2 - 3	2, 3, 4
Failure alarm from failure input	*Input failure*		Opening of a failure input	2, 3, 4
End of alarm from failure input	*Input restored*		Closing of the failure input	2, 3, 4
Failure alarm PSTN telephone line	*Telephone line failure*		Anomaly detected on PSTN telephone line	
End of PSTN telephone line failure	*Telephone line restored*		Anomaly corrected on PSTN telephone line	
GSM line failure alarm	*GSM line failure*		Anomaly detected on GSM line	
End of GSM line failure	*Telephone line restored*		Anomaly corrected on GSM telephone line	
System failure alarm	*System fault*		Anomaly detected on the system	
End of system failure alarm	*System fault restored*		Anomaly corrected on system	
Continuous lack of power alarm	*Mains power failure*		No mains power in control panel for longer than programmed time ("lack of power" time)	
End of lack of power alarm	*Electric line restored*		Power restored to control panel	
Low battery alarm	*Battery fault*		Flat or missing control panel battery	
End of low battery alarm	*Battery restored*		Control panel battery charge restored	
Arm partition(s)	*Armed*		Some partitions armed	2, 4
Disarm partition(s)	*Disarm*		Some partitions disarmed	2, 4
SIM expiry warning	*SIM Card expiry*		The first day of the month set for the warning reached	

Table 14 - Vocal messages for MP500/4N, MP500/8 and MP500/16 control panels

10.2 ALARM SENDING TYPES

One or more sending modes can be selected according to the alarm type to be sent.

Event	Sending priority	Transmission mode			
		Vocal	IDP, ADF, C200B, C200B P-P	Modem	Text message
Burglar alarm	1	■	■	■	■
Pre-alarm	1		■	■	
Technological type 1 event	7	■	■	■	■
Technological type 2 event	7	■	■	■	■
Technological type 3 event	7	■	■	■	■
Fire alarm	5	■	■	■	■
Panic	0	■	■	■	
Silent panic	0	■	■	■	
Emergency	4	■	■	■	
Hold-up alarm	0	■	■	■	
Arm/disarm partition(s)	1	■	■	■	■
Maintenance	8		■	■	
Input isolation	8		■	■	
Tamper	3	■	■	■	■
Lack of power	6	■	■	■	
Low battery	6	■	■	■	
System failure	6	■	■	■	
Wrong code	3		■	■	
Notices (SIM expiry)	8	■			■

Multiple, simultaneous alarms will be send in order of priority (0 = maximum priority, 8 = minimum priority).

Table 15 - Alarm sending types

10.3 IDP MESSAGE STRUCTURE

One message is sent for each single event. Several events will be sent in the same telephone call, if applicable.
For example, messages related to each partition concerned by an arming or disarming event will be sent in sequence in the same telephone call because the global system arming or disarming does not exist as an event.
The message string structure is applicable for all events.

A	A	A	A	1	8	Q	E	E	E	G	G	C	C	C	S
Rem.Ctrl Code				FIXED		Qualification	Event			Group		Code or input ID			Cks

Where:

Block	Code	Description
Rem.Ctrl Code	xxxx	these are the last four digits of the remote control code
Qualification	1	this indicates the beginning of an event or disarming
	3	this indicates the end of an event or arming
Event	100	emergency alarm from input
	101	emergency alarm from function key on keypad
	110	fire alarm from input
	111	fire alarm from function key on keypad
	120	panic alarm from input
	121	hold-up alarm from input
	122	silent panic alarm from input or from function key on keypad
	130	hold-up alarm from input and way (route) input (entry / way / exit)
	137	tamper input alarm
	138	input pre-alarm
	145	control panel and/or peripheral device tamper alarm
	150	technological event 1 from input
	151	technological event 2 from input
	152	technological event 3 from input
	300	failure alarm from failure input
	301	lack of power alarm
	302	low battery alarm
	307	power failure alarm
	320	siren failure
	330	control panel bus communication to peripheral device error alarm
	344	jamming alarm (in presence of radio expansion module only)
	351	PSTN telephone failure alarm
	354	GSM telephone failure alarm
	355	no supervision alarm (in presence of radio expansion module with devices only)
	380	detector failure
	388	jamming
	401	arming/disarming from user code, key, remote control
	403	arming/disarming from timed programmer
	407	arming/disarming from remote with DTMF code or Hi-Connect
	409	arming/disarming from key input
	450	arming with overriding
	454	partitions not armed because more than 70% of the total inputs are open or isolated in presence of faults, tampering
	458	maintenance (installer working on site)
	461	wrong code alarm
	570	input isolation
	573	input inhibition
	601	manual test call
	602	cycle test call
Group	00	the event refers to the entire system
	01 ÷ 16	the event is referred to partitions 1 - 16

Table 16 - IDP message structure

Code or input ID
The meaning of the code depends on the event.

Event	Code	Description
For arming events	000	Event generated by Installer code, Timed Programmer or Hi-Connect
To identify a user or a key	001	Event generated by the master user code
	002 ÷ 063	Event generated by the user code 2 ÷ 63
	101 ÷ 164	Event generated by key 1 ÷ 64
	2<radio.exp.num> <rem.ctrl.num.>	Event generated by remote control of a radio expansion module
To indicate the logical number of the concerned input	001 ÷ 128	
To identify the keypad which generated a function key event	101 ÷ 108	Event generated by keypad 1 ÷ 8
To identify the device which generated the tamper alarm	000	Event generated by tamper or SAB input of control panel
	101 ÷ 108	Event generated by tamper of keypad 1 ÷ 8
	401 ÷ 415	Event generated by tamper of an expansion module or supplementary power unit
	501 ÷ 502	Event generated by the tamper of a radio expansion module
To identify the device which generated the failure alarm consequent to loss of communication	101 ÷ 108	Event generated by no communication of keypad 1 ÷ 8
	301 ÷ 316	Event generated by no communication of reader 1 ÷ 16
	401 ÷ 415	Event generated by no communication of expansion of supplementary power unit 1 ÷ 16
	501 ÷ 502	Event generated by no communication of a radio expansion module
To identify the device which generated the low battery alarm	000	Event generated by the control panel battery
	401 ÷ 415	Event generated by the battery of a supplementary power unit 1 ÷ 16
	5xx	Event generated by the battery of a radio device **(*)**
To identify the device which generated the lack of power alarm	000	Event generated by "lack of power" on control panel
	401 ÷ 415	Event generated by "lack of power" on a supplementary power unit 1 ÷ 16

Table 17 - ID code or input with IDP protocol

(*) Encoding (For more information see dedicated manual).

10.4 DETAIL OF EVENTS AND MANAGEMENT

Cause	LED		Log	Memory	Description of the event (Event Log and Diagnose Log)	Auxiliary indication (controlled output)	Telephone message EN50131 NOT RELATED
	Keypad	Reader					
Burglar alarm (immediate, delayed, delayed way, last exit)		■	■	■	Inxxx:name IN customisation	Burglar	Burglar alarm
Burglar pre-alarm		■	■	■	Inxxx:name IN customisation	Burglar	Burglar alarm
Panic indication from input / function key / remote control		■	■	■	“KP xx”	Panic	Panic
Fire indication from input / function key / remote control		■	■	■	“KP xx”	Fire	Fire alarm
Emergency indication from input / function key / remote control		■	■	■	“KP xx”	Emergency	Emergency request
Silent panic indication from input / function key / remote control			■	■	“KP xx”	Silent panic	Panic
Technological input / output 1 activation		■	■	■	Inxxx:name TECHNOL. TYPE 1	Technological 1	Technological service 1
Technological input / output 2 activation		■	■	■	Inxxx:name TECHNOL. TYPE 2	Technological 2	Technological service 2
Technological input / output 3 activation		■	■	■	Inxxx:name TECHNOL. TYPE 3	Technological 3	Technological service 3
Low battery					LOW BATTERY CONTROL PANEL or device	Low battery	Battery fault/restored
Detector fault input alarm				■	Inxxx:name DETECTOR FAILURE	Detector fault	Anomaly
Siren failure input alarm		■		■	SIREN FAILURE	System failure	Anomaly
Fault input alarm		■		■	Inxxx:name FAILURE	Failure	Anomaly
Jamming fault input alarm		■		■	Inxxx:name JAMMING	Detector fault	Anomaly
External communicator fault input alarm		■		■	Inxxx:name COM. FAULT	Telephone fault	Anomaly
Other faults				■		System failure	Failure
No communication with device on bus		■		■	BUS COMM.FAILURE BUS device (DDxx:name)	Sys fault	System tamper
Isolated inputs			■		Inxxx:name	Isolated inputs	Excluded input
Inhibited inputs (temporarily during arming)			■		INHIBIT	Isolated inputs	Excluded input
After having entered 21 wrong codes			■	■	WRONG CODE device (DDxx:name)	Tamper	
Tamper or SAB input indicating tampering		■		■	device (DDxx:name)	Tamper	System tamper
Balanced input imbalance		■		■	Inxxx:name IN customisation	Tamper	System tamper
Radio jamming		■		■	JAMMING device (DDxx:name)	Tamper	Radio tamper
No wireless device supervision		■		■	SUPERVISION device (DDxx:name)	Tamper	Radio tamper
Enter menu with installer code			■				
Open input		■			Inxxx:name IN customisation	Open input	
Test input opening			■	■	Inxxx:name INPUT OF TEST	Open input	
PO warning / arm partitions / enable-disable user or key / enable-disable output			■			PO warning	
Instantaneous lack of power					POWER INSTANT. (START/END)		
"Lack of power" after programmed timeout				■	POWER (START/END)	Lack of power	Power mains fault/restored
Arm/disarm partitions			■		EXECUTED or PARTIALLY DONE	Partition status	Armed Partition xx Disarmed partition xx

Cause	LED		Log	Memory	Description of the event (Event Log and Diagnose Log)	Auxiliary indication (controlled output)	Telephone message EN50131 NOT RELATED
	Keypad	Reader					
Override partition arming			■		SETT. OVERRIDDEN	Partition status	
System block, no mains power, battery not OK					ARREST SYSTEM		
Enter valid code on KPxx keypad			■		VALID CODE		
Edit date-time on KPxx keypad			■		Date Time + KPxx: name		
Enable/disable code			■		Start user enabling + KPxx: name		
Arm partition command not executed			■		NOT EXECUTED		Arming not executed
Hold-up alarm			■		ALARM HOLD-UP	Hold-up	Attack in progress
Inhibit tamper input					INHIB. TAMPER IN		

Table 18 - Detail of events and management

See paragraph *10.3 IDP message structure* for interpreting IDP messages.

10.5 FACTORY SETTINGS

10.5.1 System code

System code (for Hi-Connect)	55555555

10.5.2 Partitions

Partition number	1
Entry time	30 s
Exit time	30 s
Arming type	Sys Arm Block

10.5.3 Users

MP500/4N	MP500/8	MP500/16	Default	Name	Enabled	Assigned partitions
Installer	**Installer**	**Installer**	000000	**Installer**	Power ON	SYSTEM
Tech. Manager	**Tech. Manager**	**Tech. Manager**	222222	**Tech. Manager**	--	SYSTEM
Master	**Master**	**Master**	111111	**Master**	Always	SYSTEM
User 2	**User 2**	**User 2**	000020	**…**	---	1
User 3	**User 3**	**User 3**	000030	**…**	---	1
User …	**User …**	**User …**	000…	**…**	---	1
User 14	**User …**	**User …**	000140	**…**	---	1
	User 30	**User 30**	000300	**…**	---	1
	--	**User …**	000…	**…**	---	1
	--	**User 62**	000620	**…**	---	1

MP500/4N	MP500/8	MP500/16	Default
HOLD UP	**HOLD UP**	**HOLD UP**	Disabled

10.5.4 Keys

MP500/4N	MP500/8	MP500/16	Default	Name	Type	Enabled	Assigned partitions
Key 1	**Key 1**	**Key 1**	Not present	…	Change Partition Status	X	1
Key ...	**Key ...**	**Key ...**	Not present	…	Change Partition Status	X	1
Key 16	**Key 32**	**Key 64**	Not present	…	Change Partition Status	X	1

10.5.5 General parameters

Parameter	Value	Default
Alarm time (burglar, tamper, panic)		180 s
Pre-alarm time		180 s
Emergency time		180 s
Alarm counter		10
Lack of mains power		1h
Mode		MODE 2 (MP500/4N)
		MODE 3 (MP500/8 - MP500/16)

10.5.6 Areas

MP500/4N	MP500/8	MP500/16	Default	Name	Assigned partitions
Area A	**Area A**	**Area A**	Not present	**…**	1
Area B	**Area B**	**Area B**	Not present	**…**	2
---	**Area C**	**Area C**	Not present	**…**	3
---	**Area D**	**Area D**	Not present	**…**	4

10.5.7 Control panel inputs

MP500/4N control panel

Attrib.	Isolable	YES			
	Common input	OR			
	Release type	SINGLE			
Partition assignment		1	1	1	1
Customisation		Entry Exit	Immediate	Failure Sirens	Failure Detector
Type		D. Bal.	D. Bal.	D. Bal.	D. Bal.
Name		…	…	…	…
Logical address		01	02	03	04
Physical address		I 01	I 02	I 03	I 04

MP500/8 and MP500/16 control panels

Attrib.	Isolable	YES							
	Common input	OR							
	Release type	SINGLE							
Partition assignment		1	1	1	1	1	1	1	1
Customisation		Entry Exit	Immediate	Immediate	Immediate	Communicator fault	Jamming	Failure Sirens	Failure Detector
Type		D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.
Name		…	…	…	…	…	…	…	…
Logical address		01	02	03	04	05	06	07	08
Physical address		I 01	I 02	I 03	I 04	I 05	I 06	I 07	I 08

10.5.8 Control panel outputs

MP500/4N control panel

Partition assignment	SYSTEM	SYSTEM
Customisation	Burglar	Tamper
Type	N.H.	N.H.
Name	…	…
Logical address	01	02
Physical address	O1	O2

MP500/8 and MP500/16 control panels

Partition assignment	SYSTEM	SYSTEM	SYSTEM	SYSTEM	SYSTEM	SYSTEM
Customisation	Burglar	Tamper	OR TC	System failure	Telephone failure	Low Battery
Type	N.H.	N.H.	N.H.	N.L.	N.H.	N.H.
Name	…	…	…	…	…	…
Logical address	01	02	03	04	05	06
Physical address	O1	O2	O3	O4	O5	O6

10.5.9 Expansion module inputs

Attrib.	Isolable	YES							
	Common input	OR							
	Release type	SINGLE							
Partition assignment		1	1	1	1	1	1	1	1
Customisation		Entry Exit	Immediate	Immediate	Immediate	Communicator fault	Jamming	Failure Sirens	Failure Detector
Type		D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.
Name		…	…	…	…	…	…	…	…
Logical address		Seq.	Seq.	Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Physical address		I n1	I n2	I n3	I n4	I n5	I n6	I n7	I n8

10.5.10 Expansion outputs

Partition assignment	SYSTEM	SYSTEM	SYSTEM
Customisation	Burglar	Tamper	OR TC
Type*	N.H.	N.H.	N.H.
Name	…	…	…
Logical address	Seq.	Seq.	Seq.
Physical address	O1	O2	O3

10.5.11 Keypad inputs

Attrib.	Isolable	YES	
	Common input	OR	
	Release type	SINGLE	
Partition assignment		1	1
Customisation		Entry Exit	Immediate
Type		Not used	Not used
Name		…	…
Logical address		Seq.	Seq.
Physical address		I n1	I n2

10.5.12 Radio expansion module inputs

For further details and information refer to the dedicated manual.

10.5.13 Radio expansion module outputs (sirens)

For further details and information refer to the dedicated manual.

10.5.14 Reader inputs

Attrib.	Isolable	YES	
	Common input	OR	
	Release type	SINGLE	
Partition assignment		System	1
Customisation		Tamper	Immediate
Type*		N.C.	Not used
Name		**…**	**…**
Logical address		Seq.	Seq.
Physical address		I n1	I n2

10.5.15 Keypad parameters

Keypads	Assigned partitions	Name	Exit time	Entry time
Keypad 1	System	…	X	X
Keypad …	System	…	X	X
Keypad 4 (MP500/4N)	System	…	X	X
Keypad …	System	…	X	X
Keypad 8	System	…	X	X

10.5.16 Reader-partition assignment

Readers	Name	LED 1 Assigned partitions	LED 2 Assigned partitions	LED 3 Assigned partitions	LED 4 Assigned partitions	Masking
Reader 1	**…**	1	---	---	---	Disabled
Reader …	**…**	1	---	---	---	Disabled
Reader 4 (MP500/4N)	**…**	1	---	---	---	Disabled
Reader …	**…**	1	---	---	---	Disabled
Reader 16	**…**	1	---	---	---	Disabled

10.5.17 Remote control key-partition assignment

KEYS	PARTITIONS	SPECIALISATIONS
Key 1	System	Arm partitions
Key 2	System	Not used
Key 3	System	Toggle
Key 4	System	Disarm partitions

10.5.18 Telephone dialler

Event	Burglar	x
	Tamper	x
	Partitions On/Off	X
	Maintenance	X
	Isolated inputs	X
	Lack of power	X
	Low battery	X
	System faults	X
	Wrong code	X
Sending type		IDP
Telephone line	PSTN	x
Partition assignment	1	SYSTEM

PARAMETER			**DEFAULT**
Vocal message sending mode			Mode 1
PSTN parameter	Nation		Italy
	PABX connection		disabled
	Tone Line Check		disabled
	Answer control		disabled
GSM parameter	SIM PIN		
	SIM Card Expiry		
	Incoming SMS		disabled
PSTN Line Test			ATS4 (*)
Period Comm Test			disabled
	hours		
	interval		
	telephone number		
Rem Ctrl Backup			disabled
Advanced	Answer Machine	PSTN	disabled
		GSM	Enabled (5 rings)
	Remote control code		66666666
	Return call		disabled
	Call delay		disabled
	Line enabling	PSTN	enabled
		GSM	disabled
		LAN	disabled
	Sending mode		Mode 1

(*) **MP500/4N control panel:** PSTN line test – Default= 24H.

10.5.19 Timed programmer

The timed programmer is deactivated by default.

10.6 TIMED PROGRAMMER CONFIGURATION

	Days						
Type	**Monday**	**Tuesday**	**Wednesday**	**Thursday**	**Friday**	**Saturday**	**Sunday**
Working day							
Pre-holiday							
Holiday							

Note: only one type may be selected for each day.

WORKING DAY COMMANDS		
Number	**Time**	**Type**
1	:	
2	:	
3	:	
4	:	
5	:	
6	:	
7	:	
8	:	

PRE-HOLIDAY DAY COMMANDS		
Number	**Time**	**Type**
1	:	
2	:	
3	:	
4	:	
5	:	
6	:	
7	:	
8	:	

HOLIDAY COMMANDS		
Number	**Time**	**Type**
1	:	
2	:	
3	:	
4	:	
5	:	
6	:	
7	:	
8	:	

ELKRON
Tel. +39 011.3986711 - Fax +39 011.3986703
www.elkron.com *– mail to: info@elkron.it*