GB

MP500/4N - MP500/16

Remote controllable alarm control panels

User Manual

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

DS80MP5L-023A LBT81214

The information contained in this manual was gathered and checked with care but the manufacturer cannot be held liable for errors or omissions.
The manufacturer reserves the right to implement improvements or changes to the products described in this manual without prior notice.

This manual may contain references or information on products (hardware or software) or services which are not yet on the market. These references and information do not imply that the manufacturer will market such products or services in the future.

Elkron is a trademark of URMET S.p.A.
All trademarks mentioned in this document are the property of their respective owners.

All rights reserved. Partial or total copies of this document are allowed for installing the MP500/4N or MP500/16 system only.

Tel. +39 011.3986711
www.elkron.com – mail to: info@elkron.it

TABLE OF CONTENTS

Introduction **8**
Conventions used 8

1 Control devices **9**
1.1 KP500D/N - KP500DV/N keypad display 9
1.1.1 Function keys *9*
1.1.2 LEDs and status icons *10*
1.1.2.1 Use of LEDs with EN50131 grade 3 compliance *11*
1.1.3 Partition indications *11*
1.1.4 Area indications *12*
1.2 KP500DP/N touch screen keypad - KP500D/ST 13
1.2.1 Function keys *14*
1.2.2 Status icons *14*
1.2.2.1 Use of LEDs and icons with EN50131 grade 3 compliance *15*
1.2.3 Partition indications *15*
1.2.4 Area indications *16*
1.3 DK500M-E electronic key readers 17
1.4 DK500M-P AND DK510M-P proximity key reader 18
1.5 RC500 remote control 19
1.6 RC600 remote control 20
1.7 KP600 keypad 21

2 System commissioning **22**
2.1 Arming procedure 22
2.2 Arming from KP500D/N and KP500DV/N keypads 22
2.2.1 Total arming (system with partitions only) *22*
2.2.2 Total arming (system with areas and partitions) *22*
2.2.3 Partial arming (system with partitions only) *23*
2.2.4 Partial arming (system with areas and partitions) *23*
2.3 Arming from KP500DP/N keypad - KP500D/ST 24
2.3.1 Total arming (system with partitions only) *24*
2.3.2 Total arming (system with areas and partitions) *24*
2.3.3 Partial arming (system with partitions only) *25*
2.3.4 Partial arming (system with areas and partitions) *25*
2.4 Arming with electronic or proximity key 26
2.4.1 Total arming from electronic key reader *26*
2.4.1.1 System in use mode = Mode 3 (EN50131 grade 3 compliant) *26*
2.4.1.2 System in use mode = Mode 2 or Mode 0 ..... *26*
2.4.2 Total arming from proximity key reader *26*
2.4.2.1 System in use mode = Mode 3 (EN50131 grade 3 compliant) *26*
2.4.2.2 System in use mode = Mode 2 or Mode 0 ..... *27*
2.4.3 Total arming from KP500DP/N keypad *27*
2.4.4 Partial arming from electronic key reader *27*
2.4.4.1 System in use mode = Mode 3 (EN50131 grade 3 compliant) *27*
2.4.4.2 System in use mode = Mode 2 or Mode 0 ..... *28*
2.4.5 Partial arming from proximity key reader *28*
2.4.5.1 System in use mode = Mode 3 (EN50131 grade 3 compliant) *28*
2.4.5.2 System in use mode = Mode 2 or Mode 0 ..... *28*
2.4.6 Partial arming from KP500DP/N keypad *28*
2.5 Arming using RC500 remote control 29
2.5.1 Total arming *29*
2.5.2 Partial arming *29*
2.6 Arming using RC600 remote control 30
2.6.1 Total arming *30*
2.6.2 Partial arming *30*
2.7 Arming using KP600 keypad 30
2.7.1 Total arming *30*
2.7.2 Partial arming *30*
2.8 Disarming procedure 31
2.9 Disarming from KP500D/N and KP500DV/N keypads 31
2.9.1 Total disarming (system with partitions only) *31*
2.9.2 Total disarming (system with areas and partitions) *31*
2.9.3 Partial disarming (system with partitions only) *32*
2.9.4 Partial disarming (system with areas and partitions) *32*
2.9.5 Disarming from keypad under hol-up *32*
2.10 Disarming from KP500DP/N keypad - KP500D/ST 33
2.10.1 Total disarming (system with partitions only) *33*
2.10.2 Total disarming (system with areas and partitions) *33*
2.10.3 Partial disarming (system with partitions only) *34*

2.10.4 Partial disarming (system with areas and partitions) ... 34
2.10.5 Disarming from keypad under hold-up ... 35
2.11 Disarming with electronic or proximity key ... 35
2.11.1 Total disarming from electronic key reader ... 35
2.11.1.1 System in use mode = Mode 3 (EN50131 grade 3 compliant) ... 35
2.11.1.2 System in use mode = Mode 2 or Mode 0 ... 35
2.11.2 Total disarming from proximity key reader ... 36
2.11.2.1 System in use mode = Mode 3 (EN50131 grade 3 compliant) ... 36
2.11.2.2 System in use mode = Mode 2 or Mode 0 ... 36
2.11.3 Total disarming from KP500DP/N keypad ... 36
2.11.4 Partial disarming from electronic key reader ... 36
2.11.5 Partial disarming from proximity key reader ... 36
2.11.6 Partial disarming from KP500DP/N keypad ... 37
2.12 Disarming using RC500 remote control ... 37
2.12.1 Total system disarming ... 37
2.12.2 Partial disarming with remote control ... 37
2.13 Disarming using RC600 remote control ... 38
2.13.1 Disarming ... 38
2.14 Disarming using KP600 keypad ... 38
2.14.1 Disarming ... 38
2.15 Splitting ... 38
2.16 Direct access function keys ... 39
2.16.1 KP500D/N and KP500DV/N keypads ... 39
2.16.2 KP500DP/N keypad - KP500D/ST ... 39
2.16.3 RC500 remote control programming key ... 39
2.16.4 RC600 remote control programming key ... 39
2.16.5 KP600 keypad programming key ... 39
2.17 How to stop alarms in progress ... 39
2.18 System status information ... 40
2.18.1 How to view system status ... 40
2.18.2 How to view the system status from the KP600 keypad ... 40
2.18.3 How to view open inputs ... 40
2.18.4 How to view isolated or inhibited inputs ... 41
2.18.5 How to examine the Alarms Memory ... 41
2.18.6 How to delete the Alarms Memory ... 41
2.18.7 How to examine the Tampers Memory ... 42
2.18.8 How to delete the Tampers Memory ... 42
2.18.9 How to examine the fault and anomaly memory ... 42
2.18.10 How to delete the fault memory ... 43
2.19 Postpone automatic activation ... 43
2.20 Service message ... 44
2.20.1 How to record a service message ... 44
2.20.2 How to play a service message ... 44

3 Failure to arm the system ... 45
3.1 System arming block ... 45
3.1.1.1 Example of overriding ... 46
3.1.1.2 Impossibility to override the arming block with open inputs ... 47

4 Alarms, events and indications ... 48
4.1 Alarm and event indications ... 48
4.1.1 How to use the table ... 48
4.1.1.1 Example of how to interpret the table ... 48
4.2 Description of alarms and indications ... 50
4.2.1 Burglar alarm ... 50
4.2.2 Burglar pre-alarm ... 50
4.2.3 Tamper alarm ... 51
4.2.4 Wrong code alarm ... 51
4.2.5 Panic indication ... 52
4.2.6 Silent panic indication ... 52
4.2.7 Hold-up indication ... 52
4.2.8 Emergency indication ... 53
4.2.9 Fire indication ... 53
4.2.10 Detector jamming alarm ... 54
4.2.11 Detector fault alarm ... 54
4.2.12 Faulty siren alarm ... 54
4.2.13 Failure alarm from failure input ... 55
4.2.14 System failure alarm ... 55
4.2.15 External communicator failure alarm ... 55
4.2.16 No Bus communication alarm ... 56
4.2.17 Protracted no mains power alarm ... 56
4.2.18 Control panel and other device low battery alarm ... 56
4.3 Description of events ... 57
4.3.1 Reset fire alarm event ... 57
4.3.2 Technological type 1 event ... 57

4.3.3 Technological type 2 event ... *57*
4.3.4 Technological type 3 event ... *57*
4.3.5 Door opener event ... *58*
4.3.6 Courtesy light event ... *58*
4.3.7 Instantaneous no mains power event ... *58*
4.3.8 Maintenance event ... *58*
4.3.9 Inhibit inputs event ... *58*
4.3.10 Isolated input event ... *59*
4.3.11 Arm/disarm partitions event ... *59*
4.3.12 Arm/disarm partitions override event ... *59*
4.3.13 Open input event ... *59*
4.3.14 Open input test event ... *59*
4.3.15 Arrest system event ... *59*
4.3.16 Valid code entered by user on keypad event ... *60*
4.3.17 Edit date-time on keypad event ... *60*
4.3.18 User code enable/disable event ... *60*
4.3.19 Key enable/disable event ... *60*
4.3.20 Key acquisition/deletion event ... *60*
4.3.21 Timed programmer warning event ... *60*
4.3.22 Arming block event ... *60*
4.3.23 Arming not executed event ... *60*
4.4 Description of acoustic indications ... 61
4.4.1 Entry/exit time indication ... *61*
4.4.2 Arming warning ... *61*
4.4.3 Gong ... *61*
4.4.4 System status by means of wireless sirens ... *61*
4.5 Description of VOCAL indications ... 61
4.5.1 Arming/disarming message ... *61*

5 Advanced system management ... 62
5.1 System access codes ... 62
5.1.1 Default access code ... *63*
5.1.2 Code change ... *64*
5.1.3 How to reset an access code ... *64*
5.1.4 Entering an invalid code or using an invalid key ... *65*
5.2 The menus ... 65
5.2.1 How to access menus ... *65*
5.2.2 How to navigate the menus ... *65*
5.3 Free access menu ... 66
5.4 Main menu ... 66
5.5 How to enter alphanumeric characters ... 67
5.6 Enabling and disabling ... 67
5.6.1 How to enable the Installer ... *67*
5.6.2 How to enable a user ... *68*
5.6.3 How to enable a key ... *68*
5.6.4 How to enable the Technical Manager code ... *69*
5.6.5 How to enable the timed programmer ... *69*
5.6.6 How to enable vocal messages ... *70*
5.6.7 How to enable remote access ... *70*
5.6.8 How to enable remote disarming ... *71*
5.6.9 How to disable the Installer ... *71*
5.6.10 How to disable a User ... *71*
5.6.11 How to disable a key ... *72*
5.6.12 How to disable the Technical Manager ... *72*
5.6.13 How to disable the timed programmer ... *72*
5.6.14 How to disable vocal messages ... *73*
5.6.15 How to disable remote access ... *73*
5.6.16 How to disable remote access ... *73*
5.7 How to set date and time ... 74
5.8 Event Log ... 75
5.8.1 How to interpret viewed data ... *75*
5.8.2 How to browse the Event Log ... *75*
5.9 Keypad customisation ... 76
5.9.1 LCD Info ... *76*
5.9.2 How to set the buzzer volume ... *76*
5.9.3 How to set the display contrast ... *77*
5.9.4 How to set backlighting ... *77*

6 Users and keys ... 78
6.1 Users ... 78
6.1.1 How to assign a user ... *78*
6.1.2 How to program a descriptive user name ... *79*

7 Telephone dialler ... 80
7.1 Alarm message sending sequence ... 80

7.2 Answering machines and call cycles ... 80
7.3 Telephone numbers ... 81
7.3.1 How to store a telephone number ... 81
7.3.2 How to edit a telephone number ... 82
7.3.3 How to delete a telephone number ... 83
7.4 SMS Text message ... 84
7.4.1 How to write SMS text messages ... 85
7.4.2 How to delete SMS text messages ... 86
7.5 End of telephone credit notice ... 86

8 User remote control ... 87
8.1 How to skip a telephone answering machine ... 87
8.2 Remote control with SMS text messages ... 87
8.3 How to activate commandable outputs at no cost ... 88
8.4 Remote control with guided vocal menu ... 88
8.5 List of VOCAL answer machine DTMF controls ... 89
8.6 Environmental listening ... 89

9 System test ... 90
9.1 Periodical tests ... 90
9.1.1 Input test ... 90
9.1.2 Output test ... 91
9.1.3 Battery test ... 91
9.1.4 Vocal call test ... 92
9.1.5 Alarm receiving centre call test ... 92
9.1.6 GSM Field Test ... 93
9.1.7 Environmental listening test ... 93
9.1.8 Radio device test ... 93

10 Quick guide to remote control ... 94

FIGURES

Figure 1 - KP500D/N and KP500DV/N keypads 9
Figure 2 - Display and status LEDs on KP500D/N and KP500DV/N keypads 10
Figure 3 - KP500DP/N keypad - KP500D/ST 13
Figure 4 - KP500DP/N - KP500D/ST keypad display and status icons 14
Figure 5 - DK500M-E electronic key readers 17
Figure 6 - DK500M-P and DK510M-P proximity key reader 18
Figure 7 - RC500 remote control 19
Figure 8 – RC600 remote control 20
Figure 9 – KP600 keypad 21

TABLES

Table 1 - KP500D/N and KP500DV/N keypad elements 9
Table 2 - KP500D/N and KP500DV/N keypad function keys 9
Table 3 - LEDs indication of KP500D/N and KP500DV/N keypads 10
Table 4 - LED indication visibility of KP500D/N and KP500DV/N keypads complying with EN50131 grade 3 11
Table 5 - KP500DP/N - KP500DP/N keypad elements 13
Table 6 - KP500DP/N - KP500D/ST keypad function keys 14
Table 7 - LED and icon indications of KP500DP/N - KP500D/ST keypad 14
Table 8 - LED indication visibility of EN50131 grade 3 compliant KP500DP/N - KP500D/ST keypad 15
Table 9 - Alarm system arming block override 46
Table 10 - Indication overview 49
Table 11 - Default access codes for MP500/4N 63
Table 12 - Default access codes for MP500/16 63
Table 13 - List of DTMF commands 89

INTRODUCTION

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>** **<Technician 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.

Pay attention to the following symbols:

This symbol indicates an important warning.

This symbol indicates advice.

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

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

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

EN50131 NOT RELATED — This symbol means that the function or device will not affect the EN50131 compliance grade.

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

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

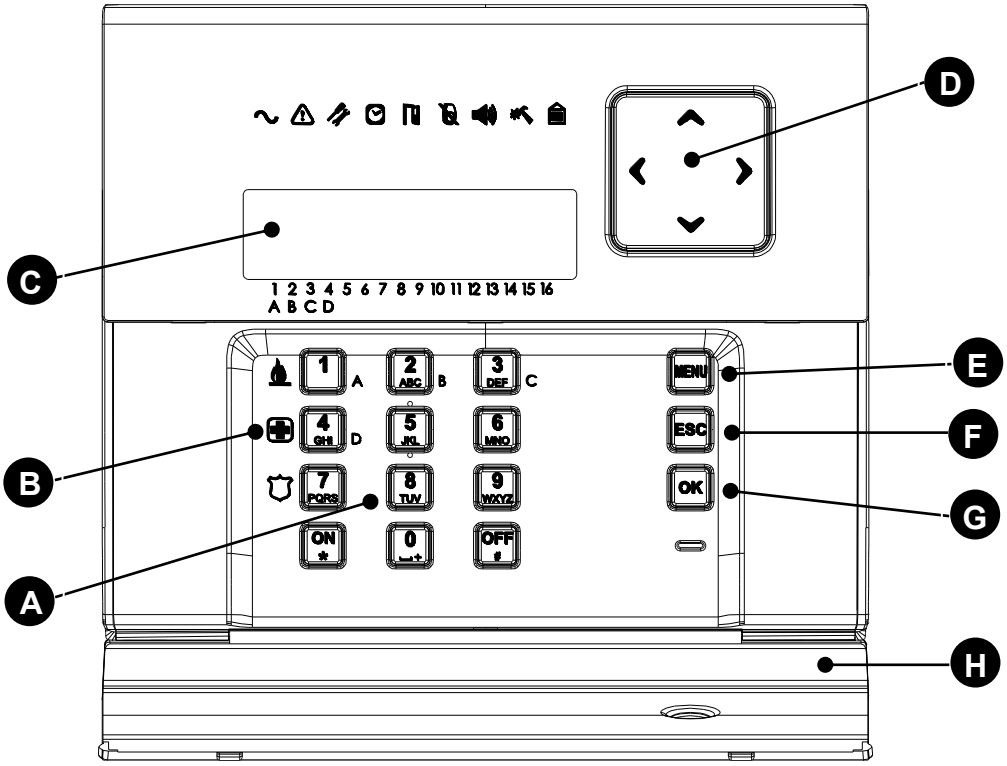


Figure 1 - KP500D/N and KP500DV/N keypads

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 compliance 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	Silent panic indication
	4 GHI	Emergency indication
	7 PQRS	Fire indication

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

1.1.2 LEDs and status icons

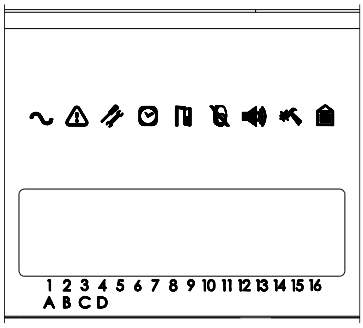


Figure 2 - Display and status LEDs on KP500D/N and KP500DV/N keypads

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

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 5.1 *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 indication of KP500D/N and KP500DV/N keypads

1.1.2.1 Use of LEDs with EN50131 grade 3 compliance

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! Mode 0 (currently present) cannot be used.

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 use 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.

```
AREAS STATUS
□□□□
1 2 3 4  5 6 7 8 9 10 11 12 13 14 15 16
A B C D
```

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.

```
AREAS STATUS
■□▩.
1 2 3 4  5 6 7 8 9 10 11 12 13 14 15 16
A B C D
```

1.2 KP500DP/N TOUCH SCREEN KEYPAD - KP500D/ST

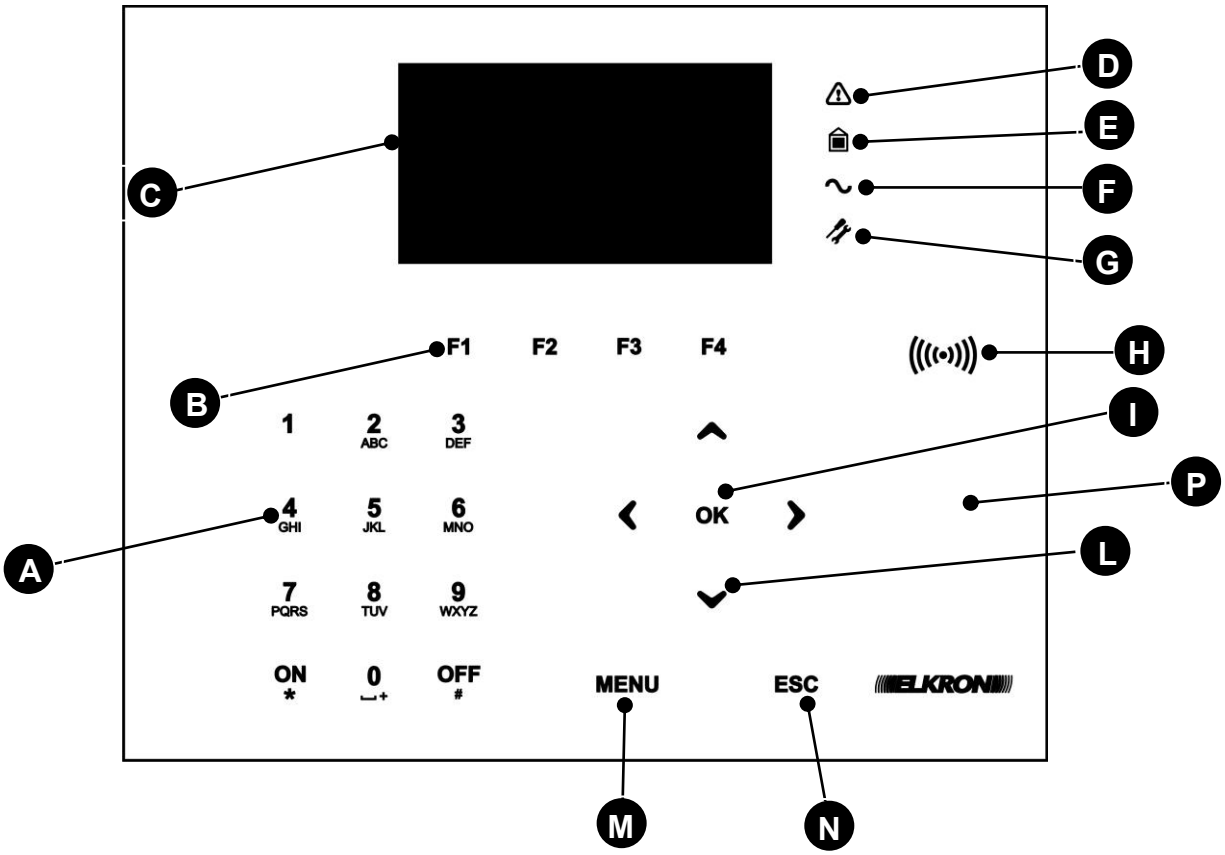


Figure 3 - KP500DP/N keypad - KP500D/ST

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 transponder

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

Table 5 - KP500DP/N - KP500DP/N 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 5.1 *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 compliance

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! Mode 0 (currently present) cannot be used.

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 a valid 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
	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

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

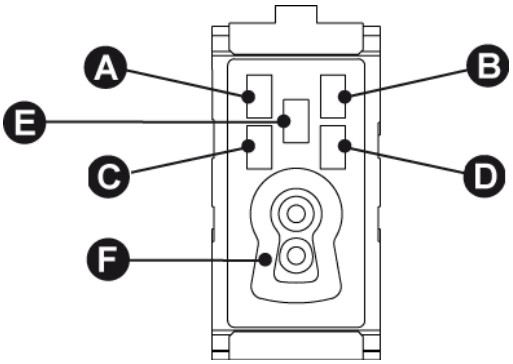


Figure 5 - DK500M-E electronic key readers

Ref.	Description	Use or indications provided	
		EN50131 grade = Mode 3	**EN50131 grade = 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

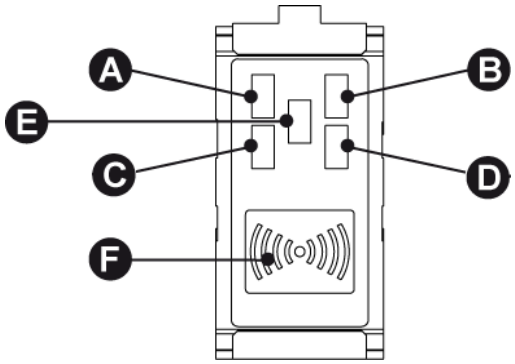


Figure 6 - DK500M-P and DK510M-P proximity key reader

Ref.	Description	Use or indications provided	
		EN50131 grade = Mode 3	**EN50131 grade = 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. <u>This LED lights up to indicate the need to check indication details on the keypad.</u>	• **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. <u>This LED lights up to indicate the need to check indication details on the keypad.</u>
F	Transponder	DK30 proximity key sensor for DK500M-P and DK70 proximity key for DK510M-P	

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 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

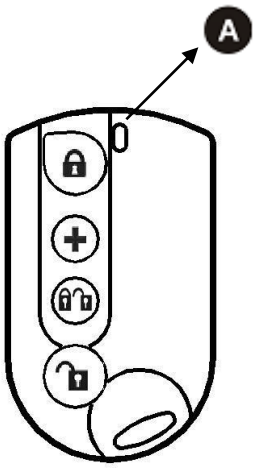


Figure 7 - RC500 remote control

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.*

1.6 RC600 REMOTE CONTROL

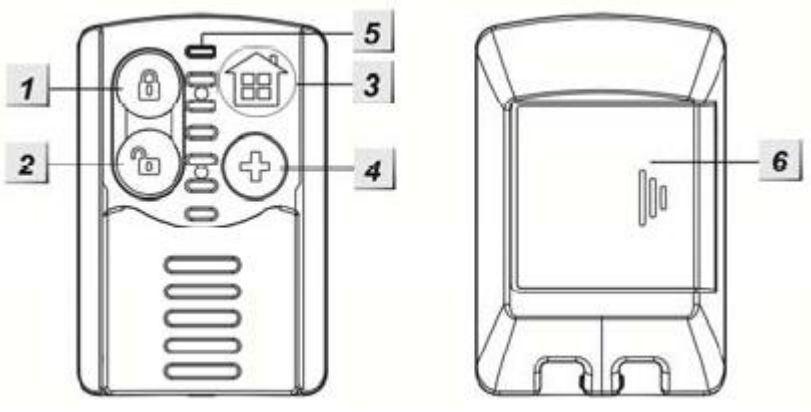


Figure 8 – RC600 remote control

Ref.	Description	Use or indications provided
	Key 1 Arm	Arms all associated partitions.
	Key 2 Disarm	Disarms all associated partitions.
	Key 3 Partial arming	Arms the associated partitions.
	Key 4 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.
5	Two-colour red/green LED	• **Red blinking** once and green once **=** the control requested by pressing the button was received and performed by the control unit • **LED blinking red six times and green once =** the control requested by pressing the GENERIC key was received and performed by the control unit. • **LED blinking red three times =** the control requested by pressing the key was NOT received and performed by the control unit. The indications disappear after short while.
6	Battery housing	The remote control is powered by a **CR2032** 3 V lithium battery

Note: *The ER600 radio expansion must be installed to use the remote control*.

1.7 KP600 KEYPAD

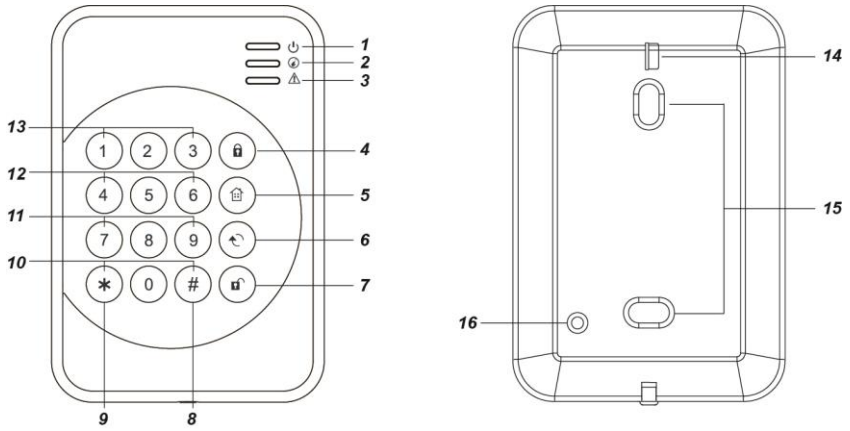


Figure 9 – KP600 keypad

Ref.	Description	Use or indications provided
1	Keypad state LED (blue/amber)	• Blue LED on for 5 seconds: the system is in normal operating mode. • The blue LED blinks for 5 seconds: it indicates flat battery in normal operating mode. • Amber LED on: the system is in test mode. • Amber LED blinking: in Test mode, this indicates flat battery.
2	System state LED (blue/red)	• Red LED on: the system is in Total Armed state. • Red LED blinking: the system is in Partial Armed state. • Blue LED on: the system is in disarmed state. • Blue LED blinking: error for the following reasons: ➢ No reply sent to control unit within 4 seconds. ➢ Incorrect error code. ➢ Request to pass to Partial Armed state when the Total Armed state. ➢ Forced arming request.
3	Future use	Not used
4	Total arming key	Enter a four-digit user code and press the key. If there are no faults and arming was successful, the red system state LED will light up and the keypad will beep.
5	Partial arming key	Enter a four-digit user code and press the key. If there are no faults and arming was successful, the red system state LED will light up and the keypad will beep.
6	System state request key	Indicated on system state LED (see indications provided by Ref. 2)
7	Disarming key	Enter a four-digit user code and press the key to disarm all associated partitions.
8-9	Not used	
10	Acquisition key	
11-12	Not used	
13	Function keys	Pressing the two keys at the same time will start the function associated to them
14	Battery isolator	
15	Mounting holes	
16	Tamper	

2 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 to arm and disarm the system and to clear the alarms, as explained in paragraph 5.6 *Enabling and disabling*.

2.1 ARMING PROCEDURE

The arm system may be armed in various manners, 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 5.1 *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.

2.2 ARMING FROM KP500D/N AND KP500DV/N KEYPADS

2.2.1 Total arming (system with partitions only)

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

1) Enter < Master / User code > and press [ON *]

```
ARM
□□□□•••••••••••••
```

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 again [ON *] if you do not want to wait for 5 seconds.

```
EXECUTED
■■■■•••••••••••••
```

3) 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.
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 arm only the assigned partitions and not necessarily all the partitions even with this procedure.

2.2.2 Total arming (system with areas and partitions)

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

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

```
1)AREAS
2)PARTITIONS
```

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]:

```
ARM
□□••
```

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.

```
EXECUTED
■■••
```

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 view immediately.

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

2.2.3 Partial arming (system with partitions only)

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

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

```
ARM
□□□□•••••••••••••
```

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.).).

```
EXECUTED
■□□■•••••••••••••
```

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 view immediately.

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

2.2.4 Partial arming (system with areas and partitions)

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

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

```
1)AREAS
2)PARTITIONS
```

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]:

```
ARM
□□••
```

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.

```
EXECUTED
■□••
```

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 view immediately.

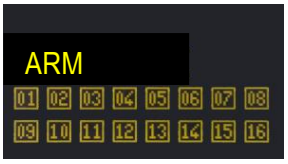
IMPORTANT! The user will arm only the assigned areas and not necessarily all the areas even with this procedure.

2.3 ARMING FROM KP500DP/N KEYPAD - KP500D/ST

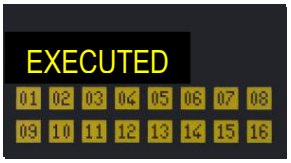
2.3.1 Total arming (system with partitions only)

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 view 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.

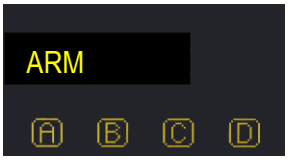
IMPORTANT! The user will arm only the assigned areas and not necessarily all the areas even with this procedure.

2.3.2 Total arming (system with areas and partitions)

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

1) Enter < Master / User 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.

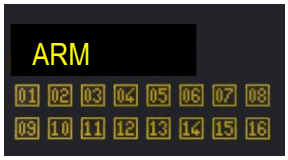


3) The keypad will beep. Press [ESC] to exit without arming. The status LED will light up after 5 seconds (fixed if all areas are armed, blinking if some areas are not armed). The squares will appear full indicating the areas which are not armed. The following will appear on the display:

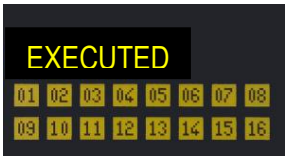
4) Press [ON *] again if you do not want to wait for 5 seconds.

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:

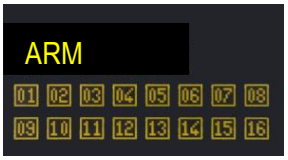


7) The display will go back to standard view automatically after one minute after arming both areas and partitions. Press [ESC] to go to standard view immediately.
8) For arming both areas and partitions, if programmed or if the system is EN50131 compliant, the keypad will sound long beeps initially followed by short beeps for the last 10 seconds.

2.3.3 Partial arming (system with partitions only)

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

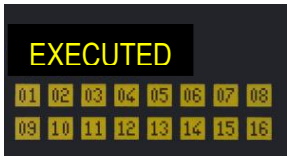
1) Enter < Master / User code > and press ON *.



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.

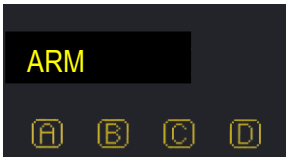
5) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.
6) If programmed or if the system is EN50131 compliant, the keypad will sound long beeps initially followed by short beeps for the last 10 seconds.

2.3.4 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 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.

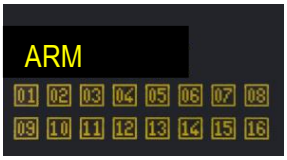


3) The keypad will beep. Press ESC to exit without arming.
4) Press the function keys (**F1**, **F2**, **F3** and **F4**) positioned under the areas to be armed: the respective squares of the areas will become full.
5) The status LED will light up after 5 seconds (fixed if all areas are armed, blinking if some areas are not armed). The 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:

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.

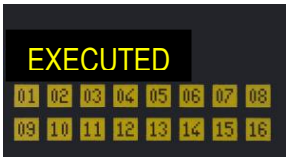
7) If **F4** (i.e. partitions) was pressed at the beginning of the procedure, an empty square will appear on the display for each programmed partition assigned to keypad and code which is not armed. Full squares indicate that the partition is armed. Circles indicate that the partition is disarmed and 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 view immediately.

12) 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.

2.4 ARMING WITH ELECTRONIC OR PROXIMITY KEY

2.4.1 Total arming from electronic key reader

IMPORTANT! This procedure can only be used if all partitions are disarmed.

2.4.1.1 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.

2.4.1.2 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.

2.4.2 Total arming from proximity key reader

IMPORTANT! This procedure can only be used if all partitions are disarmed.

2.4.2.1 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.

2.4.2.2 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.

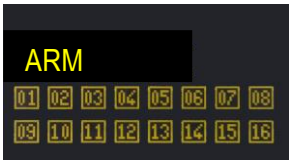
IMPORTANT! The key will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

2.4.3 Total arming from KP500DP/N keypad

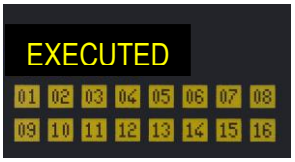
Proceed as follows to arm all partitions using the proximity key on a KP500DP/N keypad:

1) Approach the proximity key to the keypad.

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 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.

2.4.4 Partial arming from electronic key reader

2.4.4.1 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 proximity 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.

2.4.4.2 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 proximity 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.

2.4.5 Partial arming from proximity key reader

2.4.5.1 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.

2.4.5.2 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 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.

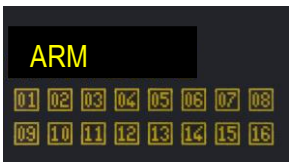
IMPORTANT! The key will arm only the assigned partitions and not necessarily all the partitions even with this procedure.

2.4.6 Partial arming from KP500DP/N keypad

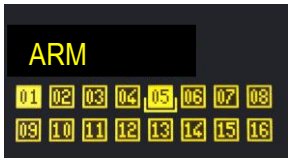
Proceed as follows to arm the partitions partially using the proximity key on a KP500DP/N keypad:

1) Approach the proximity key to the keypad.

2) The keypad will beep. Press **F4** within 5 seconds. Press ESC to exit without arming.

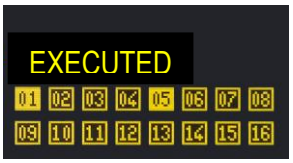


3) Enter the number of the partitions to be armed on the keypad: the respective squares will become full.



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 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.

2.5 ARMING USING RC500 REMOTE CONTROL

EN50131

2.5.1 Total arming

The remote control must have been duly programmed for all partitions to arm all the partitions in the system (see *Programming Manual*).

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: <u>any partitions which are disarmed will be armed</u>.
3. Pressing the key again will cause the system to be totally disarmed (the entire system, not only the armed partitions).

2.5.2 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 (see *Programming Manual*).

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: 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: <u>any partitions which are disarmed will be armed</u>.
3. Pressing the key again will cause the partitions to be totally disarmed (not only the previously armed partitions).

2.6 ARMING USING RC600 REMOTE CONTROL

2.6.1 Total arming

The remote control must have been duly programmed for all partitions to arm all the partitions in the system.

Press the button on the remote control to arm all partitions. If the control unit has accepted the command, the LED will light up red and then green.

2.6.2 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 the key on the remote control to arm the partitions to which the remote control is assigned. If the control unit has accepted the command, the LED will light up red and then green.

2.7 ARMING USING KP600 KEYPAD

2.7.1 Total arming

The keypad must have been duly programmed for all partitions and a four-digit user code is needed to arm all the partitions in the system.

To arm all partitions, enter the four-digit user code on the keypad and then press the key on the keypad. If the control unit has received the command, the two-colour system LED on the keypad will light up red fixed for approximately 4 seconds to indicate the state of the partitions.

WARNING! The arming and disarming operations from KP600 keypad require the use of four-digit user codes only. Five or six digit codes cannot be used.

2.7.2 Partial arming

The partial arming of only some partitions in the system is possible only if the keypad has been duly programmed for all partitions and a 4-digit user code is available.

Press the key on the keypad to arm the partitions with which the keypad was associated. If the control unit has received the command, the two-colour system LED on the keypad will light up red fixed for approximately 4 seconds to indicate the state of the partitions.

WARNING! The arming and disarming operations from KP600 keypad require the use of four-digit user codes only. Five or six digit codes cannot be used.

2.8 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 *5.1 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.

2.9 DISARMING FROM KP500D/N AND KP500DV/N KEYPADS

2.9.1 Total disarming (system with partitions only)

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

1) Enter <Master / User code> [OFF #].

```
DISARM
■■■■••••••••••••
```

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.

```
EXECUTED
□□□□••••••••••••
```

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.

2.9.2 Total disarming (system with areas and partitions)

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

1) Enter <Master / User code> [OFF #].

```
1)AREAS
2)PARTITIONS
```

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]:

```
DISARM
■■□□
```

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:

```
EXECUTED
□□□□
```

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.

2.9.3 Partial disarming (system with partitions only)

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

1) Enter <Master / User code> [OFF #].

```
DISARM
■□□■••••••••••••
```

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.

```
EXECUTED
□□□■••••••••••••
```

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.

2.9.4 Partial disarming (system with areas and partitions)

Proceed as follows to disarm the alarm system partially if areas are defined:

1) Enter <Master / User code> [OFF #].

```
1)AREAS
2)PARTITIONS
```

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]:

```
DISARM
■■••
```

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.

```
EXECUTED
■□••
```

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.

2.9.5 Disarming from keypad under hol-up

On MP500/4N and MP500/16 control panels, starting from control panel SW version 1.01, if the hold-up function has been enabled 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 you are under hold-up, 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.

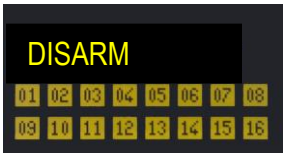
IMPORTANT! Enabling the hold-up function will cancel EN50131 compliance.

2.10 DISARMING FROM KP500DP/N KEYPAD - KP500D/ST

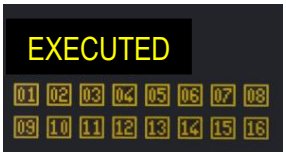
2.10.1 Total disarming (system with partitions only)

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

1) Enter < Master / User 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:



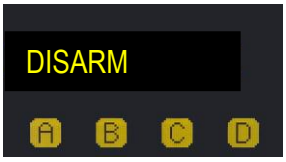
3) Press OFF # again if you do not want to wait for 5 seconds.
4) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

2.10.2 Total disarming (system with areas and partitions)

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

1) Enter < Master / User 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.

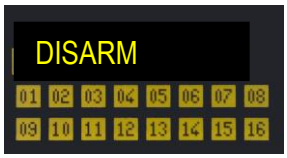


3) The keypad will beep. Press ESC to exit without disarming. After 5 seconds, the status LED will switch off and the squares will become empty indicating that the areas have been disarmed. Any half-full squares indicate that the area is partially armed. The following will appear on the display:

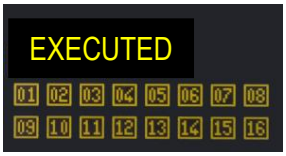
4) Press OFF # if you do not want to wait for 5 seconds.

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:

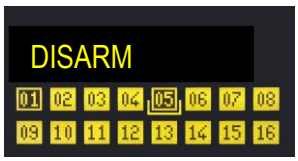


7) Press OFF # again if you do not want to wait for 5 seconds.
8) The display will go back to standard view automatically after one minute. Press ESC to go to standard view immediately.

2.10.3 Partial disarming (system with partitions only)

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

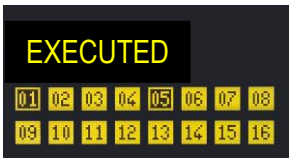
1) Enter < Master / User code > and press OFF #
2) The keypad will beep. Press ESC to exit without disarming. The following will appear on the display:



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.

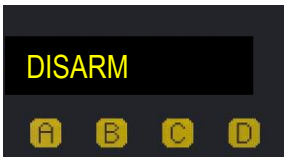
IMPORTANT! The user will disarm only the assigned partitions and not necessarily all the partitions even with this procedure.

2.10.4 Partial disarming (system with areas and partitions)

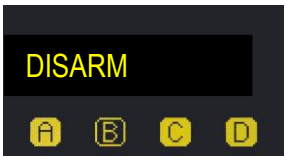
Proceed as follows to arm the entire alarm system if areas are defined:

1) Enter < Master / User 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:

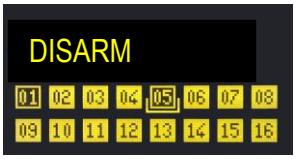


5) After 5 seconds, the status LED will switch off and the squares will become empty indicating that the areas have been disarmed. The following will appear on the display:

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.

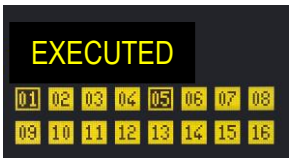
7) If **F4** was pressed, the following will appear on the display:



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.

2.10.5 Disarming from keypad under hold-up

On MP500/4N and MP500/16 control panels, starting from control panel SW version 1.01, if the hold-up function has been enabled 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 you are under hold-up, 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.

2.11 DISARMING WITH ELECTRONIC OR PROXIMITY KEY

2.11.1 Total disarming from electronic key reader

2.11.1.1 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.

2.11.1.2 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.

2.11.2 Total disarming from proximity key reader

2.11.2.1 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.

2.11.2.2 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 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.

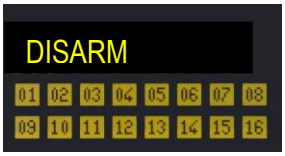
IMPORTANT! The key will disarm only the assigned partitions and not necessarily all the partitions even with this procedure.

2.11.3 Total disarming from KP500DP/N keypad

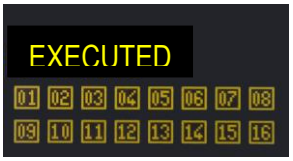
Proceed as follows to disarm all partitions using the proximity key on a KP500DP/N keypad:

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 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.

2.11.4 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.

2.11.5 Partial disarming from proximity key reader

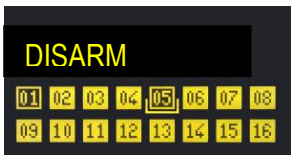
Follow the same procedure used for partial disarming from proximity key reader to partially disarm the system with a proximity key reader.

2.11.6 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.

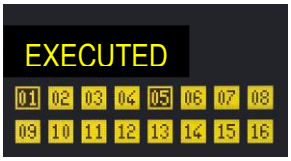
2) The keypad will beep. Press ESC to exit without disarming.



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 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.

2.12 DISARMING USING RC500 REMOTE CONTROL

EN50131

2.12.1 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.

2.12.2 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.

2.13 DISARMING USING RC600 REMOTE CONTROL

2.13.1 Disarming

The partial or total disarming of the partitions in the system is possible only if the remote control is duly programmed to do so.

Press to disarm the system totally or partially using the remote control. If the control unit has accepted the command, the LED will light up red and then green.

2.14 DISARMING USING KP600 KEYPAD

2.14.1 Disarming

The keypad must have been duly programmed and a four-digit user code is needed to disarm the partitions in the system totally or partially.

To disarm the system totally or partially using the keypad, enter the four-digit user code and then press the key. If the control unit has received the command, the keypad will indicate the state of the partitions by switching off the two-colour system LED.

IMPORTANT! The arming and disarming operations from KP600 keypad require the use of four-digit user codes only. Five or six digit codes cannot be used.

2.15 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 code >, press OK and then MENU.

```
UT02:...
SYSTEM STATUS
```

2) Press OK. The empty squares indicate a disarmed partition, the full squares indicate an armed partition.

```
SE01:
□■□□□••••••••••••
```

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.

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

2.16 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

2.16.1 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.

2.16.2 KP500DP/N keypad - KP500D/ST

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.

2.16.3 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 alarm event.

2.16.4 RC600 remote control programming key

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.

2.16.5 KP600 keypad programming key

During programming, a direct access function can be associated with the simultaneous pressing of keys 1 and 3, e.g. to activate or deactivate a specific output or a technological function (fire, emergency, panic, silent panic). Hold keys 1 and 3 pressed for at least five seconds to generate the respective event.

2.17 HOW TO STOP ALARMS IN PROGRESS

The procedure for stopping an alarm is shown in detail in paragraph 4.2 *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 SP4 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.

2.18 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.

2.18.1 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 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.

2.18.2 How to view the system status from the KP600 keypad

The system state can be viewed on the KP600 keypad by directly pressing the key. The "System state" LED will light up as follows when the keypad key is pressed:

- Red LED on: the system is in Total Armed state.
- Red LED blinking: the system is in Partial Armed state.
- Blue LED on fixed: the system is disarmed.

2.18.3 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 code>, press OK twice and then press ▼ repeatedly until OPEN INPUTS appears.

```
UT02:...
OPEN INPUTS
```

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".

```
OPEN INPUTS
IN001:...
```

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.

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

2.18.4 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 code>, press OK twice and then press ⌄ repeatedly until ISOLATED INPUTS appears.

```
UT02:...
ISOLATED INPUTS
```

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".

```
ISOLATED INPUTS
IN001:...
```

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.

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

2.18.5 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 code>, press OK twice and then press ⌄ repeatedly until ALARMS MEM appears.

```
UT02:...
ALARMS MEM
```

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".

```
ALARMS MEM
IN001:...
```

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.

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

2.18.6 How to delete the Alarms Memory

Proceed as follows to delete the Alarms Memory:

1) Enter <Master / User code>, press OK twice and then press ⌄ repeatedly until ALARMS MEM appears.

```
UT02:...
ALARMS MEM
```

2) Press OK. The alarm LED will blink.

```
ALARMS MEM
IN001:...
```

3) Use ⌄ and ⌃ to scroll the list of inputs which caused the alarm.
4) The following after examining the list:

```
ALARM
DELETE MEMORY?
```

5) Press OK to delete the Alarms Memory.
6) Press ESC repeatedly to exit from the menu.

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

2.18.7 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 code>, press OK twice and then press ▼ repeatedly until TAMPERS MEM appears.

```
UT02:...
TAMPERS MEM
```

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”.

```
TAMPERS MEM
IN001:...
```

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.

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

2.18.8 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.

```
UT02:...
TAMPERS MEM
```

2) Press OK. The tamper LED will blink.

```
TAMPERS MEM
IN001:...
```

3) Use ▼ and ▲ to scroll the list of inputs which caused the alarm.
4) The following after examining the list:

```
ALARM
DELETE MEMORY?
```

5) Press OK to delete the Tampers Memory.
6) Press ESC repeatedly to exit from the menu.

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

⚠ **IMPORTANT!** A tamper event which is still present cannot be deleted.

2.18.9 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 code >, press OK twice.

```
UT02:...
FAULT
```

2) Press OK. The fault LED will blink.

```
LOW BATTERY
CONTROL PANEL
```

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.

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

2.18.10 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 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.

```
UT02:...
FAULT
```

```
LOW BATTERY
CONTROL PANEL
```

```
FAILURE
DELETE MEMORY?
```

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

2.19 POSTPONE AUTOMATIC ACTIVATION

Times and actions to be performed are set by the installer during programming on the timed programmer.

For instance, automatic arming of the alarm system may be programmed but it could be necessary to delay actual arming. This can be achieved without changing the timed programmer configuration.

Arming can be postponed by 30, 60 or 90 minutes during the warning time (which can be configured during programming) before the burglar alarm system is automatically armed by the timed programmer. This operation can be repeated several times before midnight.

The warning time is indicated on the keypads (buzzer sounding and the P.O. LED blinking). The "arming warning" outputs are also activated.

Proceed as follows to postpone automatic arming:

1) Enter <Master / User code>, press OK twice and then press ▼ repeatedly until MOVE COMMAND appears.
2) Press OK.
3) Press ▼ and ▲ to select the delay time. Press OK to confirm.
4) The P.O. LED on the keypad will stop blinking.
5) Press ESC repeatedly to exit from the menu.

```
UT01:MASTER
MOVE COMMAND
```

```
MOVE COMMAND
 30min
```

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

2.20 SERVICE MESSAGE

A service message up to 10 seconds long may be recorded on vocal keypads. The message can be played from any vocal keypad and is played automatically whenever the system is disarmed. See paragraph 5.6 *Enabling and disabling* for how to enable vocal messages. The service message is a sort of "vocal Post-it®".

2.20.1 How to record a service message

Proceed as follows to record the service message:

1) Press MENU.

```
SYSTEM STATUS
SERVICE MESSAGE
```

2) Press OK.

```
ENTER CODE
```

3) Enter < Master / User code > and press OK.

```
SERVICE MESSAGE
PLAY
```

4) Press ✓.

```
SERVICE MESSAGE
RECORD
```

5) Press OK.

```
RECORD
IN PROGRESS...
```

6) Speak at a distance of approximately 20cm from the keypad. Recording is interrupted automatically after 10 seconds.

7) Press ESC repeatedly to exit from the menu.

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

TIP. Play the message back to test that it is recorded properly.

2.20.2 How to play a service message

Proceed as follows to play the service message:

1) Press MENU.

```
SYSTEM STATUS
SERVICE MESSAGE
```

2) Press OK.

```
ENTER CODE
```

3) Enter < Master / User code > and press OK.

```
SERVICE MESSAGE
PLAY
```

4) Press OK.

```
PLAY
IN PROGRESS...
```

5) Press ESC repeatedly to exit from the menu.

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

3 FAILURE TO ARM THE SYSTEM

This chapter contains a detailed description of reasons which could prevent the alarm system from being armed and provide the solutions to be adopted.

3.1 SYSTEM ARMING BLOCK

An EN50131 compliant burglar alarm system cannot be armed if certain conditions are present. More specifically, the system cannot automatically "ignore" the blocking conditions and be armed all the same. The blocking conditions, with some restrictions, may be overridden and consequently bypassed by means of specific manual commands imparted by the user or by the installer.

The purpose is to prevent false alarms or false feelings of security because the system would not always be able to indicate break-in attempts in these conditions.

The conditions which prevent system arming are:

- One or more open burglar inputs in the partitions to be armed.
- One or more jammed motion detectors in the partitions to be armed (not applicable for MP500/4N).
- Tampering of one or more open inputs or devices in the partitions to be armed.
- Interconnection (e.g. line) faults.
- Primary power failure (no electricity from the mains).
- Secondary power failure (batteries not working perfectly).
- Alarm transmission device failure (SP4 or PSTN telephone interface)
- Alarm signalling device failure (sirens)
- Failure of all alarm transmission and signalling devices.
- Battery charger fault.

The electronic and proximity keys, the timed programmer and the special key input will not arm the alarm system in these cases. The failure to arm event caused by the block is stored in the Events Log with a description of the reason.

You can attempt to override the block and arm the system all the same by operating on the alarm system using the keypad.

The cause or causes which prevent arming will appear on the keypad display. You can try to eliminate the causes of the block, for example by closing the open inputs, or force the block with the keypad by checking each block, overriding them one by one with subsequent confirmations, force the block.

The block override operation is stored step by step in the Events Log.

IMPORTANT! It is not always possible to override the arming block. The possibility of overriding depends on the access code used, as shown in *Table 9 - Alarm system arming block override.*
Some causes and conditions prevent overriding and cannot be bypassed even using the Installer code. In these cases, remove the causes which prevent arming the system before arming it.
Furthermore, you cannot override the arming block in one step. You must override the single blocks one by one.

IMPORTANT! The arming block will be overridden until the system is disarmed. The override will be end when the system is disarmed and must be repeated when the system is armed again. The event is stored in the Events Log and the end of the override.

IMPORTANT! Overriding the arming block is a <u>temporary solution to allow to arm the alarm system</u> also when conditions which may compromise efficacy are present. It is advisable to remove the causes of the arming block and to restore perfect efficacy of the system as soon as possible.

The possibility of overriding the block depends on the access level and the cause of the block.

The override possibilities are shown in the table.

Arming block condition	Access code that can override arming	
	Level 2 (Master and User)	**Level 3 (Installer and Technical Manager)**
Open burglar input	■	■
Jammed motion detector	■	■
Faulty motion detector	■	■
Tampered input or device		■
Interconnection faults		■
Primary power failure	■	■
Secondary power failure	■	■
Alarm transmission device failure		■
Alarm signalling device failure (sirens)		■
Failure of all alarm transmission and signalling devices		■
Battery charger failure	■	■

Table 9 - Alarm system arming block override

3.1.1.1 Example of overriding

In this example, we will describe a system with four partitions (no areas): partition 1 has 3 inputs and the inputs 2 and 3 of partition 1 are open. In this case, the arming sequence performed by a normal user will be:

1) Enter **< User code >** and press [ON *]. The keypad will beep and the partitions assigned to the user will appear on the display. **0** will appear next to partition 1 because some inputs are open.

```
ARM
0□□□••••••••••••
```

2) The first input which is open will appear in the list and a prompt asking whether you want to inhibit it will appear. Press [OK] to inhibit it.

```
INHIBIT   OK?
IN002:...
```

3) The second input which is open will appear in the list and a prompt asking whether you want to inhibit it will appear. Press [OK] to inhibit it.

```
INHIBIT   OK?
IN003:...
```

4) Press [OK] to confirm inhibiting.

```
SETT. OVERRIDDEN
ARE YOU SURE?
```

5) The message shown here appears. See paragraph 3.1.1.2 *Impossibility to override the arming block with open inputs* if the message is different or alarm notifications appear at the end of the procedure.

```
EXECUTED
■■■■••••••••••••
```

3.1.1.2 Impossibility to override the arming block with open inputs

The arming can be overridden with open burglar inputs, providing that:

- fewer than 70% of the inputs of the concerned partition are open;
- the inputs are configured as “isolable” during programming, and
- the open inputs are not customised as First Entry/Last Exit, Last Exit or Delayed.

In our example, the following would occur if one or more of these conditions are not respected:

- The message shown here appears. In this case, partition 1 (the partition with the open inputs) will not be armed but the other partitions will be armed. In other words, the system is only partially armed. This will occur if more than 70% of the inputs of the partition are open or if any input is "not isolable”.

```
PARTIALLY DONE
0■■■•••••••••••••
```

- The message shown here and the alarm warnings will appear. This occurs if one of the open inputs is programmed as First Entry/Last Exit, Last Exit or Delayed.

```
EXECUTED
■■■■••••••••••••
```

Arming will not be possible, even by overriding, if more than 70% of the inputs are open or if an input is not "isolable". You will need to attempt to close some of the open inputs (some inputs could be left open deliberately and not because of a fault of the detector).

In other words, if a partition has 10 assigned inputs, it can be overridden and armed if 7 “isolable” inputs are open but this will not be possible if 8 inputs are open (or if there are fewer than 7 open inputs, but one or more of them is “not isolable”).

The customised First Entry/Last Exit, Last Exit or Delayed inputs are ignored by the control panel when the open inputs are checked during arming. Their feature is to be able to be or remain open to allow users to leave the protected rooms. For this reason, you will not be asked to inhibit them and when the alarm system is eventually armed at the end of the delay time, the control panel will detect an open burglar input and trip the alarm.

IMPORTANT! The max. 70% open input check is performed, partition by partition, on the total of the inputs of the single partition and not on the entire system.

Only burglar inputs are taken into consideration. Technological, fire alarm, panic alarms, for instance, will be ignored because whether they are open or closed is irrelevant for the purposes of system arming. For this reason, these inputs are not included in the 70% count.

4 ALARMS, EVENTS AND INDICATIONS

This chapter contains a detailed description of the alarms, events and indications managed by MP500/4N and MP500/16 control panels.

4.1 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.

4.1.1 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 (for example DK – EP).

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.

4.1.1.1 Example of how to interpret the table

The LED ⚠ may light up for several different reasons. Read the Event Log or Diagnose Log (see paragraph 2.18.9 *How to examine the fault and anomaly memory*) 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 4.2 *Description of alarms and indications* and paragraph 4.2.18 *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 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			■		START MAINTENANCE KPxx: name UT00: name		
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		

* 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 10 - Indication overview

4.2 DESCRIPTION OF ALARMS AND INDICATIONS

4.2.1 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. See the "*Programming Manual*" for more information.

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! The “Alarm Count” function is activated and configured to comply with EN50131 by default on MP500/4N and MP500/16 control panels. Changing this configuration will cancel EN50131 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. • Activates 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.

4.2.2 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.

4.2.3 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.

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 pre-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.

4.2.4 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.

4.2.5 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.

4.2.6 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.
It lasts ...	• For the burglar/tamper/panic alarm time.
It is stopped ...	• 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.

4.2.7 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.

4.2.8 Emergency indication

The MP500/16 control panel 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.

4.2.9 Fire indication

The MP500/4N and MP500/16 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.

4.2.10 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.

4.2.11 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.

4.2.12 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.

4.2.13 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 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 end of fault in the Event Log. • Deactivates the programmed failure outputs.

4.2.14 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.

4.2.15 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 tel. 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.

4.2.16 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 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.

4.2.17 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.

4.2.18 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.

4.3 DESCRIPTION OF EVENTS

An event is a voluntary or involuntary occurrence managed by MP500/4N and MP500/16 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.

4.3.1 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.

4.3.2 Technological type 1 event

The MP500/4N 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 and courtesy light 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.

4.3.3 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.

4.3.4 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.

4.3.5 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.

4.3.6 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.

4.3.7 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 *Installation Manual* for more details.

4.3.8 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 *Installation Manual* for more details.

4.3.9 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.

4.3.10 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.

See *Programming Manual* for more details.

4.3.11 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.

4.3.12 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.

4.3.13 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...	• 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.

4.3.14 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.

4.3.15 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).

4.3.16 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.

4.3.17 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.

4.3.18 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.

4.3.19 Key enable/disable 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.

4.3.20 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.

4.3.21 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).

4.3.22 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.

4.3.23 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.

4.4 DESCRIPTION OF ACOUSTIC INDICATIONS

If appropriately programmed, the keypads can emit auditory indications following given events.

4.4.1 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.

4.4.2 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.

4.4.3 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. • Programmed gong outputs which have at least one partition in common for one second.

4.4.4 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.

4.5 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.

4.5.1 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: input 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.

5 ADVANCED SYSTEM MANAGEMENT

This chapter contains information for complete system management including the procedures which are used less frequently that the system arming and disarming procedures.

5.1 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 installer 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! Through 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 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 when user code is modified automatically, the system will also assign 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.

5.1.1 Default access code

MP500/4N 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	Assigned 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 11 - Default access codes for MP500/4N

Code type	Level	Default code	Assigned partitions	Enabled when leaving the factory	Enable time (once enabled)
Manager	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 12 - Default access codes for MP500/16

5.1.2 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.

```
UT02:...
SYSTEM STATUS
```

2) Press ▼ repeatedly until SETTINGS appears.

```
UT02:...
SETTINGS
```

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

```
SETTINGS
CHANGE CODE
```

4) Press OK.

```
CHANGE CODE
NEW:     ------
```

5) Enter the new code, from four to six digits, and press OK.

IMPORTANT! Through 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
```

5.1.3 How to reset an access code

An access code can be reset to its default value if a user forgets it (see paragraph 5.1.1 *Default access code*).

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
```

5.1.4 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.

5.2 THE MENUS

All system configuration and enabling operations are performed using menus. The operations for accessing and navigating menus are described below.

5.2.1 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.

5.2.2 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 device 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.

5.3 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 vocal keypads (KP500DV/N) and the optional SV500N board must be installed in the control panel. See paragraph 2.20 *Service message* 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 paragraph 5.9.1 *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 paragraph 5.9.2 *How to set the buzzer volume* for more details.
- **SET CONTRAST**. This is used to adjust the contrast of the display. See paragraph 5.9.3 *How to set the display contrast* for more details.
- **SET BACKLIGHT**. This is used to adjust the backlighting intensity of the display. See paragraph 5.9.4 *How to set backlighting* for more details.

5.4 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.
As shown in the diagram below, the Master (**M**) has access to more options and functions than other users (**U**). In other words, the Master can do everything the other users can do, and more.

There may be differences for Master and User in the submenus as well. For example, they can both access the SETTINGS menu, but only the Master can access the submenus for enabling or disabling users, keys and other functions.

M U	SYSTEM STATUS		→	Submenu...	This shows the system status and can be used to change the partition status.
M U #	EVENT LOG		→	Submenu...	This is used to read the list of events stored on the control panel.
M U #	SETTINGS		→	Submenu...	This is used to isolate inputs, set the current date and time, configure the users or reset codes to default value, configure electronic and proximity keys and configure the timed programmer.
M #	ENABLE		→	Submenu...	This is used to enable and disable users, keys, timed programmer and remote access.
M #	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, vocal calls to and from Alarm Receiving Centres the GSM signal and the telephone call dialler separately.
M #	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.

#: accessible with the system disarmed only.

5.5 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 be 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 + -

5.6 ENABLING AND DISABLING

Installers and normal users must be enabled to operate on the system. Only the Master is always enabled. The Master can enable and disable the other users and the keys (electronic and proximity) and can enable and disable particular system functions.

The procedure for enabling and disabling users and key is described in detail below. Users and keys must be configured during programming, i.e. to specify what they can do. However, their "capabilities" will be put on hold until the Master authorises to use them. Similarly, the Master can revoke the authorisation and put the "capabilities" back on-hold at any time. Enabling and disabling means authorising and revoking authorisations. It is important to note that disabling does not means deleting the configuration made during programming but simply suspending it. Indeed, a previously disabled user or key (electronic or proximity) may be enabled again and immediately require all their "capabilities".

ADVICE: The user code and key enabling and disabling procedures are very useful particularly in combination with the timed programmer to permit entry restricted in time to the protected rooms.

An example will help understanding the concepts of configuration, programming, enabling and disabling in greater detail.

Everyone of us has many keys: to open the gate, the garage door, the front door, the car, the basement, the utility room, the bicycle lock etc. Each key lets you open or use something. In an alarm system, you have functions which let you do something instead of keys.

A set of keys can be put on a key ring and each key ring will allow to do some things and not others. For example, we could make one set with the garage key and the bicycle padlock key and another set with the garage key and the car key. Both sets of keys will open the garage but the vehicle you can use will be different. Configuration is the equivalent for the set of keys and programming is the procedure used to make each set.

The enabling and disabling actions used for the alarm system are equivalent to giving the keys to someone or taking them away.

Enabling and disabling applies to other functions in the system, and not only users and keys. The functions can be easily made operational or not without needing to program the configurations again.

5.6.1 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
```

5.6.2 How to enable a user

Each user must have been previously enabled to work on the system.

Proceed as follows to enable a user:

1) Enter **<Master code>**, press OK, then MENU and finally press ▼ repeatedly until ENABLE appears.
2) Press OK and then ▼ several times until USER appears.
3) Press OK.
4) Press ▼ and ▲ to select the user. Press OK to confirm.
5) Press OK. If, necessary, press ▼ to make ENABLE appear.
6) Press OK to enable the user.
7) Press ESC repeatedly to exit from the menu.

```
UT01:MASTER
ENABLE
```

```
ENABLE
USER
```

```
USER
UT02:...
```

```
UT02:...
ENABLE/DIS USER
```

```
ENABLE/DIS USER
ENABLE
```

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

5.6.3 How to enable a key

Each key must have been previously enabled to work on the system.

IMPORTANT! Each key must have been previously acquired to be enabled.

Proceed as follows to enable a key:

1) Enter **<Master code>**, press OK, then MENU and finally press ▼ repeatedly until ENABLE appears.
2) Press OK and then ▼ several times until KEY appears.
3) Press OK.
4) Press ▼ and ▲ to select the key. Press OK to confirm.
5) Press OK. If, necessary, press ▼ to make ENABLE appear.
6) Press OK to enable the key.
7) Press ESC repeatedly to exit from the menu.

```
UT01:MASTER
ENABLE
```

```
ENABLE
KEY
```

```
KEY
KE01:...
```

```
KE01:...
ENABLE/DIS KEY
```

```
ENABLE/DIS KEY
ENABLE
```

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

5.6.4 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
```

5.6.5 How to enable the timed programmer

The timed programmer must have been previously enabled to be used. It can only be enabled if timed commands are programmed.

Proceed as follows to enable the timed programmer:

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 TIMED COMMANDS appears.

```
ENABLE
TIMED COMMANDS
```

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

```
TIMED COMMANDS
ENABLE
```

4) Press OK to enable the timed commands.

5) Press ESC repeatedly to exit from the menu.

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

5.6.6 How to enable vocal messages

EN50131 NOT RELATED

Proceed as follows to enable the vocal messages:

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 VOCAL MESSAGES appears.

```
ENABLE
VOCAL MESSAGES
```

3) Press OK.

4) Press ▼ and ▲ to select the vocal message to be enabled. FAILURE, PARTITION STATUS, SYSTEM STATUS, SERVICE MESSAGE.

```
VOCAL MESSAGES
FAILURE
```

5) Press OK to confirm the selected message.

6) Press ▼ and ▲ to select ENABLE.

7) Press OK to enable the vocal message.

8) Repeat the steps from step 4 to enable other vocal messages. Press ESC repeatedly to exit from the menu.

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

5.6.7 How to enable remote access

EN50131

Remote access must be enabled to allow remote control of the system, e.g. for the installer to carry out maintenance operations.

Proceed as follows to enable remote access to the system:

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 ADVANCED appears.

```
ENABLE
ADVANCED
```

3) Press OK.

```
ADVANCED
REMOTE ACCESS
```

4) Press OK. If, necessary, press ▼ to make ENABLE appear.

```
REMOTE ACCESS
ENABLE
```

5) Press OK to enable remote access.

6) Press ESC repeatedly to exit from the menu.

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

5.6.8 How to enable remote disarming

Enabling remote disarming means being able to disarm the system either totally or partially, from a distance, e.g. to allow access to the rooms even if you are not physically present.
Proceed as follows to enable remote system disarming:

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 ADVANCED appears.

```
ENABLE
ADVANCED
```

3) Press OK and then ▼ until REMOTE DISARM appears.

```
ADVANCED
REMOTE DISARM
```

4) Press OK. If, necessary, press ▼ to make ENABLE appear.

```
REMOTE DISARM
ENABLE
```

5) Press OK to enable remote disarming.
6) Press ESC repeatedly to exit from the menu.

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

5.6.9 How to disable the Installer

Installer enabling is revoked whenever a User or Master code is entered or when an electronic or proximity key is used.

5.6.10 How to disable a User

Proceed as follows to disable a user:

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 USER appears.

```
ENABLE
USER
```

3) Press OK.

```
USER
UT02:...
```

4) Press ▼ and ▲ to select the user. Press OK to confirm.

```
UT02:...
ENABLE/DIS USER
```

5) Press OK. If, necessary, press ▼ to make DISABLE appear.

```
ENABLE/DIS USER
DISABLE
```

6) Press OK to disable the user.
7) Press ESC repeatedly to exit from the menu.

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

5.6.11 How to disable a key

Proceed as follows to disable a key:

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 KEY appears.

```
ENABLE
KEY
```

3) Press OK.

```
KEY
KE01:...
```

4) Press ▼ and ▲ to select the key. Press OK to confirm.

```
KE01:...
ENABLE/DIS KEY
```

5) Press OK. If, necessary, press ▼ to make DISABLE appear.

```
ENABLE/DIS KEY
DISABLE
```

6) Press OK to disable the key.

7) Press ESC repeatedly to exit from the menu.

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

5.6.12 How to disable the Technical Manager

Technical Manager enabling is revoked whenever a User or Master code is entered or when an electronic or proximity key is used.

5.6.13 How to disable the timed programmer

No timed commands will be performed if the timed programmer is disarmed. The programmed timed commands will be stored and may be re-activated when the timed programmer is enabled again.

Proceed as follows to disable the timed programmer:

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 TIMED COMMANDS appears.

```
ENABLE
TIMED COMMANDS
```

3) Press OK. If, necessary, press ▼ to make DISABLE appear.

```
TIMED COMMANDS
DISABLE
```

4) Press OK to disable the timed commands.

5) Press ESC repeatedly to exit from the menu.

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

EN50131
NOT RELATED

5.6.14 How to disable vocal messages

Proceed as follows to disable vocal messages on the vocal keypads:

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 VOCAL MESSAGES appears.

```
ENABLE
VOCAL MESSAGES
```

3) Press OK.
4) Press ▼ and ▲ to select the vocal message to be disabled. FAILURE, PARTITION STATUS, SYSTEM STATUS, SERVICE MESSAGE.

```
VOCAL MESSAGES
FAILURE
```

5) Press OK to confirm the selected message.
6) Press ▼ and ▲ to select DISABLE.
7) Press OK to disable the vocal message.
8) Repeat the steps from step 4 to disable other vocal messages. Press ESC repeatedly to exit from the menu.

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

5.6.15 How to disable remote access

Proceed as follows to disable remote access to the system:

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 ADVANCED appears.

```
ENABLE
ADVANCED
```

3) Press OK.

```
ADVANCED
REMOTE ACCESS
```

4) Press OK. If, necessary, press ▼ to make DISABLE appear.

```
REMOTE ACCESS
DISABLE
```

5) Press OK to disable remote access.
6) Press ESC repeatedly to exit from the menu.

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

5.6.16 How to disable remote access

Proceed as follows to disable remote system disarming:

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 ADVANCED appears.

```
ENABLE
ADVANCED
```

3) Press OK and then ▼ until REMOTE DISARM appears.

```
ADVANCED
REMOTE DISARM
```

4) Press OK. If, necessary, press ▼ to make DISABLE appear.

```
REMOTE DISARM
DISABLE
```

5) Press OK to disable remote disarming.
6) Press ESC repeatedly to exit from the menu.

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

5.7 HOW TO SET DATE AND TIME

In addition to being shown on the keypad in stand-by viewing mode (see paragraph 5.9.1 *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 code>, press OK, then MENU and finally press ▼ repeatedly until SETTINGS appears.

```
UT01:MASTER
SETTINGS
```

2) Press OK.

```
SETTINGS
HOUR - DATE
```

3) Press OK.

```
HOUR - DATE
SET HOUR
```

4) Press OK.

```
SET HOUR
HOUR 10:05
```

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 ▼.

```
HOUR - DATE
SET DATE
```

7) Press OK.

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

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 ▼.

```
HOUR - DATE
SUMMER TIME
```

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.

```
SUMMER TIME
ENABLE
```

11) Press OK to confirm the entered setting then ▼.

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

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.

```
LEGAL T. MONTH
        10
```

13) Press OK to confirm the month then ▼.

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

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.

```
SUMMER T. MONTH
         3
```

15) Press OK to confirm the month then ▼.

```
HOUR - DATE
SUNDAY
```

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.

```
SUNDAY
LAST SUNDAY
```

17) Press ESC repeatedly to exit from the menu.

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

5.8 EVENT LOG

The Event 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 Event Log reaches the maximum size (1000 events), each new event will be written over the oldest stored event.

The Event Log may be examined by the Master user and by the other users but may only be deleted by the Installer (see *Programming Manual*).

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.

5.8.1 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.

5.8.2 How to browse the Event Log

Proceed as follows to browse the Event Log:

1) Enter <Master/ User 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
```

5.9 KEYPAD CUSTOMISATION

Each keypad can be independently customised by means of some parameters which can be configured locally. No authorisation codes are needed in most cases.

5.9.1 LCD Info

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

- date and time

```
    MP500/16
22/01/2014 15:20
```

- system partition status

```
SYSTEM STATUS
□□■■□••••••••••
```

- system area status

```
AREAS 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.

1) To change the display view in stand-by:
2) Press MENU.

```
SYSTEM STATUS
SERVICE MESSAGE
```

3) Press ▼.

```
SYSTEM STATUS
LCD INFO
```

4) Press OK

```
ENTER CODE
```

5) Enter <Master / User code>, then OK.

```
LCD INFO
DATE/TIME
```

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

5.9.2 How to set the buzzer volume

Proceed as follows to adjust the buzzer volume:

1) To change the display view in stand-by:
2) Press MENU.

```
SYSTEM STATUS
SERVICE MESSAGE
```

3) Press ▼ repeatedly until SET BUZZER appears.

```
SYSTEM STATUS
SET BUZZER
```

4) Press OK

```
SET BUZZER
    - _▄■  +
```

5) Press ▼ and ▲ to adjust. The buzzer will generate a tone at the corresponding volume each time a key is pressed. Press OK to confirm the new volume.
6) Press ESC repeatedly to exit from the menu.

5.9.3 How to set the display contrast

IMPORTANT! The display contrast setting procedure does not apply to KP500DP/N keypads.

Proceed as follows to adjust the display contrast:

1) Press MENU.

2) Press ∨ repeatedly until SET CONTRAST appears.

3) Press OK.

4) Press ∨ and ∧ to set. Press OK to confirm the new contrast.

5) Press ESC repeatedly to exit from the menu.

```
SYSTEM STATUS
SERVICE MESSAGE
```

```
SYSTEM STATUS
SET CONTRAST
```

```
SET CONTRAST
    - _▪■  +
```

5.9.4 How to set backlighting

Proceed as follows to adjust the brightness of display, buttons and LEDs:

1) Press MENU.

2) Press ∨ repeatedly until SET BACKLIGHT appears.

3) Press OK

4) Press ∨ and ∧ to set. Press OK to confirm the new brightness level.

IMPORTANT! If level 0 is set (no square on) the keys will be switched off and the display can only be read in adequate ambient lighting conditions. Backlighting will not be switched back on even if a key is pressed.

IMPORTANT! The backlighting setting will also concern the status LED brightness (the LED will not be switched off by setting level 0). This setting concerns the power consumption of the keypad.

5) Press ESC repeatedly to exit from the menu.

```
SYSTEM STATUS
SERVICE MESSAGE
```

```
SYSTEM STATUS
SET BACKLIGHT
```

```
SET BACKLIGHT
    - _▪■  +
```

6 USERS AND KEYS

This chapter explains how to add new users and acquire new keys.

Adding a user essentially means configuring a user memory of the control panel, i.e. defining whether it is associated to the entire system or only to some partitions and to program a descriptive name.

Acquiring a new key is needed to make the control panel recognise a key code and to assign the key to the entire system or only to some partitions and to program a descriptive name.

In both cases, the new user and new key must be enabled after they have been created (see paragraph 5.6 *Enabling and disabling*).

6.1 USERS

6.1.1 How to assign a user

Proceed as follows to assign a user to the system (all partitions):

1) Enter < Master 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.

```
USERS
CONFIGURE USER
```

5) Press OK.

```
CONFIGURE USER
UT00:INSTALLER
```

6) Press ∨ and ∧ to select the required user. Press OK to confirm.

```
UT03:…
ASSIGN
```

7) Press OK.

```
ASSIGN
SYSTEM
```

8) Press ∨ and ∧ to assign the user to the entire system (SYSTEM) or to some partitions only. Press OK to confirm.
9) The following will appear if PARTITIONS is selected.

```
SE01:
□□□□□•••••••••••
```

10) 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.
11) In both cases, press ESC repeatedly to exit from the menu.

6.1.2 How to program a descriptive user name

Providing a descriptive name to a user helps to recognise the user during enabling and configuration and when reading the Events Log.

Proceed as follows to assign a descriptive name to a user.

1) Enter < Master / User 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.

```
USERS
CONFIGURE USER
```

5) Press OK.

```
CONFIGURE USER
UT00:INSTALLER
```

6) Press ⌄ and ⌃ to select the required user. Press OK to confirm.

```
UT03:…
ASSIGN
```

7) Press ⌄ repeatedly until NAME appears.

```
UT03:…
NAME
```

8) Press OK to confirm.

```
NAME
UT03:
```

9) Enter a descriptive name for the user using the keypad (see paragraph 5.5 *How to enter alphanumeric characters*). The name can be up to 24 characters long. Press OK to confirm.

10) Press ESC repeatedly to exit from the menu.

7 TELEPHONE DIALLER

IMPORTANT! For the procedures contained in this chapter it is assumed that the MP500/4N or MP500/16 control panels are connected to at least one telephone network (PSTN or GSM).

IMPORTANT! The control panel connection type determines EN50131 compliance.

If MP500/16 control panel connected via the ILT500-N interface to an SP4 external communicator, connected in turn to a modem/router with ADSL line, is EN50131 grade 3 compliant.

A MP500/4N 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.

This chapter explains how:

- the telephone alarms work
- to add, edit or delete a telephone number
- to write or delete a text message.

7.1 ALARM MESSAGE SENDING SEQUENCE

EN50131 NOT RELATED

In case of one or more alarm events, the dialler:

1) identifies the event with the highest priority if the events are different and simultaneous.
2) calls the telephone number or numbers configured for the alarm event starting from the one with the lowest memory position (e.g. T02 is called before T05).
3) the dialler make three attempts for each telephone number and calling mode.
4) when several telephone numbers are programmed, a sequence is created to which the calls are sent alternatively to the various numbers always respecting the event priority order. The called number sequence is dynamic and depends on a case-by-case basis on the involved events and the concerned telephone numbers.

The vocal call cycle to be stopped by entering code "12" on the answering telephone after having listened to the message and having received the block code prompt tone.

IMPORTANT! The text message sending sequence and the numeric protocol sending sequence cannot be stopped.

For emergency vocal calls, the block code "12" can be entered 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 disarming the partitions assigned to the telephone numbers programmed for sending the alarm. The function is useful in case of false alarms.

It is important to note that a telephone call cycle cannot be stopped once it has started and the system will continue to call the given number until the end of the three attempts. No further calls will be made to any subsequent numbers programmed for the burglar event.

The delivery time of SMS text messages depends on the GSM network company.

7.2 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".

7.3 TELEPHONE NUMBERS

The dialler of the MP500/4N and MP500/16 control panels may store up to 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 [v] 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.

7.3.1 How to store a telephone number

Proceed as follows to store a telephone number:

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

```
UT01:MASTER
SYSTEM STATUS
```

2) Press [v] repeatedly until TELEPHONE DIALER appears.

```
UT01:MASTER
TELEPHONE DIALER
```

3) Press [OK].

```
TELEPHONE DIALER
PHONE NUMBERS
```

4) Press [OK].

```
PHONE NUMBERS
TEL. NUMBER
```

5) Press [OK].

```
TEL. NUMBER
T01:...
```

6) Press [v] and [^] to select the memory position of the telephone number. Press [OK] to confirm.
7) Enter the telephone number and press [OK]. Press [ESC] to cancel the number.
8) Press [ESC].

```
PHONE NUMBERS
TEL. NUMBER
```

9) Press [v].

```
PHONE NUMBERS
ASSIGN TEL N.
```

10) Press [OK].

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

11) Press [v] and [^] to select the telephone number. Press [OK] to confirm.

```
T01:???
SYSTEM
```

12) Press [v] and [^] to assign the telephone number to the entire system or to specific partitions. Press [OK] to confirm.

13) If SYSTEM is selected:

```
SYSTEM
ASSIGN
```

14) Press ⌄ and ⌃ to assign the telephone number to the entire system or not. Press OK to confirm.

15) The following will appear if PARTITIONS is selected.

```
SE01:
□□□□□•••••••••••
```

16) 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.

17) Press ESC repeatedly until TELEPHONE LINE appears.

```
PHONE NUMBERS
TELEPHONE LINE
```

18) Press OK.

```
TELEPHONE LINE
T01:...
```

19) Press ⌄ and ⌃ to select the telephone number. Press OK to confirm.

```
T01:...
SELECT LINE
```

20) Press OK.

```
SELECT LINE
PSTN LINE
```

21) Press ⌄ and ⌃ to select the line or network to be used: PSTN, GSM, LAN or GPRS. Press OK to confirm.

⚠ **IMPORTANT!** Only the PSTN line can be used in a EN50131 compliant system.

⚠ **IMPORTANT!** The calls will be not be sent if a telephone number is assigned to a network or line which is not enabled.

22) Press ESC repeatedly to exit from the menu.

7.3.2 How to edit a telephone number

Proceed as follows to edit a telephone number:

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

```
UT01:MASTER
SYSTEM STATUS
```

2) Press ⌄ repeatedly until TELEPHONE DIALER appears.

```
UT01:MASTER
TELEPHONE DIALER
```

3) Press OK.

```
TELEPHONE DIALER
PHONE NUMBERS
```

4) Press OK.

```
PHONE NUMBERS
TEL. NUMBER
```

5) Press OK.

```
TEL. NUMBER
T01:...
```

6) Press ⌄ and ⌃ to select the memory position of the telephone number. Press OK to confirm.

7) Press ESC to delete the existing number and enter the new telephone number. Press OK to confirm and store the new number.

8) Press ESC repeatedly to exit from the menu.

7.3.3 How to delete a telephone number

IMPORTANT! Deleting telephone numbers may not comply with EN50131 and cancel compliance of the entire burglar alarm system. In particular:

- for EN50131 grade 3 compliance, do not delete the telephone numbers which use the SP4 external communicator with IDP numeric protocol.
- for EN50131 grade 2 compliance, do not delete the telephone numbers which use a PSTN line with numeric protocol.
- regardless of EN50131 compliance, the system will not be able to communicate with the outside if all the telephone numbers are deleted.

Proceed as follows to delete a telephone number:

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

```
UT01:MASTER
SYSTEM STATUS
```

2) Press ▼ repeatedly until TELEPHONE DIALER appears.

```
UT01:MASTER
TELEPHONE DIALER
```

3) Press OK.

```
TELEPHONE DIALER
PHONE NUMBERS
```

4) Press OK.

```
PHONE NUMBERS
TEL. NUMBER
```

5) Press OK.

```
TEL. NUMBER
T01:...
```

6) Press ▼ and ▲ to select the memory position of the telephone number. Press OK to confirm.
7) Press ESC to delete the current number and press OK to confirm.
8) Press ESC repeatedly to exit from the menu.

7.4 SMS TEXT MESSAGE

IMPORTANT! SMS text alarm notification is not EN50131 compliant and will cancel the compliance of the entire burglar alarm system.

MP500/4N and MP500/16 control panels can send text messages to the programmed telephone numbers when the following events occur:

- Burglar alarm
- Technological type 1 event
- Technological type 2 event
- Technological type 3 event
- Fire indication
- System/partition arming *
- System/partition disarming *
- Tamper
- Notices (SIM expiry)

*) The SMS text message can be up to 40 characters long, except for the arming/disarming messages which are only 24 long because the numbers of the concerned partitions are added to the message.

All SMS text messages are empty by default.

The GSM module must be installed in the control panel to send SMS text messages.

	SMS for control panels with SW any versions	***SMS extension for control panels from SW version 1.03***
Events	***USER SMS***	***Automated message from Control Panel***
Burglar alarm:	*SMS* programmed by user	In <xxx> : <Input name>
Technological type 1 event:	*SMS* programmed by user	U <yy> : <Output name>
Technological type 2 event:	*SMS* programmed by user	U <yy> : <Output name>
Technological type 3 event:	*SMS* programmed by user	U <yy> : <Output name>
Fire indication:	*SMS* programmed by user	In <xxx> : <Input name>
		KP <zz> : <Keypad name>
		RC<zz> : <Remote control name>
System/partition arming:	*SMS* programmed by user	< partition/s arming >
System/partition disarming:	*SMS* programmed by user	< partition/s disarming >
Tamper:	*SMS* programmed by user	In <xxx> : <Input name>
		IR<zz> : < radio detector name >
		DC<zz> : < radio detector name >
		HP<zz>: < radio siren name >
		KP <zz> : <Keypad name>
		EP <zz> : <Expansion name >
		AS <zz> : <Supplemental power supply name>
		DK <zz> : <Reader name>
		ER <zz> : <Radio expansion name>

Where

xxx: Logic input number
yy: Logic output number
zz: Device number (keypad / reader / expansion / radio expansion / supplemental power supply / radio detectors / radio sirens / Remote controls)

7.4.1 How to write SMS text messages

Proceed as follows to write an SMS text message:

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

```
UT01:MASTER
SYSTEM STATUS
```

2) Press ⌄ repeatedly until TELEPHONE DIALER appears.

```
UT01:MASTER
TELEPHONE DIALER
```

3) Press OK.

```
TELEPHONE DIALER
PHONE NUMBERS
```

4) Press ⌄ repeatedly until SMS TEXT MESSAGES appears.

```
TELEPHONE DIALER
SMS MESSAGES
```

5) Press OK.

```
SMS MESSAGES
WRITE SMS
```

6) Press OK.

```
WRITE SMS
BURGLAR
```

7) Press ⌄ and ⌃ to select the type of event which will cause the message to be sent: burglar, technological type 1, technological type 2, technological type 3, fire, partition arming, partition disarming, tamper, notices. Press OK to confirm.

```
BURGLAR
```

8) Write the text using the alphanumeric keyboard and keys ‹ and › (see paragraph 5.5 *How to enter alphanumeric characters*). At the end, press OK to store or ESC to delete everything.
9) Repeat from step 7 to store other text messages.
10) Press ESC repeatedly to exit from the menu.

7.4.2 How to delete SMS text messages

Proceed as follows to delete an SMS text message:

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

```
UT01:MASTER
SYSTEM STATUS
```

2) Press ▼ repeatedly until TELEPHONE DIALER appears.

```
UT01:MASTER
TELEPHONE DIALER
```

3) Press OK.

```
TELEPHONE DIALER
PHONE NUMBERS
```

4) Press ▼ repeatedly until SMS TEXT MESSAGES appears.

```
TELEPHONE DIALER
SMS MESSAGES
```

5) Press OK.

```
SMS MESSAGES
WRITE SMS
```

6) Press OK.

```
WRITE SMS
BURGLAR
```

7) Press ▼ and ▲ to select the event type related to the text message (burglar, technological type 1, technological type 2, technological type 3, fire, partition arming, partition disarming, tamper, notices). Press OK to confirm.

```
BURGLAR
```

8) The stored message will appear and the cursor will blink on the display. Press ESC to delete the message. Press OK to confirm deletion.
9) Repeat from step 7 for deleting any one text messages.
10) Press ESC repeatedly to exit from the menu.

7.5 END OF TELEPHONE CREDIT NOTICE

EN50131

With GSM transmitter (IMG500/N module) you can be notified of the residual credit on the prepaid SIM Card.

The MP500/4N and MP500/16 control panels can forward all the text messages received from numbers external to the system (i.e. not one of the 12 telephone numbers which can be stored on the control panel) to the number stored in position 12.

In this manner, you will receive messages from the telephone operator informing that the credit has reached a given threshold and other service messages.

This function must be enabled by the installer during installation.

8 USER REMOTE CONTROL

8.1 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.

8.2 REMOTE CONTROL WITH SMS 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 SMS 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 SMS 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 SMS 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 SMS text message containing exclamation marks **“!!!”** followed by the received message to confirm command reception.

8.3 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.

8.4 REMOTE CONTROL WITH GUIDED VOCAL 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 paragraph 5.6.8 *How to enable remote disarming*).

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 13 - List of DTMF commands*) and access the required menu directly. Otherwise, follow the vocal 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.

8.5 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 13 - 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

8.6 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.

9 SYSTEM TEST

9.1 PERIODICAL TESTS

It is advisable to check perfect operation of the burglar alarm system regularly. 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
- Environmental listening test

ADVICE: Test the MP500/4N or MP500/16 before prolonged absences, for example before the summer holidays.

9.1.1 Input test

Proceed as follows to test that the inputs work perfectly:

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

```
UT01:MASTER
SYSTEM STATUS
```

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.

9.1.2 Output test

Proceed as follows to test that the outputs work perfectly:

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

```
UT01:MASTER
SYSTEM STATUS
```

2) Press ▼ repeatedly until TEST appears.

```
UT01:MASTER
TEST
```

3) Press OK and press ▼ repeatedly until TEST OUTPUTS appears.

```
TEST
TEST OUTPUTS
```

4) Press OK.

```
TEST OUTPUTS
CONTROL PANEL
```

5) Press ▼ and ▲ to select the device the outputs of which you want to test. Press OK to confirm.

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

6) Press ▼ and ▲ to select the output to test. Press OK to confirm.

```
UC.U1        U01
ARM
```

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.

9.1.3 Battery test

Proceed as follows to check the condition of the control panel battery:

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

```
UT01:MASTER
SYSTEM STATUS
```

2) Press ▼ repeatedly until TEST appears.

```
UT01:MASTER
TEST
```

3) Press OK and press ▼ repeatedly until TEST BATTERY appears.

```
TEST
TEST BATTERY
```

4) Press OK.

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

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.

9.1.4 Vocal call test

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

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

```
UT01:MASTER
SYSTEM STATUS
```

2) Press ▼ repeatedly until TEST appears.

```
UT01:MASTER
TEST
```

3) Press OK and press ▼ repeatedly until ADVANCED TESTS appears.

```
TEST
ADVANCED TESTS
```

4) Press OK.

```
ADVANCED
VOCAL CALL
```

5) Press OK.

```
VOCAL CALL
T01:xxxxxxxx
```

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.

9.1.5 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.

```
UT01:MASTER
SYSTEM STATUS
```

2) Press ▼ repeatedly until TEST appears.

```
UT01:MASTER
TEST
```

3) Press OK and press ▼ repeatedly until ADVANCED TESTS appears.

```
TEST
ADVANCED TESTS
```

4) Press OK and press ▼ repeatedly until PROTOCOL CALL appears.

```
ADVANCED
PROTOCOL CALL
```

5) Press OK.

```
PROTOCOL CALL
T01:xxxxxxxx
```

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.

9.1.6 GSM Field Test

Proceed as follows to test the GSM network signal level:

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

```
UT01:MASTER
SYSTEM STATUS
```

2) Press ▼ repeatedly until TEST appears.

```
UT01:MASTER
TEST
```

3) Press OK and press ▼ repeatedly until ADVANCED TESTS appears.

```
TEST
ADVANCED TESTS
```

4) Press OK and press ▼ repeatedly until GSM FIELD TEST appears.

```
ADVANCED
GSM FIELD TEST
```

5) Press OK.

```
GSM FIELD TEST
```

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.

9.1.7 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 8.6 *Environmental* listening.

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.

9.1.8 Radio device test

The radio input and output devices are tested together with the wired inputs and outputs. The test result is in common. The radio input and output devices are identified by means of logical address or name.

Proceed as follows to test the wireless signal level of the various devices:

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

```
UT01:MASTER
SYSTEM STATUS
```

2) Press ▼ repeatedly until TEST appears.

```
UT01:MASTER
TEST
```

3) Press OK and press ▼ repeatedly until ADVANCED TESTS appears.

```
TEST
ADVANCED TESTS
```

4) Press OK and then ▼ several times until RADIO DEVICES appears.

```
ADVANCED
RADIO DEVICES
```

5) Press OK.

```
RADIO DEVICES
ER01:ER 01
```

6) Press ▼ and ▲ to select the radio expansion module to test. Press OK to confirm.

```
ER01:ER 01
ARE YOU SURE?
```

7) Press OK.

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

8) Energise each detector, e.g. by opening the door or window with magnetic contacts or passing in front of IR detectors.
9) The wireless level will appear in graphic form at the end of the test for each device. Use ▼ and ▲ to scroll the list of devices.
10) Press ESC repeatedly to exit from the menu.

10 QUICK GUIDE TO REMOTE CONTROL

Cut out the following quick reference guides along the lines to keep the list of remote control commands handy at all times. The folded guide is credit-card-sized to conveniently fit in a wallet or purse.

How to skip a telephone answering machine EN50131 NOT RELATED

Call the control panel number and hang up after the first ring.
Call the control panel back within 30 seconds.

How to manage outputs using text messages ~~EN50131~~

Send a text message to the control panel in the following format: *2 nn s.* ,where *nn* is the two digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=arm; 0 =disarm).
In case of pulsed commandable output only **1** (arm) can be used.
Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (“.”).

Guided vocal menu EN50131 NOT RELATED

Call the control panel from a DTMF tone telephone.
Enter the Master code within 10 seconds.
Follow the vocal instructions.
Press * (asterisk) to go back to the previous menu or to end remote control.

Environmental listening EN50131 NOT RELATED

Select "Environmental listening" from the guided vocal menu.
Press “0” to switch from listening to speaking and vice versa.
The listening function will be automatically interrupted after approximately one minute and a half. Press "*" to stop it before the timeout.

How to skip a telephone answering machine EN50131 NOT RELATED

Call the control panel number and hang up after the first ring.
Call the control panel back within 30 seconds.

How to manage outputs using text messages ~~EN50131~~

Send a text message to the control panel in the following format: *2 nn s.* ,where *nn* is the two digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=arm; 0 =disarm).
In case of pulsed commandable output only **1** (arm) can be used.
Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (“.”).

Guided vocal menu EN50131 NOT RELATED

Call the control panel from a DTMF tone telephone.
Enter the Master code within 10 seconds.
Follow the vocal instructions.
Press * (asterisk) to go back to the previous menu or to end remote control.

Environmental listening EN50131 NOT RELATED

Select "Environmental listening" from the guided vocal menu.
Press “0” to switch from listening to speaking and vice versa.
The listening function will be automatically interrupted after approximately one minute and a half. Press "*" to stop it before the timeout.

How to skip a telephone answering machine EN50131 NOT RELATED

Call the control panel number and hang up after the first ring.
Call the control panel back within 30 seconds.

How to manage outputs using text messages ~~EN50131~~

Send a text message to the control panel in the following format: *2 nn s.* ,where *nn* is the two digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=arm; 0 =disarm).
In case of pulsed commandable output only **1** (arm) can be used.
Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (“.”).

Guided vocal menu EN50131 NOT RELATED

Call the control panel from a DTMF tone telephone.
Enter the Master code within 10 seconds.
Follow the vocal instructions.
Press * (asterisk) to go back to the previous menu or to end remote control.

Environmental listening EN50131 NOT RELATED

Select "Environmental listening" from the guided vocal menu.
Press “0” to switch from listening to speaking and vice versa.
The listening function will be automatically interrupted after approximately one minute and a half. Press "*" to stop it before the timeout.

Cut out the following quick reference guides along the lines to keep the list of remote control commands handy at all times. The folded guide is credit-card-sized to conveniently fit in a wallet or purse.

How to skip a telephone answering machine EN50131 NOT RELATED

Call the control panel number and hang up after the first ring.
Call the control panel back within 30 seconds.

How to manage outputs using text messages ~~EN50131~~

Send a text message to the control panel in the following format: *2 nn s. ,*where *nn* is the two digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=arm; 0 =disarm).
In case of pulsed commandable output only **1** (arm) can be used.
Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (“.”).

Guided vocal menu EN50131 NOT RELATED

Call the control panel from a DTMF tone telephone.
Enter the Master code within 10 seconds.
Follow the vocal instructions.
Press * (asterisk) to go back to the previous menu or to end remote control.

Environmental listening EN50131 NOT RELATED

Select "Environmental listening" from the guided vocal menu.
Press “0” to switch from listening to speaking and vice versa.
The listening function will be automatically interrupted after approximately one minute and a half. Press "*" to stop it before the timeout.

How to skip a telephone answering machine EN50131 NOT RELATED

Call the control panel number and hang up after the first ring.
Call the control panel back within 30 seconds.

How to manage outputs using text messages ~~EN50131~~

Send a text message to the control panel in the following format: *2 nn s. ,*where *nn* is the two digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=arm; 0 =disarm).
In case of pulsed commandable output only **1** (arm) can be used.
Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (“.”).

Guided vocal menu EN50131 NOT RELATED

Call the control panel from a DTMF tone telephone.
Enter the Master code within 10 seconds.
Follow the vocal instructions.
Press * (asterisk) to go back to the previous menu or to end remote control.

Environmental listening EN50131 NOT RELATED

Select "Environmental listening" from the guided vocal menu.
Press “0” to switch from listening to speaking and vice versa.
The listening function will be automatically interrupted after approximately one minute and a half. Press "*" to stop it before the timeout.

How to skip a telephone answering machine EN50131 NOT RELATED

Call the control panel number and hang up after the first ring.
Call the control panel back within 30 seconds.

How to manage outputs using text messages ~~EN50131~~

Send a text message to the control panel in the following format: *2 nn s. ,*where *nn* is the two digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=arm; 0 =disarm).
In case of pulsed commandable output only **1** (arm) can be used.
Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (“.”).

Guided vocal menu EN50131 NOT RELATED

Call the control panel from a DTMF tone telephone.
Enter the Master code within 10 seconds.
Follow the vocal instructions.
Press * (asterisk) to go back to the previous menu or to end remote control.

Environmental listening EN50131 NOT RELATED

Select "Environmental listening" from the guided vocal menu.
Press “0” to switch from listening to speaking and vice versa.
The listening function will be automatically interrupted after approximately one minute and a half. Press "*" to stop it before the timeout.

ELKRON
Tel. +39 011.3986711
www.elkron.com – *mail to: info@elkron.it*

ELKRON is a trademark of **URMET S.p.A.**
Via Bologna, 188/C - 10154 Torino (TO) – Italy
www.urmet.com