



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

DS80MP5L-024A

LBT81215

MP500/4N - MP500/16

Remote controllable alarm
control panels

Installation Manual



ELKRON

The information in this document were carefully assembled and controlled, but the company cannot in any case be held responsible for potential errors or omissions.

The company reserves the right to make improvements or modifications to the products described in the manual at any time and without advanced notice.

This manual may also contain references to or information about products (hardware or software) or services that are not yet on the market. These references or information in no way mean that the company intends to market such product or services.

Elkron is a brand name of URMET S.p.A.

All the brands cited in the document belong to their respective owners.

All rights reserved. The partial or total reproduction of this document is authorised only for the purpose of installing the MP500/4N or MP500/16 System.



Tel. +39 011.3986711

www.elkron.com – mail to: info@elkron.it

TABLE OF CONTENTS

Preface	9
Conformity with EN50131-1	9
Conformity with EN50136-1	9
Conformity with EN50131-10	10
How the manual is organised	10
Conventions used	10
Glossary	11
1 - The MP500/4N- MP500/16 systems	12
1.1 Main characteristics	12
1.2 System Architecture	13
1.2.1 Architecture	13
1.2.2 Bus Data	13
1.2.3 Maximum system size	14
1.3 System connectivity	14
1.3.1 Connection with remote user	16
1.3.2 Connection with a remote PC	17
1.3.3 Connection with a local PC	18
1.3.4 Connection with an alarm reception centre	19
1.4 System components	19
1.4.1 MP500/4N Control panel	19
1.4.2 MP500/16 Control panel	20
1.4.3 KP500D/N Command Keypad	20
1.4.4 KP500DV/N Vocal command keypad	20
1.4.5 KP500DP/N Touch Screen keypad	21
1.4.6 KP500D/ST Touch Screen keypad	21
1.4.7 EP508 Expansion module	21
1.4.8 CP/EXP Container	21
1.4.9 CP/EP500 Container	22
1.4.10 DK500M-E Electronic key reader	22
1.4.11 DK50 Electronic key	22
1.4.12 DK500M-P Transponder reader	22
1.4.13 DK30 Proximity key	23
1.4.14 DK30-50 key personalisation kit	23
1.4.15 MIFARE DK510M-P Transponder reader	23
1.4.16 MIFARE DK70 Proximity key	23
1.4.17 AS500/RPT supplemental power supply with repeater	23
1.4.18 SV500N-I-F-GB vocal synthesis board	24
1.4.19 ILT500-N PSTN telephone communicator	24
1.4.20 IMG500/N GSM Module	24
1.4.21 Remote GSM 1 antenna	24
1.4.22 Antenna for GSM 2 metallic box	24
1.4.23 Cable for KP SERVICE keypad	24
1.4.24 USB interface for connection to the PC and USB IT-USB/KEY keys	25
1.4.25 Hi-Connect application software (rev. 3.60 or later)	25
1.4.26 IT500WEB web server interface	25
2 - Basic information	26
2.1 How an intrusion alarm system is made	26
2.1.1 The simplest system	26
2.1.2 Wired, radio, and bus	26
2.1.2.1 Radio apparatus	27
2.1.2.2 The bus	27
2.2 Communicating with the external environment	27
2.3 The devices used to create an alarm system	28
2.3.1 The control panel	28
2.3.2 The detectors	28
2.3.2.1 Button	28
2.3.2.2 Magnetic contact (reed)	28
2.3.2.3 Cable contacts for rollers	28
2.3.2.4 Broken glass detector	28
2.3.2.5 Vibration detector	28
2.3.2.6 Passive infra-red detector (IR)	29
2.3.2.7 Active infra-red detectors	29
2.3.2.8 Microwave detector (MW)	29
2.3.2.9 Combined passive IR and microwave detector	29

2.3.2.10	External detectors	29
2.3.3	The signalling devices	29
2.3.3.1	Siren	29
2.3.3.2	Flasher	29
2.3.3.3	Communicator	29
2.3.4	The complementary devices	30
2.3.4.1	Keypad	30
2.3.4.2	Reader	30
2.3.4.3	Remote control	30
2.3.4.4	Power supply	30
2.3.4.5	Expansion	30
2.4	Other devices that can be integrated into the alarm system	30
3 -	Design: configuration of the alarm system	31
3.1	Identifying the grade of protection	31
3.2	The alarm system power supply	31
3.3	How to design an alarm system	32
3.3.1	Analysis of the site and needs	32
3.3.2	Certification requirements	32
3.3.3	How to protect areas and people	33
3.3.4	The subdivision into partitions	34
3.3.5	Choosing devices	35
3.3.5.1	The detectors	35
3.3.5.2	Sirens	35
3.3.5.3	Keypads, readers and remote controls	35
3.3.5.4	External communications	35
3.3.6	Positioning the system devices	36
3.3.6.1	Positioning the control panel	36
3.3.6.2	Positioning the keypads	36
3.3.6.3	Positioning readers	36
3.3.6.4	Positioning expansions	36
3.3.6.5	Positioning sirens and flashing lights	36
3.3.6.6	Positioning the supplementary power supplies	37
3.3.7	Tips about installing the radio devices	37
3.3.8	Tips about the mobile phone network (GSM)	37
3.4	Advanced functions	38
3.4.1	The partitions and the areas	38
3.4.1.1	How to use areas	38
3.4.2	Input and output: select the delay to avoid setting off the alarm	38
3.4.2.1	Intrusion – First entry	39
3.4.2.2	Intrusion – Way	39
3.4.2.3	Intrusion – Last exit	39
3.4.2.4	Intrusion – First entry – Last exit	39
3.4.2.5	Examples of the first entry, last exit, and way specialisations	39
3.4.3	The complementary functions (gong, courtesy light, door opener, absence of move)	40
3.4.4	The attributes of the intrusion inputs (Release type, AND / OR partitions, AND inputs)	40
3.4.5	Remote activation of commandable outputs free of charge	41
3.4.6	Environmental listening	41
4 -	Design: calculations and tests	42
4.1	Sizing of the power supplies and the batteries	42
4.1.1	Battery sizing	42
4.1.2	Calculation of the total absorption of the system	43
4.1.3	Using supplementary power supply units	43
4.2	Cable Sizing	43
4.2.1	Cables to be used, connections of the shields and installation	43
4.2.2	Sizing of the power supply cable	44
4.2.3	Sizing the power supply and data transmission bus	45
4.2.4	Extending the bus with the repeater	45
4.2.4.1	System with 1 supplementary power supply repeater	46
4.2.4.2	System with 2 supplementary power supply repeaters	46
4.2.4.3	System with multiple supplementary power supply units	47
4.2.5	Sizing of audio Bus	47
4.2.6	Sizing of Input/Output connections	47
4.3	Control criteria of the mains power supply voltage	47
4.3.1	Blackout event	47
4.3.2	Continued blackout alarm	48
4.3.3	Restoration of the mains power supply	48
4.4	Battery management criteria	48
4.4.1	Control and charging of the battery with the mains power supply present	48
4.4.2	Controlling the battery with mains power supply absent	48
4.4.3	Test battery	48

4.5	Self-diagnostic functions.....	48
5 -	Installation.....	49
5.1	Installation procedure	49
5.2	Wiring	49
5.3	Preparing the MP500/4N control panel	50
5.3.1	Opening the cover	50
5.3.2	Openings for cables	50
5.3.3	Fastening to the wall	51
5.3.4	Battery compartment and fastening points for the optional features in the MP500/4N control panel	52
5.3.5	Assembling expansion modules in the MP500/4N control panel	53
5.4	Preparing the MP500/16 control panel.....	54
5.4.1	Opening the cover	54
5.4.2	Openings for cables	55
5.4.3	Fastening to the wall	55
5.4.4	Battery compartment and fastening points for the optional features in the MP500/16 control panel	57
5.4.5	Assembling expansion modules in the MP500/16 control panel	57
5.5	Installing the MP500/4N - MP500/16 control panels	58
5.5.1	Description of the main parts of the MP500/4N control panel	58
5.5.2	Description of the main parts of the MP500/16 control panel	59
5.5.3	Assembly of the PSTN ILT500-N communicator	61
5.5.4	Assembly of the SV500N Vocal synthesis board	62
5.5.5	Installation of the GSM Module	64
5.5.5.1	Installation of the GSM antenna on the MP500/4N control panel	64
5.5.5.2	Installation of the GSM antenna on the MP500/16 control panel	65
5.5.5.3	Important information about the SIM Card	65
5.5.5.4	Setting up the SIM Card.....	65
5.5.5.5	Inserting the SIM Card.....	66
5.6	Connection of the USB interface and web server	66
5.6.1	Temporary connection of the IT - USB/KEY interface for the USB pen drive for connecting to the PC	66
5.6.2	Installation of the IT500WEB web server interface	67
5.7	Installation of the EP508 expansion	68
5.8	Installation of the KP500D/N – KP500DV/N keypads.....	69
5.9	Installation of the KP500DP/N - KP500D/ST touch screen.....	70
5.10	Installing the reader.....	72
5.11	Installation of the AS500/RPT supplementary power supply	72
5.11.1	Fastening to the wall	72
5.11.2	Connecting the power supply and battery	73
5.11.3	The AS500/RPT board	73
5.11.3.1	The Expansion.....	74
5.11.3.2	The Repeater.....	75
5.11.3.3	Power supply	75
5.12	Connections	76
5.12.1	Power supply line	76
5.12.2	Connecting the data Bus	77
5.12.3	Connecting the audio Bus	77
5.12.4	Connecting the supplementary power supplies/repeater	78
5.12.4.1	Connection of the detectors to the expansion module of the AS500/RPT	78
5.12.5	Connecting inputs	79
5.12.6	Connecting outputs	81
5.12.6.1	Relay outputs.....	81
5.12.6.2	Electrical outputs.....	81
5.12.6.3	Output stand-by: N.H. and N.L.....	82
5.12.7	Connecting the cable for KP SERVICE keypad	82
5.12.8	Connecting the telephone dialler	83
5.12.8.1	Connecting the SP4 dialler to the MP500/16 control panel.....	83
5.13	Example of diagram with N.C. inputs MP500/4N CONTROL PANEL	84
5.14	Example of diagram with double balancing INPUTS MP500/4N	86
5.15	Example of diagram with NC inputs MP500/16	88
5.16	Example of diagram with DOUBLE bAL. inputs MP500/16.....	90
6 -	COMMISSIONING.....	92
6.1	SYSTEM POWER SUPPLY	92
6.1.1	RUN LED Indications	92
6.2	ACQUISITION OF BUS DEVICES	92
6.2.1	Position of the programming buttons	92
6.2.2	Procedure for acquiring bus devices	93
6.3	USING THE SERVICE KEYPAD.....	93
7 -	MAINTENANCE	94
7.1	MAINTENANCE PROCEDURE	94
7.2	ADDITION AND ACQUISITION OF A NEW DEVICE BUS	94
7.3	REPLACING A BUS DEVICE.....	94

7.4	IDENTIFYING A BUS DEVICE	95
7.4.1	<i>Interrogating a bus device</i>	95
7.4.2	<i>Searching for a device</i>	95
7.5	DELETING A BUS DEVICE	95
7.5.1	<i>Deleting a radio expansion</i>	95
7.6	ACQUISITION/ MAINTENANCE OF THE RADIO DEVICES	96
7.6.1	<i>Radio connection test</i>	97
7.7	CONFIGURING RADIO PARAMETERS	98
7.8	DELETING A RADIO DEVICE	98
7.9	RESETTING FACTORY SETTINGS	99
7.9.1	<i>Partial reset</i>	99
7.9.2	<i>Global reset</i>	100
7.9.3	<i>Resetting Installer, Tech. Manager, Master and User codes</i>	100
7.9.4	<i>Resetting hardware installer code and Tech. Manager Code</i>	100
7.9.5	<i>Resetting hardware to factory settings</i>	100
7.9.6	<i>Resetting devices</i>	100
7.10	REPLACING THE BATTERY	101
7.11	TURNING OFF THE ENTIRE SYSTEM	101
7.12	TROUBLESHOOTING	102
8 -	TECHNICAL SPECIFICATIONS	105
8.1	MP500/4N CONTROL PANEL	105
8.2	MP500/16 CONTROL PANEL	106
8.3	KEYPAD DISPLAY KP500D/N - KP500DV/N	107
8.4	KEYPAD TOUCH SCREEN KP500DP/N	107
8.5	KEYPAD TOUCH SCREEN KP500D/ST	108
8.6	DK500M-E ELECTRONIC KEY READER	108
8.7	DK500M-P PROXIMITY READER	108
8.8	DK510M-P PROXIMITY READER	109
8.9	8-INPUT EP508 EXPANSION MODULE	109
8.10	VOCAL SYNTHESIS BOARD SV500N-I-F-GB	109
8.11	ILT500-N PSTN COMMUNICATOR	109
8.12	IMG500/N GSM MODULE	110
8.13	USB INTERFACE FOR CONNECTION TO THE PC AND USB IT-USB/KEY KEYS	110
8.14	IT500WEB INTERFACE	110
8.15	Supplementary power unit AS500/RPT	111

FIGURE INDEX

Figure 1 - System Architecture of the MP500/4N - MP500/16	13
Figure 2 - Diagram of connection with remote user	16
Figure 3 - Diagram of connection with remote PC	17
Figure 4 - Diagram of connection with local PC	18
Figure 5 - Diagram of connection with an alarm reception centre	19
Figure 6 - Perimeter and trap protection	33
Figure 7 - Subdivision into partitions	34
Figure 8 - Examples of the first entry, last exit, and way specialisations	39
Figure 9 - AND and OR partitions	41
Figure 10 - Topologies of the bus connection	45
Figure 11 - Rings on the bus	45
Figure 12 - Diagram with 1 supplementary power supply repeater	46
Figure 13 - Diagram with 2 supplementary power supply repeater	46
Figure 14 - Diagram with 15 supplementary power supply repeater	47
Figure 15 - Opening the MP500/4N control panel	50
Figure 16 - Setup for running the cables	50
Figure 17 - Holes for fastening the MP500/4N	51
Figure 18 - Releasing the mother board	51
Figure 19 - Protection of the MP500/4N from tampering and removal	51
Figure 20 - Fastening points for optional features in the MP500/4N control panel	52
Figure 21 - Fastening points for optional features in the MP500/4N control panel	52
Figure 22 - Fastening points for optional features in the MP500/4N control panel	53
Figure 23 - Opening the control panel by totally removing the cover MP500/16	54
Figure 24 - Opening the control panel without totally removing the cover MP500/16	54
Figure 25 - Set-up for running cables and fastening the GSM antenna MP500/16	55
Figure 26 - Holes for fastening the MP500/16	55
Figure 27 - Releasing the MP500/16 mother board	56
Figure 28 - Assembly of tamper for the MP500/16 control panel	56
Figure 29 - Fastening points for optional features in the MP500/16 control panel	57
Figure 30 - Available positions for expansion in the MP500/16 control panel	57
Figure 31 - Connections and main parts of the MP500/4N control panel	58
Figure 32 - Configuration of the electric output hardware	59
Figure 33 - Connections and main parts of the MP500/16 control panel	59
Figure 34 - Configuration of the electric output hardware	61
Figure 35 - Assembling PSTN communicator board	61
Figure 36 - Vocal synthesis board SV500N	62
Figure 37 - Assembling the vocal synthesis board	63
Figure 38 - Installation of the GSM module	64
Figure 39 - Installation of the GSM1 antenna on MP500/4N	64
Figure 40 - Insertion of the GSM2 antenna on MP500/16	65
Figure 41 - Insertion of the GSM2 MP500/16 antenna	66
Figure 42 - Connecting the IT-USB/KEY INTERFACE	66
Figure 43 - Installing the web server interface on MP500/4N	67
Figure 44 - Installing the web server interface on MP500/16	67
Figure 45 - EP508 Expansion	68
Figure 46 - Opening the keypad	69
Figure 47 - Holes in the keypad and running cables	69
Figure 48 - Keypad boards	70
Figure 49 - Removal of the KP500DP/N - KP500D/ST keypad bracket	70
Figure 50 - Opening the KP500DP/N - KP500D/ST keypad	71
Figure 51 - Holes for fastening and running the cables of the KP500DP/N - KP500D/ST keypad	71
Figure 52 - Holes for fastening the AS500/RPT	72
Figure 53 - Connecting the power supply and battery	73
Figure 54 - AS500/RPT Board	73
Figure 55 - Diagram of the connections to the mains power supply	76
Figure 56 - Connections via bus	77
Figure 57 - Connections the audio bus	77
Figure 58 - Connecting the supplementary power supplies	78
Figure 59 - Diagram of how to connect a locally powered detector	78
Figure 60 - Diagrams of input connections	80
Figure 61 - Cable for KP SERVICE keypad	82
Figure 62 - Telephone connections	83
Figure 63 - Position of the programming buttons	92
Figure 64 - Message of KP500DP/N - KP500D/ST keypad acquisition	93
Figure 65 - Radio devices menu diagram	96
Figure 66 - Radio connection test menu	97

TABLE INDEX

Table 1 - Maximum system dimension MP500/4N and MP500/16	14
Table 2 - Max number of wired inputs and outputs.....	14
Table 3 - Comparison of wired and radio technologies	26
Table 4 - Control panel battery autonomy	42
Table 5 - Copper wire resistance.....	44
Table 6 - Functions associated with the DIP-switches of the mother board	59
Table 7 - Functions associated with the DIP-switches of the mother board	61
Table 8 - Interval of voltage present at inputs.....	80
Table 9 - Line diagram of output programmed N.H.	82
Table 10 - Line diagram of output programmed N.L.....	82
Table 11 - Variations of the configuration with reset.....	99

PREFACE

CONFORMITY WITH EN50131-1

The EN50131-1 standard calls for the installation of a grade four intruder alarm system, based on the level of risk determined in function of the type of environments, of the value of the goods to be protected, and the typical intruder expected.

Grade 1: Low risk

It is expected that the intruders have little knowledge of intrusion alarm systems and have a limited range of tools that can be easily obtained. It is indicated for premises with contents of low value.

The system is simple and equipped with external and/or internal acoustic alarms, optical warnings, and eventually a telephonic communicator to vocal messages to other people.

Grade 2: Average-low risk

It is expected that the intruders have limited knowledge of intruder alarm systems and use some tools and portable instruments (for example, a multimeter).

It is the minimum level that can be recognised by insurance companies.

It involves mostly residential and commercial premises of low value.

The system can be connected with a Security Service.

Grade 3: Average-high risk

It is expected that the intruders have knowledge of intruder alarm systems and have a full range of tools and portable electronic equipment.

It is indicated for commercial and industrial premises, as well as for residential premises with a high value.

The system is usually connected with a Security Service.

Grade 4: High risk

To be used when security has the priority over all other factors. It is expected that the intruders have the skills and resources to plan a detailed intrusion and have a complete set of tools available, including the means for substituting components of an intruder alarm system. This is indicated for particularly sensitive premises, for example, banks.



ATTENTION! The grade of an intruder alarm system is the one of its lowest grade component.

The EN50131-1 standard requires that the components of the intruder alarm system are suitable to be used in one of the following environmental classes, where Class I is the most moderate and class IV is the most severe.

Environmental class I – Indoors

Environmental influences normally present in closed environments, when the temperature is well-controlled (ex: in a residential or commercial property).

NOTE: The environment should not be subject to condensation and the temperature should vary between +5°C and +40°C with an average relative humidity of about 75%.

Environmental class II – Indoors – General

Environmental influences normally present in closed environments, when the temperature has not been controlled (ex: in corridors, other spaces or stairways where condensation may form on windows and in unheated areas used as a deposit or in warehouses where heating is intermittent).

NOTE: The environment should not be subject to condensation and the temperature should vary between -10°C and +40°C with an average relative humidity of about 75%.

Environmental class III – Outdoors – Sheltered or indoors under extreme conditions

Environmental influences normally present outdoors when components of the intruder alarm system are not totally exposed to atmospheric agents or indoors, when the environmental conditions are extreme.

NOTE: The environment should not be subject to condensation and the temperature should vary between -25°C and +50°C with an average relative humidity of about 75%. For 30 days a year it is expected that the relative humidity will vary between 85% and 95% without being subject to condensation.

Environmental class IV – Outdoors – General

Environmental influences normally present outdoors, when the components of the intruder alarm system are completely exposed to the elements.

NOTE: The environment should not be subject to condensation and the temperature should vary between -25°C and +60°C with an average relative humidity of about 75%. For 30 days a year it is expected that the relative humidity will vary between 85% and 95% without being subject to condensation.

CONFORMITY WITH EN50136-1

Standard EN 50136-1 establishes the general requirements for performance, reliability, and security of alarm transmission systems. In particular, it regulates how alarm signals (intrusion, fire, access control, social alarms, etc.) must be transmitted from the system installed at a monitored site to the alarm receiving centre.

CONFORMITY WITH EN50131-10

The EN50131-10 standard defines the performance requirements for intrusion and hold-up alarm transmission systems to remote monitoring centers. In summary, it defines the operating procedures for devices and protocols responsible for transmitting alarm signals, ensuring that communication occurs in a secure and reliable manne.

HOW THE MANUAL IS ORGANISED

This manual is divided into chapters and the topics included are organised sequentially to accompany each phase, from the system installation to its successive maintenance, step by step.

Chapter 1 describes the MP500/4N and MP500/16 systems, their architecture and devices that may be part of the systems.

Chapter 2 provides basic information about the alarm systems: how the alarm system is made, what it can do, the components it is made of and how they work.

Chapter 3 explains how to design an alarm system using the MP500/4N and MP500/16 control panels, optimising all their potential.

Chapter 4 explains how to install the control panel, the devices, the accessories, and how to connect them all together.

Chapter 5 illustrates the preliminary operations to be carried out to start up the system, before its configuration (for the configuration, see the *Programming Manual*).

Chapter 6 illustrates all the operations to be performed for starting up the alarm system, after having installed all the devices and carried out all the required connections.

Chapter 7 illustrates all the maintenance activities necessary to keep the alarm system functioning with perfect efficiency and provides troubleshooting advice.

Chapter 8 contains the technical specifications of the control panel and the various devices.

The description of the programming and configuration of the system are contained in the *Programming Manual*.

The descriptions the end user will need to use the system are contained in the *User Manual*.

CONVENTIONS USED

For clarity, the manual applies the following conventions:



This symbol signals an important warning.



This symbol signals a recommendation.



This symbol indicates the compatibility with EN50131 grade 3 compliance.

The overall certification of the system is equal to the minimum certification of the devices installed and the functions enabled.



This symbol indicates the compatibility with EN50131 grade 2 compliance.

The overall certification of the system is equal to the minimum certification of the devices installed and the functions enabled.



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



This symbol indicates that the function or the device are not complied according to Standard EN50131.



This symbol indicates that the function or the device invalidate the EN50131 compliance.



Direct input voltage.



Alternating input voltage.



Power supply fitted with double insulator.



See the installation manual of the device.

GLOSSARY

AND	A logical function that requires that all the terms of the operation be true in order for the result to be true.
Open	An input is open when it receives a signal from a detector that is no longer in stand-by, for example, because of an attempted intrusion has been detected.
ATS category SP	Acronym for Alarm Transmission System . Based on the performance they are capable of providing, they are classified from SP 1 to SP 6, where SP 1 is the simplest system and SP 6 is the system with the highest performance. SP = Acronym for Single Path Performance Category.
Communicator	A device capable of sending and transferring alarm signals and events via a telephone line.
Default	The initial value of a device before configuration or when it is restored to the values set by the manufacturer.
DTMF	Dual Tone Multi Frequency, indicates the "tonal" mode of composition of a telephone.
Entry	A point of access to rooms protected by the anti-intrusion system.
Event	A fact that occurs accidentally or when a specific condition is met, for example when a certain period of time has passed.
Physical address	Method used by the control panel to identify and locate inputs and outputs.
Logical address	An alternative addressing method by which the control panel displays inputs and outputs and identifies them in the alarm messages. The addresses can be freely assigned by the user.
Input	A point (terminal block) for the physical connection of a detector (usually a sensor or a contact). An input can be connected to multiple sensors, which are perceived as a single physical entity. The input is defined as being open when the sensor signals that it is no longer in stand-by, for example because it has verified an attempted intrusion.
OC	Open Collector transistor.
OR	A logical function that requires that at least one of the terms of operation be true for the result to be true.
Way	A set of one or more inputs that temporarily inhibit the signalling of sensor alarms connected to enable the entry into or exit of a protected partition. The duration of the temporary disabling is defined as entry or exit time.
Protocol	Set of rules that govern the exchange or the transmission of data among devices.
PSTN	Public Switched Telephone Network indicates the telephone land line.
SELV	Acronym for Safety Extra-Low Voltage (rated voltage max 25 V~ and 50 V=).
Partition	Grouping of entries, exits, user codes, and keys that are associated with a space to be controlled.
Tamper	Protective micro-contact of a device.
TC	Trigger Control, is a signal (voltage) of control that can inhibit the functioning of a sensor or of a signalling device, for example, by putting it in stand-by.
Entry time	The time that the user has available from the moment in which he opens the first input to deactivate the desired partition/s and prevent the generation of an intrusion alarm by the inputs configured as a "Way".
Delay time	The time that the user has available from the moment he opens the delayed input to the moment in which the alarm is generated. It can be programmed for each individual input.
Exit time	The time that the user has available from the moment he activates the partition/s to exit the protected area and prevent the generation of an intrusion alarm by the inputs configured as "Way".
Output	Point (terminal) for the physical connection of a device that enables the intrusion alarm system to act in the external environment, e.g. by signalling an alarm (with a siren), communicating a system status (with a warning light or an acoustic warning device), or activating electrical apparatus.
User	Grouping of one or more partitions.

1 - THE MP500/4N- MP500/16 SYSTEMS

This chapter illustrates the MP500/4N and MP500/16 systems. More specifically, the following are analysed:

- the main characteristics of the systems;
- the system architecture and the maximum dimension possible;
- the connectivity of systems towards outside;
- the various devices and accessories that make up the systems.

1.1 MAIN CHARACTERISTICS

The MP500/xx wired intrusion alarm systems are modular, suitable for small - mid-sized systems in residential, industrial, and service settings.

The components and main functions of the system are complied Grade 3, according to EN50131 standards.

Keypads, readers and expansions are connected to the control panel microprocessor by a proprietary field bus.

Detectors, sirens, and other signals are instead connected to the inputs and outputs present in the control panels and in other devices connected to the bus.

All the inputs can be configured for both type and specialisation.

The remote alarm notifications can be made with vocal message, text message, or numerical protocol (for the connection to alarm reception units).

The system can be managed locally and remotely by means of a land line, cell phone, text message, and Internet.

Other functions available are:

- **Programming via PC** equipped with Hi-Connect software (3.50 or higher).
- **Saving of the program on a USB pen drive** to transfer the program between PCs and control panel or save a back-up copy.
- **Firmware device updates** via USB interface with a pen drive
- **Technological signalling**, that are activated by an event other than intrusion. Following an event of this type, the system can command even specific actuations.
- **Advanced vocal alarm calls**, that allow specific alarm messages to be sent for individual partitions and/or inputs.
- **Vocal message diffusion**, system armed, system disarmed, system diagnostic information can be communicated to user via hands-free vocal messages diffused by vocal keypad.
- **Service vocal message**, the user may use any vocal keypad to issue a memo that will be reproduced locally until the subsequent deactivation, by any vocal keypad.
- **Remote ambient listening function**, enables the user to hear, via telephone, to what is happening in the environment, by addressing up to 8 listening points through the vocal keypads.
- **Vocal help for remote management**, used by the system to guide the user with vocal messages.
- **Door opener**, the electric lock can be controlled via the customized output, limiting access to specific areas only to authorised personnel. Date, time and user who have commanded the opening are recorded in the control panel.
- **Telephonic activation of an output without a connection charge**. By taking advantage of the GSM telephone number recognition by the control panel, it is possible to generate a command on the specific output and close communications after the first 3-4 rings without charging for the call.
- **Advanced automation**. Through the timing programmer built into the control panel, it is possible to arrange a series of automatic and repetitive commands weekly.

Moreover, there are two auxiliary functions that are not in conformity with current laws that allow the guaranteed security of the system to be increased easily and economically, without however replacing the dedicated systems:

- **Emergency response signal**, which generates service signals when a dedicated button is activated or no movement is detected in the controlled environment.
- **Fire alarm**, which generates service signals from part of the control panel when fire detectors managed by the same are installed.



ATTENTION! If the “emergency response call” is required, it is necessary to have a remote emergency response system in conformity with current legislation on this topic.

To create a system that fully meets all the requirements of a fire detection system, consult Elkron's general catalogue in the Fire Prevention section.

1.2 SYSTEM ARCHITECTURE

1.2.1 Architecture

The diagram illustrates the devices and connections that can eventually be managed by the MP500/4N and MP500/16 control panels. For the maximum dimensions the system can reach (combinations of devices and their maximum number) see the paragraph 1.2.3 *Maximum system size*.

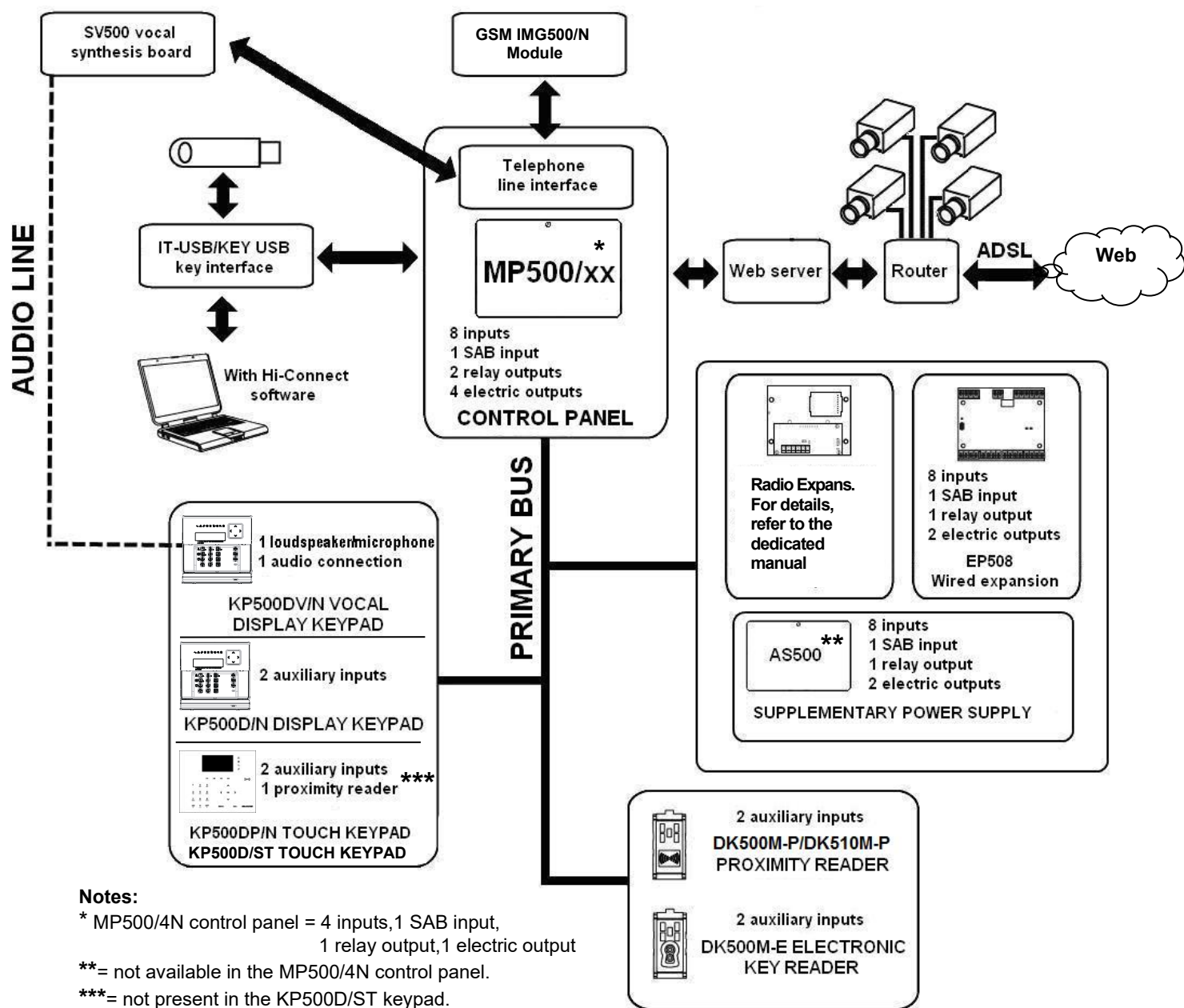


Figure 1 - System Architecture of the MP500/4N - MP500/16

1.2.2 Bus Data

Control panel, keypads, readers, expansion modules and radio modules are interconnected by a 4-wire bus.

The 4 wires transmit information among the various devices and supply 12 V_{DC} power from the MP500/4N or MP500/16 control panel to the keypad, readers, expansion modules, and radio modules.

The use of the bus noticeably simplifies the wiring, given that, for example, the information of a group of detectors located far from the control panel and concentrated on a remote EP508 expansion module can be controlled with just 4 wires.

1.2.3 Maximum system size

Table 1 illustrates the maximum number of keypads, readers, keys and expansion modules that can comprise the MP500/xx systems. For each device, the maximum individuals and combinations are indicated when the system comprises similar devices. For example, the table makes it possible to deduce that the maximum number of readers that can be installed is 32, regardless if just one type or both types in the desired combination are used.

Device	MP500/4N System		MP500/16 System	
	Max Number of each type	Max Number of mixed combination	Max Number of each type	Max Number of mixed combination
KP500D/N Command keypad	4	4**	8	8**
KP500DV/N Vocal command keypad	4		8	
KP500DP/N - KP500D/ST Touch Screen	4		8	
EP508 Expansion module	3	3 (§)	15	15 (§)
Radio expansion	1		2	
AS500/RPT supplemental power supply with repeater	-		15	
DK500M-E Electronic key reader	4	4	16	16
DK500M-P/DK510M-P Transponder reader	4		16	
DK50 Electronic key	16	16	64	64
DK30/DK70 Proximity key	16		64	
Access Code*	16	-	64	-

* of which 1 Master, 1 Technician and 1 Technical Manager.

** by using the Service keypad, the max number is decreased by one unit: it becomes 3 in the MP500/4N control panel, 7 in the MP500/16 control panel.

§ - **WARNING!** The maximum number of the mixed combination must take into account the number of radio expansions.

Table 1 - Maximum system dimension MP500/4N and MP500/16

Table 2 illustrates the maximum number of wired inputs and outputs that a system can reach at its maximum expansion.

Type	MP500/4N System	MP500/16 System
	Max Number	Max Number
Inputs for general use	32	128
Tamper inputs (SAB)	4	16
Relay outputs	4	17
Electrical outputs	7	34

Table 2 - Max number of wired inputs and outputs

1.3 SYSTEM CONNECTIVITY

The MP500/4N and MP500/16 systems can be connected to the external environment in different ways, sending signals and receiving commands.

Possible connection methods are:

- **Public Switched Telephone Network (PSTN).** Requires ILT500-N interface (standard in MP500/16 control panel).
- **Mobile network (GSM).** Requires optional IMG500/N interface.
- **USB.** Requires optional IT-USB/KEY interface.
- **Web Server:** Requires optional IT500WEB interface.

The vocal function requires an optional SV500N.

The table below illustrates the functions available according to the means of communications used.

	Description of information transmitted or received	Means of communications used					
		PSTN and GSM (vocal)	GSM (SMS)	PSTN and GSM (DTMF tones)	Web Server:	PSTN (modem)	SP (IDP, ADF, C200B, C200B P-P)
Sent by the control panel	Signalling of the intrusion/tamper alarm	■	■		■	■	■
	Signalling of pre-alarm					■	■
	Signalling of a technological event	■	■		■	■	■
	Signal of panic/silent panic/emergency response/hold-up	■			■	■	■
	Signalling of arming/disarming of system	■	■			■	■
	Signalling of arming/disarming of partition/s	■	■			■	■
	Signalling of maintenance					■	■
	Signalling of input isolation					■	■
	Signalling of anomaly (black-out/ battery low/system breakdown)	■			■	■	■
	Signalling of end of anomaly	■					■
	Signalling of a communications breakdown ⁽¹⁾	■					■
	Signalling of the end of a communications breakdown	■					■
	Signalling of the use of a false code					■	■
	SIM expiration notice	■	■		■		
	Send images to various alarms				■		
Interaction with the control panel	System arming/disarming command			■	■		
	Command of arming/disarming of partition/s			■	■		
	Video camera activation command				■		
	Controlled output activation command		■	■			
	Controlled output deactivation command		■	■			
	Ambient listening arming command			■			
	Input isolation/inclusion command			■	■		
	Read event log command				■		
	System status request			■	■		

Note ⁽¹⁾: Potential signalling is transmitted from the means of communication available not involved in the anomaly.

DISCLAIMER

The company declines any and all responsibility concerning the unavailability, temporary or permanent, of the PSTN or GSM telephone network that may affect the making of calls or the sending or programmed messages.
Under conditions of a weak or disturbed field, there may be a decline in the performances of the GSM communication vector.

Below are the various connections that can be managed by the MP500 systems and the functions that each one offers.



ATTENTION! Some connections may require the installation of interfaces or other devices that invalidate the EN50131 compliance.

1.3.1 Connection with remote user

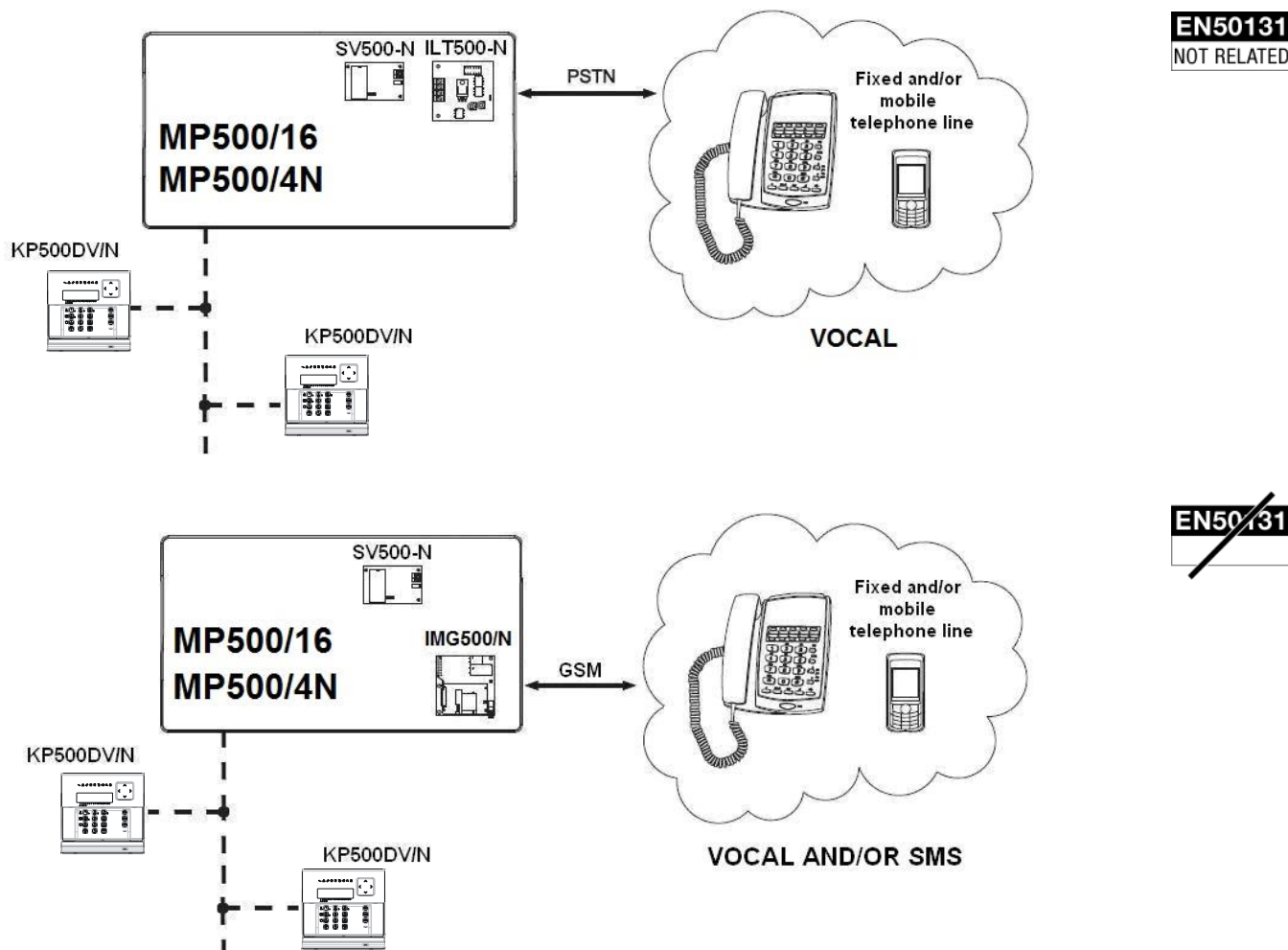


Figure 2 - Diagram of connection with remote user

From the control panel towards the remote user

The control panel, via outgoing calls, can:

- Send alarms and vocal signals (PSTN and GSM).
- Send alarms and signals via SMS (GSM)
- Send calls to request emergency response with the possibility of ambient listening and hands-free listening and speaking (PSTN and GSM). Listening and conversation are possible only if a vocal keypad was installed in the system.

From the remote user towards the control panel

The user, via calls to the control panel, can:

- Use remote management with vocal guide and commands in DTMF for:
 - inquiring about the system status (armed/disarmed, alarms, and anomalies present);
 - partition activation and deactivation;
 - isolation and resetting of inputs;
 - output remote controls (for gate opening devices, heating equipment, irrigation, etc.);
 - environment listening (through optional vocal keypads);
 - environment speaking (through optional vocal keypads);
- Remote management with SMS for output remote controls (for gate opening devices, heating equipment, irrigation, etc.);
- "Zero cost" remote management through the Caller ID for output remote controls (gate opening devices, typically).

Notes:

- The GSM IMG500/N interface is an optional item and can be used either as an alternative or together with the PSTN ILT500 interface.
- As regards the GSM interface, using a SIM card (either of the pre-paid or the subscriber type) is sufficient; to avail of the signalling for running out of credit, it is necessary to ascertain this service with the respective mobile phone carrier.

For further information, please see 5.12.8 *Connecting the telephone dialler*.

1.3.2 Connection with a remote PC

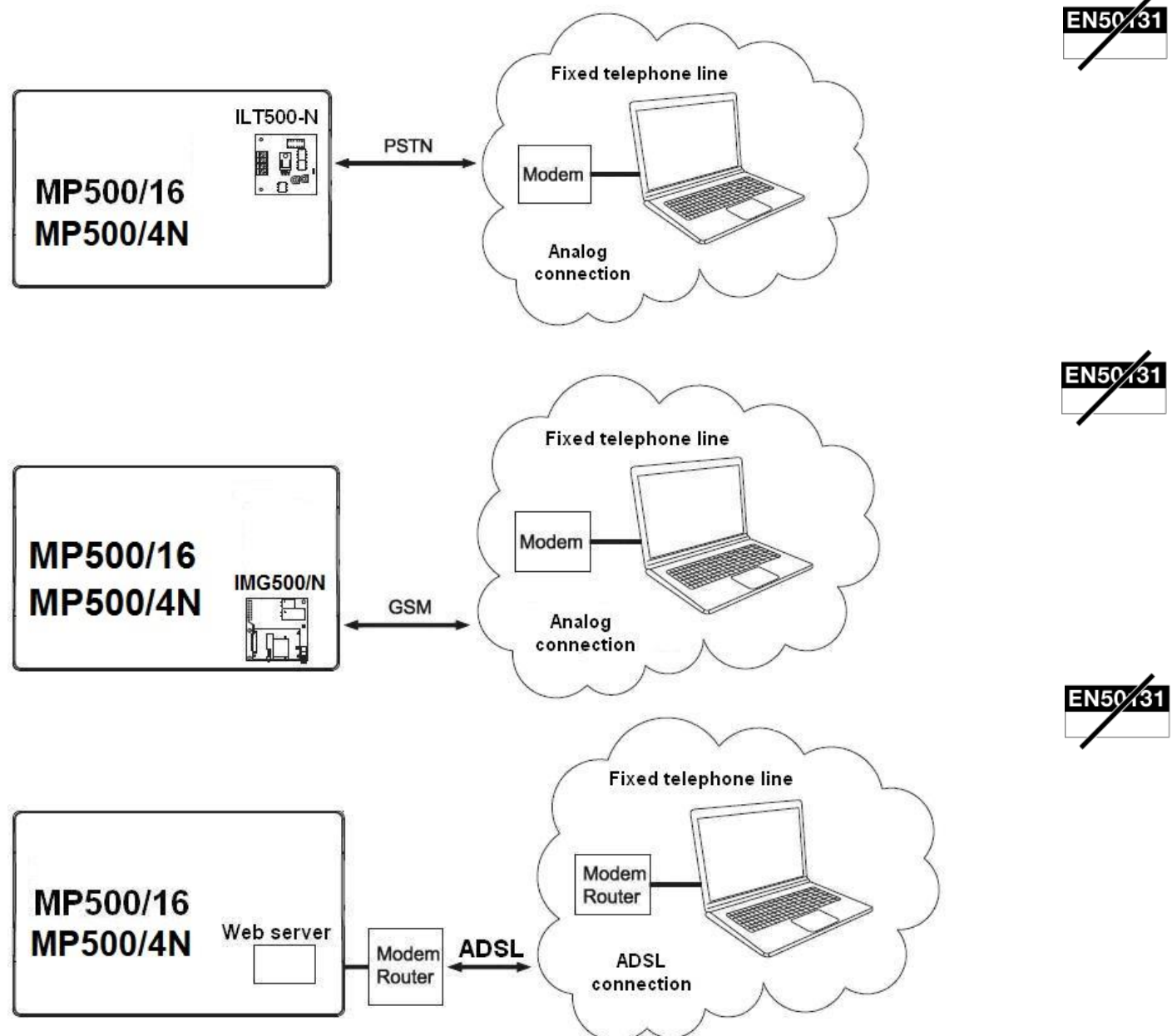


Figure 3 - Diagram of connection with remote PC

From the control panel towards the remote user

From the control panel, via outgoing calls, alarms and signals can be sent directly to the PC.

From the remote user towards the control panel

The user or installer, via calls to the control panel, or incoming calls to the control panel with return call, can:

- Carry out remote programming.
- Carry out remote management for:
 - inquiring about the system status (armed/disarmed, alarms, and anomalies present);
 - visualization of the input status;
 - partition activation and deactivation;
 - isolation and resetting of inputs;
 - enabling and disabling of codes and keys;
 - event log reading.

Notes:

- The GSM IMG500/N interface is an optional item and can be used either as an alternative or together with the PSTN ILT500-N interface.
- In the GSM interface it is necessary to use a SIM card enabled for data/incoming fax + voice (the SIM500 was tested with a TIM SIM)
- The PC must have Hi-Connect software installed.

For further information, please see 5.12.8 *Connecting the telephone dialler*.

1.3.3 Connection with a local PC

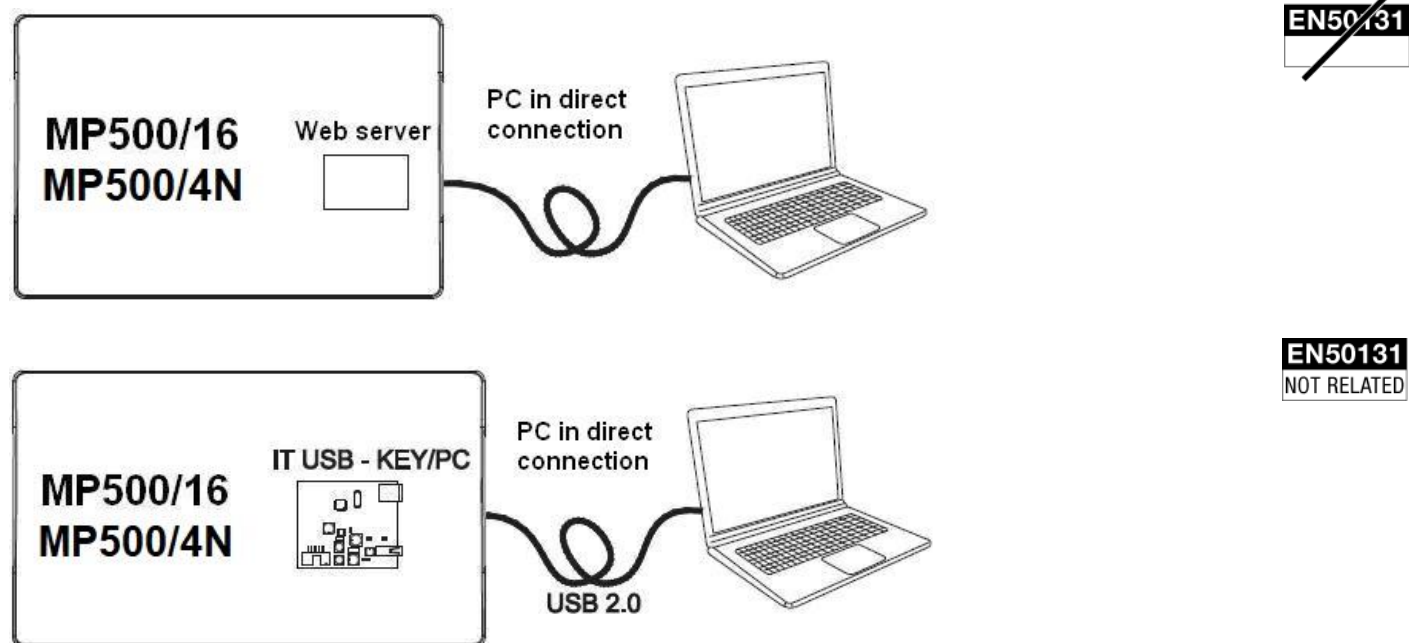


Figure 4 - Diagram of connection with local PC

With the USB and Web server interface, the same functions illustrated in paragraph 1.3.2 *Connection with a remote PC* are available.

Notes:

- The USB interface is generally used during maintenance to programme the control panel.
- For connection via USB, use the IT USB/KEY.
- The PC must have Hi-Connect software installed.

1.3.4 Connection with an alarm reception centre

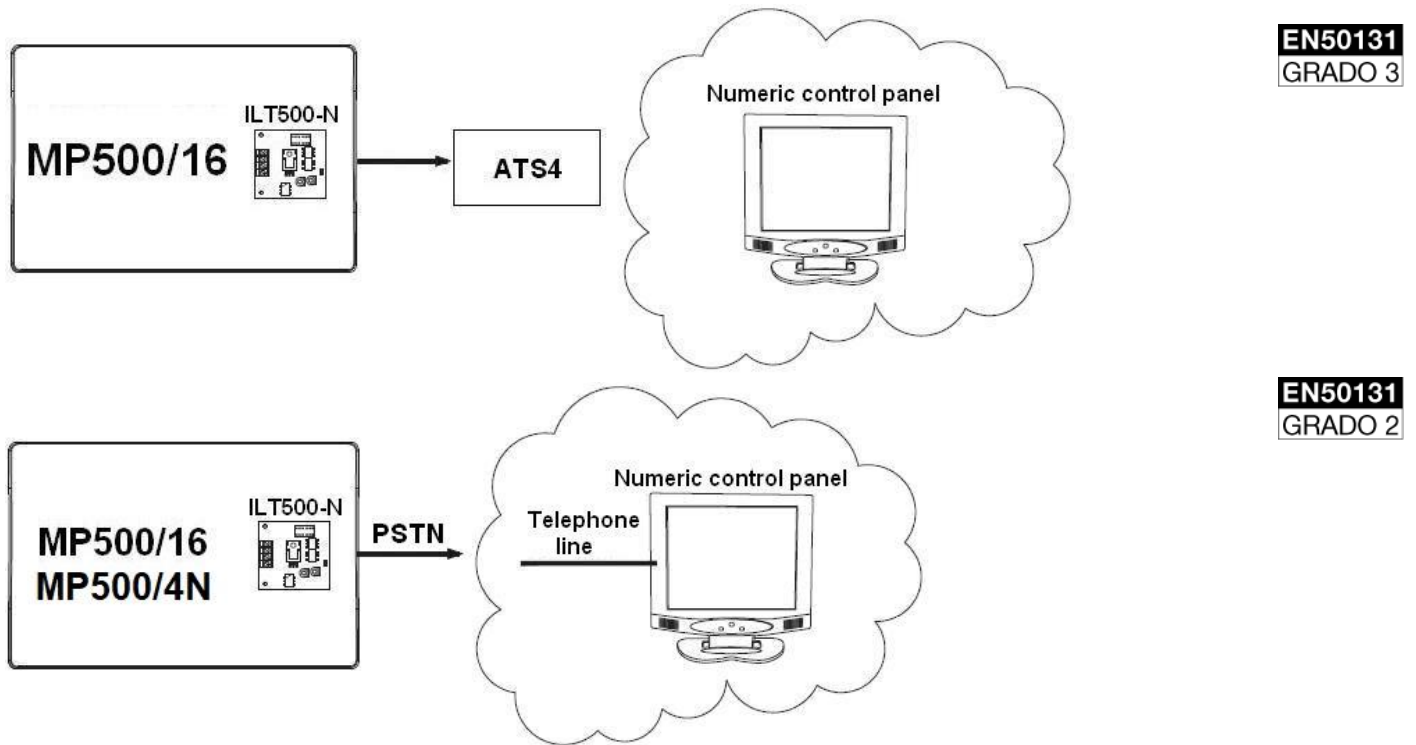


Figure 5 - Diagram of connection with an alarm reception centre

With the traditional telephone network interface (PSTN) ILT500-N, remote surveillance by an alarm reception centre may be used. The control panel sends alarms and signals to the centre using the IDP, ADF, or C200b protocols. The only certified protocol is IDP.

For further information, please see 5.12.8 *Connecting the telephone dialler*.

1.4 SYSTEM COMPONENTS

1.4.1 MP500/4N Control panel



Control panel with a programmable bus to control the system, capable of managing signals relative to intrusion, sabotage, and technological events separately.

The control panel is equipped with:

- 4 inputs;
- 1 balanced SAB input;
- 2 outputs (1 relay output and 1 electric output);
- 1 switching power supply to provide power to internal circuits and devices;
- internal seating for battery;
- internal seating for 4 expansions.

The control panel manages up to 4 distinct partitions.

Other characteristics of the control panel are:

- protection against opening and removal;
- saving of the last 1000 events;
- management of a timing programmer.

The power supply of all the internal circuits and devices is provided by a 230 V~ - 14,4 V_{DC} - 1,5 A switching power supply; the use of a 12 V, 7.2 Ah battery backup is also provided.

The programming is carried out with a keypad through a simple tree menu available in 10 languages.

Otherwise, for greater convenience, the system can be programmed with a local PC, connected to the control panel via the IT-USB/KEY interface and with Hi-Connect software installed (revision 3.60 or later). The programming can be saved on a USB pen drive.

The functional capacities of the MP500/4N control panel can be increased with optional devices.

EN50131 Compliant : Grade 2 - Class II



IMPORTANT! For EN50131 compliance is essential to use the PSTN ILT500-N Communicator.

1.4.2 MP500/16 Control panel



Control panel with a programmable bus to control the system, capable of managing signals relative to intrusion, sabotage, and technological events separately.

The control panel is equipped with:

- 8 inputs;
- 1 balanced SAB input;
- 6 outputs (2 relay output and 4 electric outputs);
- 1 ILT500-N interface for integrated PSTN telephone line;
- 1 switching power supply to provide power to internal circuits and devices;
- internal seating for battery.
- internal seating for 4 expansions

The control panel manages up to 16 distinct partitions.

Other characteristics of the control panel are:

- protection against opening and removal;
- saving of the last 1000 events;
- extractable connector terminals to facilitate wiring;
- management of a timing programmer.

The power supply of all the internal circuits and devices is provided by a 100-240 V~ - 14,4 V $\overline{\text{DC}}$ - 3,4 A switching power supply; the use of a 12 V, 18 Ah battery backup is also provided.

The programming is carried out with a keypad through a simple tree menu available in 10 languages.

Otherwise, for greater convenience, the system can be programmed with a local PC, connected to the control panel via the IT-USB/KEY interface and with Hi-Connect software installed (revision 3.50 or later). The programming can be saved on a USB pen drive.

The functional capacities of the MP500/16 control panel can be increased with optional devices.

EN50131 Compliant: Grade 2 or Grade 3 - Class II

1.4.3 KP500D/N Command Keypad



Keypad with LCD display for interiors. Enables control and programming of the MP500/4N and MP500/16 systems. The keypad is equipped with:

- LCD backlit display with 2x 16 characters with contrast and luminosity regulation;
- 9 LED to signal the system status;
- 12 alphanumerical keys;
- 7 browser keys;
- buzzer with adjustable volume;
- 2 auxiliary inputs.

The keypad is protected against opening and removal and is powered by the bus that connects it to the control panel.

EN50131 Compliant: Grade 3 - Class II - Type B

1.4.4 KP500DV/N Vocal command keypad



The same characteristics as the KP500D/N command keypad, with the 2 programmable inputs. Moreover, it comes equipped with a microphone, loudspeaker, and audio connection for ambient listening, communications with the external environment and/or the alarm reception centre, the emission of vocal recall messages.

ATTENTION! It can be used with MP500/4N and MP500/16 systems. The SV500N is required to be able to use the vocal functions. The installation of the vocal synthesis board results in the loss of EN50131 compliance.

EN50131 Compliant: Grade 3 - Class II - Type B

1.4.5 KP500DP/N Touch Screen keypad



Keypad with OLED display and soft-touch keys for interiors. Enables control and programming of the MP500/4N and MP500/16 systems.

The keypad is equipped with:

- OLED technology graphic display with luminosity regulation;
- signalling of the system status via graphic icons.
- 7 browser keys;
- 4 function keys;
- 12 alphanumerical keys;
- 4 signal LEDs;
- buzzer with adjustable volume;
- transponder reader for proximity keys;
- 2 auxiliary inputs;
- approach sensor.

The keypad is protected against opening and removal and is powered by the bus that connects it to the control panel.

EN50131 Compliant: Grade 3 - Class II - Type B

1.4.6 KP500D/ST Touch Screen keypad



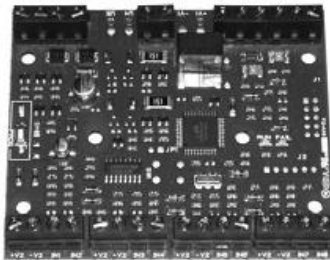
Keypad with OLED display and soft-touch keys for interiors. Enables control and programming of the MP500/4N and MP500/16 systems.

The keypad is equipped with:

- OLED technology graphic display with luminosity regulation;
- signalling of the system status via graphic icons.
- 7 browser keys;
- 4 function keys;
- 12 alphanumerical keys;
- 4 signal LEDs;
- buzzer with adjustable volume;
- 2 auxiliary inputs;
- approach sensor.

The keypad is protected against opening and removal and is powered by the bus that connects it to the control panel.

1.4.7 EP508 Expansion module



Expansion module equipped with:

- 8 inputs;
- 1 balanced SAB input;
- 3 outputs (1 relay output and 2 electric outputs).

The expansion is provided with no casing. It can be installed inside the MP500/4N or MP500/16 control panels or inside a CP/EXP container.

ATTENTION! the absence of a casing compliant Grade 2 or 3 results in the loss of EN 50131 compliance.

The module is connected to the control panel via bus.

EN50131 Compliant: Grade 3 - Class II

From revision SW 3.00.

1.4.8 CP/EXP Container



Container for the EP508 expansion module.

It comes equipped with a tamper device against opening and remove and makes it possible to maintain EN50131 Grade 3 compliance for the EP508 expansion module.

EN50131 Compliant: Grade 3 - Class II

1.4.9 CP/EP500 Container

Protective plastic container for EP508 (not certified).



1.4.10 DK500M-E Electronic key reader

Reader for DK50 keys.

The device comes equipped with:

- 5 signal LEDs: 4 for system status and 1 for the alarm and signal memory;
- 2 inputs.



With the use of optional adaptor frames, the reader is compatible with the following civil lines: Simon Urmet nea, BTicino Living International, BTicino Light, BTicino Living, BTicino Axolute, Gewiss Playbus, Ave Habitat Sistema 45, Vimar Idea, Vimar 8000, Vimar Eikon.

The reader is powered by the bus that connects it to the control panel and is configured via programming.

The reader is to be assembled on a civil line electrical box protected by a tamper device suitable connected to the reader.

ATTENTION! the absence of a tamper compliant Grade 2 or 3 results in the loss of EN 50131 compliance.

The reader is powered by the bus that connects it to the control panel and is configured via programming.

EN50131 Compliant: Grade 3 - Class II.

Also available in white with the product code DK500M-E/B

1.4.11 DK50 Electronic key

Electronic key for total or partial connection or disconnection of the system via the DK500M-E reader.



Each key has a distinct code, set by default, with more than 1099 billion possible combinations. It is possible to program up to 16 keys for the MP500/4N control panel and up to 64 keys for the MP500/16 control panel. Moreover, each key can be enabled or disabled individually and equipped with a descriptive name.

EN50131 Compliant: Grade 3 - Class II

1.4.12 DK500M-P Transponder reader

Transponder reader for DK30 keys. The device comes equipped with:

- 5 signal LEDs: 4 for system status and 1 for the alarm and signal memory;
- 2 inputs.



With the use of optional adaptor frames, the reader is compatible with the following civil lines: B-ticino® Light / International / Living ; Gewiss® Playbus ; AVE® Sistema 45 ; Axolute® ; Eikon® ; Vimar® Idea ; Vimar® Plana; Vimar 8000 ; Simon Urmet nea.

The reader is powered by the bus that connects it to the control panel and is configured via programming.

The reader is to be assembled on a civil line electrical box protected by a tamper device suitable connected to the reader.

ATTENTION: the absence of a tamper compliant Grade 2 or 3 results in the loss of EN 50131 compliance.

The reader is powered by the bus that connects it to the control panel and is configured via programming.

EN50131 Compliant: Grade 3 - Class II

Also available in white with the product code DK500M-P/B

1.4.13 DK30 Proximity key



Programmable electronic key for total or partial connection or disconnection of the system via the DK500M-P reader.

Each key has a distinct code, set by default, with more than 4 billion possible combinations. It is possible to program up to 16 keys for the MP500/4N control panel and up to 64 keys for the MP500/16 control panel. Moreover, each key can be enabled or disabled individually and equipped with a descriptive name.

EN50131 Compliant : Grade 3 - Class II

1.4.14 DK30-50 key personalisation kit

A kit to personalise DK30 and DK50 keys with coloured inserts.

The package contains inserts in 6 different colours that result in 27 different colour combinations.

1.4.15 MIFARE DK510M-P Transponder reader

Transponder reader for MIFARE DK70 keys. The device comes equipped with:

- 5 signal LEDs: 4 for system status and 1 for the alarm and signal memory;
- 2 inputs.



With the use of optional adaptor frames, the reader is compatible with the following civil lines: B-ticino® Light / International / Living ; Gewiss® Playbus ; AVE® Sistema 45 ; Axolute® ; Eikon® ; Vimar® Idea ; Vimar® Plana; Vimar 8000 ; Simon Urmet nea.

The reader is powered by the bus that connects it to the control panel and is configured via programming.

The reader is to be assembled on a civil line electrical box protected by a tamper device suitable connected to the reader.

ATTENTION: the absence of a tamper compliant Grade 2 or 3 results in the loss of EN 50131 compliance.

The reader is powered by the bus that connects it to the control panel and is configured via programming.

Also available in white with the product code DK510M-P/B.

1.4.16 MIFARE DK70 Proximity key



MIFARE Programmable electronic key for total or partial connection or disconnection of the system via the DK510M-P reader.

Each key has a distinct code, set by default, with more than 4 billion possible combinations. It is possible to program up to 16 keys for the MP500/4N control panel and up to 64 keys for the MP500/16 control panel. Moreover, each key can be enabled or disabled individually and equipped with a descriptive name.

1.4.17 AS500/RPT supplemental power supply with repeater



The AS500 supplementary power supply unit is an optional device for the MP500/16 control panel.

It comes equipped with an electronic board that integrates an EP508 type expansion connected directly to the control panel BUS, a repeater module to extend the control panel BUS, and a supplementary power supply unit capable of powering the devices connected to the system.

The AS500 unit comes equipped with:

- 8 inputs;
- 1 balanced SAB input;
- 3 outputs (1 relay output and 2 electric outputs).
- 1 switching power supply;
- internal seating for battery;
- internal seating for 2 expansions.

The power supply is provided by a 100-240 V~ - 14.4 V $\overline{\text{---}}$ 3.4 A switching power supply; the use of a 12 V, 18 Ah battery backup is also provided.

ATTENTION! It can only be used with MP500/16 system.

EN50131 Compliant: Grade 2 - Class II

From the revision SW 2.00.

1.4.18 SV500N-I-F-GB vocal synthesis board



A vocal synthesis board for the MP500/4N and MP500/16 control panels with pre-recorded messages in Italian, French, and English makes it possible to record and listen to vocal messages. The KP500DV/N vocal display keypad or the microphone with earphone can be used to record the messages.

The SV500N E/D/SL version is available with pre-recorded messages in Spanish, German, and Slovenian.

1.4.19 ILT500-N PSTN telephone communicator



ILT500-N Communicator is the interface allowing to connect the control panel to the normal PSTN phone line for sending alarm signalling and receiving remote commands. It can also be used combined with the GSM IMG500/N module.

PSTN Communicator is equipped with a phone line input / output terminal block and a yellow LED indicating that the phone line is busy.

The ILT500-N communicator is supplied as standard equipment in MP500/16 control panel.

1.4.20 IMG500/N GSM Module



This interface enables the connection of the MP500/4N and MP500/16 control panels with the cellular telephone network (GSM) to send alarm notifications and receive remote commands.

The interface comes equipped with a GSM dual-band transmitter-receiver (900/1800 MHz) and an antenna to be installed inside the MP500/4N control panel. The MP500/16 control panel requires that the antenna be suitable for GSM2 metallic box.

If the internal antenna should fail to guarantee the GSM module adequate signal levels, due to the position of the control panel, it is possible to use an external GSM 1 antenna (not included in the package).

IMPORTANT! The installation of the IMG500/N GSM module results in the loss of EN50131 compliance.

1.4.21 Remote GSM 1 antenna



Optional external antenna to be used with the GSM IMG500/N module when, due to the position of the control panels, the internal antenna provided with the package should not guarantee the module adequate signal levels.

The remote antenna come complete with a bracket, expansion screws, and 5 metres of coaxial cable with an SMA-M connector.

1.4.22 Antenna for GSM 2 metallic box



Antenna with an SMA-M connector compatible with the GSM IMG500/N module, to be used when the GSM IMG500/N model is installed inside the MP500/16 control panel (metallic box).

1.4.23 Cable for KP SERVICE keypad



Optional cable to connect a service keypad (KP500D/N or KP500DV/N, as desired) to the MP500/4N and MP500/16 control panels for programming the system.

The cable comes equipped with a connector compatible with the mother board SERVICE connector of the MP500/4N and MP500/16 control panels.

1.4.24 USB interface for connection to the PC and USB IT-USB/KEY keys



Optional interface to connect a PC to the MP500/4N and MP500/16 control panels for programming and a USB Pen Drive for saving and restoring system programming and other data.

1.4.25 Hi-Connect application software (rev. 3.60 or later)



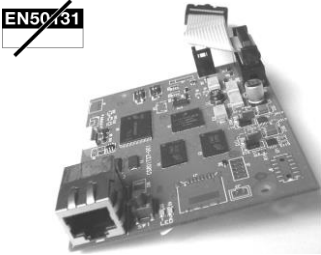
Software for local programming with a PC and remote management of the MP500/4N and MP500/16 control panels.

Minimum PC configuration requirements:

- Intel Pentium IV 1. GHz processor or equivalent;
- 256 MB RAM;
- Internet Explorer 5 or later;
- Windows 2000 / XP Service Pack 2 / Vista / Windows 7 / Windows 8 / Windows 10;
- CD ROM reader;
- USB port available.

The minimum HW configuration also depends on the operating system installed (more recent operating systems may require more powerful processors or a greater quantity of RAM).

1.4.26 IT500WEB web server interface



Optional interface with integrated web server function to connect the MP500/4N and MP500/16 control panels to the LAN network or through an ADSL modem router to the Internet.

It makes it possible for any device with a web browser (PC, tablet, smart phone) to access safety (http, VPN) a series of control panel functions, like: system status, activations, event logs, etc...

It is also compatible with the use of the IP Elkron video cameras.

2 - BASIC INFORMATION

This chapter explains the composition of the intrusion alarm system and is intended for those who are designing an alarm system for the first time.

If you have experience in designing installations, you can skip directly to Chapter 4, where the MP500/4N and MP500/16 systems are discussed and their advanced and special functions are illustrated and explained with specific examples.

2.1 HOW AN INTRUSION ALARM SYSTEM IS MADE

2.1.1 The simplest system

The most elementary alarm system consists of just 3 devices: a detector, a siren, and a management device called a control panel, which receives information from the detector, processes it and, if necessary, sounds the siren to warn of potential danger. Although simple, this type of system is perfectly adequate for fulfilling the use for which it was intended: generate an alarm when an attempted intrusion is detected.

Actually, alarm system are more complex and consists of a higher number and variety of devices, both because the need for protection is greater and because it is always necessary to use the device best-suited to attaining a specific objective, whether with regards to user friendliness or the desired option of integrating advanced functions and not being limited to a simple alarm. It is important to note that every system, regardless of its complexity or size, has only one control panel that acts as the "brain" for the entire system.

2.1.2 Wired, radio, and bus

This main distinction between installations is based on the technology used to connect the various devices to the control panel and each other: wired or radio. The latter system is also called wireless.

Each of these two types of connections has strong points, while other characteristics make it less suitable for specific uses. The table below illustrates the pros and cons of both solutions.

WIRED		RADIO	
Pros		Pros	
• The system is not affected by radio shields and within the maximum distances indicated, the control panel can be positioned at the most convenient point. • It is essentially immune to standard electromagnetic disturbances: devices that emit radio frequencies or power lines create no communication problems.		• Requires no wiring: all communications occur via radio and components can be positioned where it is most convenient. • The devices can be easily moved if the need should arise, for example if the arrangement of furniture should change in a room protected by a volumetric detector. • It is possible to create a system where all the components are powered by long-life batteries, so it is not necessary to connect the system to the electrical power supply *.	
Cons			
• Wiring is necessary: all the detectors and signalling devices must be connected to the control panel with wires. • The positions of the devices are practically fixed, given that moving them would require rewiring everything, with all the difficulties inherent to such a project. • Installation times are longer, as it is necessary to wire everything. If the apartment or office does not already have a conduit system, installation times are prolonged because the wiring must be run under the board and door casing to hide it, create holes in the walls and ceilings, etc. • Extensive installation times may create inconveniences if the premises are inhabited.		• Quick installation: it is sufficient to install the system components where needed, with no need to wire them. • Installation times are considerably shorter, so as not to create inconveniences in the home or workplace.	
	Cons		
	• It is sensitive to radio shielding: some materials can affect the radio waves, impeding or making communication more difficult among the various devices. • It is more sensitive to sources of electromagnetic disturbances (ex. electric meters, electric motors, washing machines, refrigerators, etc.), which may make communications among the various devices difficult. • It is necessary for at least one radio channel to be free (in other words, one channel with no other systems using it).		

* Not all manufacturers have radio alarm systems that can function entirely without being connected to the electrical utility.

Table 3 - Comparison of wired and radio technologies

Wired technology is particularly indicated:

- in new constructions or in those to be remodelled, where it is possible to have a conduit system where wires can be passed;
- in those situations where radio shields or significant sources of electromagnetic disturbances are found;

Radio technology is particularly indicated:

- in inhabited buildings or where it is not possible to intervene on the wall structure;
- where wiring can be particularly costly and difficult;
- for temporary intrusion alarm systems;

As can be deduced from this information, both technologies are in some way complementary. Where one is weaker, the other is stronger. For this reason, there are market solutions that allow the creation of hybrid systems, where both technologies can be used to benefit from the best of both.

2.1.2.1 Radio apparatus

There are two types of radio apparatus used in the alarm systems: those that allow the system to connect to the external environment, like the radio modules for the cell phone network, and those that allow wireless communications within the system, mainly between radio devices and the control panel.

It is important to verify that the radio devices of the alarm system use the specific frequencies established by legislation and that they are capable of using more than one radio channel.

Some may ask: can these radio devices create disturbances for other equipment present? Are all these electromagnetic waves harmful?

The answer to the first question is very simple: the conformity with laws practically excludes this type of problem.

The same is true for the second question, but in this case it is better to analyse the topic in more detail. Above all, the radio devices transmit with extremely low power; secondly they mainly work as receivers and transmit only when necessary and for durations of just a few seconds. In other words: they almost never transmit and so do not emit electromagnetic waves; when they must do so it is only for very brief moments and very low power.

2.1.2.2 The bus

A particular type of connection is the bus, which can be either wired or radio. It is essentially a channel of communication that transfers data and information among the various devices of the system, guaranteeing their interaction.

A wired bus may physically resemble an ordinary "electrical connection, but one that transmits enormous quantities of data and information in digital format, following a specific protocol. One bus can connect several devices together, thereby simplifying a wiring project.

2.2 COMMUNICATING WITH THE EXTERNAL ENVIRONMENT

If suitable designed, the alarm system may interact with the external environment not only locally, but also remotely. Alarms, signalling, images, and sounds can be replicated event at a distance of thousands of kilometres. Likewise, although far away, enabled users can send commands to the system, activate its functions, and even manage it.

What it is possible to receive or do depends on the functions offered by the system, on the means of communication used, and on the remote device used.

The main means of communication used by the intrusion alarm systems are:

- Telephone network
- Mobile network (GSM).
- Internet
- LAN

The receivers of the signals may be, in addition to the owner and other contacts he selects, Law Enforcement bodies, Security agencies, and alarm reception centres.



ATTENTION! The possibility of sending alarm signals to State or local law enforcement must be requested explicitly and authorised by them. More details can be obtained at the local or regional police station. Security services and alarm reception centres offer the service for payment.

The company that installed the system may be among those enabled to remotely operate it. In this way it is possible to conduct diagnostics and eventual maintenance more easily, because the technician need not go there directly, but will be able to work remotely with a PC.

In the best systems, security against unauthorised access is guaranteed by the fact that each remote connection session by the installer must be previously authorised by the owner.

Maintenance interventions of this type may be charged for separately.

The presence and type of the means of communication used by the intrusion alarm system can influence its certification.

2.3 THE DEVICES USED TO CREATE AN ALARM SYSTEM

Essentially, an intrusion alarm system consists of four types of components:

- the control panel;
- the detectors;
- the signalling devices;
- the complementary devices.

These components are generally separate, but sometimes a single device may enclose more than one.

Below are illustrations of these components: what they are called, how they are made, and how they work.

2.3.1 The control panel

The control panel is the "brain" of the system and has various functions:

- it interprets different signals that arrive from the detectors and then takes the most appropriate action, like ignoring the opening of a window if the system is disarmed or activating notification devices if it is opened while the system is armed;
- check that all the system devices are always functioning correctly;
- signal potential anomalies that may threaten security and the functionality of the system;
- record all the main events.

An intrusion alarm system only has one control panel.

2.3.2 The detectors

The detectors are devices capable of detecting changes - voluntary or involuntary - that an element or physical characteristic of the environment where they are installed may undergo. A detector has one or more sensors that perceive these changes.

The detectors must be designed and installed so as to maximise the detection and minimise the risk of false alarms.

For the alarm system, the detectors are equivalent to our senses.

The detectors may distinguish events according to:

- a functioning principle;
- a type of change that must be signalled;
- where they must be applied and what they must control;
- the physical characteristics of the environment they must monitor.

2.3.2.1 Button

This is absolutely the easiest detector to use. There are all types available, from those that are activated manually, those that must be pulled, and those that can be pressed by foot. It is sometimes an extension of a more advanced detector.

2.3.2.2 Magnetic contact (reed)

This contact is used to control the opening of doors and windows. The opening sensor has two parts: a magnet and a blade contact, or something similar. When they are placed next to each other, at a distance of a few millimetres, the magnetic field of the magnet keeps the blade contact in position to close the electrical circuit. Separating them reduces the force of the magnetic field, the blade is no longer in position, and the electric circuit is broken, generating an opening signal. The magnet is applied to the door or casement and the magnetic contact is applied to the frame, as far as possible from the hinges, so that even slightly opening the door or window may break the circuit. There are various models available to meet a wide range of aesthetic and technical demands (wooden doors and windows, security doors, sunken contacts, etc.). This detector is used mainly to create perimeter protection.

2.3.2.3 Cable contacts for rollers

The detector is installed inside the roller box. The sensor is an impulse counter that is paired with an automatic cable winder. By connecting the end of the thin cable to the lower part of the roller, each time the blind is raised or lowered, the cable winder turns and generates the impulses detected to the counter. Depending on the number of impulses generated during a specific interval, the detector can signal an attempted intrusion. This type of detector makes it possible to keep the windows open and the rollers closed to help air to circulate, thereby guaranteeing perimeter protection.

2.3.2.4 Broken glass detector

This detector can be created using various technologies and exploiting different principles of physics. For example, it can detect the oscillations caused by the breaking or cutting of glass when it is glued to the glass or crystal to be protected, or detect the characteristic sound waves generated by glass breaking, when it is positioned in the immediate vicinity. It is used to signal the breaking of shop or showcase windows, large plate glass windows and skylights for perimeter protection, but also for breaking of bulletin boards and display cases inside buildings.

2.3.2.5 Vibration detector

Also known as a seismic detector, this device picks up vibrations from the surfaces it is glued or screwed to and filters them to prevent false alarms. When applied to a door or window, unlike the magnetic contact, it can signal an attempted break-in before the door or window is actually opened. Indeed, by seeking to force the opening, vibrations are produced that generate a signal of attempted intrusion.

2.3.2.6 Passive infra-red detector (IR)

This detector is equipped with one or more IR sensors that measure the rapid variations of infra-red traces of the environment being controlled, indicating the presence of human beings, animals, or other "warm" objects that move. A variation of this type generates a signalling by the detector. The effectiveness of the detector and the area covered are changed by adjusting its sensitivity, changing the Fresnel lenses that focus on the sensor the controlled area or by suitably masking the sensor itself. Some detectors make it possible to create a curtain covering, or to monitor a very long and narrow vertical area, typically positioned parallel and not far from a group of windows or doors (hence its name). In the intrusion alarm system, these detectors are used to control extensive spaces and obligatory passages, also being identified as volumetric sensors.

2.3.2.7 Active infra-red detectors

This IR detector consists of two elements that face each other and are aligned to create an infra-red ray barrier. When an object passes through the passage controlled by the detector, the rays are interrupted and the IR sensor generates a signal. Technically, the detector can be created in two different ways. In the first way, the two elements contain one sensor and the other light sources that emit a ray of infra-red light. In the other, an element contains both the sensor and the infra-red light source and the other element consists of a mirror that reflects the IR light towards the sensor.

2.3.2.8 Microwave detector (MW)

This detector acts like a radar: it emits a radio signal and then detects and analyses the return signal (reflected waves). When the return signal varies, due to something that has moved in the area covered by the detector, a signal is generated by the detector. Unlike the passive IR detector, the movement are detected even if the person moving emits or blocks heat. In the intrusion alarm system, these detector are used to control extensive spaces and obligatory passages, also being identified as volumetric sensors.

2.3.2.9 Combined passive IR and microwave detector

This type of detector combines both technologies. The signals generated by the sensors can be compared to OR or AND logic. In the first case it is sufficient for just one sensor to detect an anomaly for the detector to send a signal; in the second case, both sensors must detect an anomaly for a signal to be sent. The two settings have a mirror effect. With OR, the possibility of identifying attempts to intrude increase (what one sensor detects, the other sensor might not), together with and increase in the generation of false alarms. With AND, the possibility of generating false alarms decreases (the sensors must essentially confirm each other), but the sensitivity in detecting attempted intrusions also decreases.

2.3.2.10 External detectors

The external detectors are essentially a specialisation of some of the types of detectors already illustrated herein.

An external detector has a more resistant protective casing that enables it to resist the elements as well as attempted sabotage. Even the sensors used can have higher performance scores, but the operational principles are the same.

2.3.3 The signalling devices

This category includes all the devices capable of notifying people and other systems or equipment of a dangerous situation for people or property placed under the protection of the intrusion alarm system.

2.3.3.1 Siren

The siren is a device that emits a very powerful sound that can easily be heard at a distance to warn of an attempted intrusion. External sirens must have a power of at least 100 dB, while internal sirens must have a power of at least 80 dB at 1 metre; if the sound is less powerful than these standards, the device is simply an acoustic signal. The siren is a mandatory element. The minimum and maximum duration of the acoustic signal is established by law and by national and local regulations and provisions. In addition to the external siren, the alarm systems must also have an internal acoustic warning device. This warning device need not necessarily be a separate component, but may be a function performed by some other device, like the control panel.

2.3.3.2 Flasher

The flasher is a visual warning usually combined with the external siren. The flasher signals a message through codified sequences of lights and is visible at a great distance. In addition to signalling an attempted intrusion, based on the capacity of the control panel the flasher can provide further information, like the visual confirmation of the system arming and disarming from the external, the presence of alarms saved, etc.

2.3.3.3 Communicator

The communicator is an interface, sometimes also called the auto-dialler, which enables the system to send alarm signals or other signals at a distance and, if configured to do so, receive commands from remote. There are two types of devices: the one to connect to the traditional telephone network (PSTN) and the one to connect to the mobile phone network (GSM and later). The two interfaces can co-exist in the same system, where each one constitutes the back-up of the other. These interfaces are usually hosted inside the control panel, but they can also be an independent device, physically separated from it.

The signals sent from a communicator can be either vocal or SMS (towards telephone numbers) or in numeric format (for an alarm reception centre). The commands can be received from the control panel in the form of DTMF signals or SMS, or in numerical format. What can be obtained by using a communicator depends on the network and on the channel of communication used, as well as the functions the control panel can carry out.

The level of detail of the signals received may vary considerably and depend on the control panel, on the channel of communication used, and on the auto-dialler. It may range from a simple vocal message like "Intrusion alarm in ...street" to a signal that includes the indication of which detector signalled the alarm, the time it occurred, and so forth.

2.3.4 The complementary devices

The complementary devices complete the alarm system by adding functions and simplifying its use.

The main complementary devices are:

2.3.4.1 Keypad

The keypad is a device with multiple functions, including:

- authenticating the users on several levels;
- totally or partially arming and disarming the alarm system;
- signalling alarms saved and potential malfunctions;
- activating alarms;
- programming the alarm system;
- enabling and disabling functions.

The keypad has the advantage, compared to other systems used to arm and disarm the alarm system, of separating the physical objects that acts (the keypad) from the enabling to do it (the authentication code that the user memorizes), contributing to a higher level of security. Some keypads have other functions, like the possibility to conduct ambient listening or establish a remote vocal communication.

Not all the keypads are separate objects. In some cases, the keypad is an integral part of the control panel.

2.3.4.2 Reader

The readers are devices for totally or partially arming and disarming the alarm system. They are typically located outside of the zone protected by the system. The reader has LEDs to signal the system status (armed/disarmed) and potential alarms or anomalies present. The two most common types of readers are those with electronic keys and a transponder. With the first, a device with surface contacts that resembles a key (hence the name) is introduced into the reader. With the second, a proximity key is put near the reader. In both cases the reader reads a code that, if recognised, enables the system status to be changed.

They are easier to use than a keypad, but the electronic and proximity keys should be stored carefully and kept separate from the other security keys (it is the same time of precaution taken with a debit card and its PIN).

2.3.4.3 Remote control

The remote control is a radio device that allows the arming and disarming of the alarm system from a distance. The latest models have the possibility to personalise the use of some keys, for example to activate or deactivate a commandable output. For this type of device, the warnings indicated for the reader are also valid.

2.3.4.4 Power supply

The power supply is used to provide electricity to the system devices, drawing it from the electrical network and transforming it into low voltage.

The supplementary power supplies are used when those already present, like the one of the control panel, are not capable of distributing all the electricity necessary or when, due to long connection wires, the correct voltage may not be reaching the remote device.

The more advanced power supplies make it possible to also connect a local back-up battery.

More detailed information on how the alarm system is powered can be found in *The alarm system power supply*.

2.3.4.5 Expansion

The generic term of expansion is used to identify an entire series of devices that can increase the dimension of the system or add new functions or capacities to it.

2.4 OTHER DEVICES THAT CAN BE INTEGRATED INTO THE ALARM SYSTEM

An alarm system can integrate other devices that offer functions other than those linked to intrusion.

The control panel must deal with this integration as it must be able to interface and manage these devices. Not all control units are capable of doing so. If you intend to add one of these devices, during the creation of the system or as a future upgrade, it is necessary to verify if the control panel to be purchased will be compatible with these devices.

These are some of the devices that could be integrated, but is not considered an exhaustive list:

- detectors links to general security, or those capable of signalling potential flooding, gas links, fumes, etc.
In this case existing signalling systems (sirens, communicators) to notify alarms can be used;
- automations, like a gate opener;
- medals, buttons, or other devices to generate an “emergency response signal”;
- programmable thermostats and other domotic devices (an interface may be necessary);
- video surveillance system. In this case, if the camera or the device that manages it are capable of automatically recognising potential movements in the zone being filmed, if necessary, it would be possible to use the signal generated as an indication of an attempted intrusion, which must be managed by the alarm system.



IMPORTANT! Many of these devices enhance the functions of the alarm system, but are not economic alternatives to systems dedicated and in compliance with current laws. If a certified solution is necessary, for example in the case of emergency response systems or fire alarms, using the intrusion alarm system may not be the best decisions.

3 - DESIGN: CONFIGURATION OF THE ALARM SYSTEM

This chapter explains how to design and alarm system with the MP500/4N and MP500/16 systems.

Even if you have experience in designing intrusion alarm system, we advise you to read this chapter because it contains important information on how to get the most out of functions provided by the devices used and to comply with relative laws.

3.1 IDENTIFYING THE GRADE OF PROTECTION

The designer of the intrusion alarm system, in order to select the grade of protection, must take into consideration:

- the nature of the rooms,
- the value of the goods to be protected,
- the potential risk of intrusion,
- potential threat to people,
- any other element that may be a cause of risk to people or property.

Once the designer has identified the necessary grade of protection, it is the responsibility of the installer to create the intrusion alarm system with the correct level of security. For more information, please see the paragraph on *Conformity with standard EN50131-1*.

3.2 THE ALARM SYSTEM POWER SUPPLY

In order to function, an alarm system needs electrical energy, which can be supplied by either mains power supply, a battery, or other instrument capable of generating or providing electrical current.

There are three types of configuration for providing the necessary electrical energy:

1. A primary power source, like the mains power supply, and a secondary source of power charged by the same system, like a rechargeable battery that is charged automatically through a system component.
2. A primary power source, like the mains power supply, and a secondary power source not charged by the same system, like a high-capacity, long-lifetime battery.
3. The only primary source with a finite capacity but that ensures extended duration, like a lithium battery.

The term "power supply" can be used to indicate any of these configurations.

The secondary power supply as a back-up to operate the alarm system in case of a breakdown or temporary loss of primary power, making it possible to continue providing the protection for which it was installed.

The minimum duration of the power supply that must be ensured by the secondary source is specified by law. During this period of time, which is measured in hours or tens of hours, normal functioning of the entire system must be guaranteed, including alarm signals and other necessary notifications. The rule establishes that the higher the grade of security of the system, the longer the minimum duration must be. If the secondary power source cannot be recharged, the minimum durations double.

Obviously, systems can be created in which the duration of the secondary power supply is higher than the minimum required, for example, by using batteries with a higher capacity. This minimum life spans may also be reduced, provided that other conditions are in place.

For example, it is possible to do so if the breakdown as the primary power source is notified to an alarm reception centre or to another remote centre, or if there is a supplementary primary power supply, like a generator, that immediately and automatically replaces the main one if needed.

In the third type of power supply listed above, the primary source must guarantee long-term functioning. Standard require that the battery be able to provide power for at least one year, under any usage conditions. Furthermore, the power supply must generate a signal or a break-down message before the voltage diminishes to below the value necessary to maintain normal functioning of the system.

The passage from the primary to secondary power supply takes place without modifying the status of the alarm system. When there is this type of switching, notifications can be generated and sent, usually one to signal the lack of mains power supply and successively, one for the reset of electrical power once the mains power supply has been restored.

The power supplies can be located in one or more components of the alarm system, or even in a separate container.

The power of the power supply is very important. It must not only be able to power the entire system at its maximum rated absorption, but must also contemporaneously recharge the batter, up to 80% of its capacity, within a maximum time established by law. To this view, the higher the grade of security of the system, the quicker the recharging must be.

Let's example the typical alarm system to understand how they are powered. Particular or complex systems can have different configurations.

Wired systems

The power supply and the battery are contained in the control panel, from which multipolar cables branch out to connect the various devices. These cables include two conductors dedicated to the transport of power to the devices. The mains power supply provides the primary source of electricity to the control panel, which in turn powers the various devices. When the power network is interrupted, the battery takes over to power all the system devices. Once the electrical current is restored, the battery is disabled and the power supply recharges it to its maximum capacity.

One particular function is the main siren. This is in fact equipped with a rechargeable battery or batteries that enable it to generate acoustic and light alarms, even if electrical current is missing from the control panel. Devices of this type are called "self-powered". If the battery installed is rechargeable, then the power supply that arrives from the control panel is also used to maintain the charge or recharge it as needed.

Radio system

In this case all the devices are equipped with non-rechargeable batteries. The radio control panel, instead, can be completely powered by batteries or have both a power supply and a battery, like a standard wired control panel. The last configuration is obligatory when the control panel has a communicator inside for the mobile telephone network. This device actually consumes a lot of electricity and would soon consume the control panel battery, making the system unusable.

3.3 HOW TO DESIGN AN ALARM SYSTEM

A good design facilitates the work involved in the installation and, more importantly, ensures that the intrusion alarm system fulfils its scope of punctually notifying the presence of any threat to the people or property that it must protect.

Step by step, beginning with defining the security needs, below is an explanation of what to do to protect property and persons, how to choose the devices to reach the objectives, how to install them effectively in the environment and, finally, which checks to carry out if radio frequency extensions are used (radio detectors and other devices connected with the mobile phone network).

3.3.1 Analysis of the site and needs

The first thing to do is to have a clear idea of what must be protected and the needs of the people who must use the system. Being able to have a floor plan or map of the places to be protected helps during the successive planning and installation phases.

The first question to ask is: "Who and what must be protected and what grade of security must be guaranteed?" Indeed, it may be that not all the property must be protected in the same way. For example, a tool shed or a garage may not need to be protected in the same way. It may be that something is not protected because it is not worthwhile, and priority will be given to using resources where there is something truly important to be protected.

It is just as important to understand what current needs are and how they may evolve in the future. The choices for a system are in fact made according to the configuration of the site and places and the user needs. Making the wrong decision because there is not a clear idea of the final result may mean redoing everything, which in turn leads to higher costs.

3.3.2 Certification requirements

The certification of a system according to intrusion alarm system laws and standards is very important. Firstly, because certification ensures that the alarm system provides the desired protection, secondly because it could be a prerequisite for eligibility for discounts on insurance policies or the possibility of being connected with Law Enforcement bodies, security agencies, and alarm reception centres.

Once the necessary and desired grade of security has been established (see paragraph *Conformity with the EN50131-1 standard*), it is necessary to verify that the system you wish to create corresponds to what the standards recommend. There are two figures that ensure this:

- the **manufacturer**, who builds and certifies his products;
- the **installer**, who constructs the system state-of-the-art, following indications provided by the standards.



IMPORTANT! It is very important to understand that the level of security guaranteed by a system is determined by both the products used and how the installation was carried out. In other words, if devices certified for high grade of security are used, but if the installation is lacking or even not in correspondence with the standards, the system will be without certification or with a very low grade of certification. Likewise, carrying out a perfect installation from a technical and standards point of view does not guarantee certification if the system uses uncertified devices.



IMPORTANT! The certification of an alarm system does not correspond to the certification of an electrical system. An alarm system could be perfectly in conformity with electrical system standards, but not respect those of an intrusion alarm system. The certification issued by the installer must explicitly declare that all the devices installed are certified for a grade of security equal or greater to the one indicated for the system and that the installation respects the standards. It is also preferable that the specific standards be cited clearly in the document.

3.3.3 How to protect areas and people

The purpose of an intrusion alarm system is to prevent some prowler from accessing the areas to be protected without him noticing the system. This means monitoring openings and passages, which lead to two different techniques:

- The **“perimeter” protection**, where detectors are installed in all the openings (entry doors, windows, skylights, and glass doors) on the exterior of the areas to be protected. The detectors must cover the entire perimeter: even one single, small, and seemingly insignificant opening that is not monitored represents a protection shortcoming and makes it a potential point of entry for intruders. The advantages of this solution are that the alarm is given as soon as someone attempts to enter and that it is possible to arm the system even if there are people in the rooms; the disadvantage is that if the intruder success in entering without setting off the alarm, it is no longer possible to detect him and he may act without consequences.
- The **“trap” protection** guarantees that the most important rooms and passages (like corridors and stairways, etc.) are surveyed. The advantage of this solution is that the intruder may not wander about undisturbed, in that sooner or later his presence would be detected; the disadvantages are that when his presence is detected, he has already entered and it is not possible to arm the alarm system with people inside the rooms.

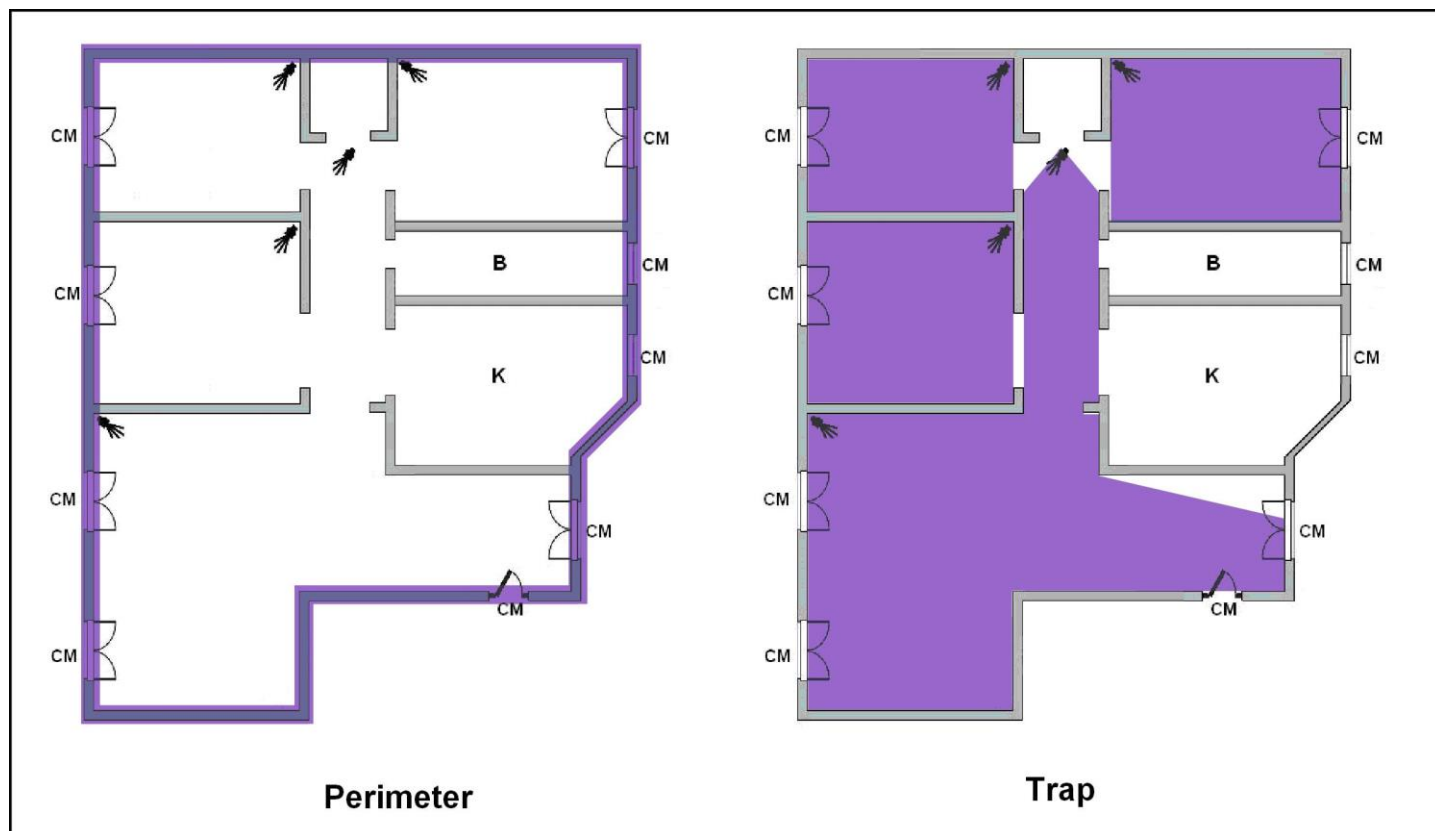


Figure 6 - Perimeter and trap protection

The best and most versatile protection is obtained, obviously, by using both techniques. In paragraph *The subdivision into* this will be explained. Protecting the same room with more than one type of detector, when technically and economically possible, is a good idea because it increases the probability of discovering an intruder.

In particular situations, like a building surrounded by a garden, it is even possible to consider a form of "advanced" protection, in the sense that it constitutes a confine of protection in front of and remotely from the actual areas to be protected, seeking to anticipate potential intrusions as much as possible. A typical example are the detectors installed along the gates or the perimeter walls of a garden or outdoor courtyard, but they might also be seismic detectors installed along a driveway within the property.

3.3.4 The subdivision into partitions

There are cases in which it is not necessary to install the alarm system everywhere or, examining the problem from another point of view, there may be occasions in which it may be preferable to be able to move freely in certain areas while leaving other protected. In other words, being able to partition the existing system, without having to plan two independent ones. The purpose is obviously to increase both security and convenience.

This result can be obtained by configuring the system in **partitions**. The partitions are logical, not physical, groups of detectors, sirens, keypads, readers etc., each of which can be associated with more than one partition if desired. It is better to remember that when the system is enabled, the detectors are not activated, but rather the control panel is commanded to consider the information received by them as attempted intrusion if they reflect specific parameters.

Here is a simple example. The magnetic detector always sends a signal to the control panel every time the door is opened. So why doesn't the alarm go off with the system disabled? This happens because the control panel, during processing, also knows that the system is disabled and so ignores the signal received. The control panel can be even more intelligent. If a "bell" function was activated for a specific detector during the system configuration phase (the name used by the MP500 control panels may differ, for example use the term "gong", but what matters is what the function does), then when the system is disarmed every time that detector is activated, opening the door or walking in front of it will cause the control panel to activate a sound. The signal from the magnetic contact is physically the same, but the way the control panel interprets it changes, producing different results.

Here is how and where partitions can be conveniently used.

A first opportunity was illustrated in *How to protect areas and people*. In that case it was best to make at least two partitions: one for perimeter protection and the other for trap protection. In this way, at night it is possible to move freely about the house while being protected from attempted night-time intrusions. When there is no one at home, both the partitions can be armed to raise the level of security.

Other examples of how the system can be divided into partitions are:

- Home with separate garage. In this case three partitions can be configured: perimeter, trap, and garage.
- Residence and professional office or shop located in the same building and formally separated from each other. In this case, three partitions may be configured: residence perimeter, residence and perimeter trap, and office/shop trap.
- Office and warehouses: In this case even more partitions can be configured for the offices as well as the warehouses in order to provide the utmost flexibility in protection without hampering work activities.

As a general rule, when in doubt, lean toward creating one partition more rather than having one less.

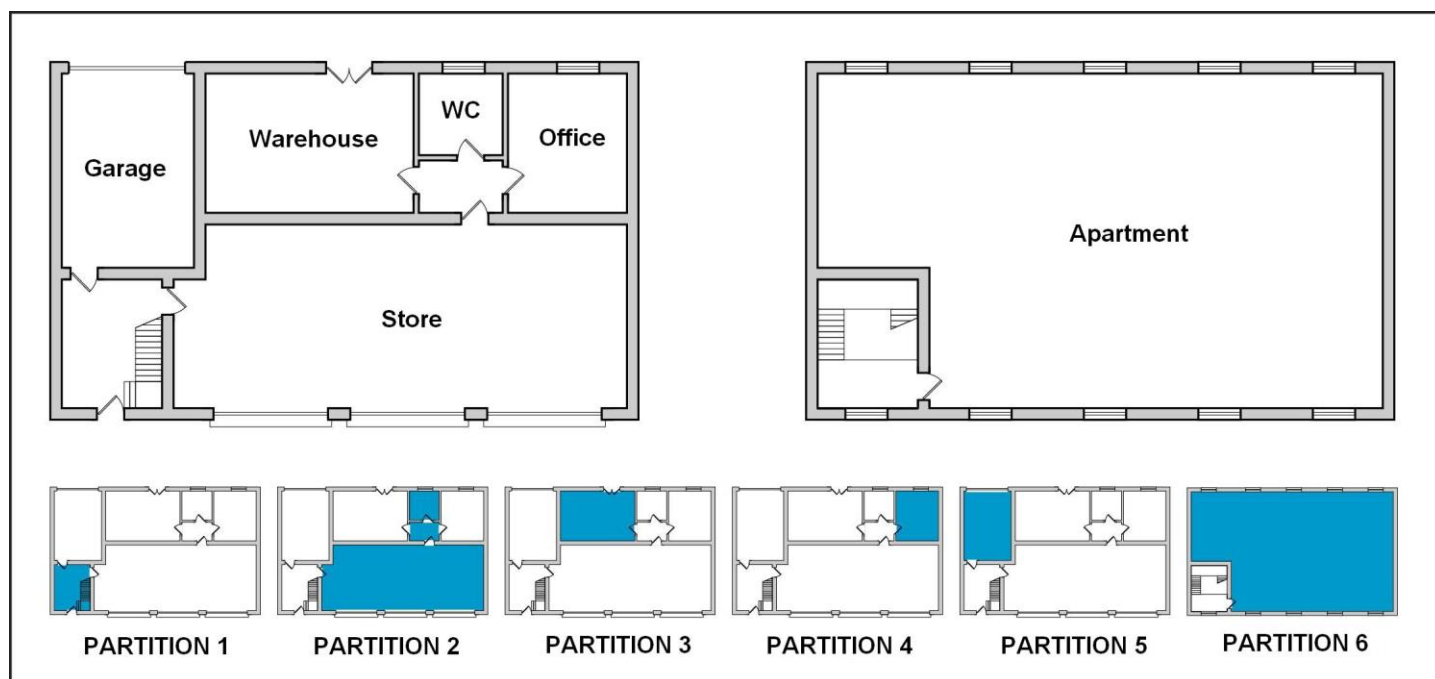


Figure 7 - Subdivision into partitions

In the example above, the apartment is a single partition, while the rooms on the ground floor, which are used for other activities, belong to different partitions. In this way it will be possible to protect the warehouse and offices with the alarm system even when the store is open.



IMPORTANT! Be careful about protecting the same areas by detectors belonging to different partitions, because there may be a risk of false alarms caused by a detector left armed when the user thought all of them had been disarmed. The coexistence of any partition with the perimeter protection partition is at low risk because of the very nature of its use.

3.3.5 Choosing devices

Choosing the devices to be used in the alarm system means having a clear idea of what they do and how they do it. If there should be any doubts, it could be useful to read paragraph *The devices used to create an alarm system*.

3.3.5.1 The detectors

- Magnetic contacts are used for the doors. For security doors and other metal objects, magnetic contacts with stronger magnets are used. Glass doors, without safety glass or bars, may resemble windows when deciding which detectors to use.
- Windows are somewhat complicated to protect. Luckily, there are different types of detectors available, so it is always possible to find a solution for any situation. If the window has a roller, a cable detector for rollers can be used. If there are shutters, a magnetic contact can protect them. A simple window with glass, if not adequately reinforced or protected by a roller or shutter, may require the contemporary use of a detector for breaking glass and a magnetic contact. For shop windows and skylights, breaking glass detectors are used. The windows can then be protected with IR detectors with a barrier or curtain; in both cases the attempt to pass through the "space" of the window is detected rather than the attempt to force the closure of the window.
- For closed environments, volumetric detectors are used. The choice between IR and microwaves can be made according to contingent factors. If the room to be protected is subject to intense and sudden changes of temperature, then using IR may result in a greater number of false alarms. Another aspect to take into consideration when choosing among various model is the roof area and its shape. If the environment is very big, just one volumetric detector may not be sufficient. It is better to understand that using multiple microwave detectors in the same room may create problems of interference among them. These problems do not exist when passive IR detectors are used or when passive IR detectors are used with a microwave detector.
- Once the selection of detectors is complete, it is necessary for their number and type be coherent with the final project to be created. It should suffice to ask a few simple questions: is there at least one sensor that protects each door or window in the perimeter protection? If a trap protection was selected, is there at least one volumetric detector covering each important room? Are all the mandatory passages, like stairways and corridors, covered by an adequate detector?

3.3.5.2 Sirens

- Plan for at least one keypad, regardless of the arming/disarming system of the alarm system adopted.
- If the complex to be protected encompasses multiple separate buildings, or if it is very extensive, or there is no façade that is more visible than the others, then it would be better to take into consideration the installation of more than one siren.

3.3.5.3 Keypads, readers and remote controls

- Plan for at least one keypad, regardless of the arming/disarming system of the alarm system adopted.
- The presence of a keypad allows, for example, entry into the home or office even if the electronic key or remote control has been lost (remember that for security reasons, it is preferable to keep the keys and electronic keys/remote controls separately), or to provide service personnel or employees only the entry keys. Moreover, obviously, this allows the programming of the system and the display of system messages.
- It is opportune to install a keypad or reader near every point of access from outdoors. This makes use of the alarm system much more convenient.
- The same consideration should be made if, in a rather large building, there are indoor areas that are physically separated from others that are identified as an alarm system partition and are always under protection. Even in this case, a keypad or a reader will be installed nearby.

3.3.5.4 External communications

- The type of communication used externally (telephone landline, mobile, SMS, etc.) may influence the certified grade of security. When in doubt, always select the solution or device that guarantees the highest level of certification.
- Due to technical or economic reasons, it is not always possible to choose the best solution. In this case, even the most restrictive solution is preferable to a non-solution.
- When making a decision, always consider not only what the control panel can communicate externally, but also what can be communicated externally to the control panel, or in other words, how it can interact remotely with the alarm system. Succeeding in interacting remotely with the system through the control panel may mean reducing maintenance costs and having a system that is always efficient.
- It is not always necessary to choose. If the budget and the technical characteristics allow it, various types of communication may coexist, each of which may act as a back-up to the others. Redundancy is a plus, because the certainty that alarm notifications are received increases.

3.3.6 Positioning the system devices

Unless they are specifically designed and constructed for outdoor installation, like the outdoor sirens, all the devices must be installed indoors, protected from the elements and vandalism.

3.3.6.1 Positioning the control panel

The control panel must be installed:

- On a dry and level wall. A damp wall may lead to potential infiltrations of water that might wet the inside of the control panel and damage it. A wavy or cracked surface may prevent a solid installation of the control panel.
- In a indoor passage, suitably aerated and protected by the intrusion alarm system. It should be noted that the control panel should not be in plain sight and that, when the system is armed, it should not be accessible to intruders unless they are obliged to pass through areas protected by detectors.
- Far from strong electromagnetic fields.
- At breast height, to facilitate installation and maintenance operations.

If one should ever want to use, immediately or in the future, radio devices or connection via GSM mobile phone network, please read paragraphs 3.3.7 *Tips about installing the radio devices* and 3.3.8 *Tips about the mobile phone network (GSM)*.



IMPORTANT! The installation of the radio expansion results in the loss of EN50131 certification.

3.3.6.2 Positioning the keypads

Keypads must be positioned:

- On a dry and level wall. A damp wall may lead to potential infiltrations of water that might wet the inside of the control panel and damage it. A wavy or cracked surface may prevent a solid installation of the control panel.
- Near the access points of the areas to be protected. In this case they are not intended only as outdoor accesses, but also indoor ones that enable entry to a zone normally protected from intrusion, like a warehouse.
- In an indoor passage protected by the intrusion alarm system. When the system is armed, the keypad must not be accessible to intruders, unless they pass through areas protected by detectors.
- Installed at a height of 160 cm for standard systems, or 120 cm for systems designed for disabled individuals.
- When a vocal keypad is used, position it according to the use one intends to make of it. If one wishes to use environmental listening, position it in the area to be monitored, if compatible with the other needs; if it is to be used for messages in loudspeaker, avoid particularly noisy areas.

3.3.6.3 Positioning readers

Readers must be positioned:

- In a dry place. When installed outdoors and potentially subject to rain and other elements, it is advisable to put it into a waterproof wall niche or to protect the built-in boxes with waterproof covers.
- Near the access points of the areas to be protected. In this case they are not intended only as outdoor accesses, but also indoor ones that enable entry to a zone normally protected from intrusion, like a warehouse.
- Inside the built-in boxes or niches, using the adapter frames for various residential lines, protected by anti-tamper devices.

3.3.6.4 Positioning expansions

When used outside the MP500/xx control panel, the expansions must be positioned:

- In a dry place.
- Inside the distribution cabinet or a similar container, adequately protected by anti-tamper devices. The use of an unsuitable container may invalidate the certification of the grade of security of the system.
- In an indoor passage, suitably aerated and protected by the intrusion alarm system. When the system is armed, the expansion must not be accessible to intruders, unless they pass through areas protected by detectors.
- Far from strong electromagnetic fields.

3.3.6.5 Positioning sirens and flashing lights

External sirens, with or without flashing lights, must be positioned:

- In a place that is not easily reached, like a place that requires use of a ladder.
- The flashing light of the siren or a simple flashing light must be in a position that is easily visible from the main street or other passages. It must also be difficult to reach or obscured.
- Carefully check that the flashing light cannot be obscured after installation. For example, a flashing light assembled during the winter may be easily visible, but during the summer it may be covered by tree foliage or a sunscreen. Remember that the sound alarm arouses attention, but the light signal allows people to identify the place where something is happening.

The internal sirens must be positioned:

- In a position that is difficult to reach.
- Where they can be easily heard in all the internal environments.

3.3.6.6 Positioning the supplementary power supplies

Any supplementary power supplies must be positioned:

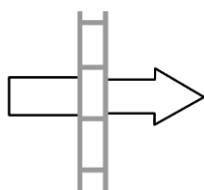
- As near as possible to the devices to be powered to minimise a loss of voltage caused by the length of the wires.
- Inside the distribution cabinet or a similar container, adequately protected by anti-tamper devices. The use of an unsuitable container may invalidate the certification of the grade of security of the system.

3.3.7 Tips about installing the radio devices

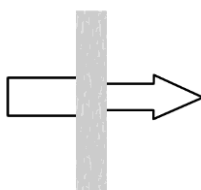
The maximum connection distance between two radio apparatus is determined by the intensity of the signal that reaches the receiver. This intensity, or strength, is determined by the power of the transmitter, by the effectiveness of the antenna, and by the losses due to resistance, one of which is linked to the distance between the apparatus. In fact, it must be remembered that in a free field with no obstacles, the power of the radio signal decreases any way with the squaring of the distance. In other words, by doubling the distance, the power is reduced by one quarter and so on.

Besides power, the antenna, and the distance, the two factors that influence the strength of the signal are absorption phenomena and reflection of the radio waves. Absorption can be considered a loss of signal power when it must travel through some materials. In this case, the higher the refractive index, the greater the absorption. In the table below are the groups of some of the most common materials divided by their refractive index.

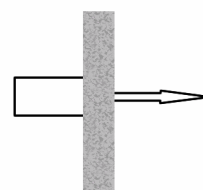
Low refractive index



Middle refractive index



High refractive index



Wood (ex. armoires, furniture), plastic, Water (ex. aquariums), solid brick, marble, synthetic materials (ex. Plexiglas), glass, hollow bricks (ex. interior walls).

Concrete, bullet-proof glass, metallic structures (desks, concrete reinforcement structures, electrical appliances, pipes, gates)

Reflection phenomena influence the signal in two ways. The first is the directivity granted to the signal from the "reflecting" surfaces, like sheet metal or mirrors, located near the radio device and that reflect many of the radio waves that strike it. The second is the phase shift of the radio signals that reach the receiver after having travelled paths that are not "optical". The sum of the signals with phase shifts may be subject to a loss of power of the radio signal received.

In some cases, the signal may even be practically cancelled. For example, a cupboard made completely in metal shields all the radio signals, which can neither enter or exit it.

Another phenomenon can obstruct radio communications: electromagnetic disturbances. In this case the signal from the radio devices, even if sufficiently powerful, may be covered and made incomprehensible, thereby obstructing communications. The phenomenon is similar to that of trying to talk normally in a very noisy room: once in a while, one word might get through, but the sense of the conversation is lost.

Different electrical and electronic devices may create electromagnetic disturbances if they are not adequately shielded: electric motors, electric control panels, computers, fluorescent light bulbs, etc.

Given that even the intensity of the disturbance lessens with the square of the distance, many times it is sufficient to move away from the source of the disturbance to solve the problem.

For a correct installation of the radio devices, take the following precautions:

- Install the control panel in the best possible barycentric position in relation to other radio devices.
- Position the devices far from electromagnetic disturbances.
- Do not install devices on metal surfaces or near large metal objects, or inside metallic structures.

3.3.8 Tips about the mobile phone network (GSM)

The information found in paragraph 3.3.7 *Tips about installing the radio devices* is also valid for the mobile phone network signal.

The main difference consists in the fact that, in place of the internal antenna of the GSM interface, an external antenna positioned in the best signal reception point can be used.

During the site survey, in order to identify the best place to install the control panel or the antenna, the quality of the mobile phone network may be empirically verified by observing the level of the signal as indicated on a cell phone. In order to carry out the test, it is important to use a SIM Card of the telephone service provider to be used, in order to prevent false indications.

3.4 ADVANCED FUNCTIONS

3.4.1 The partitions and the areas

The partition is a virtual space that can be attributed precise characteristics during programming. These characteristics will be acquired from the various devices that were freely associated to it with the programming: inputs, outputs, keypads, readers, etc. The same device can belong contemporarily to more than one partition.

The area is a group of partitions that enable the "subdivision" of the control panels into small, virtual, autonomous control panels, each at the service of a different user.

The rules for using the areas are:

- A system must have at least 2 areas (max 4).
- An area can be associated with up to 15 partitions.
- A partition can belong to only one area, unlike devices (inputs, outputs, keypads, etc.), which can belong to multiple partitions. This means that the same detectors, for example, a siren or a detector, can in any case belong to more than one area, but only belong to distinct partitions, each of which is part of a different area.
- A user code or an electronic key or transponder can be associated with multiple areas, making it possible to create areas managed jointly by different users.
- The use of areas is not mandatory, but if used there can be partitions that do not belong to an area.

3.4.1.1 How to use areas

In order to better understand how areas can be used, here are a couple of examples.

Two- family home

A two-family home is shared by parents and their son with his family. Instead of purchasing two separate alarm systems, they can share one MP500/xx control panel and configure it with two areas. Given that each of them will be able to manage only their own parts of the system (partitions, detectors, keypads, telephone numbers for alarm notifications, dedicated event log, etc.) and visualize only their own information (system status, events, alarms, etc.), it is as if they actually had two separate alarm systems.

The shared shed

A large shed is divided into 4 distinct warehouses to be rented. The owner installs only one MP500/xx control panel and configures the system subdivided into 4 areas, one for each warehouse. For each warehouse there is a keypad and a siren with separate flashing lights, plus all the other necessary devices. The separate sirens make it possible to immediately identify the warehouse being subjected to the attempted intrusion. In this way, the owner created 4 distinct alarm systems (virtual), using just one control panel and just one telephone line.

3.4.2 Input and output: select the delay to avoid setting off the alarm

When the keypad is inside the place protected by the alarm system, the problem arises as how to arm the system and exit, or enter and disarm the system before the alarm goes off. The problem is resolved by programming a delay that inhibits the system and enables people to exit or enter without consequences.

The MP500/xx control panels leaves the factory with the delay times programmed in conformity with EN50131 standard.

Above all, it must be remembered that a detector can be associated with multiple partitions. The descriptions that follow for the "detector activation" is intended as any action that changes the stand-by status of the detector, for example the opening of a door or window, a person walking in front of an IR detector, the forcing of a roller, and so on.



IMPORTANT! Never use, within the same partition, inputs with "Delay" specialisation and inputs with "First entry", "Last exit", "First entry/Last exit", "Way" specialisation.

In the paragraph 3.4.2.5 *Examples of the first entry, last exit, and way specialisations*, which uses the same home and modifies the specialisations of the various detectors, what happens in individual cases can be better understood.

3.4.2.1 Intrusion – First entry

The activation of the detector triggers the longer "Delay times entry way" of the partitions associated with the detector. During this interval, the activations of the "Way" specialised detectors that have at least one partition in common are ignored. Once the "Delay times entry way" has expired, an intrusion alarm is generated.

The "Delay times entry way", and consequently the generation of the alarm, can be interrupted:

- by disarming all the partitions with OR associations to which the detector belongs, or
- by disarming at least one of the partitions with AND associations to which the detector belongs.

When the "Delay times entry way" is already running, all the activations of the "First entry" specialised detectors belonging to the partitions associated with the detector whose activation triggered the delay time are ignored.

The activations of the "First entry" specialised detectors that belong to other partitions are instead managed independently, each with its own "Time entry way".

3.4.2.2 Intrusion – Way

The activation of the detectors triggers the Intrusion alarm, unless it is running the "Time entry way" or the "Time exit way" of:

- all the partitions with AND associations to which the detector belongs, or
- at least one of the partitions with an OR association to which the detector belongs.

If the "Time entry way" is not running, the activation of the detector generates an intrusion alarm immediately.

3.4.2.3 Intrusion – Last exit

When the detector returns to stand-by (magnetic contact closed, no movement for IR detector etc.), it interrupts all the potential "Times exit way" active in the partitions associated with it (resetting them at "zero"). This interruption occurs with about 5 seconds delay compared to the real detector stand-by to prevent the involuntary generation of alarms during the exit phase. The opening of a "Last exit" Intrusion input belonging to an activated partition, after the "Time exit way" is expired generates an Intrusion alarm.

3.4.2.4 Intrusion – First entry – Last exit

Combine the "First entry" and "Last exit" behaviours to enable the use of the same access door for both exit and entry.

The passing of the time can be marked by the sounding of keypad buzzers for both the "Time entry way" and "Time exit way".

3.4.2.5 Examples of the first entry, last exit, and way specialisations

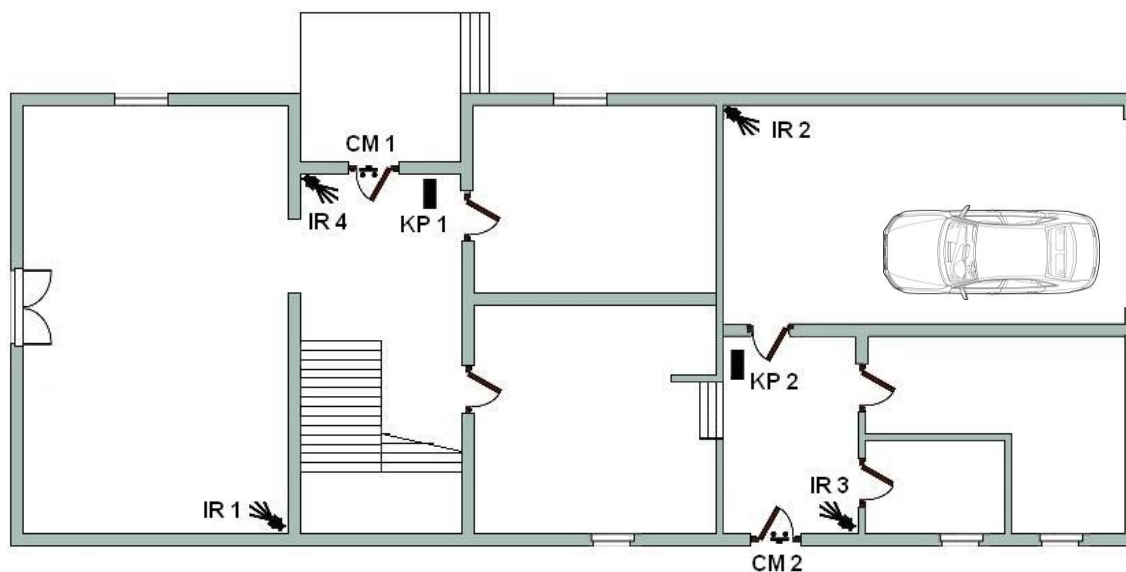


Figure 8 - Examples of the first entry, last exit, and way specialisations

3.4.3 The complementary functions (gong, courtesy light, door opener, absence of move)

Complementary functions that can be used when the system is disarmed can be associated with the inputs. Only one complementary function can be matched with each input.



IMPORTANT! The complementary function chosen is executed only if all the partitions associated with the input are deactivated. If at least one partition is activated, the signal generated by the input is interpreted as an attempted intrusion and the control panel will function accordingly.

The available functions are:

- **Absence of move:** when the alarm system is disarmed, the control panel constantly controls the inputs where this function was enabled. If the inputs, for the period of time established (12 hours, cannot be modified), record no variation in status, an emergency response signal is generated. The timer that counts the time is reset to zero for each opening of the input. The enable the function, after the programming, it is necessary to activate and deactivate the partitions associated with the inputs for which this complementary function is enabled.

This function can be an auxiliary in the control of elderly people who live alone. If the detectors on which the "Absence of move" function was enabled were chosen adequately (for example, the IR detectors in the corridor and bedroom), it is assumed that the person at home does not let more than 12 hours pass without involuntarily activating the detector. If this does not occur, it is believed that the person is unconscious or otherwise unable to move, and therefore in need of help. However, it must be remembered that 12 hours can be too long a time to wait for a person who may be facing serious difficulties.

If there are vocal keypads in the system, it is possible to enable the "Environment listening" function for just one of them during the programming phase. In this case, after the pre-recorded message for emergency response has been sent, the keypad is automatically activated and it is possible to listen to what is happening in the environment where it is located.



IMPORTANT! This function absolutely cannot replace a certified remote control emergency rescue system. If there is a need to monitor the condition of a person continually and safely, it is necessary to back up the intrusion alarm system with a system dedicated to remote emergency response.

- **Gong:** when all the partitions the input is associated with are deactivated, its opening generates a gong event. The typical use is the acoustic signal that warns when someone is entering or passing through a certain zone. For example, in a shop the magnetic contact of the entry door could be configured as a Gong. The gong event emits a buzzer signal from the keypad and activates the outputs configured as Gong.
- **Courtesy light:** the opening of the input generates a courtesy light event, when the system only when is either disarmed. The courtesy light outputs associated with the input partitions are activated for 3 minutes. This function can be used, for example, to automatically turn on the lights in a room or in along an access path.
- **Door opener:** when all the partitions with an input associated with them are disarmed, their opening activates the door opener outputs associated with the same partitions. The opening time of the door opener outputs lasts a few seconds.

3.4.4 The attributes of the intrusion inputs (Release type, AND / OR partitions, AND inputs)

The functioning of the anti-intrusion inputs can be further personalised by setting the attributes:

- **Release type**, determines when the alarm signal is generated. Possible settings:
 - **Single release:** the alarm is generated as soon as the input is opened.
 - **Double release:** the alarm is generated at the end of the second even only if it occurs within 120 seconds after the first.
- **Common input**, determines the belonging to more than one partition. Possible settings:
 - **AND partitions:** logically connect partitions to which the input belongs to each other and the alarm is generated only if all the partitions are armed.
 - **OR partitions:** logically connect partitions to which the input belongs to each other and the alarm is generated is at least one partition is armed.
- **AND inputs**, logically connect two intrusion inputs with the same specialisation together and the alarm is generated only if both are opened within 5 minutes of each other (the first input to be opened can also be reclosed in the meantime). The 5-minute interval cannot be changed. The AND inputs can be used, for example, to reduce the possibility of false alarms of the sensors positioned in critical areas.

Release type with "double release" and AND inputs are used to prevent false alarms. In the first case the detectors is required to confirm its findings within a short period of time, while in the second case a different detector must confirm the finding within 5 minutes of the first.

The *Figure 9 - AND and OR partitions* demonstrates the use of AND and OR with the partitions, where each partition has a room in common with another partition. The  icon visualises when the alarm is set off in case of an intrusion in the armed partitions. Notice how the alarm signals of the room in common (Room B) are strongly influenced by the logical combination between partitions S1 and S2, while the ones not in common behave traditionally.

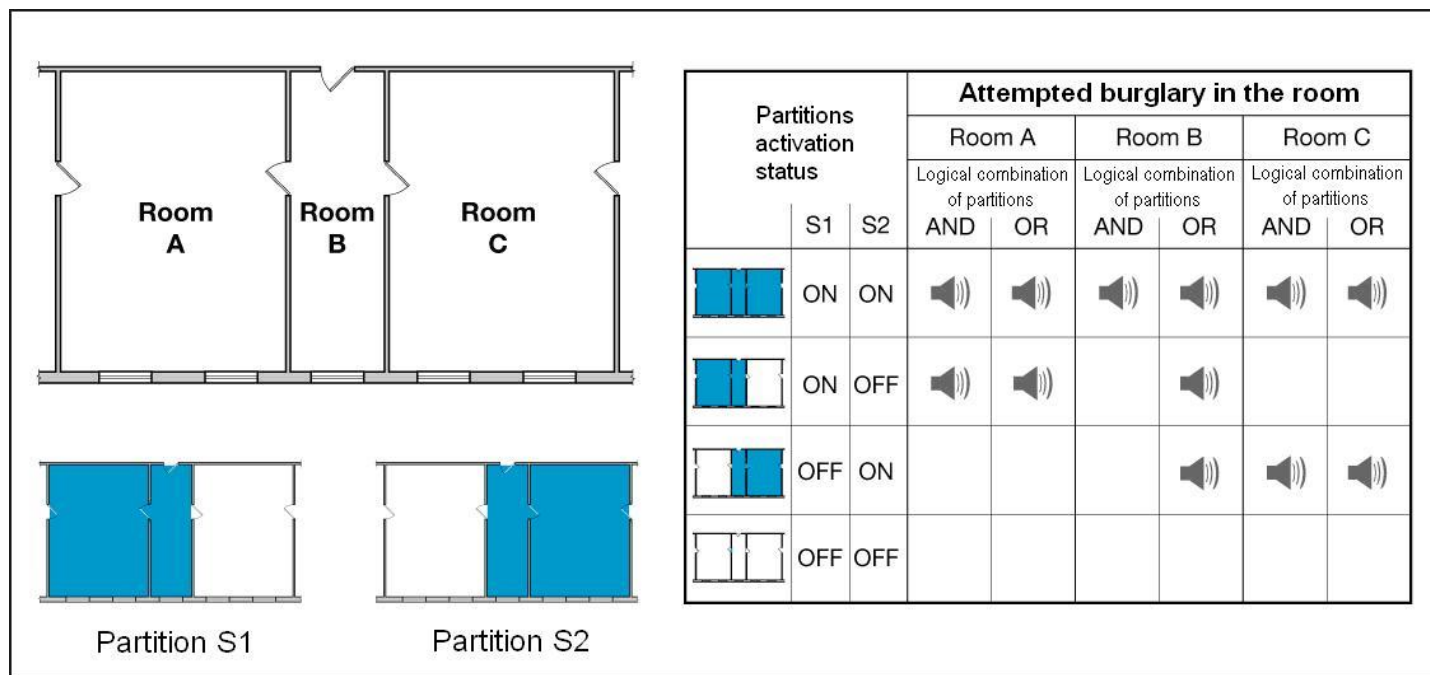


Figure 9 - AND and OR partitions

3.4.5 Remote activation of commandable outputs free of charge

If the control panel is equipped with a GSM module and the GSM responder has been enabled, a valid SIM card can be used to make activations remotely with no additional costs.

This function is based on the Caller ID of the telephones calling to carry out a quick activation of the programmed commandable outputs. During the programming, the commandable outputs are associated with a cell phone number memorized in the control panel (one of the ones used to send the alarms and other functions).

 **IMPORTANT!** The same telephone number may command multiple outputs. Just one output can be commanded by multiple telephone numbers.

The operating principle is the following:

1. The GSM number of the control panel is called using the telephone number memorized.
2. The call is ended before 3 rings to avoid costs.
3. All the associated commandable outputs are activated: the pulsed ones for about one second (typical application of a gate opener), commutable ones or bistable ones change status and remain active until they are deactivated by sending the relative command via SMS.
4. To confirm reception of the command, the control panel calls the number that originally called for a few seconds. This phone call must not be answered in order to avoid having the cost charged to the control panel SIM card.

3.4.6 Environmental listening

When there is a vocal keypad in the alarm system, it is possible to listen, via telephone, to what is going on in the room where it is located. If the system has multiple vocal keypads, then a selection may be made, from time to time, as to which room the user wishes to monitor.

The environmental listening remains active for about a minute and a half before being automatically interrupted. If so desired, the listening can be interrupted sooner by pressing the “*” key.

In addition to listening, it is also possible to speak through the keypad loud speaker. The communication is one-way (one either speaks or listens), but it is possible to switch between “speak” and “listen” as desired by pressing the “0” key of the telephone each time.

4 - DESIGN: CALCULATIONS AND TESTS

4.1 SIZING OF THE POWER SUPPLIES AND THE BATTERIES

All the tests and calculations to be carried out in order to ensure that the power supplies and batteries to be installed are capable of powering all the devices for the period of time specified by standard EN50131 are illustrated below.

4.1.1 Battery sizing

The system must be sized so as to guarantee, in case of a blackout, the minimum time of autonomy required by standard EN50131, depending on the selected grade of security. Therefore, in order to guarantee minimum duration of the battery, the system powered directly by the control panel must comply with the following requirements.

MP500/4N control panel with 7.2 Ah battery					
EN50131	Communicator used	Autonomy	Absorption allowed		
			Control panel	All the devices powered by the control panel	Total
Grade 2	SP2	12 hours	75 mA	375 mA	450 mA

MP500/16 control panel with 18 Ah battery					
EN50131	Communicator used	Autonomy	Absorption allowed		
			Control panel	All the devices powered by the control panel	Total
Grade 3	SP4	60 hours	85 mA	175 mA	260 mA
Grade 3	SP4	30 hours*	85 mA	435 mA	520 mA
Grade 2	SP2	12 hours	85 mA	1065 mA	1150 mA

(*) the time of autonomy can be halved to 30 hours if the system is remotely assisted with a guarantee of intervention in case of blackout.

Table 4 - Control panel battery autonomy

The power supply for all internal circuits and devices is provided by an internal switching power supply.
The use of a 12 V lead-acid rechargeable battery is envisaged.

The battery to be used must:

- Type VRLA (Valve Regulated Lead Acid)
- Casing: UL94V-1 or higher flammability rating
- Comply to IEC 60896-21: 2004, IEC 60896-22: 2004

4.1.2 Calculation of the total absorption of the system

Before proceeding with the installation, it is necessary to know the total absorption of the system in order to be able to proceed with the control for the sizing of the power supplies and batteries.

The calculation procedure is as follows:

- list all the necessary devices, with their quantity and maximum absorption per unit in stand-by (which is all available from the technical specifications), multiplying then the quantity and the absorption to obtain the partial total for each type of device;
- sum all the partial totals to obtain the subtotal;
- add 10% to the subtotal for potential future upgrades;
- calculate the total.

The table below illustrates an example of how to calculate the total absorption:

Device	Quantity		Max absorption:		Total
Control panel	1	X	85 mA	=	85 mA
Keypads	...	X	... mA	=	... mA
Readers	...	X	... mA	=	... mA
Expansion modules	...	X	... mA	=	... mA
Supplementary power supply unit (Expansion)	...	x	55 mA	=	... mA
IR detectors	...	x	... mA	=	... mA
SUBTOTAL					... mA
+ 10% for future upgrades					... mA
TOTAL					... mA

Note: ▪ Magnetic contacts do not absorb electricity.

- The self-powered siren, when it sounds, draws electricity from its own battery.



IMPORTANT! To not overload the control panel battery, when the mains power supply is absent, plan to use the self-powered sirens and optical signals (equipped with their own battery).



IMPORTANT! Make sure the total does not exceed the values shown in Table 4, in order to ensure the required autonomy.

4.1.3 Using supplementary power supply units

If ever the electricity necessary to power the system should be more than what can be supplied by the control panel (see *Table 5*), it is necessary to split the system by using one or more AS500/RPT supplementary power supply units.



IMPORTANT! The AS500/RPT supplementary power supply unit can be used only with the and MP500/16 system.

IMPORTANT! In any case, each AS500/RPT supplementary power supply unit impacts the control panel absorption when it comes to its expansion section (55 mA max). Considering the potential detectors and actuators powered by its outputs +V1 and +V2.

For more information on the supplementary power supply units, see paragraph *5.11 Installation of the AS500/RPT Supplementary Power Supply*.

4.2 CABLE SIZING

The formulas for sizing the connection, audio, and power cables are illustrated below. There are also the criteria to follow when creating busses and in connecting power supplies/repeaters.

4.2.1 Cables to be used, connections of the shields and installation

For the wiring, use a shielded multipolar cable with 4 or more conductors for anti-intrusion. The conductors that connect the inputs and the data Bus signals **+D** and **D** must have a minimum gauge of 0.22 mm².

The shieldings can be connected together at the negative pole of the control panel power supply.

If AS500/RPT supplementary power supplies are used, the secondary bus shields can be connected together at the negative pole of the power unit of the AS500/RPT supplementary power supply unit.



IMPORTANT! Never connect the cable shields to the earth.

For the audio bus, use a normal telephone wire (twisted pair).



IMPORTANT! When installing the cables, keep the anti-intrusion system cables separate from the electrical system of the apartment or office (separate ducts).

4.2.2 Sizing of the power supply cable

The section of the cables must be selected so that the voltage of the power supply to various devices is correct, for the purpose of obtaining stability, efficiency, and immunity from disturbances.

The section must be calculated after having taken into account the most critical situation of the system power supply, which is equal to a blackout and the back-up battery with only a minimal charge (10.5 V_{nom}). Under these conditions, when fully charged, all the devices in the MP500/4N and MP500/16 systems must be guaranteed at least 9 V_{nom}.



IMPORTANT! Check that there is in any case the minimum voltage of the functioning of the other devices used, like the IR detectors, actuators, and sirens, etc.. Some of these devices may require a power supply voltage of over 9 V_{nom} (the power supply data and the tolerances allowed are reported in the technical specifications of the various devices).

As a result,

The maximum voltage reduction admitted on cables is: 1.5 V_{nom}

or 0.75 V on the positive cable and 0.75 V on the negative cable.

The formula to calculate this is

$$V_{\text{CONTROL PANEL}} = 2 \times \text{length} \times R_{\text{CABLE}} \times I_{\text{DEVICES}}$$

where:

V_{CONTROL PANEL} is the reduction in power in Volts
length is the length of the cable (single conductor), in metres
R_{CABLE} is the resistance of the cable in ohm/m
I_{DEVICES} is the maximum current absorbed by the devices in Amperes (a value that can be found on their technical specifications)

The values of copper cable resistance are:

Cross section sq.mm ² (*)	0.22	0.50	0.75	1.00	1.50
Resistance in Ohm/m	0.0795	0.0350	0.0233	0.0175	0.0117

(*) Standards require that the cross-section of the cable cannot be less than 0.1 mm².

Table 5 - Copper wire resistance

In the case of a complex power supply network, with multiple branches, it is necessary to calculate each individual stretch.

For different wire sizes the maximum acceptable lengths according to the maximum current running in the conductor are shown by way of example only.

Section 0.22 mm ²		Section 0.50 mm ²		Section 0.75 mm ²		Section 1 mm ²		Section 1.5 mm ²	
Current	Length	Current	Length	Current	Length	Current	Length	Current	Length
0.300 A	31 m	0.300 A	71 m	0.300 A	107 m	0.300 A	143 m	0.300 A	214 m
0.500 A	19 m	0.500 A	43 m	0.500 A	64 m	0.500 A	86 m	0.500 A	129 m
0.750 A	13 m	0.750 A	29 m	0.750 A	43 m	0.750 A	57 m	0.750 A	86 m
1.000 A	9 m	1.000 A	21 m	1.000 A	32 m	1.000 A	43 m	1.000 A	64 m
1.500 A	6 m	1.500 A	14 m	1.500 A	21 m	1.500 A	29 m	1.500 A	43 m
2.000 A	5 m	2.000 A	11 m	2.000 A	16 m	2.000 A	21 m	2.000 A	32 m
2.500 A	4 m	2.500 A	9 m	2.500 A	13 m	2.500 A	17 m	2.500 A	26 m
3.000 A	3 m	3.000 A	7 m	3.000 A	11 m	3.000 A	14 m	3.000 A	21 m

4.2.3 Sizing the power supply and data transmission bus

The bus connects the various devices and guarantees their power supply and data transmission. The total length of the bus must be as short as possible and, in any case **the extension, that is the sum of all the stretches of bus must not exceed 400 metres**.

In order to reach this result, and facilitate the wiring work, in the creation of the system any of the topologies illustrated here below can be used freely.

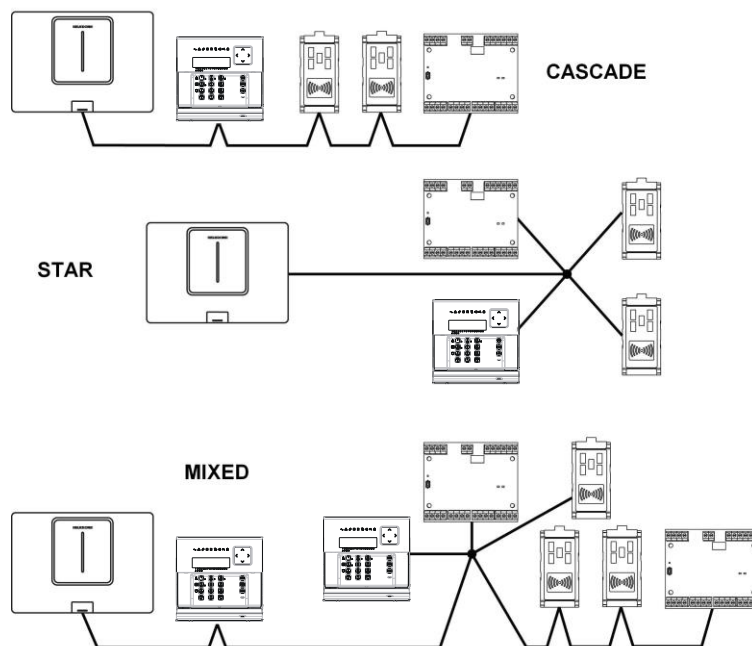


Figure 10 - Topologies of the bus connection

! IMPORTANT! Do not create closed rings with the bus to prevent malfunctions.

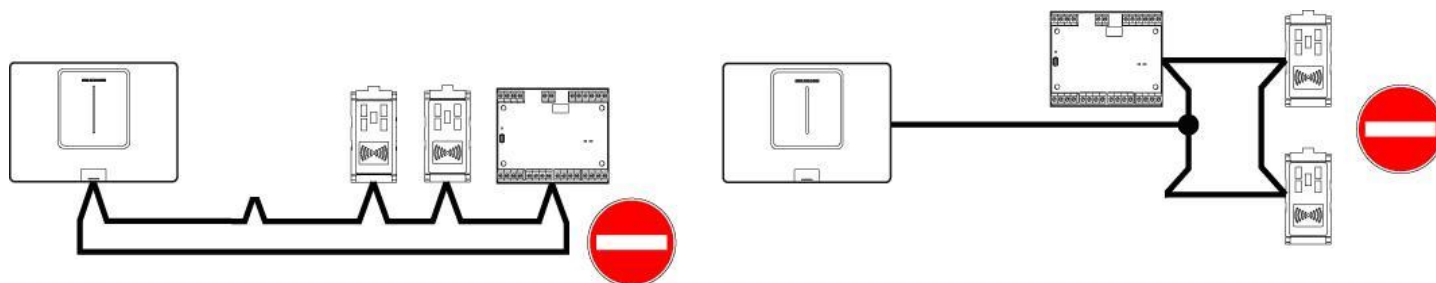


Figure 11 - Rings on the bus

It is not necessary to tend the bus line and each individual stretch (as typically occurs instead with the RS485 type).

In the bus, the sizing calculation for the cables is carried out only to determine the size of the power supply cables “+” and “-”.

4.2.4 Extending the bus with the repeater

The 400-metre length limit of the bus can be overcome with the use of the AS500/RPT supplementary power supply unit.

Indeed AS500/RPT power supplies, in fact, in addition to serving as supplementary power supplies, they make the repeater function available.

! IMPORTANT! The supplementary power supply with repeater AS500/RPT can only be used with the and MP500/16 system.

When using the repeater with the MP500/16 control panel always follow 3 simple rules.

- The maximum number of repeaters allowed is 15.
- The length of the stretches of each secondary bus cannot exceed 400 metres.
- It is not possible to connect two or more repeaters.

Below are some examples of how to use the repeater.

In the example, it is possible to see the primary bus with the bus that exits directly from the control panel, with the secondary bus deriving from the repeaters.

4.2.4.1 System with 1 supplementary power supply repeater

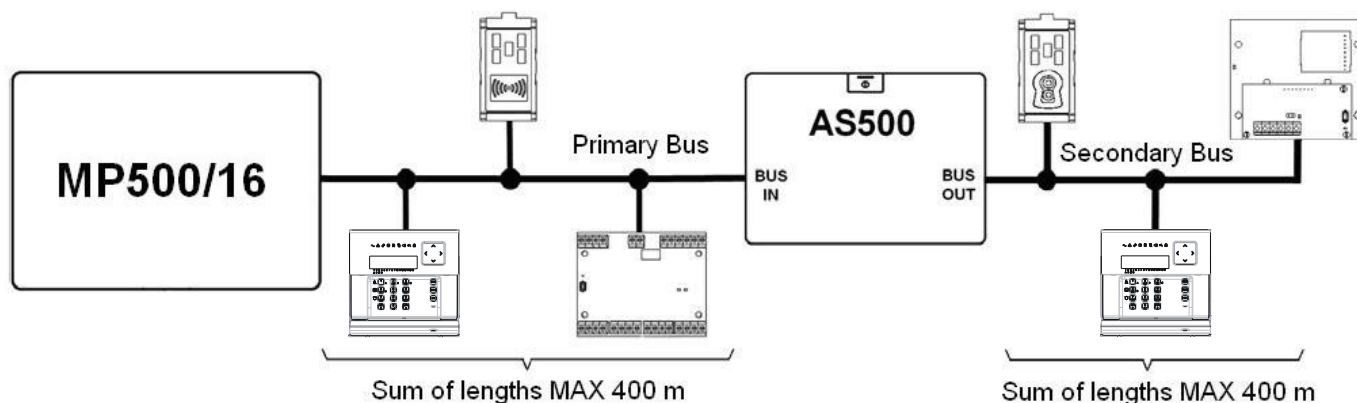


Figure 12 - Diagram with 1 supplementary power supply repeater

Sum of stretches of each BUS (primary BUS = secondary BUS) = **400 m**
 Distance BUS point/point = (primary BUS + secondary BUS) = **800 m**
 Sum of the stretches of all the BUSSES = **800 m**

4.2.4.2 System with 2 supplementary power supply repeaters

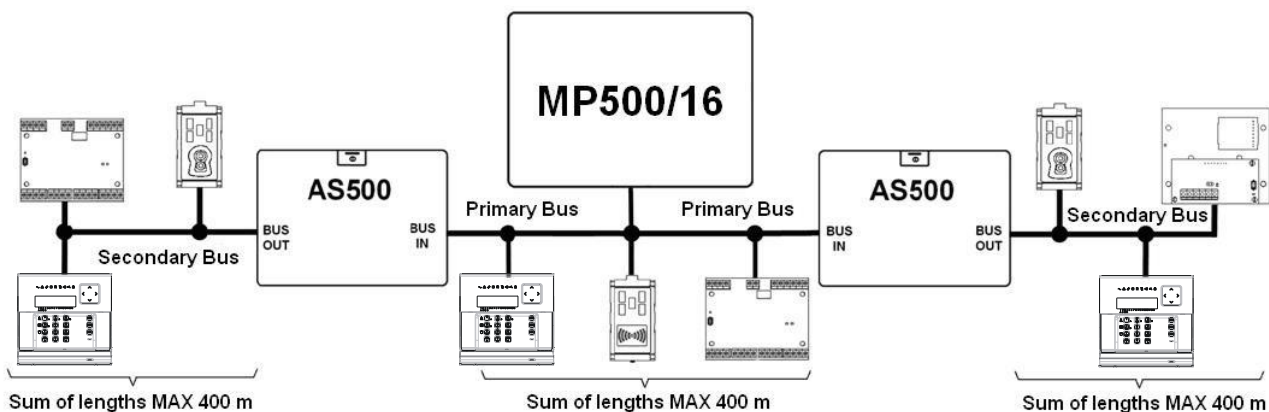


Figure 13 - Diagram with 2 supplementary power supply repeater

Sum of stretches of each BUS (primary BUS = secondary BUS) = **400 m**
 Distance BUS point/point = (primary BUS + secondary BUS) = **1200 m**
 Sum of the stretches of all the BUSSES = **1200 m**

4.2.4.3 System with multiple supplementary power supply units

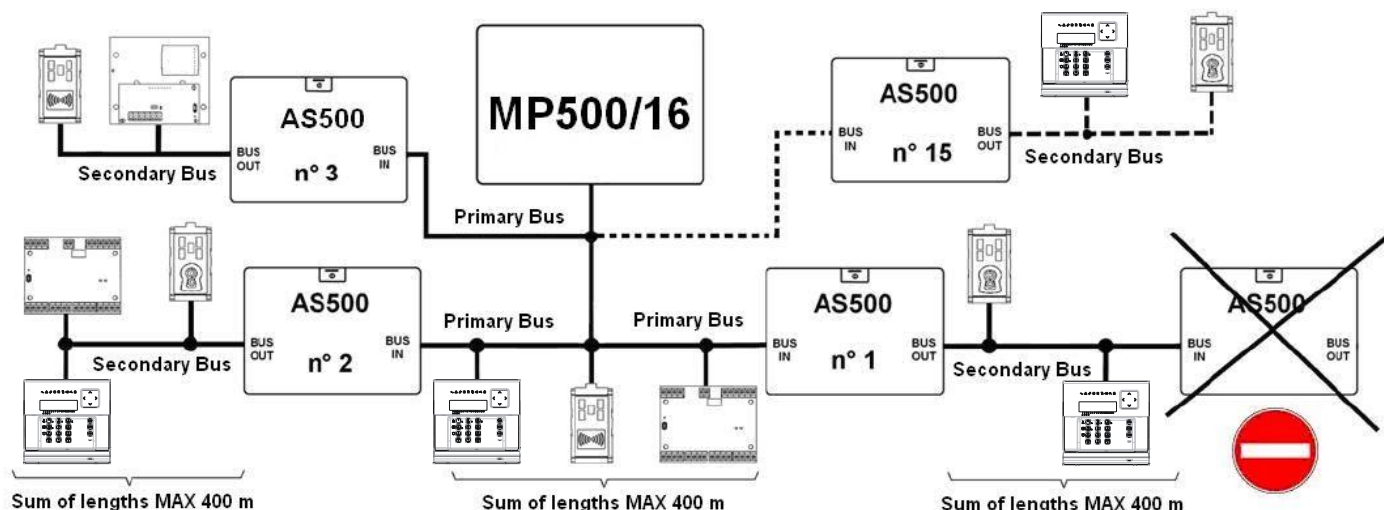


Figure 14 - Diagram with 15 supplementary power supply repeater

Sum of stretches of each BUS (primary BUS = secondary BUS) = **400 m**
 Distance BUS point/point = (primary BUS + secondary BUS) = **1200 m**
 Sum of the stretches of all the BUSSES = **6400 m**

4.2.5 Sizing of audio Bus

Whenever vocal keypads are used, it is necessary to connect them to the SV500N vocal synthesis board, which must be added in the MP500/4N and MP500/16 control panels. To connect the audio bus, only a cascade connection can be used, beginning at the control panel.

The total length of the audio bus must not exceed 300 metres.



IMPORTANT! The use of the vocal card invalidates the EN50131 compliance.

4.2.6 Sizing of Input/Output connections

The length of the cable connection between the detector or the actuator and the input to which it is connected must not exceed 500 metres.

If the device should be connected to an input configured for fast pulses (rollers, shock etc.), the length of the connection must not exceed 100 metres.

4.3 CONTROL CRITERIA OF THE MAINS POWER SUPPLY VOLTAGE

The MP500/4N and MP500/16 systems constantly control the presence of the mains power supply in the control panel, which is detected by means of the presence of voltage in the power supply unit.

The absence and return of the mains power supply generate the following behaviours.

4.3.1 Blackout event

When the absence of the mains power supply is detected:

- The alarm system is powered by the battery.
- The green power supply LEDs of the keypads flash to signal the problem.
- The event is recorded in the Diagnose Log.
- The system does not generate an alarm immediately, but starts the "T Lack of power" count (1 hour). This parameter can be modified during programming. Every time electrical power is restored, the "T Lack of power" count is reset to zero.

The delay determined by the "T Lack of power" serves to prevent the sending of alarms due to brief interruptions in the mains power supply.

This is particularly useful in those places where temporary blackouts are frequent. In this way the sending of a telephone message to signal a brief blackout and a successive call at the time power is restored are avoided.

4.3.2 Continued blackout alarm

If the blackout persists until the Time of the Lack of power set expires, the following occurs:

- The system generates a "Continued blackout alarm".
- The specialised lack of power outputs are activated ("LACK OF POWER")
- A dedicated alarm message is sent via the telephone transmitter.
- The alarm is memorized in the Diagnose Log.



IMPORTANT! If the battery level descends below the threshold of 12.5 V, the "Continued blackout alarm" is generated immediately, even if the time Lack of power has not yet passed.

4.3.3 Restoration of the mains power supply

Once the mains power supply restores power, the green power supply LEDs of the keypads stop flashing and remain on and the system restarts a time count. Once 5 minutes have passed, if the power has been continuously present, the following occurs:

- Via the telephone transmitter, the message dedicated to the restoration of mains power supply is sent.
- The event of the restoration of the mains power supply is memorized in the Diagnose Log.

Potential brief interruption in the mains power supply during the time count will result in the resetting of this time.

4.4 BATTERY MANAGEMENT CRITERIA

The system is capable of detecting all the possible conditions under which the back-up battery may be needed and to provide for its management adequately in automatic mode. The detection is based on the voltage read at the battery terminals **+BT** and **-BT**.

The control carried out on the status of the battery is done in two ways, depending on the presence or absence of the mains power supply.

4.4.1 Control and charging of the battery with the mains power supply present

The MP500 systems, when the mains power supply is present, provide constant control of the battery. If the battery is not detected, or if it is completely dead, the system assumes the status of "No battery". In this status the battery charging circuit is turned off: this means that if the battery is not connected to the terminals of the connection cables, (red and black faston) there is no power. As soon as battery is connected, the charging circuit is once again activated and keeps the battery charged with a limited maximum current.

Note: If due to some anomaly the battery should reach a charge of 14 V, the charging circuit is automatically deactivated to prevent damage to the battery.

4.4.2 Controlling the battery with mains power supply absent

Even if the mains power supply is absent, the battery is controlled continually.

When the voltage at the battery terminals falls below 11.5 V, the "Battery low" event is generated.

When the voltage at the battery terminals drops further and reaches 10.5 V, the control panel disconnects the battery to prevent potential damage due to a deep discharge (a function present only in the MP500/16 system). The restoration to the "Battery low" condition occurs only after a return of the mains power supply and after a Test battery gives positive results.

4.4.3 Test battery

To test the efficiency of the battery, the "Test battery" is carried out periodically. This test is carried out:

- 30 seconds after the return of the control panel power supply or of the mains power supply.
- Every 24 hours (automatically).
- After a "Test battery" command from the Installer or Master menu (manual test).

The Test battery lasts 30 seconds during which the battery is charged. If the battery is deemed inefficient, the test is interrupted and the "Battery low" event is generated, resulting in the immediate "Battery low alarm".

The "Battery low" status lasts until the next "Test battery" that concludes with a positive result.

If the mains power supply is absent, the Test battery is not carried out.

4.5 SELF-DIAGNOSTIC FUNCTIONS

The system autonomously and continuously carries out controls to ensure that the system functions correctly and is perfectly efficient. In addition to testing the presence of the mains power supply and the battery as illustrated above, the tests below are also carried out:

- Control of the system power supply voltage.
- Control of the battery charging circuit efficiency.
- Control of the correct communication among the devices.
- Control of the correct functioning of the secondary bus with the automatic cut-off in case of sabotage or malfunction.
- Control of the correct functioning of the control panel CPU.
- Control of the PSTN telephone line.
- Control of the SIM-Card and connection with the GSM telephone network.

When the system detects a critical condition, a specific signal is given. The beginning of the anomalous event and its end are recorded in the Diagnose Log. Some anomalies can also activate dedicated outputs. If there is an anomaly in the power supply with the increase in output voltage higher than 15 V (for example, as a consequence of a lightning strike to the mains power supply), the MP500/16 control panel automatically disconnect all the power supply outputs to protect the devices connected from damage due to a power surge.

5 - INSTALLATION

This chapter will explain all the procedures to follow to install the entire system, from the wiring to the assembly of the devices, from the installation of various options and interfaces in the control panel to bus connections and those of detectors and output devices.

An explanation of how to open the control panel will be given, how to recognise the various parts of the control panel, of its expansion modules and interfaces, and of the system devices.

The next chapter explains how to buy the various devices and start up the system.

5.1 INSTALLATION PROCEDURE

The best operation sequence for installing an alarm system with MP500 control panels, in the least time possible while guaranteeing optimal results, calls for the following steps to be taken:

1. Wiring.
2. Installing the control panel on the wall.
3. Assembly of expansion modules, optional, and accessories in the control panel.
4. Connections in the control panel.
5. Installation and connection of expansion modules, keypads, and readers.
6. Installation and connection of the detectors and alarm and signalling devices.
7. Power supply and acquisition of the devices.
8. Configuration of the system and its testing (procedure illustrated in the *Programming Manual*).

Nothing prohibits following a different procedure. For example, step 3 can be anticipated, assembling the expansion modules and interfaces in the control panel in the workshop.

Even steps 7 and 8 can be completed beforehand, in the workshop, using temporary wiring, provided that the various devices are duly identified with labels so as to be able to subsequently install them correctly on site.

Alternatively, the entire system can be programmed on a PC equipped with Hi-Connect software, saved, and later downloaded on site from the PC or from a USB pen drive.

5.2 WIRING

Run all the connection cables necessary: bus, detectors, alarm and signalling devices, electric power supply, telephone connection, eventual audio bus. Before running the cables, check their sizes.



IMPORTANT! When installing the cables, keep the anti-intrusion system cables separate from the electrical system of the apartment or office (separate ducts).



IMPORTANT! In fulfilment of the electrical security standards, the wiring must be done carefully and all the connection cables must be blocked in position near the terminal board to prevent the Safety Extra Low Voltage conductors (SELV) from making contact with dangerous live wires (mains terminals).

Block the cables by fixing them with bands to the anchoring points “F” (see figures Figure 16 – Figure 26 - Figure 52).

5.3 PREPARING THE MP500/4N CONTROL PANEL

! **IMPORTANT!** During installation of the control panel, be very careful to not accidentally damage the mother board.

5.3.1 Opening the cover

To access the screws that close the MP500/4N control panel, open the screw covers by sliding them downward as illustrated in the figure.

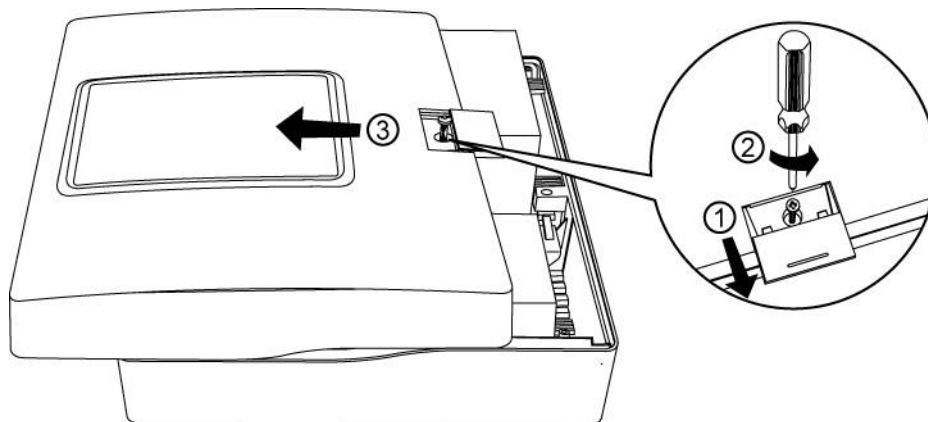


Figure 15 - Opening the MP500/4N control panel

5.3.2 Openings for cables

The figure below illustrates all the set-up for running the cables (power supply, bus, signalling detectors and devices, potential telephone line) of the MP500/4N control panel.

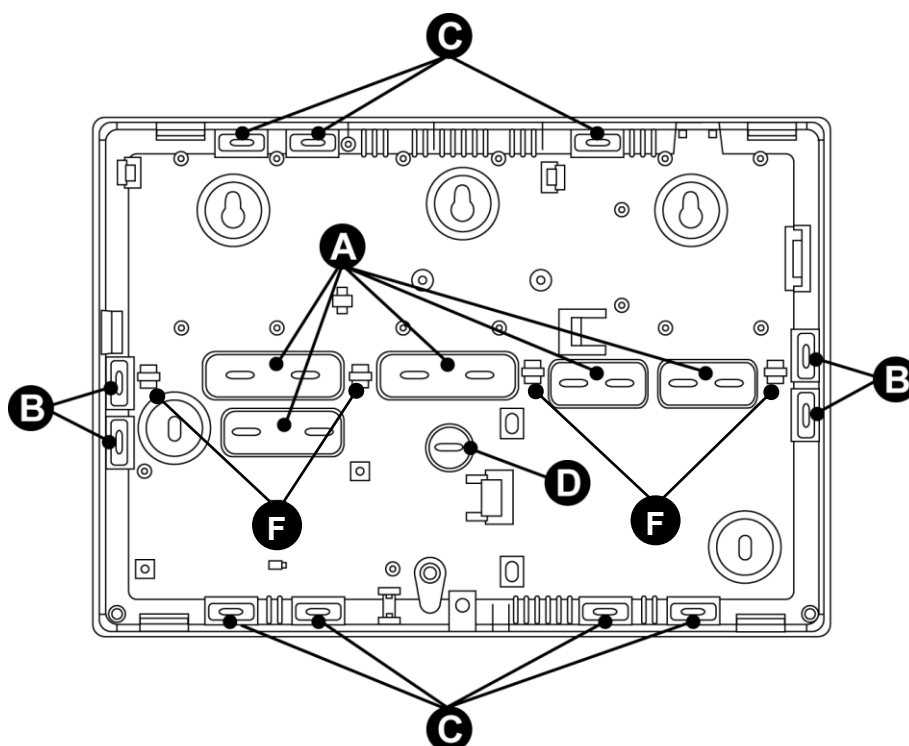


Figure 16 - Setup for running the cables

The set-up for running the cables are:

- A** - for embedded corrugated tube;
- B** - for rectangular wall duct;
- C** - for rectangular wall duct or rigid tube;
- D** - for corrugated tube dedicated to the power supply.
- F** - points for anchoring cables with bands.

5.3.3 Fastening to the wall

The figure illustrates the holes available for fastening the control panel to the wall with self-locking dowels with a maximum size of 6 mm (not included). For a firm fastening, it is necessary to use at least 4 holes. Holes **A** and **B** can be accessed by releasing the mother board from the clips and turning it (*Figure 18 - Releasing the mother board*).

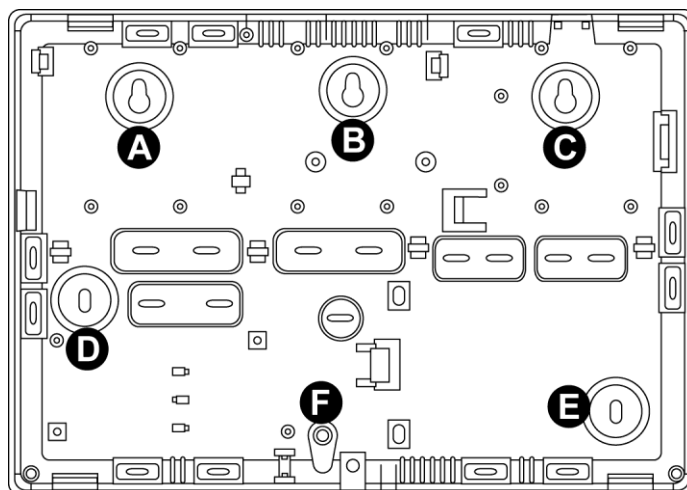


Figure 17 - Holes for fastening the MP500/4N

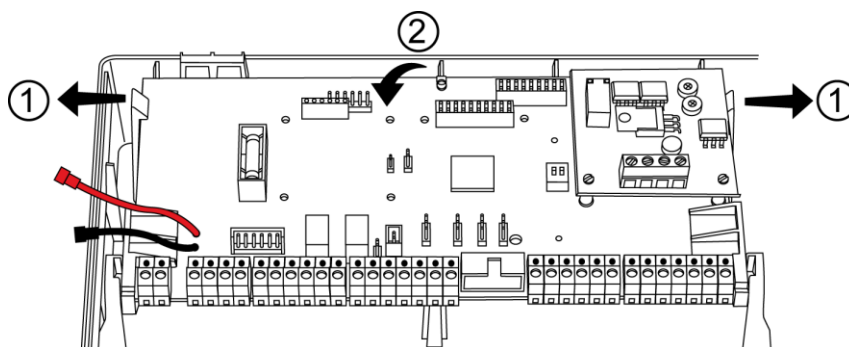


Figure 18 - Releasing the mother board

To guarantee the MP500/4N control panel protection from tampering and removal, it is necessary to use hole **F** for fastening as well. Protection against removal is mandatory for guaranteeing EN50131 grade 3 compliance.

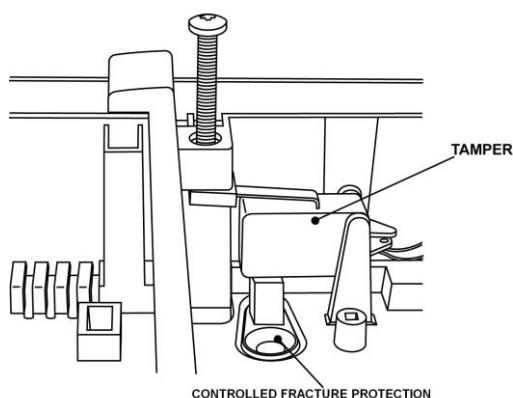


Figure 19 - Protection of the MP500/4N from tampering and removal

5.3.4 Battery compartment and fastening points for the optional features in the MP500/4N control panel

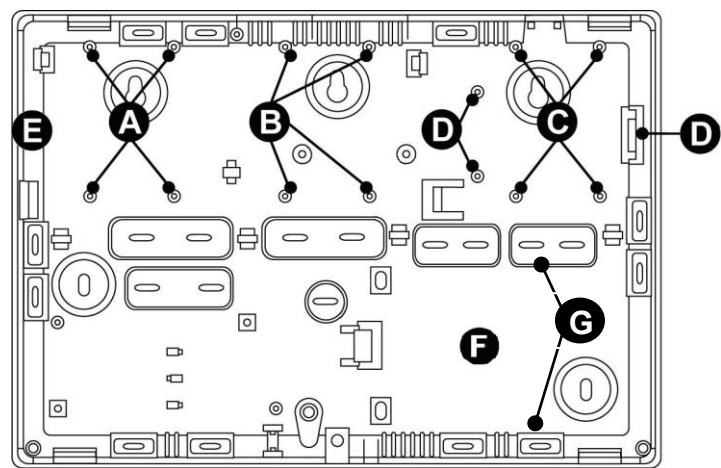


Figure 20 - Fastening points for optional features in the MP500/4N control panel

MP500/4N	Expansion
A	Fastening points for EP508 expansion
C	Fastening points for EP508 expansion
D	Fastening points for EP508 expansion
E	Compartment for internal GSM antenna
F	Battery compartment
G	Pre-scored holes for fastening the battery with the band

 **IMPORTANT!** In order to guarantee conformity with Standard EN50131-3, the battery must be fastened using the band supplied as illustrated in the figure below.

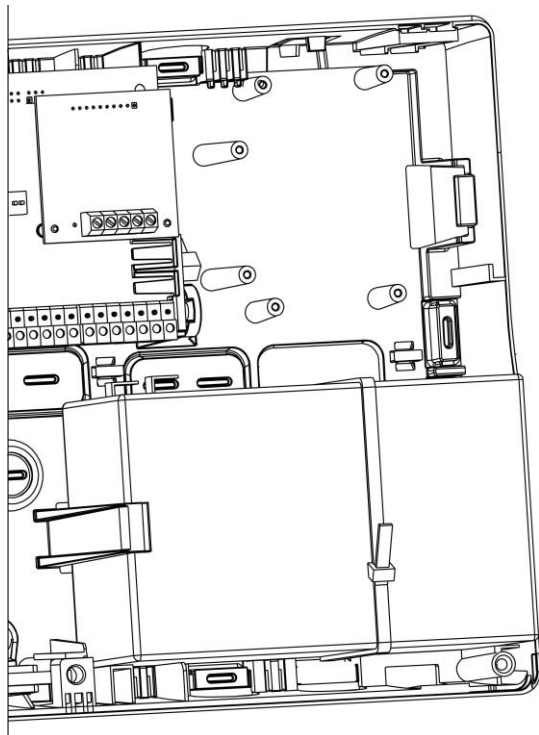


Figure 21 - Fastening points for optional features in the MP500/4N control panel

5.3.5 Assembling expansion modules in the MP500/4N control panel



IMPORTANT! The connection and disconnection of the optionals and accessories must always be done while the control panel is disconnected from all power supplies (both mains and battery).

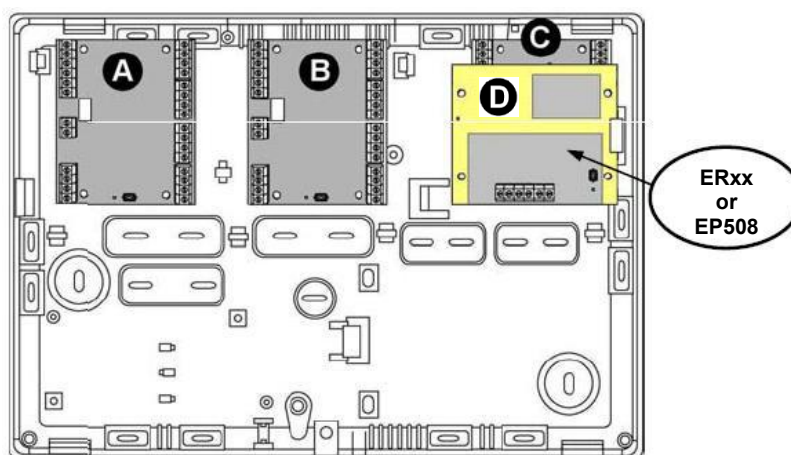


Figure 22 - Fastening points for optional features in the MP500/4N control panel

Inside the MP500/4N control panel, 3 EP508 expansions (positions **A**, **C** and **D**) or 2 EP508 expansions and 1 radio expansion can be assembled.

The position **D** calls for the assembly of the board in the raised position and turned 90°, inserting the board into slot on the right and fastening it with 2 self-tapping screws onto the two supports on the left; the programming (PROG) key must be between the left-hand support if an EP508 is installed, or on the bottom right of a radio expansion is installed.

The expansions must be fastened with the self-tapping screws supplied.

The positions **A** and **B** can be accessed by releasing and turning the mother board (*Figure 18 - Releasing the mother board*). If the GSM module is used, it is not possible to use position **B**.

Position **A** is dedicated to the IT500WEB interface, but in its place an EP508 board can be installed.

5.4 PREPARING THE MP500/16 CONTROL PANEL

 **IMPORTANT!** During installation of the control panel, be very careful to not accidentally damage the mother board.

5.4.1 Opening the cover

There are two ways to open the MP500/16 control panel: by removing the cover or by flipping it open.

1) Removing the cover.

- Unscrew the screws on the cover (1), slide it upwards (2) and lift it (3)

2) Opening the hinged cover

- Unscrew the screws on the cover (1) and flip it downward (2)

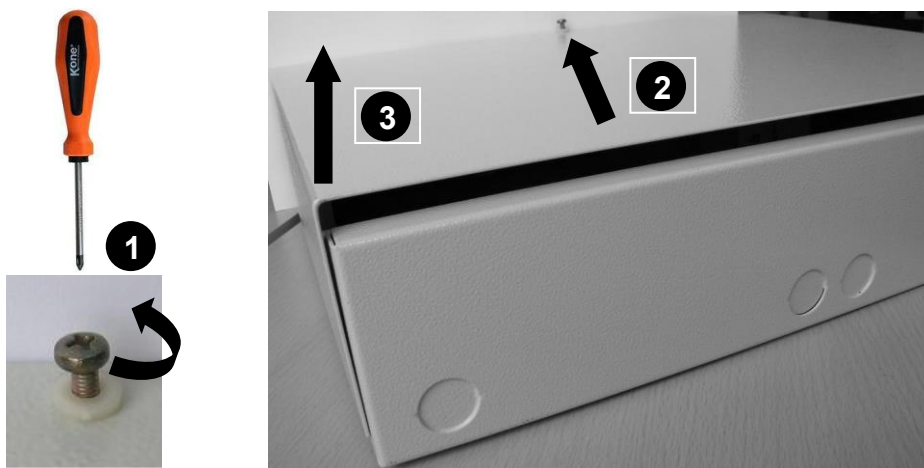


Figure 23 - Opening the control panel by totally removing the cover MP500/16

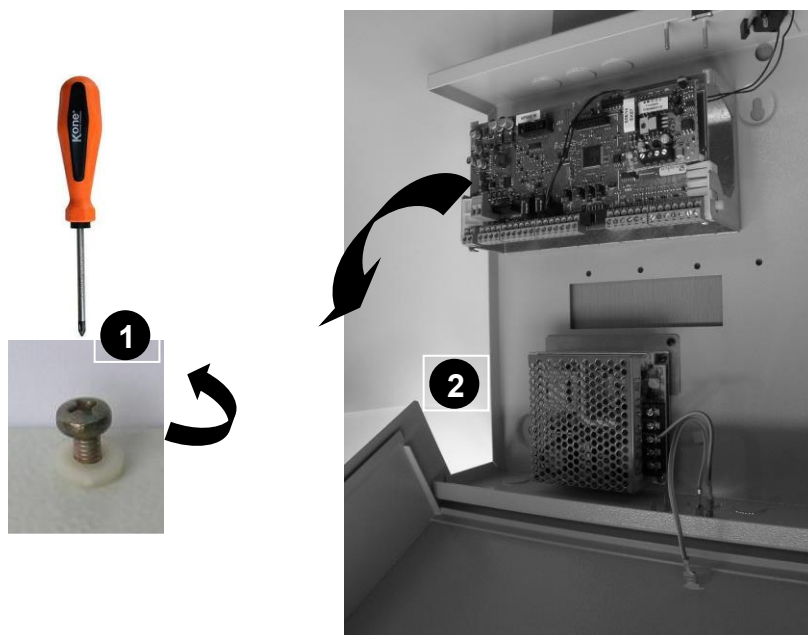


Figure 24 - Opening the control panel without totally removing the cover MP500/16

5.4.2 Openings for cables

The figure below illustrates the hole for the optional GSM antenna (A) and all the set-up (B) for running the power supply, bus, signalling detector and device, potential telephone line cables of the MP500/16 control panel.

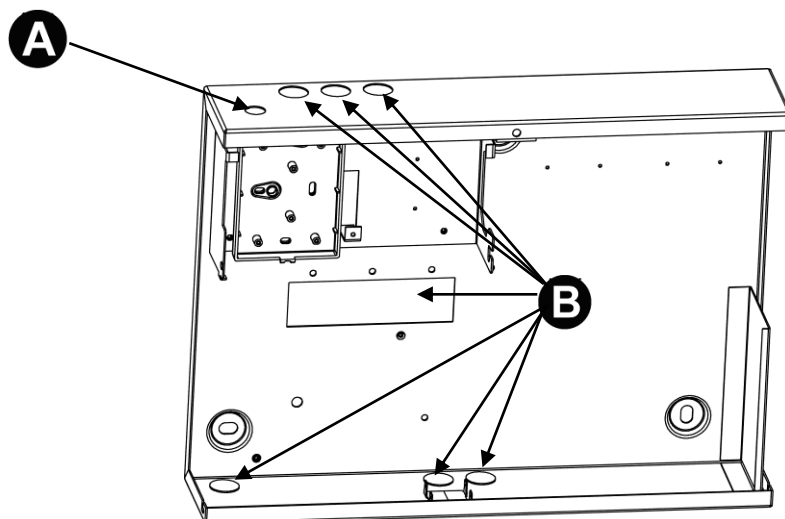


Figure 25 - Set-up for running cables and fastening the GSM antenna MP500/16

5.4.3 Fastening to the wall

The figure illustrates the holes available for fastening the control panel to the wall. Use the 8 mm expansion screws suitable to the type of wall (for this step, consult qualified personnel).

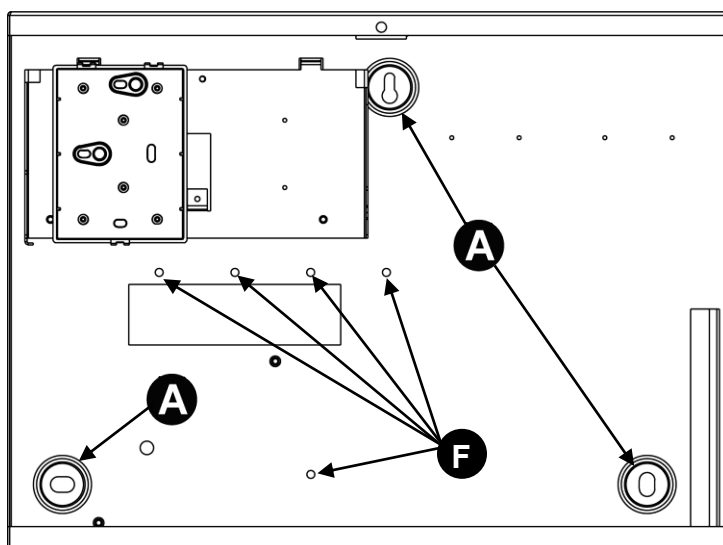


Figure 26 - Holes for fastening the MP500/16

The set-up for running the cables are:

- A - for embedded corrugated tube;
- F – points for anchoring cables with bands.

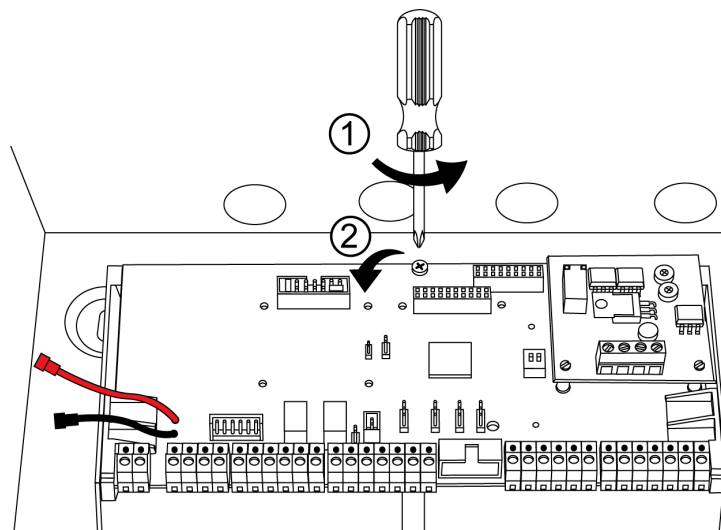


Figure 27 - Releasing the MP500/16 mother board

To guarantee protection against opening, tampering and removal of the MP500/16 control panel, it is necessary to install the tamper (microswitch).

Positioning the tamper in position **A** or **S**, according to the type of application desired:

- In position **A** only protection against opening is guaranteed, but not against removal (the system is not in conformity with the EN50131 grade 3 standard).
- In position **S**, for protection against opening and removal, use the screw and the expansion screw supplied as illustrated in the figure. The protection against removal is mandatory to guarantee EN50131 grade 3 compliance (already attained in the factory).

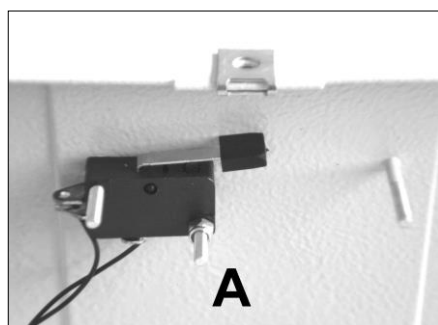


Figure 28 - Assembly of tamper for the MP500/16 control panel

In both cases, it is necessary to connect the tamper connection to the mother board.

(See

Figure 33 - Connections and main parts of the MP500/16 control panel – position **P**)

5.4.4 Battery compartment and fastening points for the optional features in the MP500/16 control panel

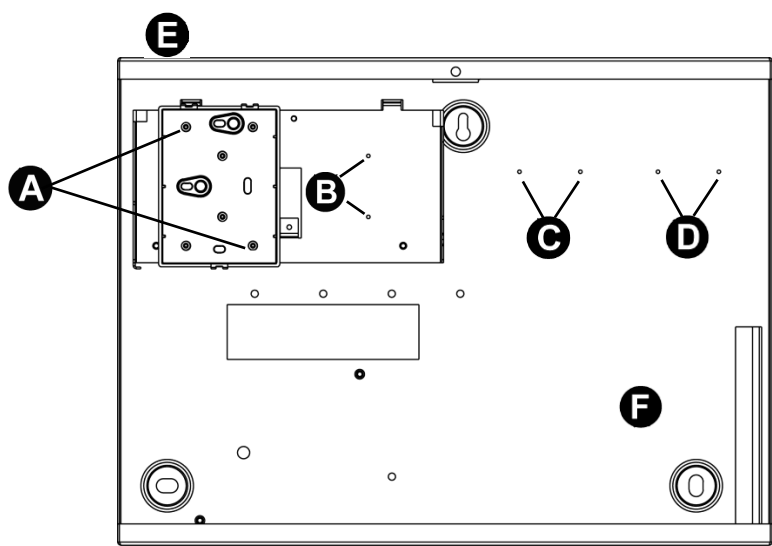


Figure 29 - Fastening points for optional features in the MP500/16 control panel

	Expansion
A	Fastening points for EP508 or Web server expansion
B	Fastening points for EP508 expansion
C	Fastening points for EP508 expansion
D	Fastening points for EP508 expansion
E	Compartment for GSM 2 antenna
F	Compartment for back-up battery

5.4.5 Assembling expansion modules in the MP500/16 control panel

 **IMPORTANT!** The connection and disconnection of the optionals and accessories must always be done while the control panel is disconnected from all power supplies (both mains and battery).

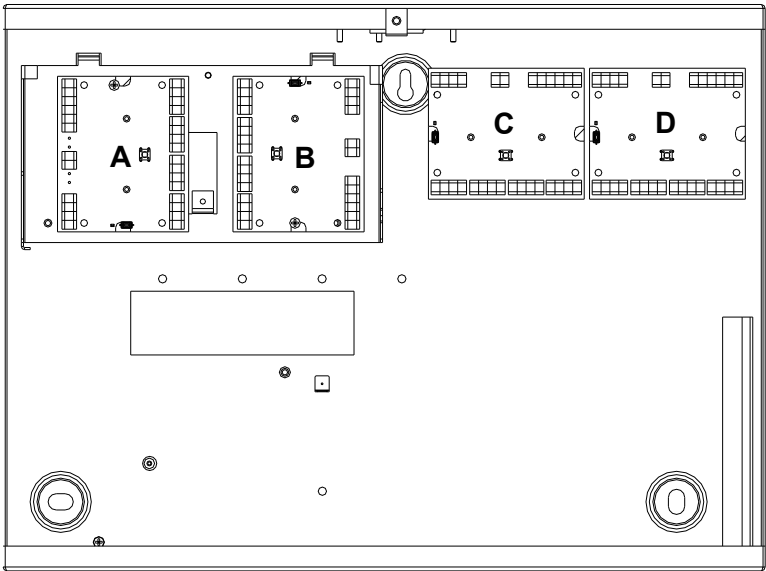


Figure 30 - Available positions for expansion in the MP500/16 control panel

Inside the MP500/16 control panel, 4 EP508 expansions (positions **A**, **B**, **C**, and **D**) can be assembled. The expansions must be fastened with the self-tapping screws supplied.
The positions **A** and **B** can be accessed by releasing and turning the mother board. If the GSM transmitter is used, it is not possible to use position **B**.
Position **A** is dedicated to the IT500WEB interface, but in its place an EP508 board can be installed.

 **IMPORTANT!** It is advisable to NOT INSTALL the radio expansion module in the MP500/16 control panel, because the metallic container of the control panel reduces reception of the radio signals, obstructing control of the radio devices associated with it.

5.5 INSTALLING THE MP500/4N - MP500/16 CONTROL PANELS

5.5.1 Description of the main parts of the MP500/4N control panel

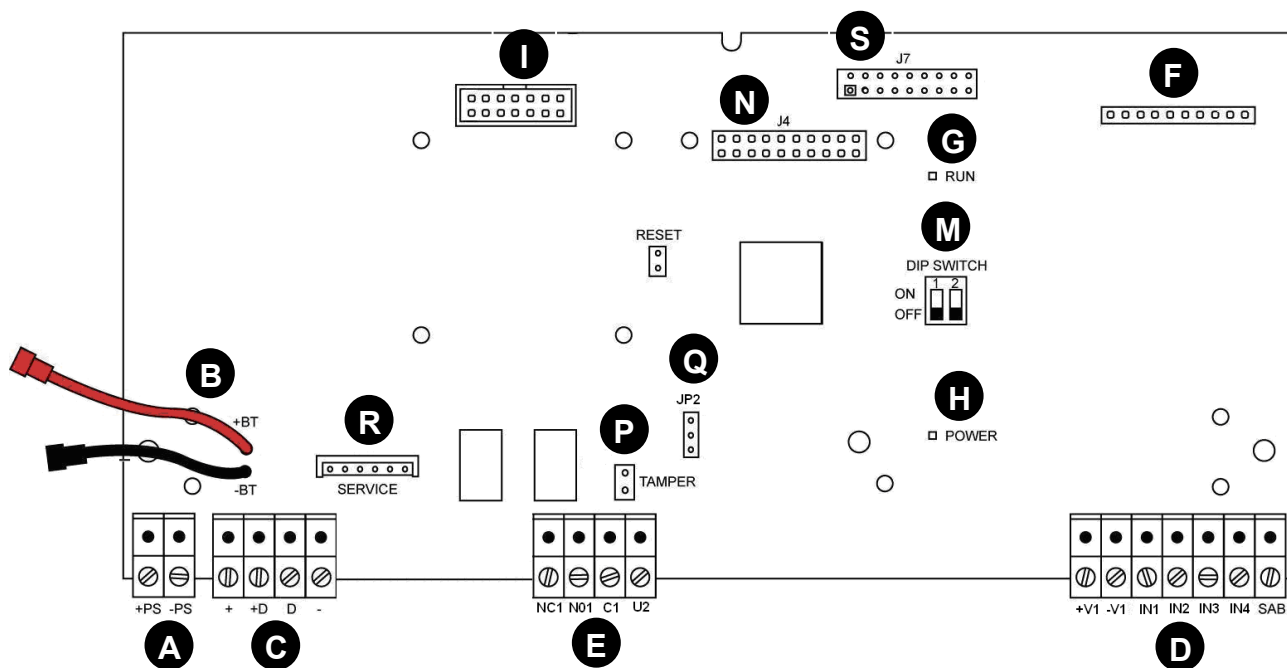


Figure 31 - Connections and main parts of the MP500/4N control panel

Detail	Terminal / Detail	Description
A	+PS	Input +14.4 V $\equiv$ power supply (at the positive pole of the power supply)
	-PS	Input power supply (at the negative pole of the power supply)
B	+BT	Connection positive pole of the back-up battery
	-BT	Connection negative pole of the back-up battery
C	+	BUS Power supply (13.8 V $\equiv$ limited to 1.1A) for devices connected via bus
	-	
	+D	BUS Data transmission/reception
	D	
D	+V1	Power supply of the detectors connected to the control panel (13.8 V $\equiv$ limited to 750 mA). The mother board has two pairs of power supply terminals.
	-V1	
	IN1	Alarm input n. 1
	IN2	Alarm input n. 2
	IN3	Alarm input n. 3
	IN4	Alarm input n. 4
E	SAB	Input 24h (for system self-protection). It must always be BALANCED and closed with a 15 k Ω balancing resistor.
	NC1	Relay output 1 – contact normally closed
	NO1	Relay output 1 – contact normally open
	C1	Relay output 1 – common (max. 1 A - 24 V $\equiv$)
F	U2	Electric output 2 (current protected max. 100 mA)
	J6	Connector for ILT500-N PSTN communicator
G	RUN	Green LED to signal functioning of the control panel (see paragraph 6.1.1 RUN LED Indications).
H	POWER	Green LED for signaling mains presence
I	J11	Connector of the USB and Web server interface
M	DIP SWITCHES	Dip-switch to reset parameter – see <i>functions associated with the dip-switches (Table 6)</i> (normally they must be left OFF)
N	J4	Connector of the vocal synthesis board
P	TAMPER	Connector for connection of the control panel tamper
Q	JP2	Jumper configuration output U2
R	SERVICE	Connector for connecting the service keypad
S	JP7	Connector for IMG500/N GSM Module (connecting point on the rear side of the motherboard)

The electric U2 output can be configured as “Positive Reference” or “Negative Reference” by means of the JP2 jumper. The default configuration is “Positive Reference”.

The electric outputs can be transformed into relay outputs – See Paragraph 5.12.6.2.

The figure illustrates how to position the JP2 jumper (Q).



Figure 32 - Configuration of the electric output hardware

For details on connections (power supplies, inputs, outputs, bus, ...) see paragraph 5.12 *Connections*.

Functions associated do the DIP-switches

To activate the reset functions associated with the DIP-switches, it is necessary to follow the indications found in paragraphs 7.9.4 *Resetting hardware installer code* and 7.9.5 *Resetting hardware to factory settings*.

DIP SWITCH	POSITION:	FUNCTION
1	OFF	Normal operation
	ON *	Reset hardware default
2	OFF	Normal operation
	ON *	Reset Technician code

*= if positioned on ON before “POWER ON”

Table 6 - Functions associated with the DIP-switches of the mother board

5.5.2 Description of the main parts of the MP500/16 control panel

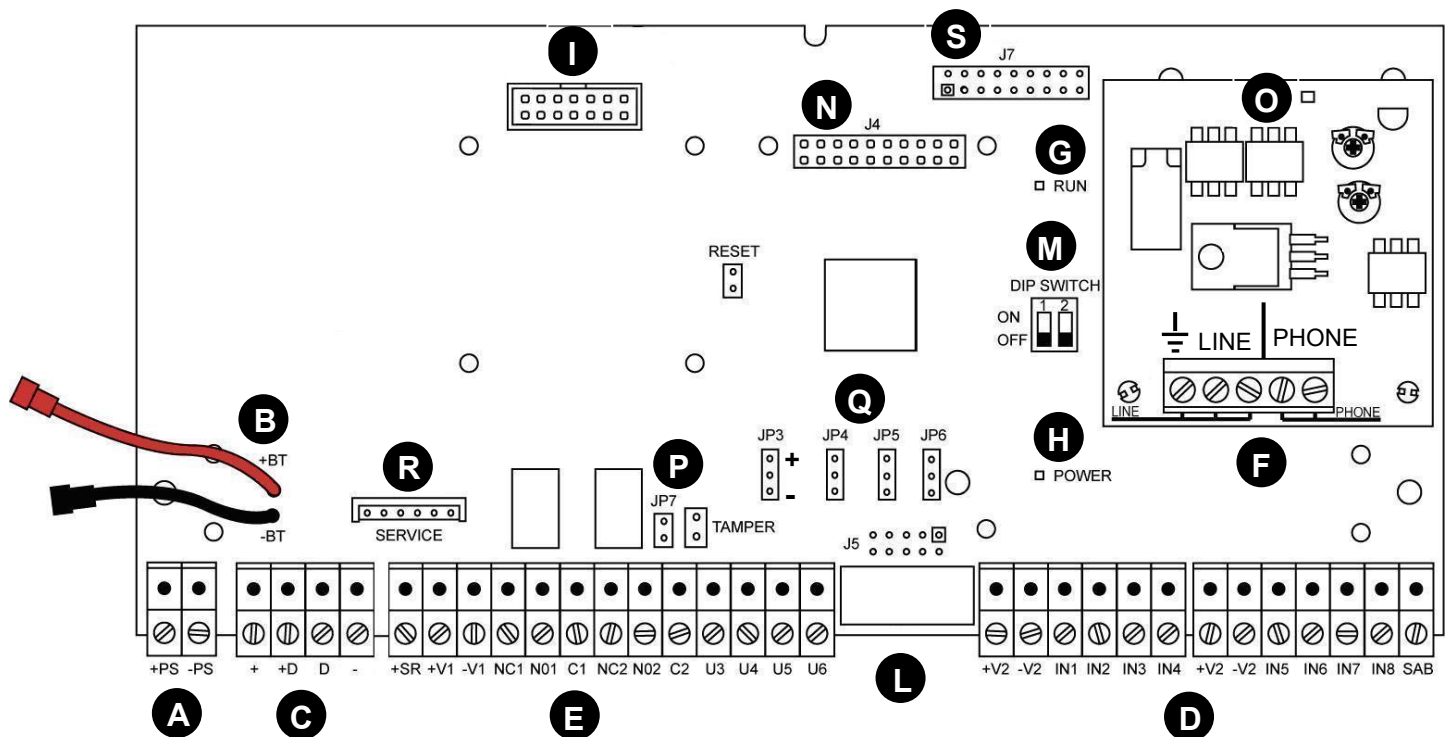


Figure 33 - Connections and main parts of the MP500/16 control panel

To facilitate the connection operations, the terminals must be unscrewed and reinserted onto the mother board.

Detail	Terminal / Detail	Description
A	+PS	Input +14.4 V ⁼⁼ power supply (at the positive pole of the power supply)
	-PS	Input power supply (at the negative pole of the power supply)
B	+BT	Connection positive pole of the back-up battery
	-BT	Connection negative pole of the back-up battery
C	+	BUS - Power supply 13.8 V ⁼⁼ — limited to 1.1A for devices connected via bus
	-	
	+D	BUS - Data transmission/reception
	D	
D	+V2	Power to detectors connected to control panel (13.8 V ⁼⁼ limited to 750 mA).
	-V2	The mother board has two pairs of power supply terminals.
	IN1	Alarm input n. 1
	IN2	Alarm input n. 2
	IN3	Alarm input n. 3
	IN4	Alarm input n. 4
	IN5	Alarm input n. 5
	IN6	Alarm input n. 6
	IN7	Alarm input n. 7
	IN8	Alarm input n. 8
E	SAB	Input 24h (for system self-protection). It must always be BALANCED and closed with a 15 kΩ balancing resistor.
	+SR	Power supply (14.4 V ⁼⁼ limited to 200 mA) - for recharging the batteries of the self-powered devices (ex. sirens). It is possible to connect up to 2 self-powered sirens. IMPORTANT! In case of blackout, +SR supplies no voltage, therefore it must be used only to connect self-powered devices. The self-powered devices must have a positive anti-return diode (all Elkron self-powered actuators are equipped with one).
	+V1	Power supply for output actuators (13.8 V ⁼⁼ limited to 750 mA)
	-V1	
	NC1	Relay output 1 – contact normally closed
	NO1	Relay output 1 – contact normally open
	C1	Relay output 1 – common (max. 1 A - 24 V ⁼⁼)
	NC2	Relay output 2 – contact normally closed
	NO2	Relay output 2 – contact normally open
	C2:	Relay output 2 – common (max. 1 A - 24 V ⁼⁼)
	U3	Electric output 3 (current protected max. 100 mA)
	U4	Electric output 4 (current protected max. 10 mA)
	U5	Electric output 5 (current protected max. 10 mA)
	U6	Electric output 6 (current protected max. 10 mA)
F	LINE	Input PSTN telephone line
	PHONE	Output PSTN telephone line
		Earth connection
G	RUN	Green LED to signal functioning of the control panel (see paragraph 6.1.1)
H	POWER	Green LED for signaling mains presence
I	J11	Connector of the USB and Web server interface
L	J5	
M	DIP SWITCHES	Dip-switch to reset parameter – see <i>functions associated with the dip-switches (Table 7)</i> (normally they must be left OFF)
N	J4	Connector of the vocal synthesis board
O	PSTN	Yellow LED signals that the telephone line is engaged
P	TAMPER	Connector for connection of the control panel tamper
	JP7	Jumper for the exclusion of the control panel tamper (Jumper inserted = tamper excluded)
Q	JP3	Jumper configuration output U3
	JP4	Jumper configuration output U4
	JP5	Jumper configuration output U5
	JP6	Jumper configuration output U6
R	SERVICE	Connector for connecting the service keypad
S	J7	Connector for GSM IMG500/N module (with insertion on the rear side of the mother board)

The electric outputs U3, U4, U5 and U6 can be individually configured as “Positive Reference” or “Negative Reference” via the JP3, JP4, JP5 and JP6 jumpers. The factory setting of the outputs is “Positive Reference”.

The electric outputs can be transformed into relay outputs – See Paragraph 5.12.6.2.

The figure illustrates how to position, for example, the JP3 jumper.

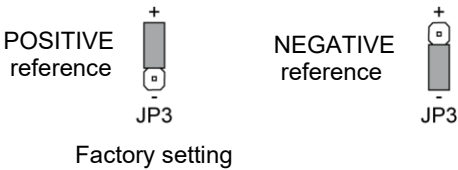


Figure 34 - Configuration of the electric output hardware

Functions associated do the DIP-switches

To activate the reset functions associated with the DIP-switches, it is necessary to follow the indications found in paragraphs 7.9.4 *Resetting hardware installer code* and 7.9.5 *Resetting hardware to factory settings*.

DIP SWITCH	POSITION	FUNCTION
1	OFF	Normal operation
	ON *	Reset hardware factory settings
2	OFF	Normal operation
	ON *	Reset Technician code

*= if positioned on ON before “POWER ON”

Table 7 - Functions associated with the DIP-switches of the mother board

5.5.3 Assembly of the PSTN ILT500-N communicator

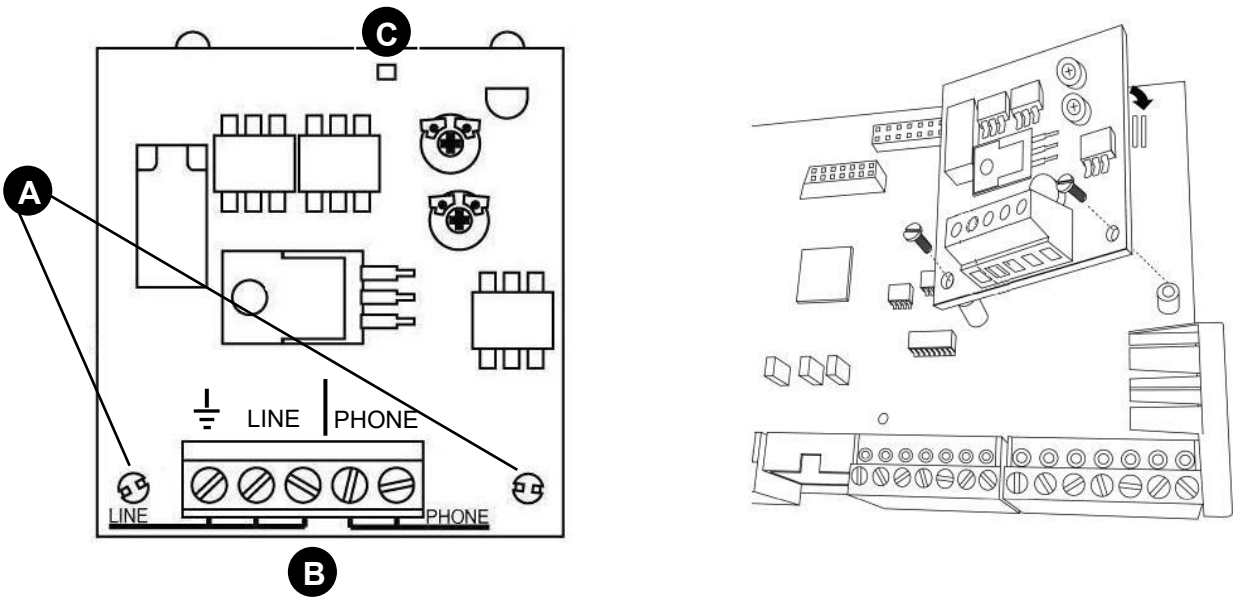


Figure 35 - Assembling PSTN communicator board

A	Holes for fixing screws
B	LINE PSTN Input telephone line
	PHONE PSTN Input telephone line
	Ground connection
C	Yellow LED signals that the telephone line is engaged

- To assemble the PSTN communicator board follow the instructions below:
- Insert the two support spacers included in the 2 holes **(A)** of the board.
 - Insert the header connector in the special connector **(F)** of the mother board.
 - Tighten the plastic nuts included to the support spacers through the holes present on the mother board.

⚠ IMPORTANT! The connection and disconnection of the optionals and accessories must always be done while the control panel is disconnected from all power supplies (both mains and battery).

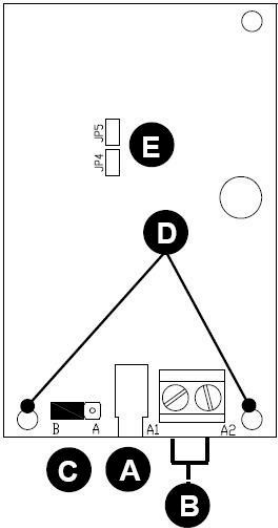


Figure 36 - Vocal synthesis board SV500N

A	Jack for earphone (included)
B	Terminal board for audio bus
C	Jumper to select recording input
D	Holes for support spacer
E	Jumper for preferred language selection

- To assemble the vocal synthesis board, follow the instructions below:
- Insert the two support spacers included in the two holes **D** of the board.
 - Insert the header connector in the special connector (**N**) of the mother board.
 - Select the input for the recording of messages by means of the Jumper **C**

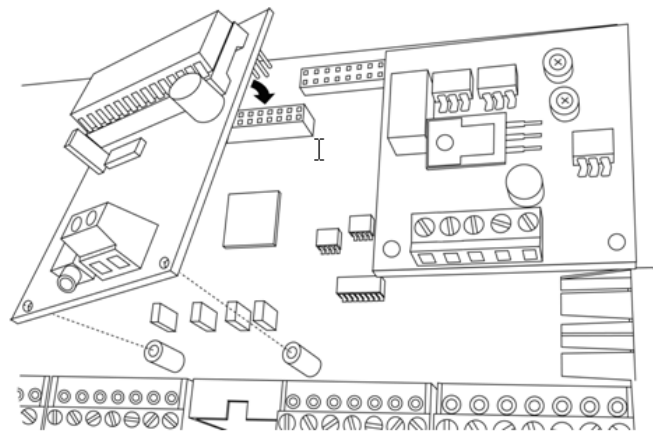


Figure 37 - Assembling the vocal synthesis board

The position of the jumper can also be modified later, without having to disconnect the power to the control panel. The position of the Jumper has no impact on the listening of the messages.

The recording takes place via a vocal keypad connected the audio bus.

The recording takes place via the earphone connected to the dedicated jack.

RECORDING AND LISTENING TO MESSAGES: For information on procedures for recording and listening to message, see the control panel *Programming Manual*.
SELECTING LANGUAGES: Use the JP4 and JP5 Jumpers to select the desired language (*Figure 36 - E*).

JP4

JP5

JP4-JP5 CLOSED:	80CT6610111	80CT6615111
	Italian	Spanish

JP4

JP5

JP5 CLOSED:	80CT6610111	80CT6615111
	English	German

JP4

JP5

JP4 CLOSED:	80CT6610111	80CT6615111
	French	Slovenian

⚠ IMPORTANT! The connection and disconnection of the optionals and accessories must always be done while the control panel is disconnected from all power supplies (both mains and battery).

5.5.5 Installation of the GSM Module

~~EN50131~~

The GSM module enables the MP500 control panels to communicate with the outside world via vocal messages and SMS.

The GSM module is installed **on the rear** of the mother board of the control panel. To install the module, follow the instructions below:

- Release the mother board as illustrated in *Figure 18 - Releasing the mother board* or *Figure 27 - Releasing the MP500/16 mother board*.
- Insert the three support spacers provided in the holes present along the sides of the module, leaving out the one found under the antenna connector.
- Insert the header connector in the holes of the mother board; these are in correspondence to the connector **C** of (welded sides with no components).
- Tighten the plastic nut included to the support spacer through the holes present on the mother board.

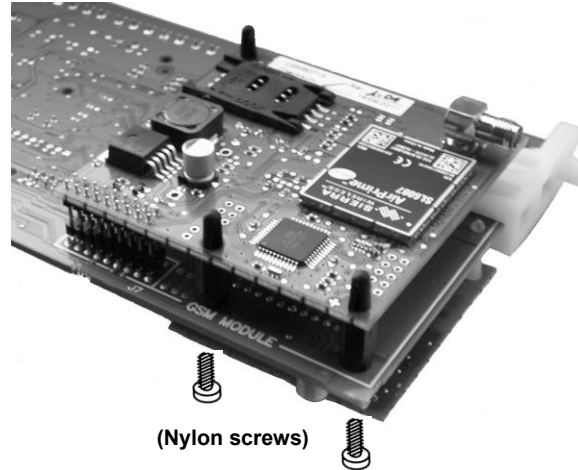


Figure 38 - Installation of the GSM module



IMPORTANT! The use of the GSM invalidates the EN50131 compliance.



IMPORTANT! The connection and disconnection of the optionals and accessories must always be done while the control panel is disconnected from all power supplies (both mains and battery).

5.5.5.1 Installation of the GSM antenna on the MP500/4N control panel

For the MP500/4N control panel, insert the GSM antenna provided in the specific compartment (*Figure 20 - Fastening points for optional features in the MP500/4N control panel*).

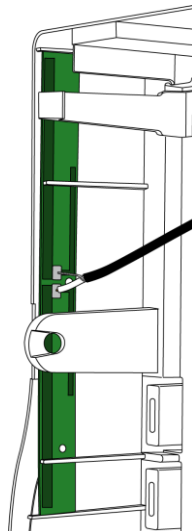


Figure 39 - Installation of the GSM1 antenna on MP500/4N

When, due to the position of the control panel, the internal antenna provided with the package should not guarantee the module adequate signal levels, use the optional GSM1 external antenna.

5.5.5.2 Installation of the GSM antenna on the MP500/16 control panel

For the MP500/16 control panel, as the container is in metal, it is necessary to replace the antenna provided with the optional GSM2 antenna for the metallic box (*Figure 29, E - Fastening point options in the MP500/16 control panel*).

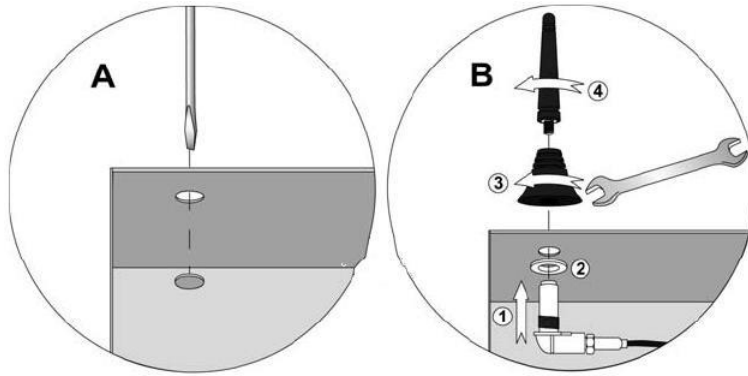


Figure 40 - Insertion of the GSM2 antenna on MP500/16

When, due to the position of the MP500/16 control panel, the internal antenna provided with the package should not guarantee the module adequate signal levels, use the optional GSM1 external antenna.



IMPORTANT! It is advisable to tighten the antenna SMA connector found on the interface firmly, but without damaging it (locking torque 0.9 Nm).

5.5.5.3 Important information about the SIM Card

The SIM Card must be purchased separately from a GSM mobile telephone provider.

In order to use the remaining credit signal via the MP500/16 system, it is advisable to use a Vodafone or TIM SIM Card: it may NOT work correctly with other providers.

If the GSM channel is used to connect to a remote PC (remote management and programming) it is necessary to acquire a SIM Card with **DATA/FAX incoming + Voice**; this application was tested with a TIM SIM Card.



IMPORTANT! To compensate for the issue of credit remaining and expiration, typical of prepaid SIM cards, it is advisable to use a SIM Card with a subscription.

5.5.5.4 Setting up the SIM Card



IMPORTANT! Before inserting the SIM Card in the GSM module, it must be activated with a mobile phone.

In the case of the prepaid SIM Card:

- Check that there is a sufficient margin of credit to ensure the functioning of the GSM module.
- Take note of the expiration date when it must be recharged (generally 12 months from the date of the last recharge; in any case, check the conditions of the provider's contract).

By setting the expiration date of the SIM Card in the control panel, it is possible to receive vocal messages and/or SMS warnings until the expiration date (see the *Programming Manual*).

It is also possible to receive messages from the provider on one's personal telephone to inform when the credit goes below a specified threshold, as well as other service messages (see the *Programming Manual*).

5.5.5.5 Inserting the SIM Card

IMPORTANT! The insertion / removal of the SIM must be carried out while the control panel is not connected to any power supply (mains power supply and battery disconnected), or provided that the GSM network has been disabled for the time necessary to complete the operation (see the *Programming Manual*).

To insert the SIM Card, follow the instructions below:

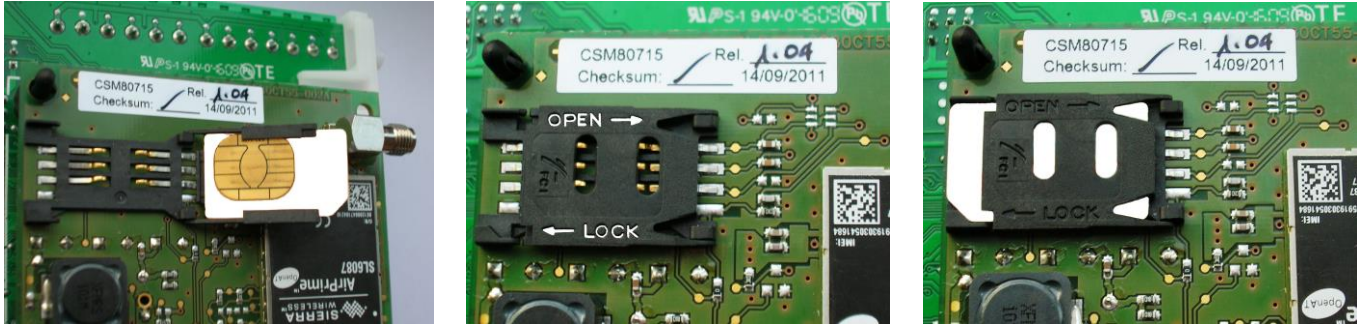


Figure 41 - Insertion of the GSM2 MP500/16 antenna

- Open the SIM Card drawer by pushing the cover in the direction indicated by the “OPEN” arrow.
- Insert the SIM Card, with the gold contacts visible from the outside.
- Reclose the cover by pushing it in the direction of the “LOCK” arrow.

5.6 CONNECTION OF THE USB INTERFACE AND WEB SERVER

5.6.1 Temporary connection of the IT - USB/KEY interface for the USB pen drive for connecting to the PC

In order to connect the interfaces, it is necessary to remove, with the control panel disconnected from the mains, the two jumpers present in the motherboard J11 connector (*Figure 31* and *Figure 33 – I*)

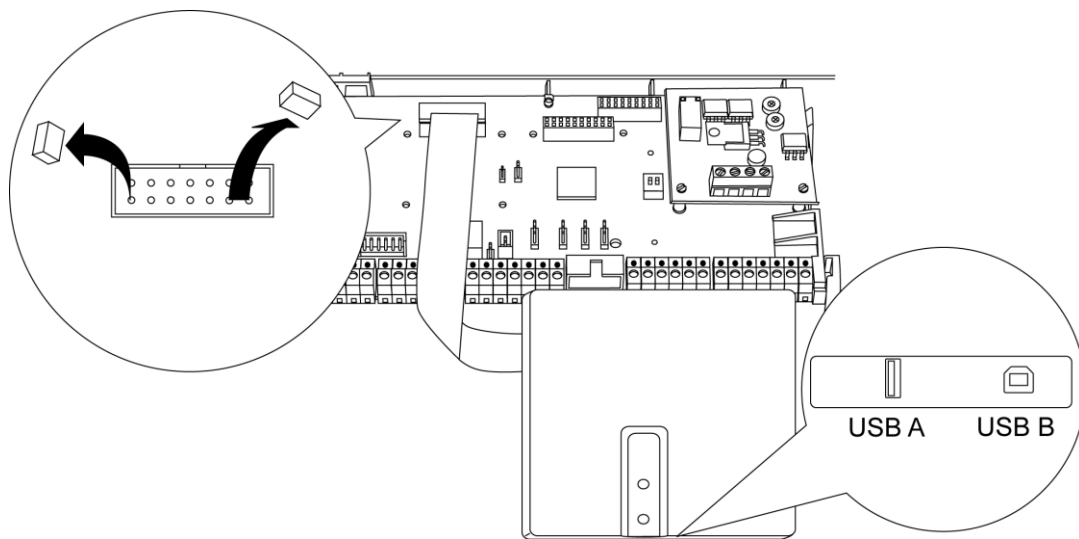


Figure 42 - Connecting the IT-USB/KEY INTERFACE

If there is an IT500WEB, disconnect its connector with control panel is disconnected from all power supplies.

IMPORTANT! Connect the USB interface to the control panel before connecting it to the PC.

IMPORTANT! The connection and disconnection of the optionals and accessories must always be done while the control panel is disconnected from all power supplies (both mains and battery).

5.6.2 Installation of the IT500WEB web server interface

In order to install the interface, follow the instructions below:

- 1) release the mother board from its compartment and flip it over
- 2) position the interface on the bottom of the control panel and fasten it using the two screws provided (Fig. a)
- 3) to connect it, insert a flat cable connector on the interface and the other on the mother board connector (J11 – Fig. b)



Fig. 1a

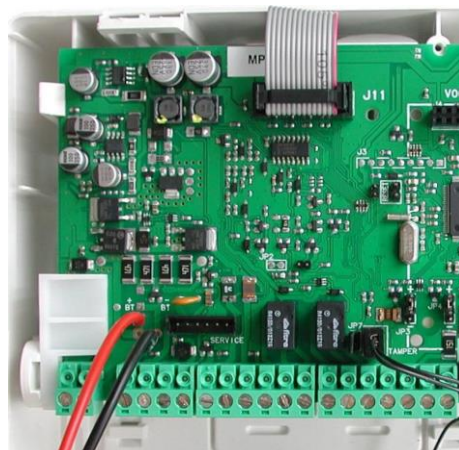


Fig. 1b

Figure 43 - Installing the web server interface on MP500/4N

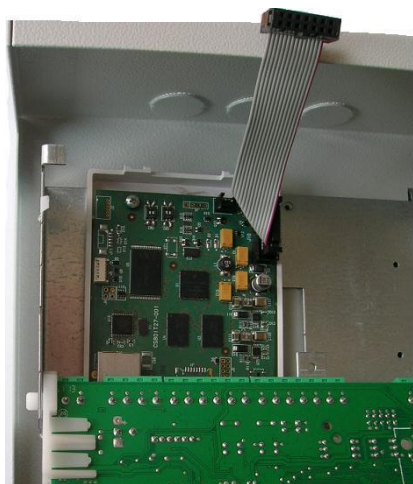


Fig. 2a



Fig. 2b

Figure 44 - Installing the web server interface on MP500/16



IMPORTANT! The connection and disconnection of the optionals and accessories must always be done while the control panel is disconnected from all power supplies (both mains and battery).

5.7 INSTALLATION OF THE EP508 EXPANSION

In addition to inside the control panel, the EP508 expansion can also be installed inside a CP/EXP container (compliant Grade 3) or a CP/EP500 container (not certified).



IMPORTANT! the absence of a casing compliant Grade 2 or 3 results in the loss of compliance.

The tamper of the container must be connected to the SAB of the expansion.

The expansion has terminals for connecting the power supply, detectors, and signalling devices, etc.

The electric outputs can be transformed into relay outputs – See Paragraph 5.12.6.2.

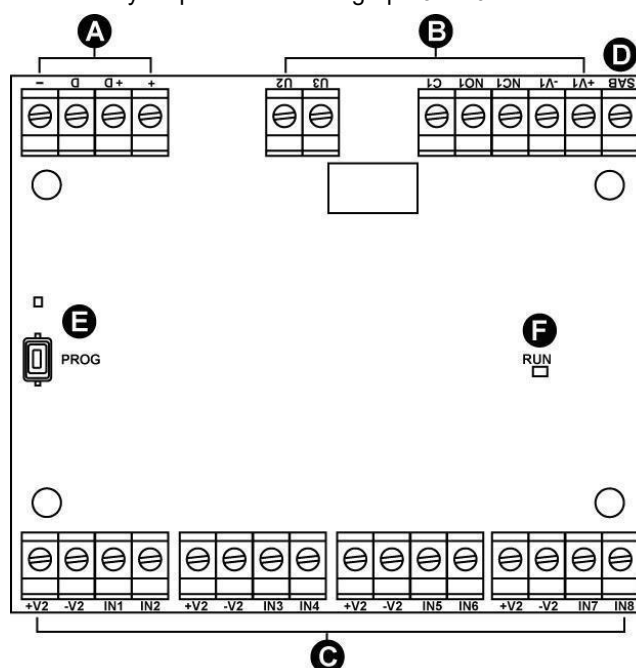


Figure 45 - EP508 Expansion

Detail	Terminal / Detail	Description
A	+	BUS Expansion unit power input via bus
	+D	BUS Data transmission / reception
	D	BUS Data transmission / reception
	-	BUS Expansion unit power input via bus
B	+V1	Power supply for output actuators (13.2 V $\approx$ limited to 500 mA)
	-V1	
	NC1	Relay output 1 – contact normally closed
	NO1	Relay output 1 – contact normally open
	C1	Relay output 1 – common (max. 1 A - 24 V $\approx$)
	U2	Electric output 2 (current protected max. 10 mA)
	U3	Electric output 3 (current protected max. 10 mA)
C	+V2	Power to detectors connected to expansion unit (13.2 V $\approx$ limited to 500 mA). Four pairs of power terminals are connected to the expansion unit.
	-V2	
	IN1	Alarm input n. 1
	IN2	Alarm input n. 2
	IN3	Alarm input n. 3
	IN4	Alarm input n. 4
	IN5	Alarm input n. 5
	IN6	Alarm input n. 6
	IN7	Alarm input n. 7
	IN8	Alarm input n. 8
D	SAB	Input 24h (for system self-protection). It must always be BALANCED and closed with a 15 k Ω balancing resistor
E	Button Yellow LED	Device acquisition button and LED
F	RUN	Green LED signals operating (for details see the <i>Programming Manual</i>) Slow blinking = normal operating conditions Fast blinking = no communication with control panel for at least 1 minute

For details on connections (power supplies, inputs, outputs, bus, etc. ...) see paragraph 5.12.2 *Connecting the data Bus* and paragraphs, 5.12.5 *Connecting inputs* and 5.12.6 *Connecting outputs*.

5.8 INSTALLATION OF THE KP500D/N – KP500DV/N KEYPADS

The differences between the two keypads are:

- The KP500D/N keypad is equipped with two freely programmable auxiliary inputs referring to positive.
- The KP500DV/N is equipped with a loudspeaker/microphone for the recording and listening of messages and environmental listening functions. To use these functions, the SV500N vocal synthesis board assembled in the control panel must be used and an audio bus with a standard twin telephone line.

The KP500 keypads can be installed on the wall or above a built-in rectangular box with 3 spaces or a 60-mm round box.

To install the keypad, follow the instructions below:

1. Opening keypad:

- open the lid;
- with the sharp edge of a screwdriver, exert a slight pressure on point indicated in picture and release closing tooth;
- then, close the lid and open the keypad.

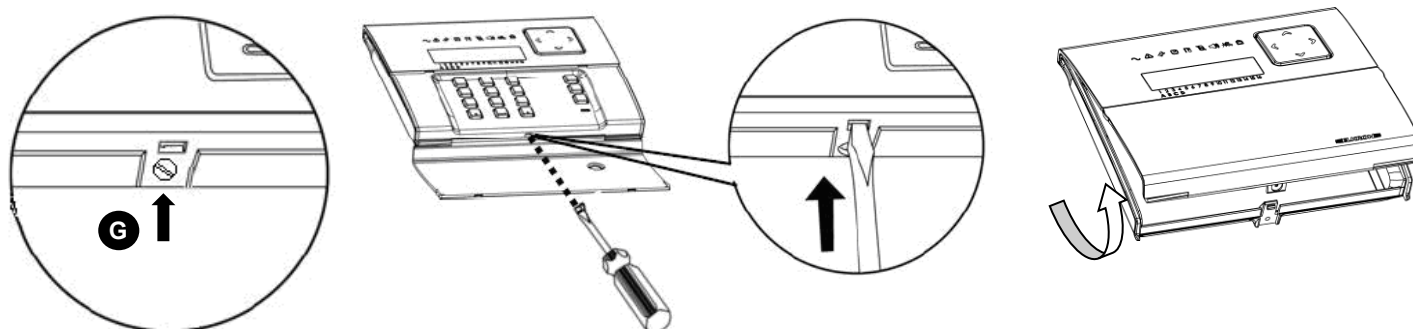


Figure 46 - Opening the keypad

2. For running the cables, open the scored hole on the bottom of the keypad. Otherwise, the scored holes for the cable ducts can be used.

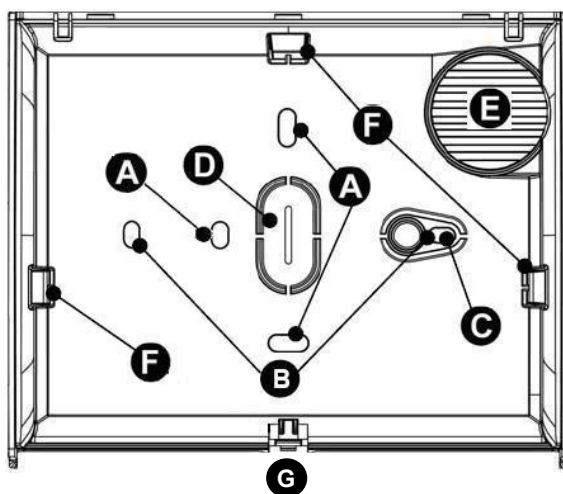


Figure 47 - Holes in the keypad and running cables

A	Screws for fastening to wall or Ø 60
B	Holes for fastening to 3-place box
C	Hole for fastening anti-removal protection
D	Scored holes for running cables
E	Loudspeaker grid
F	Scored holes for cable ducts
G	Closing screws (provided)

3. Fasten the bottom of the keypad to the wall using 6mm expansion screws (not supplied). For EN50131 Degree 3 compliance, always use the anchor bolt in position **C**, even if the keypad is fixed to a flush-mounting box. This requirement is not mandatory for Degree 2 or lower installations.

! IMPORTANT! Before fastening, check the orientation of the bottom: The loudspeaker grid must be in the upper right.

4. Connect any other devices to the auxiliary inputs or the audio line to the dedicated terminals. For easier wiring, it is advisable to strip the cable as far as the access hole.

The keypad boards differ slightly, depending on the model.

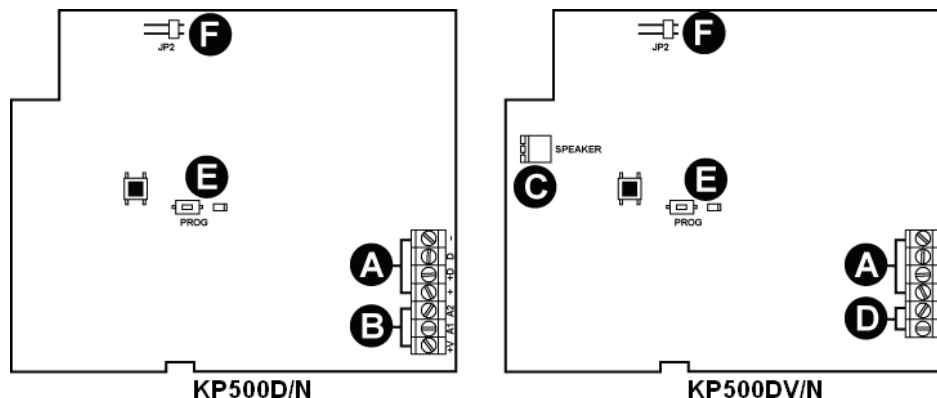


Figure 48 - Keypad boards

Detail	Terminal / Detail	Description
A	+	BUS Expansion unit power input via bus
	+D	BUS Data transmission/reception
	D	
	—	BUS Keypad power supply via bus
B only KP500D/N	+V	Power supply for auxiliary inputs (13.8 V $\approx$ limited to 100 mA)
	A1	Auxiliary input 1
	A2	Auxiliary input 2
C only KP500DV/N	SPEAKER	Connector for loudspeaker
D only KP500DV/N	A1	Audio bus
	A2	
E	Button Yellow LED	Device acquisition button and LED
F	JP2	Jumper for the exclusion of the keypads tamper (Jumper inserted = tamper excluded)

5. Close the keypad using the screw provided - *Figure 46 (G)*.

For details on connections (power supplies, inputs, bus, etc. ...) see paragraphs 5.12.2 *Connecting the data Bus*, 5.12.3 *Connecting the audio Bus*, and 5.12.5 *Connecting inputs*.

5.9 INSTALLATION OF THE KP500DP/N - KP500D/ST TOUCH SCREEN

The KP500DP/N or KP500D/ST keypad can be installed on the wall or above a built-in rectangular box with 3 spaces or a 60-mm round box.

To install the keypad, follow the instructions below:

1. Release the keypad from the wall bracket by sliding it off.

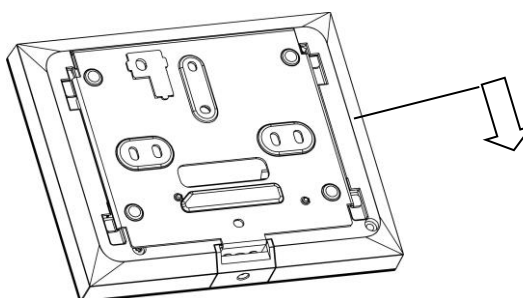


Figure 49 - Removal of the KP500DP/N - KP500D/ST keypad bracket

2. Fasten the support bracket to the wall using 6-mm expansion screws (not provided), or on the built-in box if present, holding the terminal board downward. Avoid over-tightening the screws, in that they may cause the bracket to curve, making it difficult to assemble the keypad onto the bracket itself.

- Open the keypad by putting a screwdriver into the slot on the lower side and lifting gently.

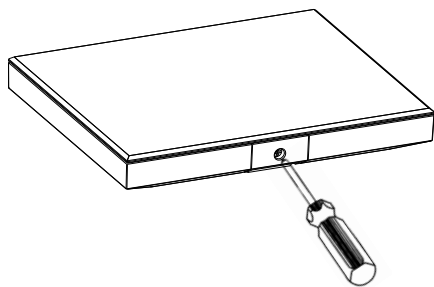


Figure 50 - Opening the KP500DP/N - KP500D/ST keypad

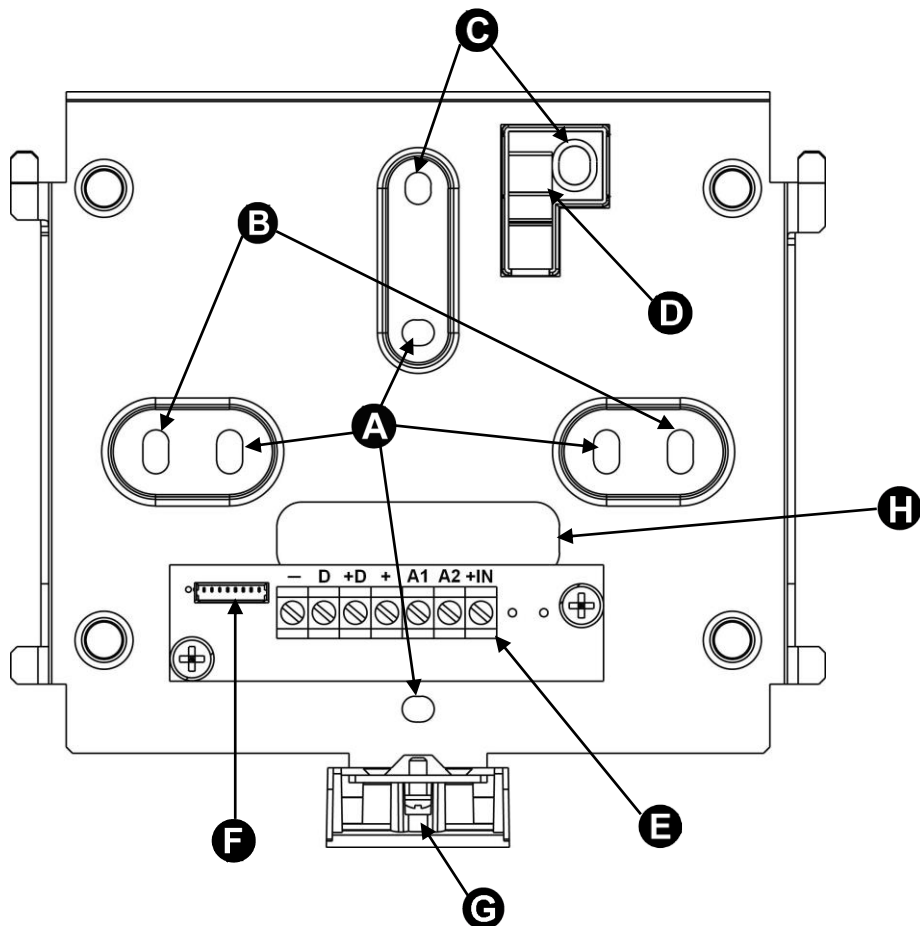


Figure 51 - Holes for fastening and running the cables of the KP500DP/N - KP500D/ST keypad

A	Holes for fastening onto the Ø 60 mm built-in box
B	Holes for fastening to 3-place box
C	Holes for removal protection screws
D	Plastic insert for anti-removal protection
E	Connection terminal board
F	Keypad connector
G	Closure screws
H	Hole for running cables

Terminal	Description of detail
+	BUS Expansion unit power input via bus
+D	BUS Data transmission/reception
D	
—	BUS keypad power supply via bus
+IN	Power supply for auxiliary inputs
A1	Auxiliary input
A2	Auxiliary input 2

- To use the anti-removal device, put an expansion screw in hole “C” and fasten it to block “D”. For EN50131 Degree 3 compliance, it must always be used, even if the keypad is fixed to a flush-mounting box. This requirement is not mandatory for Degree 2 or lower installations.
- Connect the bus cable to the terminal board. For details of the connection, see paragraph 5.12.2 *Connecting the data Bus*.
- Insert the small cable coming out of the keypad in the dedicated connector “F”. Place the cable so that it fits into the specially designed space at the bottom of the keypad; this prevents it from being crimped when assembling the keypad to the bracket.
- Insert the keypad block into the bracket and slide it downward.
- Block it with a fastening screw “G”.

5.10 INSTALLING THE READER

The electronic key readers and transponders are installed in boxes to be built-in or wall-mounted and positioned in a dry area. The reader is suitable to be installed on BTicino Magic frame and using BTicino code A5374/1 adapters, on BTicino TT Matix frames. Moreover, by using the adaptor frames (not provided), the readers can be inserted as switches within the wiring, like the B-ticino® Light / International / Living ; Gewiss® Playbus ; AVE® Sistema 45 ; Axolute® ; Eikon® ; Vimar® Idea ; Vimar® Plana; Vimar 8000 ; Simon Urmet nea, etc.

! IMPORTANT! In accordance with EN50131 standards, the readers installed outside the protected zone must be protected by devices to prevent tampering.

! IMPORTANT! The absence of the tamper results in the loss of EN50131 compliance.

The readers are equipped with two freely programmable auxiliary inputs referring to positive.

To install the reader, follow the instructions below:

1. Connect the reader to the Bus.
2. Install the reader, with the adapter if necessary, on the switch frame available, possibly in a position that leaves it accessible to the button and to the programming LED located on the side of the reader.
3. Connect the tamper to the input 1 of the reader (yellow wire: interrupt the wire by cutting it and connect the two ends to the tamper). The TAMPER is the default setting.
4. Connect another optional device to input 2 (green wire: interrupt the wire by cutting it and connect the two ends to the device).

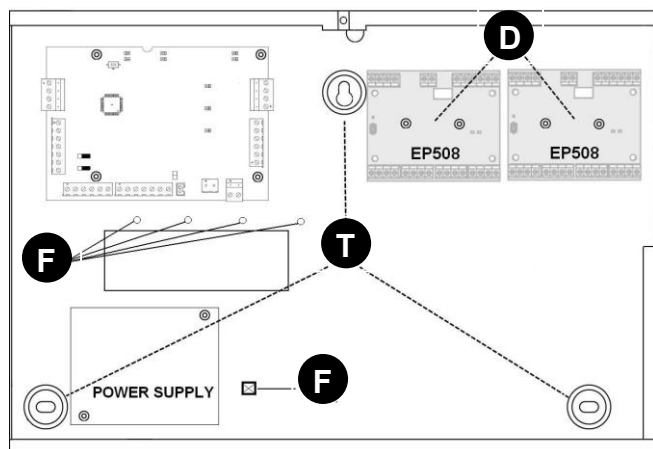
! IMPORTANT! If two readers must be installed near each other in the same box, whether build-in or wall-mounted, leave at least the space of one switch between them.

For details on connections (power supplies, inputs, bus, etc. ...) see paragraphs 5.12.2 *Connecting the data Bus* and 5.12.5 *Connecting inputs*.

5.11 INSTALLATION OF THE AS500/RPT SUPPLEMENTARY POWER SUPPLY

! IMPORTANT! During installation of the control panel, be very careful to not accidentally damage the board.

5.11.1 Fastening to the wall



T Holes for fastening to the wall. Use Ø 6mm plugs depending on the type of material making up the wall with TCB screw DIN 7981 3.9 x 32.

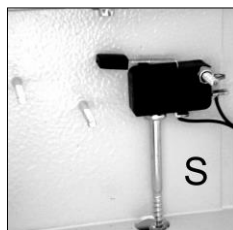
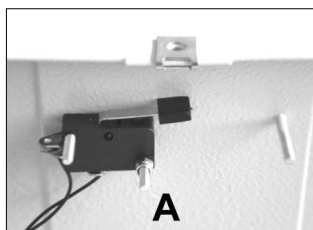
D Holes for fastening 2 optional EP508 expansions

F Band to fasten power supply cables

Figure 52 - Holes for fastening the AS500/RPT

Position the tamper in position **A** or **S**, according to the type of application desired:

- in position **A**, only for protection against opening
- in position **S**, for protection against opening and removal, in this case using the expansion screws with for the support of contact.

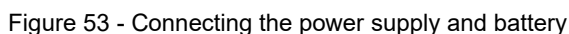


Connect the tamper connection to the board in both cases.

5.11.3 The AS500/RPT board

In the BUS IN section there is an EP508 integrated expansion (**E**).

In the BUS OUT section there is an integrated repeater function (**R**) and power supply (**P**).



5.11.3 The AS500/RPT board

In the BUS IN section there is an EP508 integrated expansion (**E**).

In the BUS OUT section there is an integrated repeater function (**R**) and power supply (**P**).



5.11.3.1 The Expansion

By referring to the *Figure 54 - AS500/RPT Board*, the functions of the terminals, LEDs, and buttons dedicated to the Expansion are the following:

Terminal board	Group	Description	Connection / Function
M1	Bus IN	+	Expansion power supply via bus
		+D	BUS Data transmission/reception
		D	
		—	Expansion power supply via bus
M2	Outputs	+V1	Power supply for output actuators (limited to 500 mA)
		-V1	
		NC1	Relay output 1 – contact normally closed
		NO1	Relay output 1 – contact normally open
		C1	Relay output 1 – common (max. 1 A - 24 V _{max})
		U2	Electric output 2 can be configured (protected from short circuit - I max 10mA)
		U3	Electric output 3 can be configured (protected from short circuit - I max 10mA)
M3 / M4	Inputs	+V2	Power supply for detectors (limited to 500 mA)
		-V2	
		IN1	Alarm input n. 1
		IN2	Alarm input n. 2
		IN3	Alarm input n. 3
		IN4	Alarm input n. 4
		IN5	Alarm input n. 5
		IN6	Alarm input n. 6
		IN7	Alarm input n. 7
		IN8	Alarm input n. 8
	TAMPER	SAB	24h input (for system self-protection), must always be BALANCED and closed with a 15 kΩ balancing resistor.
		Tamper	Connector for connection of the tamper
		JP1	Jumper for the exclusion of the tamper (Jumper inserted = tamper excluded)
	PROG	Button and LED	Button and LED (yellow) for programming.
	RUN	LED	Green LED to signal operation.

The electric outputs U2 and U3 can be individually configured as “positive reference” or “negative reference” via the JP2, and JP3 jumpers. The default configuration of the outputs is “Positive Reference”.

The electric outputs can be transformed into relay outputs – See Paragraph 5.12.6.2.

For details on connections (power supplies, inputs, outputs, bus, etc. ...) see paragraph 5.12.2 *Connecting the data Bus* and paragraphs 5.12.5 *Connecting inputs* and 5.12.6 *Connecting outputs*.

The expansion is always powered by the control panel via the bus connected to the M1 terminals. The power supply for the detectors and the signalling devices connected to the M2 / M3 / M4 terminal boards always arrives from the control panel.

The expansion section also controls the functioning of the secondary bus. If an attempted tampering should be detected or merely a malfunction should be detected, disconnect the secondary bus to prevent compromising the functioning of the entire system.

The MP500/16 control panels receive information on the functioning of the supplementary power supply from the expansion: black out, battery low, and power supply breakdown.

5.11.3.2 The Repeater

The Repeater circuit regenerates the data and provide power for the extension of the new length of Bus for the control panel (drawn from the power supply and the local battery). By referring to the *Figure 54 - AS500/RPT Board*, the functions of the terminals and LEDs dedicated to the Repeater are the following:

Terminal board	Group	Terminal	Connection/Function
M8	OUT BUS	+	Bus extension power supply
		+D	BUS Data transmission/reception
		D	
		—	Bus extension power supply
LED data	IN	TX	Green LED (TX BUS control panel) (data transmission to control panel)
		RX	Yellow LED (RX BUS control panel) (data reception from control panel)
	OUT	TX	Green LED (extended TX BUS) (data transmission to extended BUS)
		RX	Yellow LED (extended RX BUS) (data reception from extended BUS)

The BUS OUT terminal board is used to connect the various devices to the new length of the Bus. The signals coming from the Bus of the control panel are repeated to be transported a long distance, with the MP500/16 control panel having complete control.

The Repeater section is irreversibly linked to the power supply section “P”, which also provides it with power. Therefore, in case of a blackout or absence of the back-up battery, it will not be possible to reproduce the data on the Bus (essentially the extension of the bus is lost together with all the devices that are connected to it).

5.11.3.3 Power supply

The power supply circuit controls the power supply and the power supply outputs, and also manages the battery. More specifically, when the battery is charging, it carries out the efficiency test and, when there is a blackout, it disconnects the battery when the voltage to the battery terminals reaches about 10.5 V, thereby protecting it from the deep discharge. The battery will be automatically recharged when the mains power supply is restored. By referring to the *Figure 54 - AS500/RPT Board*, the functions of the terminals and LEDs dedicated to the Power supply are the following:

Terminal board	Group	Terminal	Connection / Function
M5	Battery	+BT	Back-up battery power supply input (positive pole)
		- BT	Back-up battery power supply input (negative pole)
M6	Power supply	+PS	Power supply input (at the positive terminal of the power supply)
		+PS	Power supply input (at the negative terminal of the power supply)
M7	Outputs Auxiliaries	+SR	Power supply (14.4 V $\approx$ limited to 200 mA) for recharging the batteries of the self-powered devices (ex. sirens). It is possible to connect up to 2 self-powered sirens.
		-	Important: In case of blackout, +SR supplies no voltage, therefore it must be used only to connect self-powered devices. The self-powered devices must have a positive anti-return diode in series. Note: all the Elkron self-powered actuators come equipped with this device.
		+	2 Auxiliary power supplies (limited to 750 mA)
		-	
LED	Green	PWR	Network/battery presence
	Yellow	BL	Battery state
	Yellow	FUSE	Power fault +SR; +; +BUS OUT; +D

5.12 CONNECTIONS

This paragraph contains instructions on how to carry out all the electrical connections and necessary signals for starting up the system.



IMPORTANT! Before running the cables, check that the sections are correct and that conform with the maximum distances. If in doubt, consult paragraph 4.2.

IMPORTANT! The end of the stranded conduction must not be consolidated with a soft-solder welding in the points where the conductor is subject to contact pressure.

Therefore it is not allowed to solder the terminals of the cables connected to the terminals of the devices.

5.12.1 Power supply line



IMPORTANT! Before making any connections to the mains power supply, disconnect the mains power supply.

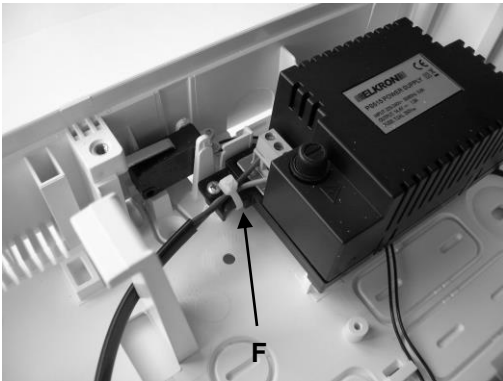
In fulfilment of the electrical safety standards for power supplies, a suitable isolating device must be installed, like a double-pole thermo-magnetic circuit breaker to protect the mains power supply (*Figure 55 - Diagram of the connections to the mains power supply*). The mains disconnect must have a separation between the contacts of at least 3 mm.

It is advisable to position the circuit breaker upstream from the differential switch (the so-called "automatic cut-out switch"), in order to be able to disconnect other sections of the electrical system, thereby maintaining the functionality of the MP500 systems.

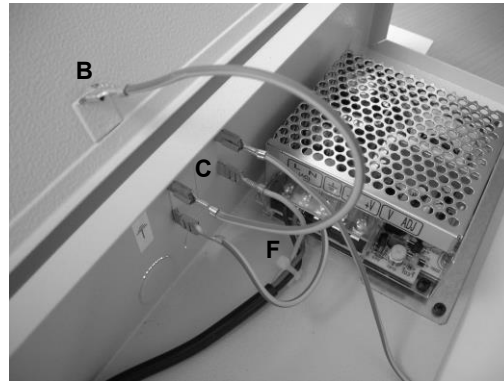
For the power supply, use a 2 x 1.5 mm² cable.

The MP500/4N control panel is double isolation and do not need earths (PE). However, the earth connection is required only for the connection to the telephone line.

The MP500/16 control panel and the AS500/RPT power supply require, instead, an each connection (PE) made with cable of a section no less than that of the cable used for the power supply. For this connection, there is a Faston connector provided with the control panel.



MP500/4N control panel



MP500/16 - AS500/RPT control panel

Female Faston connector
6.3 x 0.8 mm



(F) Point where power cables are fastened with the band

(F) Point where power cables are fastened with the band

1. Connect the mains power supply cables to the 2 terminals of the control panel power supply.
2. *Only for MP500/16 and AS500/RPT:* To connect the earth of the equipment, crimp the Faston terminal (A) (provided with the system) onto the earth cable that will be inserted into one of the Faston terminals on the wall of the box (C) and connect the small earth cable to the cover Faston (B).
3. Secure the wires by fastening them in anchoring point (F) with the strip provided.



IMPORTANT! After having connected the wires, remember to insert the plastic protection on the terminals.

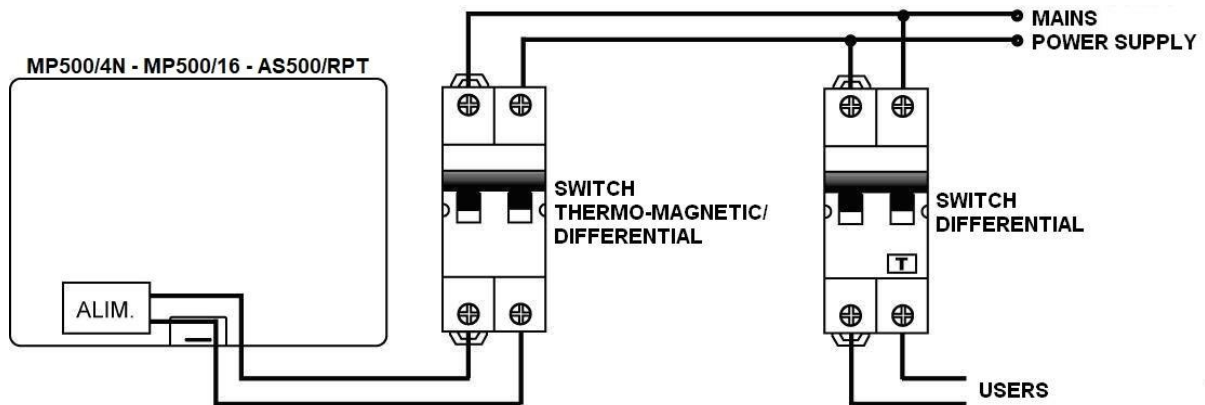


Figure 55 - Diagram of the connections to the mains power supply



IMPORTANT! The system must be powered by the mains only when all the devices are installed correctly, making it possible to proceed with their acquisition. For security purposes, close even the control panel casing before powering it up.

5.12.2 Connecting the data Bus

Connect the terminals **+**, **+D**, **D** and **—** the cable to the 4 wires of the bus; this will enable the communications among the control panel, readers, keypads, any expansions present.

The data bus requires no terminal resistors.

The cable shieldings can be connected together in the control panel at the negative pole (**—**) of the power supply.

The *Figure 56 - Connections via bus* demonstrates how to connect the various devices to each other via the bus line.

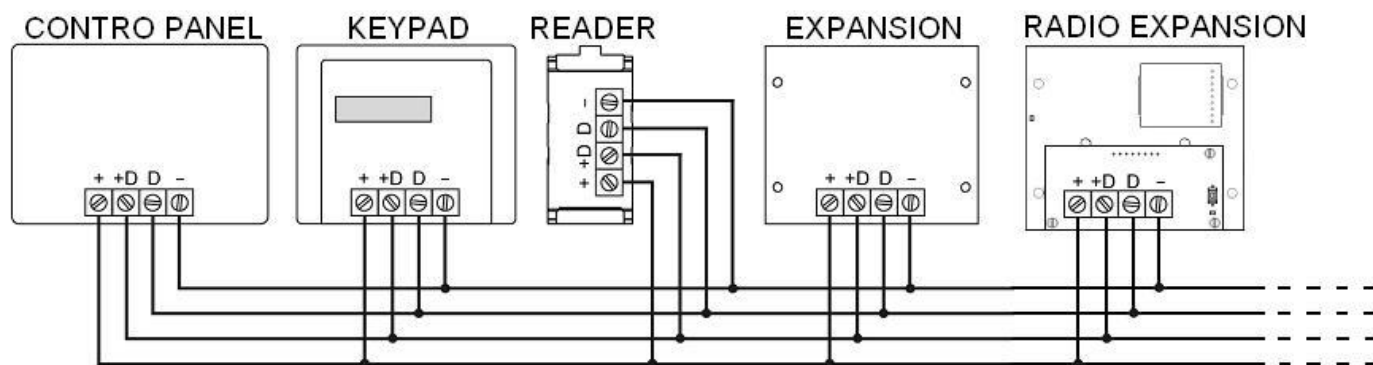


Figure 56 - Connections via bus

5.12.3 Connecting the audio Bus

Connect, if necessary, the twisted pair of the audio bus to the A1 and A2 terminals of the SV500N vocal synthesis board.

When connecting the audio bus, it is not necessary to take the polarity into account.

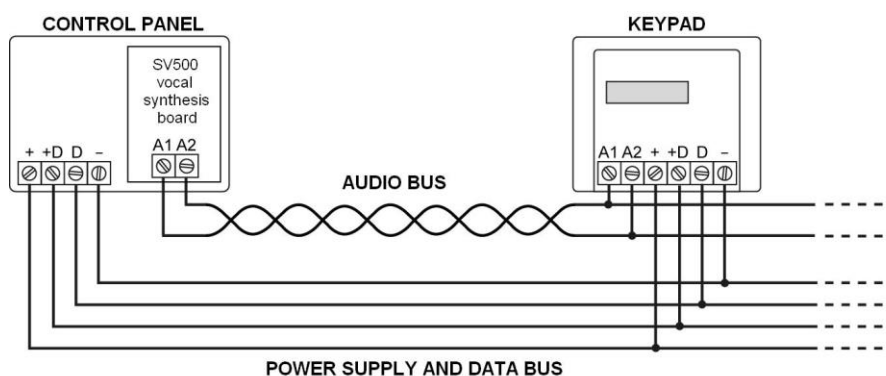


Figure 57 - Connections the audio bus

5.12.4 Connecting the supplementary power supplies/repeater

To understand which the length limits of the bus and how to calculate them, read paragraph 4.2.4 *Extending the bus with the repeater*.

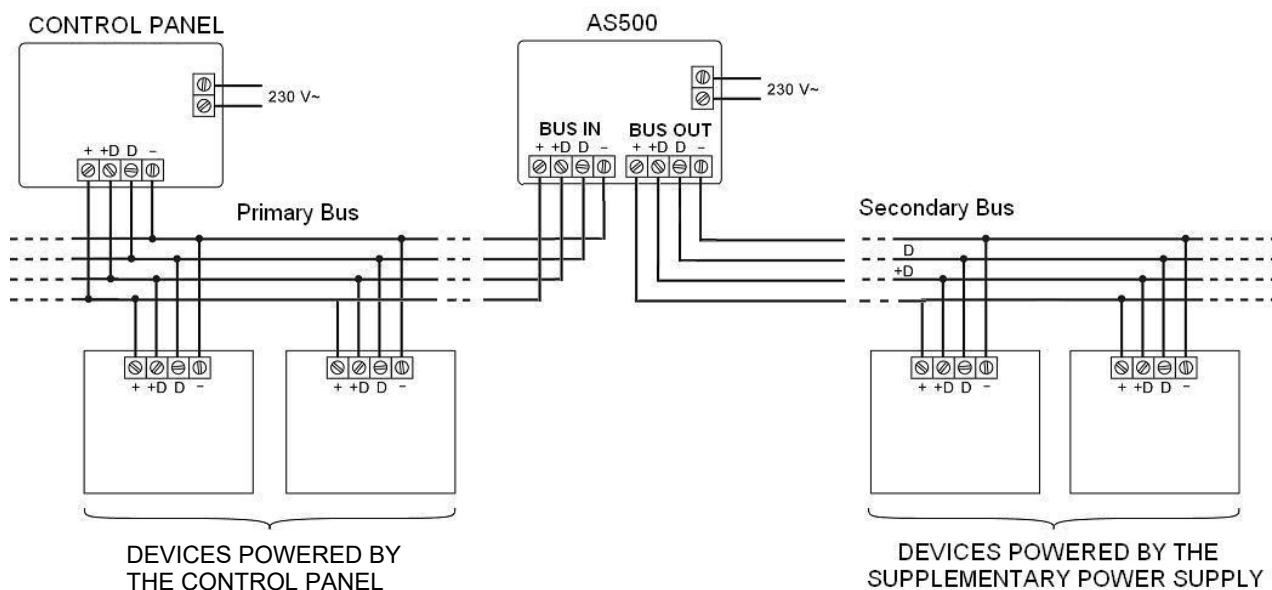


Figure 58 - Connecting the supplementary power supplies

5.12.4.1 Connection of the detectors to the expansion module of the AS500/RPT

For the connection of the inputs of the various typologies (NC – NO – to single/double balancing) see paragraph 5.12.5.

! IMPORTANT! *Do not join the earths of the BUS IN section with those of the BUS OUT section in order to guarantee a better immunity to RF disturbances.*

If a sensor must be powered by the local power supply, because the power from the control panel is insufficient, it is necessary to use relay devices to maintain galvanic isolation.

The diagram below illustrates how the connection must be made.

Otherwise, an EP508 expansion module connected to the BUS OUT can be used.

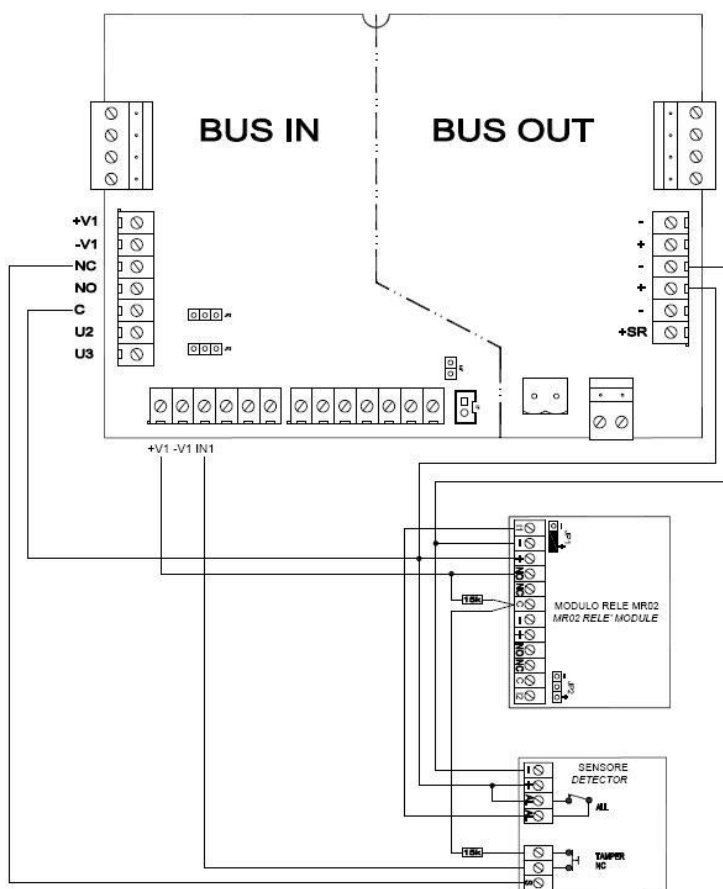


Figure 59 - Diagram of how to connect a locally powered detector

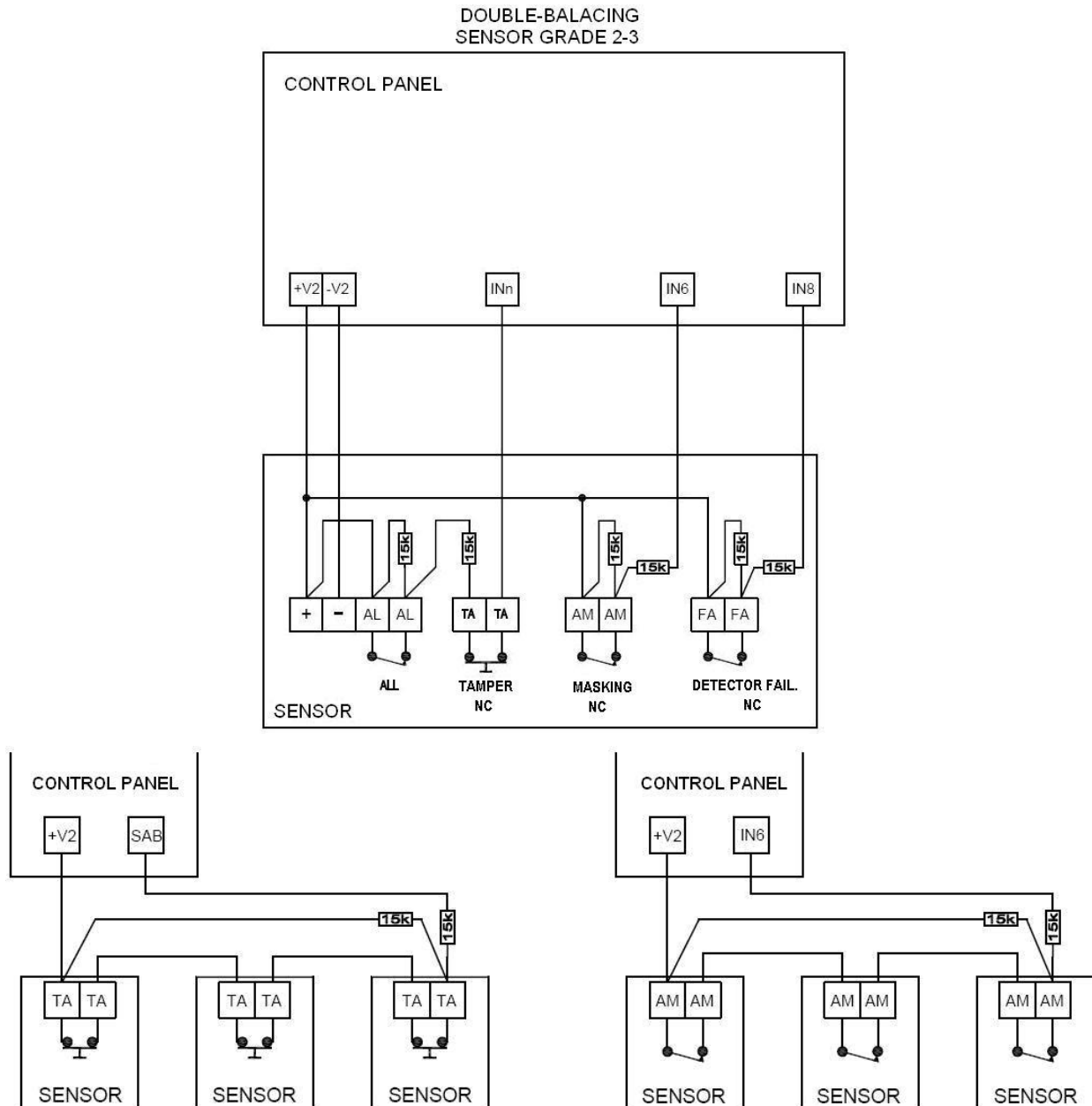
5.12.5 Connecting inputs

The type of inputs is determined by the way in which the detectors are connected. Instead, their specialization is defined with the programming.

The type for each individual input is specified during programming. It is therefore possible to create a system that includes different types of inputs.

Based on the type of connection, the inputs are divided into:

- **Double balanced:** when in stand-by, the electrical circuit connected to the input must be closed with 2 - 15 kohm resistors, tolerance 1%. Connection in conformity with EN50131.
- **NC (normally closed):** when in stand-by the electrical circuit connected to the input must be closed towards the positive.
- **Single balanced:** when in stand-by, the electrical circuit connected to the input must be closed toward the positive with a 15 kohm resistor tolerance 1%.
- **NO (normally open):** when in stand-by, the electrical circuit connected to the input must be open (it closes towards positive when in a state of alarm).
- **Shock / Roller:** this type of input is used to connect the sensors that generate quick signals (shock, roller, seismic ...). In this case connection method is necessarily type NC.



IMPORTANT! Each sensor must be powered by the device that controls it (control panel, expansion, keypad, or reader). The balancing resistors must be connected to the positive of the power supply of the same device. Connections with different power supplies may cause false alarms.

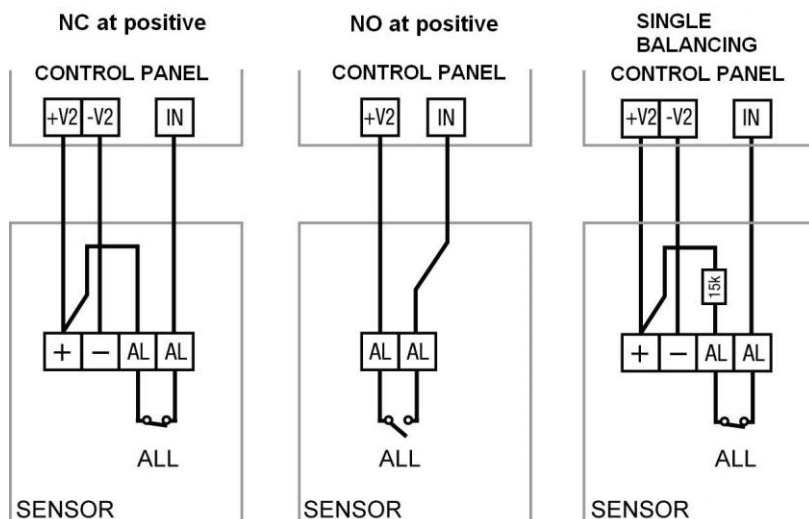
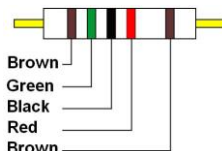


Figure 60 - Diagrams of input connections

- IMPORTANT!** In order to maintain conformity with Standard EN50131-3, the CUSTOMIZATION functions of the INPUTS present in the control panel must be modified.
- IMPORTANT!** In order to maintain conformity with Standard EN50131, the inputs must not be programmed as NORMALLY CLOSED and NORMALLY OPEN in that they would not be protected against short circuits and cut wires.
- IMPORTANT!** In order to maintain conformity with Standard EN50131, the inputs must not be programmed as SHOCK and ROLLER in that they would not be protected against short circuits.
- IMPORTANT!** Each sensor must be powered by the device that controls it (control panel, expansion, keypad, or reader). The balancing resistors must be connected to the positive of the power supply of the same device. Connections with different power supplies may cause false alarms.
It due to wiring problems this is not possible use the NC or NO type inputs.

Colour code for 15 kohm resistor, tolerance 1%



All the resistors provided with the MP500/16 are 15 kohm, tolerance 1%.

- IMPORTANT!** It is not necessary to close the unused inputs because they can be excluded via the programming.
- IMPORTANT!** The SAB inputs must also be reclosed by a 15 kohm balancing resistor.

The table below indicates the voltage intervals used in the various types of inputs.

The input status according to type				voltage present on the input terminal (*)	resistor between the input and +V2
N.C. dual balancing	N.C. single balancing	N.C.	N.O.		
TAMPER (wire short circuit)	TAMPER (wire short circuit)	STAND-BY	ALARM INPUT	11.8 ÷ 13.8 V	0 Ω
STAND-BY	STAND-BY			6.7 ÷ 7.9 V	15 kΩ
ALARM INPUT	ALARM INPUT	ALARM INPUT	STAND-BY	4.6 ÷ 5.6 V	30 kΩ
TAMPER (cut wires)				0 ÷ 0.5 V	∞ Ω

(*) with voltage between 12 V and 13.8 V.

Table 8 - Interval of voltage present at inputs

5.12.6 Connecting outputs

Alarm devices (sirens and flashing lights), signalling devices (LEDs or buzzers), or even other devices that operate automatically upon the activation of a detector can be connected to system outputs.



IMPORTANT! Never exceed the current or voltage supported by the outputs (see the technical characteristics of individual products).



IMPORTANT! Connect only operating circuits with SELV voltage.

Output specialisation (intrusion, tampering, panic, technological, etc.) is specified successively via programming. At least one output must be programmed for the signalling of alarms (siren).



IMPORTANT! In order to maintain conformity with standard EN50131-3, the CUSTOMIZATION functions of the OUTPUTS present in the control panel must not be modified.



IMPORTANT! In order to guarantee conformity with standard EN50131-3, the TAMPER output (OUTPUT No. 2) must command only sirens for indoors, in that when the system is disarmed it does not allow an external alarm to be activated in case of tampering.

Two types of output are available: a relay and an electrical one.

5.12.6.1 Relay outputs

Relay outputs have a switch contact between **C** terminal (shared contact) and **NC** terminals (contact normally closed) and **NO** (contact normally open).

5.12.6.2 Electrical outputs

Electrical outputs can be:

- "positive reference", providing +12 V
- "negative reference", providing 0 V

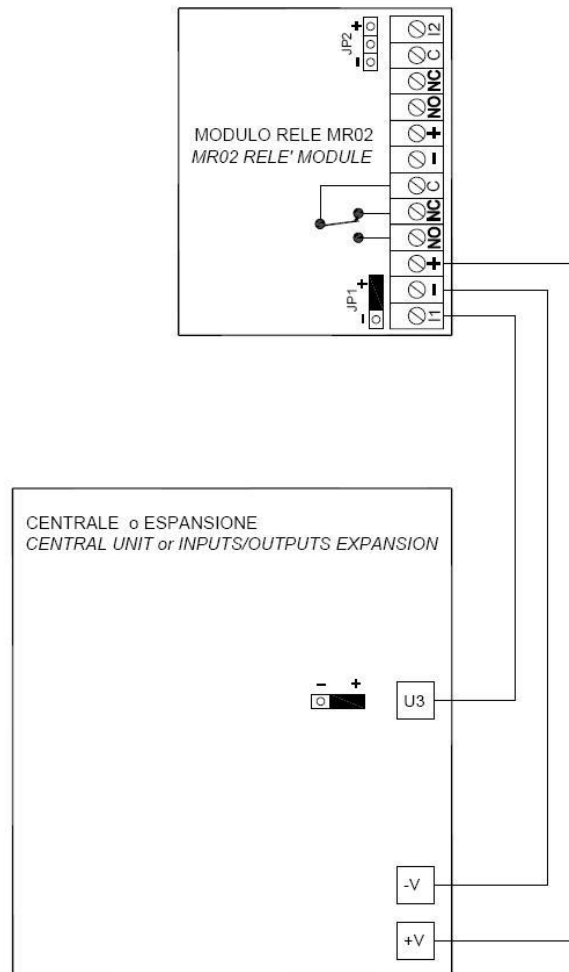
In both cases, the electrical output is "high impedance" (∞ ohm) when it is open (with no electric potential).

Electric outputs can be used to control power relays or signalling LEDs.

In the control panels, electrical outputs can be individually configured as "positive reference" or "negative reference", as detailed in *Figure 32* and *Figure 34*.

The expansion has only 2 electrical outputs available, both only "positive reference": U2 and U3.

It is possible to transform an electrical output into a relay output by using the Elcron MR02 module, equipped with two single-switch relays.



5.12.6.3 Output stand-by: N.H. and N.L.

The stand-by status of each output is programmable as either N.H. or N.L. (for more details, see the *Programming Manual*). The tables below illustrate how the various outputs appear when in stand-by and when they are on.

Outputs programmed N.H. (positive safety)		
	Stand-by	On
RELAY OUTPUT	relay energised 	relay de-energised
ELECTRICAL OUTPUT POSITIVE reference		
ELECTRICAL OUTPUT NEGATIVE reference		

Table 9 - Line diagram of output programmed N.H.

Outputs programmed N.L.		
	Stand-by	On
RELAY OUTPUT	relay de-energised 	relay energised
ELECTRICAL OUTPUT POSITIVE reference		
ELECTRICAL OUTPUT NEGATIVE reference		



Table 10 - Line diagram of output programmed N.L.

Suggestion: To reduce the consumption of electricity, it is advisable to program all the relay outputs not being used as N.L. or NOT USED.

5.12.7 Connecting the cable for KP SERVICE keypad

It is possible to connect a keypad directly to the control panel (SERVICE connector) without using the bus outputs. The purpose is to be able to program the control panel more easily, without having to use one of the keypads already installed elsewhere. To connect a keypad directly from the control panel to the SERVICE connector, connect the special cable as illustrated in the figure:



Figure 61 - Cable for KP SERVICE keypad

Keypad terminal	–	D	+ D	+
Wire colour	Black	White	Blue	Brown

The service keypad can be used only for this purpose.

IMPORTANT! By using the Service keypad, the max number of keypads which can be used in the system is decreased by one unit: it becomes 3 in the MP500/4N control panel, 7 in the MP500/16 control panel.

5.12.8 Connecting the telephone dialler

The connection of the MP500/4N or MP500/16 control panels to the telephone line is obligatory in order to conform to standard EN50131. Grade 3 and Grade 2.

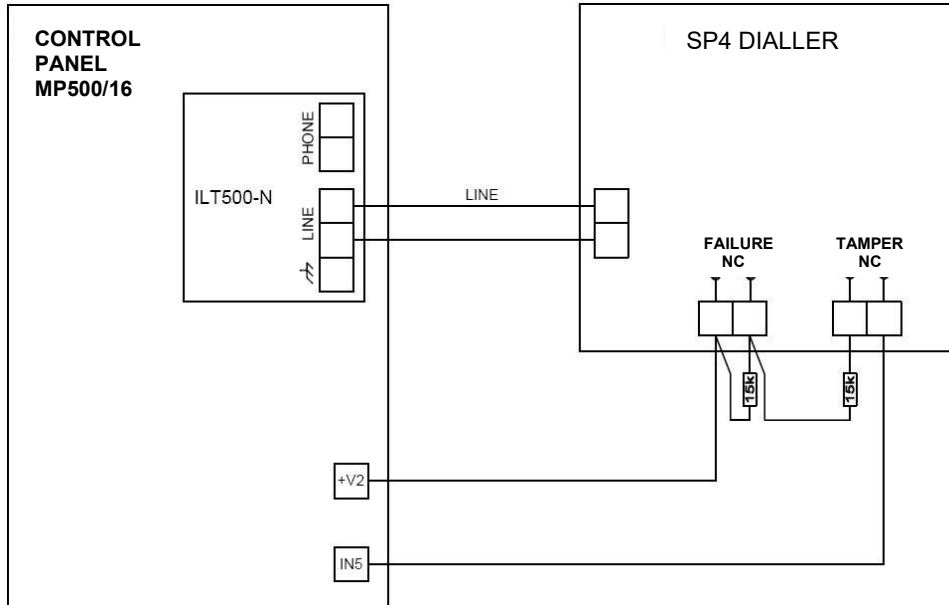
In order to conform to standard EN50131 Grade 3, it is necessary to use an external dialler, like the SP4, which is compliant EN50131 Grade 3.

In order to conform to standard EN50131 Grade 2, it is necessary to use a dialler like the SP2.

The PSTN dialler in the control panel (ILT500-N) is an SP2.

5.12.8.1 Connecting the SP4 dialler to the MP500/16 control panel

The diagram below illustrates how an SP4 dialler must be connected to the MP500/16 control panel.



Connecting the PSTN telephone line to the ILT500-N interface

The diagram below illustrates how the PSTN telephone line must be connected to the ILT500-N interface.

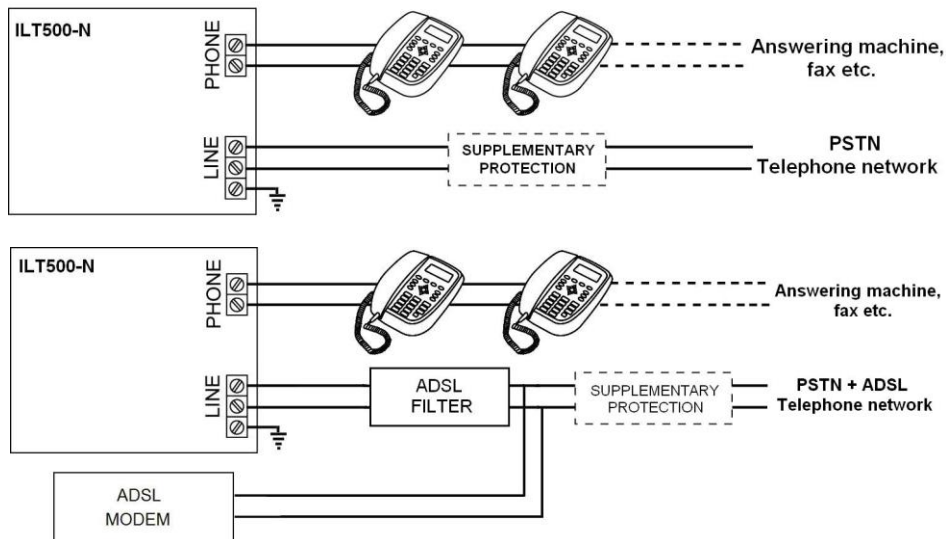


Figure 62 - Telephone connections

The control panel must be the first device connected to the incoming telephone line (all the other potential devices - fax, answering machine, and telephones - must be downstream from the control panel).

This type of connection guarantees that, if needed, the control panel can always engage the telephone line, excluding all the other devices connected if necessary.

Handle the twin telephone line carefully, as it may be live from the telephone control panel power supply.

When connecting the twin telephone line to the LA and LB terminals of the interface, it is not necessary to take polarity into account.

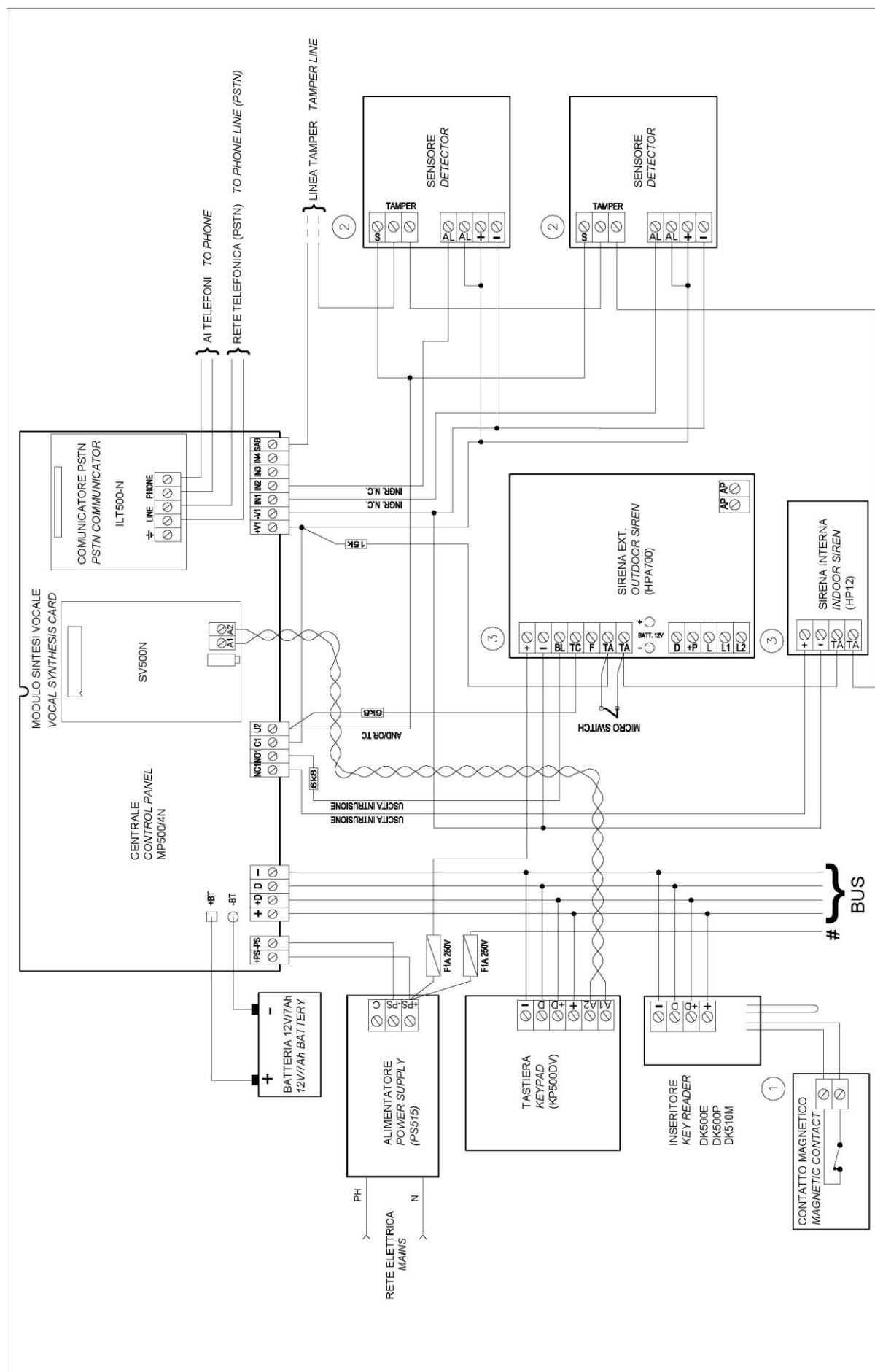
The ILT500-N board has a yellow LED to indicate if the telephone line is engaged.

The telephone interface must be grounded. The MP500/16 control panel comes with a cable for the earth that must be inserted in a Faston terminal on the wall where the box is located (C).

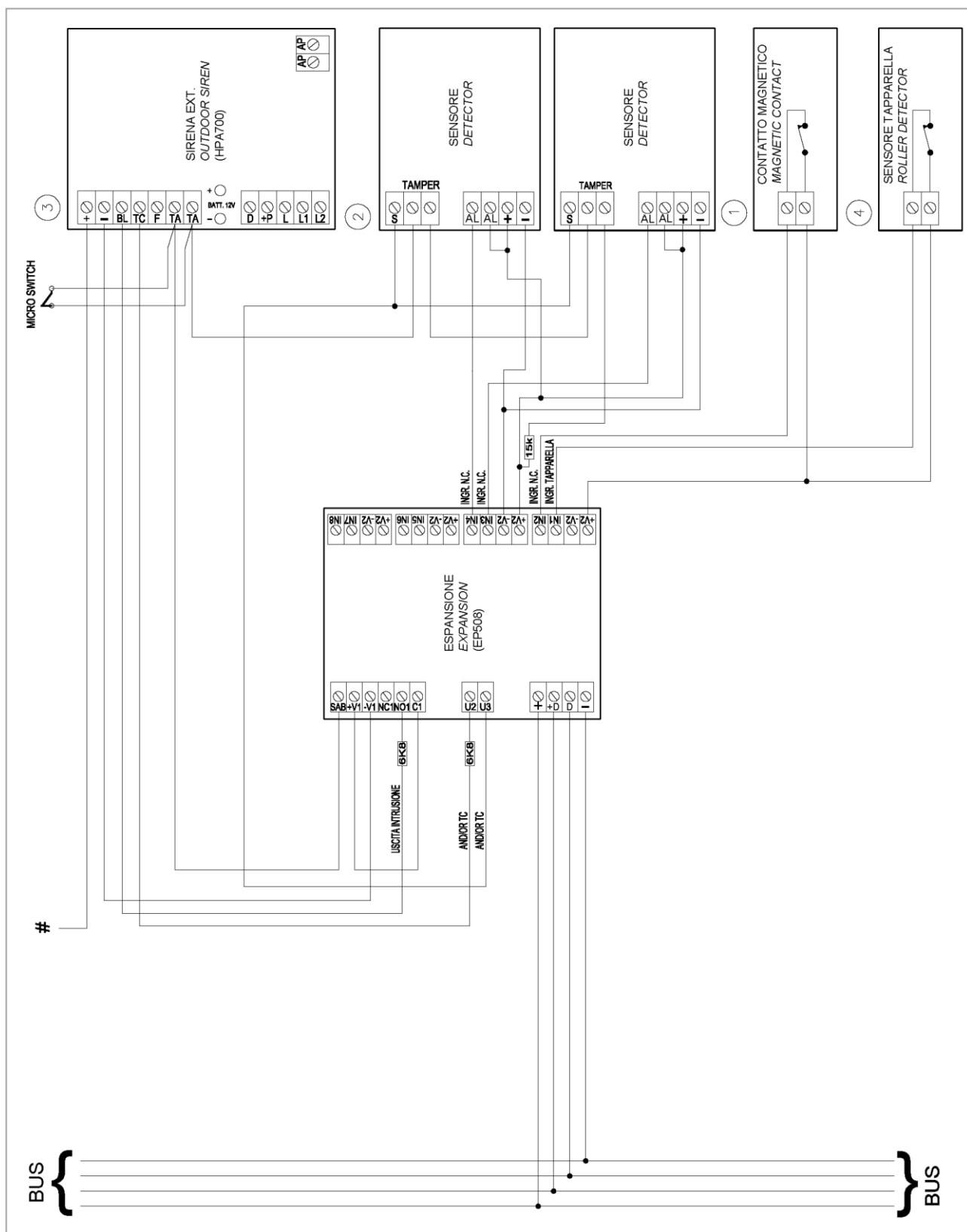
If there should be high risk of electrical shock on the telephone line in the work area, it is advisable to install supplementary protection (not provided) on upstream of the control panel on the telephone line.

5.13 EXAMPLE OF DIAGRAM WITH N.C. INPUTS MP500/4N CONTROL PANEL

EN50131

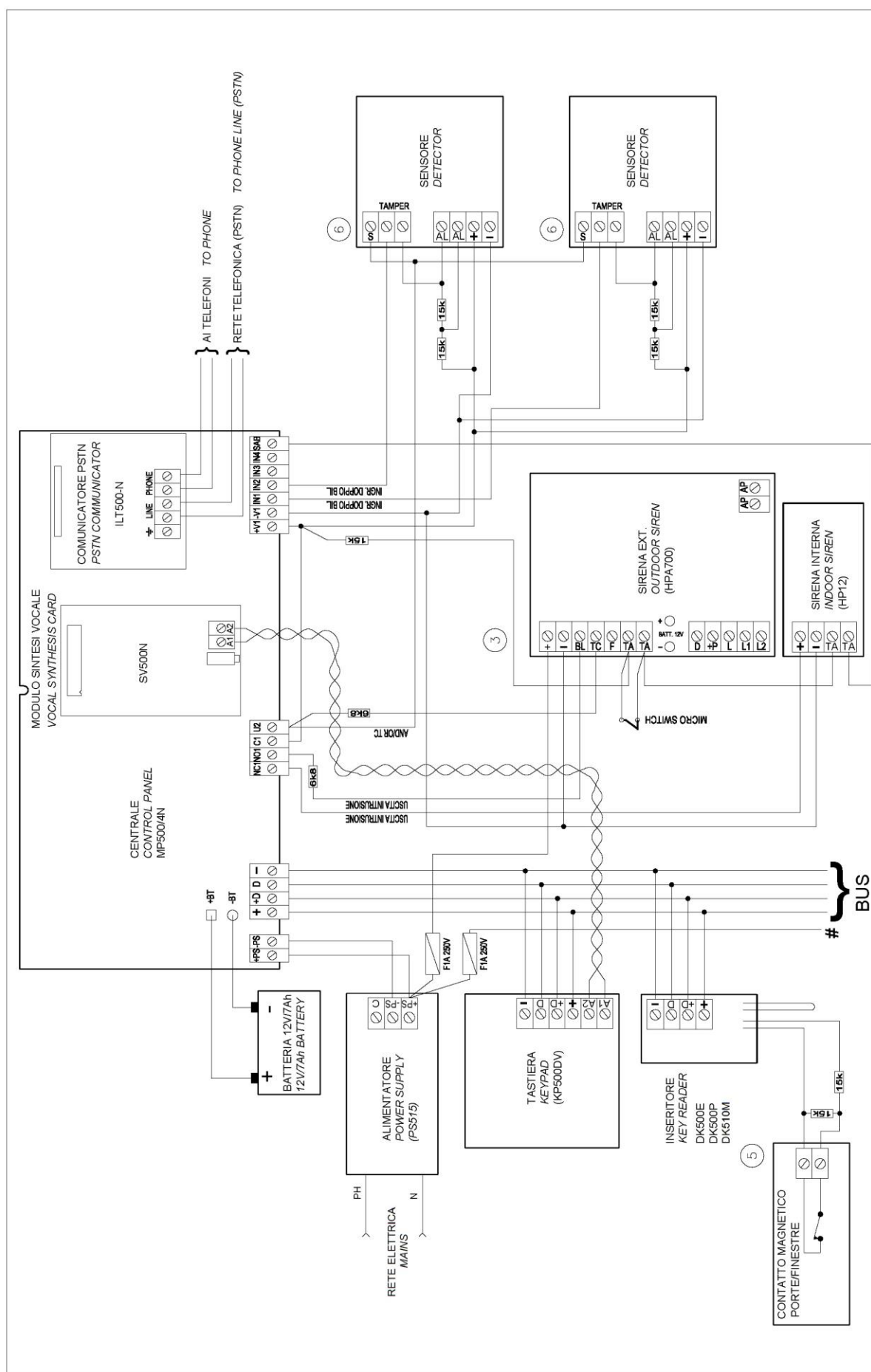


- 1) Example of connections on N.C. input
 - 2) Example of connection with alarm on N.C. input and tamper on SAB input
 - 3) Example of connection with tamper on SAB input
- IMPORTANT!** Each sensor must be powered by the device that controls it.



- 1) Example of connections on N.C. input
 2) Example of connection with alarm on N.C. input and tamper on SAB input
 3) Example of connection with tamper on SAB input
 4) Example of connection with alarm on roller input
IMPORTANT! Each sensor must be powered by the device that controls it.

5.14 EXAMPLE OF DIAGRAM WITH DOUBLE BALANCING INPUTS MP500/4N

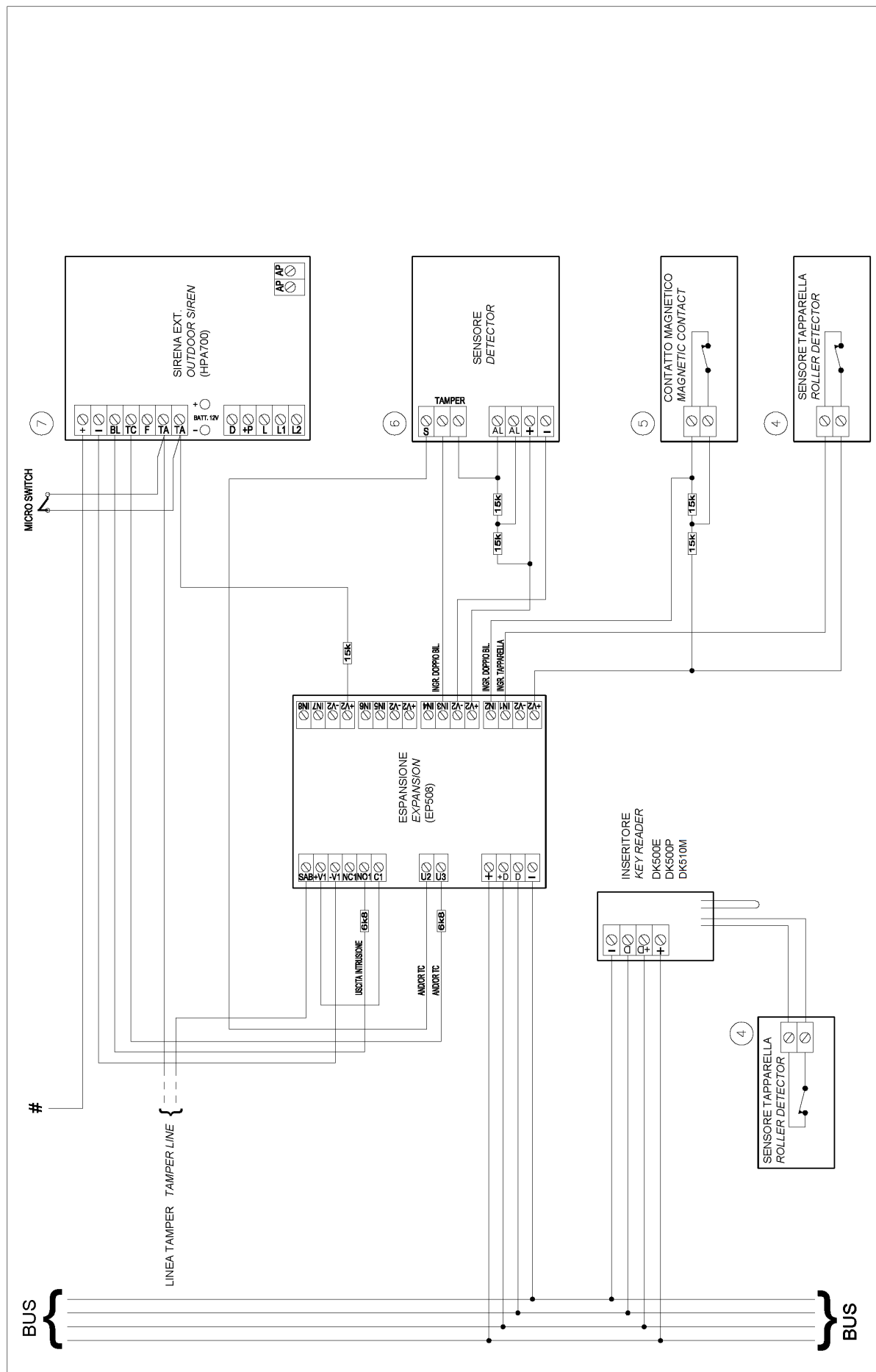


33) Example of connection with tamper on SAB input

3) Example of connection with tamper on SAB input

5) Example of connection on double BAL input

b) Example of connection with alarm and tamper on double BAL input



4) Example of connection with alarm on roller input

5) Example of connection on double BAL input

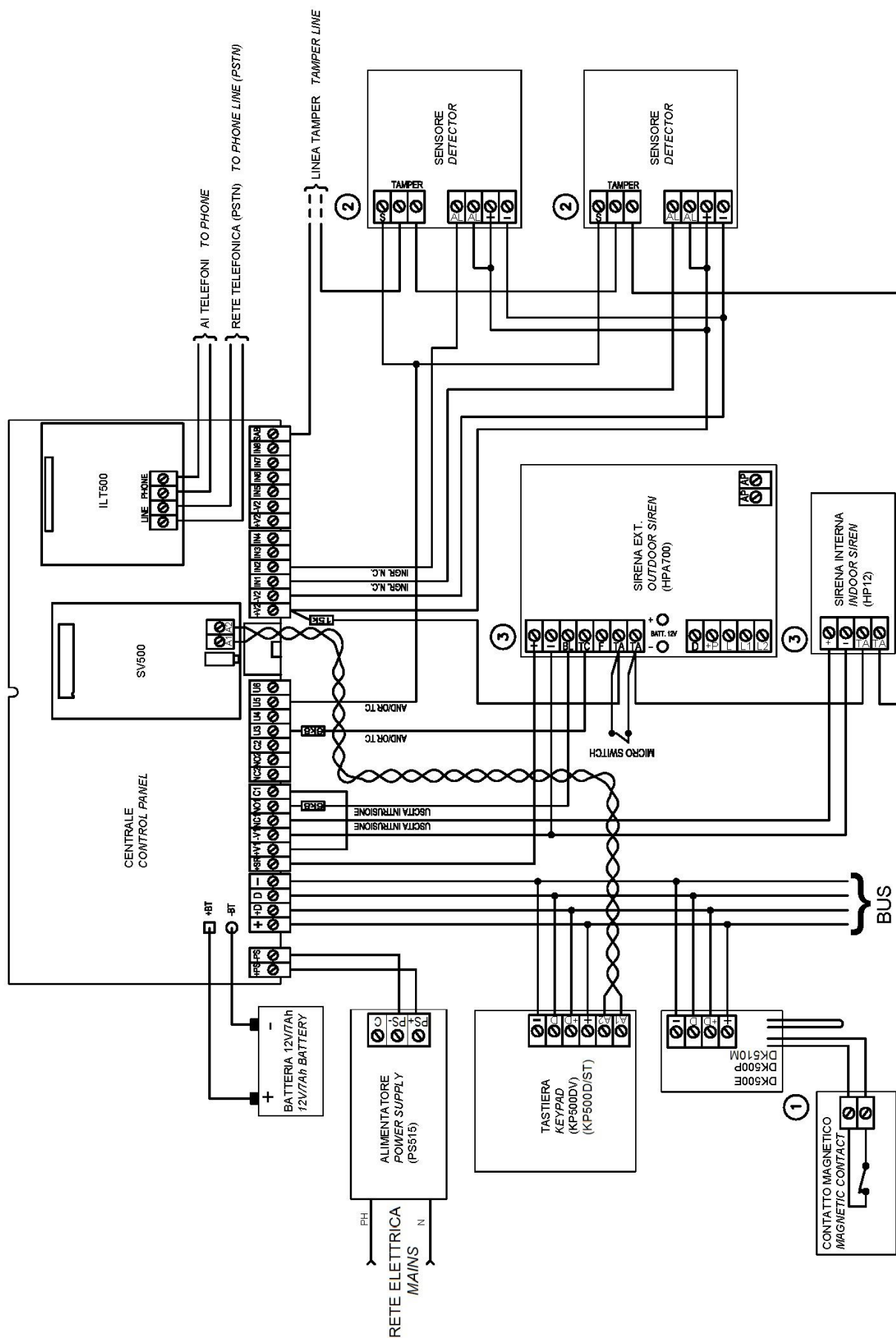
6) Example of connection with alarm and tamper on double BAL input

7) Example of connection with tamper and anti-foam module on double BAL input.

IMPORTANT! Each sensor must be powered by the device that controls it. The balancing resistors must be connected to the positive of the power supply of the same device.

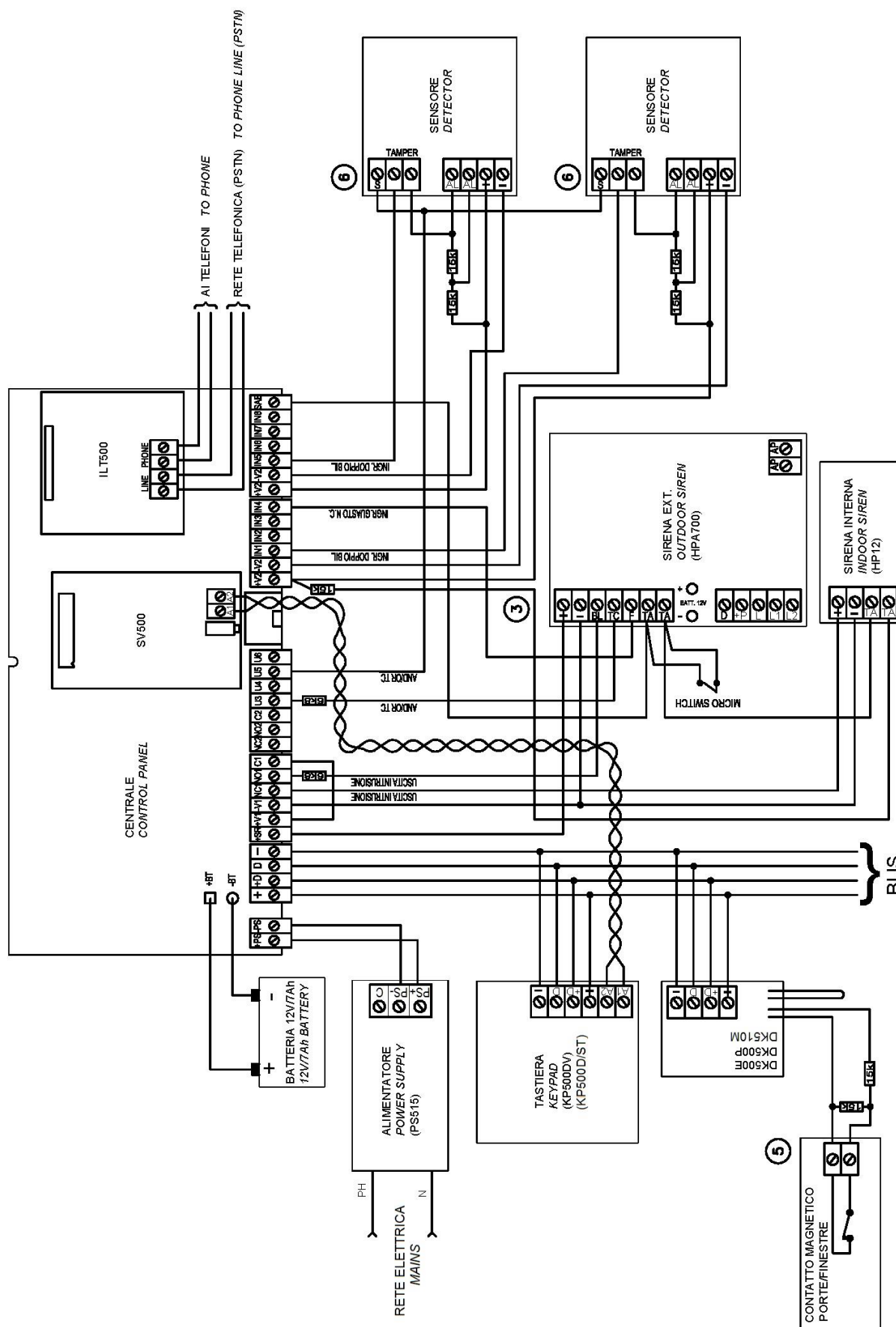
5.15 EXAMPLE OF DIAGRAM WITH NC INPUTS MP500/16

EN50131



- 1) Example of connections on N.C. input
 - 2) Example of connection with alarm on N.C. input and tamper on SAB input
 - 3) Example of connection with tamper on SAB input
- IMPORTANT!** Each sensor must be powered by the device that controls it.

5.16 EXAMPLE OF DIAGRAM WITH DOUBLE BAL. INPUTS MP500/16



- 3) Example of connection with tamper on SAB input
- 6) Example of connection with alarm and tamper on double BAL input
- IMPORTANT!** Each sensor must be powered by the device that controls it. The balancing resistors must be connected to the positive of the power supply of the same device. In order to guarantee conformity to the EN50131 standard, the U2 output, tamper alarm, must be connected to the internal siren. For Grade 3 use an SP4 dialler (see paragraph 5.12.8.1).

6 - COMMISSIONING

This chapter contains explanations for all the operations to be carried out for the commissioning of the alarm system, after having fastened all the devices and made all the connections.

Once the operations described in this chapter have been concluded, the system can then be programmed according to the instructions found in the *Programming Manual*.

6.1 SYSTEM POWER SUPPLY

Before powering up the system, it is necessary to check that the connections are all correct. Therefore, power up the system according to the sequence below.

1. If there are supplementary power supply units, power them up before connecting the control panel.
2. Insert the battery in the dedicated compartment of the control panel and connect the Faston connectors to the relative terminals: red "+", black "-", and then turn on mains power supply. The rated voltage to the battery terminals once charged reaches 13.8 V. The power supply does not need calibration.

IMPORTANT! The control panel has a battery control circuit. If the battery is not connected to the terminals of the connection cables, (red and black Faston) there is no power.

3. On the control panel, the POWER LED is on (indicating the presence of current). After a few seconds, when the start-up routine has been completed and the control panel is fully operative, the RUN LED begins to flash slowly (approximately one flash every 2 seconds).
4. In the other devices, when they are powered, the yellow LED next to the programming button will flash for 10 seconds (the buzzer in the keypad will also sound). After 10 seconds have passed, this LED begins to flash slowly (approximately once every 2 seconds) until the device is not acquired, and will then shut off. For the acquisition procedure, see paragraph 6.2 ACQUISITION OF BUS DEVICES. If the device results already acquired and configured, the LED turns off after 10 seconds.
5. Check that voltages arriving to the devices in the various points of the system are in conformity with the indications described in paragraph 4.2.2 Sizing of the power supply cable

IMPORTANT! To turn off the system completely, follow the procedure indicated in paragraph 7.11 TURNING OFF THE ENTIRE SYSTEM.

6.1.1 RUN LED Indications

The RUN LEDs provide the following information.

Warning	LED	Description	Meaning	When
Normal operation		Blink every 2 seconds	Control panel without peripheral devices registered	The blinking continues until the first keypad is acquired
		Slow blinking	Microprocessor in run and nothing else to signal	Always present when the control panel functions normally
Fault		Fast blinking	No battery or connection cables inverted	The blinking continues until the battery is connected or the right cables are inserted
		Steady on with brief interruption every 2 seconds	Irreversible failure	

6.2 ACQUISITION OF BUS DEVICES

6.2.1 Position of the programming buttons

For the acquisition of the bus devices, use their programming buttons (PROG). The images below demonstrate where these buttons are positioned.

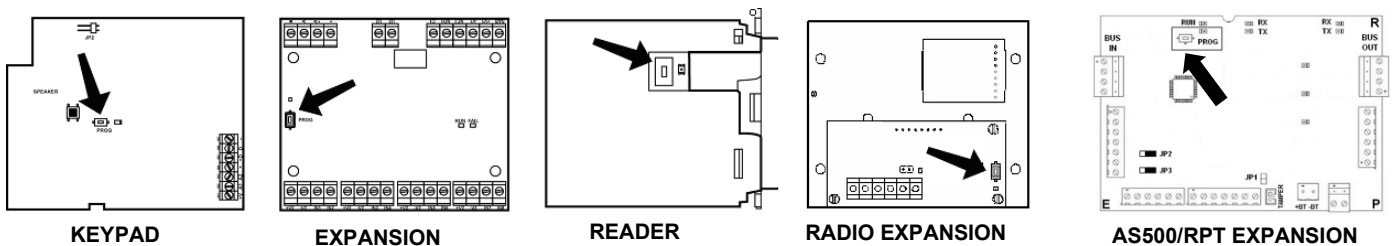


Figure 63 - Position of the programming buttons

To acquire a KP500DP/N or KP500D/ST touch screen keypad, it is sufficient to press the **F4** key when the following message appears on the display.



Figure 64 - Message of KP500DP/N - KP500D/ST keypad acquisition

6.2.2 Procedure for acquiring bus devices

 **IMPORTANT!** The instructions below assume that the devices have not yet been acquired. Otherwise, see Chapter 7 - *MAINTENANCE*.

To acquire the various devices on the system bus, follow the instructions below:

1. Select the keypad to be used to acquire system devices from among the keypads present in the system. It is also possible to use the service keypad (see paragraph 6.3 *USING THE SERVICE KEYPAD*).
2. Press the programming button (PROG) on the keypad display (if there is a KP500DP/N or KP500D/ST keypad, press **F4**). The control panel registers it by assigning the "KP01" address. If it is a service keypad, it will be assigned the address "KP08".
3. The «MAINTENANCE» / «LINGUA-LANGUAGE» menu will appear on the keypad display. If the language is to be changed, press the **OK** button, otherwise press the **▼** key until «MAINTENANCE» / «ACQUIRE» appears, press **OK** again and go on to point 7.
4. «LINGUA-LANGUAGE» / «KP01:KP 01» appears on the display (second line). KP01 is the first keypad of the system, or the one that was just acquired. If the service keypad is being used, the message «KP08:KP 08» will appear. Press the **OK** button.
5. «ITALIANO» will appear on the display. Use the **▼▲** keys to select the language desired and confirm the selection by pressing the **OK** key.
6. «Download in progress >>>>...» will appear on the display. When the download of the new language is complete, the message «DOWNLOAD OK» will appear. Press **OK** and then **ESC**.

 **IMPORTANT!** During the download, the power supply must absolutely not be disconnected from the keypad!

7. "ACQUISITION IN PROGRESS..." will appear on the display and the control panel is ready to acquire other devices.
8. Proceed with the acquisition of the other devices by pressing the programming button of each of them. The yellow LED located next to the button of the device will turn off as soon as it is acquired. Each time a new device is acquired, the keypad emits 3 beeps and the device type will appear on the display (KP = keypad; EP = expansion; DK = reader; ER = radio expansion; AS = POWER/S.) with the address assigned to it. Once the acquisition of all the devices is complete, press **ESC** to exit from the menu.

Now it is possible to proceed with the system configuration as illustrated in the *Programming Manual*.

 **IMPORTANT!** The addresses are assigned progressively and according to family of belonging; it is not necessary to follow a pre-established order. If the operator wants the device addresses to follow certain logic, they must be acquired in that order.

Example:

In a system with two keypads, one expansion, two readers, and a radio expansion, there will be the following combination:

- KP01
- KP02
- EP01
- DK01
- DK02
- ER01
- AS01

 **Suggestion:** Take note of the address of each individual device on the labels provided with the control panel.

6.3 USING THE SERVICE KEYPAD

For the system acquisition and programming operations, it is possible to use a keypad connected directly to the SERVICE connector of the control panel via the specific cable. For more details, see paragraph 5.12.7 *Connecting the cable for KP SERVICE keypad*.

The service keypad must be acquired according to the method described above. The system automatically assigns it the address n. 08. At the end of the operation, it is possible to disconnect this keypad without generating tamper and therefore without having to delete it. When inserted again, it does not require another acquisition and the keypad will be immediately operative.

 **IMPORTANT!** Using the service keypad precludes the possibility of having 8 keypads on the system (as address 8 is already occupied, it will be possible to connect a maximum of 7 keypads).

7 - MAINTENANCE

This paragraph describes the procedure to be followed to carry out system maintenance: add new devices, replace a malfunctioning device, eliminate a device, restore default settings to devices, and troubleshooting, etc.

For the navigation in the menu and to know the functions offered by the Maintenance submenu, please see the *Programming Manual*.

7.1 MAINTENANCE PROCEDURE

The maintenance procedure is useful each time it is necessary to intervene on the system and therefore open the tamper of the control panel and any device, or disconnect peripheral devices, without creating tamper events. In this way no outputs of any type of alarm is activated and the telephone transmitter will be inhibited to outgoing calls, with the exception of service calls (Tests for Battery low, Lack of power, SIM card expiry...). The Maintenance event, if programmed, can be send via the Telephone transmitter to the numbers with the Numeric and Modem type of transmission.

To enter the maintenance procedure, follow the instructions below:

1. Disarm the system completely.
2. With the Master code (default 111111) enable the Installer code; then exit the Master menu.
3. Insert the Installer code (default 000000) and press the **OK** button followed by **MENU**. The system enters the maintenance mode.
4. To confirm that system has entered maintenance mode, the LED on the keypads lights up.

If the control panel tamper is opened under these conditions, the system remains in maintenance phase even if the operator exits from the menu; indeed, the "Maintenance" LED remains on.

This is useful to be able to continue operating on the keypad with the system in maintenance status, for example to be able use the LED to check "Sabotage" and "Inputs open", the status of the various inputs.

To exit the maintenance status and return to normal operating conditions, it is first necessary to check that there are no sabotage situations still present on the various devices (tamper and H24 SAB inputs closed, serial Bus correctly connected), then reclose the control panel as the last step.

As soon as the tamper of the control panel recloses, the "Maintenance" LED on the keypad turns off and, from this point onward, each tamper will be signalled again as planned.

7.2 ADDITION AND ACQUISITION OF A NEW DEVICE BUS

To acquire a new bus device, like a keypad or reader, follow the instructions below:

1. Turn off the entire system (see paragraph 7.11 *Turning off the entire system*).
2. Connect the new device to the bus.
3. Then power up the system again. The yellow LED of the new device flashes slowly for about 10 second before changing the speed of flashing.
4. Select the item «MAINTENANCE» / «ACQUIRE» in the Installer menu and confirm with **OK**.
5. "ACQUISITION IN PROGRESS..." will appear on the display; press the programming button of the device to acquire it; its yellow LED will turn off.
6. Complete installation of the new device and exit the maintenance menu.
7. Configure the new device via programming (see the *Programming Manual*).

7.3 REPLACING A BUS DEVICE

To replace a bus device that has already been acquired, follow the instructions below:

1. Delete the device to be replaced (see paragraph 7.5 *DELETING A BUS DEVICE*).
2. Turn off the entire system (see paragraph 7.11 *TURNING OFF THE ENTIRE SYSTEM*).
3. Disconnect the old device and connect the new one to the bus.
4. Then power up the system again. The yellow LED of the new device flashes slowly for about 10 second before changing the speed of flashing.
5. Select the item «MAINTENANCE» / «ACQUIRE» in the Installer menu and confirm with **OK**.
6. "ACQUISITION IN PROGRESS..." will appear on the display; press the programming button of the device to acquire it; its yellow LED will turn off. The control panel assigns the same address as the device deleted.
7. Complete installation of the new device and exit the maintenance menu.
8. Configure the new device via programming (see the *Programming Manual*) with the same parameters as the device deleted.



IMPORTANT! If for any reason it should become necessary to delete any bus device and later reacquire it, the power supply to the system or the bus device (reset) must be disconnected before carrying out any reacquisition procedure.

7.4 IDENTIFYING A BUS DEVICE

7.4.1 Interrogating a bus device

In order to find the address of a device already acquired on the bus, following the instructions below:

1. Activate the maintenance mode (see paragraph 7.1 *MAINTENANCE PROCEDURE*) to avoid generating tamper events.
2. Press and release the programming button of the device whose address you want to know.
3. The yellow LED of the device will emit a series of flashes equal to the number of its address.

7.4.2 Searching for a device

To identify a specific device on the bus, follow the instructions below:

1. Activate the maintenance mode (see paragraph 7.1 *MAINTENANCE PROCEDURE*) to avoid generating tamper events.
2. Select «MAINTENANCE» / «SHOW ADDRESSES» from the Installer menu.
3. Then select the type of device to be identified in the submenu and select its address from inside the list it proposes; confirm by pressing **OK**. The message “IN PROGRESS...” appears.
4. Then look at all the devices installed: the one with the address requested will have the yellow acquisition LED flashing quickly and is valid for wired, radio, and AS500/RPT supplementary power supply expansions, while on the readers, the LEDs presents will flash quickly and, in the device address and relative software version will appear in the keypad display.
5. Press **ESC** to conclude the search.



IMPORTANT! It is possible to interrogate and/or search exclusively devices connected to the data Bus.

7.5 DELETING A BUS DEVICE

To remove an existing device from the bus, for example a keypad or reader, simply delete its address by following the instructions below:

1. Activate the Maintenance mode (see paragraph 7.1 *MAINTENANCE PROCEDURE*).
2. Select «MAINTENANCE» / «DELETE» from the Installer menu.
3. Select the type of device to be deleted and select its number from within the list proposed. The device is no longer considered connected to the control panel and its memory will be restored to default values.
4. Turn off the entire system (see paragraph 7.11 *TURNING OFF THE ENTIRE SYSTEM*).
5. Physically disconnect the device from the bus.
6. Then power up the system again.

To restore the device removed to default parameters in order to reacquire it again, it is necessary to reset it as described in paragraph 7.9.5 *Resetting hardware to factory settings*.



IMPORTANT! The control panel automatically saves at least one keypad.

If a device must be replaced, use a keypad to delete the device, proceed with the removal and the connection of the new device, and finally proceed with the acquisition procedure.

Otherwise, the new device can be pre-acquired with the same address as the one to be replaced by using another control panel and positioning it directly in the system.

7.5.1 Deleting a radio expansion

The procedure to delete a radio expansion is the same as the one to remove any bus device, as described in the previous paragraph.

However, as it takes a longer time, it is useful to highlight some differences:

1. Select «MAINTENANCE» / «DELETE» from the Installer menu.
2. Select the «RADIO EXP.» submenu and select the radio expansion from among those available.
The yellow LED “B” (see dedicated manual) of the device flashes quickly for 40 seconds; the delete operation is concluded only when the LED stops flashing and remains on steadily.
3. Turn the system off (see paragraph 7.11 *TURNING OFF THE ENTIRE SYSTEM*).
4. Physically disconnect the device from the Bus.
5. Then power up the system again.



IMPORTANT! When deleting a radio expansion, all the radio devices associated with it are automatically deleted. At the same time, the “Radio Devices” menu will no longer be displayed on the system keypads.

As soon as the control panel acquires the first radio expansion (see paragraph 6.2 ACQUISITION OF BUS DEVICES), the specific menu to acquire and configure radio devices will appear on the system keypads. Below is a diagram of the navigation flow of the “Radio Devices” menu.

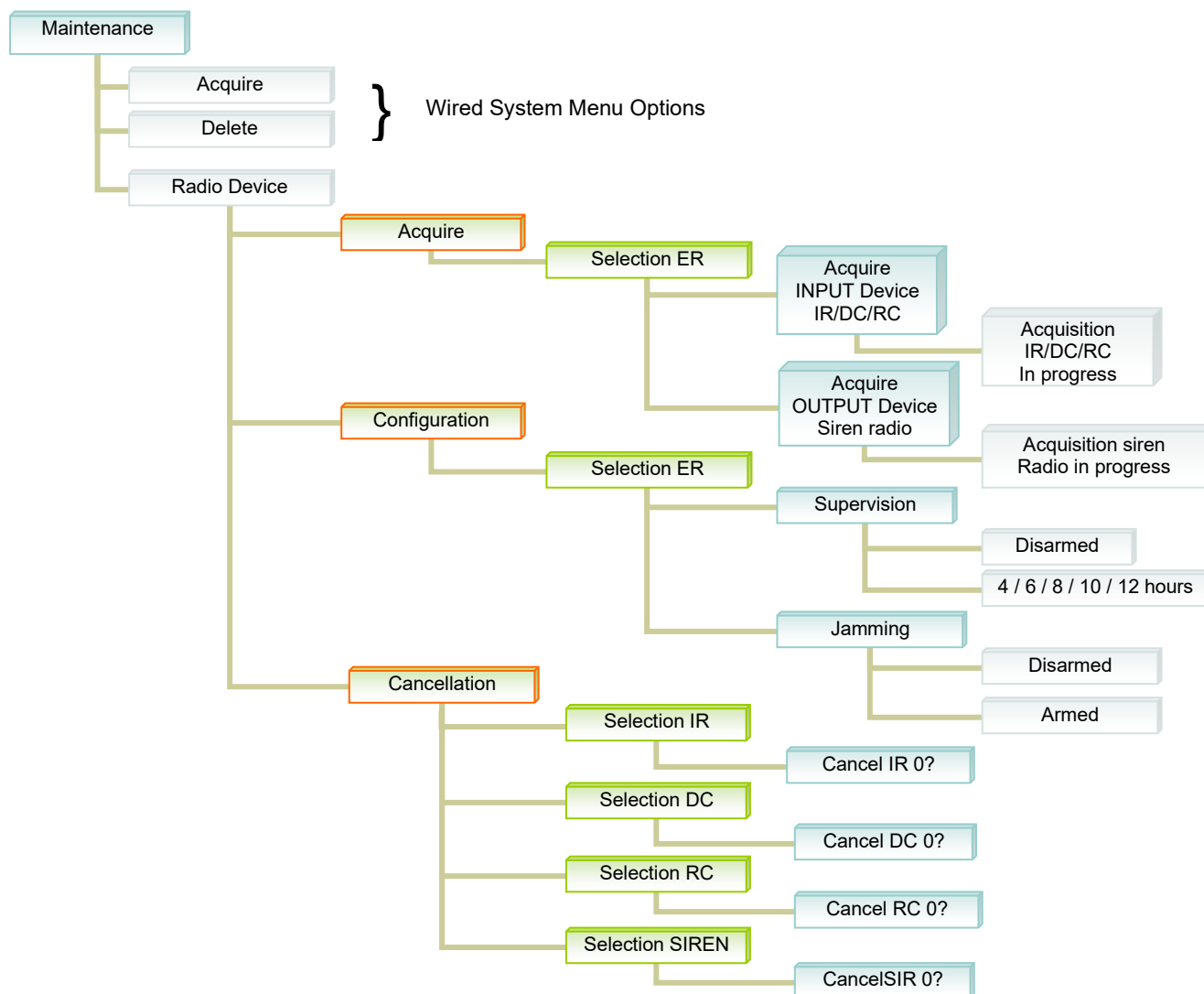


Figure 65 - Radio devices menu diagram

After entering «Radio devices» → «Acquire» menu, the control panel and the radio expansion are ready to acquire devices.

When the acquisition request arrives from a radio device, the control panel proceeds to acquire it and the type of radio device and its address appear on the keypad (for example: “IR01”).

If it has acquired a number of radio devices equal to the maximum, the control panel will not allow the acquisition of others. In this specific case, the keypad in acquisition will continue to show the date of the last device acquired and emit an error signal (a long beep).



Suggestion: Device acquisition is progressive. Therefore, if they are to be matched to inputs and outputs in a certain order, the precise sequence must be defined before carrying out the acquisition procedure.



IMPORTANT! If there are two radio expansions, the devices must be acquired separately. The same device **must not be** acquired on both expansions.

7.6.1 Radio connection test

The radio expansion makes it possible to evaluate the quality of the radio connection between the peripheral devices subject to supervision through an integrated test that provides an indication correlated to the power of the signal measured by each individual device.

The diagram below illustrates the operations to be carried out to conduct the test.

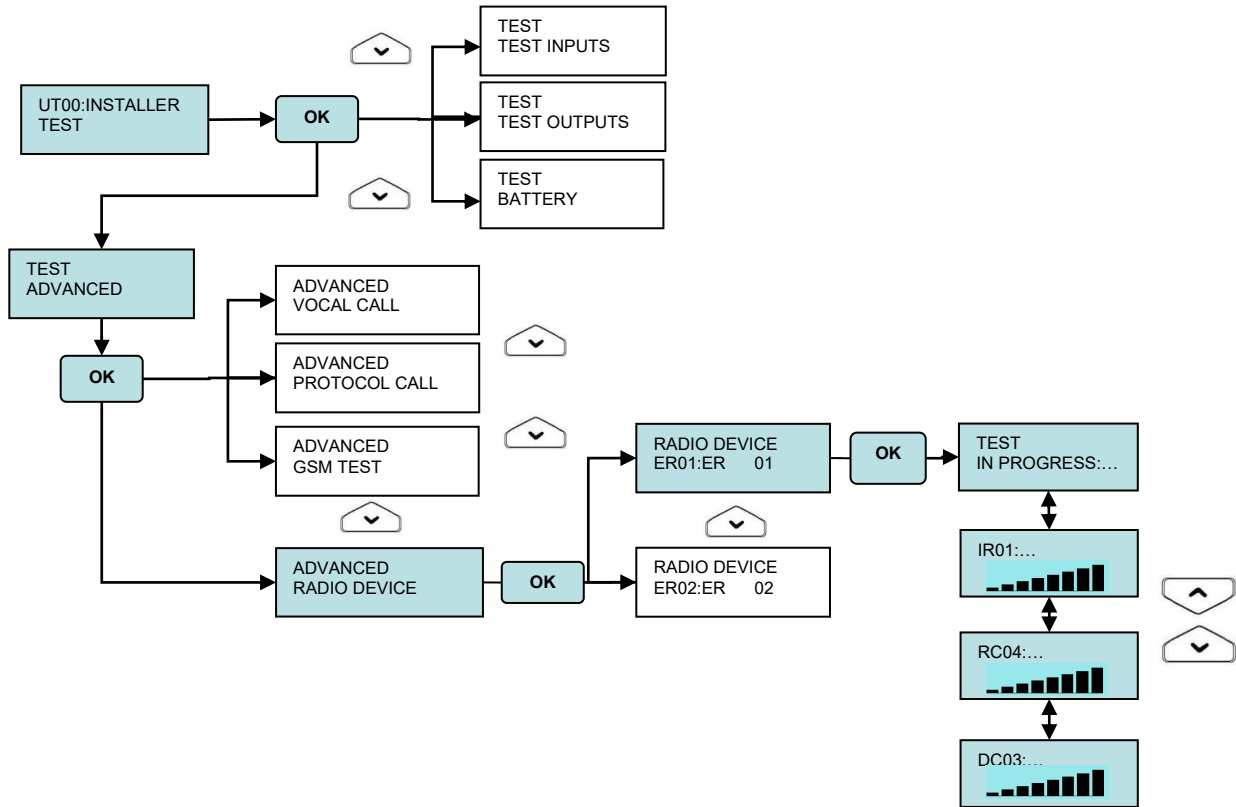


Figure 66 - Radio connection test menu

To control that the various system devices are able to communicate with the control panel, follow the instructions below:

1. Position each system device in the definitive final position or nearby, without securing it.
All the devices must be powered and already acquired.
2. Position the control panel in the definitive final position.
3. Enter the "Master" or "Installer" menu to access the «**TEST**» / «**ADVANCED**» / «**RADIO DEVICES**» menu and select the radio expansion to be tested: es. ER01: ER 01.
4. The message «ARE YOU SURE?» appears on the display.
5. Start the automatic test procedure by pressing the **OK** key. The message «TEST: IN PROGRESS...» will appear on the display.
6. Press the programming key on all the radio devices to be installed, in order to activate an immediate connection with the radio expansion where they were acquired.
7. For each device that makes contact with the expansion, the keypad emits a brief beep and the test result appears on the display.
8. When completed it is possible to visualize all the devices tested on the display, using the arrow keys; each device is identified by: device type, address, and test result.
9. The table below illustrates what the test results might be:

	Excellent connection
	Good connection
	Sufficient connection
	Insufficient connection

Use the ▼▲ key to see the test result for the various devices: if the result for all the devices is between "SUFFICIENT" and "EXCELLENT", the position of the devices is adequate.

10. If the test result of any device is "INSUFFICIENT", it is necessary to move these devices to a more favourable position in relation to the control panel press **OK** and repeat the test from point 5.

Note: When it is not possible to obtain an acceptable signal level by only moving the devices (the excessive fading of the signal, radio dead zones, ...), it is necessary to identify a different site for the radio expansion.
Once the radio expansion has been moved, press the **OK** key and repeat the test from point 5.

11. In case of doubt on the functioning of a device, position it temporarily near the control panel (about one metre) and repeat the test. If the result for the device in question is "EXCELLENT", it is functioning correctly; otherwise, it could be broken or lacking power.

12. Exit the menu by pressing the **ESC** key more than once.

7.7 CONFIGURING RADIO PARAMETERS

To modify the default configuration of the radio parameters of a single radio expansion:

- Enter the menu: Maintenance → Radio devices → Configuration → Radio expansion Selection
- Modify the Supervision/Jamming configuration according to one's needs.

Supervision	Functional notes
Disabled	The radio expansion does not control the presence or absence of radio devices belonging to it.
4 hours	The radio expansion controls the presence of radio devices belonging to it, considering the absence of communication as the pre-selected time interval.
6 hours	
8 hours	
10 hours	
12 hours	

Jamming	Functional notes
Disabled	The radio expansion does not control the occupation of the radio band by devices foreign to the system.
Enabled	The radio expansion does control the occupation of the radio band by devices foreign to the system.

7.8 DELETING A RADIO DEVICE

To delete a radio associated with a radio expansion, follow the instructions below:

1. Use the arrows to enter the «**Maintenance**» → «**Radio devices**» → «**Delete**» menu; confirm each selection by pressing **OK**.
2. Select the radio expansion to be deleted.
3. Continue with the function keys and select the type of device to be deleted.
4. Select the device to be deleted. «**Select IR 01**» o «**Select IR 02**», etc.
5. For greater security, before deleting the device, the system requests further confirmation by visualizing the message: «**Are you sure? »**; press the **OK** key to start the deletion.
6. The message «**Deletion in progress...**» will appear on the display.
7. Once the device has been deleted, the system will return to the menu at point 2.
To delete other radio devices, repeat the process by following points 2 to 5.
8. Once the deletion of radio devices is complete, press the **ESC** key on the keypad to exit the menu.

7.9 RESETTING FACTORY SETTINGS

The table below indicates the various possibilities for resetting the control panel and system devices to default values as needed. The default values can be found in the *Programming Manual*.

	Partial reset	Global reset	Reset Installer, Master, and User codes	Reset installer hardware code	Reset hardware factory settings	Reset devices
PARAMETERS IN THE CONTROL PANEL MEMORY						
Control panel programming	■	■			■	
Device addresses		■			■	
Event log		■			■	
Installer Code		■	■	■	■	
Tech. Manager Code		■	■	■	■	
Master Code		■	■		■	
User codes		■	■		■	
Keys		■			■	
PARAMETERS IN THE DEVICE MEMORIES						
Number of the device		■				■
Device parameters	■	■				■

Table 11 - Variations of the configuration with reset



IMPORTANT! The reset operations are irreversible and therefore once carried out, it become necessary to reacquire and/or reprogram any devices involved.

The programming of the control panel consists in the configuration and the naming of inputs, outputs, times and partitions, the timing programmer, the parameters, and the PSTN/GSM telephone numbers.

The event log can also be deleted from the Installer menu at «DIAGNOSE LOG». For more details, please see the *Programming Manual*.

The keys can also be deleted individually from the Installer menu or from the Technical Manager at «SETTINGS». For more details, please see the *Programming Manual*.

To restore a keypad to Italian, it is necessary to access «MAINTENANCE» / «LINGUA-LANGUAGE» in the Installer menu.

The sequence is: <<Installer Code>> → **OK** → **Menu** → **▲** → **OK** → **Maintenance OK**

« LINGUA-LANGUAGE » «KP01:KP 01» will appear on the display. Select the number of the key that you wish to reset to Italian and press **OK**.

Use the **▼ ▲** keys to scroll the languages until you find « ITALIANO » and confirm your choice by pressing the **OK** key.

«Download in progress >>>>...» will appear on the display. when the download of the new language is complete, the message «DOWNLOAD OK» will appear.



IMPORTANT! For the Vocal Synthesis board it is not possible to restore the message to default.

7.9.1 Partial reset

Reset the control panel programming to default.

The following are not deleted: the Diagnose Log., the codes, the keys, and the device acquisitions.

To carry out the partial reset:

1. Select the item «**MAINTENANCE**» / «**PARTIAL RESET**» in the Installer menu and confirm with **OK**.
2. When asked «**ARE YOU SURE?**» press **OK** to confirm or **ESC** to cancel the operation.
3. The message «**PARTIAL RESET**» «**IN PROGRESS...**» will appear when **OK** is pressed and the buzzer will sound. «**MAINTENANCE**» «**PARTIAL RESET**» will appear then the operation is concluded.
4. At this point, the reprogramming of the system can be started.

7.9.2 Global reset

Resets the control panel programming and all the devices connected to the system data BUS to default. It is therefore necessary, following this command, to reacquire all the devices (keypads, expansions, readers, radio expansions, etc.). In reference to the radio expansion it is also necessary to reacquire all the radio devices associated with it.



IMPORTANT! For the Vocal Synthesis board it is not possible to restore the message to default.



IMPORTANT! Following the Global reset command, it is necessary to carry out the local reset of all the radio sirens of the system, and then reacquire them.

To carry out the Global reset:

1. Select the item «**MAINTENANCE**» / «**GLOBAL RESET**» in the Installer menu and confirm with **OK**.
2. When asked «**ARE YOU SURE?**» press **OK** to confirm or **ESC** to cancel the operation.
3. The message «**IN PROGRESS...**» will appear when **OK** is pressed and the buzzer will sound.
4. At the end of the operation, a series of full stops will appear on the display. Turn off the system and restart from *Chapter 6 - COMMISSIONING*.

7.9.3 Resetting Installer, Tech. Manager, Master and User codes

To reset the user codes, the Master code, the Installer Code or or Tech. Manager Code to their default value, access «**SETTINGS**» / «**USERS**» / «**DEFAULT CODE**», from the Installer menu, select the code desired and confirm with **OK**.

7.9.4 Resetting hardware installer code and Tech. Manager Code

To reset the Installer code and Tech. Manager Code to its default value if you don't know the Master Code, following the instructions below:

1. Turn off the control panel completely (see paragraph 7.11 *TURNING OFF THE ENTIRE SYSTEM*)
2. Set the Dip switch to 2 to ON.
3. Reconnect the control panel to the power supply, during the initialisation phase the Installer code will be set to its default value (000000) and automatically enabled.
4. When the green RUN LED of the control panel begins to flash, reposition the Dip-switch 2 to OFF.

7.9.5 Resetting hardware to factory settings

Only in particular cases, like when there is no keypad to access the menu, if it is in any case necessary to reset the control panel to default, can the Reset hardware be used. Remember that this method has the same effect as the Global reset (see paragraph 7.9.2 *Global reset*) in that only the control panel is reset to default. When this procedure is used, the individual devices maintain their programming.

When this operation is completed, it is therefore essential to reset each device individually, as described in paragraph 7.9.6 *Resetting devices* and reacquiring devices, as indicated in the *Programming Manual*.

In reference to the radio expansion, it is also necessary to reacquire all the radio devices associated with it.



IMPORTANT! Following the Reset hardware command, it is necessary to carry out the local reset of all the radio sirens of the system, and then reacquire them.

To carry out the Reset hardware, follow the instructions below:

1. Turn off the control panel completely (see paragraph 7.11 *TURNING OFF THE ENTIRE SYSTEM*)
2. Set the Dip switch to 1 to ON.
3. Reconnect the control panel to the power supply; during the initialisation phase all the parameters will be reset to default.
4. When the green RUN LED of the control panel begins to flash, reposition the Dip-switch 1 to OFF.
5. Reprogram the control panel parameters as indicated in the *Programming Manual*.

7.9.6 Resetting devices

The deletion of any device in the system and connected to the bus must be done according to the procedure described in paragraph 7.5 *DELETING A BUS DEVICE*.

Only in special cases, for example if a device has already been acquired by another control panel or following a "Resetting hardware to default" can the Reset devices been used.



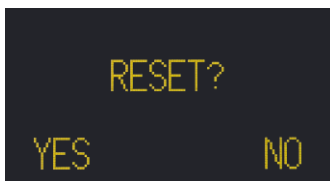
IMPORTANT! Remember that this method only deletes the data on the device. Of the device is also acquired on the control panel, it will continue to be present there, generating and signalling a tamper error.

To cancel the address of any device and reset its programming to default, follow the instructions below:

1. Disconnect power from the device and reconnect it. The yellow LED will begin flashing slowly.
2. Within 10 seconds, press and hold down the "PROG" button for about 5 seconds until the yellow LED flashes at a different speed.
3. Release the button. The Reset phase is concluded. The yellow LED will continue to flash until the device is reacquired (for acquisition see paragraph 6.2.2 *Procedure for acquiring bus devices*).

To delete the address of the KP500DP/N or KP500D/ST keypad, follow the instructions below:

1. Open the tamper contact (release the keypad from the relative bracket - see *Figure 49 - Removal of the KP500DP/N - KP500D/ST keypad bracket*)
2. Press the **F4** key for at least 5 seconds. This will appear on the display:



3. Press **F1** to confirm or **F4** to cancel.

In reference to the radio expansion reset, it is also necessary to reacquire all the radio devices associated with it.



IMPORTANT! Following the Reset command of the radio expansion, it is necessary to carry out the local reset of all the radio sirens of the system, and then reacquire them.

7.10 REPLACING THE BATTERY

When a battery can no longer maintain its charge, it must be replaced with a similar one in order not to compromise the correct functioning of the system.

To replace the battery, follow the instructions below:

1. Activate the Maintenance status (see paragraph 7.1 *MAINTENANCE PROCEDURE*) and open the device containing the battery.
2. Disconnect the old battery and remove it.
3. Insert the new battery and connect it with the special connectors, matching the polarity.
4. Close the device.
5. Carry out a Test battery check (see the *Programming Manual*).



IMPORTANT! The battery may only be replaced by trained and qualified personnel.

7.11 TURNING OFF THE ENTIRE SYSTEM

Whenever the entire system must be turned off, follow the instructions below:

1. Activate Maintenance status (see paragraph 7.1 *MAINTENANCE PROCEDURE*) and open the control panel.
2. Disconnect the mains power supply.
3. Disconnect the battery.
4. If supplemental power supply units are present, disconnect them in the same sequence (points 2 and 3).

Before restoring power, wait at least 1 minute.



IMPORTANT! It is fundamental to put the control panel in Maintenance status before turning it off. Failure to follow these instructions may cause a loss of data and compromise the correct functioning of the system.

7.12 TROUBLESHOOTING

Failures and malfunctions are identified by specific messages of the failure memory and the Diagnose Log. The table below contains the messages that are visualised, the possible causes of the failure or malfunction that occurred, actions to take to find the problem and resolve it.

MESSAGE FAILURE MEMORY	MESSAGE DIAGNOSE LOG.	CAUSE	FINDING AND RESOLVING THE PROBLEM
ANOM. +PS CONTROL PANEL	FAILURE STARTS UC00.CONTROL PANEL ANOM. +PS	The input voltage to the +PS terminal (control panel power supply) of the control panel is malfunctioning. Power supply voltage is < 13.5 V or > 15 V.	- Check the power supply voltage, both empty (disconnected from the control panel) and when charging (connected to the control panel): it must be between 14.25 V and 14.55 V. In case of a 4 A power supply, this voltage can be regulated with a trimmer. - If the voltage should drop when the power supply is connected to the control panel, check that there is not an overload disconnecting one branch of the power supply at a time. - If the voltage increases when the power supply is connected to the control panel, check if an incorrect power supply from a self-powered device is arriving at the +SR terminal.
ANOM. +SR CONTROL PANEL	FAILURE STARTS UC00.CONTROL PANEL ANOM. +SR	The output voltage on the +SR terminal (power supply for the self-powered devices) of the control panel is incorrect (< 11.4 V or > 14.9 V).	- If the voltage measured on the +SR terminal is low or absent, check if there is an overload or a short circuit. - If the voltage measured on the +SR terminal is high, check that if it is coming from a self-powered device (such devices must have a diode to prevent this from happening).
ANOM. +V1 CONTROL PANEL	FAILURE STARTS UC00.CONTROL PANEL ANOM. +V1	The output voltage on the +V1 terminal (power supply for output actuators) of the control panel is incorrect (< 12.9 V or > 14.2 V).	- If the voltage measured on the +V1 terminal is low or absent, check if there is an overload or a short circuit. - If the voltage measured on the +V1 terminal is high, check if there is an incorrect power supply from the system. Note: in this case, there is also a signal for the +V2.
ANOM. +V2 CONTROL PANEL	FAILURE STARTS UC00.CONTROL PANEL ANOM. +V2	The output voltage on the +V2 terminal (power supply for the detectors on the inputs) of the control panel is incorrect (< 12.9 V or > 14.2 V).	- If the voltage measured on the +V2 terminal is low or absent, check if there is an overload or a short circuit. - If the voltage measured on the +V2 terminal is high, check if there is an incorrect power supply from the system. Note: in this case, there is also a signal for the +V1.
ANOM. +D CONTROL PANEL	FAILURE STARTS UC00.CONTROL PANEL ANOM. +D	The output voltage on the +D terminal (polarisation of the data bus) of the control panel is incorrect (< 13 V or > 15 V).	- If the voltage measured on the +D terminal is low or absent, check if there is an overload or a short circuit. - If the voltage measured on the +D terminal is high, check if there is an incorrect power supply from the system.
ANOM. +VBUS CONTROL PANEL	FAILURE STARTS UC00.CONTROL PANEL ANOM. +VBUS	The output voltage on the + terminal (+ power supply of the data bus) of the control panel is incorrect (< 12.9 V or > 14.2 V).	- If the voltage measured on the + terminal is low or absent, check if there is an overload or a short circuit. - If the voltage measured on the + terminal is high, check if there is an incorrect power supply from the system.
ANOM. +V2 KPnn.KP xx	FAILURE STARTS KPnn.KP xx ANOM. +V2	The output voltage +V (power supply for the detectors on the inputs) from the device is incorrect (< 7 V or > 14.3 V).	- If the voltage measured on the +V terminal of the device is low or absent, check if there is an overload or short circuit. - If the voltage measured on the +V terminal of the device is high, check if there is an incorrect power supply from the system (also check the voltage supplied on the + terminal, which must not be > 14.3 V).
ANOM. +V2 DKnn.DK xx	FAILURE STARTS DKnn.DK xx ANOM. +V2		
ANOM. +V2 EPnn.EP xx	FAILURE STARTS EPnn.EP xx ANOM. +V2		
ANOM. +V2 ASnn.AS xx	FAILURE STARTS ASnn.AS xx ANOM. +V2		
PSTN FAILURE CONTROL PANEL	FAILURE STARTS UC00.CONTROL PANEL PSTN FAILURE	Failure on the PSTN telephone line: the call tone was not detected for 3 consecutive line tests, during the automatic line control or when trying to send a message. Note: The line test, if enabled, is carried out every 15 minutes. The SP4 test, if enabled, is carried out continually.	- Check if the PSTN line was mistakenly enabled when not in use. - Check the connection of the telephone line on the "LINE" input terminals. - Check the efficiency of the telephone line. - Check if there is a telephone device connected upstream, between the control panel and the telephone line (in case of connection of a PABX switchboard, exclude the line test).

MESSAGE FAILURE MEMORY	MESSAGE DIAGNOSE LOG.	CAUSE	FINDING AND RESOLVING THE PROBLEM
GSM FAILURE CONTROL PANEL	FAILURE STARTS UC00.CONTROL PANEL GSM FAILURE	Failure on the GSM channel caused by: prolonged absence of the GSM field, absence of the SIM card, incorrect PIN of the SIM card or there is no credit on the SIM card.	• Check if the GSM line was mistakenly enabled in absence of the GSM module. • Check the correct assembly of the GSM antenna and correct fitting of the SMA connector. • Check the presence and intensity of the GSM field via a test (try installing a remote GSM1 antenna). • Check for the presence and the correct positioning of the SIM card (delete any potential contacts). • Check if the SIM card has the PIN enabled and, if so, that it was programmed correctly in the control panel. • Check the remaining credit on the SIM card.
ANOM. BUS KPnn.KP xx	FAILURE STARTS BUS KPnn.KP xx FAILURE BUS CONNECTION	The bus device signalled is not communicating (keypad, reader key, expansion), that control panel has not been answered.	• Check the cabling of the device/s at the bus (disconnected wires or short circuits or inverted polarity). • Check the bus power supply.
ANOM. BUS DKnn.DK xx	FAILURE STARTS BUS DKnn.DK xx FAILURE BUS CONNECTION		
ANOM. CONNECTION EPnn.EP xx	FAILURE STARTS BUS EPnn.EP xx FAILURE BUS CONNECTION		
ANOM. BUS ASnn.AS xx	FAILURE STARTS BUS ASnn.AS xx FAILURE BUS CONNECTION		
ANOM. BUS ERnn.ER xx	FAILURE STARTS BUS ERnn.ER xx FAILURE BUS CONNECTION		
	FAILURE STARTS POWER INSTANT CONTROL PANEL LACK OF POWER	Instantaneous absence of mains power supply in control panel (power supply voltage < 9 V for at least 3 seconds).	• Check the presence and the connection of the mains power supply. • Check the quality of the connection between the power supply and the control panel (+PS and -PS).
	FAILURE STARTS POWER INSTANT ASnn.AS xx LACK OF POWER	Instantaneous absence of mains power supply in supplementary power supply ASnn (power supply voltage < 9 V for at least 3 seconds).	• Check the presence and the connection of the mains power supply. • Check the quality of the connection between the power supply and the ASnn (+PS and -PS).
	FAILURE STARTS NETWORK SYSTEM LACK OF POWER	Prolonged absence of mains power supply (power supply voltage < 9 V for a time longer than "lack of power time")	• Check the presence and the connection of the mains power supply. • Check the quality of the connection between the power supply and the control panel or AS (+PS and -PS).
LOW BATTERY CONTROL PANEL	FAILURE STARTS BATT. CONTROL PANEL BATTERY LOW	Battery voltage < 2 V.	• Check the battery connection • Replace the battery.
		Battery voltage < 12.5 V during test.	If the problem persists for a few days, replace the battery.
		During a lack of power, the voltage of the battery went below 11.5 V (flat battery).	If after the mains power supply is restored the problem persists for a few days, replace the battery.

MESSAGE FAILURE MEMORY	MESSAGE DIAGNOSE LOG.	CAUSE	FINDING AND RESOLVING THE PROBLEM
BATTERY LOW ERnn:DCmm ERnn:IRmm ERnn:RCmm ERnn:HPmm ERnn:ISmm		Radio devices battery flat	Replace the battery
BATTERY LOW ASnn: ASxx “	FAILURE STARTS BATT. ASnn: ASxx BATTERY LOW	Voltage of the supplementary power supply battery ASxx < 2 V.	• Check the battery connection • Replace the battery.
		Voltage of the supplementary power supply battery ASxx < 12.5 V during the test.	If the problem persists for a few days, replace the battery.
		During a lack of power, the voltage of the supplementary power supply battery ASxx went below 11.5 V (flat battery).	If after the mains power supply is restored the problem persists for a few days, replace the battery.

8 - TECHNICAL SPECIFICATIONS

8.1 MP500/4N CONTROL PANEL

Nominal power voltage	230 V~ +10% -15% 50/60 Hz
Max absorption power at 230 V (PS515)	600 mA
PS515 power output nominal voltage - type A power supply	14.4 V $\overline{=}$
Max current deliverable PS515 power supply	1.5 A
Ripple max PS515	100 mV p.p. with I = 1 A
Control panel operating voltage	10.5 V $\overline{=}$ to 16 V $\overline{=}$
Overload protection tripping current	16 V $\overline{=}$
Nominal current absorbed by control panel board with IL500-N at 12 V $\overline{=}$ (with relays energised, default condition) (with relays de-energised)	75 mA stand-by with balanced inputs 65 mA with balanced inputs
Installable battery	12 V – 7.2 Ah
Nominal voltage of battery charger (Note 1)	13.8 V $\overline{=}$
Max current supplied to charge battery	350 mA
Max time for recharging battery to 80%	24 hours
Battery flat threshold	11.5 V
Battery release threshold	10.5 V
Low battery fault reset threshold	12.5 V $\overline{=}$
Automatic test battery	every 24 hours (with mains)
Max current for external devices (keypads, sensors, sirens): taken from +, +V1 terminals Degree 2 – with SP2 dialler and 12 hour autonomy (total 450 mA, of which 75 mA for the control panel with ILT500-N)	375 mA
Nominal voltage on the + terminal	13.8 V $\overline{=}$ $\pm$ 1.5%
Max current deliverable from + terminal	1100 mA (with overload protection)
Nominal voltage on the +V1 terminal	13.8 V $\overline{=}$ $\pm$ 1.5%
Max. current deliverable from +V1 terminal	750 mA (with overload protection)
Ripple max on outputs + +V1 with flat battery	100 mV (0.7%)
Max current and voltage of relay contact switch of outputs O1	1 A – 24 V $\overline{=}$ with resistive load
Max current deliverable from electric output O2	100 mA
Tamperproof switch	1 A – 24 V $\overline{=}$
Max total length of control panel-peripheral serial Bus line	400 m
Max length of the audio line (audio bus)	300 m with twin telephone line
Max length of the connection between each sensor or actuator and the control panel	500 m
Max length of the connection between a fast sensor (roller, shock,...) and the control panel	100 m
Max number possible code combinations	from 10,000 to 1,000,000
Number of possible combinations of DK50 electronic keys	more than 1099 billion
Number of possible combinations of DK30 proximity keys	more than 4 billion
Number of possible combinations of DK70 proximity keys	more than 4 billion
Programmable time entry	5 s to 5 minutes
Programmable exit entry	5 s to 5 minutes
Programmable alarm time	30 s to 15 minutes (default 3 minutes)
Programmable tamper alarm time	30 s to 15 minutes (default 3 minutes)
Failure signal	optical (LED) and electric for control panel battery low, fuses, low power supply expansion boards
Type of memory for programming, Events log, and diagnose log maintenance	Data Flash
Operating temperature	-10°C to +40°C
Average relative humidity during operation	75%
Storage temperature	-20°C to +60°C
Pollution degree	Grade 2
Overvoltage Category	CAT II
Degree of protection of casing	IP40/ IK06
Dimensions (W x H x D)	338 x 240 x 90 mm
Weight (without battery)	1400 g

For further information, see also paragraph 1.2.3 *Maximum system size*.

Note 1) If the battery is not connected to the terminals of the connection cables, (red and black Faston) there is no power.

8.2 MP500/16 CONTROL PANEL

Mains power supply	100 - 240 V~ -15/+10%, 50/60 Hz
Max. absorption current (PS534 – MW RS-50-15)	1.3 A
PS534 (MW RS-50-15) power output nominal voltage - Type A power supply	14.4 V _{DC}
Max current deliverable PS515 (MW RS-50-15) power supply	3.4 A
Ripple max PS534 (MW RS-50-15)	150 mV p.p. with I = 3,4 A
Control panel operating voltage	10.5 V _{DC} to 16 V _{DC}
Overload protection tripping current	16 V _{DC}
Max current absorbed by control panel board at 12 V _{DC} (with relays energised, default condition)	85 mA stand-by with balanced inputs
Max current absorbed by the control panel board (with relays de-energised)	65 mA with balanced inputs
Installable battery	12 V – 18 Ah
Nominal voltage of battery charger note 1)	13.8 V _{DC}
Max current supplied to charge battery	850 mA
Max time for recharging battery to 80%	24 hours
Battery flat threshold	11.5 V
Battery release threshold	10.5 V
Low battery fault reset threshold	12.5 V _{DC}
Automatic test battery	every 24 hours (with mains)
Max current for external devices (keypads, sensors, sirens): taken from +, +V1, +V2 terminals	
Degree 3 – with SP4 dialler and 60 hours autonomy (total 260 mA, of which 85 mA for the control panel)	175 mA
Degree 3 – with SP4 dialler and 30-hour autonomy (total 520 mA, of which 85 mA for the control panel) note 2)	435 mA
Degree 2 – with SP2 dialler and 12 hour autonomy (total 1150 mA, of which 85 mA for the control panel)	1065 mA
Nominal voltage on the +SR terminal note 3)	14.4 V _{DC}
Max current deliverable from the +SR terminal	200 mA (with overload protection)
Nominal voltage on the + terminal	13.8 V _{DC} ±1.5%
Max current deliverable from + terminal	1100 mA (with overload protection)
Nominal voltage on the +V1 terminal	13.8 V _{DC} ±1.5%
Max current deliverable from +V1 terminal	750 mA (with overload protection)
Nominal voltage on the +V2 terminal	13.8 V _{DC} ±1.5%
Max total current deliverable from the +V2 terminals	750 mA (with overload protection)
Ripple max on outputs +SR + +V1 +V2 with flat battery	150 mV (1.1%)
Max current and voltage of relay contact switch of outputs U1 and U2	1 A – 24 V _{DC} with resistive load
Max current deliverable from electric output U3	100 mA
Max current deliverable from electric outputs U4, U5, U6	10 mA
Tamperproof switch	1 A – 24 V _{DC}
Max total length of control panel-peripheral serial Bus line	400 m
Max length of the audio line (audio bus)	300 m with twin telephone line
Max length of the connection between each sensor or actuator and the control panel	500 m
Max length of the connection between a fast sensor (roller, shock, ...) and the control panel	100 m
Max number possible code combinations	from 10,000 to 1,000,000
Number of possible combinations of DK50 electronic keys	more than 1099 billion
Number of possible combinations of DK30 proximity keys	more than 4 billion
Number of possible combinations of DK70 proximity keys	more than 4 billion
Programmable time entry	5 s to 5 minutes
Programmable exit entry	5 s to 5 minutes
Programmable alarm time	30 s to 15 minutes (default 3 minutes)
Programmable tamper alarm time	30 s to 15 minutes (default 3 minutes)
Failure signal	optical (LED) and electric for control panel battery low, fuses, low power supply expansion boards
Type of memory for programming, Events log, and diagnose log maintenance	Data Flash
Operating temperature	-10°C to +40°C
Average relative humidity during operation	75%
Storage temperature	-20°C to +60°C
Pollution degree	Grade 2
Overvoltage Category	CAT II
Degree of protection of casing	IP40/ IK06
Dimensions (W x H x D)	435 x 320 x 93 mm
Weight (without battery)	5600 g

For further information, see also paragraph 1.2.3 *Maximum system size*.

Note 1) If the battery is not connected to the terminals of the connection cables, (red and black Faston) there is no power.

Note 2): remotely assisted system with guaranteed intervention in case of lack of power;

Note 3) in case of blackout, the **+SR** does not supply voltage.

8.3 KEYPAD DISPLAY KP500D/N - KP500DV/N

Nominal power voltage	13.8 V $\overline{=}$ (taken from bus)
Keypad operating voltage	9 V $\overline{=}$ to 15 V $\overline{=}$
Nominal current absorbed at 12 V $\overline{=}$	20 mA (in stand-by, only LED for presence mains supply) 32 mA (operative, with level 1 backlighting) 120 mA (operative, with level 4 backlighting) 200 mA max. (in message listening – version DV/N)
Nominal voltage on +V outputs	13.8 V $\overline{=}$
Max current deliverable on +V outputs	100 mA
Max total length of control panel-peripheral serial Bus line	400 m
Max length of the audio line (audio bus)	300 m with twin telephone line
Max length of the connection between each sensor and the keypad	500 m
Max length of the connection between a fast sensor (roller, shock, ...) and the keypad.	100 m
Type of communication	Elkron serial protocol
Tamperproof switch	standard with clear channel signalling in the control panel
Auxiliary inputs (only KP500D/N)	2
Protection against inserting false codes	Yes
Operating temperature	-10°C to +40°C
Average relative humidity during operation	75%
Storage temperature	-20°C to +60°C
Degree of protection of casing	IP40 / IK06
Weight	250 g
Dimensions (W x H x D)	151 x 125 x 29 mm

8.4 KEYPAD TOUCH SCREEN KP500DP/N

Nominal power voltage	13.8 V $\overline{=}$ (taken from bus)
Keypad operating voltage	10 V $\overline{=}$ to 15 V $\overline{=}$
Nominal current absorbed at 12 V $\overline{=}$	32 mA (in stand-by, only LED for presence mains supply) 68 mA (average absorption with backlighting at level 1) 110 mA (average absorption with backlighting at level 4) 200 mA (maximum peak absorption)
Max total length of control panel-peripheral serial Bus line	400 m
Type of communication	Elkron serial protocol
Type of memory for program maintenance	Data Flash
Type of memory for vocabulary maintenance	Data Flash
Operating temperature	-10°C to +40°C
Average relative humidity during operation	75%
Storage temperature	-20°C to +60°C
Degree of protection of casing	IP40 / IK06
Weight	460 g
Dimensions (W x H x D)	160 x 130 x 23.5 mm

8.5 KEYPAD TOUCH SCREEN KP500D/ST

Nominal power voltage	13.8 V _{DC} (taken from bus)
Keypad operating voltage	10 V _{DC} to 15 V _{DC}
Nominal current absorbed at 12 V _{DC}	32 mA (in stand-by, only LED for presence mains supply) 68 mA (average absorption with backlighting at level 1) 110 mA (average absorption with backlighting at level 4) 200 mA (maximum peak absorption)
Max total length of control panel-peripheral serial Bus line	400 m
Type of communication	Elkron serial protocol
Type of memory for program maintenance	Data Flash
Type of memory for vocabulary maintenance	Data Flash
Operating temperature	-10°C to +40°C
Average relative humidity during operation	75%
Storage temperature	-20°C to +60°C
Degree of protection of casing	IP40 / IK06
Weight	460 g
Dimensions (W x H x D)	160 x 130 x 23.5 mm

8.6 DK500M-E ELECTRONIC KEY READER

Nominal power voltage	13.8 V _{DC} (taken from bus)
Reader operating voltage	9 V _{DC} to 15 V _{DC}
Nominal current absorbed at 12 V _{DC}	6 mA in stand-by 56 mA max (with all LEDs on)
Max total length of control panel-peripheral serial Bus line	400 m
Max length of the connection between each sensor and the reader	500 m
Max length of the connection between a fast sensor (roller, shock, ...) and the reader	100 m
Type of communication	Elkron serial protocol
Auxiliary inputs	2
Operating temperature	-10°C to +40°C
Average relative humidity during operation	75%
Storage temperature	-20°C to +60°C
Degree of protection of casing	IP40 / IK06

8.7 DK500M-P PROXIMITY READER

Nominal power voltage	13.8 V _{DC} (taken from bus)
Reader operating voltage	9 V _{DC} to 15 V _{DC}
Nominal current absorbed at 12 V _{DC}	40 mA in stand-by 68 mA max (with all LEDs ON)
Max total length of control panel-peripheral serial Bus line	400 m
Max length of the connection between each sensor and the reader	500 m
Max length of the connection between a fast sensor (roller, shock, ...) and the reader	100 m
Type of communication	Elkron serial protocol
Auxiliary inputs	2
Operating temperature	-10°C to +40°C
Average relative humidity during operation	75%
Storage temperature	-20°C to +60°C
Degree of protection of casing	IP40 / IK06

8.8 DK510M-P PROXIMITY READER

Nominal power voltage	13.8 V _{DC} (taken from bus)
Reader operating voltage	9 V _{DC} to 15 V _{DC}
Nominal current absorbed at 12 V _{DC}	40 mA in stand-by 68 mA max (with all LEDs ON)
Max total length of control panel-peripheral serial Bus line	400 m
Max length of the connection between each sensor and the reader	500 m
Max length of the connection between a fast sensor (roller, shock, ...) and the reader	100 m
Type of communication	Elkron serial protocol
Auxiliary inputs	2
Operating temperature	-10°C ÷ +40°C
Average relative humidity during operation	75%
Storage temperature	-20°C ÷ +60°C
Degree of protection of casing	IP40 / IK06

8.9 8-INPUT EP508 EXPANSION MODULE

Nominal power voltage	13.8 V _{DC} (taken from bus)
Expansion operating voltage	9 V _{DC} to 15 V _{DC}
Nominal current absorbed at 12 V _{DC}	35 mA stand-by (with energised relay, default condition) 22 mA max. with relay de-energised
Nominal voltage on the +V1 terminal	13.2 V _{DC}
Max current deliverable from +V1 terminal	500 mA
Nominal voltage on the +V2 terminal	13.2 V _{DC}
Max total current deliverable from the +V2 terminals	500 mA
Max current and voltage of relay contact switch of outputs U1	1 A – 24 V _{DC} with resistive load
Max current deliverable from electric outputs U2 and U3	10 mA
Max total length of control panel-peripheral serial Bus line	400 m
Max. connection length between each sensor and the expansion	500 m
Max length of the connection between a fast sensor (roller, shock, ...) and the expansion	100 m
Type of communication	Elkron serial protocol
Operating temperature	-10°C to +40°C
Average relative humidity during operation	75%
Storage temperature	-20°C to +60°C

8.10 VOCAL SYNTHESIS BOARD SV500N-I-F-GB

EN50131
NOT RELATED

Nominal power voltage	13.8 V _{DC} (taken from the control panel)
Operating voltage of the vocal synthesis board	10.5 V _{DC} to 15 V _{DC}
Nominal current absorbed at 12 V _{DC}	3 mA in stand-by 20 mA max. (during message reproduction)
Max length of the audio line (audio bus)	300 m with twin telephone line
Max number of messages that can be recorded	94

8.11 ILT500-N PSTN COMMUNICATOR

Nominal power voltage	13.8 V _{DC} (taken from the control panel)
Nominal current absorbed at 12 V _{DC}	3 mA in stand-by 20 mA max. (during telephone connection)
Reference legislation	EN50136-2
SP classification	SP2
Operating mode	Pass-Through

8.12 IMG500/N GSM MODULE

EN50131

Nominal power voltage	13.8 V _{DC} (taken from the control panel)
GSM module operating voltage	10.5 V _{DC} to 15 V _{DC}
Absorption at nominal voltage of 12 V _{DC}	150 mA

8.13 USB INTERFACE FOR CONNECTION TO THE PC AND USB IT-USB/KEY KEYS

Nominal power voltage	13.8 V _{DC} (taken from the control panel via flat cable)
Operating voltage of the USB interface	9 V _{DC} to 15 V _{DC}
Absorption at nominal voltage of 12 V _{DC}	5 mA max in Standby (USB key and PC not connected) 65 mA max with USB key in read/write 15 mA max with PC connected and communicating
Max current supplied to the USB Key	100 mA

8.14 IT500WEB INTERFACE

EN50131

Nominal power voltage	13.8 V _{DC} (taken from the control panel via flat cable)
Operating voltage of the Web server interface	9 V _{DC} to 15 V _{DC}
Absorption at nominal voltage of 12 V _{DC}	150 mA max (1,8 W)
Connection port	LAN - RJ45 Speed 100Mbps
Operating temperature	-10 °C to +40°C
Average relative humidity during operation	75%
Storage temperature	-20 °C to +60°C

8.15 SUPPLEMENTARY POWER UNIT AS500/RPT

Section - BUS IN	
Nominal power voltage	13.8 V $\overline{\text{---}}$ (supplied by control panel BUS)
Expansion operating voltage	9 V $\overline{\text{---}}$ to 15 V $\overline{\text{---}}$
Maximum current absorbed from the expansion at 12 V $\overline{\text{---}}$ (with relays energised, default condition)	50 mA stand-by with balanced inputs 55 mA with NC inputs
Maximum current absorbed from the expansion at 12 V $\overline{\text{---}}$ (with relays de-energised)	40 mA with balanced inputs 45 mA with NC inputs
Nominal voltage on the +V1 terminal	13.2 V $\overline{\text{---}}$ (supplied by control panel BUS)
Max current deliverable from +V1 terminal	500 mA (with overload protection)
Nominal voltage on the +V2 terminal	13.2 V $\overline{\text{---}}$ (supplied by control panel BUS)
Max total current deliverable from the +V2 terminals	500 mA (with overload protection)
Max current and voltage of relay contact switch of outputs U1	1 A – 24 V $\overline{\text{---}}$ with resistive load
Max current deliverable from electric outputs U2 and U3	10 mA
Max total length of control panel-peripheral serial Bus line (primary BUS)	400 m
Max. connection length between each sensor or actuator and expansion	500 m
Max length of the connection between a fast sensor (roller, shock, ...) and the expansion	100 m
Supplementary power section and BUS OUT	
Mains power supply	100 – 240 V $\sim$ -15/+10%, 50/60 Hz
Max. absorption current (PS534 – MW RS-50-15)	1.3 A
PS534 (MW RS-50-15) power output nominal voltage	14.4 V $\overline{\text{---}}$
Type A power supply	
Max. deliverable current	3.4 A
Ripple max PS534 (MW RS-50-15)	120 mV p.p. with I = 3.4 A
Operating voltage of the electronic power supply and repeater	9 V $\overline{\text{---}}$ to 15 V $\overline{\text{---}}$
Max current absorbed by the electronic power supply and repeater	100 mA
Installable battery	12 V – 18 Ah
Nominal voltage of battery charger note 1)	13.8 V $\overline{\text{---}}$
Max. current supply to charge battery	500 mA
Max time for recharging battery to 80%	48 hours
Battery flat threshold	11.5 V
Battery release threshold	10.5 V
Low battery fault reset threshold	12.5 V $\overline{\text{---}}$
Automatic test battery (controlled by control panel)	every 24 hours (with mains)
Max current for external devices (keypads, sensors, sirens): taken from + (BUS OUT), +, + terminals Degree 2 – with SP2 dialler and 12 hour autonomy (total 1150 mA, of which 100 mA for electronics)	1050 mA
Nominal voltage on the +SR terminal note 3)	14.4 V $\overline{\text{---}}$
Max current deliverable from the +SR terminal	200 mA (with overload protection)
Nominal voltage on the + (BUS OUT) terminal	13.8 V $\overline{\text{---}}$ $\pm$ 1.5%
Max. current deliverable from + (BUS OUT) terminal	1100 mA (with overload protection)
Nominal voltage on the + terminal	13.8 V $\overline{\text{---}}$ $\pm$ 1.5%
Max. total current deliverable from +V terminals	750 mA each (with overload protection)
Ripple max on outputs +SR + + with flat battery	120 mV (0.9%)
Max. total length of serial power supply-peripheral BUS OUT line (secondary BUS)	400 m
Operating temperature	-10°C to +40°C
Average relative humidity during operation	75%
Storage temperature	-20°C to +60°C
Pollution degree	Grade 2
Overvoltage Category	CAT II
Degree of protection of casing	IP40/ IK06
Dimensions (W x H x D)	435 x 320 x 93 mm
Weight (without battery)	5600 g

Note 1): if the battery is not connected to the head of the terminal +BT -BT there is no power.

Note 3) in case of blackout, the +SR does not supply voltage.



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