

TP10-42 - TP10-42 EN

Expandable serial alarm systems



Installation manual

Document release:	2.1
FW release:	1.7.04
HW release:	TP10-42 - TP10-42 EN
Programming SW release:	5.2 - - - ➔
Update:	10/2017
Language:	English

CONFORMITY

The present equipment is in compliance with the essential requirements and other relevant provisions of the R&TTE 1999/05/EC directive. The equipment is also in compliance with the standards EN 50131-1, EN 50131-3, EN 50136-1 and EN 50136-2.

The declaration of conformity is available on the website: www.tecnoalarm.com.

The product features can be subject to change without notice. Unauthorized reproduction or distribution of this manual, or any portion of it, on any device and in any form, is prohibited. The contents of this manual may be subject to change without notice.

INDEX

1 - GENERAL REFERENCES

7

2 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS

9

3 - WARNINGS FOR INSTALLATION

3.1	Casing	11
3.2	General warnings	11
3.3	Fixing of the casing	12
3.4	Conformity with EN 60950-1 - Electrical safety	12
3.5	Mains and ground connection	13

4 - ADDITIONAL REFERENCES

4.1	Control panel and certified accessories	15
4.2	Access levels	15
4.3	System management	16
4.4	Special functioning modes	16
4.5	Telephone settings	17
4.6	Events with obligation of notification	18
4.7	Notification requirements	18
4.8	Zone input programming	19
4.9	Power supply	19

5 - PROGRAMMING BY CONSOLE

5.1	Programming menu	21
5.2	Menu guide	22

6 - HARDWARE

6.1	CPU board	33
6.2	Terminals	34
6.3	Power supply	35
6.4	Mounting position of plug-in modules	36
6.5	Plug-in input expansion	36
6.6	Mounting of plug-in input expansion	36
6.7	Plug-in GSM-GPRS interface	37
6.8	Mounting of GSM antenna	37
6.9	Plug-in Ethernet interface	38
6.10	Consumption	38
6.11	Available current for loads	38
6.12	Output expansions	39
6.13	Zone distribution	41
6.14	Wireless modules	41
6.15	Installation notes for wireless modules	42
6.16	Serial buses	43
6.17	Standard serial bus	43
6.18	Connection to standard serial bus	44
6.19	Connection to Sensor Bus	44
6.20	Connection to Siren Bus	44
6.21	Connection of conventional peripherals	45

7 - SPECIAL PROCEDURES

7.1	Firmware upgrade	47
7.2	Reset of codes	50
7.3	Reset of system configuration	51

1 - GENERAL REFERENCES

Premise

Before you proceed to the installation, read this manual thoroughly. It contains important references and instructions concerning the correct installation, operation and servicing of the alarm systems TP10-42 and TP10-42 EN.

Operational restrictions and purpose of an intrusion alarm system

It is fundamental to consider that an intrusion alarm system does not guarantee protection and immunity against material damages, of any kind and nature, caused or induced by intrusion attempts. It is equally important to state that any intrusion alarm system must be installed and kept in a state of perfect functioning according to the instructions provided by the manufacturer.

The Tecnoalarm systems, designed for the protection of property and persons, are able to notify alarm events promptly to the final user and/or a monitoring station. The systems process the events automatically and, according to programming, transmit acoustic and/or telematic notifications apt to activate automatic control systems or induce the intervention of special personnel, with the aim of guaranteeing the safety of the persons and the safeguard of the property.

Authorized installer

Although this manual contains all the necessary procedures for a correct installation of the equipment, the interpretation and correct application of its contents requires adequate training of the technical staff in charge of the installation. In particular, the installer must have the necessary technical skills, be familiar with the valid European standards regarding both the general requirements for burglar alarm systems and the specific provisions for installation, electrical safety and maintenance. In addition, he must be an authorized installer and have a thorough knowledge of the products of Tecnoalarm S.r.l.

Environmental provisions

If not specified otherwise, the control panel and all the system components must be installed inside structures or buildings with climatic characteristics (temperature and non-condensing relative humidity) that comply with the standards applied during certification. Specific modes and places of installation and specific operating temperature and humidity values are indicated in the technical data tables of the individual products.

Customer Service

The Customer Service Department of Tecnoalarm provides assistance and answers to technical queries regarding the installation, functioning and operation of the Tecnoalarm products.

Power supply

In the planning phase, to ensure the autonomy of service requested by the standards, it is important to size the primary (mains power) and secondary (battery) power supply correctly.

Consider that, in case of power failure, the system ensures functioning by means of batteries for a limited period of time, the length of which depends on the capacity and the state of efficiency of the batteries.

Induced damage

Prior to acting on any system component, while installing or servicing the equipment, always disconnect both the primary (mains power) and secondary (battery) power supply of the system. To avoid damages caused by electrostatic discharges, handle the equipment with care and avoid any contact with the electronic components.

Periodic maintenance

To guarantee the efficiency of the burglar alarm system, it is necessary to provide an appropriate maintenance program.

The frequency of the maintenance depends on different aspects, however, it is recommended to have the system serviced at least once every 6 months. The maintenance operations should be made by specialized technical staff, the same who has designed and installed the system. The European standards series EN 50131 include the possibility of remotely executing one of the two required annual inspections.

The most important controls are:

- The status of the power supplies and batteries
- The status of the batteries and self-powered devices (sirens and transmitters)
- The functional efficiency and coverage of the movement and perimeter detectors
- The efficiency of the control units and procedures for arming of the program
- The efficiency of the alarm transmission equipment (e.g. activation of telephone call cycle)
- The efficiency of the warning devices
- The correct detection and management of the tamper alarms
- The other secondary functions (e.g. activation of hold-up alarm)
- The correct connection of the cables to the terminals
- The final inspection report

2 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS

TP10-42 - TP10-42 EN

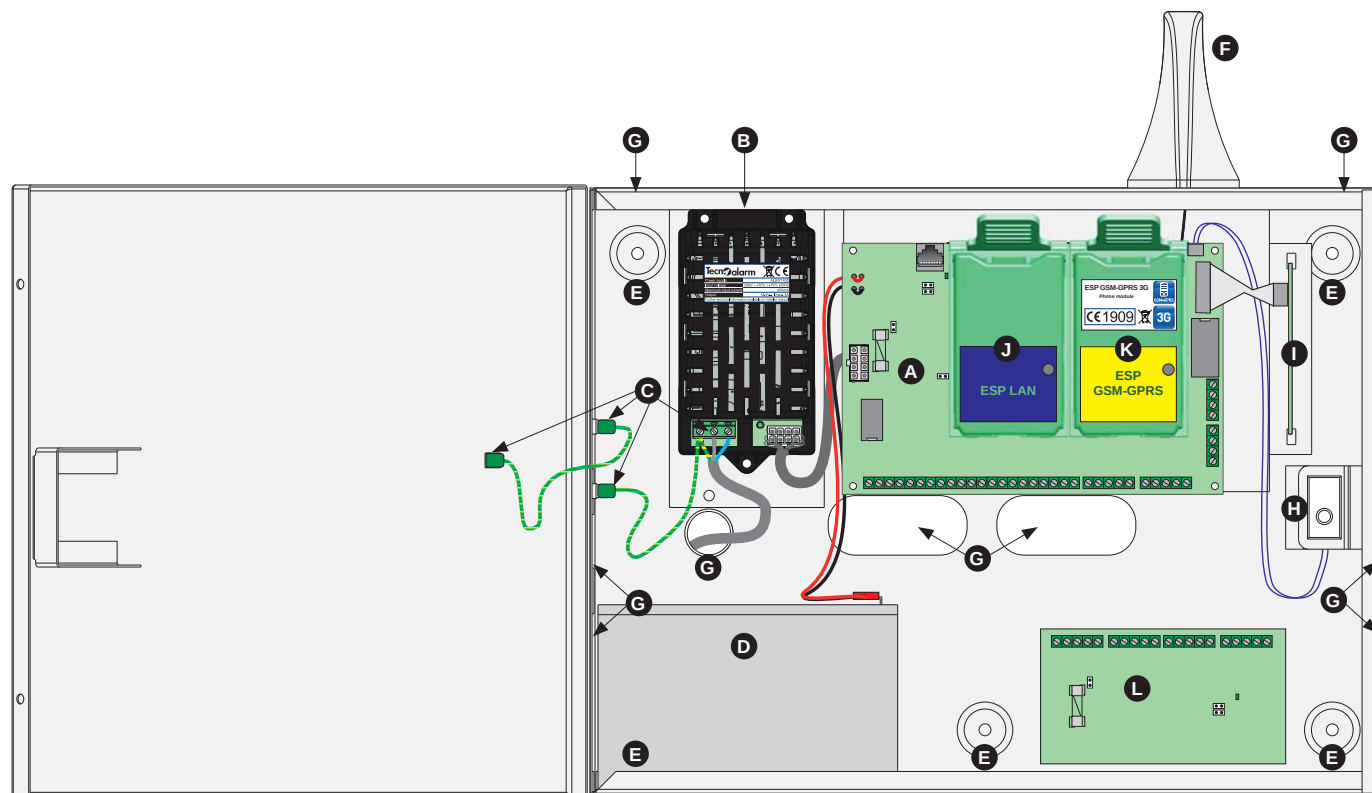
Zones	Total logic zones	42
	CPU hard-wired zones	4 conventional 6 Sensor Bus
	Total hard-wired zones	42
	Total wireless zones	42
Uscite	CPU outputs	6 programmable
	Logic sirens	8
System features	RS485 serial ports	3
	Voice synthesis	✓
Event buffer	Memory type	Circular non-volatile
	Storage capacity	7,600 events
	Storage time	>10 years
Programs and control modes	Programs	8
	Codes	122
	Finger prints	100
	Transponders/RFID cards	100
	Wireless keys	80
Access code combinations	Codes	100,000 (5 digits) 1,000,000 (6 digits)
	False code alarm	After 32 digits
	RFID	Min. 2 ²²
Automation	Timers	8
	Access periods	6
	Calendar	quadrennial or perpetual
	Remote controls	8
	Cyclic timers	8
	Test call with TCP/IP	1
Telephone section	PSTN interface	SP2 (acknowledgement pass-through)
	Conformity	ETSI ES 203-021 R&TTE
	Vocal transmission time	12s
	Transmission time D2	Contact ID 17s
	Transmission time M2	Contact ID 19s
	GSM interface (optional)	SP3 (standard protocols) SP5 (128/256 bit encryption)
	Transmission time D2	SIA IP DC-09 10s
	Transmission time M2	SIA IP DC-09 10s
	IP interface (optional)	SP3 (standard protocols) SP5 (128/256 bit encryption)
	Channels	8
	Transmittable events	157
	Telephone no./IP address	Max. 24 digits
	Call event queue	32
	Communication protocols	216
Accessory management	App (iPhone - Android)	✓
	Printer management	✓
Serial expansions	Hard-wired input expansions	10
	Wireless modules ASYNC@WL	2
	Wireless modules SYNC@BWL	1
	Consoles	8
	Auxiliary control units	8
	Output expansions	16
	GSM telephone communicator	1
	Bus sirens	4
Advanced programming	Actions	1024
	Timers	512
	Counters	128
	Telephone numbers	48
	Output expansions	4
Electrical specifications CPU board	CPU consumption	150mA @ 13.8V DC
	Logic outputs	I max. 30mA
	Output voltage control	10.5V...15V DC
	Detector power supply	Vout 13.8V DC
	Siren power supply	Vout 14.4V DC
Power supply	Type	A - 230V AC +10% -15% 50Hz
	Conformity	EN 50131-6
	Max. consumption	450mA AC
	Max. output voltage	3A @ 14.4V DC
	Max. current available	I max. 3A
	Max. ripple	80mV @ 3A
	Failure signaling	<8V
	Overcharge signaling	>15.6V DC
Battery	Mains fuse (non replaceable)	F1:T1.6AL
	Capacity	1x 12V/12Ah
	Flame class	UL94-HB
	Low battery threshold	11.6V DC
	Restore threshold	12.2V DC
	Release voltage	<8.5V DC
	Recharge time	80% approx. 24h
Physical specifications	Environmental class	II
	Casing	Metal
	Dimensions (L x H x D) (w/o antenna)	398 x 309 x 108mm
	Antenna height	90mm
	Weight (without battery)	4.5kg
	Operating temperature	-10°C...+55°C
	Relative humidity (non-condensing)	95%
Conformity TP10-42 EN	European standards	EN 50131-1 EN 50131-3 EN 50136-1 EN 50136-2
	Security grade	2
	Notified body	IMQ

3 - WARNINGS FOR INSTALLATION

3.1 - Casing

The control panel must be installed in indoor areas, monitoring of temperature and humidity is not required.

The control panel is composed of three macro elements: the metal casing, the CPU board and the switching power supply (primary supply). The casing provides a battery bay (secondary supply). The plug-in expansion modules may be installed in the positions I, L, M indicated in the below figure. In addition, the casing provides a space for installing a serial input expansion (N).

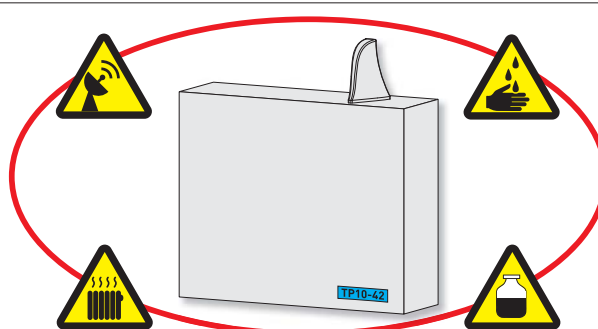


A	CPU board	E	Mounting holes	I	Mounting position ESP4-20
B	Power supply ALSW1430	F	GSM antenna	J	Mounting position ESP LAN
C	Ground connectors	G	Cable entry	K	Mounting position GSM-GPRS
D	12V/12Ah battery	H	Anti-tamper protection	L	Mounting position serial input expansion

3.2 - General warnings

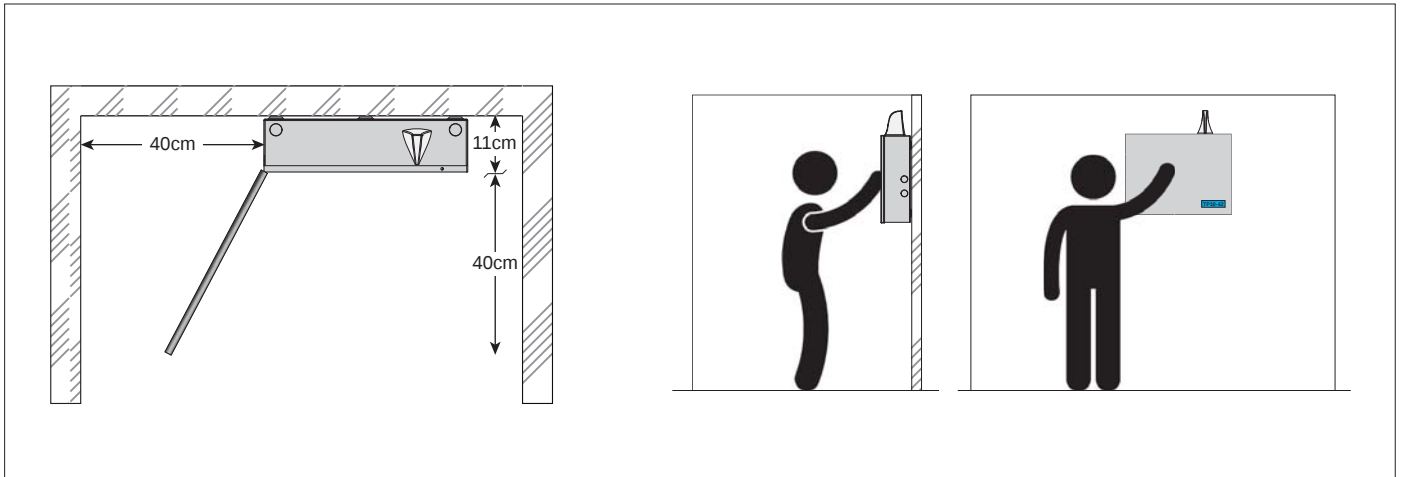
For the safety of the operators protect the control panel, as any electronic device, against splashes and avoid placing recipients containing liquids next to it. The control panel must be installed so as to ensure adequate ventilation. Do not cover the device with things that may hinder correct heat dissipation.

Install the control panel at an adequate distance from heat sources (e.g. radiators) and any device that may cause electromagnetic disturbances (e.g. radio antennas).



3.3 - Fixing of the casing

The casing of the control panel must be fixed in a position that guarantees adequate protection from accidental shocks and at a height that grants full access to the operator. Consider the space necessary for fully opening of the casing door (approx. 40cm). Fix the casing horizontally on a solid surface using 4 dowels with 8mm diameter.



3.4 - Conformity with EN 60950-1 - Electrical safety

Ground connection

The ground connection must comply with the valid European standards. It is mandatory to connect the ground conductor between the casing and the door.

External circuit breaker

The power supply of the control panel is not equipped with a circuit breaker. To guarantee accordance of the installation with the valid European standards, it is necessary to connect an external circuit breaker or a bipolar mains switch (16A curve C, opening stroke min. 3mm) in an accessible part of the electric installation (230V AC).

The circuit breaker must be installed close to the control panel and must be clearly labeled.

Mains connection (230V AC)

The mains cable is not included. To reduce the risk of electric shocks in normal operating conditions, observe the following precautions:

- Use a double insulation cable (with shielding) for the connection to mains power.
- The mains cable should have a diameter of minimum 3x 1.5mm² and, once it has been connected to the corresponding power input, it should be attached with a cable tie to the mounting base of the power supply.
- To guarantee the electrical safety and correct functioning, always connect the ground conductor to the corresponding terminal and between the base and the door of the casing.

3.5 - Mains and ground connection

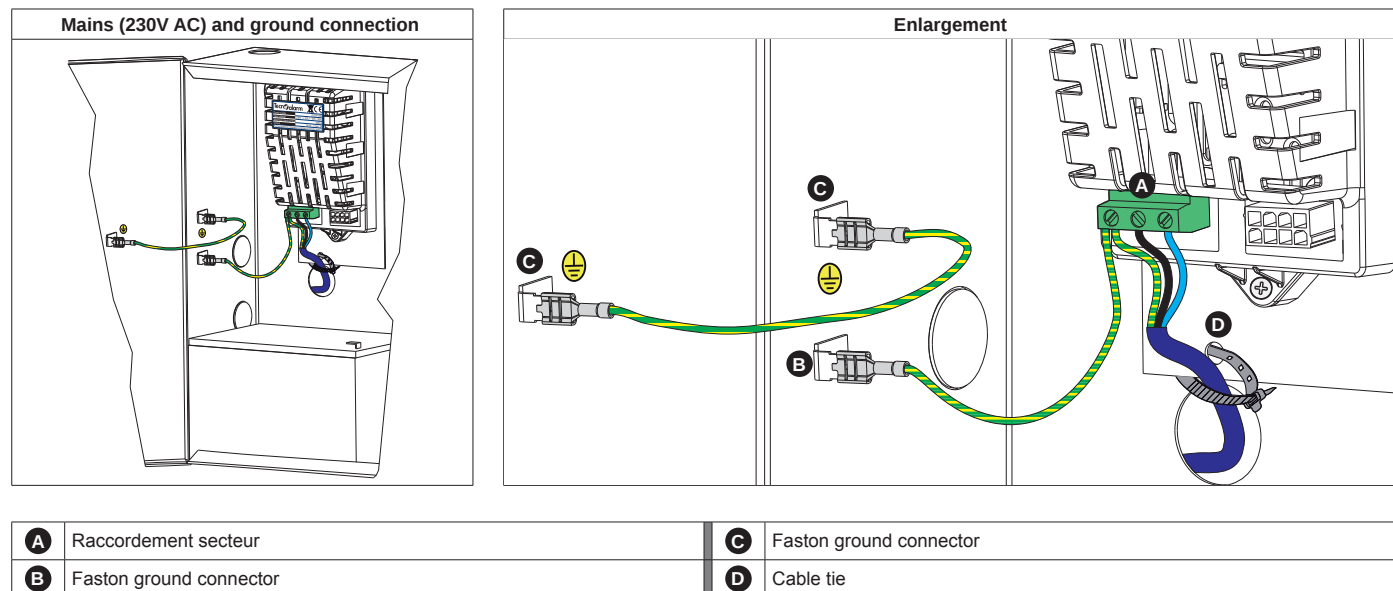
Connect the mains conductor and the ground conductor as illustrated in the below figure.

The mains conductor must be wired in the absence of voltage.

The ground conductor must be connected to the ground terminal of the power supply and to the faston connector soldered to the casing.

It is mandatory to connect the ground conductor between the casing and the door.

For safety reasons, attach the connection cable with a cable tie to the mounting base of the power supply



4 - ADDITIONAL REFERENCES

This chapter provides relevant references for the installation, programming and use of the control panel **TP10-42 EN**.

4.1 - Control panel and certified accessories

Model	Certification	Notes
TP10-42 EN		Metal casing - 1x 12V/12Ah battery - on-board PSTN interface Certified to EN 50131 - Notified body IMQ - Security grade 2

Accessories approved for use with certified control panels

Internal expansions and interfaces			
Model	Description	Item no.	
ESP4-20	Expansion module with 4 standard inputs	F127TP420ESP	
ESP GSM-GPRS	GSM 2G interface	F127ESPGSMGPRS	
ESP GSM-GPRS 3G	GSM 3G interface	F127ESPGSMGPRS3	
ESP LAN	Ethernet interface	F127ESPLAN	

Serial expansions			
Model	Description	Item no.	
LCD300/S	LCD console	F127LCD300S	
LCDPROX1	LCD console with transponder reader	F127LCDPROX1	
UTS C	Touch screen console	F127UTSC	
UTS 4.3 PROX	Touch screen console with transponder reader	F127UTS43PROX	
DIGITEX	Keypad	F103DIGITEX	
TP SKN	Interface for ATPROX transponder readers	F127TP-SKN	
ATPROX	Transponder reader	F103ATPROX	
PROXKEY	Transponder	F103PROXKEY	
PROXKEY HS	Unduplicatable transponder	F103PROXKEYHS	
SPEED 4	Expansion module with 4 standard inputs*	F101SPEED4	
SPEED 8	Expansion module with 8 standard inputs*	F101SPEED8	
SPEED 4 PLUS	Expansion module with 4 standard and 4 Sensor Bus inputs*	F101SPEED4PLUS	
SPEED 8 PLUS	Expansion module with 8 Sensor Bus inputs*	F101SPEED8PLUS	
ESP 8RP	Expansion module with 8 power relay outputs	F127ESP8RP	
ESP 8RSP	Expansion module with 7 signal relay and 1 power relay outputs	F127ESP8RSP	
ESP 4RS	Expansion module with 4 signal relay outputs	F127ESP4RS	

* The modules can be installed either inside the control panel casing or in one of the optional casings (C90 or C100P).

4.2 - Access levels

The standards **EN 50131** distinguish 4 access levels:

Level 1 - Access of any subject (e.g. direct viewing on the console or access by keystroke without entering a code)

Level 2 - Access of authorized users by code

The system recognizes 122 standard user codes and 1 master code. Whereas the privileges of the standard user codes can be customized, the master code always has all the privileges. This access level permits the reset of zone alarm signaling.

Level 3 - Access of the installer by code

The access must be authorized by a user with a level 2 access code (enabling by menu). This access level permits the reset of zone, tamper and failure alarm signaling.

Level 4 - Access of the manufacturer

Conformità alle EN 50136-2

In compliance with the standard **EN 50136-2** the minimum code length must be 6 digits (1 mln combinations).

The options (e.g. inputs programmed as key zone) which permit arming/disarming of the system without an adequate access control are not compliant with the standards **EN 50131**.

4.3 - System management

Timers

To use the timers it is mandatory to activate the arming warning option, i.e. an optical-acoustic indication on the console which indicates an imminent event. To verify the good outcome of the operation, it is advisable to make a call confirming the arming.

Timers - Unauthorized functions

According to the standards EN 50131, the use of timers for arming, forced arming and conditioned forced arming is not permitted as it is impossible to block the automatic arming when the procedure is started.

Timers - Authorized functions

The standards EN 50131 allow the use of timers for conditioned arming and arming with exclusion of the open zones, on condition that the arming of the system with open zones does not cause an alarm condition.

Arming of the programs during failure condition

In compliance with the standards EN 50131, arming of a program during a failure condition, e.g. tamper, low battery, power failure, failure of interconnections, interruption of fuse, is not permitted. However, a user of the level 2 can force arming by pressing the YES-key on the console. The anomalous procedure will be stored in the event log.

Quick arming and disarming

It is not permitted to use the quick commands for arming/disarming of the programs.

4.4 - Special functioning modes

Arming of the system with open zones

The arming of the system with open zones is possible using the forced arming procedure. Enter a valid code followed by the number of the program to be armed and press the YES-key. This procedure causes the automatic exclusion of the open zones on arming. The zones will automatically be included on disarming of the programs. The event is stored in the event log.

Hiding of system status

According to the standards EN 50131, the information about the status of the system must not be available if the system is active (programs armed). Once the exit time has elapsed, they are no longer displayed. All information is hidden (the console displays "Info available") and will only be available upon entering of a valid code.

Range reduction

Every input can be programmed as "reduction of range" to manage this failure signal (only for detectors with the corresponding output).

Enabling of the installer access

The access by installer code must be enabled by one of the others codes. The access is limited to 12 hours.

The installer must use his personal code (by default 654321).

Entry time 1 and 2

The entry time must not exceed 45 seconds.

Alarm time

The alarm time must be minimum 1 minute and 30 seconds and maximum 14 minutes and 59 seconds.

Siren activation delay

The maximum activation delay for outdoor sirens is 10 minutes.

N.B. This restriction is valid regardless of the certification.

Zone exclusion

The exclusion affects only the primary function of the zone, i.e. the detection of alarms, but it does not exclude the anti-tamper protection, which is always active.

N.B. This restriction is valid regardless of the certification.

Isolation

The isolation puts a zone or, more generally, a device completely out of service. The zone loses all detection capacity and the device loses all operability regarding both the primary function and the anti-tamper protection (i.e. the anti-tamper protection is not active).

4.5 - Telephone settings

In compliance with the standards EN 50136, the following provisions concerning the telephone notification equipment are mandatory:

Telephone line test

The dial tone check must always be active.

Call confirmation

For the voice calls it is mandatory to enable the confirmation option.

Test call

The call test must be programmed with the intervals indicated in the below table (test interval).

Classification	PSTN interface	ESP GSM-GPRS with standard data protocols (a)	ESP GSM-GPRS with encrypted data protocols (a)	ESP LAN with standard data protocols (b)	ESP LAN with encrypted data protocols (b)	Test interval
SP2	✓					25h
SP3				✓		30min
		✓				
SP4			✓		✓	3min
SP5			✓		✓	90sec
DP1	✓			✓		25h
	✓	✓				
DP3	✓				✓	3min
	✓		✓			

Legend:

SPx (Single path) - Value which indicates the performance level achieved by the single vector, according to the standard EN 50136-1

DPx (Dual path) - Value which indicates the performance level achieved by a combination of two vectors, according to the standard EN 50136-1

(a) The available protocols are listed in table

(b) The available protocols are listed in table

Table 1 - IP mobile protocols available

115	SIA-GPRS-T	SIA-GPRS-T Reporting (TCP-2007)	Standard	156	SIA-GPRS 256b	SIA-GPRS Encrypt-256	Encrypted
116	C.ID-GPRS-T	C.ID-GPRS-T Reporting (TCP-2007)	Standard	157	C.ID-GPRS 256b	C.ID-GPRS Encrypt-256	Encrypted
117	SIA-GPRS 128b	SIA-GPRS Encrypt-128 (TCP-2007)	Encrypted	182	Tecno GPRS-DAT	Tecnoalarm GPRS-DATA	Encrypted
118	C.ID-GPRS 128b	C.ID-GPRS Encrypt-128 (TCP-2007)	Encrypted				

Table 2 - IP protocols available

119	SIA-IP 128b	SIA-IP Encrypt-128 (TCP-2007)	Encrypted	149	C.ID-UDP-T 128b	CID-IP Encrypt-128 (UDP-2012)	Encrypted
123	SIA-IP	SIA-IP Reporting (TCP-2007)	Standard	150	SIA-UDP 256b	SIA-UDP Encrypt-256	Encrypted
124	SIA-IP-T	SIA-IP-T Reporting (TCP-2007)	Standard	151	C.ID-UDP 256b	C.ID-UDP Encrypt-256	Encrypted
125	C.ID-IP	C.ID-IP Reporting (TCP-2007)	Standard	152	EMS-IP	Milestone server	Standard
126	C.ID-IP-T	C.ID-IP-T Reporting (TCP-2007)	Standard	153	EMS-IP CF	Milestone server w.conf.	Standard
127	C.ID-IP 128b	C.ID-IP Encrypt-128 (TCP-2007)	Encrypted	154	SIA-IP 256b	SIA-IP Encrypt-256	Encrypted
146	SIA-UDP-T	SIA-IP (UDP-2012)	Standard	155	C.ID-IP 256b	C.ID-IP Encrypt-256	Encrypted
147	C.ID-UDP-T	CID-IP (UDP-2012)	Standard	192	TCPIP	Tecnoalarm TCPIP	Encrypted
148	SIA-UDP-T 128b	SIA-IP Encrypt-128 (UDP-2012)	Encrypted	210	eMail Tecno	Tecnoalarm (eMail server)	Standard

4.6 - Events with obligation of notification

According to the standards EN 50131, the events with obligation of notification belonging to the categories intrusion, hold-up, failure and tamper must be associated to a channel which is programmed with a telephone number.



The events with obligation of notification are indicated by this symbol in the table below.

Transmittable events							
	Beginning of alarm zone 1-42		Tamper alarm serial devices lost		Hold-up code		Event download request
	End of alarm zone 1-42		End of tamper alarm serial devices lost		Confirmation of disarming		Code denied
	Beginning of alarm program 1-8		Failure serial devices		Panic		Timer reset
	End of alarm program 1-8		End of failure serial devices		Beginning of antijamming alarm		Other events
	Arming program 1-8		Low battery		End of antijamming alarm		Test call 1
	Disarming program 1-8		Battery restore		Beginning of supervision alarm		Test call 2
	By-pass program 1-8		Power failure		End of supervision alarm		
	End of by-pass program 1-8		Mains restore		Cut telephone line		
	Exclusion/Isolation zone		Wrong password		Telephone line ok		

4.7 - Notification requirements

The standard EN 50131-1 defines for each security grade the type of warning device (WD) and alarm transmission equipment (ATE) required.

The alarm transmission equipment (ATE) provided for TP10-42 EN is composed of an on-board PSTN interface and optional GSM 2G, GSM 3G and IP interfaces. For compliance with security grade 2, the alarm system must be equipped with either a SP2, SP3 or DP1 class alarm transmission equipment.

The below table (taken from the standard EN 50131-1 annex A2) shows the provisions for security grade 2. It is possible to apply one of the indicated options (A, B, C or D).

Table C Notification equipment	Security grade 2			
	Possible options: A, B, C, D			
	A	B	C	D
Acoustic warning device with external power supply	2*	Op.	Op.	Op.
Acoustic self-powered warning device	Op.	1*	Op.	Op.
Alarm transmission equipment	SP2	SP2	DP1	SP3
* Required minimum number.				
Legend: Op. - optional SPx (Single path) - Value which indicates the performance level achieved by the single vector, according to the standard EN 50136-1 DPx (Dual path) - Value which indicates the performance level achieved by a combination of two vectors, according to the standard EN 50136-1				

Restrictions on notification

The delay of notification of intrusion, hold-up, tamper for more than 10 seconds it is not permitted.

The failure of a power supply must be notified with a delay of maximum 1 hour (EN 50131-3 annex B).

N.B. The remote management software and the connections through PC and software are not covered by the certification.



4.8 - Zone input programming

In compliance with the standards EN 50131, the following provisions concerning the zone inputs are mandatory:

Input filter

The input filter (minimum time of persistence of the alarm condition) must be minimum 50ms and maximum 400ms.

Hold-up zone

It is not allowed to program the number of activations or the alarm cycles for the inputs programmed as hold-up zones (infinite cycles).

It is mandatory to associate a hold-up zone to a channel programmed with a telephone number.

N.B. A hold-up alarm information is hidden (the console displays "Info available") and will only be available upon entering of a valid code.

Technical zone

The zone inputs programmed as technical zones are not covered by the certification.

Key zone

It is not permitted to program the inputs of the control panel as key zones (setting in conflict with the standard EN 50131-3).

NO/NC zone

It is not permitted to program the inputs of the control panel as normally open (NO) or normally closed (NC) (setting in conflict with the standard EN 50131-3).

Anti-tamper protection

All the options which involve disabling of the tamper protection are in conflict with the standards EN 50131.

4.9 - Power supply

Primary supply - Power supply

The power supply of the control panel complies with the provisions of the standard EN 50131-6 and performs the following controls imposed by the standard:

- Every 24h the status of the alternative power supply (APS) is checked. The battery test is executed under load.
In the absence of mains voltage the test is not executed.
- Every 10 seconds the output voltage is checked.
- The battery is disconnected if voltage drops below 8.8V (protection against the deep discharge).

N.B. All the functions listed are subject to the status of the W1 jumper on the CPU board (must be open).

Secondary supply - Battery

The control panel must be equipped with a battery with 12V/12Ah capacity.

Autonomy

The below table shows the provisions regarding autonomy defined by the standard EN 50131 security grade 2 for non-remotely managed functioning.

In particular, it shows the distribution of the available current:

Self consumption - Current needed for the CPU board

Recharge current - Current needed for recharge of the battery within the charging time imposed by the standard

Load current - Total current available for the devices connected to the control panel (e.g. consoles, detectors, outdoor sirens)

The total consumption of all connected devices must be less than the available current (850mA).

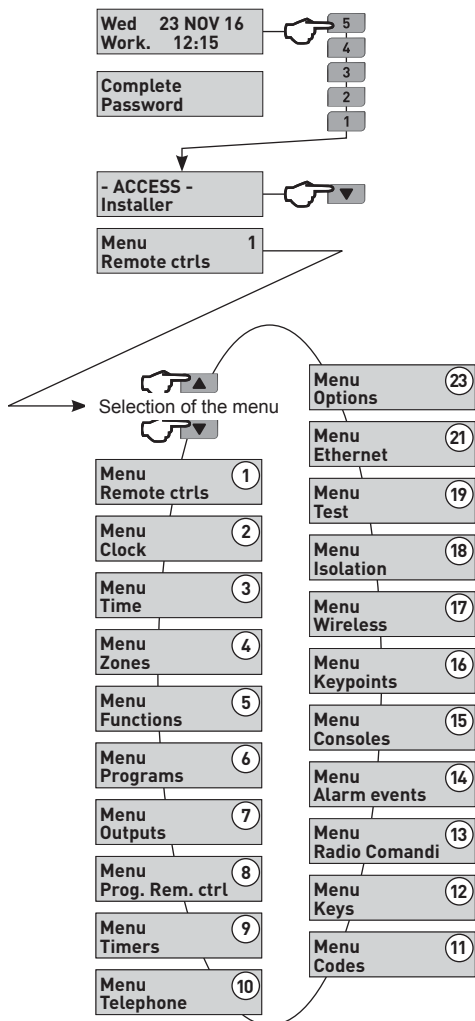
Autonomy						
TP10-42 EN			12V/12Ah battery			
			Autonomy required	Self consumption	Recharge current	Load current
Security grade 2	non-remotely managed system		12 heures	Max. 150mA	850mA*	850mA
* Charging time: approx. 20 hours (80% required in 72 hours)						

5 - PROGRAMMING BY CONSOLE

5.1 - Programming menu

Access to the programming menu is given only to the installer.

The access can be made from any console and automatically inhibits all the other consoles connected to the control panel.



Access to the programming menu

Follow the below procedure

- 1 - Enter the installer code
- 2 - Select the programming menu
- 3 - Confirm the selection with the YES key

N.B. The default installer code of TP10-42 is a 5-digits code (54321), whereas that of TP10-42 EN is composed of 6 digits (654321).

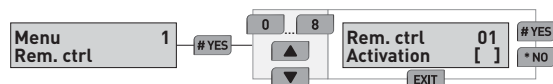
Menu selection

Each menu is identified by a name viewed in the second line and by a number viewed in the first line on the right (see beside figure).

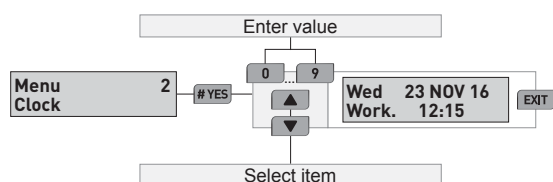
The menu can be selected either by scrolling the list with the arrow keys or by entering the menu number.

5.2 - Menu guide

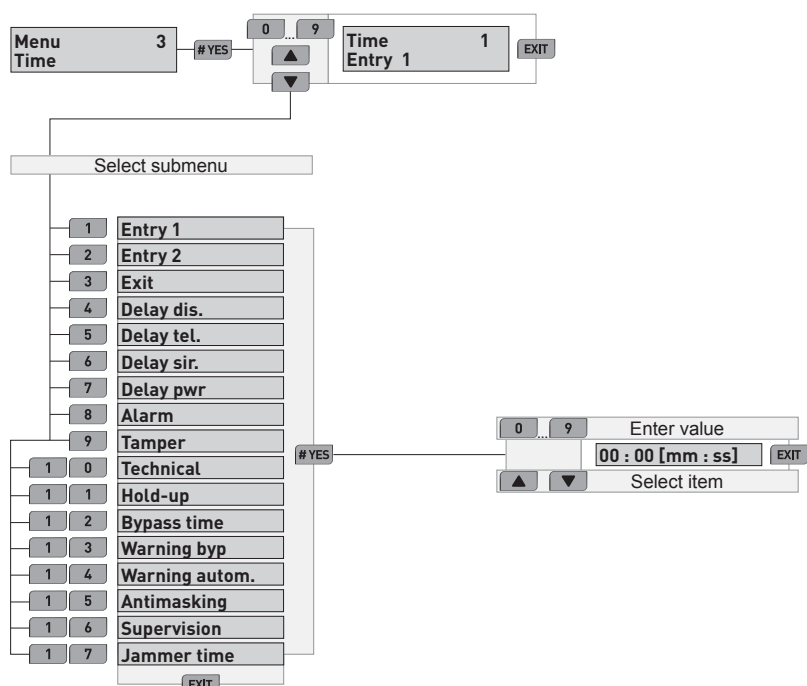
Menu Rem. ctrl 1	The menu permits the activation and deactivation of the remote controls. Select the remote control and press the YES key to activate or the NO key to deactivate it.			
1 Remote control 01	3 Remote control 03	5 Remote control 05	7 Remote control 07	
2 Remote control 02	4 Remote control 04	6 Remote control 06	8 Remote control 08	



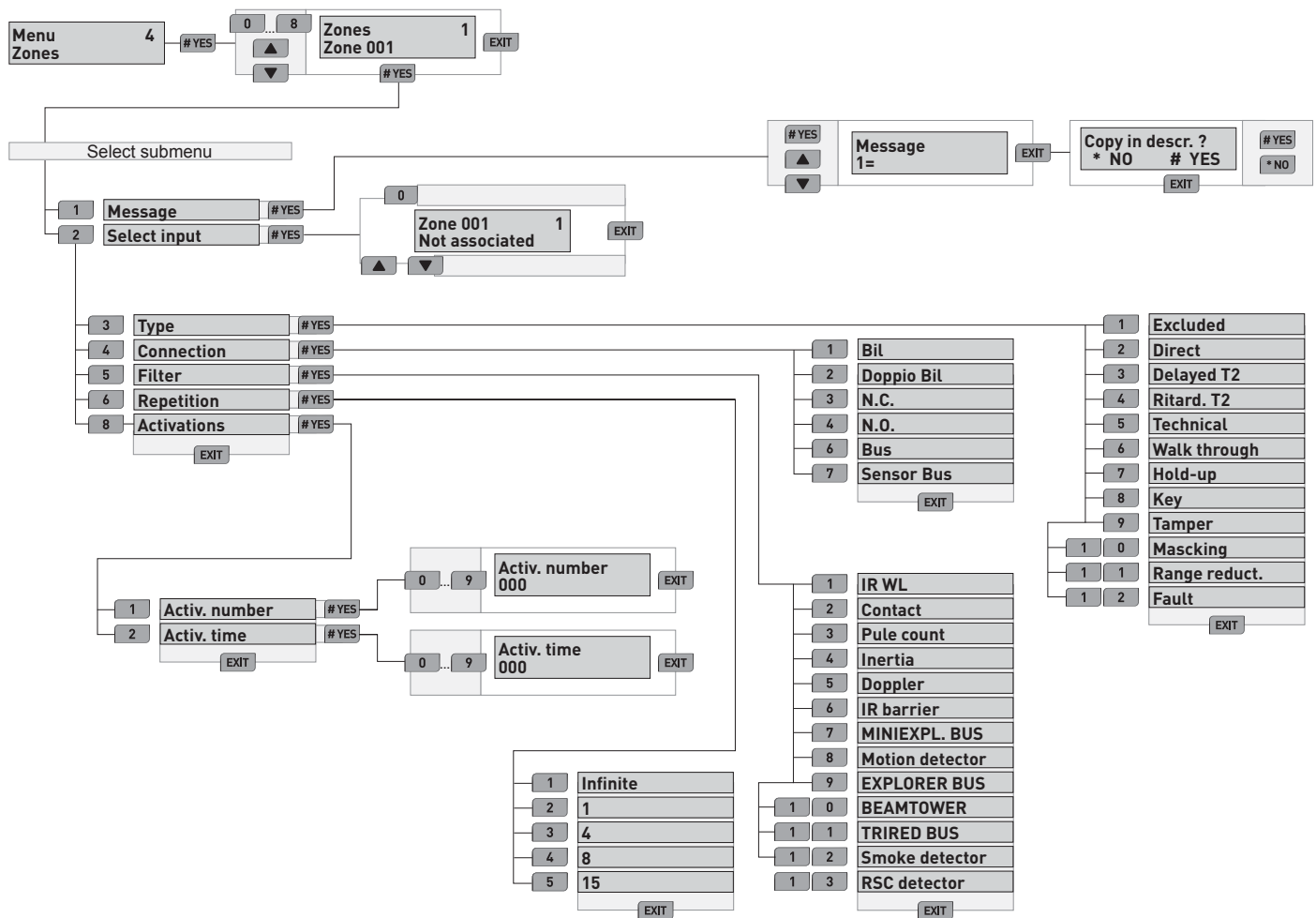
Menu Clock 2	The menu permits setting of the date and time of the system. The date is viewed in the format DD MMM YY, the time is viewed in the format HH:MM. Select the item to be programmed with the arrow keys and program the value with the number keys.			
---------------------	---	--	--	--



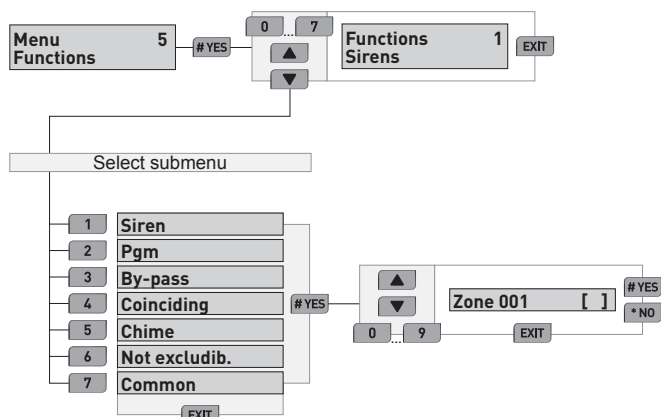
Menu Time 3	The menu permits programming of the time parameters that are valid for all programs. N.B. The parameters entry time, exit time, disarming delay, siren activation delay and alarm time can be programmed specifically for each program in the program menu.			
1 Entry time 1	6 Siren activation delay	11 Hold-up alarm delay	16 Supervision intervall	
2 Entry time 2	7 Power failure alarm delay	12 Maximum by-pass time	17 GSM jammer alarm delay	
3 Exit time	8 Alarm time	13 End-of-by-pass warning		
4 Disarming delay	9 Tamper alarm time	14 Automatic arming warning		
5 Channel activation delay	10 Technical alarm time	15 Antimasking alarm delay		



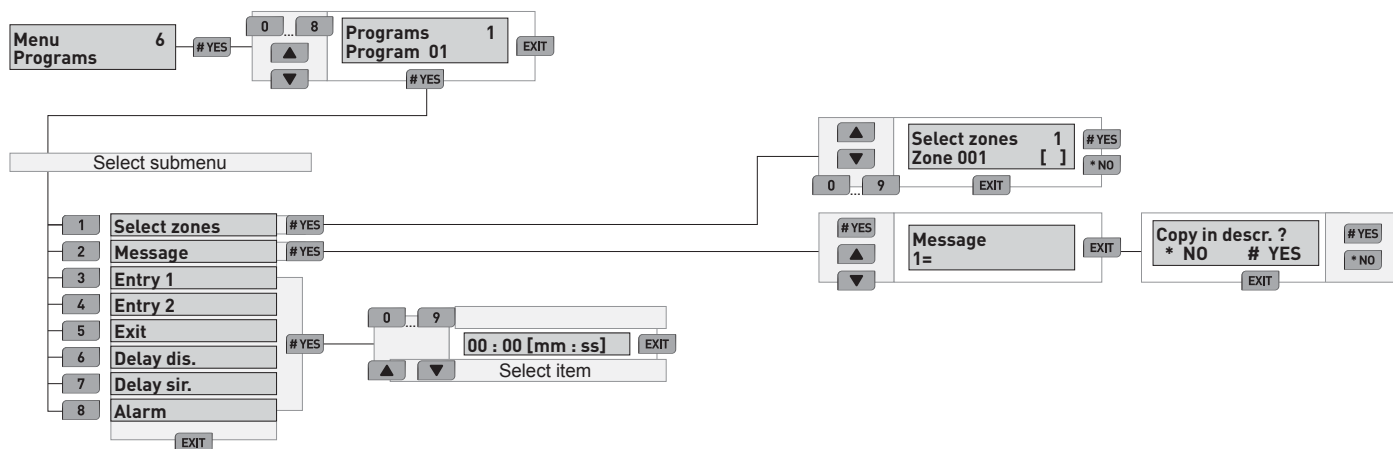
Menu Zones 4		The menu permits programming of the zones, i.e. association of a description, association of the physical input, setting of the other features. The submenus available depend on the previous choices.			
1	Description	3	Zone type	5	Filter
2	Zone-input association	4	Contact type	6	Alarm repetitions (cycles)
				8	Number of activations



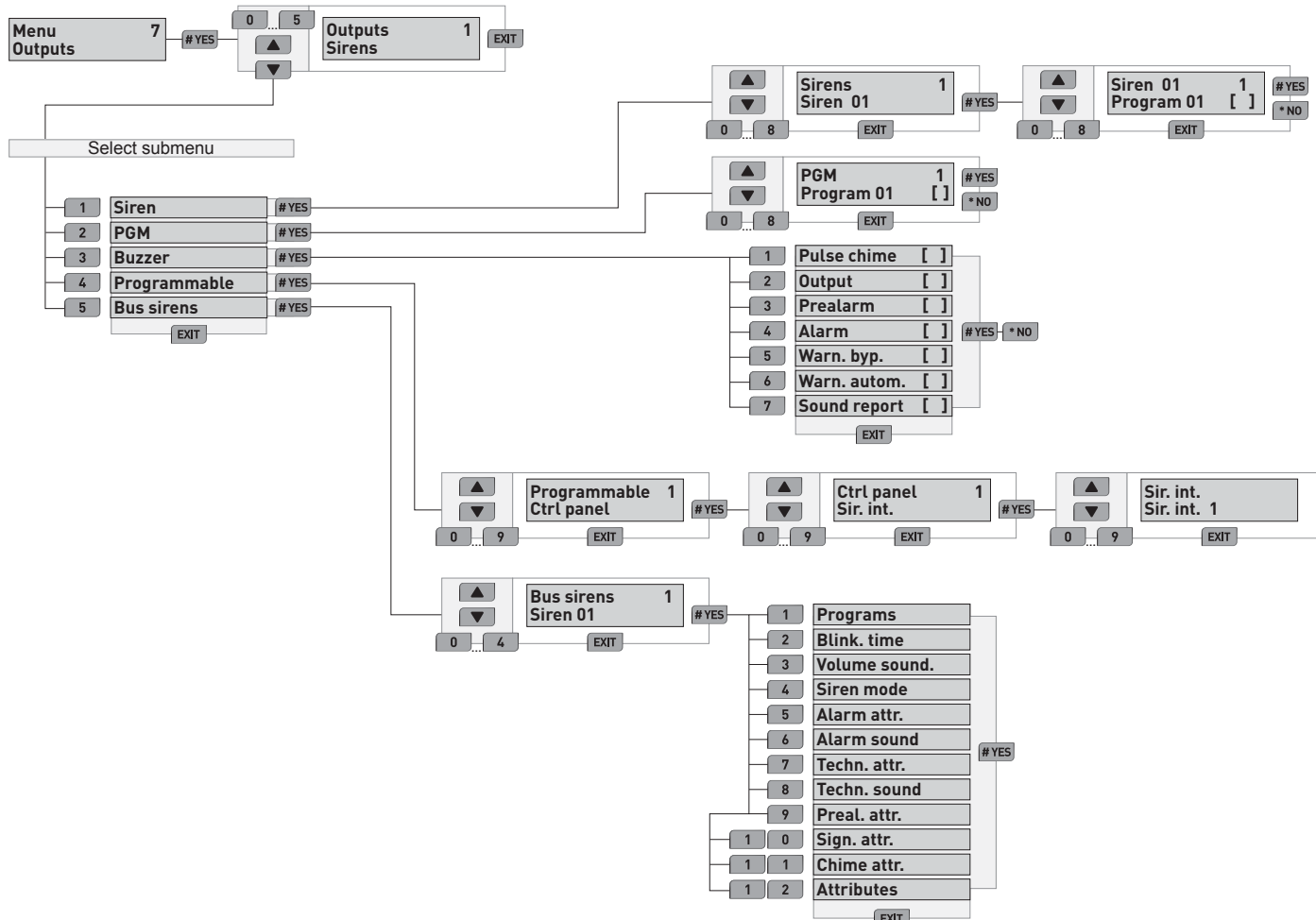
Menu Functions 5		The menu permits the association of the functions to the zones.			
1	Siren (opening activates siren)	3	By-pass (can by-passed)	5	Chime (opening activates chime)
2	PGM (opening activates outputs)	4	Coinciding (linked to other zone)	6	Not excludible (cannot be excluded)
				7	Common (included in >1 program)



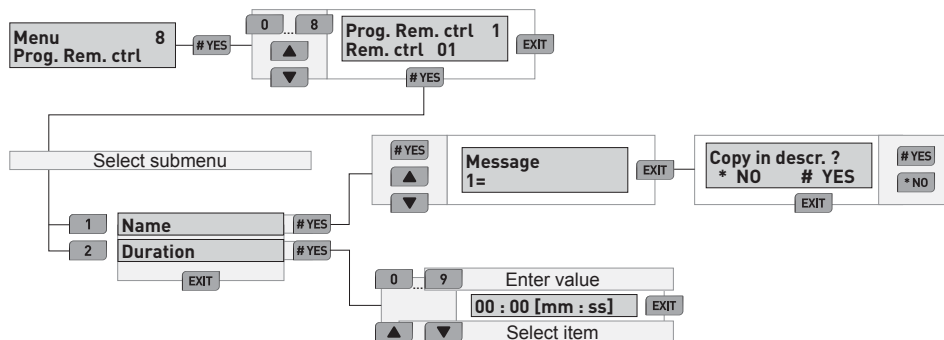
Menu Programs 6		The menu permits programming of the programs, i.e. association of a descriptor, of the zones and the functions. In addition, it is possible to program the time parameters entry time, exit time, disarming delay, siren activation delay and alarm time specifically for each program.					
1	Zone association	3	Entry time 1	5	Exit time	7	Siren activation delay
2	Description	4	Entry time 2	6	Disarming delay	8	Alarm time



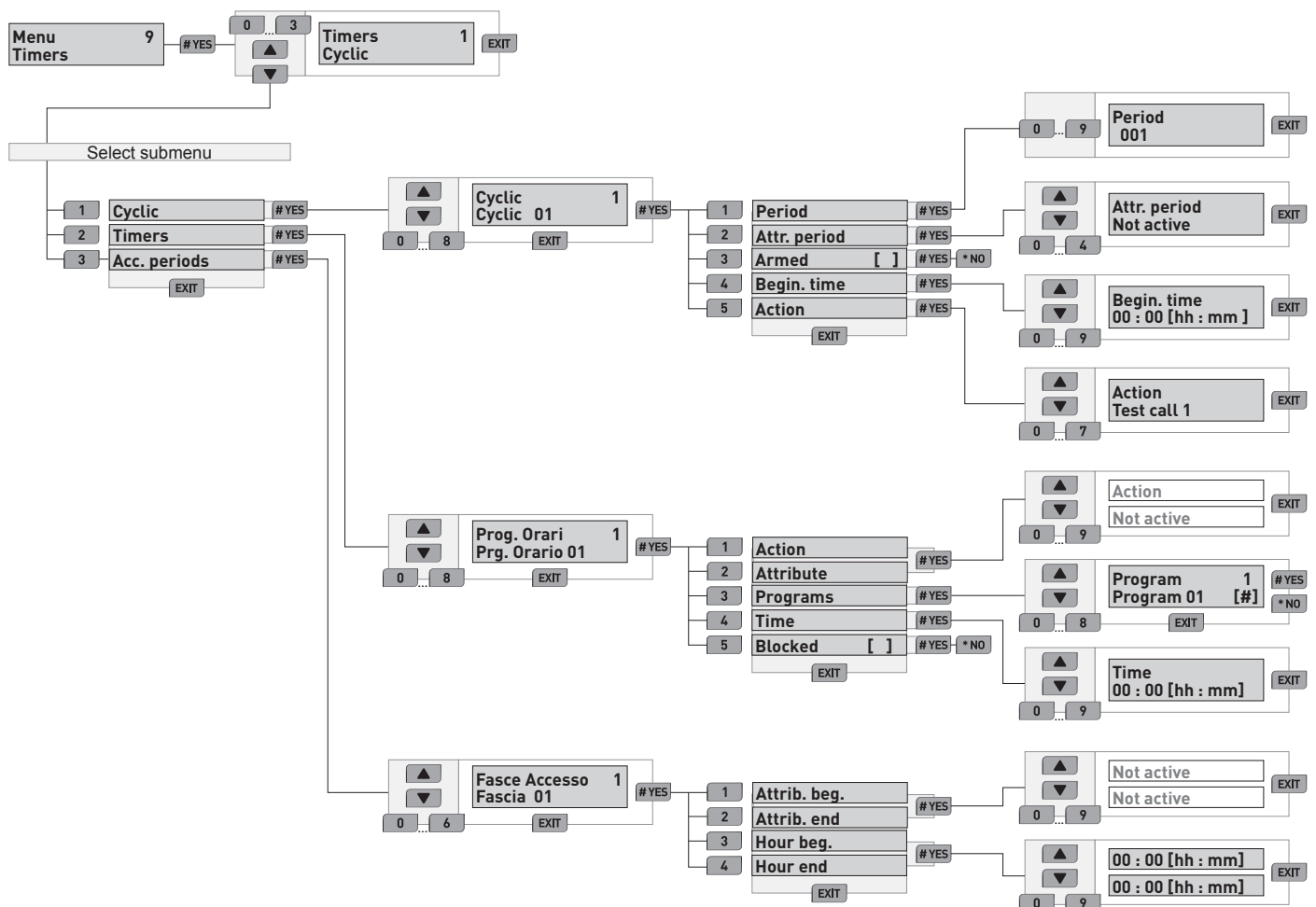
Menu Outputs		7		The menu permits the configuration of the outputs, i.e. association of the siren and PGM outputs to the programs, configuration of the buzzer, configuration of the programmable outputs of the control panel and the expansion modules and programming of the bus sirens.	
1	Siren-program association		3	Buzzer configuration	
2	PGM-program association		4	Programmable outputs	
			5	Bus sirens	



Menu Prog. telec.	8 The menu permits programming of the remote controls, i.e. the association of a description and the activation time.
1 Description	2 Activation time



Menu Timers9		The menu permits programming of the cyclic timers, timers and access periods.	
1	Cyclic timers	2	Timers
3	Access periods		



```

graph TD
    Menu[Menu Telephone 10] -- "# YES" --> Select[Select submenu]
    Select --> Settings[1 Settings # YES]
    Select --> PSTN[2 PSTN # YES]
    Select --> GSM[3 GSM # YES]
    Select --> TECNOCELL[4 TECNOCELL # YES]
    Select --> ChannelA[5 Channel A]
    Select --> ChannelB[6 Channel B]
    Select --> ChannelC[7 Channel C]
    Select --> GPRS[8 GPRS Enab. [#] # YES]
    Select --> ChannelE[9 Channel E]
    Select --> ChannelF[1 0 Channel F]
    Select --> ChannelG[1 1 Channel G]
    Select --> ChannelH[1 2 Channel H]
    Select --> CallBack[1 3 Call back]
    Select --> Exit1[EXIT]

    Settings --> Answer[1 Answer [#] # YES * NO]
    Settings --> Pulses[2 Pulses [ ] # YES * NO]
    Settings --> LineTest[3 Line test # YES]
    Settings --> DialTone[4 Dial tone [#] # YES * NO]
    Settings --> Rings[5 Rings 0 9]
    Settings --> PABX[6 PABX # YES 0 9]
    Settings --> Exit2[EXIT]

    Answer --> Disabled[1 Disabled]
    Answer --> AlwaysActive[2 Always active]
    Answer --> IfPArmed[3 If P armed]
    IfPArmed --> Exit3[EXIT]

    GlobalBlock[1 Global block [ ]]
    GlobalBlock --> VocalBlock[2 Vocal block [ ]]
    GlobalBlock --> DigitBlock[3 Digit. block [ ]]
    GlobalBlock --> TecnoBlock[4 Tecno block [ ] # YES * NO]
    GlobalBlock --> OpeningMsg[5 Opening msg [#]]
    GlobalBlock --> RingBack[6 Ring back [#]]
    GlobalBlock --> CtrlNotify[8 Ctrl notify [ ]]
    CtrlNotify --> Exit4[EXIT]

    Enabled[1 Enabled [ ] # YES * NO]
    Answer2[2 Answer [#] # YES * NO]
    Rings2[3 Rings # YES 0 9]
    CreditNo[4 Credit no. # YES 0 9]
    EnabCredSMS[5 Enab.cred.SMS [ ] # YES * NO]
    ProgCredSMS[6 Prog.cred.SMS # YES]
    ProgSMSHeading[7 Prog.SMS heading]
    GPRSEnab[8 GPRS Enab. [#] # YES * NO]
    GPRSPort[1 0 GPRS port # YES 0 9]
    PAccessPoint[1 1 P. access point]
    PUserName[1 2 P. user name]
    PPassword[1 3 P. password]
    SMSRemCtrl[1 4 SMS rem. ctrl [ ] # YES * NO]
    SMSPassword[1 5 SMS password # YES]
    SMSWhitelist1[1 6 SMS whitelist 1]
    SMSWhitelist2[1 7 SMS whitelist 2]
    SMSWhitelist3[1 8 SMS whitelist 3]
    JDRJamDetect[1 9 JDR jam detect # YES]
    AirtimeControl[2 0 Airtime control [ ] # YES * NO]
    AirtimeLimit[2 1 Airtime limit # YES 0 9]
    SearchString[2 2 Search string # YES]
    RechargeMessage[2 3 Recharge message]
    WDSNetwork[2 4 WDS network # YES]
    WDSNetwork --> Exit5[EXIT]

    Waiting1[Waiting]
    Completed1[Completed]
    Completed1 --> Exit6[EXIT]

    Waiting2[Waiting]
    Completed2[Completed]
    Completed2 --> Exit7[EXIT]

    Waiting3[Waiting]
    Completed3[Completed]
    Completed3 --> Exit8[EXIT]

    OnlyStored[1 Only stored]
    FaultReports[2 Fault reports]
    TamperReports[3 Tamper reports]
    Disabled2[4 Disabled]
    Disabled2 --> Exit9[EXIT]

    Automatique[1 Automatique]
    2G[2 2G]
    3G[3 3G]
    2G3G[4 2G / 3G]
    2G3G --> Exit10[EXIT]

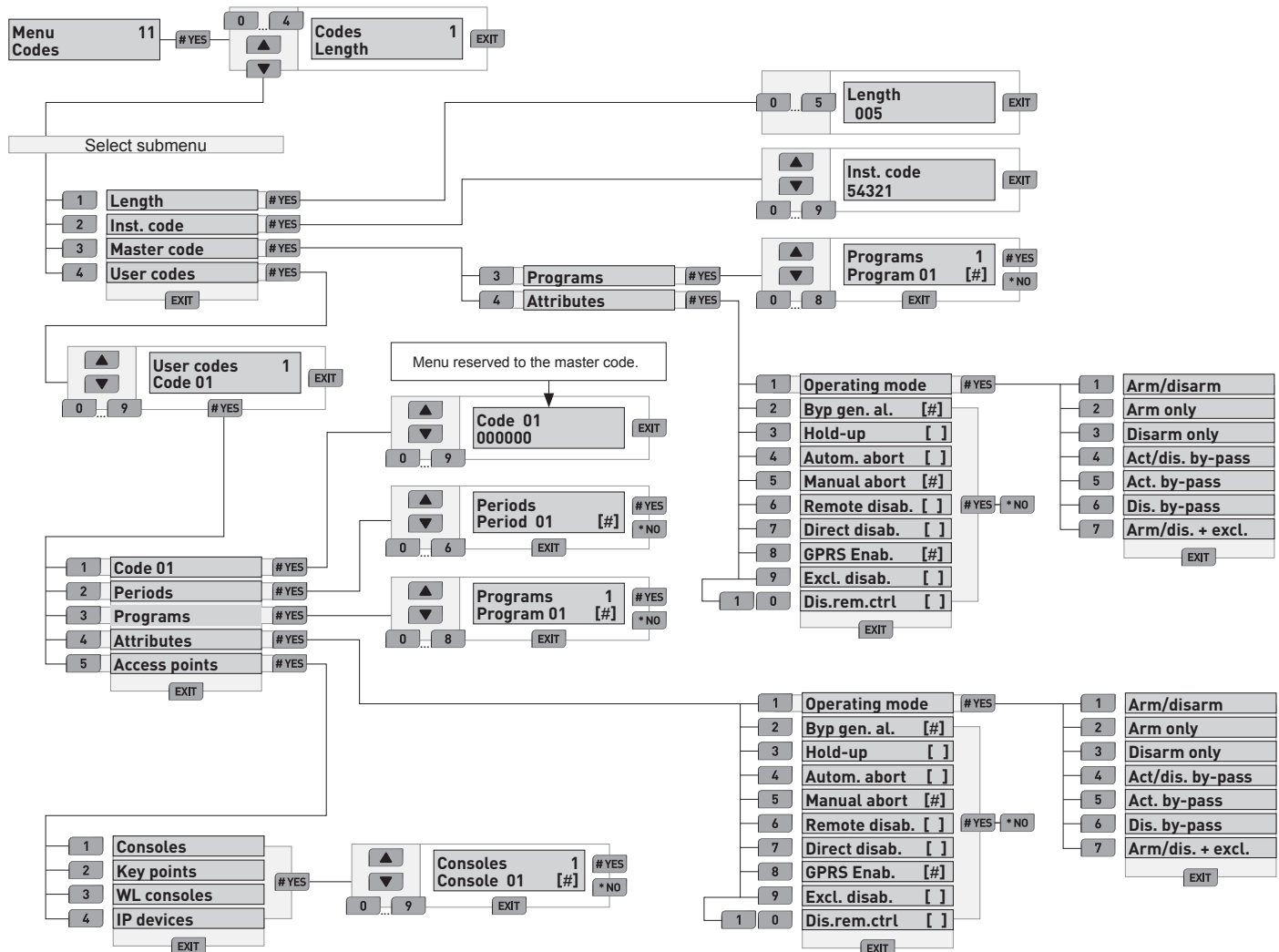
    Enabled3[1 Enabled [ ] # YES * NO]
    Reponse[2 Reponse [ ] # YES * NO]
    Rings3[3 Rings # YES 0 9]
    EmergencyMsg[4 Emergency msg # YES 1 4]
    EmergencyNo[5 Emergency no. # YES 0 9]
    AnswViaBUS[6 Answ. via BUS [#] # YES * NO]
    EnabEmerSMS[7 Enabl.emer.SMS [ ] # YES * NO]
    ProgEmerSMS[8 Prog. emer. SMS # YES]
    EnablDigit[9 Enabl. digit. [ ] # YES * NO]
    EnablDigit --> Exit11[EXIT]

    Waiting4[Waiting]
    Completed4[Completed]
    Completed4 --> Exit12[EXIT]

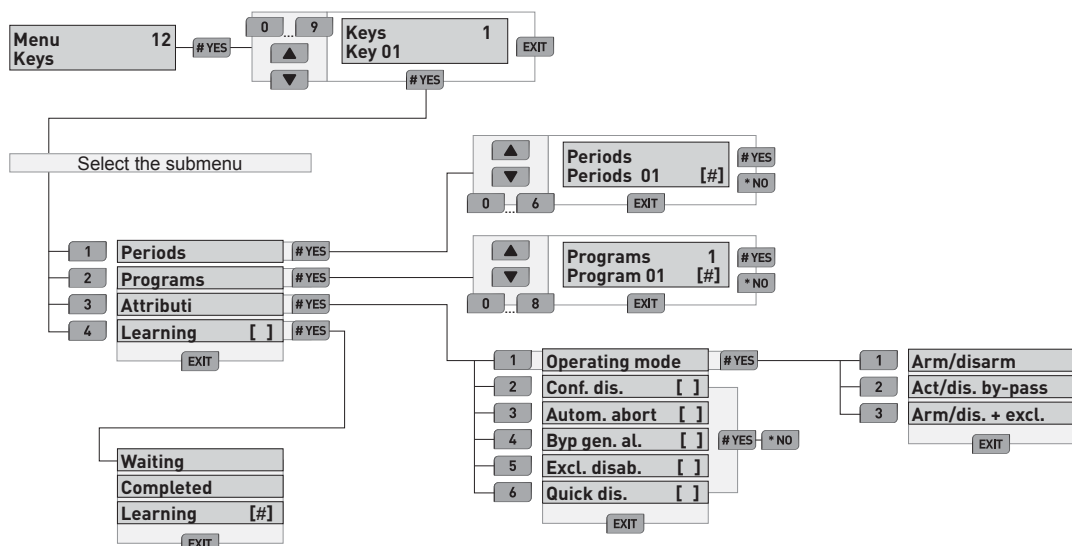
    FirstNumber[1 First number]
    SecondNumber[2 Second number]
    ID[3 ID]
    Format[4 Format]
    TestCall[5 Test call]
    TestCall --> Exit13[EXIT]
  
```



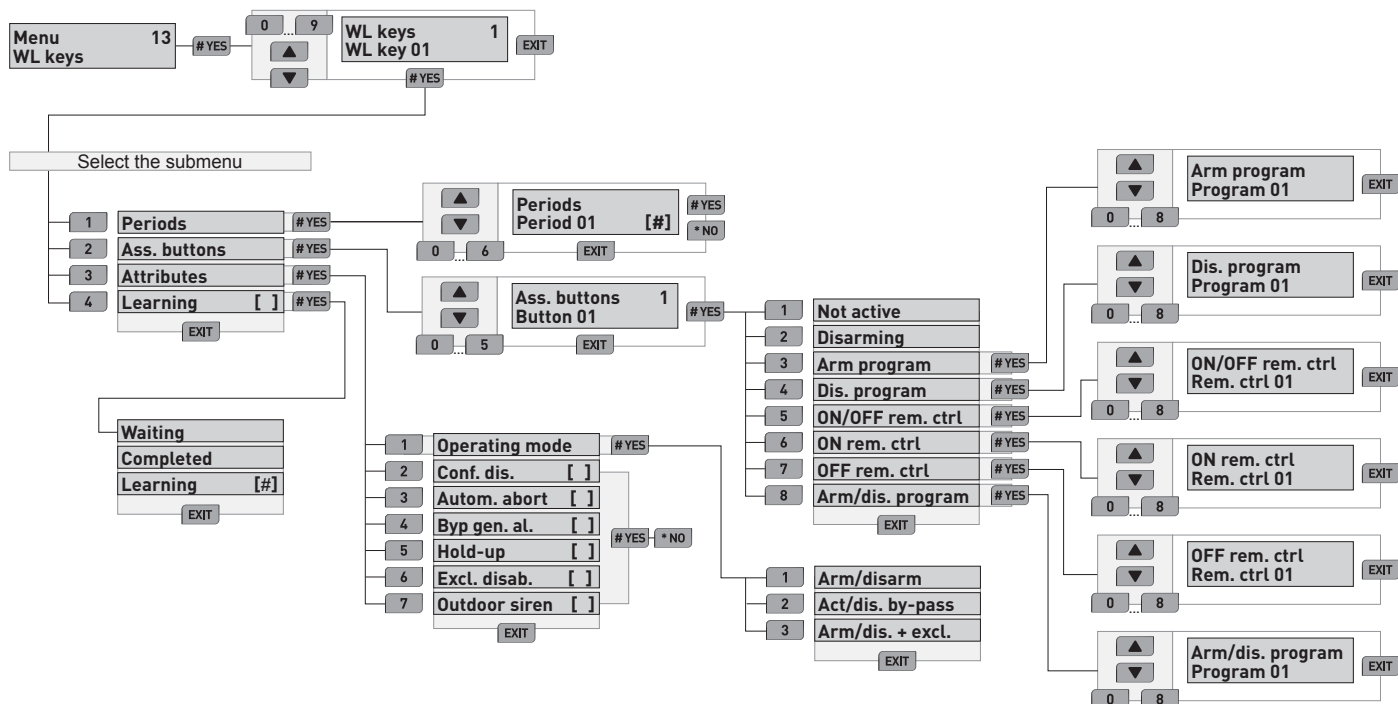
Menu Codes	11	The menu permits setting of the length of all the access codes and programming of the codes (installer, master and standard user), i.e. programming of the values, functions and attributes as well as association of the programs and access periods.	
1	Code length	3	Master code
2	Installer code	4	User codes



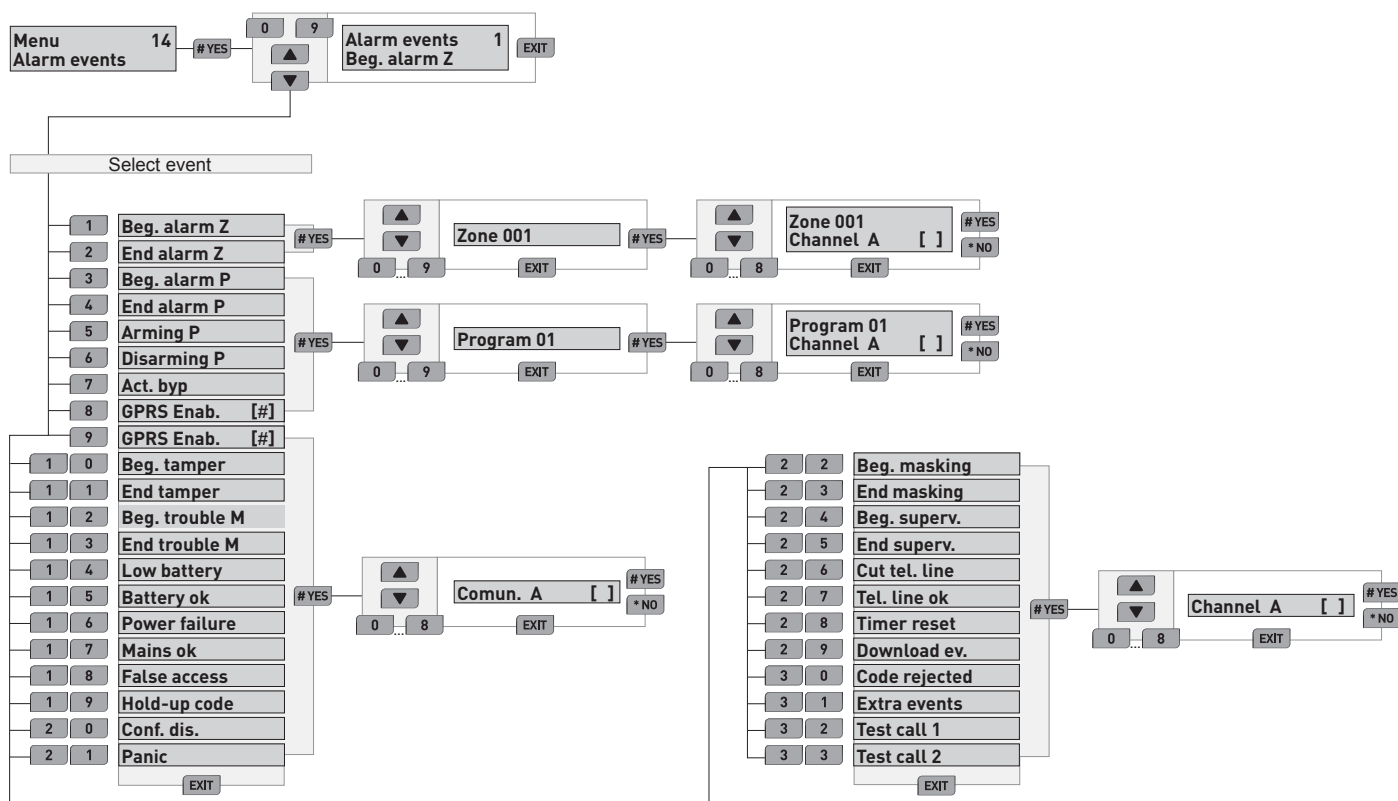
Menu Keys	12	The menu permits programming of the keys, i.e. programming of the functions and attributes, association of the programs and access periods as well as learning of the keys.	
1	Association of access periods	3	Attributes
2	Association of programs	4	Learning



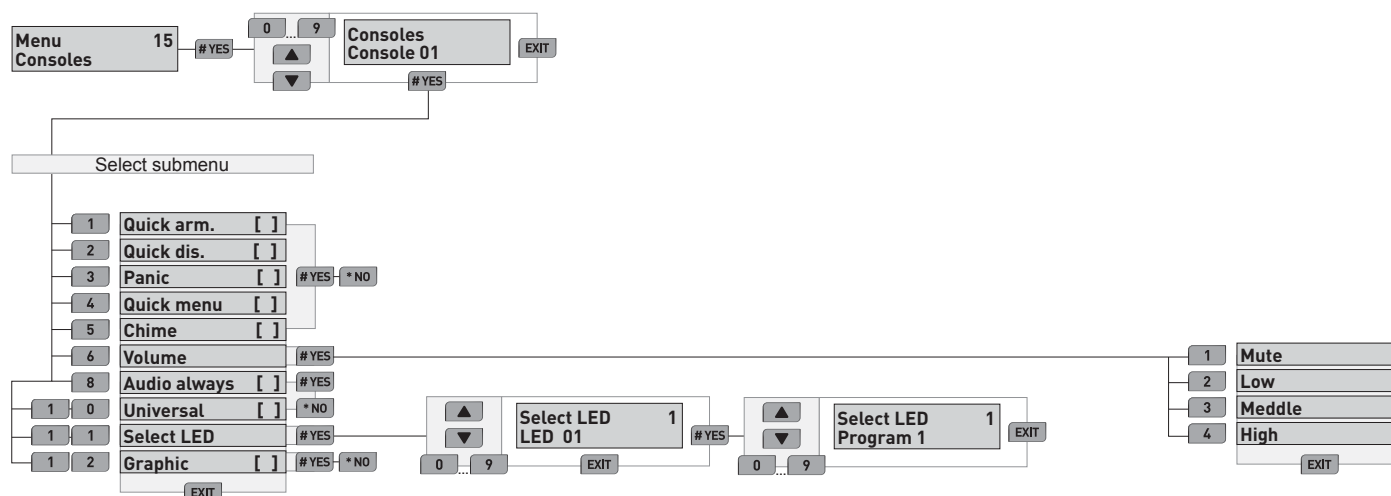
Menu WL keys	13	The menu permits programming of the wireless keys, i.e. programming of the attributes and function keys, association of the access periods as well as learning of the wireless keys.	
1	Association of access periods	3	Attributes
2	Function keys	4	Learning



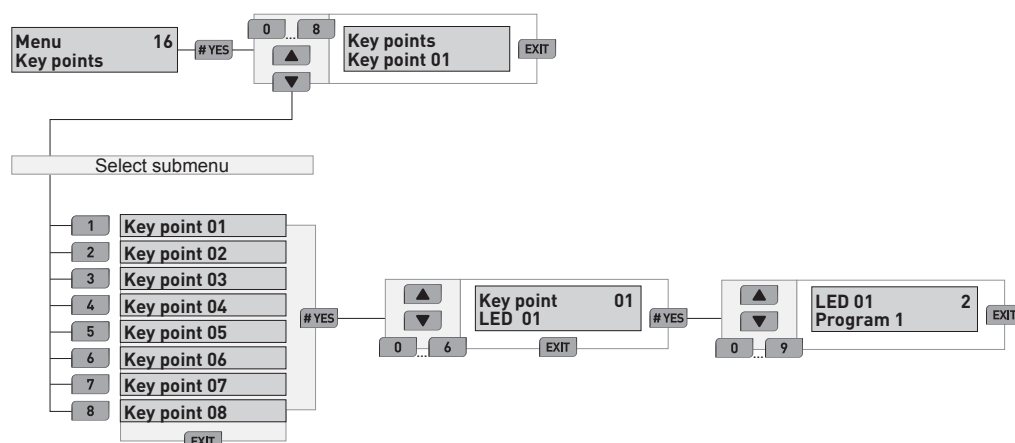
Menu Alarm events	14	The menu permits the association of the events to the channels (A to H) for notification.	
1	Beginning of zone alarm	4	End of program alarm
2	End of zone alarm	5	Arming of programs
3	Beginning of program alarm	6	Disarming of programs
7	Activation of by-passv	8	Deactivation of by-pass
9	Exclusion of zones	10-21	General alarms



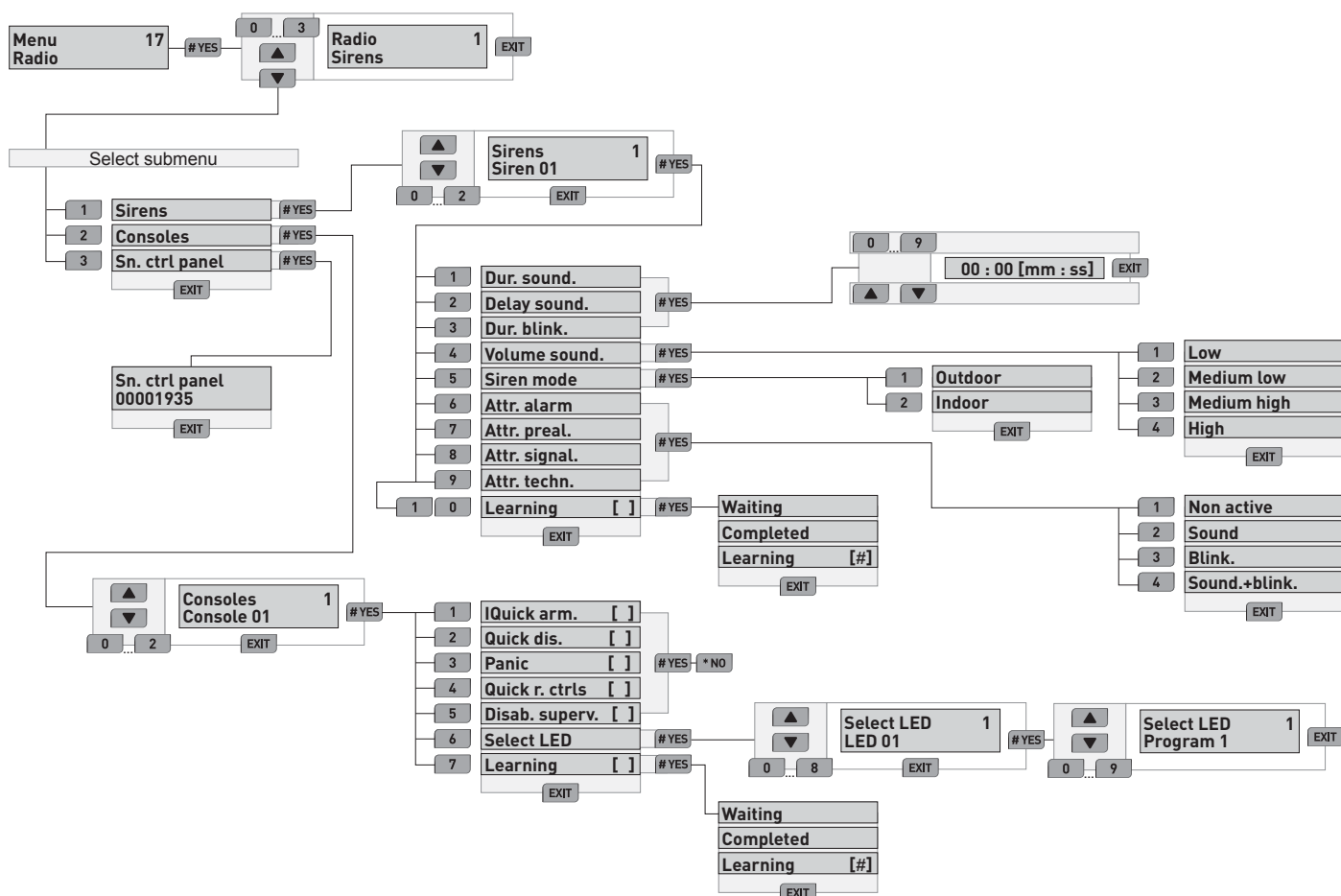
Menu Consoles		15		The menu permits programming of the consoles.			
1	Quick arming function	4	Quick menu	8	Audio always	12	Graphic display
2	Quick disarming function	5	Chime function	10	Universal (enabled for all programs)		
3	Panic function	6	Volume	11	Association of LED to programs		



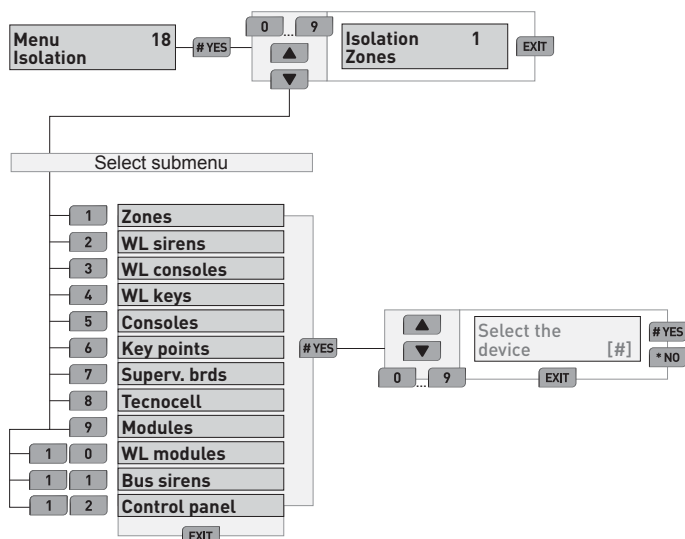
Menu Key points	16	The menu permits the association of the LED of the key points to the programs.
------------------------	-----------	--



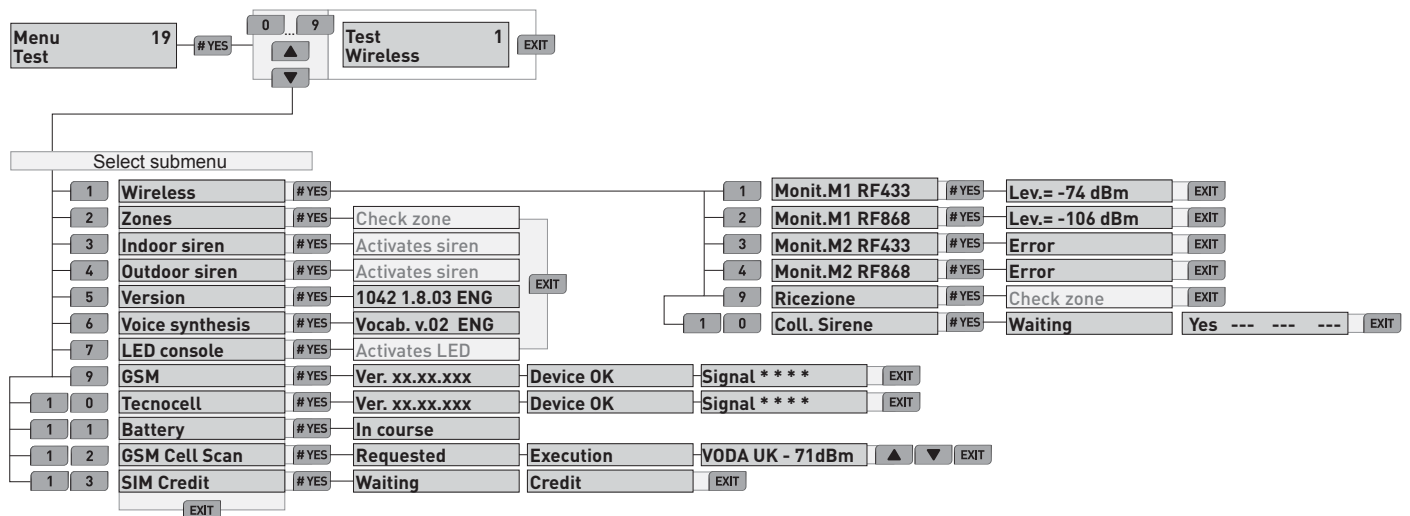
Menu Radio 17		The menu permits programming of the wireless sirens and consoles and viewing of the serial number of the wireless module.	
1	Wireless sirens	3	Viewing of serial number of the wireless module (needed for back-up/restore)
2	Wireless consoles		



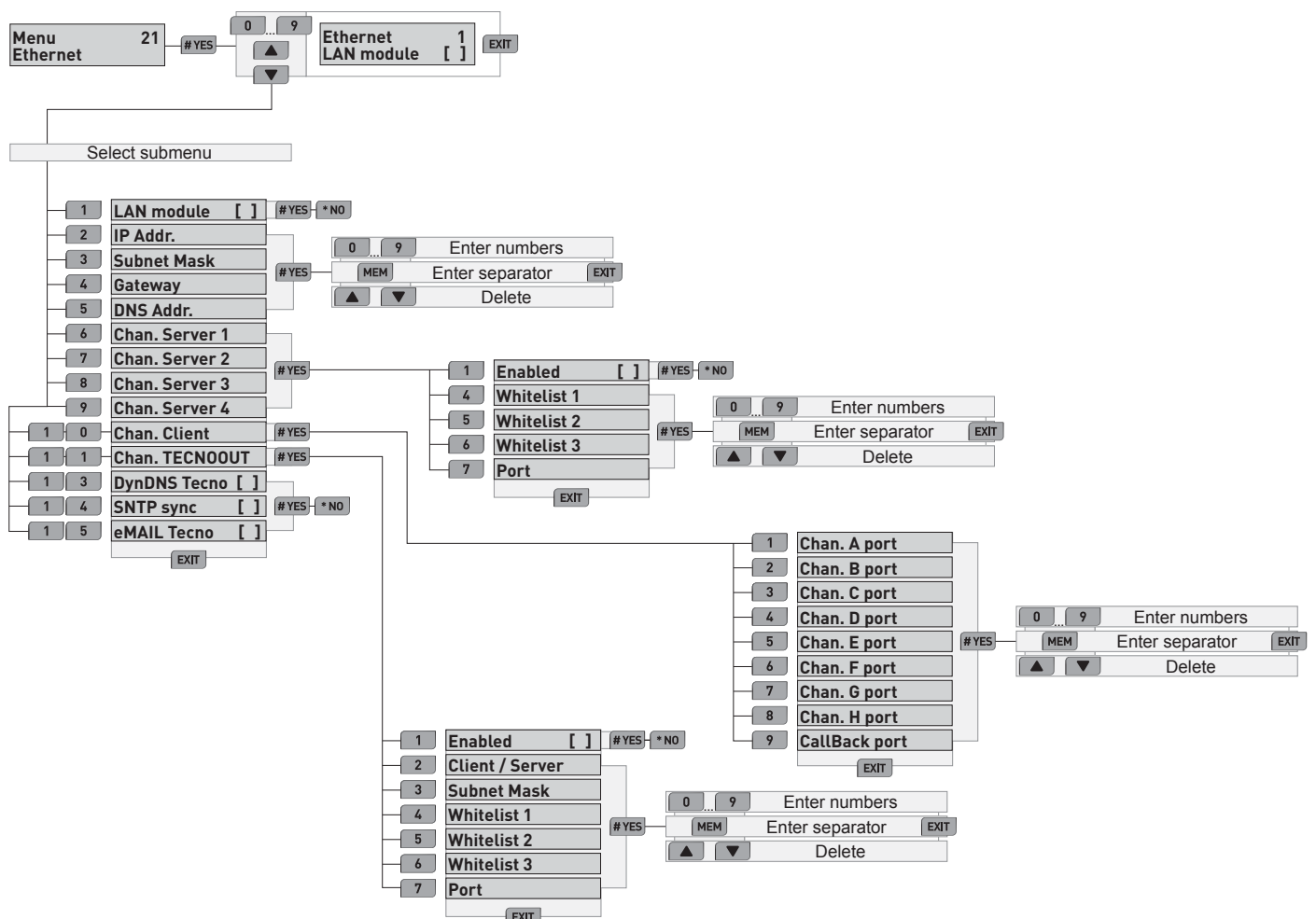
Menu Isolation 18	The menu permits the isolation, i.e. the permanent exclusion of the system components.		
1 Zone 001-042	4 WL key 01-80	7 LED signaling panel 01-16	10 WL module 01-02
2 WL siren 01-02	5 Console 01-08	8 Tecnocell	11 Bus siren 01-04
3 WL console 01-02	6 Key point 01-08	9 Expansion module 01-10	12 Outputs



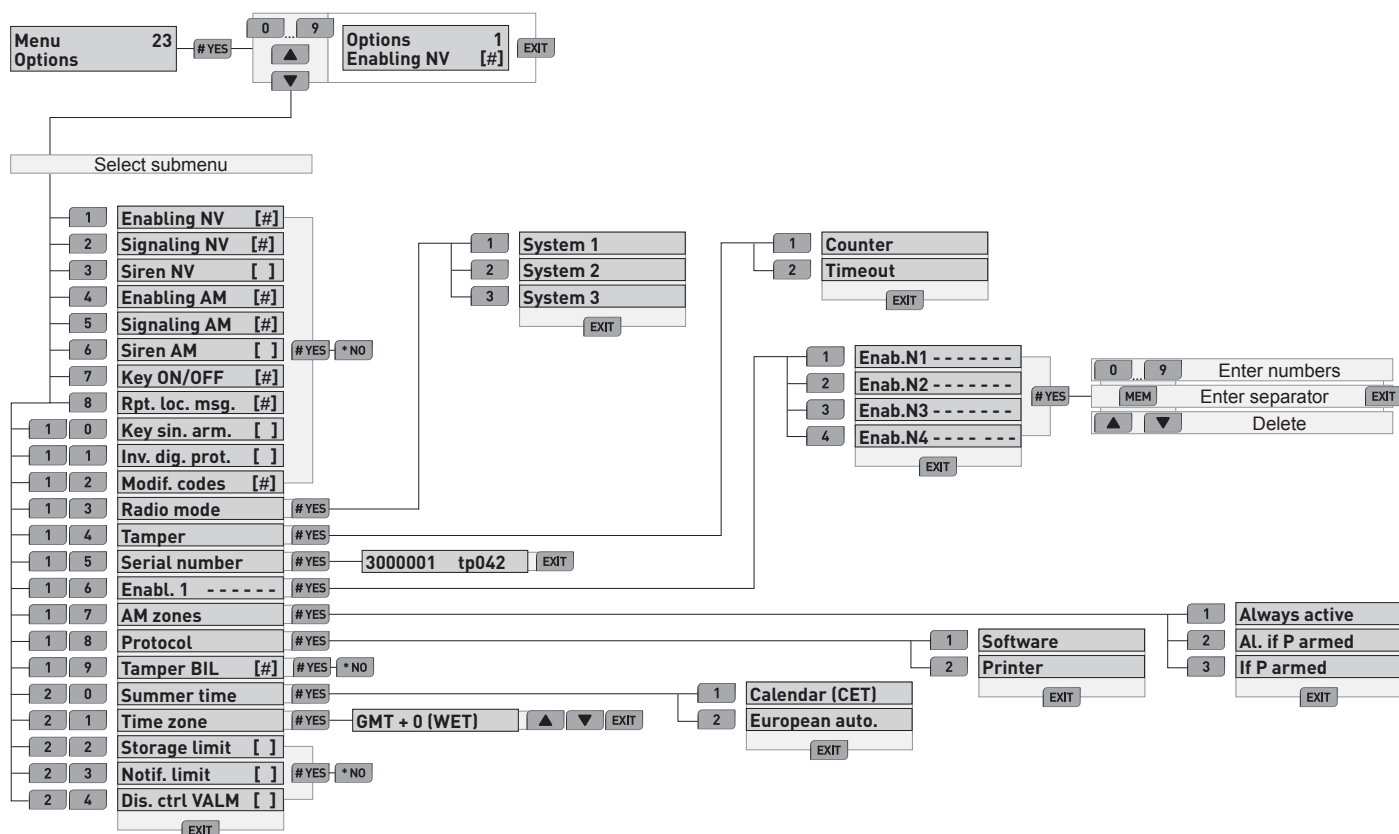
Menu Test 19	The menu performs the functioning tests and shows the firmware and vocabulary releases as well as the GSM functioning parameters.		
1 Test of wireless sirens	4 Test of outdoor sirens	7 Test of consoles	11 Test of battery
2 Test of hard-wired zones	5 Viewing of firmware release	9 Viewing of GSM parameters	12 Viewing of available GSM cells
3 Test of indoor sirens	6 Viewing of vocabulary release	10 Viewing of TecnoCell parameters	13 Viewing of SIM credit



Menu Ethernet 21	The menu permits programming of the Ethernet access parameters.		
1 Enabling of LAN module	4 Gateway	10 Client channel	14 Enabling of SNTP service
2 IP address	5 DNS address	11 Tecno Out channel	15 Enabling of eMAIL service
3 Subnet Mask	6 - 9 Server channels	13 Enabling of DDNS service	

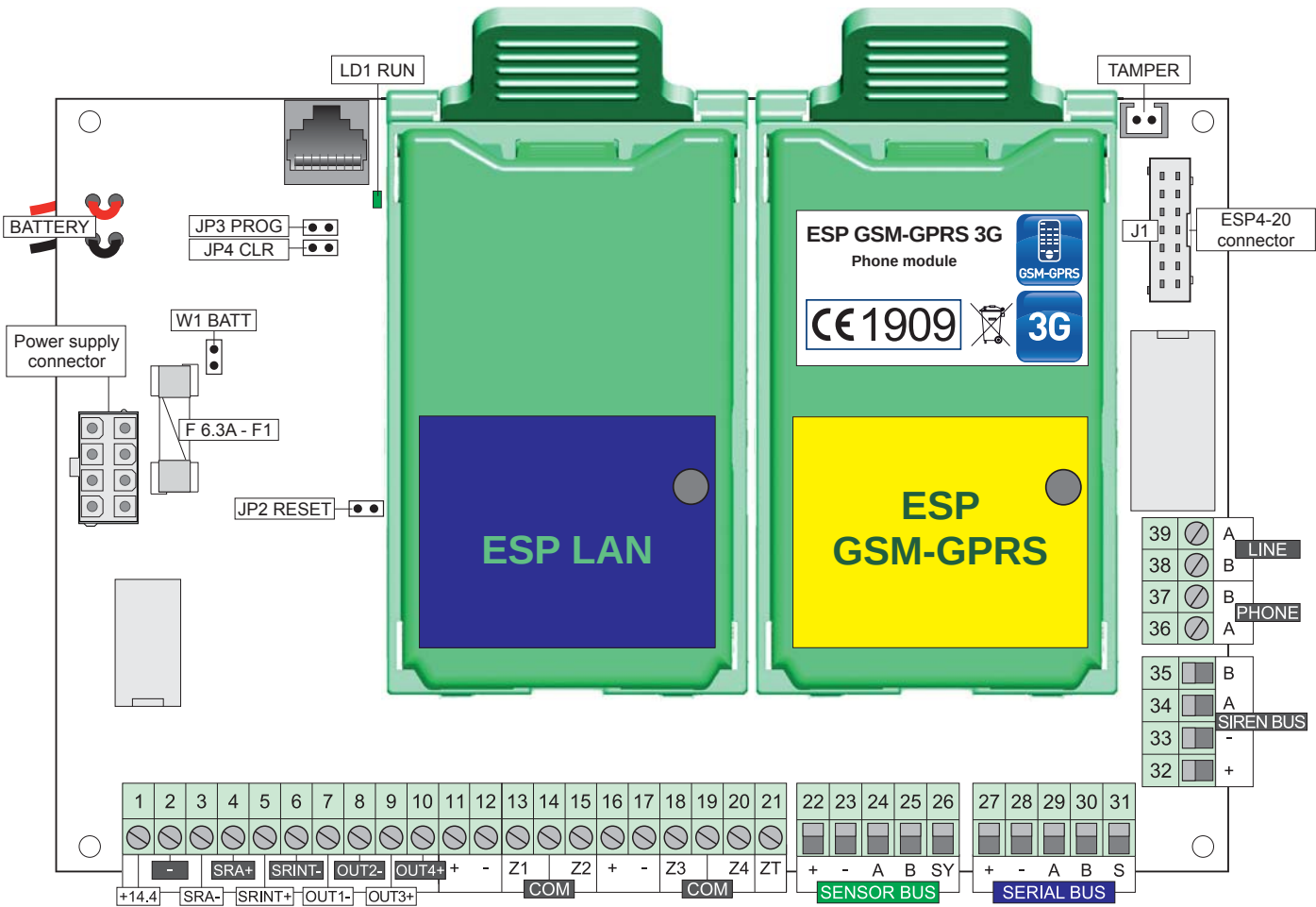


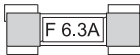
Menu Options 23		The menu permits programming of the options, e.g. anti-jamming and supervision control of the wireless section.			
1	Enabling of supervision control	7	On/off functioning of key zone	14	Automatic disabling of tamper
2	Signaling for supervision alarm	8	Voice synthesis	15	Viewing of serial number
3	Sirens for supervision alarm	10	Single arming with key	16	Software options
4	Enabling of jamming control	11	Inversion of report codes	17	Antimasking
5	Signaling for jamming alarm	12	Code management by user	18	Selection of protocol (SW/printer)
6	Sirens for jamming alarm	13	RF power setting (RTX200/433868)	19	BIL tamper input
				20	Daylight saving time
				21	Time zone
				22	Limitation of event registration
				23	Limitation of event notification
				24	Disabling of output voltage check



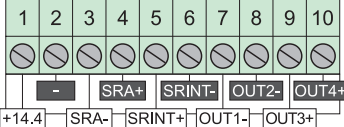
6 - HARDWARE

6.1 - CPU board

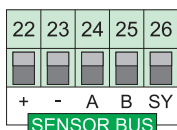


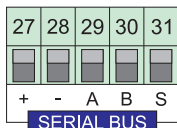
Protection against deep discharge and polarity reversal			
W1 - BATT		Automatic battery disconnection for Vbat <8.8V DC and protection against polarity reversal active	
		Protection against deep discharge and polarity reversal of battery deactivated	
Special procedures			
JP2 - RESET	Leave open during normal functioning (jumpers reserved for firmware update and reset of codes or system configuration)		
JP3 - PROG			
JP4 - CLR			
Tamper connector			
	Normal functioning	Connect prewired tamper contact (mandatory for TP10-42 EN)	
	Maintenance	Disconnect prewired tamper contact and insert jumper	
LED		Signaling	
	Green	Flashing	Normal functioning
	Fuse F1		
Protection of primary supply (F 6.3A)			
	Connector J1		
Connector for plug-in input expansion ESP2-40			

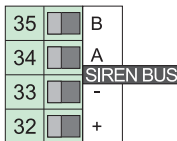
6.2 - Terminals

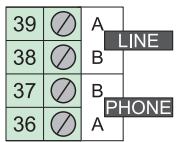
	Outputs			Signal	Max. current
	1	+14,4	Positive recharge power for self-powered siren	+14.4V DC	750mA*
	2	-	Negative voltage	-	
	3	SRA-	Negative reference voltage for self-powered siren	-	
	4	SRA+	Positive control voltage for self-powered siren	+13.8V DC	750mA
	5	SRINT+	Positive control voltage for indoor siren	+13.8V DC	500mA
	6	SRINT-	Negative reference voltage for indoor siren	-	
	7	OUT1-	Negative logic output (programmable logic)	- / O.C.	100mA
	8	OUT2-	Negative logic output (programmable logic)	- / O.C.	100mA
	9	OUT3+	Positive logic output (programmable logic)	+ / O.C.	300mA
	10	OUT4+	Positive logic output (programmable logic)	+ / O.C.	300mA

<table><tr><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td></tr><tr><td>⊖</td><td>⊖</td><td>⊖</td><td>⊖</td><td>⊖</td><td>⊖</td><td>⊖</td><td>⊖</td><td>⊖</td><td>⊖</td></tr><tr><td>+</td><td>-</td><td>Z1</td><td>Z2</td><td>+</td><td>-</td><td>Z3</td><td>Z4</td><td>ZT</td><td></td></tr><tr><td colspan="2"></td><td colspan="2">COM</td><td colspan="2"></td><td colspan="2">COM</td><td colspan="2"></td></tr></table>	11	12	13	14	15	16	17	18	19	20	21	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	+	-	Z1	Z2	+	-	Z3	Z4	ZT				COM				COM				Zone inputs 1 - 4			Signal	Max. current
	11	12	13	14	15	16	17	18	19	20	21																																			
	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖																																				
	+	-	Z1	Z2	+	-	Z3	Z4	ZT																																					
			COM				COM																																							
	11	+	Positive power supply voltage for detectors		+13.8V DC	1100mA**																																								
	12	-	Negative power supply voltage for detectors		-																																									
	13	Z1	Zone input 1 (NC-NO-BIL-B24)																																											
	14	COM	Common terminal for Z1 and Z2		0V DC (reference)																																									
	15	Z2	Zone input 2 (NC-NO-BIL-B24)																																											
	16	+	Positive power supply voltage for detectors		+13.8V DC	1100mA**																																								
	17	-	Negative power supply voltage for detectors		-																																									
18	Z3	Zone input 3 (NC-NO-BIL-B24)																																												
19	COM	Common terminal for Z3 and Z4		0V DC (reference)																																										
20	Z4	Zone input 4 (NC-NO-BIL-B24)																																												
21	ZT	Tamper input (BIL)																																												

	SENSOR BUS			Signal	Max. current
	22	+	Positive power supply voltage for Sensor Bus	+13.8V DC	1100mA**
	23	-	Negative power supply voltage for Sensor Bus	-	
	24	A	Channel A Sensor Bus	Serial	
	25	B	Channel B Sensor Bus	Serial	
	26	SY	Synchronization output	Sync	

	SERIAL BUS			Signal	Max. current
	27	+	Positive power supply voltage for Serial Bus	+13.8V DC	1100mA
	28	-	Negative power supply voltage for Serial Bus	-	
	29	A	Channel A Serial Bus	Serial	
	30	B	Channel B Serial Bus	Serial	
	31	S	Vocal output for consoles	Vocal	

	SIREN BUS			Signal	Max. current
	32	+	Positive power supply voltage for Siren Bus	+14.4V DC	750mA*
	33	-	Negative power supply voltage for Siren Bus	-	
	34	A	Channel A Siren Bus	Serial	
	35	B	Channel B Siren Bus	Serial	

	Telephone line		Note	
	36	A (PHONE)	Telephone line output A	PSTN telephone line (DC)
	37	B (PHONE)	Telephone line output B	
	38	B (LINE)	Telephone line input B	
	39	A (LINE)	Telephone line input A	

* The value refers to the maximum current provided for the power supply of conventional and bus sirens, without the intervention of the overload protection. The current is distributed among the terminals 1 and 32 and supplies a total of 3 sirens.

** The value refers to the maximum current provided for the power supply of conventional and bus detectors, without the intervention of the overload protection. The current is distributed among the terminals 11, 16 and 22.

6.3 - Power supply

The control panel is equipped with a switching power supply type ALSW1430 providing a maximum output current of 3A (14.4V DC). The connection to the control panel is made through a pre-wired polarized connector.

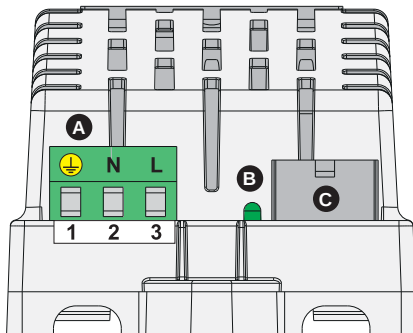
Input protection

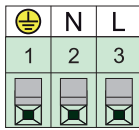
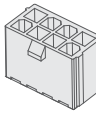
The 230V AC mains input is protected against overvoltage by varistors and a non replaceable fuse.

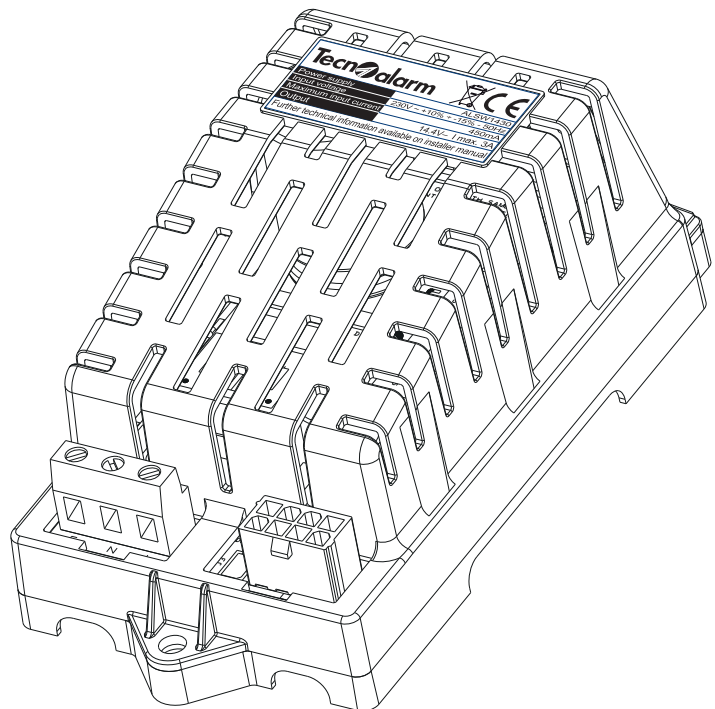
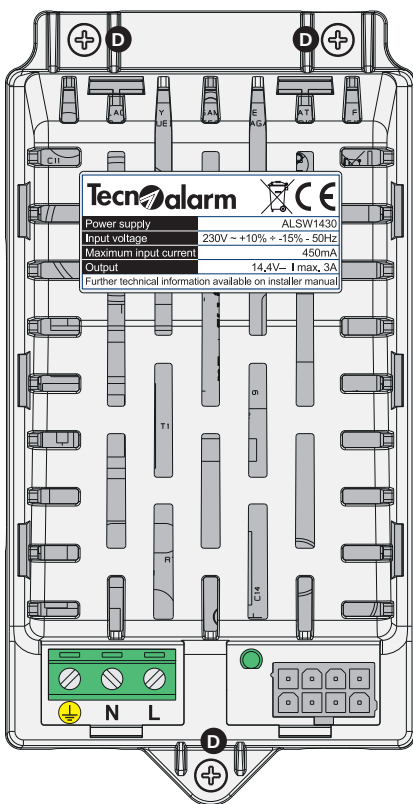
The interruption of the fuse is necessarily attributed to a failure or an exceptionally violent electromagnetic discharge (e.g. lightning).

Output protection

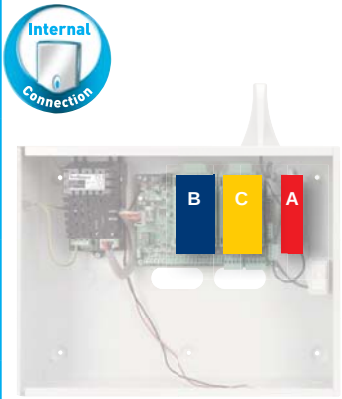
The output section of the power supply is protected against short circuits and overcharge. In case one of these events occurs, the power supply is automatically deactivated and will be reactivated only after restoring the normal functioning conditions.



A		Terminals	
		1	 Ground conductor
		2	N Neutral conductor 230V AC
		3	L Phase conductor 230V AC
B		LED	
		Green	On = normal functioning
C			
		Pre-wired polarized control panel connector	
D			
		Mounting holes for fixing to control panel casing	



6.4 - Mounting position of plug-in modules

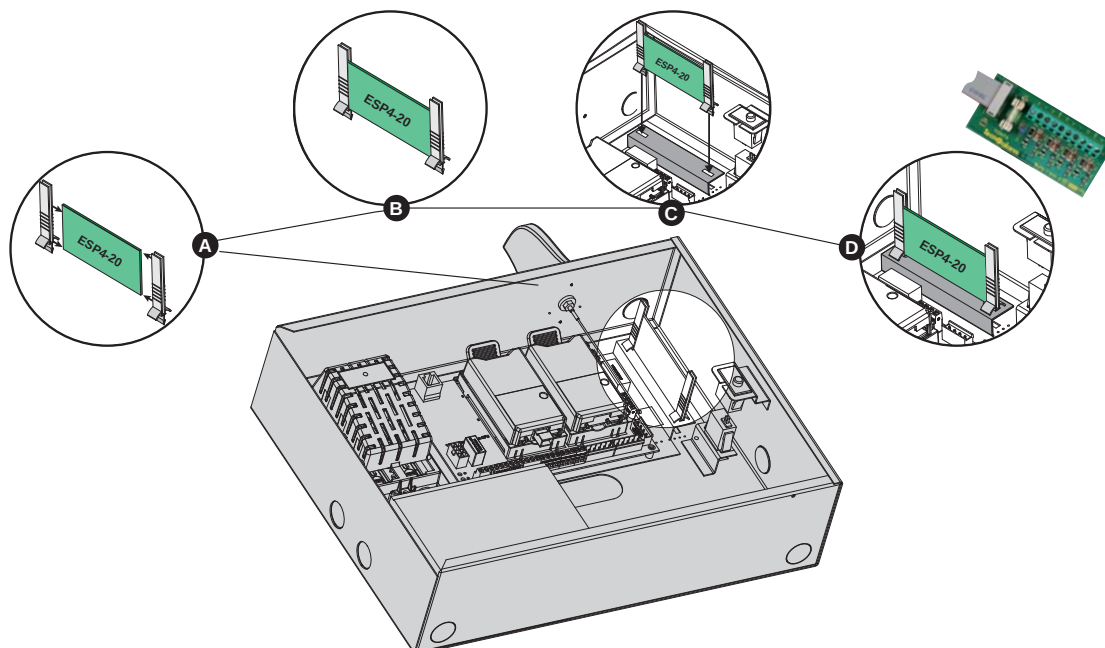
	A	ESP4-20	ZONE BUS DETECTORS	4 CONVENTIONAL DETECTORS				
	B	ESP LAN			IP			
	C	ESP GSM-GPRS				GSM-GPRS	2G	
	C	ESP GSM-GPRS 3G				GSM-GPRS		3G

6.5 - Plug-in input expansion

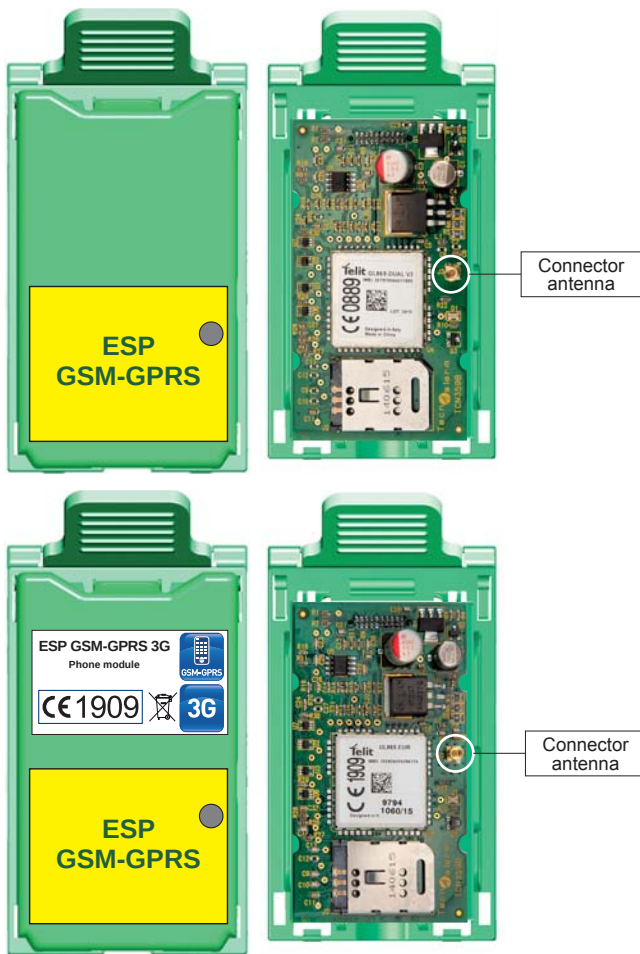
Terminals		Signal	Max. current
1	+	Positive power supply voltage for detectors	+13.8V DC
2	-	Negative power supply voltage for detectors	-
3	Z4	Zone input 4 (NC-NO-BIL-B24-ZBUS)	
4	COM	Common terminal for Z3 and Z4	0V DC (reference)
5	Z3	Zone input 3 (NC-NO-BIL-B24-ZBUS)	
6	+	Positive power supply voltage for detectors	+13.8V DC
7	-	Negative power supply voltage for detectors	-
8	Z2	Zone input 2 (NC-NO-BIL-B24-ZBUS)	
9	COM	Common terminal for Z3 and Z4	0V DC (reference)
10	Z1	Zone input 1 (NC-NO-BIL-B24-ZBUS)	

6.6 - Mounting of plug-in input expansion

A	Approach the guide rails laterally	C	Insert the guide rails in the sockets
B	Insert the module in the guide rails	D	Snap into place and connect the flat cable to the control panel



6.7 - Plug-in GSM-GPRS interface



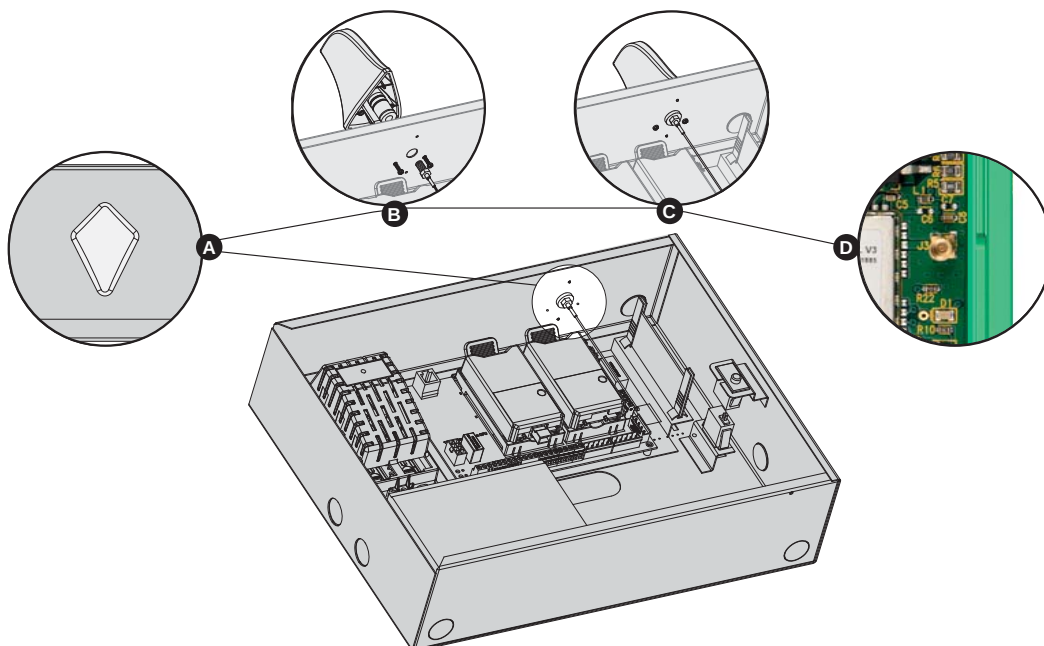
SIM card insertion		
A		Unlock tray by pushing it to the left
B		Open up tray
C		Insert SIM card with the contacts facing down
D		Close tray
E		Lock tray by pushing it to the right

N.B. To avoid damaging, the connection and disconnection of any component must be made in the absence of power supply.

The GSM-GPRS 3G interface provides the GSM 3G vector, which reduces the upload/download time up to eight times compared to the GSM 2G vector. The communication speed is extremely important from a point of view of data traffic congestion.

6.8 - Mounting of GSM antenna

A	Remove the stopper	C	Fix the antenna to the casing using the two screws
B	Place the fin and connect the antenna cable	D	Connect the antenna cable to the module ESP GSM-GPRS



6.9 - Plug-in Ethernet interface



Ethernet connector RJ45			
1	White/green	5	White/blue
2	Green	6	Orange
3	White/Orange	7	White/brown
4	Blue	8	Brown

Ethernet connector RJ45 - LED		
LED	Signaling	
Green	On	Communication speed 100Mbps
	Off	Communication speed 10Mbps
Yellow	Flashing	Communication active
	On	Connected
	Off	No connection

N.B. To avoid damaging, the connection and disconnection of any component must be made in the absence of power supply.

6.10 - Consumption

Consumption of CPU board and plug-in modules					
	Typical consumption	Max. consumption		Typical consumption	Max. consumption
TP10-42	120mA	150mA	ESP GSM-GPRS	130mA	160mA
ESP4-20	-	10mA	ESP GSM-GPRS 3G	130mA	160mA
ESP LAN	-	35mA			

N.B. The total consumption of all connected internal and external devices must not exceed 3A (total current provided by the power supply).
The maximum current available for loads is 2A.

6.11 - Available current for loads

Available current (without the intervention of overload protections)			
Battery charger	850mA	Output for self-powered siren (+SRA)	750mA
Power supply for Siren Bus + 14.4V terminal	750mA	Output for indoor siren (+SRINT)	500mA
Power supply for Serial Bus	800mA	Output OUT1	100mA
Power supply for Sensor Bus	500mA	Output OUT2	100mA
Power supply for detectors	500mA	Output OUT3	300mA
Power supply for ESP4-20	200mA	Output OUT4	300mA

N.B. The total consumption of all connected internal and external devices and all loads must not exceed 3A (total current provided by the power supply).

6.12 - Output expansions

The output expansions have the task to signal system status. The states of the system are divided into several groups identifiable by the address.

N.B. The addresses 13 to 16 are reserved to advanced programming and therefore are freely programmable.

The addresses 7, 10 and 12 are not available.

ESP 8RP ESP 8RSP ESP 4RS ESP32-OCN SINOTTICO 32N	Address 1 	Program status and alarm memory	Program status		Program alarm memory	
			OFF	ON	OFF	ON
			→ deactivated	→ armed	→ no alarm	→ no alarm
			Flashing quickly	→ exit time	Flashing quickly	→ Pré-alarme
			Flashing slowly	→ partset	Flashing slowly	→ Alarme active
01	Status program 1	09	Alarm memory program 1	17		25
02	Status program 2	10	Alarm memory program 2	18		26
03	Status program 3	11	Alarm memory program 3	19		27
04	Status program 4	12	Alarm memory program 4	20		28
05	Status program 5	13	Alarm memory program 5	21		29
06	Status program 6	14	Alarm memory program 6	22		30
07	Status program 7	15	Alarm memory program 7	23		31
08	Status program 8	16	Alarm memory program 8	24		32

ESP 8RP ESP 8RSP ESP 4RS ESP32-OCN SINOTTICO 32N	Address 2 	State of remote control and program alarm or stand-by	Remote control status		Program stand-by status	
			OFF	ON	OFF	ON
			→ deactivated	→ active	→ armed	→ disarmed
			OFF	→ no alarm		
			ON	→ Alarme active		
01	Status remote control 1	09		17	Status stand-by program 1	25
02	Status remote control 2	10		18	Status stand-by program 2	26
03	Status remote control 3	11		19	Status stand-by program 3	27
04	Status remote control 4	12		20	Status stand-by program 4	28
05	Status remote control 5	13		21	Status stand-by program 5	29
06	Status remote control 6	14		22	Status stand-by program 6	30
07	Status remote control 7	15		23	Status stand-by program 7	31
08	Status remote control 8	16		24	Status stand-by program 8	32

ESP 8RP ESP 8RSP ESP 4RS ESP32-OCN SINOTTICO 32N	Address 3 	General alarm states 1	General alarm states 1			
			OFF	ON		
			→ output deactivated**	→ output active*		
			* The outputs 1 and 15 behave oppositely			
01	General stand-by	09	Status chime zone	17	General tamper alarm	25
02	Status failure (battery/power supply)	10	Status telephone line	18	General failure alarm	26
03	Status low battery	11	General prealarm	19	False code alarm	27
04	Status power failure	12	Status PGM output	20	False key alarm	28
05	Status tamper	13	Access denied	21	Supervision alarm	29
06	Status failure (zones/modules)	14	General program alarm	22	Antijamming alarm	30
07	Status hold-up (code/zone)	15	System OK	23	General hold-up alarm	31
08	Status technical zone	16	Status GSM failure	24	General technical alarm	32

ESP 8RP ESP 8RSP ESP 4RS ESP32-OCN SINOTTICO 32N	Address 4 	General alarm states 2	General alarm states 2			
			OFF	ON		
			→ output deactivated	→ output active		
01	General exit time	09	Error notification CMS	17	GPRS call active	25
02	General by-pass	10	PSTN line OK	18	PSTN answer	26
03	Range reduction	11	GSM OK	19	GSM answer	27
04	Masking	12	Tecnocell OK	20		28
05	Supervision wireless devices	13	GPRS OK	21		29
06		14	Ethernet OK	22		30
07		15	PSTN call active	23	Airtime warning	31
08		16	GSM call active	24	Alarm memory zone	32

ESP 8RP ESP 8RSP ESP 4RS ESP32-OCN SINOTTICO 32N		Address 5	Status of zones 1-32		Zone status	
					OFF → closed ON → alarm stored flashing quickly → open flashing slowly → alarm active	
01	Status zone 1		09	Status zone 9	17	Status zone 17
02	Status zone 2		10	Status zone 10	18	Status zone 18
03	Status zone 3		11	Status zone 11	19	Status zone 19
04	Status zone 4		12	Status zone 12	20	Status zone 20
05	Status zone 5		13	Status zone 13	21	Status zone 21
06	Status zone 6		14	Status zone 14	22	Status zone 22
07	Status zone 7		15	Status zone 15	23	Status zone 23
08	Status zone 8		16	Status zone 16	24	Status zone 24
					25	Status zone 25
					26	Status zone 26
					27	Status zone 27
					28	Status zone 28
					29	Status zone 29
					30	Status zone 30
					31	Status zone 31
					32	Status zone 32

ESP 8RP ESP 8RSP ESP 4RS ESP32-OCN SINOTTICO 32N		Address 6	Status of zones 33-42		Zone status	
					OFF → closed ON → alarm stored flashing quickly → open flashing slowly → alarm active	
01	Status zone 33		09	Status zone 41	17	
02	Status zone 34		10	Status zone 42	18	
03	Status zone 35		11		19	
04	Status zone 36		12		20	
05	Status zone 37		13		21	
06	Status zone 38		14		22	
07	Status zone 39		15		23	
08	Status zone 40		16		24	
					25	
					26	
					27	
					28	
					29	
					30	
					31	
					32	

ESP 8RP ESP 8RSP ESP 4RS ESP32-OCN SINOTTICO 32N		Address 8	Alarm and tamper of zones 1-32		Zone alarm	
					OFF → no alarm ON → alarm active	
01	Alarm zone 1		09	Alarm zone 9	17	Alarm zone 17
02	Alarm zone 2		10	Alarm zone 10	18	Alarm zone 18
03	Alarm zone 3		11	Alarm zone 11	19	Alarm zone 19
04	Alarm zone 4		12	Alarm zone 12	20	Alarm zone 20
05	Alarm zone 5		13	Alarm zone 13	21	Alarm zone 21
06	Alarm zone 6		14	Alarm zone 14	22	Alarm zone 22
07	Alarm zone 7		15	Alarm zone 15	23	Alarm zone 23
08	Alarm zone 8		16	Alarm zone 16	24	Alarm zone 24
					25	Alarm zone 25
					26	Alarm zone 26
					27	Alarm zone 27
					28	Alarm zone 28
					29	Alarm zone 29
					30	Alarm zone 30
					31	Alarm zone 31
					32	Alarm zone 32

ESP 8RP ESP 8RSP ESP 4RS ESP32-OCN SINOTTICO 32N		Address 9	Alarm and tamper of zones 33-42		Zone alarm	
					OFF → no alarm ON → alarm active	
01	Alarm zone 33		09	Alarm zone 41	17	
02	Alarm zone 34		10	Alarm zone 42	18	
03	Alarm zone 35		11		19	
04	Alarm zone 36		12		20	
05	Alarm zone 37		13		21	
06	Alarm zone 38		14		22	
07	Alarm zone 39		15		23	
08	Alarm zone 40		16		24	
					25	
					26	
					27	
					28	
					29	
					30	
					31	
					32	

ESP 8RP ESP 8RSP ESP 4RS ESP32-OCN SINOTTICO 32N		Address 11	Status of indoor and outdoor sirens		Siren status	
					OFF → deactivated ON → active	
01	Indoor siren 1		09	Outdoor siren 1	17	
02	Indoor siren 2		10	Outdoor siren 2	18	
03	Indoor siren 3		11	Outdoor siren 3	19	
04	Indoor siren 4		12	Outdoor siren 4	20	
05	Indoor siren 5		13	Outdoor siren 5	21	
06	Indoor siren 6		14	Outdoor siren 6	22	
07	Indoor siren 7		15	Outdoor siren 7	23	
08	Indoor siren 8		16	Outdoor siren 8	24	
					25	
					26	
					27	
					28	
					29	
					30	
					31	
					32	

6.13 - Zone distribution

The system manages a total of 42 zones that can be freely associated to the same number of inputs, distributed across the connected hardware. The CPU board of the control panel provides 4 conventional and 6 Sensor Bus inputs. The expansion modules provide conventional, Zone Bus, Sensor Bus, SYNC@BWL, ASYNC@WL inputs.

INPUTS	CPU	ESP4-20	SPEED 8 STD	SPEED 4	SPEED 4-140C	SPEED 8	SPEED ALM8 PL	SPEED 4 PLUS	SPEED 8 PLUS	SPEED ALM8 PLUS	RX300 HS	RTX500S BWL	RTX500 BWL
CONVENTIONAL*	4	4	8	4	4	8	8	4	-	-			
ZONE BUS	-		-										
SENSOR BUS	6	-	-	-	-	-	-	4	8	8			
SYNC@BWL											-	42	42
ASYNC@WL											42		

* The contact type can be programmed as normally closed (NC), normally open (NO), end-of-line resistor (BIL) or double end-of-line resistor (B24) and the filter can be programmed as time, pulse count or inertial.

6.14 - Wireless modules

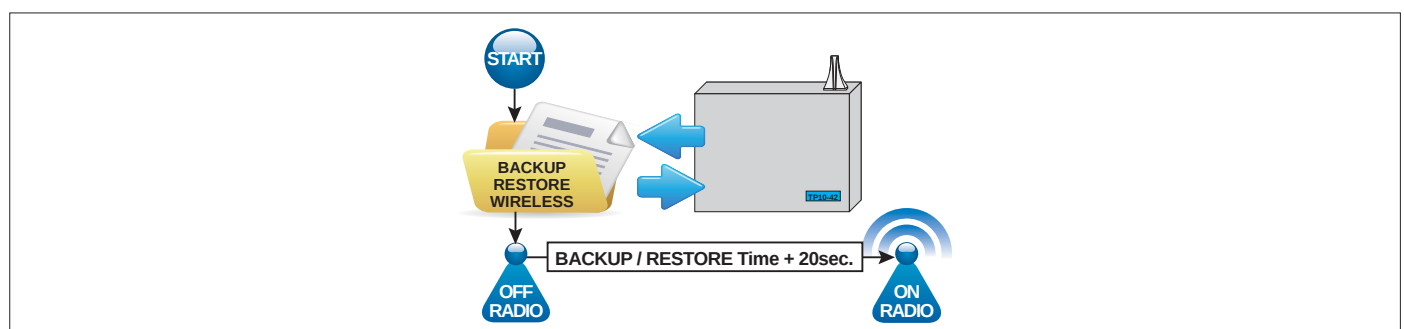
The system manages wireless devices through wireless receivers or coordinators connected via serial bus. The receiver and the coordinators are compatible with either the ASYNC@WL or the SYNC@BWL or both wireless communication protocols. The below table indicates the compatibility of the receiver and the coordinators with the protocols and the number of wireless devices managed.

	WIRELESS DEVICES MANAGED											
	 PROTOCOL ASync@WL			 PROTOCOL Sync@BWL								
				MEDIUM DATA RATE				MEDIUM DATA RATE				
RX300 HS	SIRENS		2									
	ZONES		42									
	WL KEYS		80									
max. 2 receivers												
RTX500S BWL				SIRENS		0	1	2				
				ZONES/ WL KEYS		105	98	91				
max. 1 coordinator												
RTX500 BWL	SIRENS		2	SIRENS		0	1	2	0		1	2
	ZONES		42	ZONES/ WL KEYS		105	98	91	133		126	119
	WL KEYS		80									
max. 1 coordinator												

Backup - Restore

After completion of the installation, we recommend to make a backup of the wireless configuration. In case of failure, the backup can be recovered using the restore function. The processes of backup and restore can be expedited considerably, if the wireless zones are programmed in sequence.

N.B. During backup and restore the radio communication is suspended and will only be restored 20 seconds after completion of the process.



6.15 - Installation notes for wireless modules

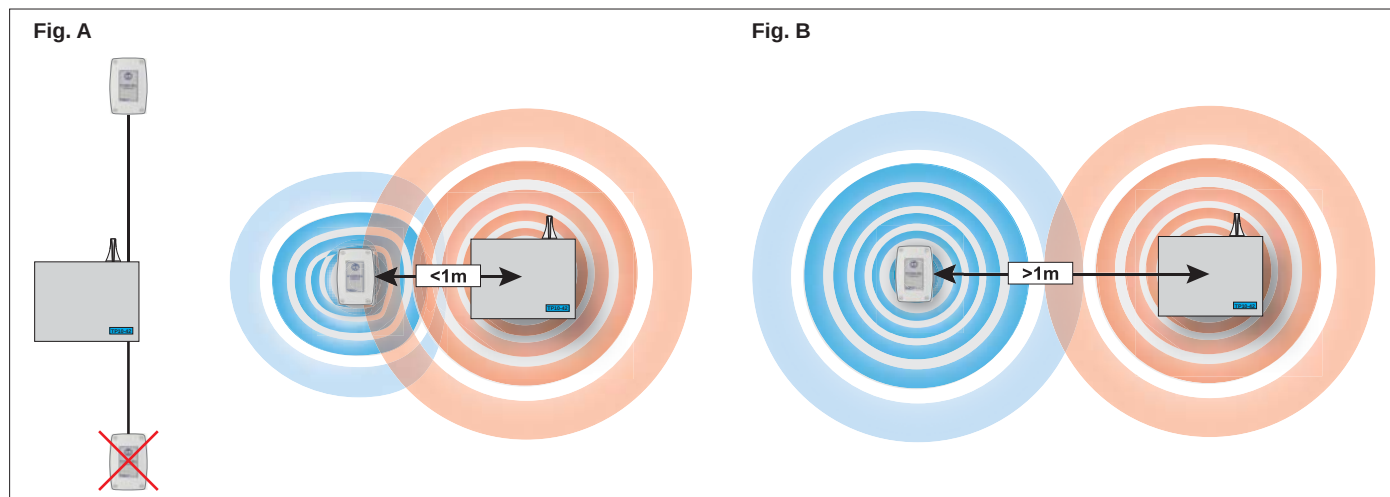
To guarantee correct functioning and coverage, observe the following instructions:

Installation position

Do not install the receiver/coordinator at ground level, but in a dominant position, above the control panel (fig. A).

Do not install the receiver/coordinator in the immediate vicinity of the control panel or other metal structures, but keep a minimum distance of 1m (fig. B).

Do not cover or shield the casing of the receiver/coordinator with objects that may interfere with the radio communication.



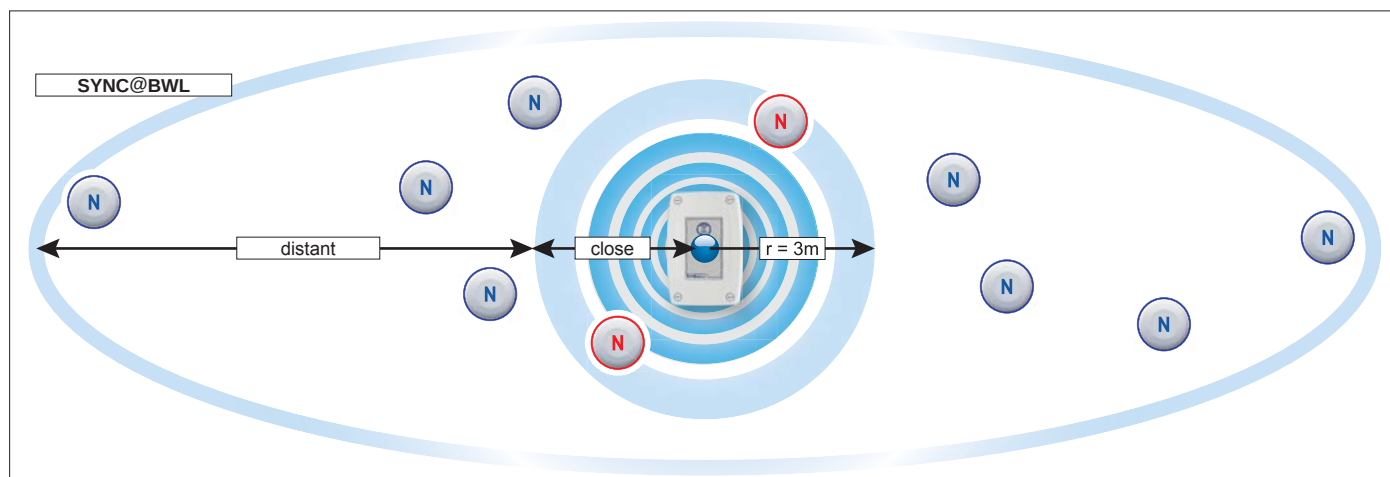
Environmental interference

Do not install the receiver/coordinator in the immediate vicinity of heat sources (radiators etc.) or devices capable of causing electromagnetic disturbances, such as radio links or antennas.



Radio range

We distinguish the area close to the receiver/coordinator (within 3 meters) from that extending from 3 meters distance to the limit of the radio range of the coordinator. In the area close to the receiver/coordinator, it is recommended to set transmission power of the nodes to medium.



6.16 - Serial buses

The system provides 3 RS485 serial buses managing different types of serial peripherals:

- Serial Bus for the connection of standard serial devices
- Sensor Bus for the connection of RSC[®] detectors
- Siren Bus for the connection of RSC[®] sirens

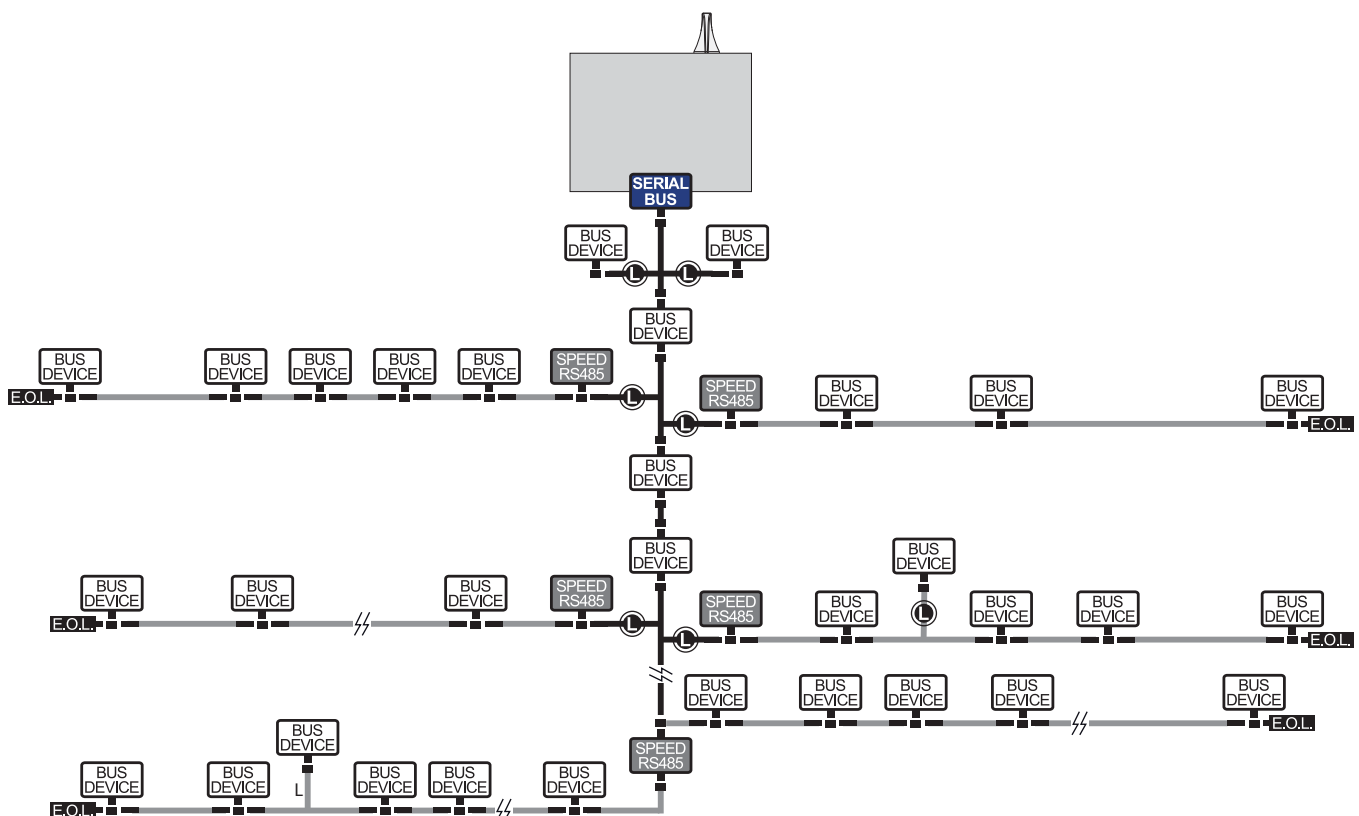
The serial buses use a baud rate of 38,400bps.

For connection it is recommended to use shielded multipolar twisted-pair cables with flexible conductors. The maximum bus length of 1km (no star connection allowed) can be extended by using fiber optic cables. The choice of the cable depends on the length of the serial bus and the total consumption of the connected devices. The serial bus must be balanced by inserting a bus termination jumper on the last device of the bus.

6.17 - Standard serial bus

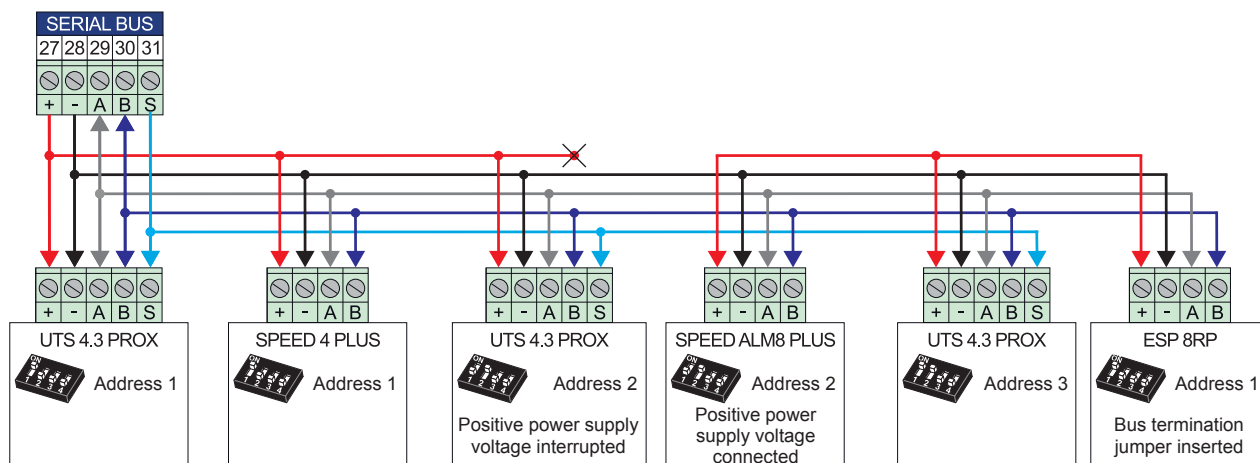
The standard serial bus manages up to 45 devices divided into five categories: 10 input expansion modules, 16 output expansion modules, 2 wireless receivers (using ASYNC@WL protocol) or 1 wireless coordinator (using SYNC@BWL protocol), 8 consoles, 8 auxiliary control units and 1 GSM telephone communicator.

The control panel identifies the devices by their address. Each category of devices uses its proper sequence of addresses (starting from address 1). The devices can be connected to the serial bus without any restrictions regarding the order or the category. The serial bus must be as linear as possible, branching is admitted provided that the branches do not exceed 1m length. Otherwise, the creation of branches requires the use of serial bus extensions connected to the main bus.



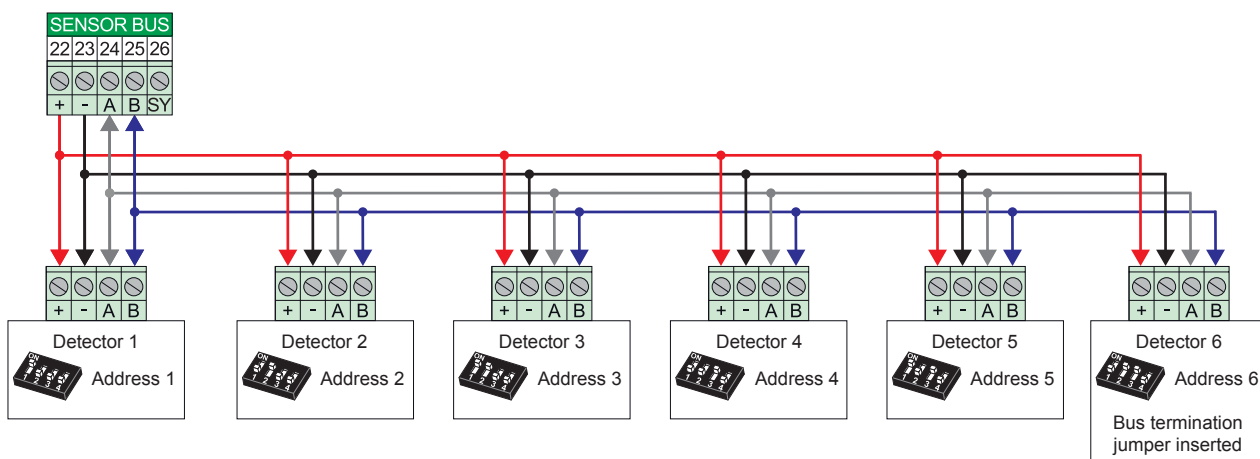
Legend of symbols					
	Serial device (console, keypad, expansion module etc.)		Serial bus extension (max. 5 modules connected to the main bus)		Branch with 1km maximum length
	Serial device (console, keypad, expansion module etc.) with end-of-line resistor		Main bus with 1km maximum length		Branch with 1km maximum length

6.18 - Connection to standard serial bus



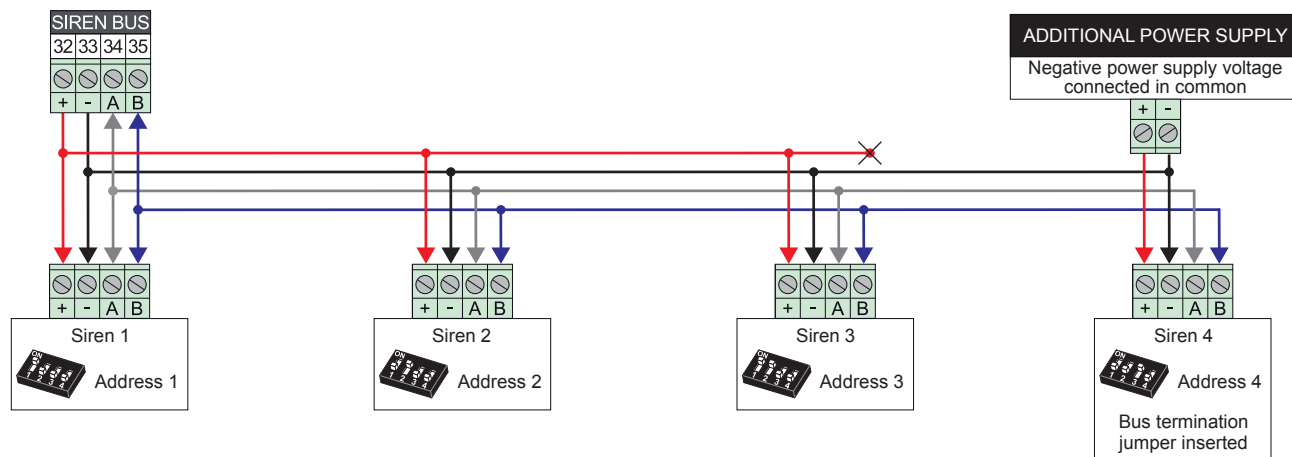
6.19 - Connection to Sensor Bus

The Sensor Bus port of the control panel manages up to 6 RSC[®] detectors, possible further detectors must be connected to the input expansions. The dip-switches program the address and synchronize the microwave emission of the connected detectors.

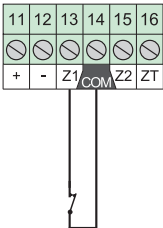
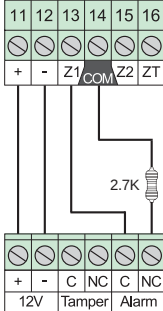
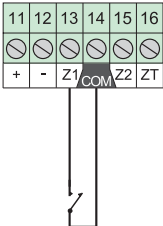
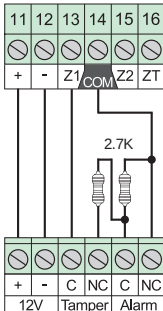


6.20 - Connection to Siren Bus

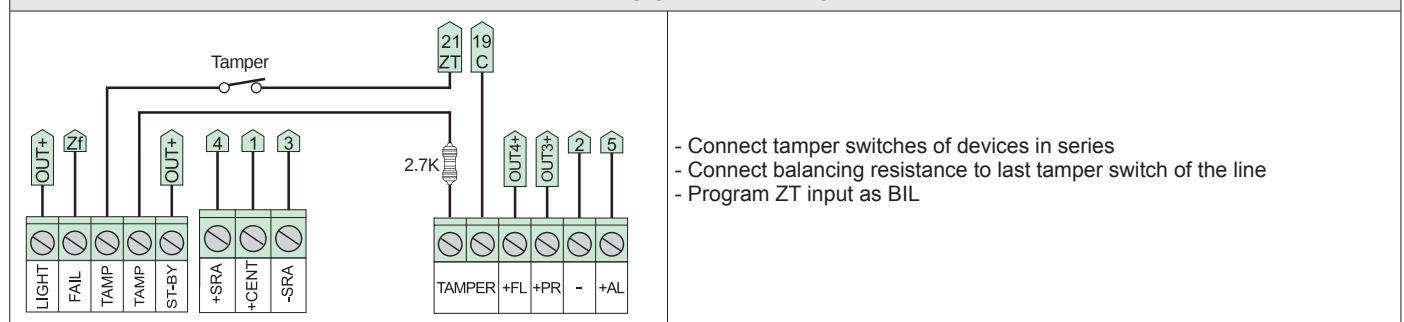
The system manages up to 4 RSC[®] sirens, however, the current provided by the control panel is enough to power a total of 3 sirens (RSC[®] and conventional). Further sirens must be powered through an additional power supply.



6.21 - Connection of conventional peripherals

CONTACT TYPES OF ZONE INPUTS			
	NC Normally closed input Stand-by: resistance 0...2KΩ (rated 0Ω) Alarm (open): resistance exceeds 2KΩ		BIL Input with end-of-line resistor Stand-by: resistance 2KΩ...4KΩ (rated 2.7KΩ) Alarm: resistance <2KΩ or >4KΩ
	NO Normally open input Stand-by: resistance exceeds 2KΩ Alarm (closed): resistance 0...2KΩ (rated 0Ω)		B24 Input with double end-of-line resistor Stand-by: resistance 2KΩ...4KΩ (rated 2.7KΩ) Alarm: resistance 4KΩ...7.4KΩ (rated 5.4KΩ) Tamper: resistance 0...2KΩ or 7.4KΩ

WIRING OF TAMPER INPUT



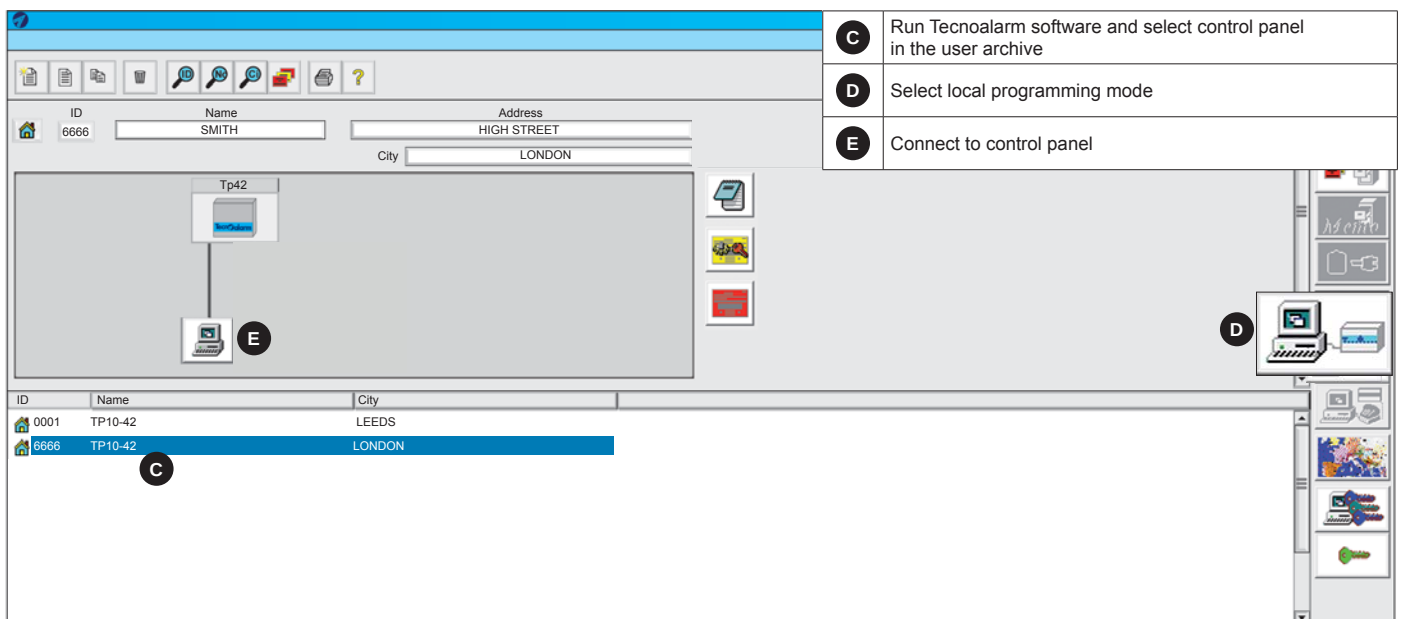
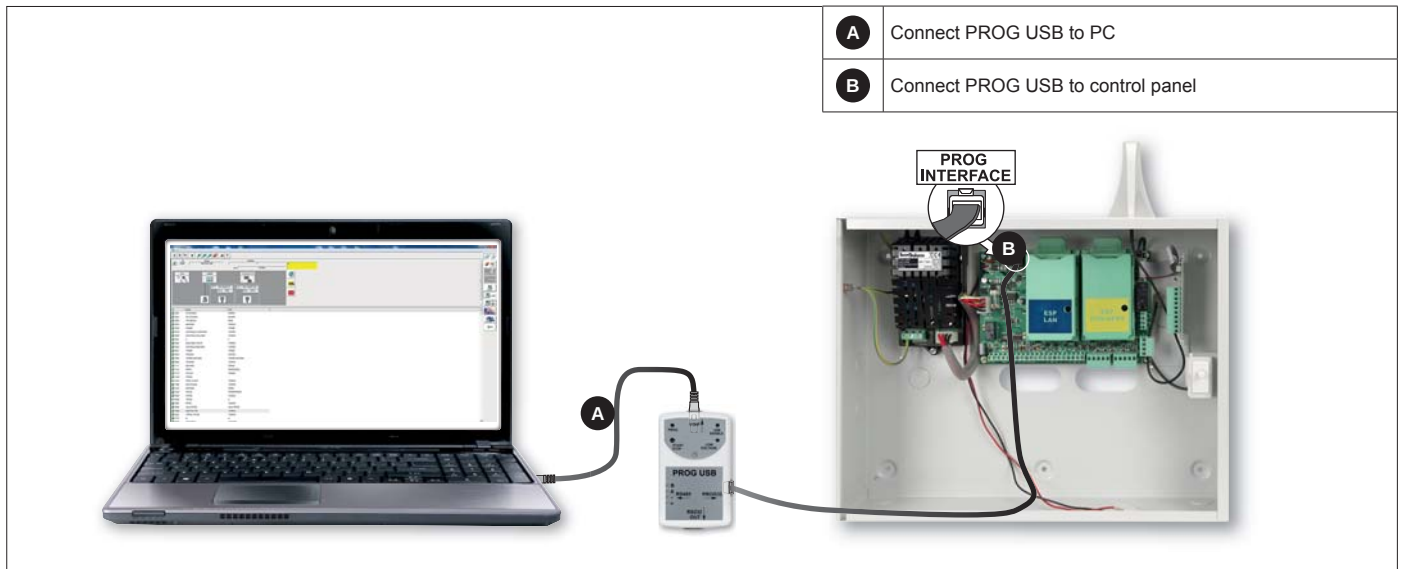
WIRING OF OUTPUTS

SAEL 2010 LED	SIREL	SIRTEC	BIRELE
Separate tamper management - Wire TAMP output to ZT input programmed as NC or BIL and corresponding common input - Connect FAIL output to technical zone programmed as NC	Separate alarm, prealarm and flashlight management - Wire +AL input to SRINT+ output - Wire +PR and +FL input to open collector outputs OUT+	Separate tamper management - Wire T output to ZT input programmed as NC or BIL and corresponding common input	Example of wiring - Wire relays to open collector outputs OUT- and OUT+ programmed as NO and NC

7 - SPECIAL PROCEDURES

7.1 - Firmware upgrade

The firmware of the control panel can be upgraded using the Tecnoalarm software and the programming interface PROG USB. **N.B.** Before proceeding, ensure that you have the file for upgrade at hand. This file is included in the CD with the latest software version or can be downloaded from the web site www.tecnoalarm.com.



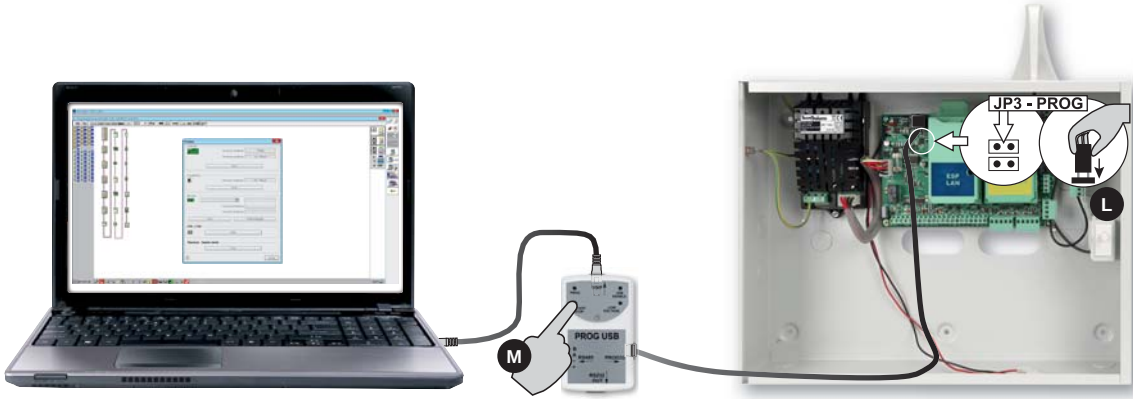
F	Check connection (ok if arrow green)
G	Select Firmware menu
H	Click on Send key in the Control panel section

I	Select upgrade file
J	Click on Open

K	The Send firmware window is opened.
----------	--

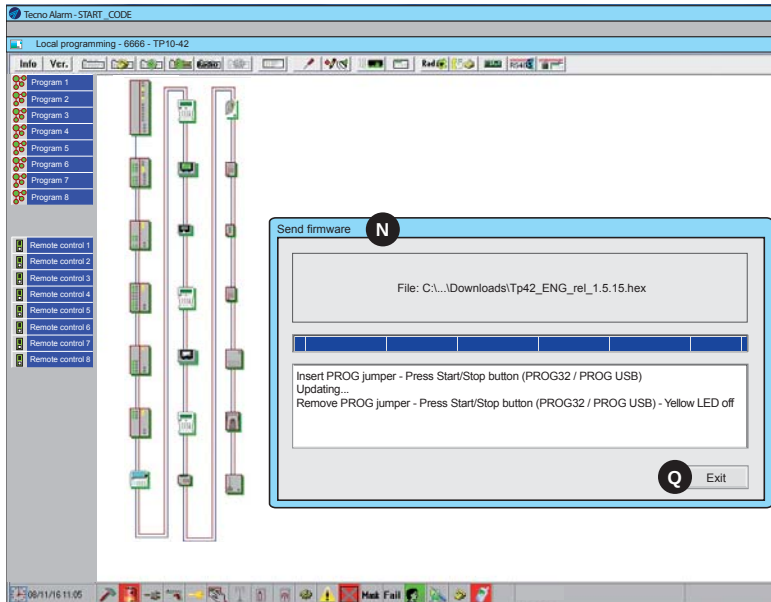
If the system contains bus sirens, put it into the maintenance mode to avoid sounding due to the interruption of the serial bus connection.

L	Insert jumper PROG on CPU board
M	Press start/stop button of PROG USB (yellow LED on)



N	Upload of firmware starts automatically, wait for completion
O	Remove jumper PROG on CPU board
P	Press start/stop button of PROG USB (yellow LED off)
Q	Quit the firmware menu

Firmware upgrade has been completed.



7.2 - Reset of codes

The below procedure deletes all the programmed access codes and restores the default values.

Default installer code: 54321
Default master code: 12345
Default user code: no default code
Default code length: 5 digits

A	Access keypad (UTS 4.3 PROX only)
B	Insert jumper CLR on CPU board
C	Insert jumper RESET on CPU board
D	Verify that RUN LED is switched off

E	Remove jumper RESET on CPU board
F	Verify that RUN LED is flashing
G	When console views the firmware version press EXIT key and wait until date and time are viewed

H	Remove jumper CLR on CPU board
I	Verify that RUN LED is flashing

7.3 - Reset of system configuration

The below procedure deletes the system configuration and restores the default values.
As a consequence of this, the default access codes will be restored.

Default installer code: 54321
Default master code: 12345
Default user code: no default code
Default code length: 5 digits

A	Access keypad (UTS 4.3 PROX only)
B	Insert jumper CLR on CPU board
C	Insert jumper RESET on CPU board
D	Verify that RUN LED is switched off

E	Remove jumper RESET on CPU board
F	Verify that RUN LED is flashing
G	When console views the firmware version press NO key and wait until date and time are viewed

H	Remove jumper CLR on CPU board
I	Verify that RUN LED is flashing

