Mod. 1068

DS1068-044 LBT21165

REMOTE MANAGED ALARM CONTROL PANELS

Ref. 1068/005A
Ref. 1068/010A

Ref. 1068/005A

Through the following QR Code, it is possible to download the eventual new version of the manual.

http://qrcode.urmet.com/default.aspx?prodUrmet=164750&lingua=en

Ref. 1068/010A

http://qrcode.urmet.com/default.aspx?prodUrmet=165029&lingua=en

INSTALLATION AND PROGRAMMING MANUAL

INTRODUCTION 8
Conformity with Standard EN50131-1 8
How the manual is organised 9
CONVENTIONS 9
GLOSSARY 10
1 THE 1068/005A AND 1068/010A SYSTEMS 12
1.1 Main characteristic 12
1.2 System Architecture 13
1.2.1 Architecture 13
1.2.2 Data Bus 13
1.2.3 Maximum system size 14
1.3 System connectivity 15
1.3.1 Connection with remote user 17
1.3.2 Remote user connection via Urmet Secure APP (Android – IOS) 18
1.3.3 Remote user connection via a Tablet with 1068set Android App 19
1.3.4 Radio device connection 19
1.3.5 Connection with an alarm reception centre 20
1.4 System components 21
1.4.1 1068/005A Control panel 21
1.4.2 1068/010A Control panel 22
1.4.3 1068/021 LCD Command Keypad 23
1.4.4 1067/008A 8-input expansion module 23
1.4.5 Housing box for expansion module 1067/017 24
1.4.6 1067/334 - 335 Electronic key reader 24
1.4.7 1067/332 Additional keys kit 25
1.4.8 1068/435 Proximity key reader 25
1.4.9 1068/432 Proximity key kit 26
1.4.10 1068/011 Radio module 26
1.4.11 1068/458 GSM/GPRS module with vocal synthesis 27
1.4.12 1067/014 Remote GSM antenna 27
1.4.13 1068/013 IP interface 27
1.4.14 1068/017 Radio interface on Bus 28
1.4.15 1067/092 supplementary power supply with repeater 28
1.4.16 1068/002 IP POE Interface 29
1.4.17 1068/027 7” Touch screen keypad 29
2 DESIGN: CALCULATIONS AND TESTS 30
2.1 Sizing of the power supplies and the batteries 30
2.1.1 Battery sizing 30
2.1.2 Calculation of the total absorption of the system 31
2.2 Cable Sizing 31
2.2.1 Cables to be used, connections of the shields and installation 31
2.2.2 Sizing of the power supply cable 32
2.2.3 Sizing the power supply and data transmission bus 33
2.2.4 Extending the bus with the repeater 34
2.2.5 Sizing of Input/Output connections 35
2.3 Control criteria of the mains power supply voltage 35
2.3.1 Blackout event 35
2.3.2 Continued blackout alarm 35
2.3.3 Restoration of the mains power supply 36
2.4 Battery management criteria 36
2.4.1 Controlling the battery with mains power supply absent 36
2.4.2 Battery test in presence of mains 36
2.5 Self-diagnostic functions 36

3 INSTALLATION 37
3.1 Installation procedure 37
3.2 Wiring 37
3.3 Preparing the 1068/005a – 1068/010a control panel 38
3.4 Installation of the 1068/005a – 1068/010a control panels 40
3.4.1 Description of the main parts of the 1068/005A control panel 40
3.4.2 Description of the main parts of the 1068/010A control panel 42
3.4.3 Installing the 1068/011 Radio module 44
3.4.4 Installing the 1068/013 IP module 44
3.4.5 Installing the 1068/002 IP POE interface 45
3.4.6 Installing the 1068/458 GSM/GPRS module with vocal synthesis 47
3.5 Installation of the 1067/008A expansion 50
3.6 Installation of the 1068/017 radio interface 51
3.7 Installation of the 1068/021 keypad 52
3.8 Installation of the 1068/027 keypad 54
3.9 Installation of the 1068/435 reader 55
3.10 Installation of the 1067/092 supplementary power supply (available only with 1068/010A control panel) 56
3.10.1 Fastening to the wall 56
3.10.2 Connecting the power supply and battery 56
3.10.3 The 1067/092 board 57
3.11 Connections 59
3.11.1 Mains power supply line 60
3.11.2 Connecting the data Bus 61
3.11.3 Connecting IP POE interface 62
3.11.4 Connecting the supplementary power supplies/repeater 63
3.11.5 Connecting inputs 64
3.11.6 Connecting outputs 66
3.11.7 Connecting the cable for the service keypad 68
3.11.8 Connecting the telephone communicator 68
3.12 Example of connection diagram of 1068/005A control panel with N.C. inputs 69
3.13 Example of connection diagram of 1068/010A control panel with N.C. inputs 70
3.14 Example of connection diagram of 1068/005A control panel with single BAL. inputs 71
3.15 Example of connection diagram of 1068/010A control panel with single BAL. inputs 72
3.16 Example of connection diagram of 1068/005A control panel with double BAL. inputs 73
3.17 Example of connection diagram of 1068/010A control panel with double BAL. inputs 74
3.18 Example of connection diagram of 1068/010A control panel with double inputs 75
3.19 Example of connection diagram of 1067/008A expansion with NC inputs 76
3.20 Example of connection diagram of 1067/008A expansion with SINGLE BAL. inputs 77
3.21 Example of connection diagram of 1067/008A expansion with DOUBLE BAL. inputs 78
4 COMMISSIONING 79
4.1 System power supply 79
4.2 Acquisitions of bus devices 80
4.2.1 Position of the programming buttons 80
4.2.2 Procedure for acquiring the first keypad 80
4.2.3 Procedure for acquiring bus devices (expansions and readers) 81
4.3 Using the service keypad 81
5 SYSTEM COMMISSIONING 82
5.1 Navigation menu 82
5.1.1 How to access menus 83
5.1.2 Free access menu 83
5.1.3 Main Menu 84
5.2 How to enter alphanumeric characters 85
5.3 How to enable the Installer 85
5.4 How to enable the Technical Manager 85

5.5 How to select the language 86
5.6 LCD Info 86
5.7 Date and time setting 86
5.8 Zones programming 87
5.9 Wired input programming 87
5.9.1 Wired input encoding 88
5.9.2 Input types 88
5.9.3 Wired input customisation 89
5.9.4 Isolable 91
5.9.5 Auxiliary functions of intrusion inputs (Gong, Courtesy light and Door opener) 92
5.9.6 Zone assignment type (AND / OR) 92
5.9.7 AND inputs 92
5.9.8 Input programming procedure 93
5.10 Wired input programming 94
5.10.1 Output encoding 94
5.10.2 Output types 95
5.10.3 Output assignment 95
5.10.4 Electrical characteristics of the outputs 95
5.10.5 Output customisations 95
5.10.6 Output behaviour when the system is being serviced 98
5.10.7 Output programming procedure 99
5.11 Keypad programming 100
5.11.1 Function programming procedure 100
5.11.2 Zones assignment 101
5.11.3 Gong function 101
5.11.4 Entry time 101
5.11.5 Exit time 102
5.11.6 Masking 102
5.11.7 Name 102
5.11.8 Function key 102
5.12 Reader programming 103
5.12.1 LED management 103
5.12.2 Programming procedure 103
5.13 Keys 103
5.13.1 Key acquisition 104
5.13.2 Key deletion 104
5.13.3 Key configuration 104
5.14 Advanced programming 105
5.14.1 Remote control system code 105
5.14.2 Programming procedure 105
5.15 General system parameters (timings) 106
5.15.1 Programming procedure Times and parameters 107
5.16 Phone dialer and IP interface 107
5.16.1 Alarm and event notifications 107
5.16.2 Phone numbers and IP addresses 107
5.16.3 Vocal messages 107
5.16.4 SMS text messages 108
5.16.5 GSM parameters 108
5.16.6 GPRS parameters 108
5.16.7 GSM field test 109
5.16.8 IP parameters 109
5.16.9 IDP protocol 111
5.16.10 IDP/IP Protocol 111
5.16.11 Advanced 112
5.17 Time scheduler 113

5.17.1 Operating principles 113
5.17.2 Programming 114
5.17.3 Deleting a command 114
5.18 System Test 115
5.18.1 Input test 115
5.18.2 Output test 115
5.18.3 Control panel battery test 115
5.18.4 Call or SMS test 115
5.18.5 Push notification sending test 115
5.18.6 GSM Field Test 115
5.18.7 IP interface test 115
5.18.8 Supplementary power supply battery test (available only with 1068/010A control panel) 115
5.18.9 System diagnostics 116
5.18.10 Final tests 116
5.19 User training 116
6 PROGRAMMING WITH TABLET 117
6.1 Prerequisites 117
6.1.1 Tablet Requirements 117
6.1.2 Enabling requirements 117
6.1.3 File types 117
6.1.4 Saving data on Micro SD card 118
6.1.5 How to restore data on the control panel 118
7 MAINTENANCE MENU 119
7.1 How to view device addresses 119
7.2 How to view the firmware release of devices 119
7.3 How to upgrade bus device firmware from menu 119
7.3.1 Upgrade files 119
7.3.2 Updating system firmware from keypad 120
7.3.3 System firmware upgrade from 1068set App 121
7.4 Reset default 122
7.5 Reset factory settings 122
7.6 System log 122
7.6.1 How to interpret viewed data 123
7.6.2 How to browse the System Log 123
7.6.3 How to browse the EN50131 Event log (available only with 1068/010A control panel) 124
7.6.4 How to delete the System Log 124
7.6.5 How to delete the EN50131 Event log (available only with 1068/010A control panel) 124
8 TABLES 125
8.1 Vocal alarm messages and SMS 125
8.2 Alarm sending types 126
8.3 Remote control functions 126
8.4 Factory settings 129
8.4.1 System code 129
8.4.2 Zones 129
8.4.3 Users 129
8.4.4 Keys 129
8.4.5 General parameters and Times 130
8.4.6 Control panel inputs 130
8.4.7 Control panel outputs 131
8.4.8 Expansion module inputs 132
8.4.9 Expansion outputs 132
8.4.10 Keypad inputs 133
8.4.11 Radio module/interface inputs 133
8.4.12 Radio module/interface outputs (sirens) 133
8.4.13 Reader inputs 133

8.4.14 Keypad parameters 134
8.4.15 Reader- zones assignment 134
8.4.16 Assignment of radio remote control keys 134
8.4.17 Communicator parameters 135
8.4.18 Time scheduler 136
8.5 Time scheduler configuration 136
9 MAINTENANCE 138
9.1 Maintenance procedure 138
9.1.1 Maintenance mode access 138
9.1.2 End of maintenance 139
9.2 Adding a new bus device 139
9.2.1 Procedure for acquiring bus devices (expansions, readers and radio interfaces) 139
9.2.2 Keypad acquisition 140
9.2.3 Touch keypad acquisition 140
9.3 Replacing a radio device 142
9.4 Replacing a bus device 143
9.4.1 Replacing the Bus devices (expansions, readers and radio interfaces) 143
9.4.2 Replacing the keypad 143
9.5 Identifying a bus device 143
9.5.1 Interrogating a bus device 143
9.5.2 Searching for and identifying a device 144
9.6 Deleting a bus device 144
9.7 Deleting 1068/017 RADIO INTERFACe or 1068/011 RADIO MODULe 144
9.8 Enabling/disabling the 1068/011 radio module 145
9.9 Enabling/disabling the 1068/017 radio interface 145
9.9.1 Radio connection test 145
9.10 Configuring radio parameters 146
9.10.1 Device supervision 146
9.10.2 Jamming 146
9.10.3 Enable 147
9.10.4 Module supervision 147
9.11 Acquisition of a new radio device 147
9.12 Deleting a radio device 147
9.13 Reset factory settings 148
9.13.1 Software partial reset 148
9.13.2 Codes software reset 149
9.13.3 Radio module software reset 149
9.13.4 Installer hardware code reset 149
9.13.5 1068/013 interface hardware reset 149
9.13.6 Hardware reset to factory settings 149
9.13.7 Wired device hardware reset 149
9.13.8 Wired keypad hardware reset 150
9.13.9 Replacing the battery 151
9.14 Turning off the entire system 151
10 TECHNICAL SPECIFICATIONS 152
10.1 1068/005A Control panel 152
10.2 1068/010A Control panel 153
10.3 1067/092 Supplementary power supply with repeater 154
10.4 1068/021 Command Keypad LCD 155
10.5 1067/334 – 1067/335 Electronic key reader 155
10.6 1068/435 proximity reader 155
10.7 1067/008A 8-input expansion module 156
10.8 1068/458 GSM/GPRS module with vocal synthesis 156
10.9 1068/013 IP interface 156

10.10 1068/002 IP interface....157
10.11 1068/027 7”touch screen KEYPAD....157

INTRODUCTION

CONFORMITY WITH STANDARD EN50131-1

The EN50131-1 standard calls for the installation of a grade four intrusion alarm system, based on the level of risk determined in function of the type of environment, 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 for vocal messages to other people.

Grade 2: Average-low risk
It is expected that the intruders have limited knowledge of intrusion 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 intrusion 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 intrusion alarm system.

This is indicated for particularly sensitive premises, for example, banks.

	**WARNING!** The grade of an intrusion alarm system is the one of its lowest grade component.

The EN50131-1 standard requires that the components of the intrusion 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).

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).

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 intrusion alarm system are not totally exposed to atmospheric agents or indoors, when the environmental conditions are extreme.

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 intrusion alarm system are completely exposed to the elements.

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.

HOW THE MANUAL IS ORGANISED

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

Chapter 1 describes the 1068A series systems, theirs architecture and the devices that constitute it.

Chapter 2 provides useful information for designing and dimensioning alarm system components.

Chapter 3 explains how to install the control panel, the devices, the accessories, and how to connect them all together.

Chapter 4 illustrates the operations to be carried out to start up the system, before its programming.

Chapter 5 describes the programmings required to operate the system.

Chapter 6 illustrates how to program the system using a Tablet with Android 1068set App.

Chapter 7 describes the maintenance operations which do not require to physically operate on the system and that can be managed via software.

Chapter 8 shows all the vocal messages (both pre-recorded and not) for the possible events and shows which messages can be customised by recording a personal message over them.

Chapter 9 illustrates all the maintenance activities necessary to keep the alarm system functioning with perfect efficiency and provides troubleshooting advice.

Chapter 10 contains the technical specifications of the control panel and the various devices.

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

CONVENTIONS

In this manual, some conventions have been used to distinguish between different types of information:

Warning! Warning messages highlight potential system damage, data loss or non-compliance with applicable regulations.

Notes: notes contain important information, which may be useful for better use of the system.

This symbol indicates compliance with EN50131 grade 1.

This symbol indicates compliance with EN50131 grade 2.

This symbol indicates that the function or device does not comply with the EN50131 standard.

⎓ Direct power supply voltage.

~ Alternated power supply voltage.

Power supply unit with double isolation.

Refer to the device's installation manual.

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 an attempted intrusion has been detected.
ATS	Acronym of Alarm Transmission System. Depending on the performances, they are capable of offering, they are classified from ATS 1 to ATS 6, where ATS 1 is the simplest system and ATS 6 is the system with the highest level of performance.
Communicator	A device capable of sending and transferring alarm signals and events via a phone line.
Default	The initial value of a device before configuration or when it is restored to the values set by the manufacturer.
DNS	Domain Transmission System, i.e. a system capable of resolving IP addresses of hosts in names and vice versa.
DTMF	Dual Tone Multi Frequency indicates the "tonal" mode of composition of a phone.
Entry	A point of access to rooms protected by the intrusion alarm system.
Event	A fact that occurs accidentally or when a specific condition is met, for example when a certain period of time has passed.
Fieldbus (FB)	Fieldbus connecting Keypads (**TS**), Readers (**LT**) and Expansions (**ER**) connected to the microprocessor control panel.
Physical address (In)	Method used by the control panel to identify and locate inputs and outputs.
Logical address (IN)	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) for the physical connection of one or more detectors (usually sensors or contacts). 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.
Path	A set of one or more inputs that temporarily inhibit the signalling of sensor alarms connected to enable the entry into or exit from a protected zone. 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.
RM	Reset Memory, is a signal (voltage) control that erases the memory of a detector and that can inhibit its functioning, for example by putting it in stand-by.
SELV	Safety Extra-Low Voltage (rated voltage max 25 V~ and 50 V⎓).
Zone	Grouping of entries, exits, user codes, and keys that are associated with a space to be controlled.
Tamper	Protective micro-contact of a device.
Entry time	The time that the user has available from the moment in which he opens the first input to deactivate the desired zones and prevent the generation of an intrusion alarm by the inputs programmed as "Path".
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 zone/s to exit the protected area and prevent the generation of an intrusion alarm by the inputs configured as "Path".
Output	Point (terminal) for the physical connection of a device that enables the 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.

IMPORTANT!

The factory control panel is released in operating mode according to EN50131-1.

The 1068A series control panels have been built and designed to comply with the requirements of the EN50131 standard.

1) The JP4 jumper must be closed in order to obtain the operating mode compliant with EN50131 grade 1.

JP4 closed	

2) To obtain the operating mode that does **NOT** comply with the EN50131 grade 1 standard, the JP4 jumper must be open.

JP4 open	

	IMPORTANT! *Incorrect selection of the JP4 jumper causes significant differences in operation.*

	IMPORTANT! System components (e.g. IP interface) must be connected to the control panel when not powered (mains power and battery disconnected).

Quick consultation of topics

To know the main characteristics and components of the system...	see pages 12 to 29
How to size and check power supply units, cables and battery...	see pages 30 to 36
How to proceed with the installation of the control panel and its components...	see pages 37 to 78
How to commission the system before programming...	see pages 79 to 81
How to proceed with the programming for the commissioning of the system...	see pages 82 to 116
How to program your system with a Tablet with Android 1068set App...	see pages 117 to 118
How to proceed with system function maintenance operations managed via Software...	see pages 119 to 124
To know all the vocal messages, either pre-recorded and not, the expected events and how to customise them…	see pages 125 to 137
How to proceed with the maintenance activities necessary to keep the system efficient and identify faults...	see pages 138 to 151
To know the technical characteristics of the control panel and the various components of the system...	see pages 152 to 157

1 THE 1068/005A AND 1068/010A SYSTEMS

This chapter describes the 1068A series systems.

More specifically, the following are analysed:

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

1.1 MAIN CHARACTERISTIC

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

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 customisation.

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

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

Other functions available are:

- **Programming via tablet with Android 1068set App.**
- **Programming saved on micro SD Card**, to transfer the programming between tablet and control unit or save a back-up copy.
- **Firmware upgrade** on devices through micro SD Card or IP 1068/013 interface.
- **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 zones and/or inputs.
- **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 phone 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 time scheduler built into the control panel, it is possible to arrange a series of automatic and repetitive commands weekly.

Moreover, there is an auxiliary function, which is not complying with current laws, that allows the guaranteed security of the system to be increased easily and economically, without however replacing the dedicated systems:

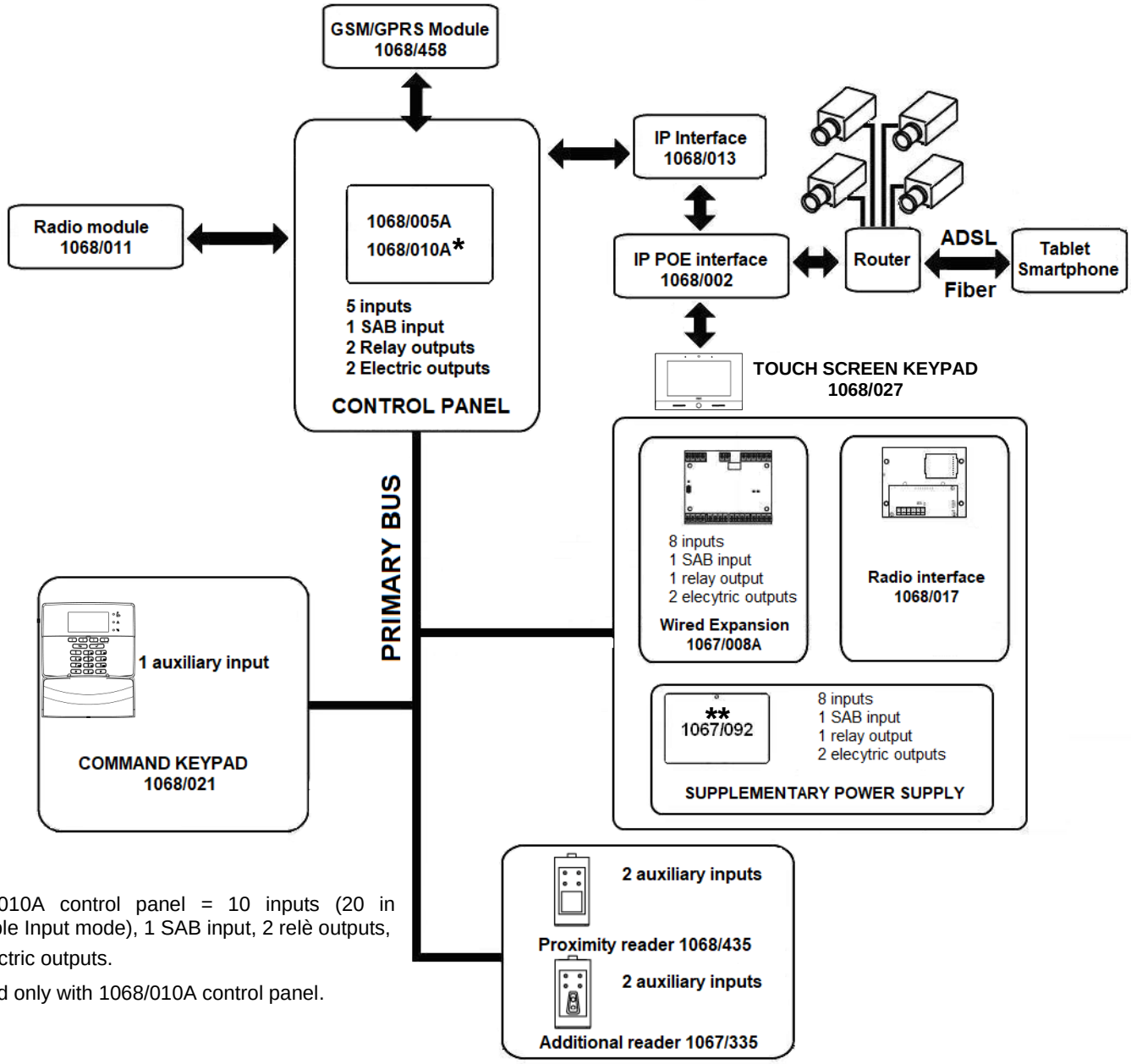
- **Emergency signalling**, generating service signals when a dedicated button is pressed.

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

1.2 SYSTEM ARCHITECTURE

1.2.1 Architecture

The following figure shows the devices that can be managed from the control panels 1068/005A and 1068/010A. For the dimensioning of the system (combinations of devices and their maximum number) see the paragraph *1.2.3 Maximum system size*.



Note:

***1068/010A control panel = 10 inputs (20 in Double Input mode), 1 SAB input, 2 relè outputs, 5 electric outputs.

****** Valid only with 1068/010A control panel.

Figure 1 – 1068A series systems architecture

1.2.2 Data Bus

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

The 4 wires transmit information among the various devices and supply 13.8 V⎓ power from the control panels to the keypads, readers, and expansion modules.

The use of the bus simplifies the wiring, given that, the information of a group of detectors located far from the control panel and concentrated on a remote 1067/008A expansion module can be controlled with just 4 wires.

1.2.3 Maximum system size

The table below shows the maximum number of keypads, readers, keys and expansions that can make up the alarm system.
Maximum limits are indicated for each single device and combined together when the system includes similar devices.
Example: the maximum number of readers that can be installed is 8, whether you use a single type or a mixed combination.

Device	1068/005A Control panel		1068/010A Control panel	
	Max Number of each type	Max Number of mixed combination	Max Number of each type	Max Number of mixed combination
1068/021 Command keypad (1)	8	------	8	------
1068/027 Touch screen keypad	1	------	1	------
1067/008A Expansion module	2	------	7	7
1067/092 Additional power supply with repeater	------			
1068/011 Radio module	1	------	1	2
1068/017 Radio interface	1		2	
1067/334 – 335 Electronic key reader	8	8	8	8
1068/435 Transponder reader	8		8	
1067/332 Electronic key	16	16	32	32
1068/432 Proximity key	16		32	
Access codes (2)	19	------	35	35

Table 1 - Maximum size of 1068A series systems

1) If service keypad is used, it is not counted.

2) Of which 1 Master, 1 Installer, and 1 Technical Manager.

The table below shows the maximum number of inputs and outputs that a system of the maximum size can include.

Type	1068/005A Control panel	1068/010A Control panel
	Max Number	Max Number
General inputs	21	66
	5 + 16	10 + 56 (Single input mode)
	----------	20 + 46 (Double input mode)
Anti-tampering inputs (SAB)	3	8
Relay outputs	4	9
Electric outputs	6	19
Radio sirens	4	8

Table 2 - Max number of inputs and outputs

1.3 SYSTEM CONNECTIVITY

The alarm system can be connected to the external environment in different ways, sending signals and receiving commands.

Possible connection methods are:

- **Mobile network (GSM)**. Requires optional 1068/458 interface.
- **Internet or Ethernet - WiFi Domestic Network**. Requires optional 1068/013 interface.

The tables below illustrate the functions available according to the means of communications used.

	Description of information transmitted	**Means of communications used**				
		GSM (Vocal)	**GSM** (SMS)	**Internet and LAN** (Secure App and 1068set App)	**GSM** (IDP)	**Internet and GPRS** (IDP/IP)
Sent by the control panel	Hold-up signalling	■	■	■	■	■
	Intrusion signalling	■	■	■	■	■
	Pre-alarm signalling	■	■	■	■	■
	System setting/unsetting signalling	■	■	■	■	■
	Tamper signalling	■	■	■	■	■
	False code signalling	■	■	■	■	■
	Emergency alarm signalling	■	■	■	■	■
	Fault signalling	■	■	■	■	■
	Loss of mains signalling	■	■	■	■	■
	Battery failure signalling	■	■	■	■	■
	Maintenance signalling	■	■	■	■	■
	Signalling of input isolation or inhibition	■	■	■	■	■
	Technological events signalling	■	■	■	■	■
	SIM expiration warning	■	■	■		

	Description of information received	Means of communications used			
		GSM (Incoming calls and answering machine)	**GSM** (Incoming calls at no cost)	**GSM** (Incoming SMS)	**Internet and LAN** (Secure App and 1068set App)
Interaction with the control panel	Zone/s setting/unsetting command	■			■
	Controlled output activation command	■	■	■	■
	Controlled output deactivation command	■		■	■
	Input isolation/inclusion command	■			■
	System status report request	■			■
	Code and key programming commands				■
	Read event log command				■

DISCLAIMER

Urmet S.p.A. declines any and all responsibility concerning the unavailability, temporary or permanent, of the GSM/GPRS phone network that may affect the making of calls or the sending of programmed messages.

Under conditions of a weak or disturbed field, there may be a decline in the performance of the GSM communication vector.

1.3.1 Connection with remote user

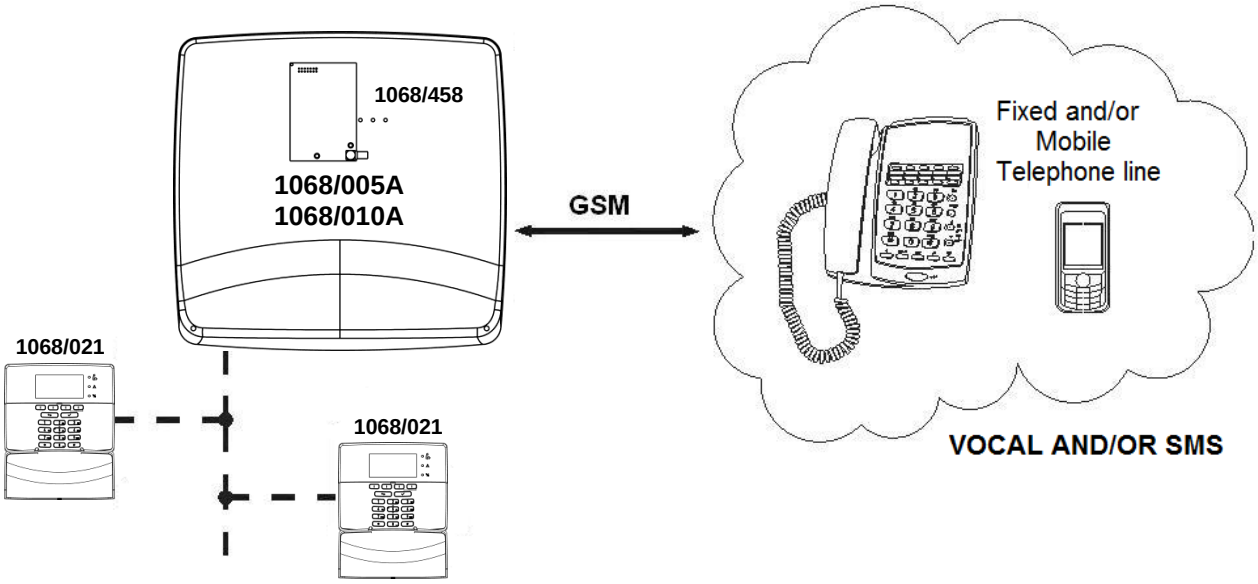


Figure 2 - Diagram of connection with remote user

From the control panel towards the remote user

The control panel, via outgoing calls, can:

- Send alarms and vocal signals (GSM network).
- Send alarms and signals via SMS (GSM network).

From the remote user towards the control panel

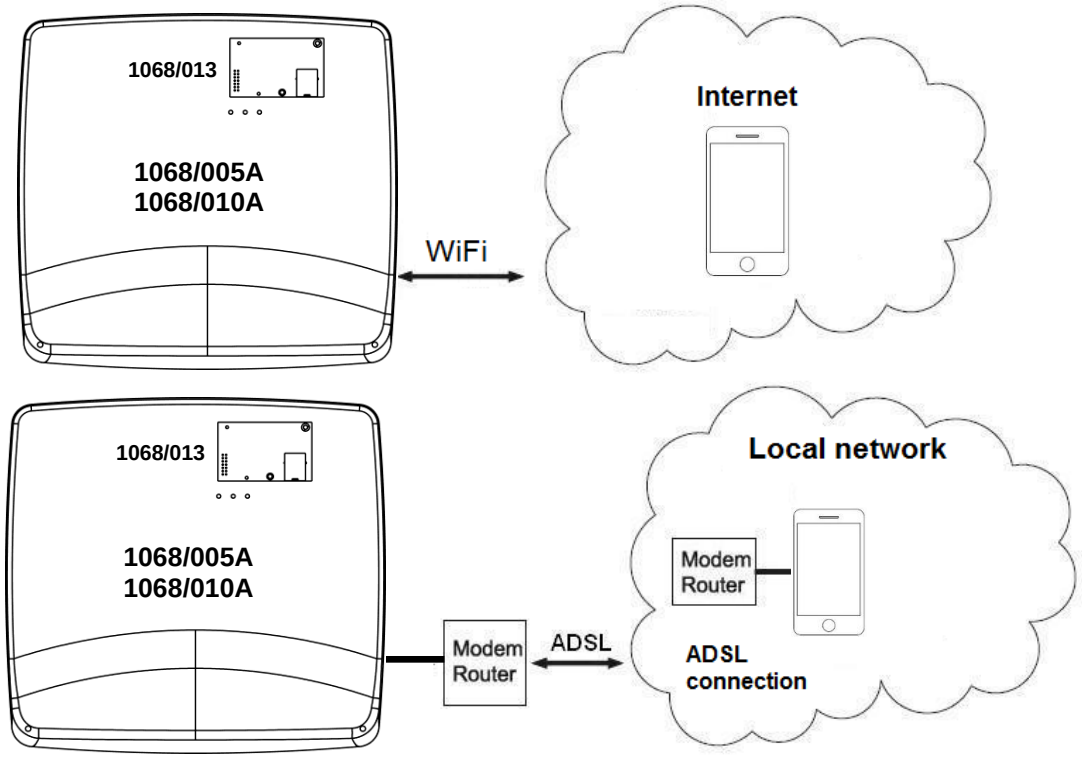
The User, via calls to the control panel, can:

- Use remote management with vocal guide and commands in DTMF for:
  - Inquire about the system status (armed/disarmed and anomalies present);
  - Activate or deactivate zones;
  - Isolate and reset inputs;
  - Remotely control outputs (for gate opening devices, heating equipment, irrigation, etc.);
- 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).

The GSM/GPRS 1068/458 interface is an optional item and can be used in control panels, either as an alternative or together with the IP 1068/013 interface.

For further information, please see paragraph *3.11.8 Connecting the telephone communicator*.

1.3.2 Remote user connection via Urmet Secure APP (Android – IOS)



From the control panel towards the remote user:

The control panel can send:

- Alarms and alerts with "Push" notifications.

From the remote user towards the control panel

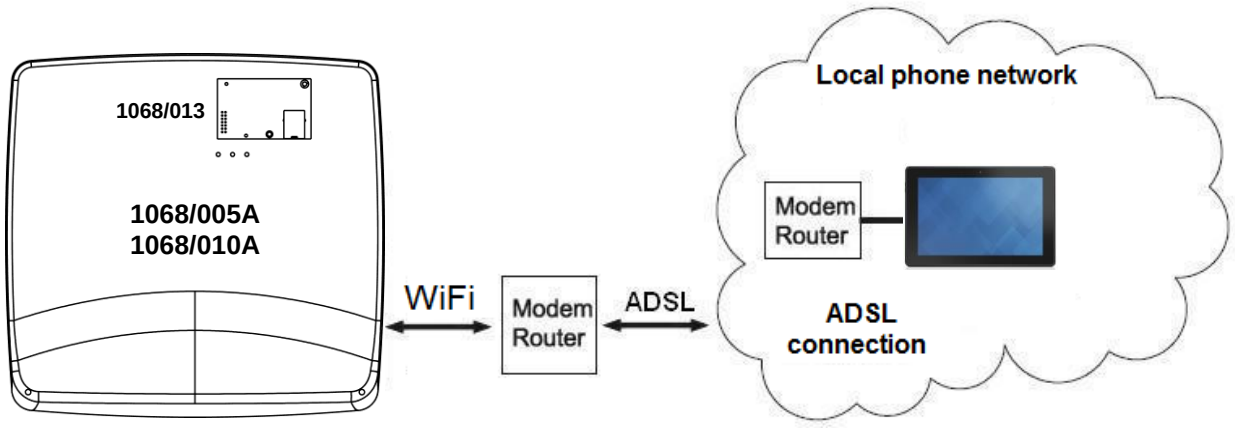
The user through mobile devices and/or tablets with Urmet Secure App can:

- Fully or partially arm the system
- Disarm the system
- Receive notifications of any alarms
- Check the status of the alarms in real time
- Check the operating status of the system in real time

The IP 1068/013 interface is an optional item and can be used in control panels, either as an alternative or together with the GSM/GPRS 1068/458 module.

Your smartphone must be equipped with the Urmet Secure App.

1.3.3 Remote user connection via a Tablet with 1068set Android App



From the control panel towards the remote user

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

From the remote user towards the control panel

The user via mobile devices and/or tablets with 1068set App can:

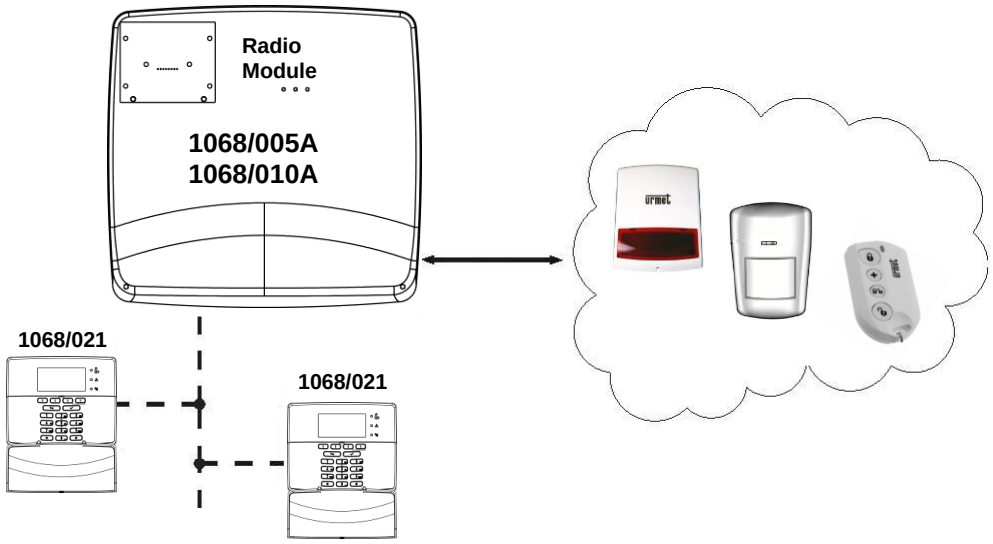
- Activate all or part of the system
- Disarm the system
- Receive notifications of any alarms
- Check the status of the alarms in real time
- Check the operating status of the system in real time
- Perform system configuration and programming

The IP 1068/013 interface is an optional item and can be used in control panels, either as an alternative or together with the GSM/GPRS 1068/458 module.

The tablet must be equipped with the 1068set Android App.

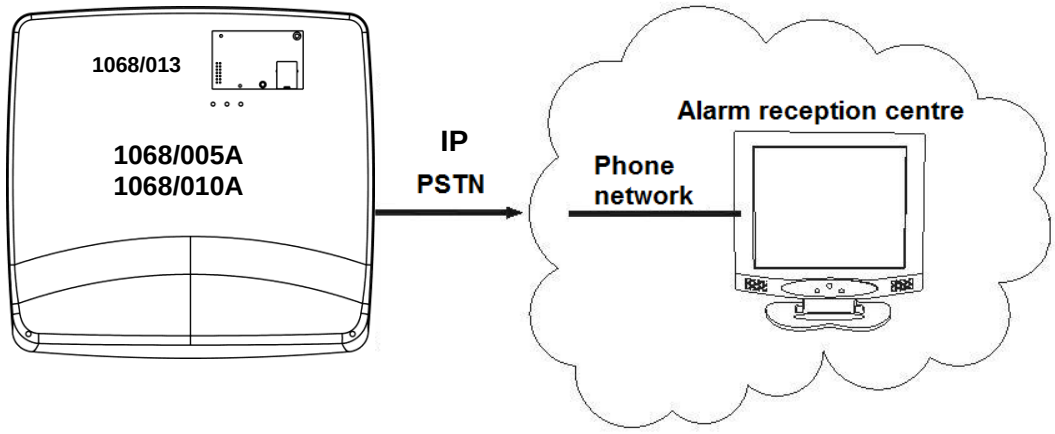
For further information, please see paragraph *3.11.8 Connecting the telephone communicator*.

1.3.4 Radio device connection

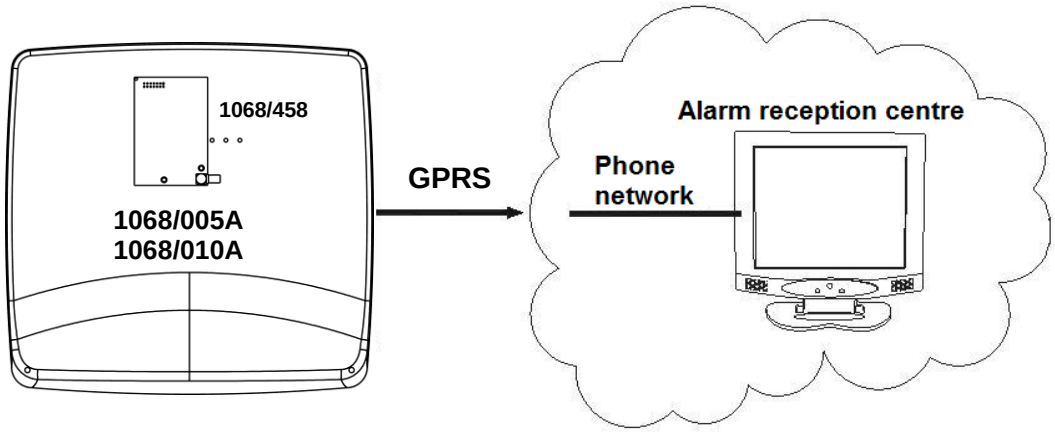


1.3.5 Connection with an alarm reception centre

1.



2.



1. With the IP 1068/013 interface, the control panel sends alarms and signals to the centre using the IDP/IP protocol.
2. With the GSM/GPRS 1068/458 module, the control panel sends alarms and signals to the centre using the IDP and IDP/IP protocols.

   (*****) The GSM / GPRS 1068/458 module used with the 1068/010A control panel complies with the EN50131 Grade 2.

For further information, please see paragraph *3.11.8 Connecting the telephone communicator*.

1.4 SYSTEM COMPONENTS

1.4.1 1068/005A Control panel

EN50131
GRADO 1

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:

- 5 inputs;
- 1 balanced SAB input;
- 4 outputs (2 relay outputs, 1 electric output and 1 internal siren command output);
- 1 switching power unit for circuit and indoor device powering nterni;
- Internal seating for battery.

The control panel manages up to 4 distinct zones.

Other characteristics of the control panel are:

- protection against opening and removal;
- saving of the last 500 events;
- management of a time scheduler.

The following LEDs are on the front side of the control panel:

Icon	Meaning
	Power supply
	Notices
	Zone status

1.4.2 1068/010A 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:

- 10 inputs (20 in Double Input mode);
- 1 balanced SAB input;
- 7 outputs (2 relay outputs, 4 electrics output and 1 internal siren command output);
- 1 switching power unit for circuit and indoor device powering nterni;
- Internal seating for battery.

The control panel manages up to 8 distinct zones.

Other characteristics of the control panel are:

- protection against opening and removal;
- saving of the last 1000 events;
- saving of the last 500 EN50131 events log;
- management of a time scheduler.

The following LEDs are on the front side of the control panel:

Icon	Meaning
	Power supply
	Notices
	Zone status

IMPORTANT! For compliance with EN50131 - Grade 2, is essential to use the 1068/458 GSM/GPRS module.

1.4.3 1068/021 LCD Command Keypad

EN50131 GRADO 1

Keypad with LCD display for interiors. It enables to control and program the 1068A series system and is equipped with:

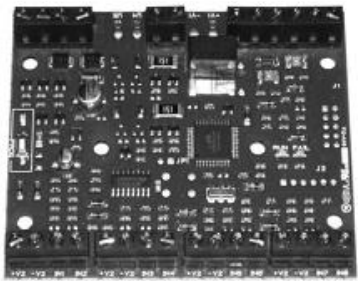
- Backlit LCD 128 x 64 pixel display with contrast and brightness adjustment;
- 3 system-state warning LEDs;
- 18 backlit keys;
- buzzer with adjustable volume;
- 1 programmable input.

The keypad is powered by the bus of the control panel to which it is connected.

Compliant with EN50131: Grade 1 - Class II - Type B.

1.4.4 1067/008A 8-input expansion module

EN50131



Expansion module equipped with:

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

IMPORTANT! The absence of a Grade 2 or 3 certified casing results in the loss of compliance with EN50131.

The module is connected to the control panel by bus.

1.4.5 Housing box for expansion module 1067/017

Housing box for the 1067/008A expansion module.

It comes equipped with a tamper device against opening and removal and makes it possible to maintain EN50131 Grade 3 compliant for the 1067/008A expansion module.

Compliant with EN50131: Grade 3 - Class II.

1.4.6 1067/334 - 335 Electronic key reader

The high-security electronic key reader is available with code 1067/334 - Electronic key reader kit including 3 keys, and with code 1067/335 - Additional key reader.

The device is equipped with:

- 4 warning LEDs: 3 for system status and 1 for alarm and signal memory;
- 2 inputs.
- The reader is suitable for installation on Bticino Magic frames and, using the Bticino adapter with Code A5374/1, on Bticino TT MATIX frames. The adapter frame supplied allows the installation of the reader on the Simon Urmet nea frames.
- By using the adapter frames (not provided), the reader can be inserted as a switch within the various civil lines on the market.
- The reader is powered by the bus of the control panel through which it is possible to configure it.

IMPORTANT! The absence of a tamper certified Grade 2 or 3 results in the loss of compliance with EN50131.

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

Compliant with EN50131: Grade 3 - Class II.

Also available in matt white with the product code1067/336.

1.4.7 1067/332 Additional keys kit

Electronic keys shall be used with 1067/334 – /335 – /336 readers for total or partial setting and unsetting of the system. Each key has a unique code, pre-set at the factory, with more than 1099 billion possible combinations.

They can be programmed:

- Up to 16 keys for the 1068/005A control panel
- Up to 32 keys for the 1068/010A control panel

Moreover, each key may be individually enabled or disabled and provided with an identification name.

The kit includes 3 keys which can be customized using the coloured gems included in the kit.

Key customisation can be worthy, for example, when a restricted operation has to be associated with a key.

1.4.8 1068/435 Proximity key reader

The proximity key reader “MIFARE Plus” is available as 1068/435 and is to be used with the keys included in kit 1068/432.

The device is equipped with:

- 4 warning LEDs: 3 for system status and 1 for alarm and signal memory;
- 2 programmable inputs.
- The reader is suitable for installation on Bticino Magic frames and, using the Bticino adapter with Code A5374/1, on Bticino TT MATIX frames. The adapter frame supplied allows the installation of the reader on the Simon Urmet nea frames.
- By using the adapter frames (not provided), the reader can be inserted as a switch within the various civil lines on the market.
- The reader is powered by the bus of the control panel through which it is possible to configure it.

Also available in matt white with the product code1068/436.

1.4.9 1068/432 Proximity key kit

"Mifare Plus" electronic keys shall be used with 1068/435 – /436 reader for total or partial setting and unsetting of the system. Each key has a unique code, pre-set at the factory, with more than 4 billion possible combinations.

They can be programmed:

- Up to 16 keys for the 1068/005A control panel
- Up to 32 keys for the 1068/010A control panel

Moreover, each key may be individually enabled or disabled and provided with an identification name.

The kit includes 3 keys which can be customized using the coloured gems included in the kit

Key customisation can be worthy, for example, when a restricted operation has to be associated with a key.

1.4.10 1068/011 Radio module

The optional radio module allows integrating in the control panels 1068A series radio devices, such as infrared detectors, magnetic contacts, sirens, remote controls and wireless keypads.
The radio module is connected through a special connector to the control panel and is equipped with antenna and transceiver at 868 MHz for two-way radio communication with paired radio devices.

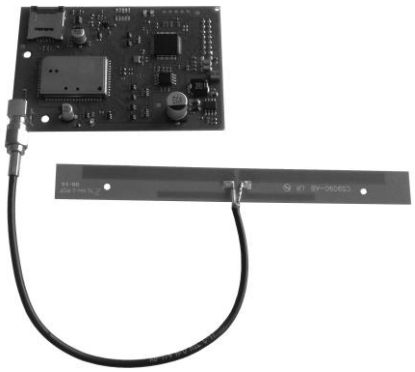
The radio module can manage up to:

- 28 IR detectors and/or magnetic contacts;
- 4 sirens;
- 8 remote controls;
- 4 wireless keypads.

Before using the module, remember to enable it, as it is disabled by default.
For the radio devices that may be paired to the 1068/011 radio module, please refer to the Urmet catalogue.

For further details and information, refer to the dedicated manual.

1.4.11 1068/458 GSM/GPRS module with vocal synthesis



Interface for connecting the 1068A series control panels to the mobile phone network (GSM) for sending alarm notifications and receiving remote commands.

The interface features a speech synthesis with messages that can be recorded by the user. The module is equipped with two-band GSM transmitter/receiver (900/1800 MHz) and it includes an antenna to be placed inside the control panel.

The GSM/GPRS 1068/458 interface is able to transmit alarms and notifications to reception centres, using the "Ademco® Contact ID protocol" (IDP) communication format.

The module is able to convey this format both through DTMF tones and TCP/IP (in this case, we are talking about IDP/IP).

(*****) The GSM / GPRS 1068/458 module used with the 1068/010A control panel complies with the EN50131 Grade 2.

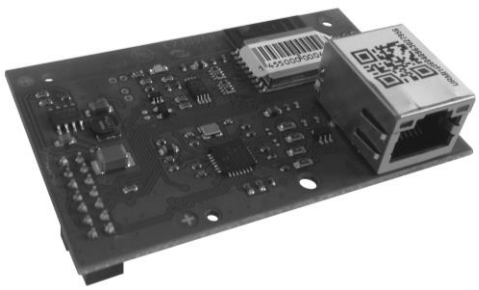
Before using the module, remember to enable it, as it is disabled by default.

1.4.12 1067/014 Remote GSM antenna

Optional external antenna to be used with the GSM/GPRS 1068/458 module when, due to the position of the control panel, the internal antenna provided with the package should not guarantee an adequate signal level. The remote antenna is supplied with a mounting bracket, blocks and 5m-long coaxial cable fitted with SMA-M connector.

(*****) The 1067/014 antenna used with the 1068/010A control panel, complies with the EN50131 Grade 2.

1.4.13 1068/013 IP interface



The Ethernet/Wi-Fi IP interface 1068/013 is an optional module which allows providing IP connectivity to control panels to allow integration with LAN network and thus remote management of control panels via APP on smartphone or tablet. The interface is directly connected to the control panel board by means of the connector and directly communicates with the host control panel by means of a dedicated serial connection.

The connection to the Internet network is made via the Ethernet or WiFi interfaces integrated in the device.

1.4.14 1068/017 Radio interface on Bus

Optional radio interface that makes it possible to integrate, radio devices as infrared detectors, magnetic contacts, sirens, remote controls radio keypads in the wired 1068A control panels series.
The radio interface is connected to the control panel via bus and is equipped with an antenna and 868 MHz receiver/transmitter apparatus for two-way radio communication with the combined radio devices.

The radio interface can manage up to:

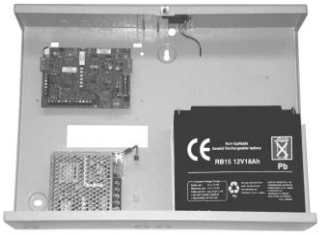
- 28 IR detectors and/or magnetic contacts;
- 4 sirens;
- 8 remote controls;
- 4 wireless keypads.

IMPORTANT! The 1068/017 radio interface is possible on the control panels and keypads that have at least SW version 1.010-xxx or higher.

For the radio devices that may be paired to the 1068/017 radio module, please refer to the Urmet catalogue.

For further details and information, refer to the dedicated manual.

1.4.15 1067/092 supplementary power supply with repeater



The 1067/092 supplementary power supply unit is an optional device for the 1068/010A control panel.

It comes equipped with an electronic board that integrates a 1067/008A 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 1067/092 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 100 - 240V~ - 14.4 V⎓ - 3.4 A; switching power supply; the use of a 12 V, 18 Ah battery backup is also provided.

From the revision sw 2.00.

1.4.16 1068/002 IP POE Interface

The interface Ref.1068/002 is a Ethernet board with 4 switch ports, one of which is PoE capable of supplying power to a PoE device. The board is connected to the power supply provided by the control panel and therefore can operate even in the absence of mains power.

1.4.17 1068/027 7” Touch screen keypad

Keypad with touch screen display for indoor use. Allows you to control and program the 1068A series systems.

The keypad is equipped with:

- 7" 1240 x 600 px IPS touch screen display.
- Integrates on its graphical interface the Urmet apps for the management of communication and home security.
- The graphic interface can be easily customized to suit the specific needs of use.
- It can be mounted on the wall or recessed with the 1760/61 accessory.
- PoE power supply via RJ45 port.

WARNING! For the operation of the touch keypad it is necessary that the FW versions are:

- 1068A series control panels: 1.025 or higher.
- Keypads: 1.025 or higher.
- IP: 1.025 or higher.

2 DESIGN: CALCULATIONS AND TESTS

2.1 SIZING OF THE POWER SUPPLIES AND THE BATTERIES

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

2.1.1 Battery sizing

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

1068/005A control panel with 7.2 Ah battery			
Duration	**Absorption allowed**		
	Control panel	**All the devices powered by the control panel**	**Total**
6 hours	75 mA	885 mA	960 mA
12 hours **(*)**	75 mA	405 mA	480 mA
24 hours	75 mA	165 mA	240 mA

(*) *minimum requirement for compliance with standard EN50131 - Grade 1.*

1068/010A control panel with 7.2 Ah battery					
EN50131	**Communicator used**	**Duration**	**Absorption allowed**		
			Control panel	**All the devices powered by the control panel**	**Total**
Grade 2	ATS2	6 hours	115 mA	845 mA	960 mA
Grade 2	ATS2	12 hours **(*)**	115 mA	365 mA	480 mA
Grade 2	ATS2	24 hours	115 mA	125 mA	240 mA

(*) *minimum requirement for compliance with standard EN50131 - Grade 2.*

Table 3 - Control panel battery autonomy

The power supply for all internal circuits and devices is provided by an internal switching power supply unit. A 12 V, 7.2 Ah rechargeable lead-acid battery is to be used.

The battery to be used must:

- Be of the VRLA (Valve Regulated Lead Acid) type
- Have an enclosure with flammability class UL94V-1 or better
- Be compliant with standards IEC 60896-21:2004, IEC 60896-22:2004

2.1.2 Calculation of the total absorption of the system

Before proceeding with the installation, it is necessary to calculate the total absorption of the system in order to be able to size the power supply units and batteries.

The calculation procedure is as follows:

- List all the necessary devices, their quantity and maximum absorption per unit in stand-by (which is all available from the technical data sheets), multiplying 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	75 mA	=	75 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**

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).

2.2 CABLE SIZING

The formulas for sizing the connection and power cables are illustrated below.

There are also the criteria to follow when creating the bus.

2.2.1 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 mm^2.

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

The cables used must comply with IEC 60332-1-2 if they have a cross-section of 0.5 mm^2 or more, or with IEC 60332-2-2 if they have a cross-section of less than 0.5 mm^2.

IMPORTANT! Never connect the cable shields to the earth.

When installing the cables, keep the intrusion alarm system cables separate from the electrical system cables using separate ducts.

2.2.2 Sizing of the power supply cable

The cross-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 cross-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 back-up battery at the hibernation voltage (11.4 V⎓). Under these conditions, when fully charged, all the devices must be guaranteed with at least 9 V⎓.

IMPORTANT!

Check that there is, in any case, the minimum operating voltage of the other devices used, like the IR detectors, actuators, sirens, etc...

Some of these devices may require a power supply voltage of over 9 V⎓ (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: 2.4 V⎓

or 1.2 V on the positive cable and 1.2 V on the negative cable

The formula to calculate this is

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

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 in mm² (*)	0.22	0.50	0.75	1.00	1.50
Resistance in Ohm/m	0.0795	0.0350	0.0233	0.0175	0.0117

Table 4 - Copper wire resistance

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

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

For example, for the various cable cross-sections, the maximum permissible lengths are given in relation to the maximum current circulating in the cable.

Cross-section 0.22 mm²	
Current	**Length**
0.300 A	31 m
0.500 A	19 m
0.750 A	13 m
1.000 A	9 m
1.500 A	6 m
2.000 A	5 m
2.500 A	4 m
3.000 A	3 m

Cross-section 0.50 mm²	
Current	**Length**
0.300 A	71 m
0.500 A	43 m
0.750 A	29 m
1.000 A	21 m
1.500 A	14 m
2.000 A	11 m
2.500 A	9 m
3.000 A	7 m

Cross-section 0.75 mm²	
Current	**Length**
0.300 A	107 m
0.500 A	64 m
0.750 A	43 m
1.000 A	32 m
1.500 A	21 m
2.000 A	16 m
2.500 A	13 m
3.000 A	11 m

Cross-section 1 mm²	
Current	**Length**
0.300 A	143 m
0.500 A	86 m
0.750 A	57 m
1.000 A	43 m
1.500 A	29 m
2.000 A	21 m
2.500 A	17 m
3.000 A	14 m

Cross-section 1.5 mm²	
Current	**Length**
0.300 A	214 m
0.500 A	129 m
0.750 A	86 m
1.000 A	64 m
1.500 A	43 m
2.000 A	32 m
2.500 A	26 m
3.000 A	21 m

2.2.3 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, i.e. 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.

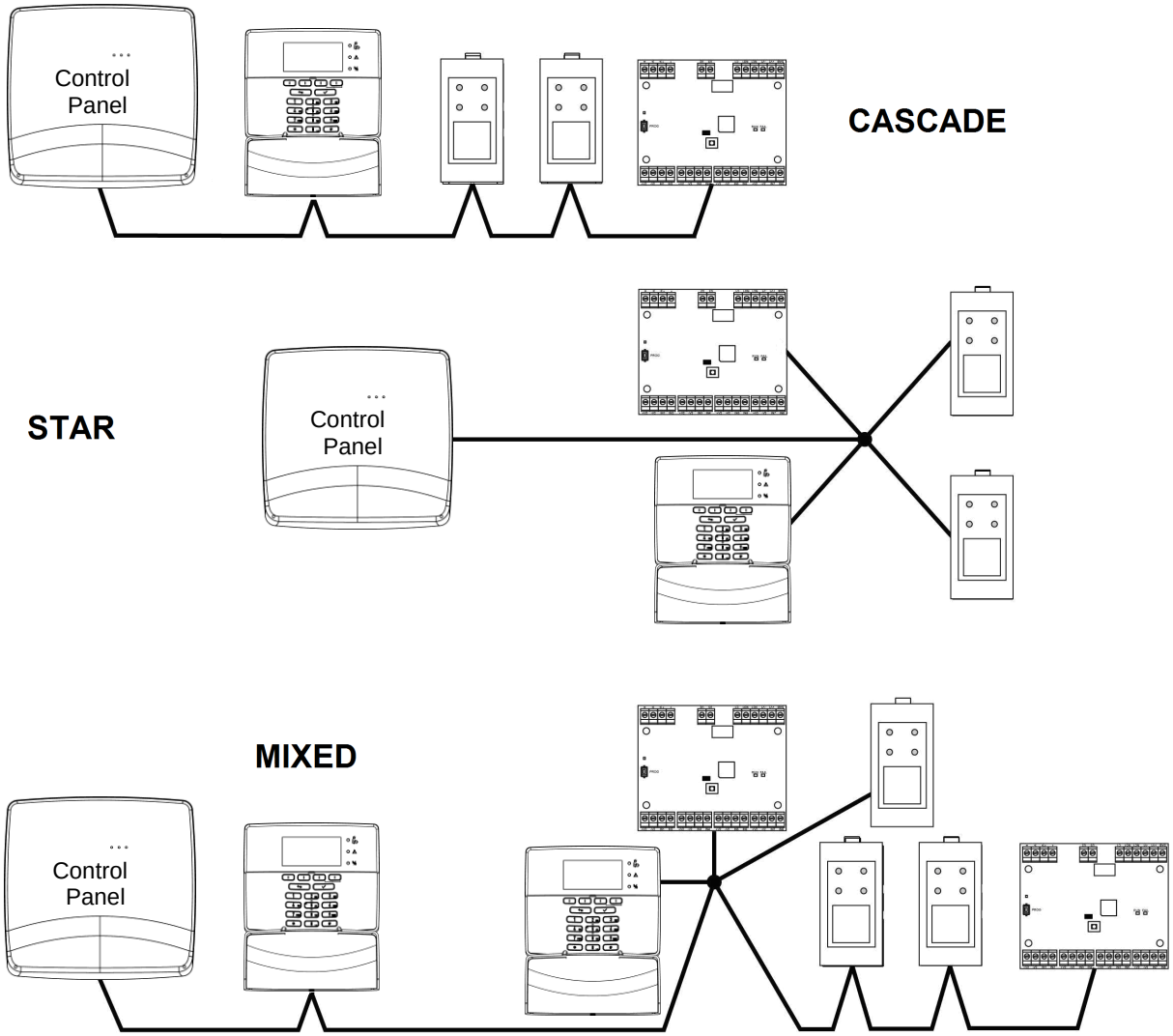


Figure 3 - Topologies of the bus connection

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

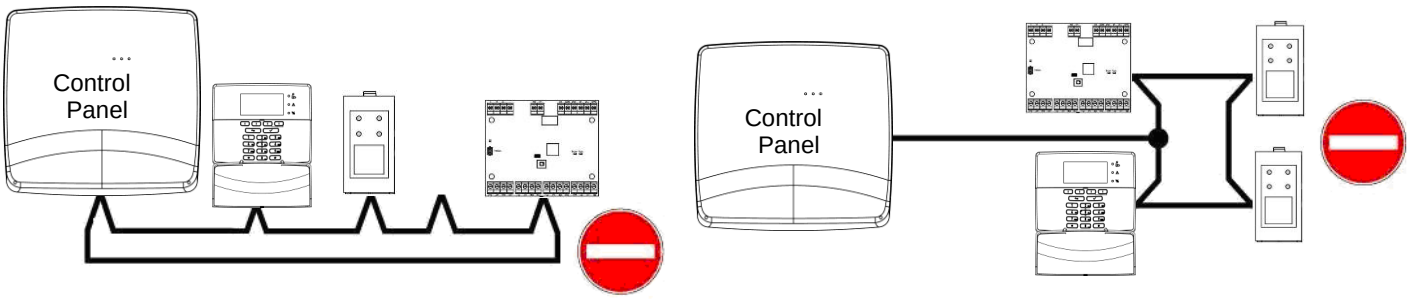


Figure 4 - Closed rings on the bus

It is not necessary to end 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 "**–**".

2.2.4 Extending the bus with the repeater

The 400-metre length limit of the bus can be overcome with the use of the 1067/092 supplementary power supply unit.
Indeed 1067/092 power supplies, in fact, in addition to serving as supplementary power supplies, they make the repeater function available.

	**IMPORTANT!** The supplementary power supply 1067/092 can only be used with the 1068/010A control panel.

When using the repeater with the 1068/010A control panel, always follow 3 simple rules:

- The maximum number of repeaters allowed is è 7.
- 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.

2.2.4.1 System with 1 supplementary power supply repeater

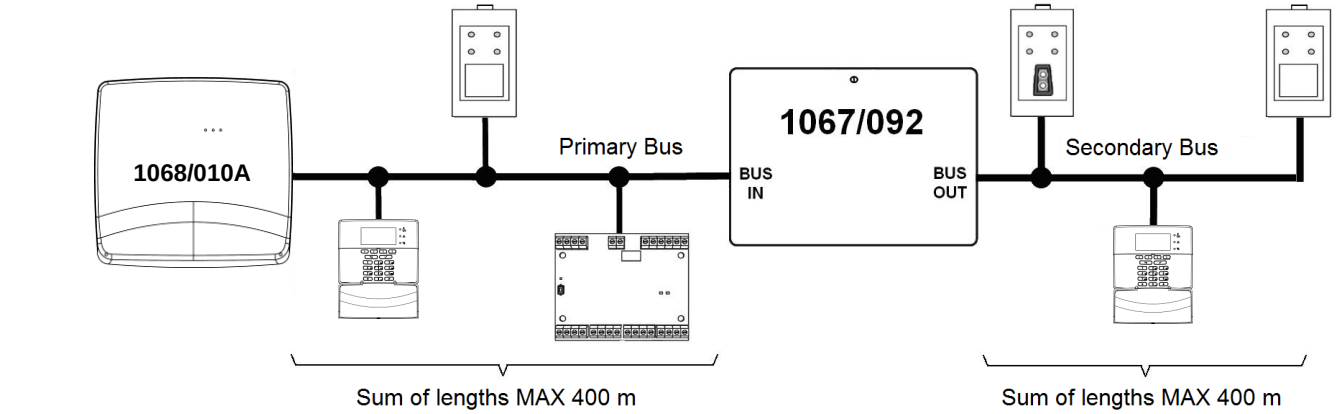


Figure 5 - Diagram with 1 supplementary power supply repeater

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**

2.2.4.2 System with 2 supplementary power supply repeaters

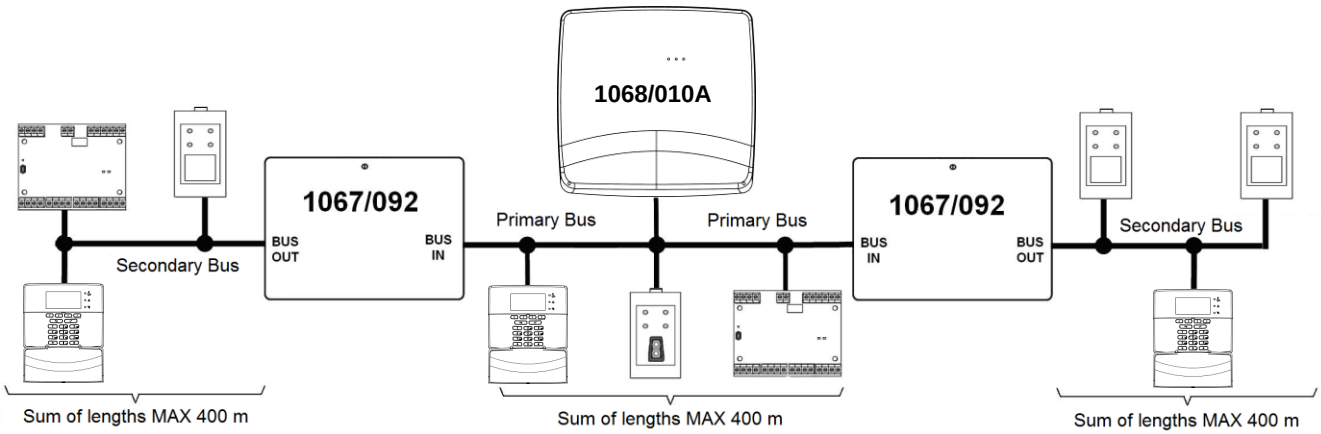


Figure 6 - Diagram with 2 supplementary power supply repeater

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**

2.2.4.3 System with multiple supplementary power supply repeaters

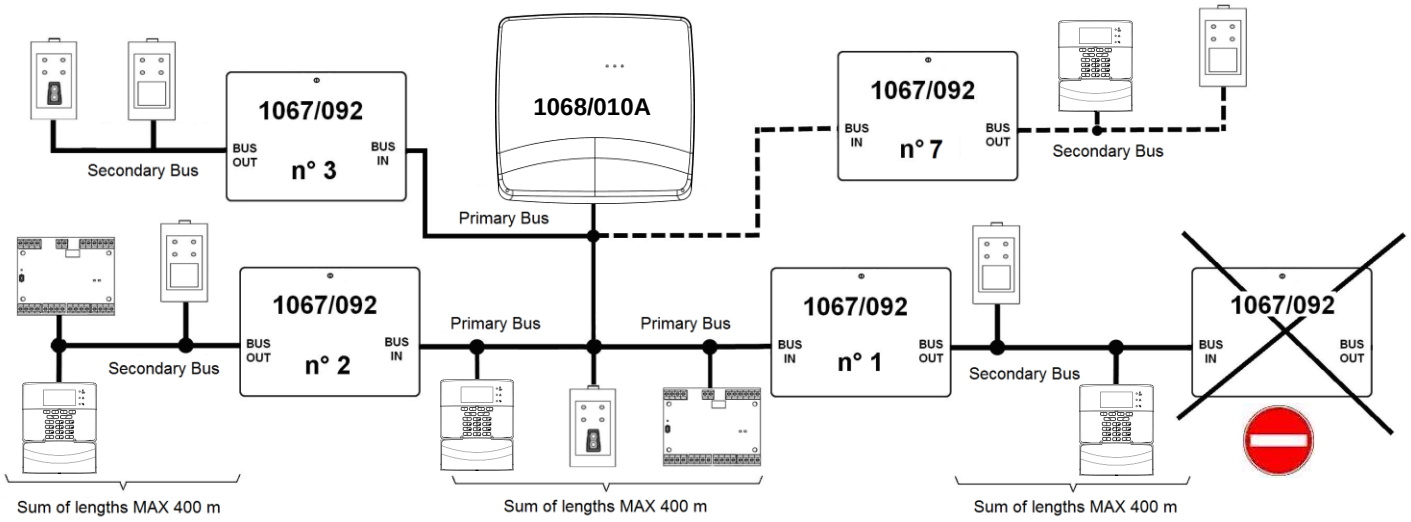


Figure 7 - Diagram with 7 supplementary power supply repeater

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 =	**3200 m**

2.2.5 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 (roller, inertial, etc.), the length of the connection must not exceed 100 metres.

2.3 CONTROL CRITERIA OF THE MAINS POWER SUPPLY VOLTAGE

The alarm systems constantly controls the presence of the power supply in the control panel, which is detected by checking the presence of voltage in the power supply unit.

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

2.3.1 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 control panel and keypads start flashing, 10 seconds after a power failure is detected, to signal the problem;
- The event is recorded in the system log (instantaneous power failure);
- The system does not generate an alarm immediately, but starts counting the power failure time (1 minute by default). This parameter can be modified during programming. Every time electrical power is restored, the power failure time count is reset to zero.

The delay determined by the power failure time 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 phone message to signal a brief blackout and a successive call at the time power is restored are avoided.

2.3.2 Continued blackout alarm

If the blackout persists until the set loss of mains time expires, the following occurs:

- The system generates a “Protracted loss of mains alarm”;
- The specialised power failure outputs are activated;
- A dedicated alarm message is sent via the phone dialer;
- The alarm is stored in the System log.

IMPORTANT!

If the battery level descends below the threshold of 12.5 V, the “Protracted loss of mains alarm” is generated immediately, even if the power failure time has not yet passed.

2.3.3 Restoration of the mains power supply

Once the mains power supply is restored, the green power supply LEDs of the keypad control panel stop flashing after 10 seconds and remain on while the system restarts a time count.

Once 5 minutes have passed, if the power has been continuously present:

- The phone dialer sends the message dedicated to the restoration of mains;
- The event of the restoration of the mains is memorised in the System log.

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

2.4 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 **BAT+** and **BAT-**.

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.

2.4.1 Controlling the battery with mains power supply absent

In the event of a power failure, the system constantly monitors the status of the battery.

When the voltage at the battery terminals falls below 12.5 V, the “Battery low” event is generated”.

When the voltage at the ends of the battery drops further and reaches the value of 11.4 V, the control panel activates the hibernation mode with limited irreversible operation.

The hibernation mode is disabled only after the power voltage has been restored for at least 5 seconds and the control panel has been restarted.

2.4.2 Battery test in presence of mains

The "Battery Test" is performed periodically to monitor battery efficiency:

- 60 seconds after the control panel has been restarted or the power supply is restored;
- Periodically (the period can be scheduled in hours);
- After a “Battery Test” command from the Installer or Master menu (manual test);
- Following system activation (if previously configured);
- Following system deactivation (if previously configured).

The Battery Test 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 followed by relevant alarm. The “Battery low” status lasts until the next “Battery test” that concludes with a positive result.

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

2.5 SELF-DIAGNOSTIC FUNCTIONS

The system carries out autonomous and continuous self-diagnosis checks:

- Control of the system power supply voltages;
- Control of the correct communication among the devices;
- Control of the correct functioning of the control panel CPU;
- Control of the SIM-Card and connection with the GSM phone network.

If the system encounters a critical condition, it records the beginning and end of the event in the System Log.

Some anomalies can also activate dedicated outputs.

3 INSTALLATION

This chapter will explain 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.

3.1 INSTALLATION PROCEDURE

To install an alarm system with the 1068A series control panels in the shortest possible time, while ensuring the best result, follow the steps below:

1) Wiring;
2) Installation of the control panel on the wall;
3) Assembly of expansions, optionals, and accessories in the control panel;
4) Connections in the control panel;
5) Installation and connection of expansions, keypads, and readers;
6) Installation and connection of the detectors and alarm and signalling devices;
7) Power supply and acquisition of the devices;
8) System configuration and testing.

The steps can be carried out also in a different order, for example step 3 can be anticipated and performed in the laboratory.

Even steps 7 and 8 can be completed beforehand, in the laboratory, 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.

Step 8 can be performed on a tablet featuring the 1068set Android App. The configuration obtained can be downloaded on site directly from the tablet or from a micro SD card on which it was previously stored.

3.2 WIRING

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

IMPORTANT!

When installing the cables, keep the intrusion alarm system cables separate from the electrical system cables using separate ducts.

IMPORTANT!

In compliance with the electrical safety standards, the wiring must be done carefully and all the cables must be blocked in position near the terminal boards to prevent the Safety Extra Low Voltage conductors (SELV) from making contact with dangerous live wires (mains terminals). Secure the cables by fastening them in provided anchoring points with ties.

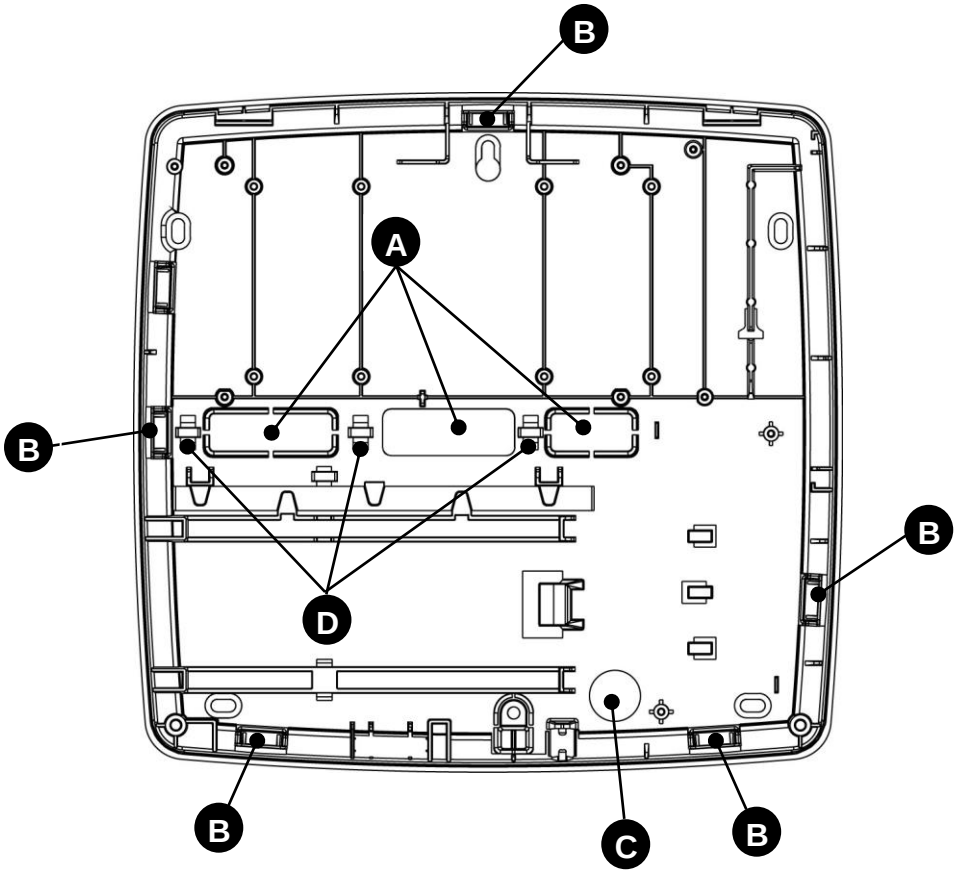
3.3 PREPARING THE 1068/005A – 1068/010A CONTROL PANEL

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

To prepare the control panel for installation, proceed as follows:

1. Open the cover of the control panel using a Phillips screwdriver (PH 0x60).

2. For the routing of the cables (power supply, bus, detectors and signalling devices, phone line, if any), use the various prearrangements of the control panel:



The set-ups for running the cables are:

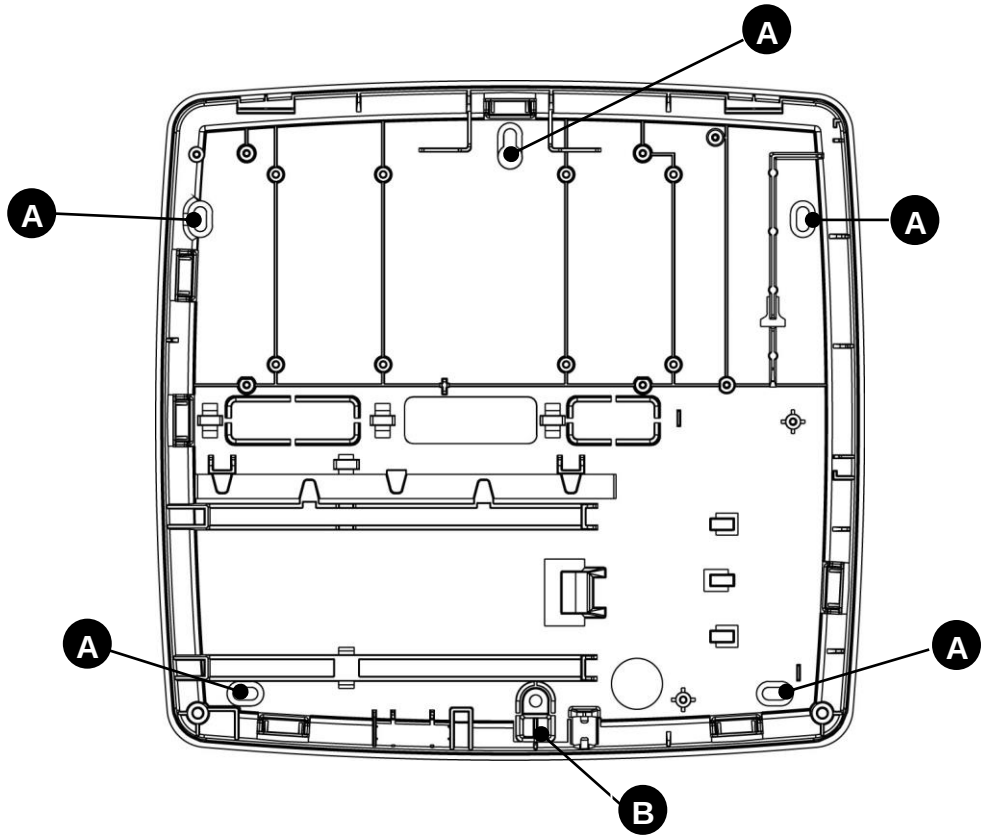
A - for embedded corrugated tube;

B - for rectangular wall duct or rigid tube;

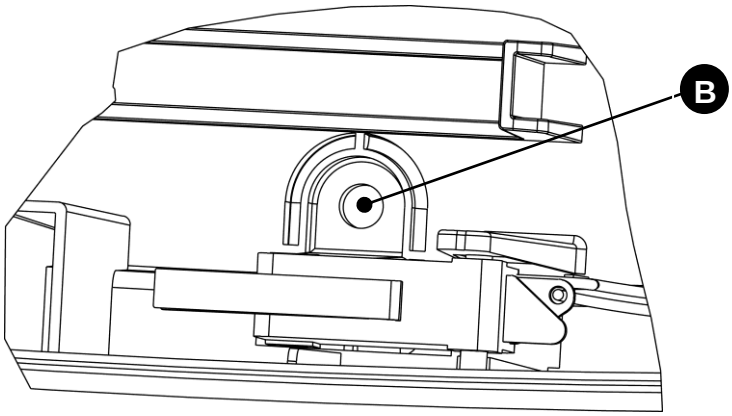
C - for corrugated tube dedicated to the power supply

D - points for anchoring cables with ties.

3. Secure the control panel bottom to the wall by means of screws and plugs (not provided). Use Ø 6mm plugs depending on the type of material making up the wall with TCB screw DIN 7981 3.9 x 32.
   For a firm fastening, it is necessary to use at least 3 holes.

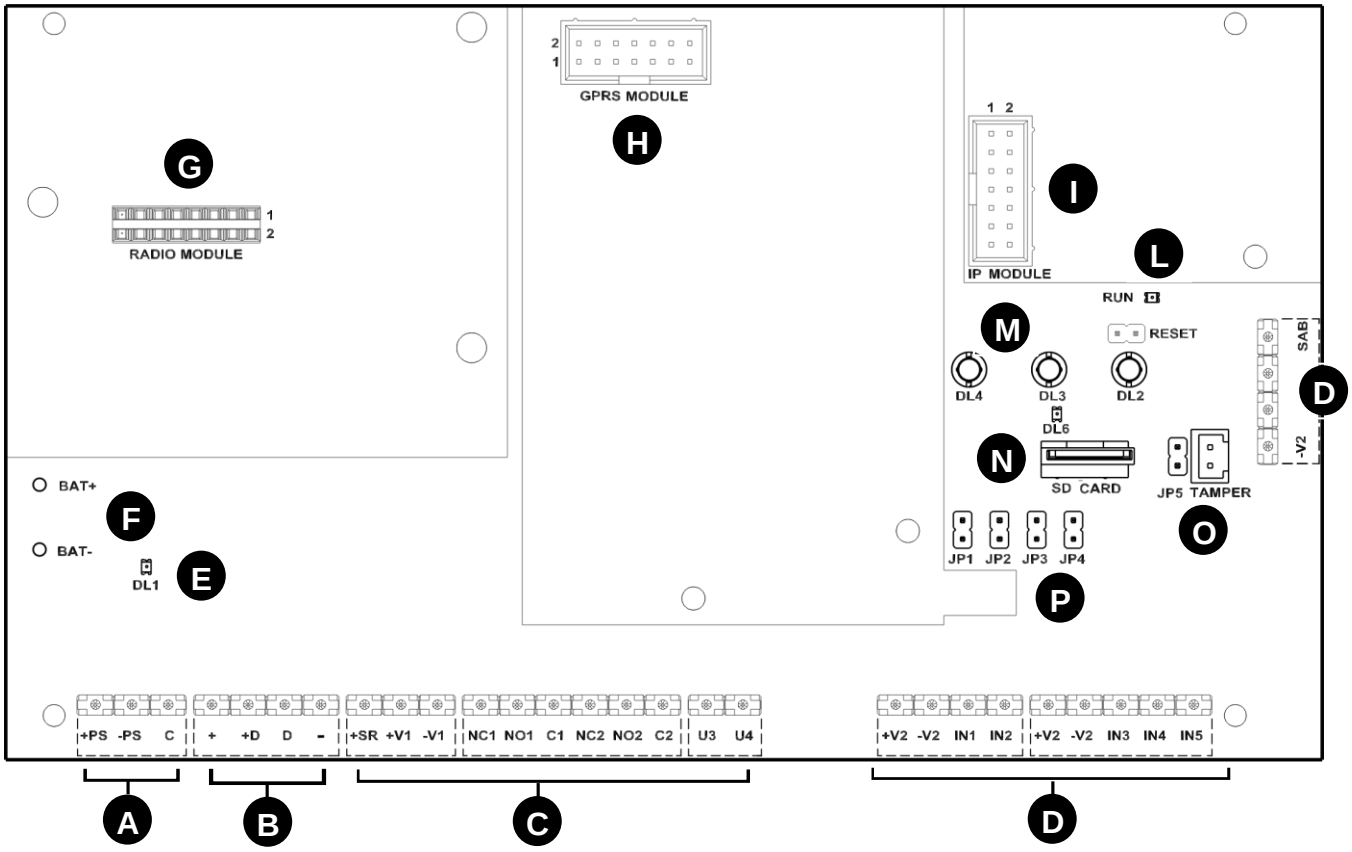


To ensure the "removal" protection of the control panel, it is necessary to use the fixing hole **B**.



3.4 INSTALLATION OF THE 1068/005A – 1068/010A CONTROL PANELS

3.4.1 Description of the main parts of the 1068/005A control panel



Detail	Terminal / Detail	Description
A	+PS	Input +14.4 V⎓ power supply (at the positive pole of the power unit)
	–PS	Input power supply (at the negative pole of the power unit)
	C	Power supply unit control signal (battery test)
B	+	BUS - Power supply (13.8 V⎓ limited to 1.1A) for devices connected via bus
	+D	Bus polarisation
	D	Bus data line
	–	BUS - Power supply (13.8 V⎓ limited to 1.1A) for devices connected via bus
C	+SR	Dedicated power supply for external siren
	+V1	Positive power supply for external devices
	–V1	Negative power supply for external devices
	NC1	Normally closed contact (NC) - external siren relay output
	NO1	Normally open contact (NO) - external siren relay output
	C1	Contact C - external siren relay output
	NC2	Normally closed contact (NC) - additional relay output
	NO2	Normally open contact (NO) - additional relay output
	C2	Contact C - additional relay output
	U3	Internal Siren Output
	U4	System Status/Reset Memories electric output

D	**+**V2	2 Sensor positive power supply
	–V2	3 Sensor negative power supply
	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
	SAB	Input 24h (for system self-protection). It must always be BALANCED and closed with a 2.7 kΩ balancing resistor.
E	DL1	External power supply presence LED
F	**+**BT	Connection of positive pole of the back-up battery
	–BT	Connection of negative pole of the back-up battery
G	RADIO MODULE	Radio module connector
H	GPRS MODULE	GSM/GPRS module connector
I	IP MODULE	IP module connector
L	RUN	Green LED signalling control panel operation
M	DL2	Zone Status LED
	DL3	Warning LEDs
	DL4	Power LED
N	DL6	Micro SD Card signalling LED
	SD CARD	Slot for micro SD Card insertion
O	JP5	Jumper for the exclusion of the control panel tamper
	TAMPER	Connector for connection of the control panel tamper
P	JP1	Jumpers to reset parameters – see functions associated with the dip-switches (Table 5). (Normally they must be left open. If the control panel is in operating mode conforming to EN50131, JP4 must be closed).
	JP2	
	JP3	
	JP4	

Functions associated with Jumpers

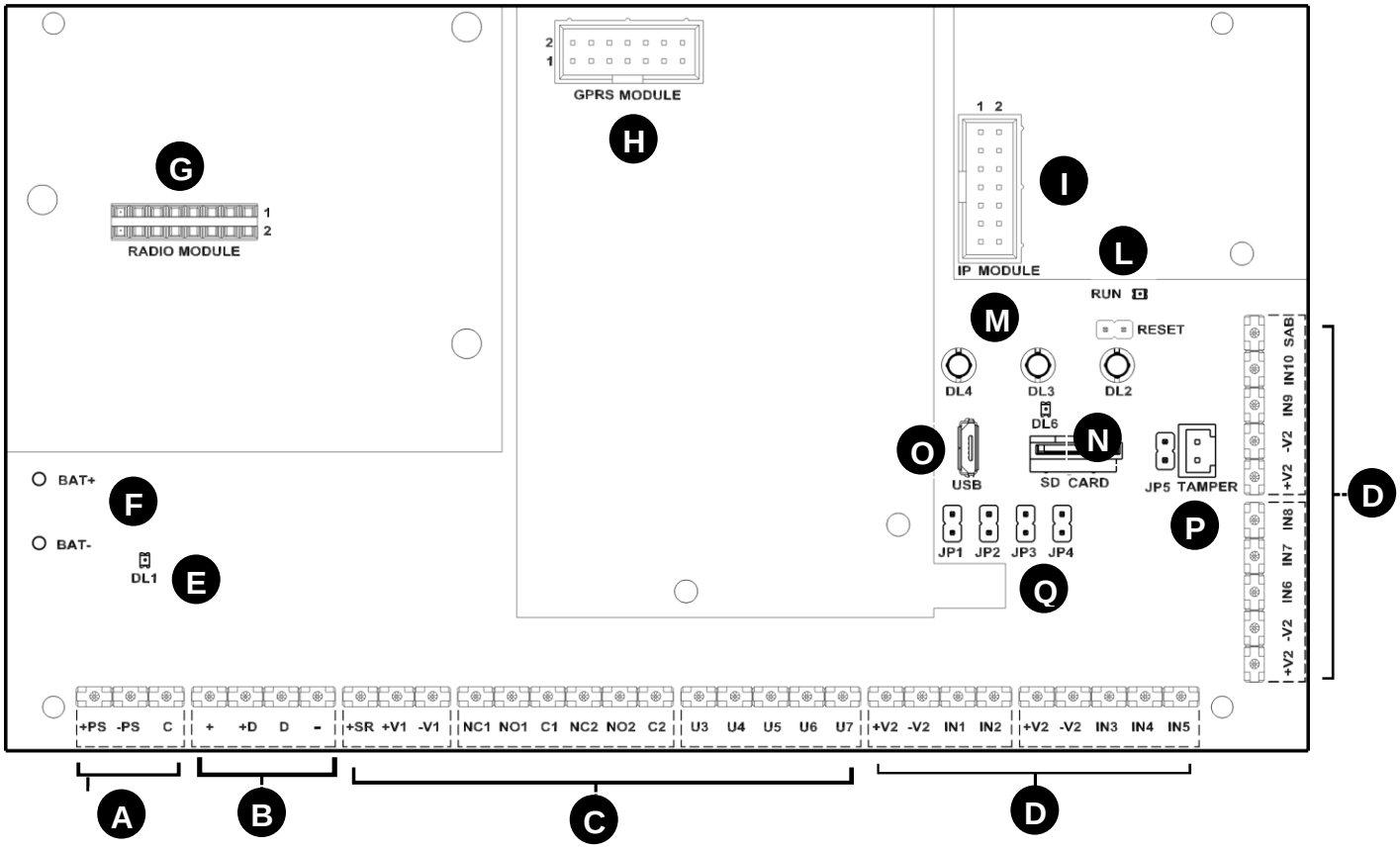
To activate the reset functions associated with the Jumpers, it is necessary to follow the indications found in paragraphs *9.13.4 Installer hardware code reset* and *9.13.6 Hardware reset to factory settings*.

JUMPER	POSITION	FUNCTION
JP1	Open	Normal operation
	Closed *	IP module reset
		Reset of HW factory settings (JP2 also closed)
JP2	Open	Normal operation
	Closed *	Reset of HW factory settings (JP1 also closed)
JP3	Open	Normal operation
	Closed *	Reset Installer code
JP4	Open	Mode not compliant with standard EN50131
	Closed *	Mode compliant with standard EN50131
JP5	Open	Normal operation
	Closed	Tamper disabling

Table 5 - Functions associated with the DIP-switches of the mother board

(*) To operate on jumpers, power down the control panel and then power it on again.

3.4.2 Description of the main parts of the 1068/010A control panel



Detail	Terminal / Detail	Description
A	+PS	Input +14.4 V⎓ power supply (at the positive pole of the power unit)
	–PS	Input power supply (at the negative pole of the power unit)
	C	Power supply unit control signal (battery test)
B	+	BUS - Power supply (13.8 V⎓ limited to 1.1A) for devices connected via bus
	+D	Bus polarisation
	D	Bus data line
	–	BUS - Power supply (13.8 V⎓ limited to 1.1A) for devices connected via bus
C	+SR	Dedicated power supply for external siren
	+V1	Positive power supply for external devices
	–V1	Negative power supply for external devices
	NC1	Normally closed contact (NC) - external siren relay output
	NO1	Normally open contact (NO) - external siren relay output
	C1	Contact C - external siren relay output
	NC2	Normally closed contact (NC) - additional relay output
	NO2	Normally open contact (NO) - additional relay output
	C2	Contact C - additional relay output
	U3	Internal Siren Output
	U4	System Status/Reset Memories electric output
	U5	Additional electrical output
	U6	Additional electrical output
	U7	Additional electrical output

D	**+**V2	4 terminals block for detectors positive power supply
	–V2	4 terminals block for the negative power supply of the detectors
	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
	IN9	Alarm input n. 9
	IN10	Alarm input n. 10
	SAB	Input 24h (for system self-protection). It must always be BALANCED and closed with a 2.7 kΩ balancing resistor.
E	DL1	External power supply presence LED
F	**+**BT	Connection of positive pole of the back-up battery
	–BT	Connection of negative pole of the back-up battery
G	RADIO MODULE	Radio module connector
H	GPRS MODULE	GSM/GPRS module connector
I	IP MODULE	IP module connector
L	RUN	Green LED signalling control panel operation
M	DL2	Zone Status LED
	DL3	Warning LEDs
	DL4	Power LED
N	DL6	Micro SD Card signalling LED
	SD CARD	Slot for micro SD Card insertion
O	USB	USB Connector
P	JP5	Jumper for the exclusion of the control panel tamper
	TAMPER	Connector for connection of the control panel tamper
Q	JP1	Jumpers to reset parameters – see functions associated with the dip-switches (Table 6). (Normally they must be left open. If the control panel is in operating mode conforming to EN50131, JP4 must be closed).
	JP2	
	JP3	
	JP4	

Functions associated with Jumpers

To activate the reset functions associated with the Jumpers, it is necessary to follow the indications found in paragraphs *9.13.4 Installer hardware code reset* and *9.13.6 Hardware reset to factory settings*.

JUMPER	POSITION	FUNCTION
JP1	Open	Normal operation
	Closed *	IP module reset
		Reset of HW factory settings (JP2 also closed)
JP2	Open	Normal operation
	Closed *	Reset of HW factory settings (JP1 also closed)
JP3	Open	Normal operation
	Closed *	Reset Installer code
JP4	Open	Mode not compliant with standard EN50131
	Closed *	Mode compliant with standard EN50131
JP5	Open	Normal operation
	Closed	Tamper disabling

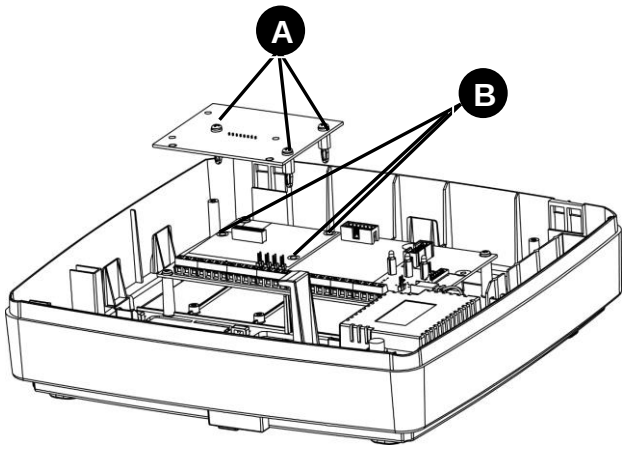
Table 6 - Functions associated with the DIP-switches of the mother board

(*) To operate on jumpers, power down the control panel and then power it on again.

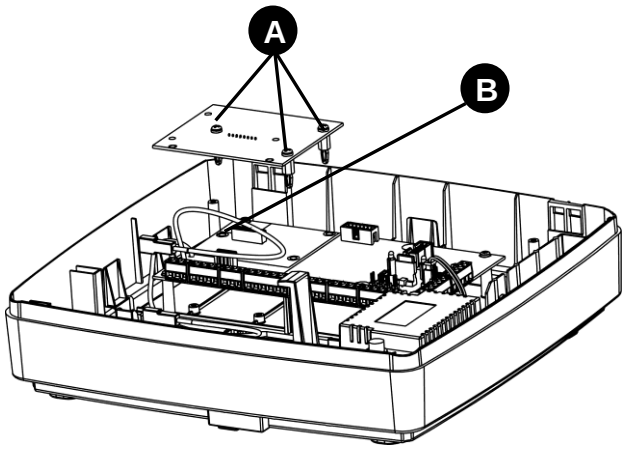
3.4.3 Installing the 1068/011 Radio module

The Radio module is already fitted with three guiding spacers **A.**
Follow the instructions below for the installation:

1. Insert the module into the three holes **B**.



1068/005A Control panel



1068/010A Control panel

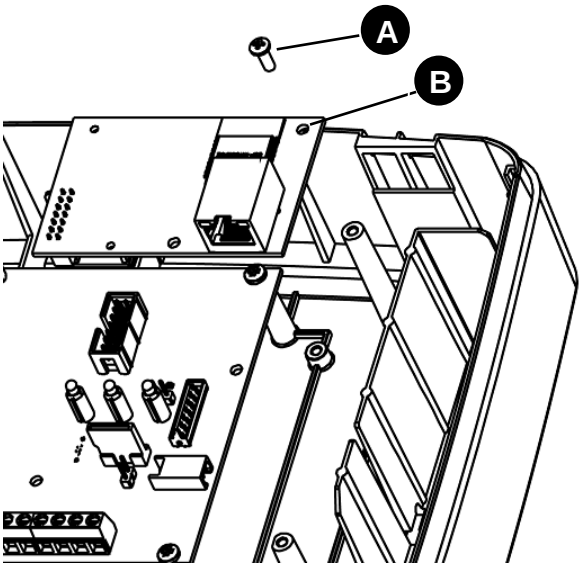
IMPORTANT!

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).

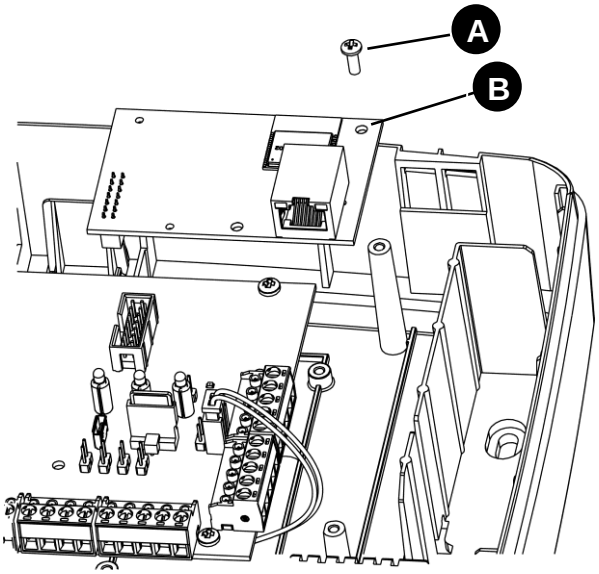
3.4.4 Installing the 1068/013 IP module

To install the IP interface, follow the instructions below:

1. Insert the board in the space provided.
2. Screw the supplied screw **A** into hole **B**.



1068/005A Control panel



1068/010A Control panel

3.4.5 Installing the 1068/002 IP POE interface

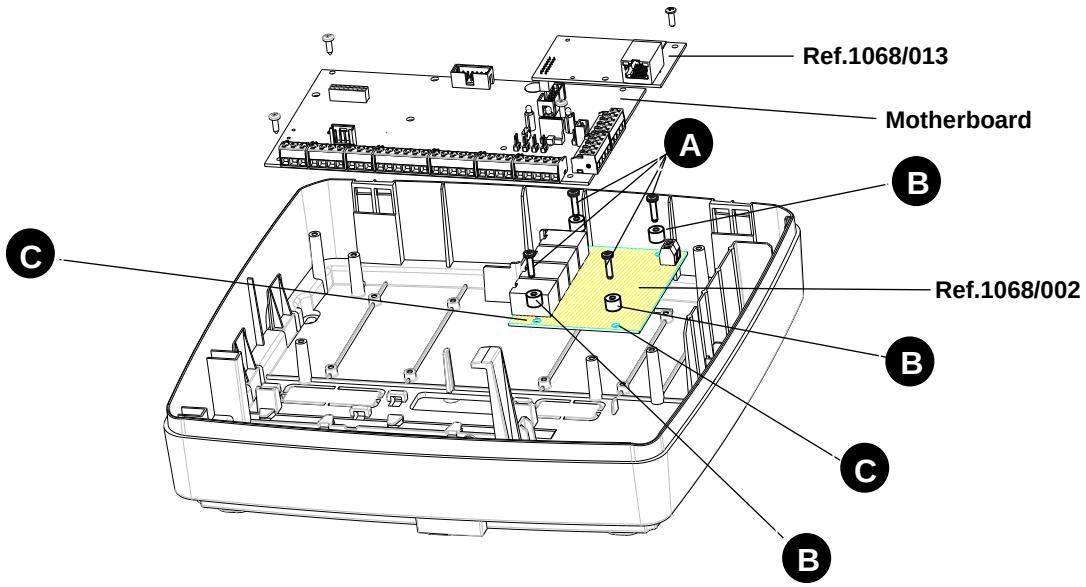
Proceed as follows to mount the interface inside the 1068A series control panels:

1. Remove the motherboard.
2. Insert the Ref.1068/002 in the space provided and fix it to the bottom in the holes provided (**C**) using the 4 screws (**A**) inserted in the supplied spacers.
3. Connect the cable supplied with Ref.1068/002 to connect it to Ref.1068/013 (see paragrap *3.11.3 Connecting IP POE interface*).
4. Refit the motherboard.
5. Insert board 1068/013 by connecting the cable leading out of interface Ref.1068/002.

Additionally, the interface can be inserted:

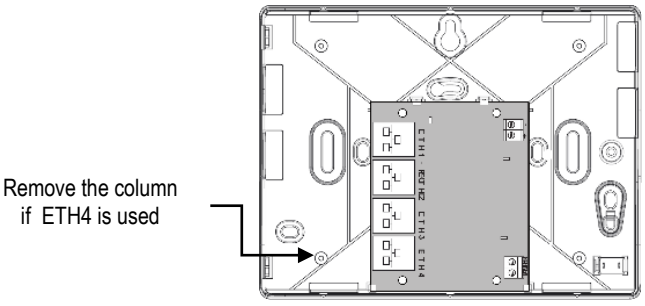
- in wall boxes Ref.1067/017.
- in distribution boxes or similar containers.

NOTE: *Use the external antenna (e.g. Ref.1067/014) if the Ref.1068/002 interface is inserted into the housing provided inside the control panel for optimum signal reception.*



Housing in plastic box

A	Screws for fixing
B	Spacers supplied
C	Holes for fixing Ref. 1068/002

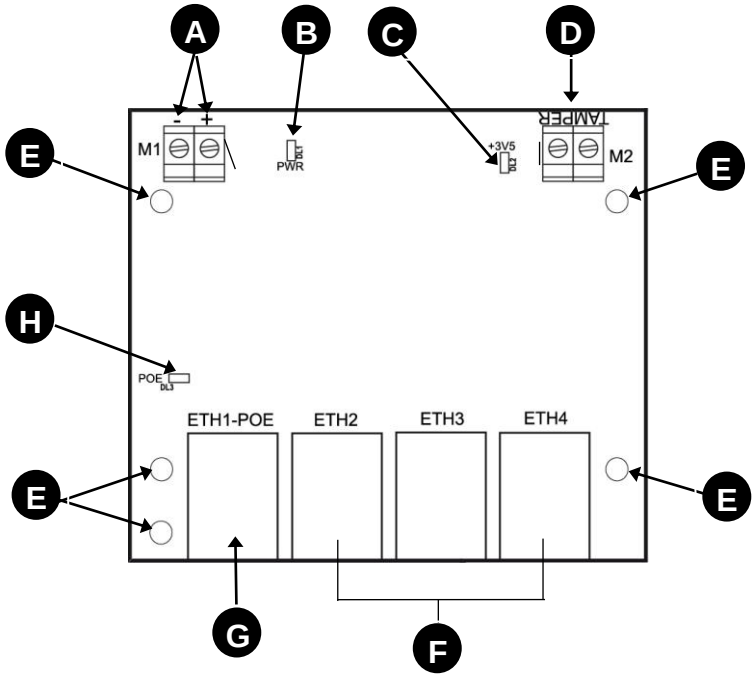


Housing inside the box Ref.1067/017

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).

3.4.5.1 Description of the main parts of the 1068/002 interface



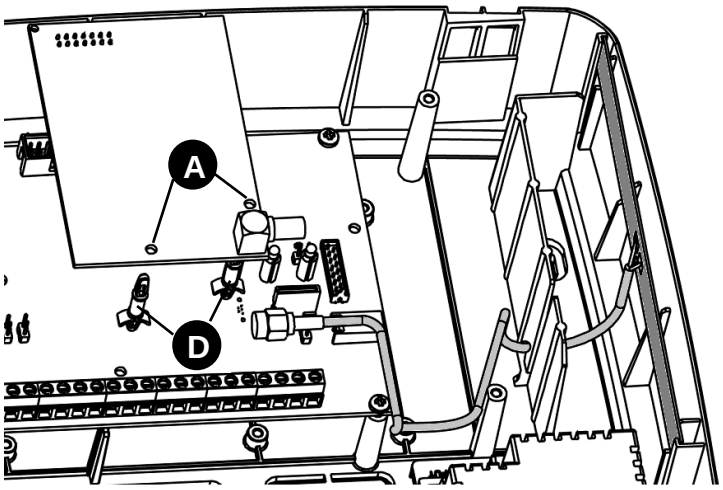
A	**+**	Positive power supply (13.8 V⎓)
	-	Negative power supply (Gnd)
B	PWR	LED power present
C	+3V5	LED logical power present (+3.5V⎓)
D	TAMPER	Terminal for tamper protection
E	------	Holes for fastening
F	ETH2,3,4	RJ45 Ethernet connectors
G	ETH1-POE	RJ45 POE Ethernet connector
H	POE	POE status LED

3.4.6 Installing the 1068/458 GSM/GPRS module with vocal synthesis

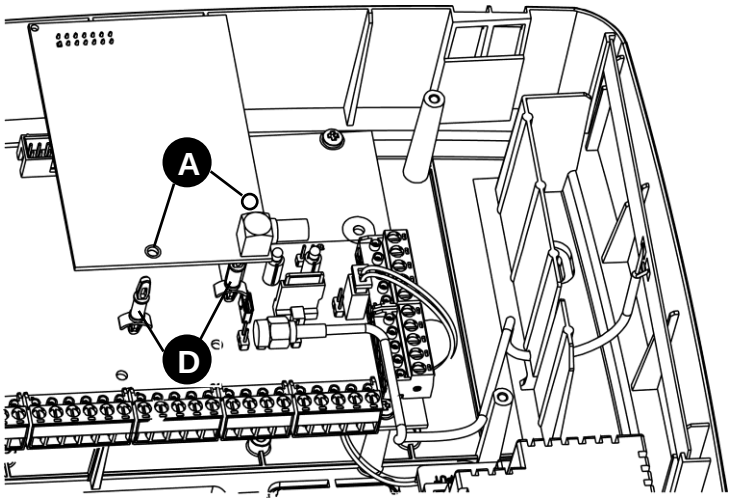
The GSM module enables the 1068/005A or 1068/010A control panel to communicate with the outside world via vocal messages, SMS and audio numerical protocol. The GSM/GPRS module allows communication via numerical data protocols.

To install the module, follow the instructions below:

1. Insert the supplied support spacers **D** in the two holes **A**.



1068/005A Control panel



1068/010A Control panel

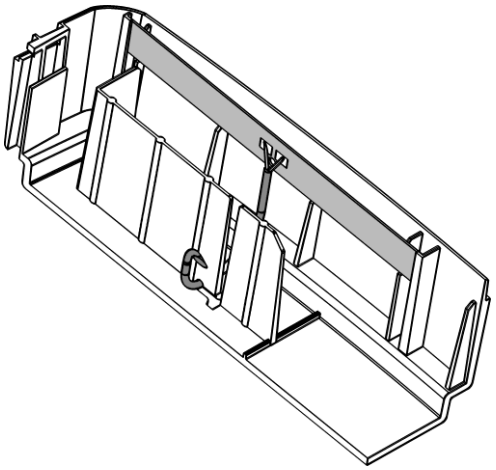
IMPORTANT! The use of the GSM module invalidates EN50131 compliance.

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).

3.4.6.1 Installation of the GSM antenna on the 1068/005A – 1068/010A control panel

Insert the GSM antenna provided in the specific compartment (see figure below).



When, due to the position of the control panel, the internal antenna provided with the package should not guarantee adequate signal levels, use the remote 1067/014 GSM external antenna.

3.4.6.2 Important information about the SIM Card

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

If you want to use the IDP/IP protocol to connect to an enabled alarm reception centre, the SIM card must be enabled to surf the Internet. Conversely, in all other cases it is sufficient to use a voice-only SIM card.

The module must recognise a minimum connection of 2G type in order to operate correctly.

It is advisable to carefully choose the tariff plan proposed by the operator. This is to avoid any additional costs related to the use of the call and/or text message functions.

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

3.4.6.3 Setting up the SIM Card

Before inserting the SIM Card in the GSM module, it is recommended to check that it is activated and operates correctly with a mobile phone. It is suggested to remove the blocking PIN (alternatively configure the control panel with the correct PIN) and check/deactivate any active service.

In the case of 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.

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.

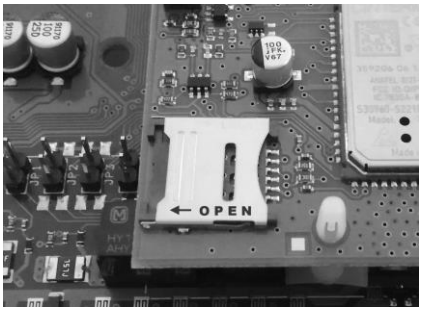
3.4.6.4 Inserting the SIM Card

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.

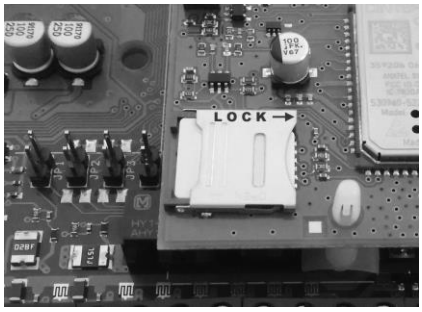
To insert the SIM Card, follow the instructions below:

1. Open the SIM housing cover by sliding it in the direction indicated by the **OPEN** arrow, and then open the door.



2. Insert the SIM card into its slot, with the gold contacts facing inwards.

3. Close the cover and lock it by sliding it in the direction indicated by the **LOCK** arrow.

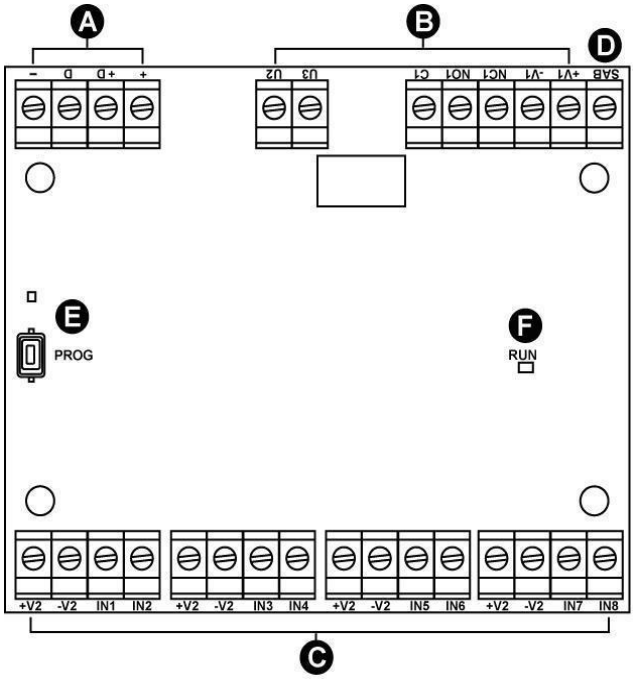


3.5 INSTALLATION OF THE 1067/008A EXPANSION

The 1067/008A expansion should be installed inside a 1067/017 housing box (Grade 3 compliant).

The tamper of the housing box must be connected to the SAB of the expansion. The expansion has terminals for connecting the power supply, detectors, ad signalling devices, etc.

The electric outputs can be transformed into relay outputs – See paragraph *3.11.6.1 Relay outputs*.



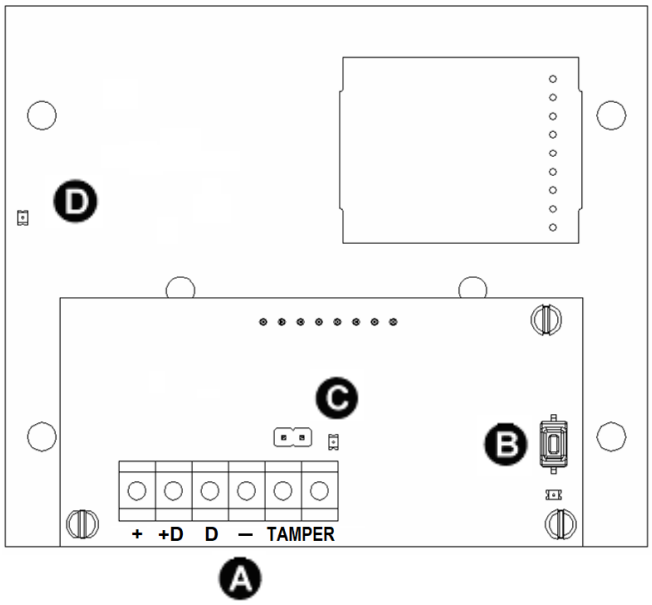
Detail	Terminal / Detail	Description
A	**+**	BUS Expansion unit power input via bus
	+D	Data transmission/reception BUS
	D	
	–	BUS Expansion unit power input via bus
B	**+**V1	Power supply for output actuators (13.2 V⎓ limited to 500 mA)
	–V1	
	NC1	Relay output 1 – contact normally closed
	NO1	Relay output 1 – contact normally open
	C1	Relay output 1 – common (max. 1 A - 24 V⎓)
	U2	Electric output 2 (current protected max. 10 mA)
	U3	Electric output 3 (current protected max. 10 mA)
C	**+**V2	Power supply of detectors connected to the expansion (13.2 V⎓ 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 2.7 kΩ balancing resistor.
E	Pushbutton Yellow LED	Device acquisition pushbutton and LED.
F	RUN	Green LED signalling operation: **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 *3.11.2 Connecting the data Bus* and paragraphs *3.11.5 Connecting inputs* and *3.11.6 Connecting outputs*.

3.6 INSTALLATION OF THE 1068/017 RADIO INTERFACE

The 1068/017 radio interface is supplied with a plastic case.

The interface has terminals for connecting it to the data BUS and the LEDs that signal the functioning of the electronic board. The tamper of the container must be connected to the SAB of the expansion.



Ref.	Terminal / Detail	Description
A	+	Interface power supply via Bus
	+D	Data transmission via bus
	D	
	—	Interface power supply via Bus
	Tamper	Connection for the box protection microswitch
B	Button	Buttons and LEDs for the interface acquisition.
	Yellow LED	**Slow blinking for 10 sec.** = possibility of deleting the device **Off after the first 10 sec.** = device acquired **Slow blinking after the first 10 sec.** = device not acquired **Fast blinking** = device in updating **Very fast blinking** = device with updating in progress
C	Green LED	Operating signalling. **Slow blinking** = normal operating conditions **Fast blinking** = no communication with control panel from at least 1 minute
	Jumper	Jumper for Tamper exclusion (Jumper inserted = Tamper excluded)
D	Green LED	Radio interface working signaling

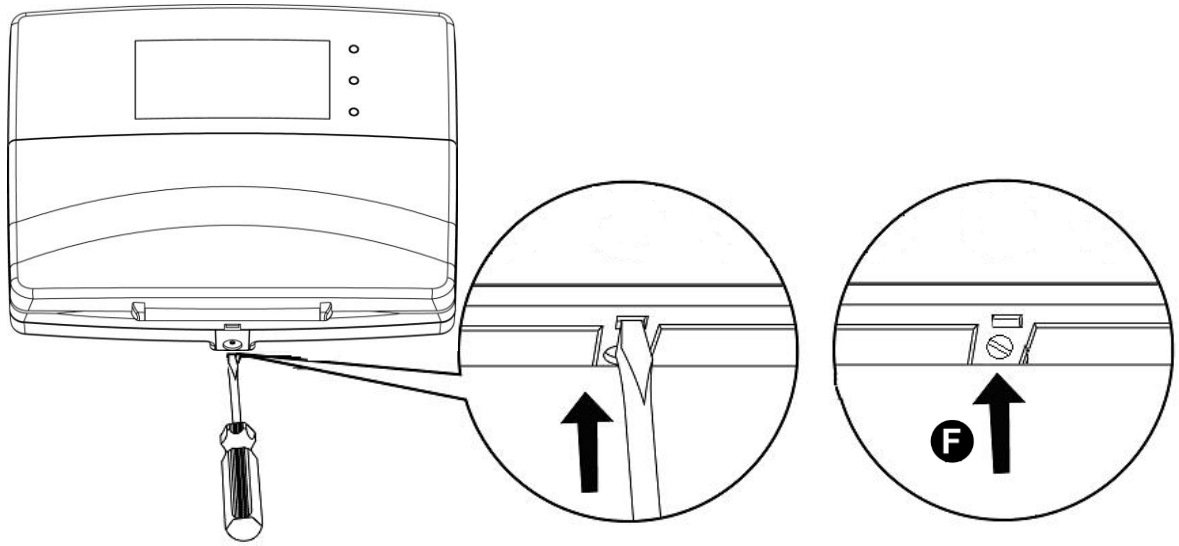
3.7 INSTALLATION OF THE 1068/021 KEYPAD

The 1068/021 keypad is equipped with a programmable auxiliary input.

The 1068/021 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. Open the keypad with a flat screwdriver by pressing gently on the point indicated in the image to release the latch and lift the cover.

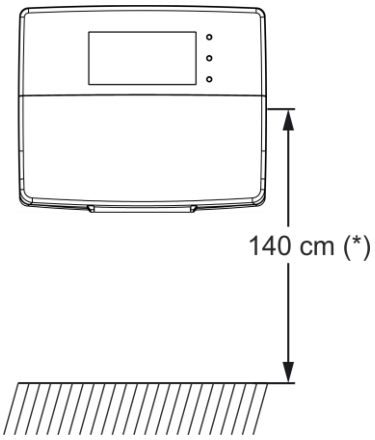


2. To route the cables, use the hole on the bottom of the keypad. Otherwise, the pre-cut holes for the cable ducts can be used.
3. Secure the keypad bottom to the wall by means of screws and plugs (not provided). Use Ø 5mm plugs depending on the type of material making up the wall with TCB screw DIN 7981 3.5 x 32.

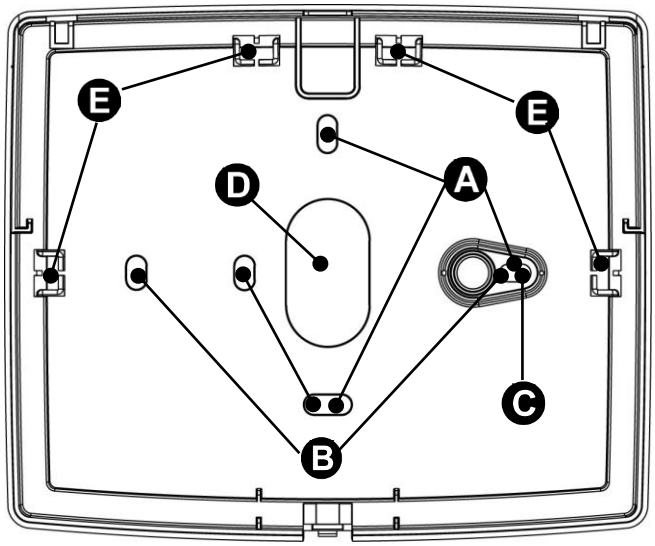
Before fixing, verify the bottom direction: cover closing hook shall be positioned at the bottom.

4. Connect any device to the auxiliary input.

For easier wiring, it is advisable to strip the cable as far as the access hole.

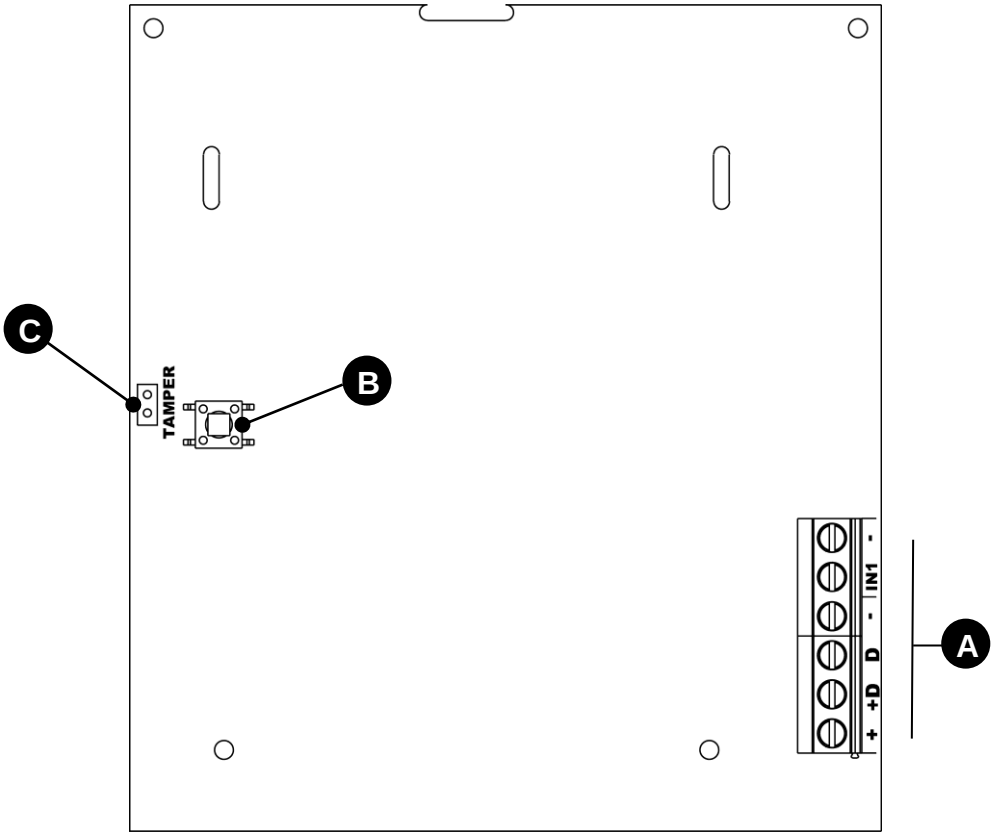


(*****) In case of disabled people or with specific needs of type D1 (elderly) and D2 (with lower limb movement difficulties), **the centre of the device** must be positioned at a height between 75 cm and 140 cm above the floor. For further details see technical Standard CEI 64-21:2016-12 - Residential environments. Systems suitable for use by persons with disabilities or specific needs.



A	Holes for fastening the Ø 60 mm box
B	Holes for fastening to 3-place box
C	Fixing hole for anti-removal protection
D	Holes for cable routing
E	Pre-cut holes for trunkings

Refer to the following image for the keypad board:



Detail	Terminal / Detail	Description
A	+	BUS for keypad power input via Bus
	+D	Data transmission/reception BUS
	D	
	–	BUS for keypad power input via Bus
	IN1	Auxiliary input 1
	–	Auxiliary input 1 negative reference
B	Tamper	Tamper anti-tamper
C	JP2	Keypad tamper exclusion jumper (Jumper inserted = tamper excluded)

5. Close the keypad by screwing the supplied screw into the hole (Point 1) - **F**).

For details on connections (power supplies, inputs, bus, etc.) see paragraphs *3.11.2 Connecting the data Bus* and *3.11.5 Connecting inputs.*

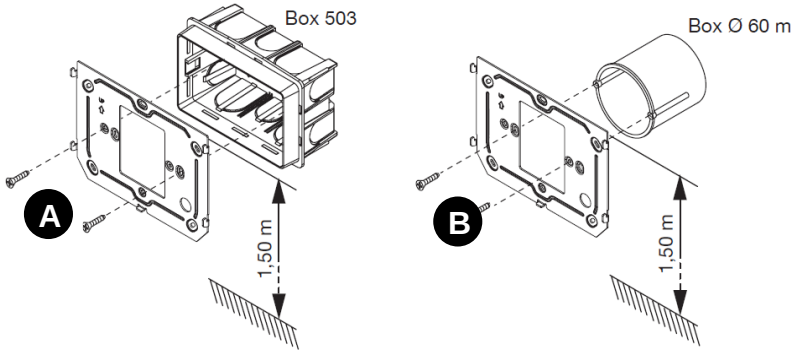
3.8 INSTALLATION OF THE 1068/027 KEYPAD

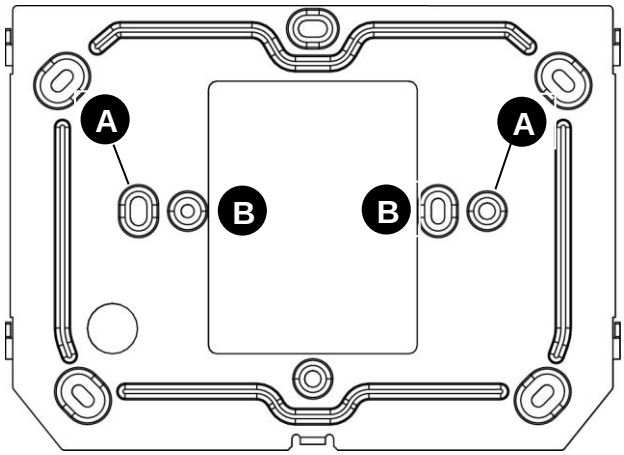
The 1068/027 keypad can be installed on the wall or above a built-in rectangular box with 3 spaces or a 60-mm round box.

To install the keypad, follow the instructions below:

- Embed the flush-mounting box Mod. 503 in the wall or the flush-mounting box Ø 60 at the height shown in the following drawing.

Note*: The flush-mounting box Mod. 503 can be installed either horizontally or vertically.*



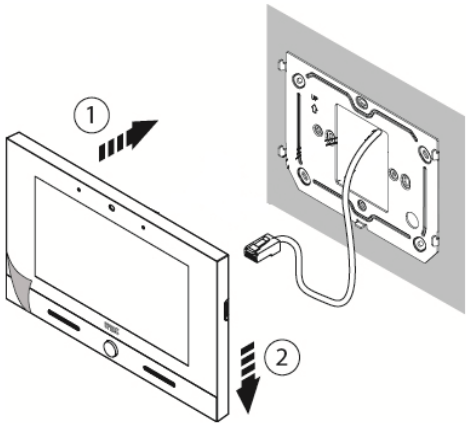


Bracket fixing holes

A	Holes for fixing the bracket on a 3-place box.
B	Holes for fixing the bracket on flush-mounted box ø 60 mm.

(*) *In case of disabled people or with specific needs of type D1 (elderly) and D2 (with lower limb movement difficulties),* ***the centre of the device*** *must be positioned at a height between 75 cm and 140 cm above the floor. For further details see technical Standard CEI 64-21:2016-12 - Residential environments. Systems suitable for use by persons with disabilities or specific needs.*

- Fix the wall bracket with the appropriate screws supplied.
- Connect the keypad via the network cable to the POE connector.
- Move the keypad close to the bracket by centring the special fixings ① and slide it down to reach its stop ②.



- Use a screwdriver to move the latch for locking the keypad to the bracket from right to left.
- Remove the protective film from the display.

3.9 INSTALLATION OF THE 1068/435 READER

The proximity and key readers are installed in boxes to be built-in or wall-mounted and positioned in a dry area.

The reader is suitable for installation on Bticino Magic frames and, using the Bticino adapter with Code A5374/1, on Bticino TT MATIX frames. The adapter frame supplied allows the installation of the reader on the Simon Urmet nea frames.

By using the adapter frames (not provided), the reader can be inserted as a switch within the various civil lines on the market.

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

	IMPORTANT! The absence of the tamper entails the loss of compliance with EN50131.

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

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 allows access 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 sections to the tamper). The input is programmed to TAMPER by default.
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.

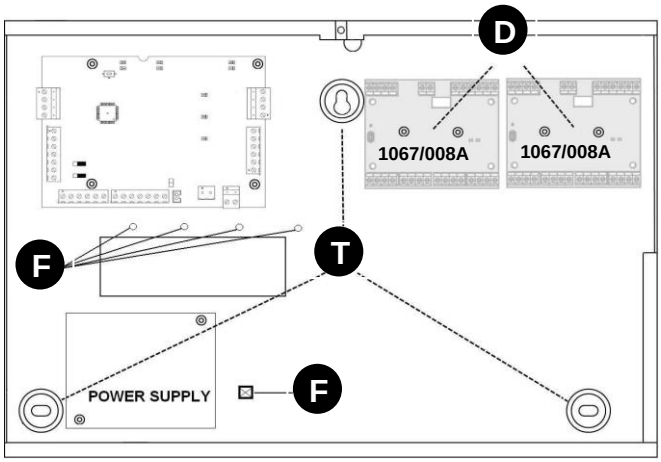
For details on connections (power supplies, inputs, bus, etc.) see paragraphs *3.11.2 Connecting the data Bus* and *3.11.5 Connecting inputs.*

3.10 INSTALLATION OF THE 1067/092 SUPPLEMENTARY POWER SUPPLY (AVAILABLE ONLY WITH 1068/010A CONTROL PANEL)

EN50131

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

3.10.1 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.

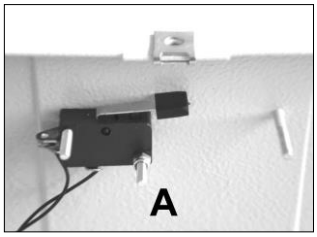
D Holes for fastening 2 optional 1067/008A expansions.

F Band to fasten power supply cables.

Figure 8 - Holes for fastening the 1067/092

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.

3.10.2 Connecting the power supply and battery

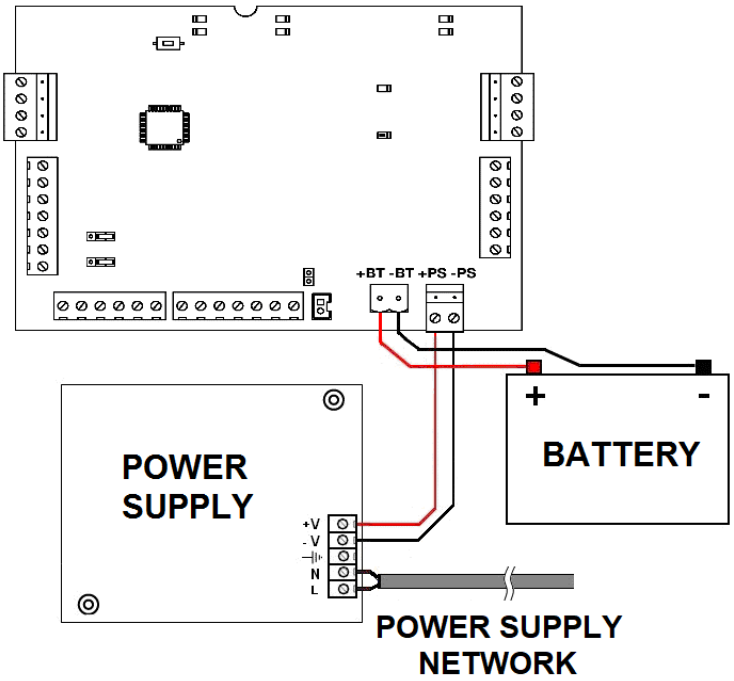


Figure 9 - Connecting the power supply and battery

3.10.3 The 1067/092 board

The 1067/092 electronic board has two distinct sections: BUS IN and BUS OUT, galvanically isolated to guarantee better immunity to RF disturbances.
In the BUS IN section there is an 1067/008A integrated expansion (**E**).
In the BUS OUT section there is an integrated repeater function (**R**) and power supply (**P**).

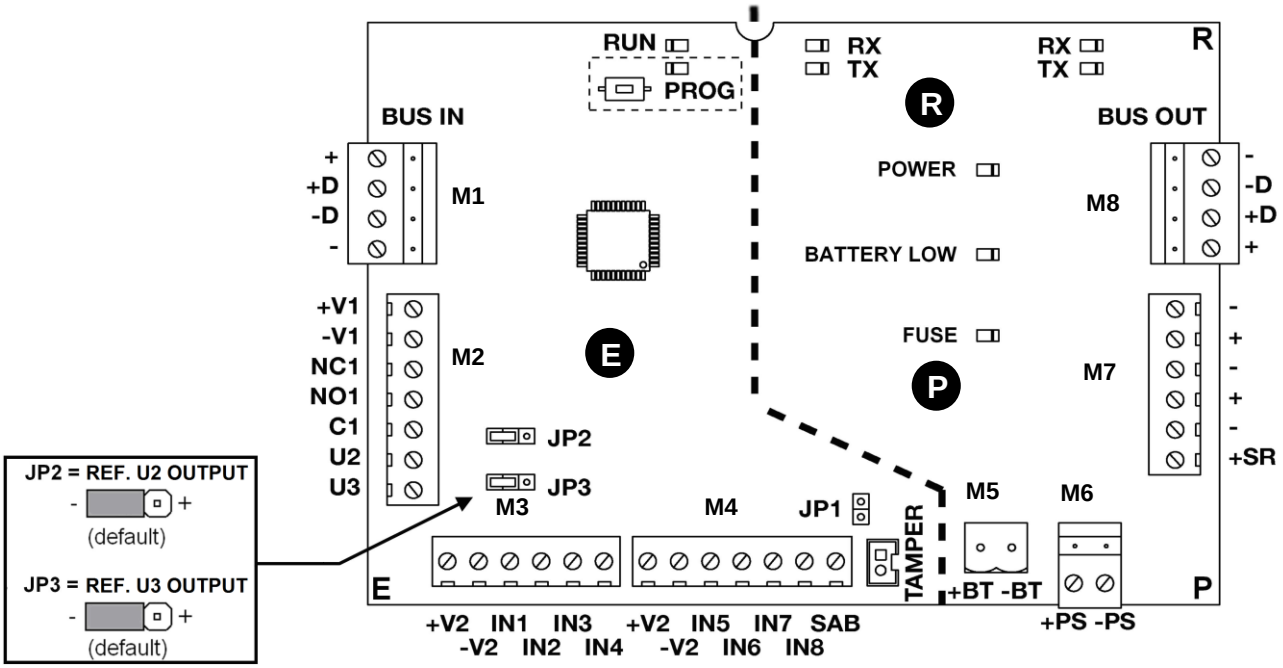


Figure 10 - 1067/092 Board

3.10.3.1 The Expansion

By referring to the *Figure 10 - 1067/092 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⎓)
		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
		SAB	24h input (for system self-protection), must always be BALANCED and closed with a 2.7 kΩ balancing resistor.

Terminal board	Group	Description	Connection / Function
	TAMPER	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 “Negative Reference”.

The electric outputs can be transformed into relay outputs – See paragraph *3.11.6.1 Relay outputs*.

For details on connections (power supplies, inputs, outputs, bus, etc. …) see paragraph *3.11.2 Connecting the data Bus* and paragraphs *3.11.5 Connecting inputs* and *3.11.6 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 1068/010A control panel receive information on the functioning of the supplementary power supply from the expansion: black out, battery low, and power supply breakdown.

3.10.3.2 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 10 - 1067/092 board*, the functions of the terminals and LEDs dedicated to the Repeater are the following:

Terminal board	Group	Terminal	Connection/Function
M8	BUS OUT	+	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 1068/010A 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).

3.10.3.3 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 10 - 1067/092 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⎓ 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 Urmet 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

3.11 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 to the maximum distances.

For more details, see chapter *2 DESIGN: calculations and tests*.

IMPORTANT!

It is not allowed to solder the ends of the cables connected to the terminals of the equipment because the end of the stranded conductor must not be consolidated with a soft-solder welding in the points where the conductor is subject to contact pressure.

3.11.1 Mains power supply line

IMPORTANT!

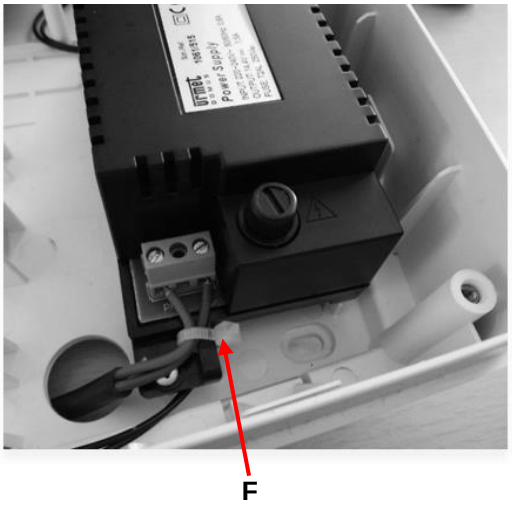
Before making any connections to the mains power supply, disconnect the mains power supply.

In fulfilment of the electrical safety standards for mains power supply, a suitable isolating device must be installed, like a double-pole thermo-magnetic circuit breaker to protect the mains power supply.

The contacts of the two-pole thermo-magnetic circuit breaker must be at a distance of at least 3mm from each other.

For the mains power supply, use a 2 x 1.5 mm^2 cable.

The control panel has double isolation and does not need earth connection (PE). The earth connection is required only for the connection to the telephone line.



1068/005A Control panel

(**F**) Point where power cables are fastened with the tie.

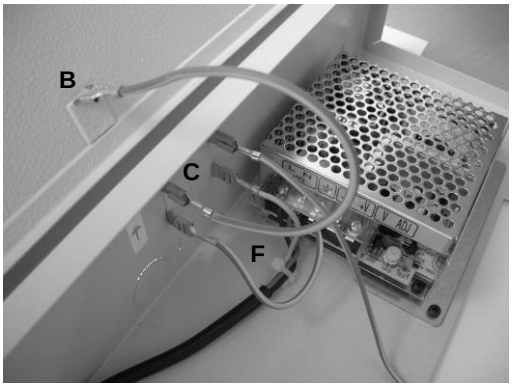
1. Connect the mains power supply cables to the 2 terminals of the control panel power supply.
2. Secure the wires by fastening them in anchoring point (**F**) with the tie provided

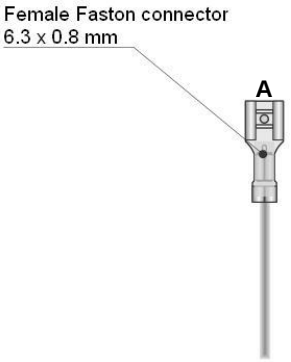
The 1067/092 power supply (optional and only available with the 1068/010A control panel), requires an earth connection (PE). For this connection, there is a Faston connector provided with the control panel.

1. Connect the mains power supply cables to the 2 terminals of the control panel power supply.
2. 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.

Wires with cross-section area of 0.5 mm^2 or larger must comply with IEC 60332-1-2; wires with crosssection area smaller than 0.5 mm^2 must comply with IEC 60332-2-2.

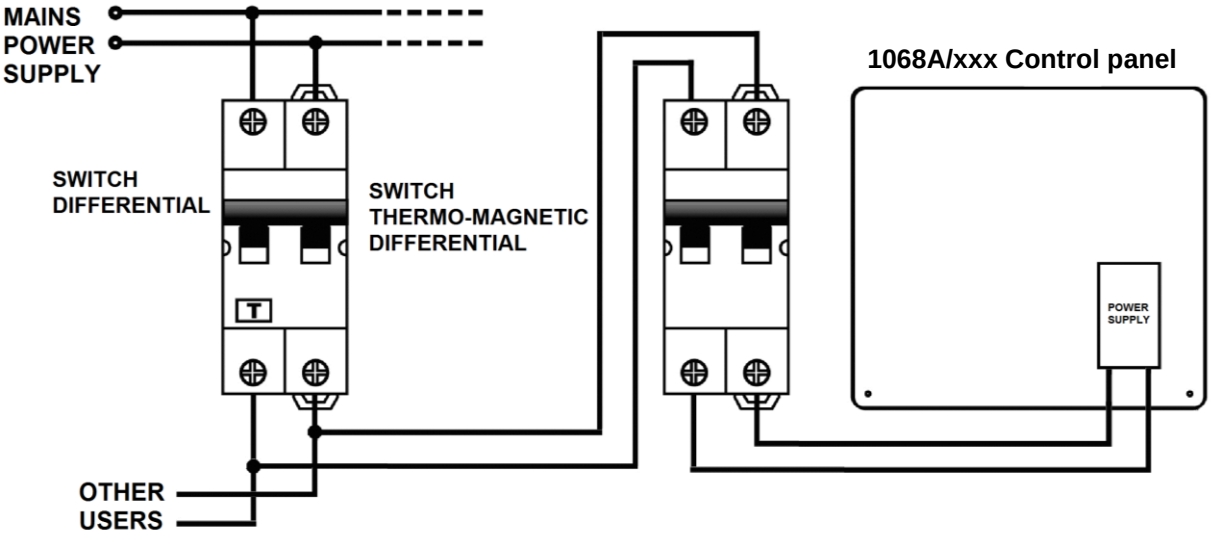
IMPORTANT! After having connected the wires, remember to insert the plastic protection on the terminals.





1067/092 supplementary power supply

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

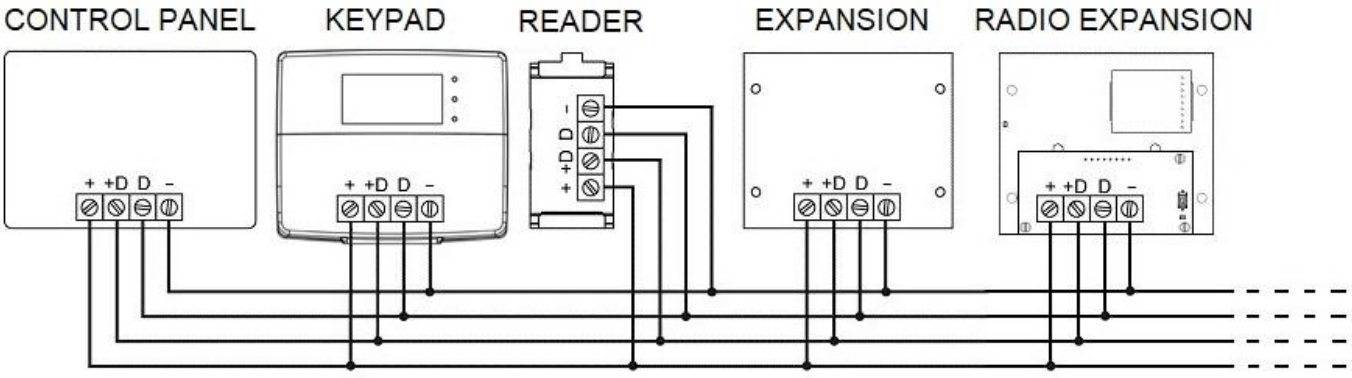


⚠	**IMPORTANT!** The system must be powered by the mains only after all devices are installed correctly, making it possible to proceed with their acquisition. For safety purposes, close the control panel casing before powering it up.

3.11.2 Connecting the data Bus

Connect the terminals **+, +D**, **D** and ─ to the 4-wire cable 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 unit.



3.11.3 Connecting IP POE interface

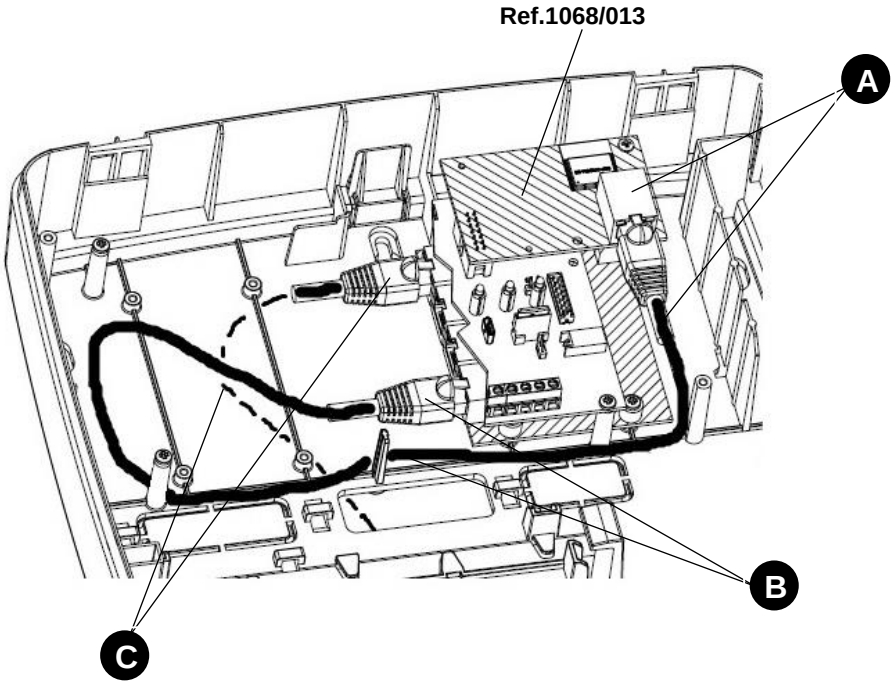
The board can be connected to the "**+**" and "**–**" terminals of the bus line both of the 1068A series control units or of an supplementary power supply Ref. 1067/092.

The connection with the IP interface Ref. 1068/013 inside the control panels must take place exclusively via the cable supplied (Length = 50cm), **which must be positioned as shown in the Figure below (A - B).**

The PoE devices (e.g. Ref.1068/027), must be connected using the ETH1-POE port as in **Figure below (C)**.

The maximum distance depends on the cross-section area of the wire and the power consumption of the board.

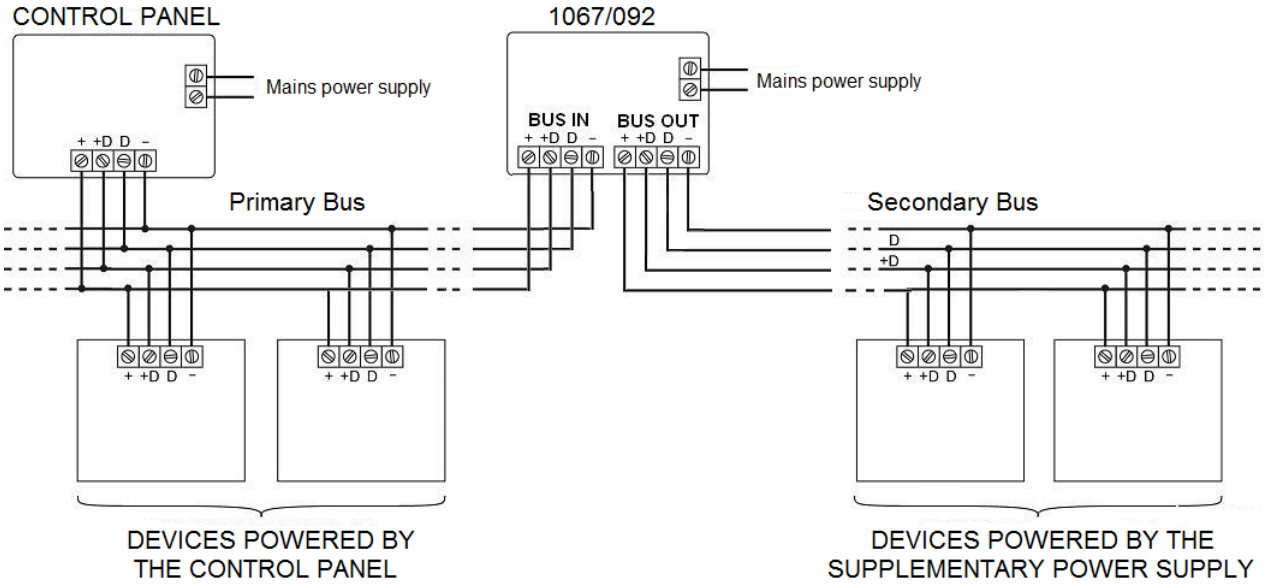
When calculating the overall system consumption, take the maximum consumption of the board and of the PoE device connected to it into account.



A	ETH	Interface Ref. 1068/013
B	ETH4	Cable for connection between Ref. 1068/002 and Ref. 1068/013
C	ETH1-POE	Cable for keypad monitor connection Ref. 1068/027

3.11.4 Connecting the supplementary power supplies/repeater

To understand which the length limits of the bus and how to calculate them, read paragraph *2.2.4 Extending the bus with the repeater*.



3.11.4.1 Connection of the detectors to the expansion module of the 1067/092

For the connection of the inputs of the various typologies (NC – NO – to single/double balancing) see paragraph *3.11.5 Connecting inputs.*

⚠	**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 detector 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, a 1067/008A expansion module connected to the BUS OUT can be used.

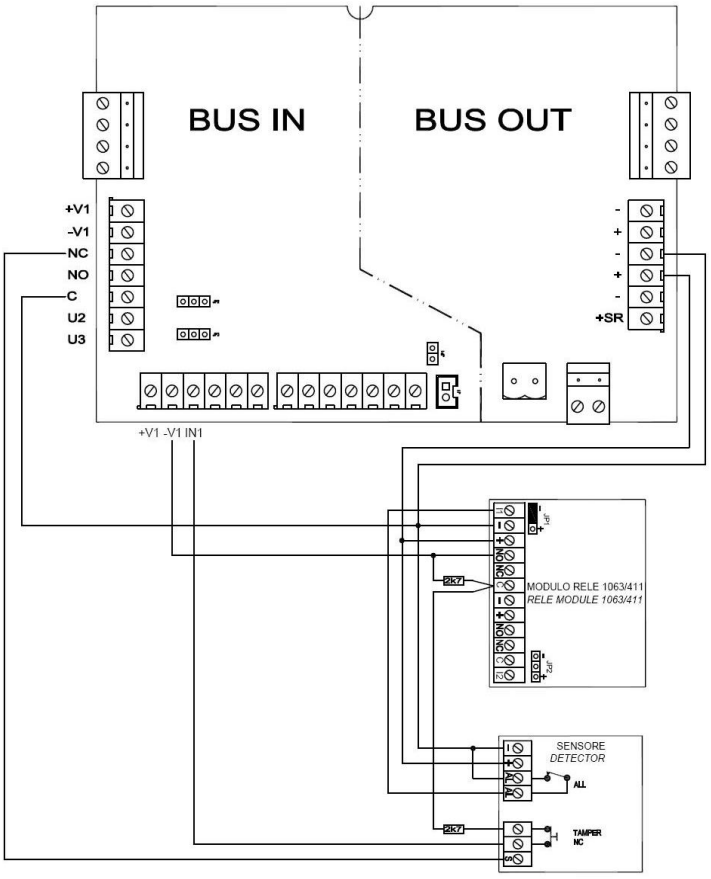


Figure 11 - Diagram of how to connect a locally powered detector

3.11.5 Connecting inputs

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

The type of inputs is specified during programming and it is possible to create a system with 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 2.7 kohm resistors, tolerance 1% (see **Fig. A**). Connection in conformity with EN50131.
- **NC** (normally closed): when in stand-by the electrical circuit connected to the input must be closed towards the negative (see **Fig. B**). Connection not compliant with EN50131.
- **Single balanced**: when in stand-by, the electrical circuit connected to the input must be closed toward the negative with a 2.7 kohm resistor, tolerance 1% (see **Fig. C**).
- **NO** (normally open): when in stand-by, the electrical circuit connected to the input must be open (it closes towards negative when in a state of alarm - see **Fig. D**).
- **Roller / Inertial**: this type of input is used to connect the sensors that generate quick signals (inertial, rollers, seismic - see **Fig. B**). In this case connection method is necessarily type NC.
- **SAB input connection:** this connection is of the single balanced type and must always be closed.
- **Double input (it can only be used with the inputs on the 1068/010A control panel):** this type of input is used to connect two detectors on the same input. The two resistors must have different values: one 2.7 kohm, the other 4.7 kohm, both with a 1% tolerance (see **Fig. E**).

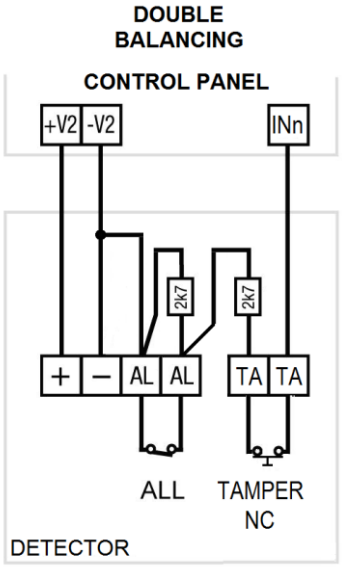


Figure A

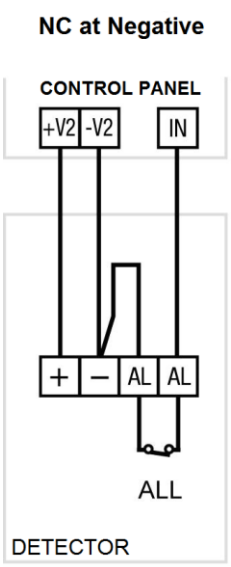


Figure B

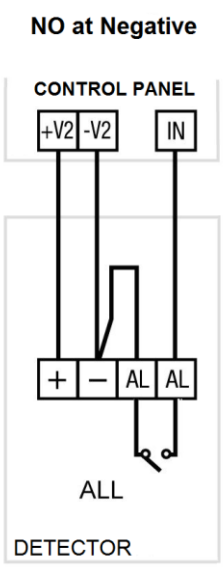


Figure C

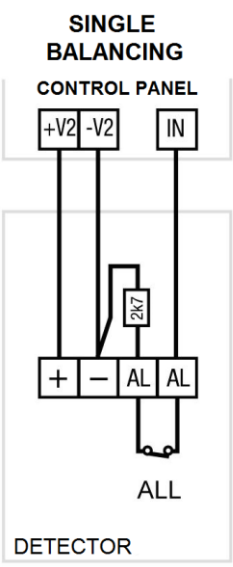


Figure D

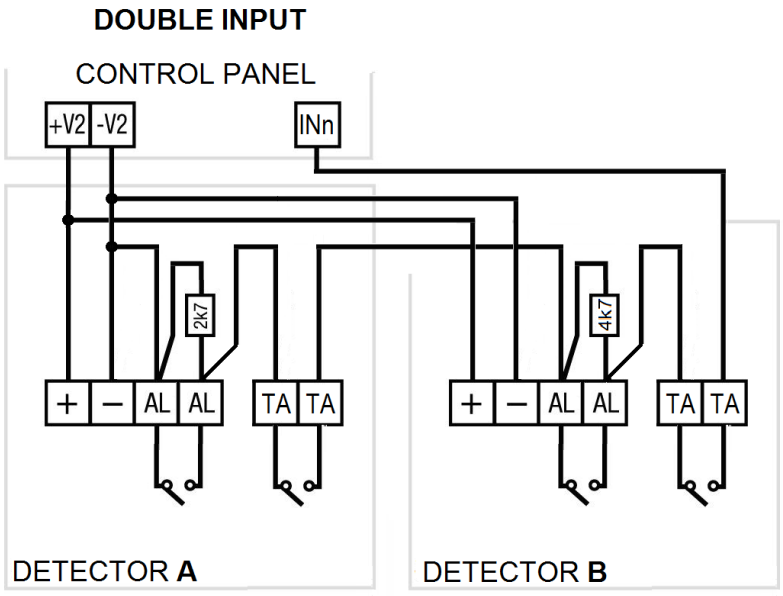


Figure **E**

Figure 12 - Input wiring diagrams

IMPORTANT!

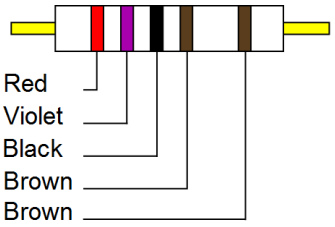
Each sensor must be powered by the device that controls it (control panel, expansion, keypad, or reader). The balancing resistors must be connected to the negative of the power supply of the same device. Connections with different power supplies may cause false alarms.

IMPORTANT!

- In order to maintain conformity with standard EN50131-3, the CUSTOMISATION functions of the INPUTS present in the control panel must not be modified.
- 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.
- In order to maintain conformity with Standard EN50131, the inputs must not be programmed as INERTIAL and ROLLER in that they would not be protected against short circuits.
- 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 negative of the power supply of the same device. Connections with different power supplies may cause false alarms.

  If due to wiring problems this is not possible use the NC or NO type inputs.

Colour code for resistor 2.7 kohm, tolerance 1%



Colour code for resistor 4.7 kohm, tolerance 1%

All the resistors provided with the 1068A system are 2.7 kohm, tolerance 1%.

The 4.7 kohm resistors - 1% tolerance, are supplied only with the 1068/010A control panel.

IMPORTANT! Do not close the unused inputs because they can be excluded via the programming.

IMPORTANT! The SAB inputs must also be reclosed by a 2.7 kohm balancing resistor.

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

Input status				Voltage at the terminal (*)	Resistor between the input and –V2 (GND)
Double BAL.	**Single BAL.**	**NC**	**N.O.**		
TAMPER (Wire cutting)	ALARM	ALARM	STAND-BY	7,2 ÷ 9,1 V	∞
ALARM	—	—	—	3,7 ÷ 4,7 V	5,4 kohm
STAND-BY	STAND-BY	—	—	2,5 ÷ 3,1 V	2,7 kohm
TAMPER (Wire short circuit)	TAMPER (Wire short circuit)	STAND-BY	ALARM	< 0,5V	0 ohm

(*) With +V2 voltage between 12 V and 14.2 V.

3.11.6 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 customisation (intrusion, tampering, 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 CUSTOMISATION functions of the OUTPUTS present in the control panel must not be modified.

IMPORTANT!
In order to ensure conformity with the standard EN50131-3, the TAMPER output (OUTPUT No.2) must NOT control outdoor sirens. For indoor sirens use the dedicated output in the control panel (U3). When the system is deactivated and in case of tampering signals the outdoor siren cannot be activated.

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

3.11.6.1 Relay outputs

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

3.11.6.2 Electric outputs

The electric outputs are:

- with "positive reference" U3, dedicated to the internal siren
- with "negative reference" U4, dedicated to the system status (default)

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

The U4 electric output can be used to control power relays or signalling LEDs.

The expansion has only 2 electrical outputs available, both only “negative reference”: U2 and U3.

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

The stand-by status of each output is programmable as either N.H. or N.L.

The tables below illustrate how the various outputs appear when in stand-by and when they are ON.

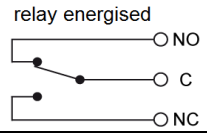
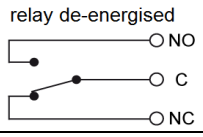
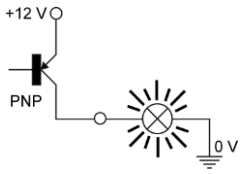
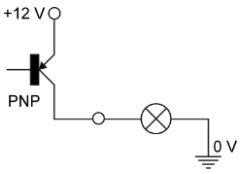
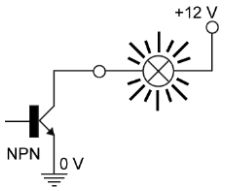
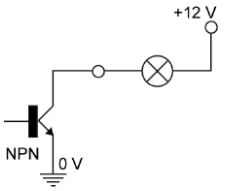
N.H. programmed output (positive safety)		
	Stand-by	**ON**
RELAY OUTPUT		
ELECTRICAL OUTPUT POSITIVE reference		
(*) ELECTRICAL OUTPUT NEGATIVE reference		

Table 7 - N.H. programmed output synoptic

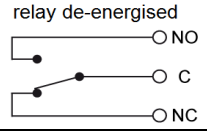
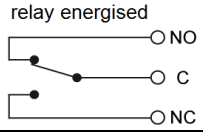
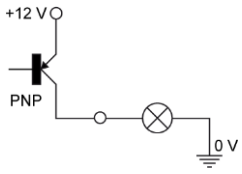
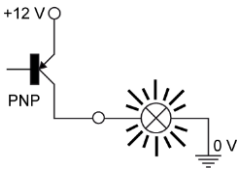
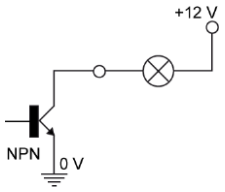
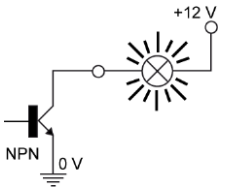
N.L. programmed output		
	Stand-by	**ON**
RELAY OUTPUT		
(**) ELECTRICAL OUTPUT POSITIVE reference		
ELECTRICAL OUTPUT NEGATIVE reference		

Table 8 - N.L. programmed output synoptic

(*) The U4 output is programmed by default as NH with negative reference.

(**) The U3 output is programmed by default as NL with positive reference.

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

3.11.7 Connecting the cable for the service keypad

The service keypad can be connected to the control panel.

The purpose is to be able to program the control panel more easily, without having to use one of the keypads already installed elsewhere.

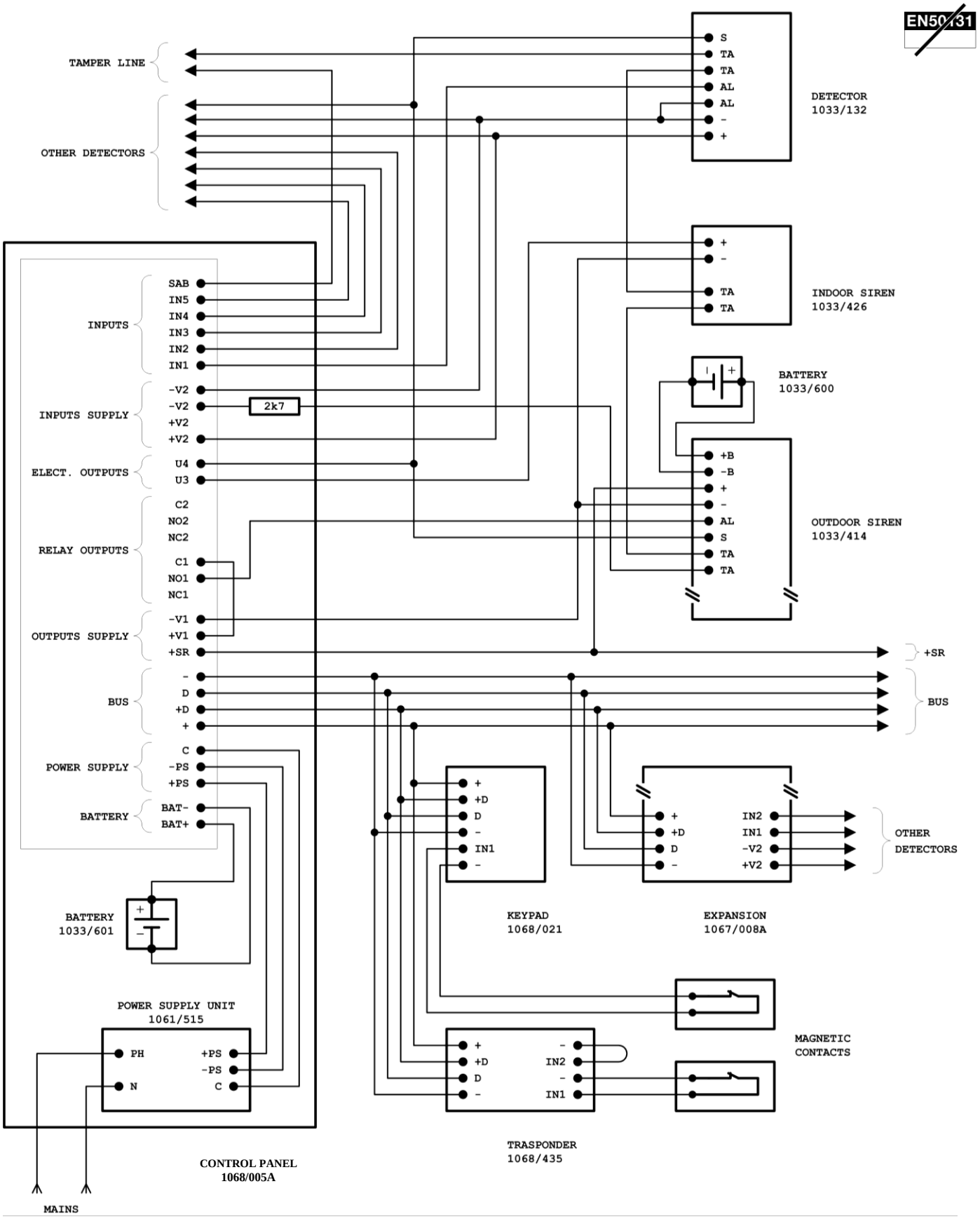
The service keypad can be used only for this purpose.

3.11.8 Connecting the telephone communicator

In order to conform to standard EN50131 Grade 2, it is necessary to use a communicator ATS2 type.

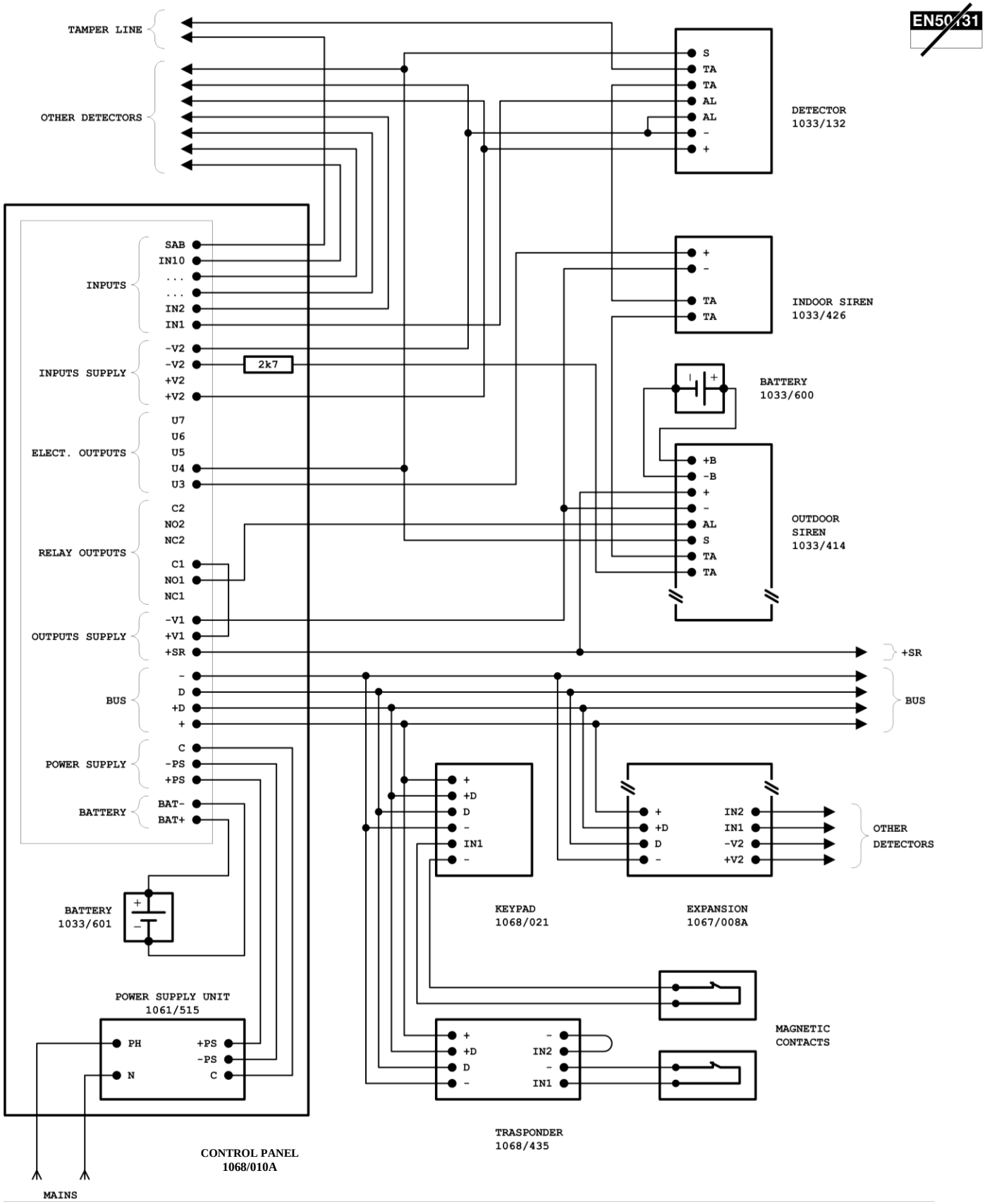
The GSM/GPRS 1068/458 module is an ATS2.

3.12 EXAMPLE OF CONNECTION DIAGRAM OF 1068/005A CONTROL PANEL WITH N.C. INPUTS



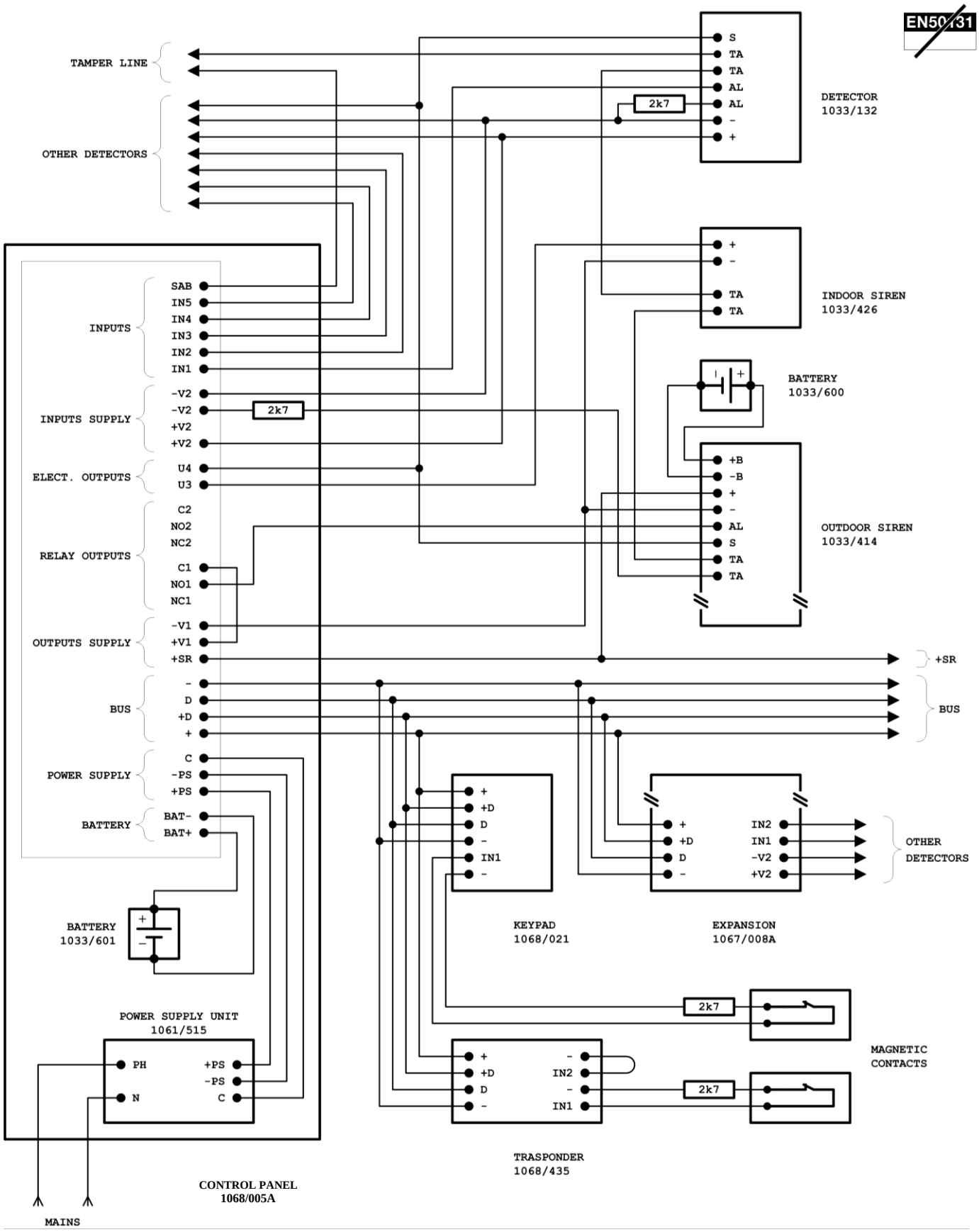
IMPORTANT! Each detector must be powered by the device that controls it.

3.13 EXAMPLE OF CONNECTION DIAGRAM OF 1068/010A CONTROL PANEL WITH N.C. INPUTS



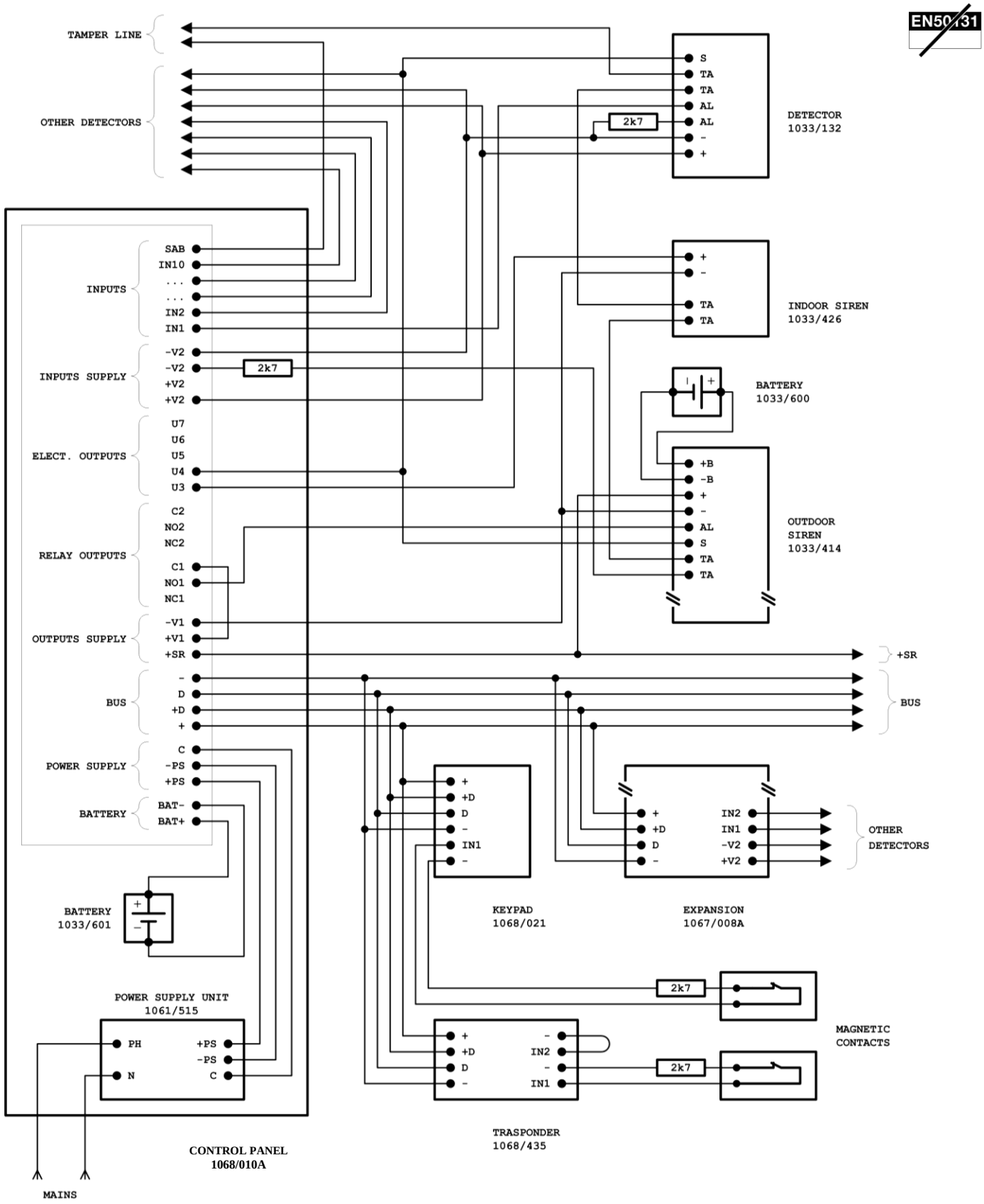
IMPORTANT! Each detector must be powered by the device that controls it.

3.14 EXAMPLE OF CONNECTION DIAGRAM OF 1068/005A CONTROL PANEL WITH SINGLE BAL. INPUTS



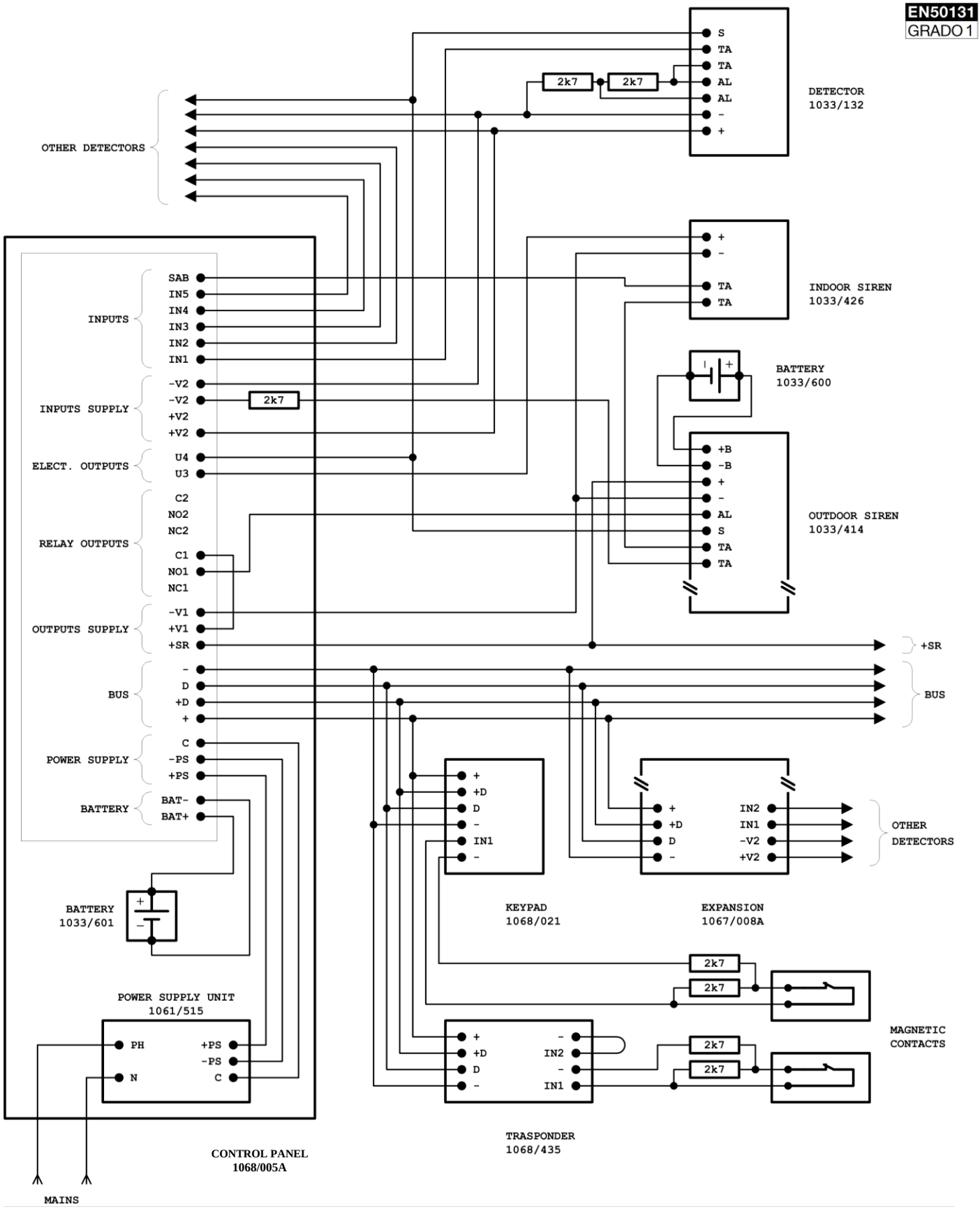
IMPORTANT! Each detector must be powered by the device that controls it. The balancing resistors must be connected to the negative of the power supply of the same device.

3.15 EXAMPLE OF CONNECTION DIAGRAM OF 1068/010A CONTROL PANEL WITH SINGLE BAL. INPUTS



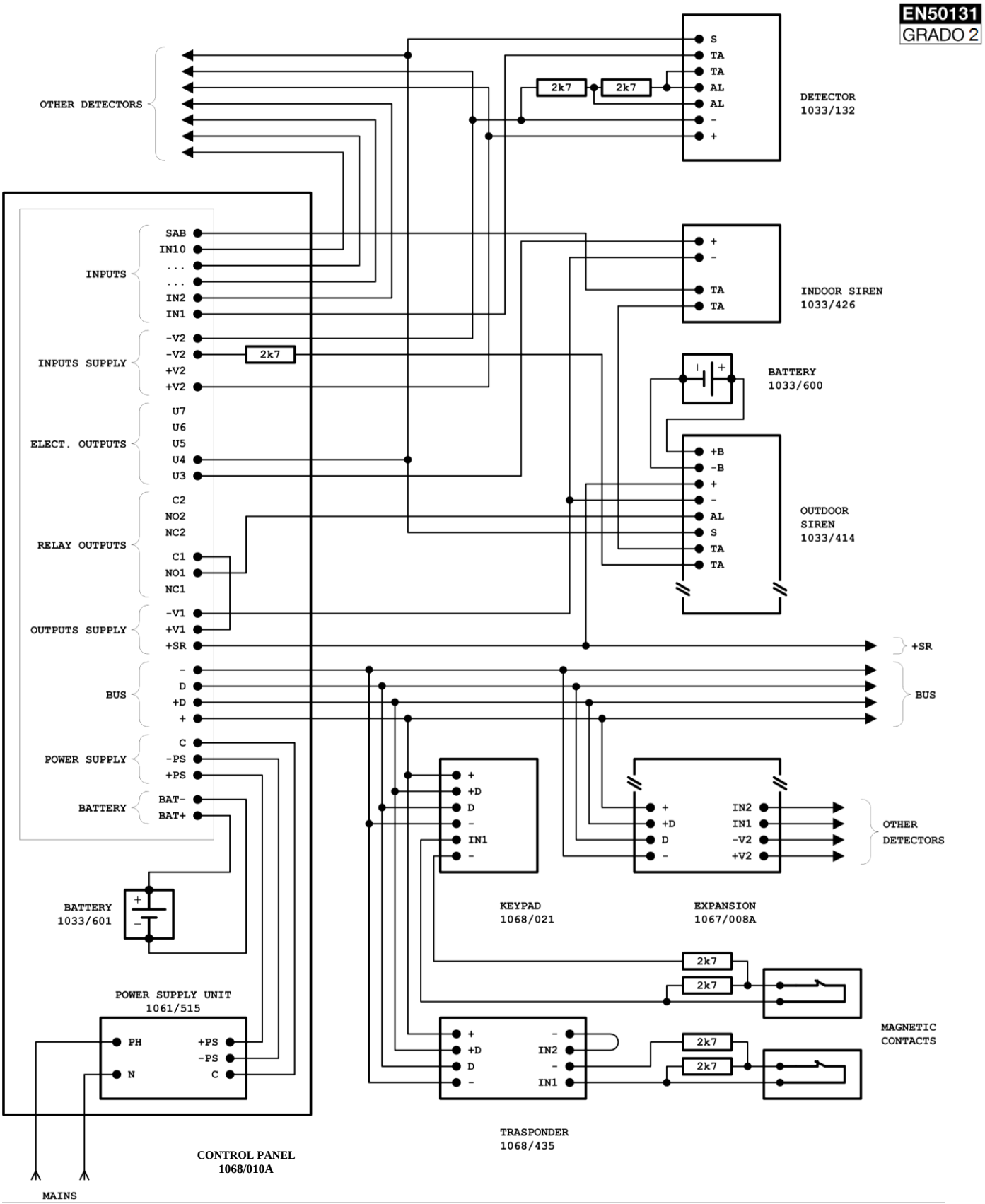
IMPORTANT! Each detector must be powered by the device that controls it. The balancing resistors must be connected to the negative of the power supply of the same device.

3.16 EXAMPLE OF CONNECTION DIAGRAM OF 1068/005A CONTROL PANEL WITH DOUBLE BAL. INPUTS



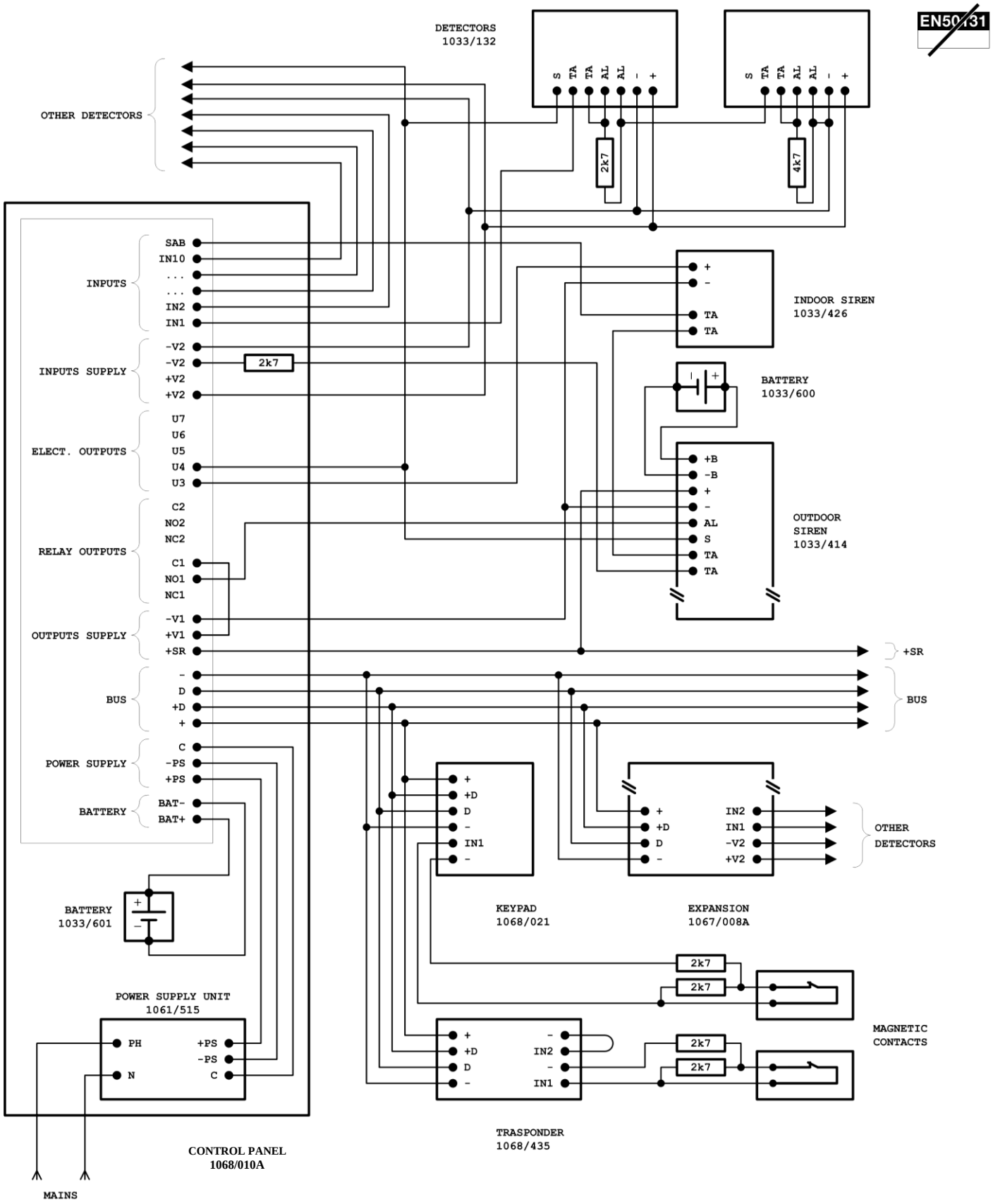
IMPORTANT! Each detector must be powered by the device that controls it. The balancing resistors must be connected to the negative of the power supply of the same device.

3.17 EXAMPLE OF CONNECTION DIAGRAM OF 1068/010A CONTROL PANEL WITH DOUBLE BAL. INPUTS



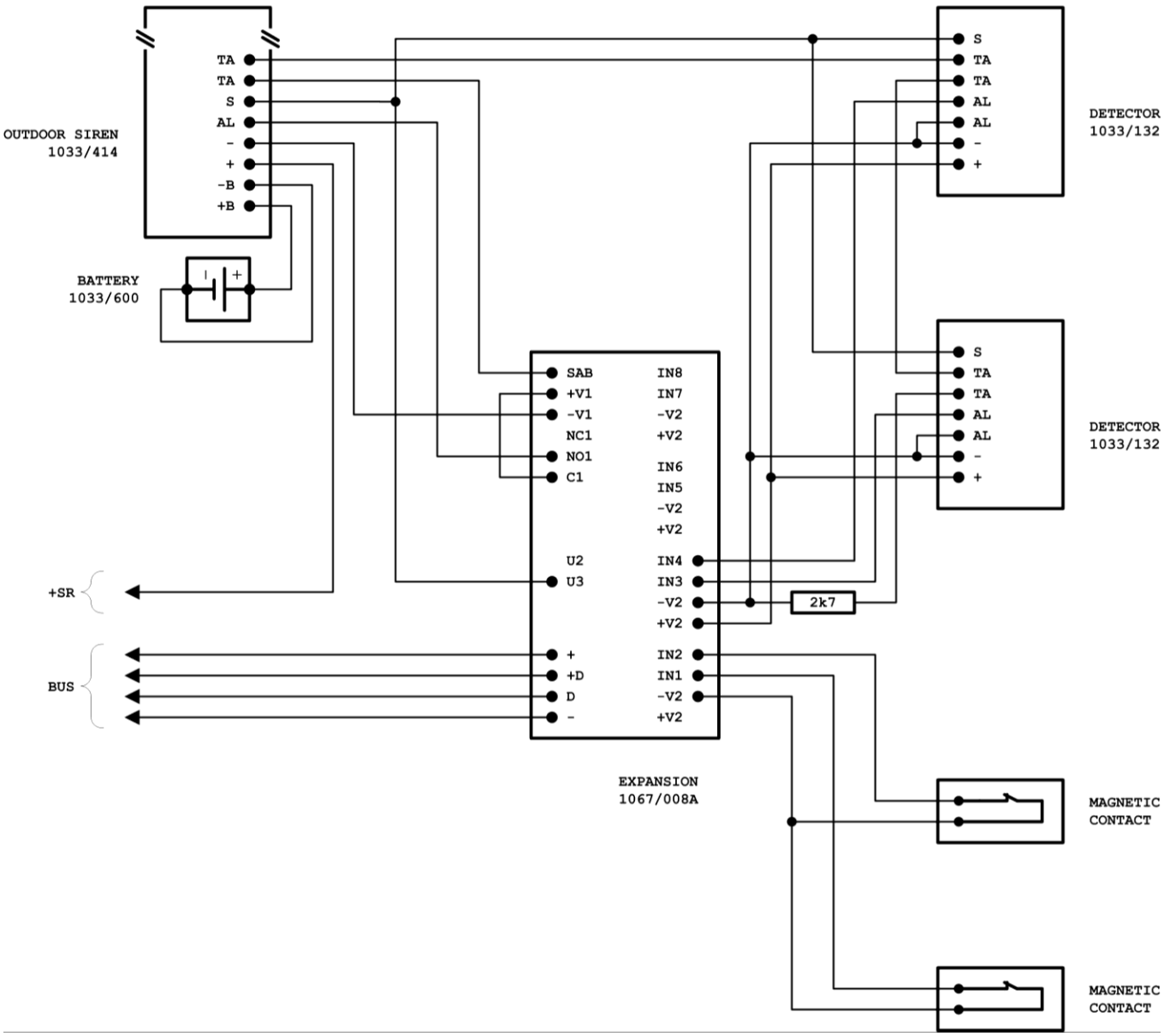
IMPORTANT! Each detector must be powered by the device that controls it. The balancing resistors must be connected to the negative of the power supply of the same device.

3.18 EXAMPLE OF CONNECTION DIAGRAM OF 1068/010A CONTROL PANEL WITH DOUBLE INPUTS



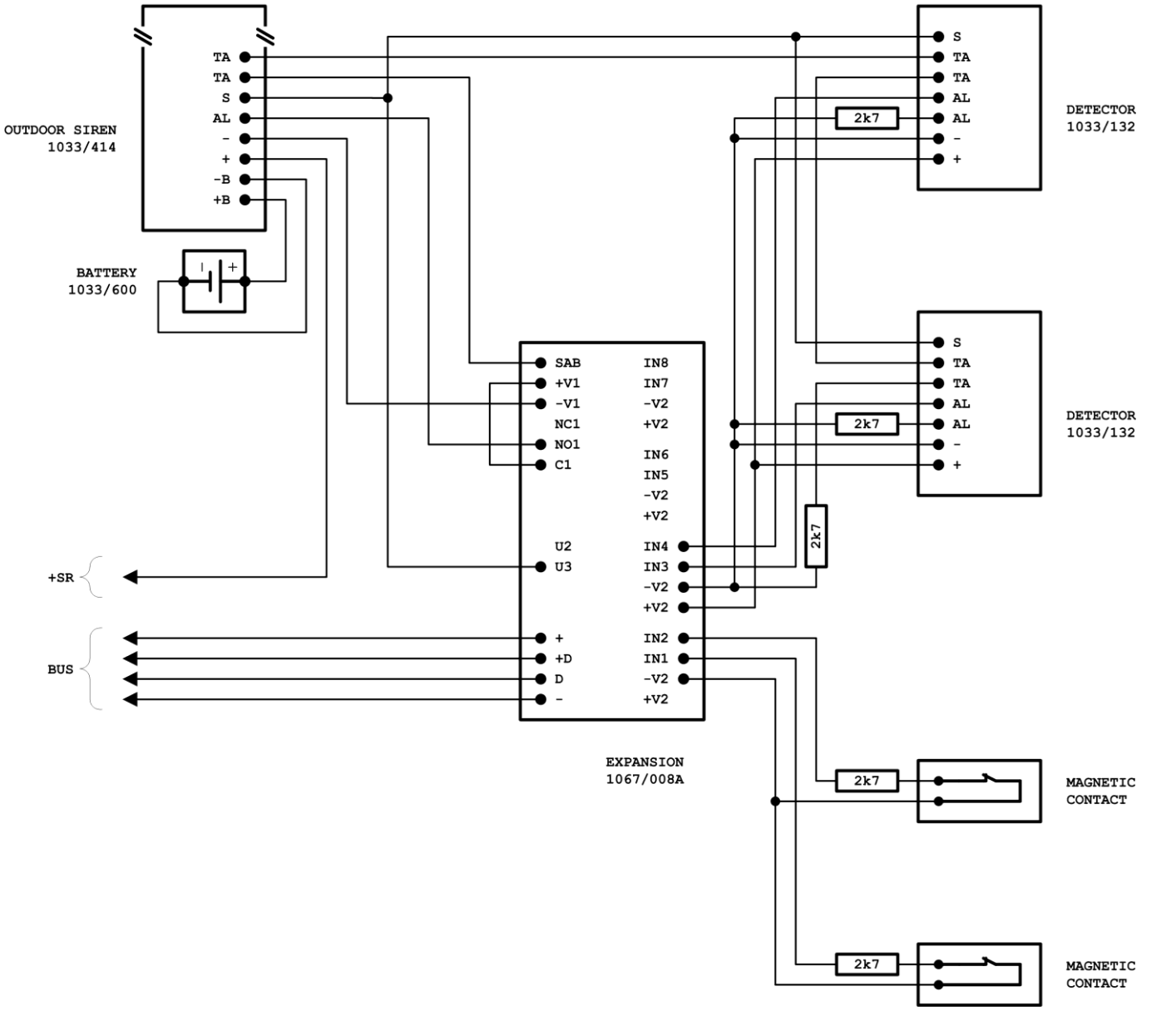
IMPORTANT! Each detector must be powered by the device that controls it. The balancing resistors must be connected to the negative of the power supply of the same device.

3.19 EXAMPLE OF CONNECTION DIAGRAM OF 1067/008A EXPANSION WITH NC INPUTS



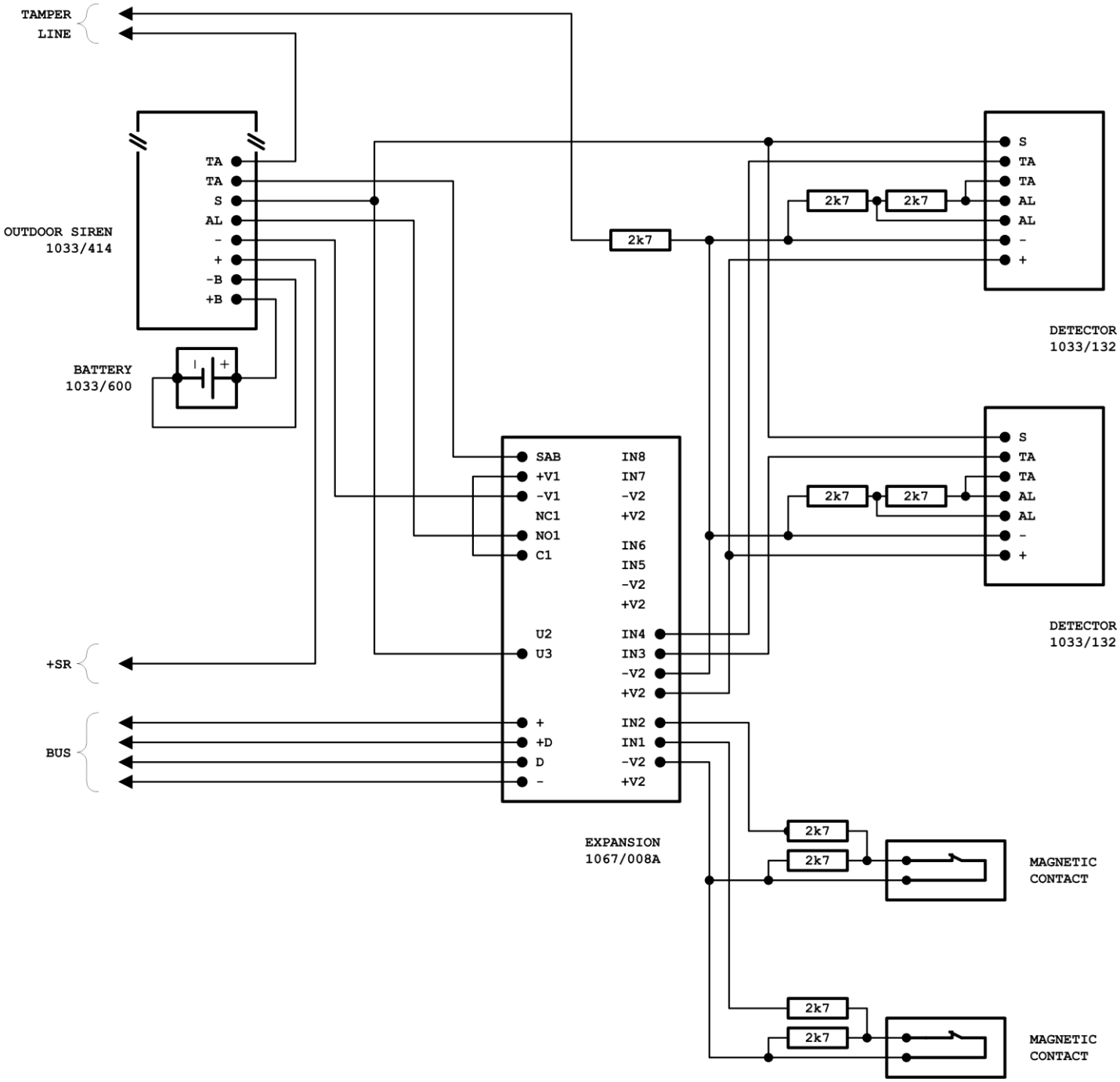
IMPORTANT! Each detector must be powered by the device that controls it.

3.20 EXAMPLE OF CONNECTION DIAGRAM OF 1067/008A EXPANSION WITH SINGLE BAL. INPUTS



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

3.21 EXAMPLE OF CONNECTION DIAGRAM OF 1067/008A EXPANSION WITH DOUBLE BAL. INPUTS



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

4 COMMISSIONING

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

Once the operations described in this chapter have been concluded, the system can then be programmed.

4.1 SYSTEM POWER SUPPLY

Before powering up the system, it is necessary to check that the connections are all correct.

Insert the battery in the dedicated compartment 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 unit does not need calibration.

At each start, the DL2, DL3, DL4 and RUN LEDs of the control panel will signal for about 20s;

- 1 Short blink every 2s

During this time, the control panel is not operational.

After the 20s, the LEDs will signal:

- DL4 steady On, if power supply is present
- RUN blinking quickly if the control panel is under maintenance
- RUN blinking slowly if the control panel is not under maintenance

Under these conditions, the control panel is operational.

In case of open inputs or tampering, the DL3 LED will:

- Blink slowly when inputs are open
- Be steady On in case of tampering

At the first start-up or after loading the factory parameters, once the control panel is operational, it is also in maintenance and ready to acquire fieldbus devices.

To avoid the control panel to be in this situation each time it is started up, acquire at least one fieldbus device or activate the system at least once.

Check that voltages arriving to the devices in the various points of the system are conforming to the indications described in paragraph *2.2.2 Sizing of the power supply cable*.

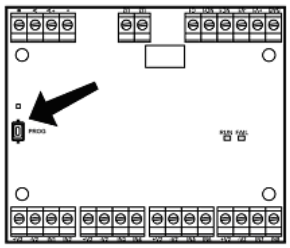
	**IMPORTANT!** To turn off the system completely, follow the procedure indicated in paragraph *9.14 Turning off the entire system*.

4.2 ACQUISITIONS OF BUS DEVICES

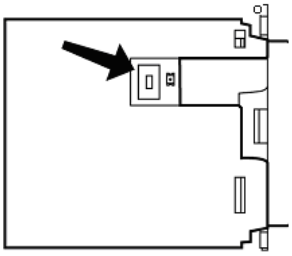
4.2.1 Position of the programming buttons

For the acquisition of the bus devices, use their programming buttons (PROG).

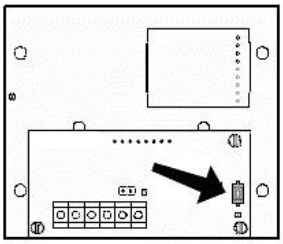
The images below demonstrate where these buttons are positioned.



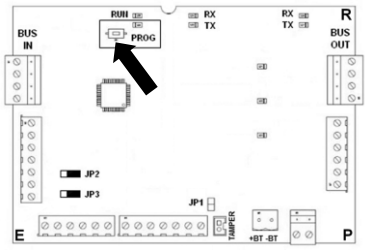
EXPANSION



READER

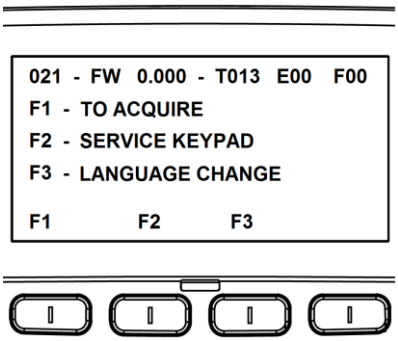


RADIO EXPANSION



1067/092 EXPANSION

To acquire the keypad during the first start-up phase, press the key associated with the **F1** symbol that appears on the display.

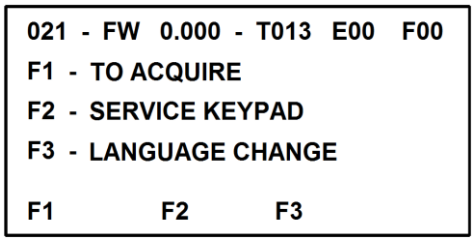


4.2.2 Procedure for acquiring the first keypad

IMPORTANT! The procedure below can be used ONLY if the BUS devices have never been acquired.

To acquire the first keypad, follow the instructions below:

1. If the device is already connected to the BUS, go directly to step 4, otherwise turn off the system completely;
2. Connect the keypad to the bus and power the system;
3. Wait for the keypad to display.



4. Press the key associated with the **F1** symbol on the keypad;

The keypad must not already have an address in its memory in order to be acquired.

To reset the address of a keypad:

- Delete it from the appropriate menu of another keypad

or

- Use the "keypad hardware reset" procedure

Example

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

- KP01
- KP02
- EP01
- DK01
- DK02
- EW01

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

4.2.3 Procedure for acquiring bus devices (expansions and readers)

See paragraph *9.2.1 Procedure for acquiring bus devices (expansions, readers and* radio interfaces).

4.3 USING THE SERVICE KEYPAD

For system acquisition and programming operations, it is possible to use a keypad connected to the Bus as the other ones, but not acquired. To decide whether to use the keypad as a service keypad, you must select the relevant option in its home page.

The service keypad is not assigned any address, so it does not preclude the possibility of acquiring other eight keypads.

At the end of the operation, it is possible to disconnect this keypad without generating tamper and therefore without having to delete it.

It is possible to connect a service keypad to any system and at any time.

5 SYSTEM COMMISSIONING

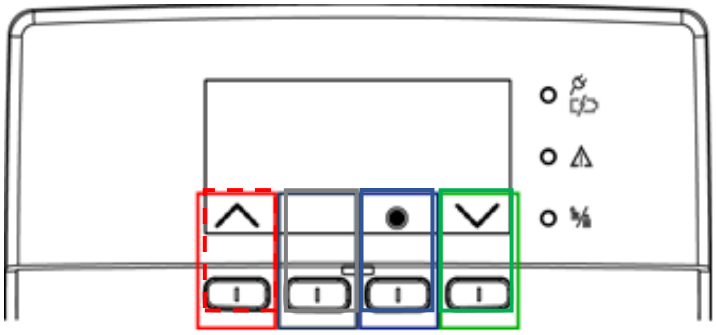
This chapter describes the structure of the various menus of the 1068/005A and 1068/010A control panels, how to access them and how to navigate them through the LCD keypad, ref. 1068/021.

The programming needed to commission the alarm system at the end of installation is also described. Programming can be carried out using a system keypad, a service keypad or a tablet featuring the 1068set Android App and connected to the control panel via an IP interface.

The programming may take place at the laboratory and then transferred to the control panel on site using an android tablet or a micro SD Card.

5.1 NAVIGATION MENU

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



IMPORTANT! The keys are associated with the respective symbols located above and shown on the display.

Key	Description
	It identifies a parameter and activates and deactivates a certain function associated with the relevant symbol positioned above according to the scrolling menu.
	It confirms the entered access code, accesses the displayed submenu or confirms the selection made.
	It goes back to the previous page or menu level.

Symbol shown on the display	Description
	Press the key associated with the symbol to activate the zones.
	Press the key associated with the symbol to deactivate the zones.
	Press the key associated with the symbol for 3 seconds to activate the auxiliary keypad functions previously programmed (for example: "Emergency" signalling).
	Press the key associated with the symbol to enter the menu.
	Press the key associated with the symbol to scroll up the menu.
	Press the key associated with the symbol to scroll down the menu.
	Press the key associated with the symbol to scroll the menu to the right. The symbol indicates that the menu or parameter includes a submenu with multiple choice.
	Press the key associated with the symbol to scroll the menu to the left. The symbol indicates that the menu or parameter includes a submenu with multiple choice.
	Press the key associated with the symbol to enable the parameter.
	Press the key associated with the symbol the parameter is NOT enabled. The symbol indicates that the parameter includes a single choice.
	Press the key associated with the symbol to enable the parameter.
	Press the key associated with the symbol the parameter is NOT enabled. The symbol indicates that the parameter includes a multiple choice.

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

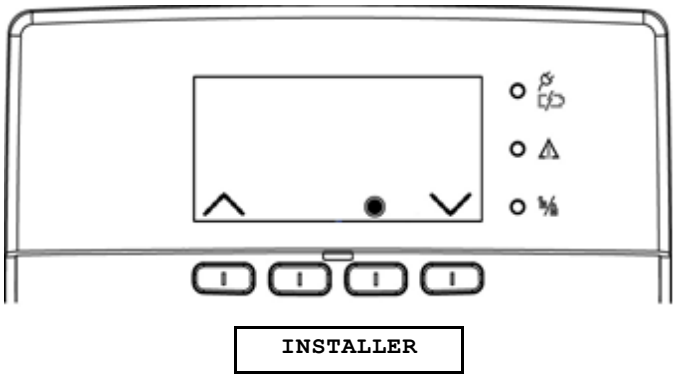
<Installer Code> (0000) **<Master Code> (1111)** **<Tech. Manager Code> (2222)** **<User Code > (0010 ÷ 0160)**	They indicate the code to be entered using the keypad. ***The factory-set codes are listed in brackets.***
< Master / User / Installer / Technical Manager Code>	This means that either code may be entered on the keypad indifferently.

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

The submenu items differ according to the access code used and the system configuration.

Example

If you have logged in as an Installer and you are in the menu item the following page will appear:



1. Press the key associated with the symbols ∨ and ∧ then scroll through the submenus of the MAIN menu;
2. The submenu items appear in cycle, i.e. the first of the list appears after the last item;
3. By pressing the key [ ] you can access the submenu limited to the "INSTALLER" profile previously added;
4. Press the key [↩] to return to the MAIN menu;
5. Press the key [↩] repeatedly to exit from the menu.

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

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

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

5.1.1 How to access menus

The menus can be accessed in two ways:

1. Enter an access code (**Master, Installer, User or Technical Manager**), then confirm with [✓];
   The displayed menu will reflect the privileges of the access code used.
2. Alternatively, press the key [ ] associated with the symbol ☰ directly.
   The free access menu described below will be opened.

5.1.2 Free access menu

Directly press the key [ ] associated with the symbol ☰, to access the following menu items:

- COMMANDS
- ICON DETAIL (visible only if there are icons to be displayed)
- SYSTEM STATUS
- KEYPAD SETTING
- SYSTEM SETTING

5.1.3 Main Menu

The main menu is the first menu that is accessed after logging in. From the items in this menu you can access all the various submenus. **M =** Master – **I =** Installer – **T =** Technical Manager – **U =** User

Profile enabled for consultation	Displayed string	Additional functions		Profile enabled for consultation	Submenu Description	
M - I - T - U	System status	→	Submenu	**M - I - T - U**	This shows the system status and can be used to change the zones status.	
M - I - T - U	Keypad settings	→	Submenu	**M - I - T – U** **Attention:** the user does not see the parts marked with asterisk of the submenu on the side.	• Display Info ***** • Set Backlight • Set Contrast • Set Buzzer	• A/B/C keys ***** • Direct setting ***** • Info (KEYPAD)
M - I - T - U	System settings	→	Submenu	**M - I - T - U**	• System log This is used to read the list of events stored on the control panel, based on the entered code.	
M - I - T - U	System settings	→	Submenu	**M - I - T - U**	• Settings This is used to isolate inputs, set the current date and time, configure the users or reset codes to default value, acquire, configure and detect electronic proximity keys and transponders and configure the time scheduler.	
M - I - T - U	System settings	→	Submenu	**M - I**	• Test This is used to carry out specific tests to check perfect operation of the system. It is possible to check the inputs of the control panel inputs and of the other devices connected to the bus, the GSM signal, the phone calls and the IP interface separately.	
M - I - T - U	System settings	→	Submenu	**I**	• Programming It allows you to configure the zones of the system, the various inputs and bus peripherals, the outputs of control panel and expansions, the keypads and readers.	
M - I - T - U	System settings	→	Submenu	**I**	• Parameters - Times This is used to set the various system timers.	
M - I - T - U	System settings	→	Submenu	**M - I**	• Communicator This is used to store the phone numbers to be dialled to send alarms and indications, customise the vocal messages, associate specific alarms to each phone number and to specify the sending methods, to set parameters of the GSM, GPRS networks and IP interface, to edit SMS messages, and to enable and configure other phone functions.	
M - I - T - U	System settings	→	Submenu	**I**	• Maintenance This is used to carry out maintenance operations on the system, such as changing the languages, acquiring devices, deleting devices, upgrading the device firmware, resetting and saving the programmed settings. • EN50131 Event log (available only with 1068/010A control panel).	
M - I - T - U	System settings	→	Submenu	**M - I**	• SIM management It allows you to set the expiry date of the SIM card used.	
M - I - T - U	System settings	→	Submenu	**M**	• Authorisations It allows you to enable or disable a user profile to perform operations.	
M - I - T - U	Commands	→	Submenu	**M - I - T - U**	• It allows you to directly control the outputs (depending on the profile added)	
M - I - T - U	Icons detail (*)	→	Submenu	**M - I – T - U**	• Faults # • Tamper # • Time scheduler #	• Open inputs # • Isolated inputs # • Alarms #

(*) = Visible in the menu only if the (#) icons are present.

5.2 HOW TO ENTER ALPHANUMERIC CHARACTERS

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

To write a name during user configuration:

1. Press the key associated to the required character until it appears;
2. Use the key associated with the symbol < and the key associated with the symbol > to go to the previous or next string position (use the "0" key to delete characters in excess);
3. Finally, press the key ✓ to save the name or to delete everything;
4. Press the key ↩ to delete what has been entered or to quit the procedure.

Key	Character
1	. , : ; ! ? / 1
2	A B C a b c 2
3	D E F d e f 3
4	G H I g h i 4
5	J K L j k l 5
6	M N O m n o 6

Key	Character
7	P Q R S p q r s 7
8	T U V t u v 8
9	W X Y Z w x y z 9
*	*
	* " $ & ' ` { } | (characters available only for password and WiFi network name)
0	[space] + - ( ) % 0
	[space] + - ( ) % = ~ 0 (characters available only for password and WiFi network name)
#	#
	# < > @ [ ] \ ^ _ (characters available only for password and WiFi network name)

5.3 HOW TO ENABLE THE INSTALLER

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

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

Proceed as follows to enable the Installer:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Users**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.
5. Select "**I: Installer**" by pressing the key associated with the ∨ or ∧ symbol.
6. Press the key associated with the "AUTHORISATIONS" message ☑ on the display to enable the **INSTALLER**. Press ✓ to confirm;
   ☑ = Installer enabled; ☐ = Installer NOT enabled
7. Press ↩ repeatedly to go back to the upper level menu.

5.4 HOW TO ENABLE THE TECHNICAL MANAGER

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

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

Proceed as follows to enable the Technical Manager:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm.
2. Select "**System Settings**" by pressing the key associated with the ∨ or symbol ∧. Press ✓ to confirm.
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.
4. Select "**Users**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Selection "**TM : Technical Manager**" by pressing the key associated with the ∨ or ∧ symbol.
6. Press the key associated with the "AUTHORISATIONS" message ☑ on the display to enable the **TECH. MANAGER**. Press ✓ to confirm; ☑ = Tech. Manager enabled ; ☐ = Tech. Manager NOT enabled
7. Press ↩ repeatedly to go back to the upper level menu.

5.5 HOW TO SELECT THE LANGUAGE

The first configuration to be carried out is the selection of the language displayed.

The default language is Italian, but you can choose between: English, French , German .

Proceed as follows to access the language selection function:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Language**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select the desired language by pressing the key associated with the ∨ or ∧ symbol.
5. Press the key associated with the "LANGUAGE" message on the display. Press ✓ to confirm;
   Selected language = ◉ ; Language NOT selected = ○
6. Press ↩ repeatedly to go back to the upper level menu.

5.6 LCD INFO

The keypad can display the following information in the home page:

- Date and time (always visible);
- Name system (visible if configured);
- Status of system zones (visible if configured);
- The display status of various icons of the system.

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

To disable the display of system zone status on the home page:

1. Access the **MASTER** / **INSTALLER / TECH. MANAGER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**LCD info**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Synoptic**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key ▭ associated with the "SYNOPTIC ☑ " message on the display;

   ENABLE ☑ : indicates the displaying mode ; ENABLE ☐ : indicates the NOT displaying mode
6. Press ✓ to confirm.
7. Press ↩ repeatedly to go back to the upper level menu.

5.7 DATE AND TIME SETTING

In addition to being shown on the keypad in the home page, date and time information is used to record events (System log) and for the Time Scheduler functions.

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

1. Access the **MASTER / INSTALLER / TECH. MANAGER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Date and Time**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Set hour**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Use the alphanumeric keypad to enter the correct time. Press ✓ to confirm;
7. Select "**Set date**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Use the alphanumeric keypad to enter the correct date. Press ✓ to confirm;
9. Press ↩ repeatedly to go back to the upper level menu.

To set the daylight saving time, follow the instructions below:

1. Access the **MASTER** / **INSTALLER** / **TECH. MANAGER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Date and Time**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Set the Daylight Saving Time**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm. Press ✓ to confirm;
6. Use the alphanumeric keypad to enter the correct time. Press ✓ to confirm.
7. Press ↩ repeatedly to go back to the upper level menu.

IMPORTANT! The time scheduler will not work properly if the date and time are not correct and the Event and System Log time references will not be correct.

5.8 ZONES PROGRAMMING

The 1068 series control panels manage:

- up to 4 zones, 1068/005A control panel
- up to 8 zones, 1068/010A control panel

The number of actual zones is determined at the programming stage, with each system having at least one.

System inputs, outputs, keypads and readers can be freely assigned and belong to more than one zone. The activation mode can be programmed for each zone when the system is activated, if some assigned intrusion inputs are open.

The available activation modes depend on the operation of the control panel (whether EN50131 or not), as shown below.

EN50131 GRADO 1

EN50131 GRADO 2

Prevention of setting: a zone programmed in this way cannot be activated, without the explicit enabling by the user if any assigned inputs are open. If the system is in EN50131 Grade 1 (Ref. 1068/005A) or EN50131 Grade 2 (Ref. 1068/010A) compliant mode, all zones are automatically set in this mode and it is not possible to change the programming. Programming only available in EN50131 compliant operating mode.

EN50131

Standard: an alarm is generated if any assigned inputs are open when the zone is armed. The system prevents this type of programming from being used when in EN50131 compliant mode.

Self inhibition: the intrusion inputs that can be isolated associated with the zone that are open at the time of activation are automatically isolated. The isolated inputs will automatically end insulation if they are closed again. The system prevents this type of programming from being used when in EN50131 compliant mode.

With open inputs, a Standard zone allows activating the system and triggering the alarm, a Prevention of setting zone prevents system activation without the explicit enabling, a Self Inhibition zone always allows system activation.

Proceed as follows to program the zones:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Zones**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Zones number**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Press the key corresponding to the "ZONES NUMBER" message on display;
   ◉ - Selected zone ; ○ - NOT selected zone
7. Press ✓ to confirm;
8. Press ↩ to return to the upper level menu;
9. Select "**Zone configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
10. Select the zone you want to configure by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
11. Select "**Name**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
12. Use the alphanumeric keypad to enter the name to be associated with the zone; Press ✓ to confirm;
13. Press ↩ to return to the upper level menu;
14. Select "**Setting mode**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
15. Select the desired customisation:
    - Standard ○
    - Self inhibition ◉
16. Press ✓ to confirm;
17. Press ↩ repeatedly to go back to the upper level menu.

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

⚠	**IMPORTANT!** The "SETTING MODE" menu is not available in EN50131 operating mode compliant.

5.9 WIRED INPUT PROGRAMMING

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

The 1068A series system manages the following number of general use inputs:

- up to 21 inputs, 1068/005A control panel
- up to 66 inputs, 1068/010A control panel.

The SAB tamper inputs of the control panel cannot be programmed.

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

5.9.1 Wired input encoding

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

physical address → logical address

and in detail

ddXX In**Y:** → In**ZZ**

where:

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

The physical address is useful for installers during system installation and maintenance. The physical location is shown on the display (**CP** = control panel, **EP** = expansion, **KP** = keypad, **DK** = reader).

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

The first 5 inputs of the system are those of the control panel itself, while the inputs of the keypads and readers are not considered, because they leave the factory as NOT USED.

For each input consider a number of elements that will then determine their functionality.

The elements are:

- Electrical and therefore wiring characteristics
- Functional customisation
- Functional options for intrusion inputs
- Auxiliary functions for customised intrusion inputs
- Isolation or inhibition of inputs

5.9.2 Input types

The input type determines the way the control panel will interpret the electric circuit signals (detector + connection wires) connected to the input itself.

The physical features of all inputs may be changed by programming, except for the SAB input which can only be of the balanced type and to which the tamper alarm is assigned. Possible alarm input types are:

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

The 1068/005A system manages up to 21 inputs, the 1068/010A system manages up to 66 inputs.
All the control panel inputs are pre-set by default.

- **N.C**. (normally closed): in stand-by mode it is set to -V⎓ and the electric circuit connected to the input must be closed. Its opening will trip the associated event. This is not EN50131 compliant.
- **N.O.** (normally open): in stand-by mode it is set to floating and the electric circuit connected to the input must be open. Its closing will trip the associated event. This is not EN50131 compliant.
- **Single balancing**: determines 2 voltage thresholds with which the following 3 statuses are recognised and managed:
  - Stand-by status;
  - Alarm signalling;
  - Tampering signalling implemented through short circuit of the wires.
- **Double balancing**: determines 3 voltage thresholds with which the following 4 statuses are recognised and managed:
  - Stand-by status;
  - Alarm signalling;
  - Tampering signalling implemented through short circuit;
  - Tampering signalling implemented through the cutting of wires

  1068/010A Control panel - Compliant with EN50131 - Grade 2

EN50131 GRADO 1 EN50131 GRADO 2

- **Inertial**: an alarm indication is tripped when the electric circuit remains open for a time equal to programmed sensitivity. The following 2 statuses are recognised and managed:
  - Closed;
  - Open.

  This is not EN50131 compliant.

EN50131

- **Roller**: this causes an alarm indication to trip when the electric circuit is opened and closed for the number of times equal to the programmed sensitivity in a given time. The following 2 statuses are recognised and managed:
  - Closed;
  - Open.

  This is not EN50131 compliant.
- **Double input**: determines 4 voltage thresholds with which the following 5 status are recognised and managed:
  - Stand by status;
  - Alarm signalling detector **A**;
  - Alarm signalling detector **B**;
  - Tampering signalling implemented through short circuit of the wires.
  - Alarm signalling of both detectors

  This is not EN50131 compliant.

5.9.3 Wired input customisation

Alarm input customisation determines how, when and what alarm type to generate. The control panel will activate the respective devices (outputs, sirens and phone dialer) according to the generated alarm type.

The possible input customisations are described below.

The customisations listed below are all EN50131 *compliant*:

INSTANTANEOUS INTRUSION

The opening of the input triggers the intrusion alarm when:

- The input has an AND type assignment and the zones to which it belongs are all active,
- The input has an OR type assignment and at least one of the zones to which it belongs is active.

DELAYED INTRUSION

This is typically used for detectors which could be triggered by the users themselves when setting and unsetting the system (for example, the magnetic contact on the entrance door).

In general, it is suggested to use this configuration to allow delayed entry and exits when the control unit with which the system is activated/deactivated is inside the protected area. In particular, it must be done if the entry/exit passage is protected not only by bistable sensors (e.g. magnetic contacts) but also by monostable sensors (e.g. seismic).

Programming this type of inputs requires the setting of a guard time, called delay.

Entry procedure

The opening of the input triggers the intrusion alarm when:

- The input has an AND type assignment and the zones to which it belongs are all active.
- The input has an OR type assignment and at least one of the zones to which it belongs is active.

The alarm is not generated instantaneously but only after its delay time has elapsed after opening (entry delay).

The entry delay count, and consequently the generation of the alarm, can be interrupted:

- Deactivating all zones with OR type assignment to which the input belongs or
- Deactivating at least one of the zones with AND type assignment to which the input belongs.

Exit procedure

When a zone with delayed inputs is activated, a time count equal to the maximum delay programmed for each input (exit delay) starts. During this count, input movements are ignored.

The exit delay count will restart if another zone containing the same input is activated.

At the end of the exit delay, if the input is opened, the entry delay count starts.

The keypad buzzers are activated by default during the “Entry Time” and during the “Exit Time” (see paragraph *5.11 Keypad programming*). The indication may be deactivated.

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

If the control device (keypad or reader) used to arm and disarm the system is located inside a protected area, it is advisable to use the first entry/last exit intrusion and Intrusion path customisations, for all the detectors interposed between the control device and the access doors.

Using Intrusion path customisation (instead of delayed intrusion) for volumetric detectors in the home has the advantage that the detectors will behave as Immediate detectors if the door is not opened.

Using the Intrusion first entry/last exit customisation (instead of delayed intrusion) has the advantage that the Exit Time is interrupted when leaving the house when the door is closed.

	IMPORTANT! Do not use inputs with Delayed customisation and with First Entry, Last Exit, Path customisation inputs in the same zone.

FIRST ENTRY/LAST EXIT

It is suggested to use this configuration in general to allow delayed inputs and outputs when the control unit with which the system is activated/deactivated is inside the protected area. In particular, it is recommended to adopt it when the path crossing time is important or variable and it is necessary to set a significant delay time. In fact, after the activation of the exit time, when the system is activated, this time will be automatically stopped at the exit of the gate, preventing the system from remaining "unprotected" until the end of the time. Usually, in this type of configuration, the access/exit gates of the area are protected by magnetic contacts and will be of the first entry/last exit type, while the other detectors, positioned along the path between the control device and the gate will be of the Intrusion path type. If the entry/exit gate is protected not only by bistable detectors (e.g. magnetic contacts) but also by monostable detectors (e.g. seismic), this configuration is not recommended.

Programming this type of inputs requires the setting of a guard time, called delay.

Entry procedure

The opening of the input triggers the intrusion alarm when:

- The input has an AND type assignment and the zones to which it belongs are all active
- The input has an OR type assignment and at least one of the zones to which it belongs is active.

The alarm is not generated instantaneously but only after its delay time has elapsed after opening (entry delay).

The entry delay count, and consequently the generation of the alarm, can be interrupted:

- Deactivating all zones with OR type assignment to which the input belongs or
- Deactivating at least one of the zones with AND type assignment to which the input belongs.

Exit procedure

When a zone containing configured first entry/last exit inputs is activated, for each input configured as first entry/last exit or Intrusion Path, a count lasting as its delay time (exit delay) starts. During this count, the input opening is ignored.

The count will restart if another zone containing the same input is activated.

If during the exit count the input is closed, all other active "exit counts" in the associated zones are interrupted.

	**IMPORTANT**! In the same zone there must **NEVER** be delayed inputs and inputs delayed as first entry - last exit.

	**IMPORTANT**! If the control panel is in a mode compliant with EN50131, if an intrusion alarm condition occurs during an entry time, any alarm notifications via vocal calls, SMS, calls to surveillance centres or PUSH notifications will be postponed by at least 30 seconds, or in any case until the end of the entry time, to allow deactivating the system.

INTRUSION PATH

This configuration is used in combination with the configuration of inputs belonging to the same zone as the first entry/last exit type.
The opening of the input triggers the intrusion alarm when:

- The input has an AND type assignment and the zones to which it belongs are all active
- The input has an OR type assignment and at least one zone to which it belongs is active unless "Entry path time" or the "Exit path time" is elapsing.

KEY

The opening of the input arms or disarms all the zones assigned to it by reversing the respective state (the zones will be disarmed if they are not, and vice versa). All zones will be disarmed if some are armed and some are disarmed.
The input is active 24 hours (24/7).

TAMPER

The opening of the input generates the Tamper event regardless of the zone setting status. The input is active 24 hours (24/7).

DETECTORS FAILURE

The opening of the input generates the Detector Failure event. The event controls the detector failure outputs with at least one zone in common with the input.
The input is active 24 hours (24/7).

SIRENS FAILURE

The opening of the input generates the Siren Failure event regardless of the zone activation status. The event controls the siren failure outputs with at least one zone in common with the input.
The input is active 24 hours (24/7).

The customisations listed below are *not compliant* with EN50131:

TECHNOLOGICAL SUSTAINED

The opening of the input generates a Technological Sustained event regardless of the zone activation status. The input is active 24 hours (24/7).

Technological sustained inputs must be assigned (by means of the zones) to at least one technological sustained output.

TIMED TECHNOLOGICAL

The opening of the input generates a Timed Technological event regardless of the zone activation status. The input is active 24 hours (24/7).

Timed technological inputs must be assigned (by means of the zones) to at least one timed technological output.

PREALARM INTRUSION

The opening of the input generates the Prealarm intrusion when:

- The input has an AND type assignment and the zones to which it belongs are all active.
- The input has an OR type assignment and at least one of the zones to which it belongs is active.

HOLD-UP

The opening of the input generates the hold-up indication regardless of the zones setting status. The input is active 24 hours (24/7).

ANTI THIEF

The opening of the input generates the Anti Thief alarm indication regardless of the zone activation status.
The signalling controls the intrusion outputs and the zone status outputs with at least one zone in common with the input.
The input is active 24 hours (24/7).

EMERGENCY

The opening of the input generates the emergency indication regardless of the zone setting status.
The signalling controls the emergency outputs with at least one zone in common with the input.
The input is active 24 hours (24/7).

FIRE (available only with 1068/010A control panel)

The opening of the input generates the Fire Alarm indication regardless of the zones arming status.
The input is active 24 hours (24/7).

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

FIRE RESET (available only with 1068/010A control panel)

The opening of the input switches the assigned reset fire alarm outputs for 1 second and resets the fire indications, regardless of the zones arming status.

The input is active 24 hours (24/7).

COMMUNICATOR FAILURE (available only with 1068/010A control panel)

The opening of the input generates the Communicator failure event. The customized failure output of the communicator must be connected to the input.

The input is active 24 hours (24/7).

5.9.4 Isolable

An input set as “isolable” will be subject to manual and automatic isolations.

Proceed as follows to isolate the input:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Inputs**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the input to be programmed by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Isolable**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Press the key I associated with the "**Isolable**" message on the display to enable input isolation;
8. ISOLABLE" ☑ : input isolation enabled; ISOLABLE" ☐ : input isolation NOT enabled.
9. Press ✓ to confirm;
10. Press ↩ repeatedly to go back to the upper level menu.

5.9.5 Auxiliary functions of intrusion inputs (Gong, Courtesy light and Door opener)

Auxiliary functions can be associated to the inputs defined as intrusion.

The auxiliary functions are not mutually exclusive (each input can be associated with more than one).

See *Alarm system design manual* for more details on the single functions.

These functions are not EN50131 compliant because they are not described in the standard.

Gong

This auxiliary function is operative in conditions in which the input, if opened, would NOT give an alarm, that is:

- Zone assignment = AND and at least one zone associated with the input is deactivated or
- Zone assignment = OR and all the zones associated with the input are deactivated.

When the function is operative, the opening of the input generates a Gong event. If there are customised outputs in the system such as Gong with at least one zone in common with the input, they will be piloted (for a predefined time of about 3 seconds).

Courtesy light with deactivated system (OFF)

This auxiliary function is operative in conditions in which the input, if opened, would NOT give an alarm, that is:

- Zone assignment = AND and at least one zone associated with the input is deactivated or
- Zone assignment = OR and all the zones associated with the input are deactivated.

When the function is operative, when the input is opened, if the system has customised outputs such as Courtesy Light with at least one zone in common with the input, these will be controlled for a time that can be configured using the "Courtesy Light Time" parameter.

Courtesy Light with actived system (ON)

This auxiliary function is operative when the input, if opened, would trigger an alarm, that is:

- Zone assignment = AND and all zones associated with the input are active or
- Zone assignment = OR and at least one zone associated with the input is active

When the function is operative, when the input is opened, if the system has customised outputs such as Courtesy Light with at least one zone in common with the input, these will be controlled for a time that can be configured using the "Courtesy Light Time" parameter.

Door opener

This auxiliary function is operative in conditions in which the input, if opened, would NOT give an alarm, that is:

- Zone assignment = AND and at least one zone associated with the input is deactivated or
- Zone assignment = OR and all the zones associated with the input are deactivated.

When the function is operative, when the input is opened, if the system has customised outputs such as Door opener with at least one zone in common with the input, these will be controlled for a time that can be configured (“Door Opener Time”).

5.9.6 Zone assignment type (AND / OR)

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

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

5.9.7 AND inputs

This function is EN50131 compliant.

It logically connects two instantaneous intrusion pre-alarm and path inputs with the same customisation, same assigned zones and AND/OR zone assignment. The alarm is generated only if both are opened within a configurable time in minutes from one another (the first input to be opened may be closed again in the meantime).

See *Alarm system design manual* for more details on the single functions.

5.9.8 Input programming procedure

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

Proceed as follows to program the inputs:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Inputs**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the ∨ or ∧ symbol and select the input to be configured by pressing ✓ to display the configuration parameters;
   - Input type
   - Zone assignment
   - Customisation
   - Isolable
   - Complementary functions
   - Assignment type
   - AND Inputs
   - Name
6. Press the key associated with the ∨ or ∧ symbol and select the parameter to be configured; Press ✓ to confirm;
7. Press ↩ to return to the upper level menu;
8. The "**Input Type**" parameter allows you to associate a type to the selected input.
   - NC ○
   - NO ○
   - Balanced ○
   - Double Balancing ◉
   - Inertial ○ > High / Medium / Low
   - Roller ○ > High / Medium / Low
   - Not used ○
9. Select the input type by pressing the key associated with the ∨ or ∧ symbol. Press the key associated with the symbol ◉, on the display the indication in the right column will change from ○ to ◉ to indicate the change of configuration. Press ✓ to confirm, press ↩ to return to the upper level menu;
10. The "**Zone assignment**" parameter allows you to associate the input with a zone.
    - ZN01: Zone 1 ☐ ; ZN02: Zone 2 ☑
11. Select the zone by pressing the key associated with the ∨ or ∧ symbol;
12. Press the key associated to the symbol ☐, in the box of the right column a confirmation sign ☑ will appear to indicate the zone assignment;
13. Press ↩ to return to the upper level menu;
14. The "**Customisation**" parameter allows you to assign a customisation to the input.
    - First Entry/Last Exit ○ >
      MIN:000 SEC:00
    - Intrusion path ○
    - Prealarm intrusion ◉
    - Tamper ○
    - Technological sustained ○
    - Timed technological ○
    - Hold-up ○
    - Emergency ○
    - Anti thief ○
    - Key ○
    - Detectors failure ○
    - Sirens failure ○
    - Instantaneous Intrusion ○
    - Delayed Intrusion >
      MIN:000 SEC:00
15. Select the function to be associated by pressing the key associated with the ∨ or ∧ symbol;
16. Press the key associated with the symbol ◉;
17. On the display, the indication in the right column will change status from ○ to ◉ to indicate the change of configuration;
18. The parameters with the symbol > allow you to set the minutes and seconds of the customisation;

IMPORTANT!
With reference to EN50131, this setting, which defines entry time and exit time, must not exceed 45 seconds.

19. Press ✓ to confirm, press ↩ to return to the upper level menu;
20. The "**Isolable**" parameter allows the selected input to be isolated.
    - Isolable ☑
21. Press the key associated to the symbol ☐, in the box of the right column a confirmation sign ☑ will appear to indicate the activation of the parameter. Press ✓ to confirm, press ↩ to return to the upper level menu.
22. The "**Complementary functions**" parameter allows you to associate complementary functions to the input.
    You can associate multiple complementary functions to one input.
    - Gong ☑
    - Courtesy light ON ☐
    - Courtesy light OFF ☐
    - Door opener ☑
23. Select the function by pressing the key associated with the ∨ or ∧ symbol.
24. Press the key associated with the symbol ☐, the confirmation sign will appear in the box in the right column.
25. Press ↩ to return to the upper level menu;
26. The "**Assignment type**" parameter allows you to choose the type of assignment of the input.
    - And ◉
    - Or ○
27. Select the parameter by pressing the key associated with the ∨ or ∧ symbol;
28. Press the key associated with the symbol ◉, on the display the indication in the right column will change status from ○ to ◉.
    Press ✓ to confirm, press ↩ to return to the upper level menu.
29. The "**AND Inputs**" parameter allows you to display, disable and select the AND inputs.
    - Display AND >
    - Disable AND >

    After the selection you will be asked to confirm the selection **Are you sure?** >
30. Press ✓ to confirm.
    - Select AND >
    - LIST OF INPUTS >
    - INPUT CHOICE >
31. The "**NAME**" parameter allows you to rename the selected input. The name can be up to 24 characters long;
32. Press ✓ to confirm;
33. Press ↩ repeatedly to go back to the upper level menu.

	**IMPORTANT**! Program all inputs used in the system.

5.10 WIRED INPUT PROGRAMMING

The 1068A series system manages the following number of general use outputs:

- up to 10 outputs, 1068/005A control panel
- up to 28 outputs, 1068/010A control panel.

See the paragraph *1.2.3 Maximum system size* for more information and connections.

5.10.1 Output encoding

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

physical address → logical address

and in detail

ddXX U**Y:** → U**ZZ**

where:

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

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

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

5.10.2 Output types

For each output consider a number of elements that will then determine their functionality. The elements are:

- Electrical and therefore wiring characteristics (paragraph *5.10.4 Electrical characteristics of the outputs).*
- Functional customisation (paragraph *5.10.5 Output customisations*).

5.10.3 Output assignment

Each output may be assigned to the entire system, i.e. to all zones, or only to some zones.

The output is activated only by events or inputs which concern the assigned zones.

5.10.4 Electrical characteristics of the outputs

In the control panel there are 2 electrical outputs and 2 relay outputs.
Each output can be programmed from the menu as:

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

See the paragraph *3.11.6.3 Output stand-by: N.H. and N.L.* for a detailed analysis of relay and electric outputs when set to N.L. or N.H.

5.10.5 Output customisations

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

For further information, please see paragraph *3.11.6.3 Output stand-by: N.H. and N.L. .*

The possible customisations for EN50131 compliant outputs are described below.

EN50131 GRADO 1 EN50131 GRADO 2

OUTPUT BURGLAR ALARM

The burglar alarm output is activated if an intrusion event is generated by 1 input and at least 1 zone associated with the output is active and in common with the input.

The zone assignment type (AND/OR) influences the MUTING.

The output is muted if

- At least 1 zone associated with the output is deactivated (or a code is entered with at least one zone in common with the output) (**if zone assignment type of the OUTPUT is OR**)

or

- All the zones associated with the output are deactivated (or a code is entered associated with all the zones associated with the output) (**if zone assignment type of the OUTPUT is AND**)

If the output is not muted, the duration of the activation is defined by the "Intrusion Alarm Time".

OUTPUT PRE-ALARM

The Pre-alarm output is activated if a pre-alarm event is generated by 1 input and at least 1 zone associated with the output is active and in common with the input.

The zone assignment type (AND/OR) influences the MUTING.

The output is muted if:

- At least 1 zone associated with the output is deactivated (or a code is entered with at least one zone in common with the output) (**if the zone assignment type of the OUTPUT is OR**).

or

- All the zones associated with the output are deactivated (or a code is entered associated with all the zones associated with the output) (**if zone assignment type of the OUTPUT is AND**).

If the output is not muted, the duration of the activation is defined by the "Pre-alarm alarm Time".

OUTPUT TAMPER

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

	**IMPORTANT**! If the tamper condition is generated by an input (tamper input or unbalance of any input): the input must have at least one zone in common with the output.

The duration of the activation is defined by the "Tamper Alarm Time".

OUTPUT INTRUSION+PRE-ALARM

The duration of the activation is defined by the "Intrusion Alarm Time" or "Pre-alarm Alarm Time" (depending on the event that caused the output to be activated).

OUTPUT INTRUSION + TAMPER

The duration of the activation is defined by the "Intrusion Alarm Time" or "Tamper Alarm Time" (depending on the event that caused the output to be activated).

OUTPUT INTRUSION + TAMPER + PRE-ALARM

The duration of the activation is defined by the "Intrusion Alarm Time" or "Tamper Alarm Time" or "Pre-alarm Alarm Time" (depending on the event that caused the output to be activated).

OUTPUT TECHNOLOGICAL SUSTAINED

The customised Technological Sustained output remains in stand-by until all the inputs with the same customisation and with at least one zone in common with the output are in stand-by, vice versa it is piloted and remains piloted as soon as an input with the same customisation and with at least one zone in common with the output sets to open. The output will obviously return to stand-by mode as soon as all the inputs with the same customisation and with at least one common zone set back to stand-by mode.

OUTPUT TIMED TECHNOLOGICAL

The customised Timed Technological output remains in stand-by until all the inputs with the same customisation and with at least one zone in common with the output are in stand-by, vice versa it is piloted as soon as an input with the same customisation and with at least one zone in common with the output sets to open. The output will return to stand-by mode after a time programmable from the menu.

This time is the same for all outputs: “Pulsed Commandable Time”.

OUTPUT EMERGENCY

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

OUTPUT COMMANDABLE SUSTAINED

The commandable output may be activated but cancels EN50131 compliance when:

- it is activated/deactivated via text message;
- it is activated/deactivated remotely by dialling an appropriate DTMF sequence;
- the control panel is called on the GSM network from the phone number to which the zero-cost call function is associated;
- the “**+**” key on the remote control is pressed.

OUTPUT TIMED COMMANDABLE

The Timed commandable output is EN50131 compliant when:

- it is activated by a time scheduler output activation command.
- it is deactivated by a time scheduler output deactivation command.

OUTPUT SYSTEM FAILURE

The System failure output is activated if a System failure alarm is generated.

OUTPUT DETECTOR FAILURE

The Detector failure alarm output is activated if a Detector failure alarm is generated.

IMPORTANT!
If the condition is generated by an input: the input must have at least one zone in common with the output.

OUTPUT SIREN FAILURE

The Siren failure alarm output is activated if a Siren failure alarm is generated.

IMPORTANT!
If the condition is generated by an input: the input must have at least one zone in common with the output.

OUTPUT SYSTEM/DETECTOR/SIREN FAILURE

The output is activated if a System/Detector/Siren failure alarm is generated.

OUTPUT LOW BATTERY

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

OUTPUT LOSS OF MAINS

The blackout output is activated if a "loss of mains" event is generated.

OUTPUT GONG

The Gong output is activated if an intrusion input, whose complementary Gong function has been enabled, is opened (only in the conditions where the input does NOT trigger the alarm). The duration of the activation is set to 2 seconds.

IMPORTANT! The input must have at least one zone in common with the output.

OUTPUT COURTESY LIGHT

The Courtesy light output is activated if an intrusion input is opened and at least one Courtesy light complementary function has been enabled (Courtesy light with active system or Courtesy light with inactive system). The duration of the activation is defined by the "Courtesy Light Time".

	**IMPORTANT**! The input must have at least one zone in common with the output.

OUTPUT DOOR OPENER

The door opener output is activated when a door opener event is generated. The duration of the activation is defined by the "Door opener time".

The Door opener event is generated:

- By the opening of an intrusion input whose complementary Door opener function has been enabled (only in the conditions where the input does NOT trigger the alarm).
- By the reading of a key with access control function.

	**IMPORTANT**! The input or key must have at least one zone in common with the output.

OUTPUT ZONE STATUS

The Zone Status output is activated when:

- At least 1 zone associated with the output is active (**if zone assignment type of the OUTPUT is OR**)

or

- All zones associated with the output are active (**if zone assignment type of the OUTPUT is AND**)

O FIRE ALARM (available only with 1068/010A control panel)

The fire alarm output is activated if a fire event is generated.

O RESET FIRE ALARM (available only with 1068/010A control panel)

The reset fire alarm output is activated if a reset fire alarm is opened.

O COMMUNICATOR FAILURE (available only with 1068/010A control panel)

The communicator failure output is activated if a communicator failure output is opened with a 10 sec delay.

O ENTRY TIME SIGNALLING (available only with 1068/010A control panel)

The output activates for 0.8 seconds ON and 0.2 seconds OFF when at least one of the associated zones is counting an entry time.

O EXIT TIME SIGNALLING (available only with 1068/010A control panel)

The output activates for 0.8 seconds OFF and 0.2 seconds ON when at least one of the associated zones is counting an exit time.

O ENTRY/EXIT TIME SIGNALING (available only with 1068/010A control panel)

The output activates for 0.8 seconds ON and 0.2 seconds OFF, or for 0.8 seconds OFF and 0.2 seconds ON when at least one of the associated zones is counting an entry or an exit time.

5.10.6 Output behaviour when the system is being serviced

The following shows the behaviour of the customised outputs when the system is being serviced:

Customised output	Behaviour in maintenance
Intrusion	It does not switch
Pre-alarm	It does not switch
Tampering	It does not switch
Intrusion + Pre-alarm	It does not switch
Intrusion + Tamper	It does not switch
Intrusion + Tamper + Pre-alarm	It does not switch
Technological sustained	It switches
Timed technological	It switches
Emergency	It switches
Commandable sustained	It switches
Timed commandable	It switches
System failure	It does not switch
Detector failure	It does not switch
Siren failure	It does not switch
System/Detector/Siren Failure	It does not switch
Low battery	It does not switch
Loss of mains	It switches
Gong	It switches
Courtesy light	It switches
Door opener	It switches
Fire*	It does not switch
Reset fire*	It does not switch
Communicator failure*	It does not switch
Entry time *	It does not switch
Exit time*	It does not switch
Entry/Exit time *	It does not switch
Zone status	It does not switch

***** = available only with 1068/010A control panel.

5.10.7 Output programming procedure

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

Proceed as follows to program the outputs:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Outputs**" by pressing the key associated with the ∨ or ∧ symbol.
   Press ✓ to display the available inputs.
   - CP .U4: UO4: … >
   - CP .U1: UO1: … >
   - CP .U2: UO2: … >
   - CP .U3: UO3: … >
5. Press the key associated with the ∨ or ∧ symbol and select the output to be configured.
   Press ✓ to display the configuration parameters:
   - Output type
   - Zone assignment
   - Customisation
   - Assignment type
   - Name
6. Press the key associated with the ∨ or ∧ symbol and select the parameter to be configured. Press ✓ to confirm.
7. Press ↩ to return to the upper level menu.
   The "**Output Type**" parameter allows you to associate a type to the selected output.
   - NH ○
   - NL ○
   - Not used ○
8. Select the type of output by pressing the key associated with the ∨ or ∧ symbol.
9. Press the key associated with the symbol ◉, on the display the indication in the right column will change from ○ to ◉ to indicate the change of configuration;
10. Press ✓ to confirm;
11. Press ↩ to return to the upper level menu;
    The "**Zone assignment**" parameter allows you to associate the output with a zone.
    a. ZN01: Zone 1 ☐
    b. ZN02: Zone 2 ☑
12. Select the zone by pressing the key associated with the ∨ or ∧ symbol
13. Press the key associated to the symbol ☐, in the box of the right column a confirmation sign ☑ will appear to indicate the zone assignment;
14. Press ↩ to return to the upper level menu;
    The "**Customisation**" parameter allows you to assign a customisation to the output.
    - Prealarm intrusion ◉
    - Intrusion Tamper ○
    - Intrusion Tamper Pre-alarm ○
    - Technological sustained ○
    - Timed technological ○
    - Emergency ○
    - Commandable sustained ○
    - Timed commandable ○
    - System failure ○
    - Detector failure ○
    - Siren failure ○
    - System / Detector / Siren Failure ○
    - Low Battery ○
    - Loss of mains ○
    - Gong ○
    - Courtesy light ○
    - Door opener ○
    - Zone status ○
    - Intrusion ○
    - Pre-alarm ○
    - Tamper ○

    Select the zone by pressing the key associated with the ∨ or ∧ symbol.
15. Select the function to be assigned by pressing the key associated with the ∨ or ∧ symbol.

16. Press the key associated with the symbol ◉, on the display the indication in the right column will change status from ○ to ◉ to indicate the change of configuration.
17. Press ✓ to confirm, press ↩ to return to the upper level menu.
    The "Assignment type" parameter allows you to choose the type of assignment of the input.
    - And ◉
    - Or ○
18. Select the parameter by pressing the key associated with the ∨ or ∧ symbol;
19. Press the key associated with the symbol ◉, on the display the indication in the right column will change status from ○ to ◉;
20. Press ✓ to confirm, press ↩ to return to the upper level menu.
    The "**Name**" parameter allows you to rename the selected input. The name can be up to 24 characters long.
21. Press ✓ to confirm. Press ↩ repeatedly to go back to the upper level menu.

5.11 KEYPAD PROGRAMMING

The keypad programming procedure is described below.

5.11.1 Function programming procedure

- **Name system:** it displays or hides the system name on the home page of the keypad.
- **Synoptic:** it displays or hides the status of the system zones on the home page.
- **Set backlight:** screen backlight adjustment.
- **Set contrast:** screen contrast adjustment.
- **Set buzzer:** Buzzer volume adjustment.
- **A / B / C keys:** association of the three rapid activation keys to the system zones.
- **Direct setting**: enables the possibility to activate the system from the keypad without entering code.

To enable the displaying of the **system Name** on the keypad, proceed as follows:
1. Access the **MASTER / INSTALLER / TECH. MANAGER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**LCD info**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Name system**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the "NAME SYSTEM" message ☐ on the display.
   ENABLE ☑ : assigned zone ; ENABLE ☐ NOT assigned zone
   Press ✓ to confirm.
6. Press ↩ to return to the upper level menu.

To enable the displaying of the **Synoptic** on the keypad, proceed as follows:
1. Access the **MASTER / INSTALLER / TECH. MANAGER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**LCD info**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Synoptic**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the "SYNOPTIC" message ☐ on the display.
   ENABLE ☑ : assigned zone ; ENABLE ☐ NOT assigned zone
   Press ✓ to confirm.
6. Press ↩ to return to the upper level menu.

To edit the **Set Backlight** parameter on the keypad, proceed as follows:
1. Access the **MASTER / INSTALLER / TECH. MANAGER** / **USER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Set backlight**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Press the key | in correspondence of the character " **+** / **-** " on the display to increase or decrease the brightness. Press ✓ to confirm;
5. Press ↩ to return to the upper level menu.

To edit the **Set contrast** parameter on the keypad, proceed as follows:
1. Access the **MASTER / INSTALLER / TECH. MANAGER** / **USER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Set contrast**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Press the key | in correspondence of the character " **+** / **-** " on the display to increase or decrease the contrast. Press ✓ to confirm;
5. Press ↩ to return to the upper level menu.

Proceed as follows to adjust the **buzzer volume**:

1. Access the **MASTER / INSTALLER / TECH. MANAGER** / **USER** menu by entering the access code. Press ✓ to confirm.
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Set buzzer**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Press the key ▮ in correspondence of the character " **+** / **-** " on the display to increase or decrease the volume.
5. Press ↩ to return to the upper level menu.

To configure the **A / B / C fast activation keys,** proceed as follows:

1. Access the **MASTER** / **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**A / B / C keys**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**A key**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the zone "**ZNXX : Zone X**" by pressing the key associated with the ∨ or ∧ symbol;
6. Press the key associated with the "ASSIGNMENT" message ☑ on the display to assign the zone to key A.

   ASSIGNMENT ☑ : assigned zone ; ASSIGNMENT ☐ : NOT assigned zone
   Press ✓ to confirm;
7. Perform the assignment operation for all zones you want to assign to key A;
8. Perform operations from Step 4 for all A / B / C keys;
9. Press ↩ repeatedly to go back to the upper level menu.

Proceed as follows to enable the **"Direct setting"** function:

1. Access the **MASTER** / **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Direct setting**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Press the key associated with the "DIRECT SETTING" message ☐ on the display.

   DIRECT SETTING ☑ : enabled ; DIRECT SETTING ☐ : NOT enabled
   Press ✓ to confirm;
5. Press ↩ repeatedly to go back to the upper level menu.

5.11.2 Zones assignment

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Keypads**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the keypad to be programmed by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Zone assignment**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select the zone by pressing the key associated with the ∨ or ∧ symbol;
8. Press the key associated with the "ASSIGNMENT" message ☐ on the display ☑ to indicate the assignment to the zone.

   ASSIGNMENT ☑ : enabled ; ASSIGNMENT ☐ : NOT enabled
9. Press ✓ to confirm;
10. Press ↩ repeatedly to go back to the upper level menu.

5.11.3 Gong function

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Keypads**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the keypad to be programmed by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Gong function**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Press the key associated with the "GONG FUNCTION" message ☑ on the display. Press ✓ to confirm;

   Enable ☑ : function enabled ; Enable ☐ : function NOT enabled
8. Press ↩ repeatedly to go back to the upper level menu.

5.11.4 Entry time

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Keypads**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the keypad to be programmed by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Entry time**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Press the key associated with the "ENTRY TIME" message ☑ on the display. Press ✓ to confirm;

   Enable ☑ : function enabled ; Enable ☐ : function NOT enabled;
8. Press ↩ repeatedly to go back to the upper level menu.

5.11.5 Exit time

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Keypads**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the keypad to be programmed by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Exit time**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Press the key associated with the "EXIT TIME" message ☑ on the display. Press ✓ to confirm;

   Enable ☑ : function enabled ; Enable ☐ : function NOT enabled;
8. Press ↩ repeatedly to go back to the upper level menu.

5.11.6 Masking

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Keypads**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the keypad to be programmed by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Masking**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Press the key associated with the "MASKING" message ☑ on the display. Press ✓ to confirm;

   Enable ☑ : function enabled ; Enable ☐ : function NOT enabled ; Press ✓ to confirm;
8. Press ↩ repeatedly to go back to the upper level menu.

5.11.7 Name

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Keypads**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the keypad to be programmed by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Name**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Enter the desired name (max 24 characters). Press ✓ to confirm;
8. Press ↩ repeatedly to go back to the upper level menu.

5.11.8 Function key

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Keypads**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the keypad to be programmed by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Function key**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select "**Activate**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Press the key associated with the ACTIVATE message ◉ on the display to activate the function. Press ✓ to confirm;

   Output selected ◉ ; Output NOT selected ○
9. Press ↩ to return to the upper level menu.
10. Select "**Deactivate**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
11. Press the key associated with the DEACTIVATE message ○ on the display to deactivate the function. Press ✓ to confirm;

    Output selected ◉ ; Output NOT selected ○
12. Press ↩ to return to the upper level menu.
13. Select "**Emergency**" by pressing the key associated with the ∨ or ∧ symbol and press the key associated with the FUNCTION KEY message ◉ on the display. Press ✓ to confirm.
    Output selected ◉ - ; Output NOT selected ○
14. Select "**Anti thief**" by pressing the key associated with the ∨ or ∧ symbol and press the key associated with the FUNCTION KEY message ◉ on the display. Press ✓ to confirm.
    Output selected ◉ - ; Output NOT selected ○
15. Press ↩ repeatedly to go back to the upper level menu.

5.12 READER PROGRAMMING

5.12.1 LED management

The reader LEDs may be freely assigned to one or more system zones.

Different associations may be implemented for each reader but it is not possible to associate a same zone to several LEDs of the same reader.

The green LEDs display the associated zone status.

The LED shows anomalies (open inputs, alarms).

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

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

5.12.2 Programming procedure

Proceed as follows to program the readers:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Readers**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the reader to be programmed by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Zone assignment**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select the LED to which you want to assign the zone(s) by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Select the zone by pressing the key associated with the ∨ or ∧ symbol.
9. Press the key associated to the ASSIGNMENT message ☑ on the display.
   ASSIGNMENT ☑ : assigned zone ; ASSIGNMENT ☐: zone NOT assigned
   Press ✓ to confirm;
10. Press ↩ to return to the LED selection menu;
11. Repeat the procedure from step 7 to program the other LEDs, (it is not necessary that all LEDs are assigned to zones);
12. Press ↩ to return to the reader programming menu;
13. Select "**Masking**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
14. Press the key associated to the MASKING message ☑ on the display. Press ✓ to confirm;
    MASKING ☑ : assigned masking ; MASKING ☐: masking NOT assigned
15. Press ↩ to return to the reader programming menu;
16. Select "**Name**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
17. Enter the desired name (max 24 characters). Press ✓ to confirm;
18. Press ↩ repeatedly to go back to the upper level menu.

	**IMPORTANT**! Program all readers used in the system.

5.13 KEYS

The 1068A series system is able to manage the following number of electronic and proximity keys.

- up to 16 keys, 1068/005A control panel
- up to 32 keys, 1068/010A control panel

Moreover, each key may be individually enabled or disabled and provided with an identification name.

The key must be acquired, i.e. the control panel must read and store its univocal code, before configuring it.

5.13.1 Key acquisition

Proceed as follows to acquire an electronic or proximity key:

1. Access the **MASTER / INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Keys**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Acquire key**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the reader from which you want to acquire the key by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm; (The 3 green LEDs of the reader will flash and the keypad will display "ESC TO FINISH");
7. Insert the key you want to acquire or move it closer to the selected reader;
8. The address of the acquired key (e.g. KE01: Key 1) will be shown on the keypad display
9. Insert or move closer any other key to be acquired, the system will automatically increase the number of keys acquired;
10. Press ↩ to end the acquisition procedure;
11. Press ↩ repeatedly to go back to the upper level menu.

5.13.2 Key deletion

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

1. Access the **MASTER / INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Keys**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**How to delete a key**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the key you wish to delete by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. The message "**Are you sure?**" appears on the display. Press ✓ to confirm;
8. Press ↩ repeatedly to go back to the upper level menu.

5.13.3 Key configuration

The following parameters can be defined for each key:

- **Key type**, i.e. what the key controls. The possible options are:
  - **Access control**: any insertion switches the door opener output and the event is stored in the system log.
  - **Zone status**: the key is enabled for the normal monitoring functions of the intrusion alarm system (setting/unsetting).
  - **Zone status + Access control**: the key is enabled for both functions.
- **Zone assignment**, i.e. the zones are assigned to the key.
- **Name**, i.e. a descriptive name to easily identify the key on the system log and in messages.

Proceed as follows to configure an electronic or proximity key:

1. Access the **MASTER / INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Keys**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Key configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the key you wish to configure by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select "**Key function**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Press the key corresponding to the associated symbol ◉ / ○ of the desired customisation.
   - Access control ○
   - Zone status ◉
   - Zone status + Access control ○
9. Press ✓ to confirm.

10. Press ⮌ to return to the key configuration menu;
11. Select "**Zone assignment**" by pressing the key associated with the ⌄ or ⌃ symbol. Press ✓ to confirm.
12. Select the zone by pressing the key associated with the ⌄ or ⌃ symbol;
13. Press the key associated to the symbol ☐, in the box of the right column a confirmation sign ☑ will appear to indicate the assignment to the zone. Press ✓ to confirm;
14. Press ⮌ to return to the key configuration menu;
15. Select "**Name**" by pressing the key associated with the ⌄ or ⌃ symbol. Press ✓ to confirm;
16. Enter the desired name (max 24 characters). Press ✓ to confirm;
17. Press ⮌ repeatedly to go back to the upper level menu.

5.14 ADVANCED PROGRAMMING

EN50131

5.14.1 Remote control system code

The code which identifies the system must be set both in the 1068/005A and in the 1068/010A control panels in order to control it remotely using the 1068set app.

The code may be selected as required by the installer and must be eight digits long (factory value 99999999).

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

5.14.2 Programming procedure

Proceed as follows to program the remote control system code:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ⌄ or ⌃ symbol. Press ✓ to confirm;
3. Select "**Programming**" by pressing the key associated with the ⌄ or ⌃ symbol. Press ✓ to confirm;
4. Select "**System code**" by pressing the key associated with the ⌄ or ⌃ symbol. Press ✓ to confirm;
5. Edit the code (max. 8 digits). Press ✓ to confirm;
6. Press ⮌ repeatedly to go back to the upper level menu.

5.15 GENERAL SYSTEM PARAMETERS (TIMINGS)

The general system parameters are used to manage alarms and indications. Some of these parameters can be configured as shown in the table below:

Time	Description	Alarm / Event	Min	Max	Default
Intrusion alarm	Duration of output activation following an alarm or event.	Instantaneous input alarm. Delayed input alarm. Path input alarm. First entry/last exit input alarm. Anti thief function key or input alarm.	1s	1800s	30s Modo EN 60s Modo no EN
Pre-alarm alarm	Duration of output activation following an alarm or event.	Pre-alarm input alarm.	1s	1800s	30s
Tampering alarm	Duration of output activation following an alarm or event.	No Bus device communication alarm. Alarm for 24 h input opening (SAB) of control panel. BUS device tamper opening alarm. Jamming alarm on radio module/interface. Continuous collision alarm on BUS. Alarm upon reaching the number of invalid code entries. “Balanced” input unbalance or TAMPER customised input opening alarm.	1s	1800s	30s
Emergency alarm	Duration of output activation following an alarm or event.	Emergency function key or input alarm.	1s	1800s	30s
Pulsed commandable	Duration of activation of customised pulsed commandable outputs.		1s	255s	3s
Technological	Duration of the activation of the customised timed technological outputs.	Timed technological input event alarm.	1s	255s	3s
Courtesy light	Duration of activation of the outputs after the following alarms/events.	Courtesy light event alarm.	1s	255s	180s
Door opener	Duration of activation of the outputs after the following alarms/events.	Access control alarm. Door access alarm.	1s	15s	5s
Call delay	Waiting time between the occurrence of an event and the start of a phone call to notify it.		0s	30s	0s
And inputs	If two inputs are configured in AND: when one of them is opened, a timer starts whose duration is determined by this parameter; if the other input is opened before the timer elapses, then the opening event is generated for both of them		1min	15min	5min
Loss of mains	Waiting time between instantaneous power failure signalling and power failure signalling.		1min	255min	1min
GSM failure	Maximum waiting time and retry management towards the network before notifying a possible GSM/GPRS failure due to insufficient reception or no connection to the public network.		1min	255min	10min
GSM network connection	Maximum time for searching and connecting to the SIM provider's network.		1min	15min	2min
Time scheduler reminder event	Time with which the execution of the zone activation commands by the time scheduler is signalled in advance.		0min	30min	30min
Battery test	Time between two battery tests.		1h	24h	24h

5.15.1 Programming procedure Times and parameters

Proceed as follows to program the times and parameters:
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Times and parameters**" by pressing the key associated with the ∨ or ∧ symbol
   Press ✓ to display the available times and parameters.
   - Intrusion alarm >
   - Prealarm alarm >
   - Tamper alarm >
   - Emergency alarm >
   - Timed commandable >
   - Technological >
   - Courtesy light >
   - Door opener >
   - AND Inputs >
   - Loss of mains >
   - GSM failure >
   - GSM network connection >
   - Time scheduler reminder event >
   - Call delay >
   - Battery test >
   - Alarm count >
4. Select the customisation to be programmed by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm
5. The parameters with the symbol " > " allow you to set the minutes and/or seconds. Press ✓ to confirm;
6. Press ✓ to confirm, press ↩ to return to the upper level menu.

5.16 PHONE DIALER AND IP INTERFACE

EN50131

⚠	**IMPORTANT!** The information contained below implies that the 1068/005A or 1068/010A control panel is connected to at least one GSM phone network (via the 1068/458* module) and/or is connected to a local area network or the Internet (via the 1068/013 module).

(*) The 1068/458 module used with the 1068/010A control panel complies with the EN50131 Grade 2.

5.16.1 Alarm and event notifications

Refer to the User Manual.

5.16.2 Phone numbers and IP addresses

Refer to the User Manual.

5.16.3 Vocal messages

Proceed as follows to program **vocal message sending mode**:
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Vocal messages**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Message sending mode**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Press the key corresponding to the message MESSAGE SENDING MODE ◉ on the display
   MESSAGE SENDING MODE ◉ : selected ; MESSAGE SENDING MODE ○ : NOT selected
   - Detailed ○
   - Base ◉

   Press ✓ to confirm;
7. Press ↩ to return to the previous menu.

Proceed as follows to load the **vocal messages**:
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Vocal messages**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Load vocal messages**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. The message "**Are you sure?**" appears on the display. Press ✓ to confirm;
7. Press ↩ to return to the previous menu.

Proceed as follows to download the personal **vocal messages**:
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Vocal messages**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Download vocal messages**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. The message "**Are you sure?**" appears on the display. Press ✓ to confirm;
7. Press ↩ to return to the previous menu.

5.16.4 SMS text messages

Refer to the User Manual.

5.16.5 GSM parameters

5.16.5.1 GSM parameter programming procedure

Proceed as follows to enable the incoming **SMS** texts:
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**GSM parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Incoming SMS**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Press the key corresponding to the "ENABLE" message ☑ on the display.
   ENABLE ☑ : function enabled ; ENABLE ☐ function NOT enabled.
   Press ✓ to confirm.
7. Press ↩ to return to the previous menu.

Proceed as follows to modify the **SIM PIN**:
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**GSM parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**SIM Pin**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Enter the desired PIN (max 8 characters). Press ✓ to confirm;
7. Press ↩ to return to the previous menu.

5.16.6 GPRS parameters

5.16.6.1 GPRS parameter programming procedure

Proceed as follows to modify the **APN** (Access Point Name):
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**GPRS parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**APN**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Enter the desired name (max 24 characters). Press ✓ to confirm;
7. Press ↩ to return to the previous menu.

Proceed as follows to modify the **User**:
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**GPRS parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**User**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Enter the desired name (max 24 characters). Press ✓ to confirm;
7. Press ↩ to return to the previous menu.

Proceed as follows to modify the **Password**:
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**GPRS parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Password**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Enter the desired name (max 24 characters). Press ✓ to confirm;
7. Press ↩ to return to the previous menu.

Proceed as follows to modify the **DNS1** (Domain Name System):
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**GPRS parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**DNS1**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Enter the desired number. Press ✓ to confirm;
7. Press ↩ to return to the previous menu.

Proceed as follows to modify the **DNS2** (Domain Name System):
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**GPRS parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**DNS2**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Enter the desired number. Press ✓ to confirm;
7. Press ↩ to return to the previous menu.

5.16.7 GSM field test

The 1068/005A and 1068/010A control panels can periodically check the GSM field to ensure that the connection is fully functional. The presence of the GSM/GPRS field is monitored and sent to the central unit following a transmission request, or every 5 minutes. If no field is detected, the monitoring becomes continuous. If the absence lasts longer than a programmable time (10 minutes by default) the module failure condition is signalled.

5.16.8 IP parameters

5.16.8.1 Connection type

Proceed as follows to select the connection type:
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**IP parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Connection type**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the type of connection by pressing the key associated with the ∨ or ∧ symbol;
   - Acces point ◉
   - WiFi ○
   - Ethernet ○

   Connection type : ◉ selected ; Connection type : ○ NOT selected .
   Press ✓ to confirm;
7. Press ↩ to return to the previous menu.

5.16.8.2 Ethernet

5.16.8.2.1 Protocol type

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**IP parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Ethernet configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Protocol**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select the type of connection by pressing the key associated with the ∨ or ∧ symbol
   - DHCP ◉
   - Manual ○

   Connection type ◉ : selected ; Connection type ○ : NOT selected.
   Press ✓ to confirm;
8. Press ↩ to return to the previous menu.

5.16.8.2.2 Configuration

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**IP parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Ethernet configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select "**IP address**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Enter the desired address. Press ✓ to confirm;
9. Press ↩ to return to the previous menu.
10. Select "**Subnet mask**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
11. Enter the desired address. Press ✓ to confirm;
12. Press ↩ to return to the previous menu;
13. Select "**Gateway**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
14. Enter the desired address. Press ✓ to confirm;
15. Press ↩ to return to the previous menu;
16. Select "**DNS1**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
17. Enter the desired address. Press ✓ to confirm;
18. Press ↩ repeatedly to go back to the previous menu.

5.16.8.3 WiFi

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**IP parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**WiFi configuration**" by pressing the button associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**WiFi network name** " by pressing the button associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Enter SSID. Press ✓ to confirm;
8. Press ↩ to return to the previous menu.

Proceed as follows to enter the **Password**:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**IP parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**WiFi configuration**" by pressing the button associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Password**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Enter the desired password. Press ✓ to confirm;
8. Press ↩ to return to the previous menu.

Proceed as follows to enter the **protocol type** from IP parameters:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**IP parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**WiFi configuration**" by pressing the button associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.
7. Select "**Protocol**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Select the type of connection:
   - Auto ◉
   - Manual ○

   Connection type : ◉ selected ; Connection type : ○ NOT selected
   Press ✓ to confirm;
9. Press ↩ to return to the previous menu.

Proceed as follows to select **configuration type** from IP parameters:
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**IP parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**WiFi configuration**" by pressing the button associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Parameters**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select "**Configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Select "**IP address**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
9. Enter the desired address. Press ✓ to confirm;
10. Press ↩ to return to the previous menu;
11. Select "**Subnet mask**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
12. Enter the desired address. Press ✓ to confirm;
13. Press ↩ to return to the previous menu.
14. Select "**Gateway**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
15. Enter the desired address. Press ✓ to confirm;
16. Press ↩ to return to the previous menu;
17. Select "**DNS1**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
18. Enter the desired address. Press ✓ to confirm;
19. Press ↩ repeatedly to go back to the previous menu.

5.16.9 IDP protocol

For further information please refer to the paragraph "Alarm and event notifications" in the user manual.

5.16.9.1 IDP parameter programming procedure

Proceed as follows to enter the subscriber code:
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**IDP Protocol**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. "**Subscriber code**" is displayed. Press ✓ to confirm;
6. Enter the desired subscriber code. Press ✓ to confirm;
7. Press ↩ repeatedly to go back to the previous menu.

5.16.10 IDP/IP Protocol

For further information please refer to the paragraph "Alarm and event notifications" in the user manual.

5.16.10.1 IDP/IP parameter programming procedure

Proceed as follows to enter the subscriber code:
1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**IDP/IP Protocol**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Subscriber Code**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Enter the desired subscriber code. Press ✓ to confirm;
7. Press ↩ to return to the previous menu.
8. Select "**Receiver code**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
9. Enter the desired receiver code. Press ✓ to confirm;
10. Press ↩ to return to the previous menu;
11. Select "**System prefix**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
12. Enter the desired prefix. Press ✓ to confirm;
13. Press ↩ to return to the previous menu;
14. Select "**Cryptography**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
15. Select the cryptography type:
    - Not used ◉
    - 128 bit ○
    - 192 bit ○
    - 256 bit ○

    Cryptography type ◉ : selected ; Cryptography type ○ : NOT selected
    Press ✓ to confirm.
16. If 128, 192 or 256 bits are selected and ✓ is pressed to confirm, a string appears where it is possible to enter the desired cryptography code. Press ✓ to confirm.
17. Press ↩ to return to the previous menu.
18. Select "**Time stamp**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.
19. Press the key corresponding to the ENABLE message ☑ on the display.

    ENABLE ☑ : function enabled ; ENABLE ☐ function NOT enabled.
    Press ✓ to confirm.
20. Press ↩ repeatedly to go back to the previous menu.

5.16.11 Advanced

5.16.11.1 Advanced parameter programming procedure

Incoming rings (0 ÷ 8): If 0, the answering machine is disabled. Otherwise, it defines the number of rings it must receive before it can automatically answer incoming calls. It should be borne in mind that the voice-over function is always present and always enabled.

Proceed as follows to select the **Answering machine**:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Answering machine**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**GSM**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.
7. Select the type:
   - Disabled ◉
   - 1 ○
   - 2 ○
   - … ○
   - 8 ○

   GSM ◉ : selected ; GSM ○ : NOT selected
   Press ✓ to confirm.
8. Press ↩ to return to the previous menu.

Proceed as follows to select the **Call delay**:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Call delay**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Press the key corresponding to the CALL DELAY message ☑ on the display

   ENABLE ☑ : function enabled ; ENABLE ☐ function NOT enabled.
   Press ✓ to confirm.
7. Press ↩ to return to the previous menu.

	**IMPORTANT!** If the control panel is in a mode compliant with EN50131, if an intrusion alarm condition occurs during an entry time, any alarm notifications via vocal calls, SMS, calls to surveillance centres or PUSH notifications will be postponed by at least 30 seconds, or in any case until the end of the entry time, to allow deactivating the system. Under these conditions, the call delay will only have an effect if longer than 30 seconds. In all other circumstances, the call delay alone determines how long the notifications will be postponed with respect to the generation of the event.

Enabling/disabling: If the network is disabled even if there are phone numbers associated with the vector, no calls are made.

Proceed as follows to select **Enable network**:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Enable network**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the type:
   - IP interface ☐
   - GSM ☐
7. Press the key corresponding to the ENABLE NETWORK message ☑ on the display.

   ENABLE NETWORK ☑ : function enabled ; ENABLE NETWORK ☐ function NOT enabled.
   Press ✓ to confirm.
8. Press ↩ to return to the previous menu.

Module supervision: If disabled, the module is not supervised, otherwise, a lack of response to polling generates a tamper signalling.

Proceed as follows to select **Module supervision**:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Module Supervision**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the type:
   - IP interface ☐
   - GSM ☐
7. Press the key corresponding to the ENABLE NETWORK message ☑ on the display.

   MODULE SUPERVISION ☑ : function enabled ; MODULE SUPERVISION ☐ function NOT enabled.
8. Press ↩ repeatedly to go back to the previous menu.

EN50131

5.17 TIME SCHEDULER

5.17.1 Operating principles

The time scheduler can be used to automate repetitive operations, such as setting or unsetting a zone or a commandable output. Programming is on a weekly basis, i.e. the commands are repeated in the same way every week.

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

The automatic zones activation command is indicated in advance on the keypads (buzzer sounding and time scheduler icon in reverse). The advance is programmed under the “WARNING TIME” parameter.

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

The available time scheduler commands are:

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

IMPORTANT!

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

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

The hourly programming state (enabled or disabled) is shown on the keypad by the time scheduler icon.

The time scheduler commands remain active until the opposite command is imparted (by the time scheduler itself or by a user using the keypad or a reader): the scheduler sends commands but does not check system or output status.

Example of operation

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

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

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

5.17.2 Programming

Fill in the respective tables before starting to program the time scheduler (see paragraph *8.5 Time scheduler configuration*): your work will be enormously simplified.

IMPORTANT!
The time and date must be right for correct operation of the time scheduler (see paragraph *5.7 Date and time setting*).

The following parameters must be configured during programming:

- **Day Type**: set whether each day of the week (Monday, Tuesday… Sunday) must be considered as a working day, a pre-holiday or a holiday.
- **Command Type**: up to eight commands can be set for each day type (working day, pre-holiday or holiday).
- **Command N**: the time and action type is defined for each command.
- **Action**: there are three possibilities: no action, arm (enable) and disarm (disable). The actions can be applied to zones, outputs, users and keys.
- **Warning Time**: this determines how many minutes of warning must be given before the command is implemented. The warning time allows you to leave the area or to interrupt the automatic implementation of the command. Possible values are: from zero to 30 minutes, where zero means No warning.

5.17.2.1 Time scheduler programming procedure

Proceed as follows to program the time scheduler:

1. Access the **MASTER / INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Time scheduler**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Day Type**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the day you wish to program by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select the type (**Working day, Holiday, Pre-holiday**) by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Repeat the above procedure for all days;
9. Press ↩ to return to the upper level menu.
10. Select "**Command Type**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
11. Select the type (**Working day, Holiday, Pre-holiday**) by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
12. Select the command (e.g. **01: Command**) by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
13. Select "**Command Type**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
14. Select the function to be associated with ENABLE/DISABLE by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
15. Select the type of function to be associated by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm
    - KEYS
    - ZONES
    - OUTPUTS
    - USERS
16. Specify the parameters using the keys associated with the symbols ∨ or ∧ and select with the key associated to the symbol with the "AUTHORISATIONS" indication ☑. Press ✓ to confirm;
17. Select "**Command hour**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
18. Enter the programming time of the command using the alphanumeric keypad. Press ✓ to confirm;
19. Press ↩ repeatedly to go back to the main menu.

5.17.3 Deleting a command

To delete a command, follow the programming procedure and select "NO ACTION" for the command.

To block the entire programming, disable it without deleting it (see *User Manual*).

5.18 SYSTEM TEST

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

- Inputs
- Outputs
- Control panel battery
- Call or SMS
- Push notification sending
- GSM field
- Radio devices (see dedicated manual)
- IP interface
- Supplementary power supply battery (available only with 1068/010A control panel)

5.18.1 Input test

See User Manual.

5.18.2 Output test

See User Manual.

5.18.3 Control panel battery test

See User Manual.

5.18.4 Call or SMS test

See User Manual.

5.18.5 Push notification sending test

See User Manual.

5.18.6 GSM Field Test

See User Manual.

5.18.7 IP interface test

See User Manual.

5.18.8 Supplementary power supply battery test (available only with 1068/010A control panel)

See User Manual.

5.18.9 System diagnostics

There is a menu allowing the user to diagnose any operating problems on the control panel and to display in real time the following information:

- Voltage values of the control panel inputs
- Voltage value PS (Ref. 1061/515)
- Voltage value BAT
- Voltage value V1
- Voltage value V2
- Voltage value BUS
- Voltage value SAB
- Voltage value SR
- Control panel TAMPER status (Open/Closed)
- Status of jumper JP1 - JP2- JP3 - JP4 (Open/Closed - available only with 1068/010A control panel)

The values are updated whenever key ✓ is pressed.

Proceed as follows to diagnose the system:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance"** by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select **"Diagnostic"** by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the type of information to display by pressing the key associated with the ∨ or ∧ symbol.
   - CP 1-5 inputs
   - CP 6-10 inputs (available only with 1068/010A control panel)
   - CP voltage
   - Jumper (available only with 1068/010A control panel)
6. Select the desired type of information and press ✓ to confirm. The display shows the information found.
7. Press ↩ repeatedly to go back to the upper level menu.

5.18.10 Final tests

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

- Arm and disarm (total and partial) the system from the keypads, if present, using all the programmed user codes.
- Arm and disarm the system using readers and/or 1068/021, keypads, if present, using all the available keys.
- Test the remote functions of the system (if a dialler is installed) from a landline, a mobile phone or via modem (external assistance may be needed).

5.19 USER TRAINING

After having ascertained that the intrusion alarm system is working perfectly, you can demonstrate the operations to be carried out on the system to the end users. Proceed as follows to obtain the best training results:

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

The main instructions to be provided to users are:

- How to arm and disarm the system totally.
- How to arm and disarm the system partially.
- How to recognise the various indications: intrusion, tamper attempt, low battery etc. (on display and auditory indications).
- How to read the events stored on the control panel (System log and EN50131 Event log).
- How to enable remote control (if applicable).
- How to test the system periodically.

Delete the System Log and the EN50131 Event log at the end of all tests to hand over a clean system. See paragraph *7.6.4 How to delete the System Log,* for instructions on how to delete it.

6 PROGRAMMING WITH TABLET

This chapter illustrates how to program the system using a Tablet with Android 1068set App.

IMPORTANT! Depending on the cases, programming via tablet may not be EN50131 compliant.

6.1 PREREQUISITES

6.1.1 Tablet Requirements

The tablet must have at least the following configuration:

- Android 6 operating system or higher
- 10” screen or with larger dimensions
- 1920 x 1200 pixel 224 PPI resolution
- USB Port
- Micro SD card slot (recommended)

6.1.2 Enabling requirements

Proceed as follows for the programming through tablet:

- Enable remote access in advance (refer to the paragraph "Enabling remote access" in the User Manual);
- Enable the Installer (refer to the paragraph "Enabling the Installer" in the User Manual);
- In the APP, set the same *system code* and *installer code* used in the system;
- No connection to any keypad.

IMPORTANT! If you are using a keypad, you cannot access with the Installer App.

6.1.3 File types

The file types are identified by the extension. The type determines how data are recorded and the possible use.

Extension	Contents	Read and/or write	Use
.cfg	Programming, configuration and releases of control panel and various device software.	The file can be read and edited on tablet with the 1068set software. It can be retrieved from the control panel.	• To restore the configuration of a control panel. • To copy the configuration from one control panel to another. • To transfer the configuration prepared in advance in a laboratory to a control panel.
.cod	Code and key data (encrypted)	No	• To restore previously saved codes and keys on a control panel at any time. • To copy codes and keys from one control panel to another.
.sto	System Log data	The file can be read on tablet with the 1068set software.	Transfer and consultation of events stored by a control panel on a tablet.

6.1.4 Saving data on Micro SD card

Proceed as follows to save data on a Micro SD card:

1. Insert the Micro SD card into the SD CARD slot on the control panel board (see image *paragraph 3.4.1* - letter **N**);
2. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm.
3. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Maintenance"** by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Backup/Restoring**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Backup**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select "**Configuration**" or "**System log**" or "**Codes/Keys**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. The message "**Are you sure?**" appears on the display. Press ✓ to confirm;
9. The system will confirm the backup with a BEEP.
10. Press ↩ repeatedly to go back to the upper level menu.

	**IMPORTANT**! **Never remove the Micro SD card** or disconnect the control panel from the power supply while the red DL6 LED located on the 1068/005A and 1068/010A control panels mother board is blinking.

6.1.5 How to restore data on the control panel

Proceed as follows to restore data stored on the Micro SD card on the control panel:

1. Insert the Micro SD card into the SD CARD slot on the control panel board (see image *paragraph 3.4.1* - letter **N**);
2. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
3. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Maintenance"** by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Backup/Restoring**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Restoring**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select "**Configuration**" or "**Codes/Keys**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. The message "**Are you sure?**" appears on the display. Press ✓ to confirm;
9. The system will confirm the restoring with a BEEP.

*In case of "**Configuration**" restoring, the system resets and the keypad display returns to the home page.*

10. Press ↩ repeatedly to go back to the upper level menu.

	**IMPORTANT**! **Never remove the Micro SD card** or disconnect the control panel from the power supply while the red DL6 LED located on the 1068/005A and 1068/010A control panels mother board is blinking.

7 MAINTENANCE MENU

The maintenance operations which do not require to operate physically on the system are described in this chapter.

7.1 HOW TO VIEW DEVICE ADDRESSES

Proceed as follows to check the address of a given bus device in the system:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance"** by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Devices identification**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Keypads / Reader / Expansion / Radio expansions**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. The address of the selected device will appear on the keypad display;
7. Press ↩ repeatedly to go back to the upper level menu.

7.2 HOW TO VIEW THE FIRMWARE RELEASE OF DEVICES

Proceed as follows to read the firmware release of a bus device of the system or of the control panel itself:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance"** by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Firmware version**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Control panel / Keypad / Reader / Expansion / Radio expansions**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm. The firmware version of the selected device will appear on the keypad display.
6. Press ↩ repeatedly to go back to the upper level menu.

7.3 HOW TO UPGRADE BUS DEVICE FIRMWARE FROM MENU

The system allows updating the firmware:

- of the control panel
- of the connected optional modules (GSM/GPRS communicator, IP interface)
- of the connected bus devices (keypads, proximity key readers, expansions)

through a single system upgrade procedure.

The system upgrade procedure can be started:

- from the keypad menu
- from the Android 1068set App

The following paragraphs describe the procedure to be applied in the two modes.

	**IMPORTANT!** Firmware can only be upgraded if the Urmet Customer Care Centre has provided the necessary file and the accompanying technical notes.

7.3.1 Upgrade files

Regardless of the selected mode (from keypad or app), a dedicated file must be used to upgrade the system.

The upgrade files have the ".bin" extension and contain the individual firmware of all possible optional modules and upgradeable bus devices. Each firmware is identified by its own version.

The upgrade files have a name in the following format:

<system name>-V- system version>.bin

- System name identifies the system (example 1068-005A)
- -V- is a constant string
- System version is a 4-digit progressive code (values from 0 to 9999)

Before upgrading the system, it is advisable to save programming and configuration data (.cfg) and the file containing the codes and keys (.cod). The procedure is shown in paragraph *6.1.4 Saving data on Micro SD card*.

	**IMPORTANT!** The "*.bin" files are supplied by Urmet only. Do not edit or open the files in read mode for any reason: they are encrypted in a proprietary binary format and protected by check fields to preserve content. Do not download binary files from websites other than the Urmet official website (www.urmet.com).

7.3.2 Updating system firmware from keypad

To upgrade the system firmware from the keypad it is necessary to:

1. Download, from the installers' area of the official Urmet website (www.urmet.com), the .bin file for the system you want to upgrade (for example 1068/005A);
2. Save the downloaded file in the root folder of a micro SD card;
3. Access the maintenance area and open the tamper of the control panel;
4. Insert the micro SD card into the control panel;
5. Carry out the following procedure (leaving the control panel tamper open for the entire duration of the procedure).

Proceed as follows to upgrade the system firmware:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance”** by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Firmware upgrade**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. The display of the keypad shows the Firmware releases present on the SD card, select the desired one by pressing the key associated with the ∨ or ∧ symbol.
6. Press ✓ to start the upgrade;
7. The message “**Are you sure?**” appears on the display. Press ✓ to start the upgrade;
8. The control panel upgrades the Firmware. When finished, the keypad display returns to the Home page

IMPORTANT!

- The devices (including the control panel) which have already been upgraded to the relevant firmware release of the “.bin” files on the Micro SD card will not be affected by the upgrade procedure.
- Make sure all wired devices are connected and acquired.

The upgrade progress will appear on the keypad display after starting the procedure. The result will appear at the end of the procedure.

During the upgrade phase, which may take several minutes, the control panel controls the DL2, DL3, DL4 LEDs, turning them on one at a time (briefly) in sequence.

IMPORTANT! Do not remove the Micro SD card until the upgrade procedure is completed.

At the end of the upgrade the result can be:

- **Positive result**. The procedure was successful.

IMPORTANT! This message also appears if the procedure has never been started, because no device can be upgraded or the devices have the same firmware version as the upgrade file.

- **Negative result**. The procedure was interrupted or was not completed correctly.

IMPORTANT!

This indication will appear if one of the following errors occurs:

- The Micro SD card does not respond
- A file (.bin) was not found in the root folder
- Despite the automatic upgrade attempts all or some devices have not completed the procedure
- The devices which do not complete the upgrade successfully will no longer be used in the system until they are reprogrammed.

Details on the firmware upgrading procedure will be saved in the Event Log in both cases at the end of the operation.

7.3.3 System firmware upgrade from 1068set App

Proceed as follows to upgrade system firmware from app:

- download, from the installers' area of the official Urmet website (www.urmet.com), a *bin file for the system you wish to upgrade (for example 1068/005A).
- save the downloaded file in the root folder of a micro SD card or (if you do not have a micro SD card) in the internal memory of the mobile device on which the 1068set app is run.
- access the maintenance area and open the tamper of the control panel.

At this point, you can choose between two alternatives:

- If the upgrade file has been saved in the Micro SD card, the micro SD card must be inserted into the control panel and the 1068set app must only be used to start the upgrade procedure.
- If the upgrade file has been saved in the internal memory of the mobile device on which the 1068set app is running, the app must be used to download the file to the internal memory of the IP interface, installed on the control panel, before the upgrade procedure can be started.

The choice between the two alternatives is guided by the app's user interface.

In both cases, the tamper must be kept open for the entire duration of the upgrade procedure.

	**IMPORTANT!** The second alternative, the one to download the upgrade file to the internal memory of the IP interface, may take a few more minutes. For this reason, if possible, it is recommended to always use a micro SD card (first alternative).

	**IMPORTANT!** The devices (including the control panel) which have already been upgraded to the relevant firmware release of the ".bin" files on the Micro SD card, or in the IP interface internal memory, will not be affected by the upgrade procedure.

The upgrade progress will appear on the 1068set app interface after starting the procedure. The result will appear at the end of the procedure.

During the upgrade phase, which may take several minutes, the control panel controls the DL2, DL3, DL4 LEDs, turning them on one at a time (briefly) in sequence.

	**IMPORTANT! When using the micro SD card, do not remove it until the upgrade procedure is complete.**

At the end of the upgrade the result can be:

- **With positive result**. The procedure was successful.

	**IMPORTANT!** This indication will appear even if the procedure never started. No device can be upgraded or the devices have the same firmware version contained in the upgrade file.

- **With negative result**. The procedure was interrupted or is not OK.

	**IMPORTANT!** This indication will appear if one of the following errors occurs: ○ The Micro SD card or IP interface do not respond. ○ A file (.bin) was not found in the root folder of the micro SD card ○ Despite the automatic upgrade attempts all or some devices have not completed the procedure ○ The devices which do not complete the upgrade successfully will no longer be used in the system until they are reprogrammed.

Details on the firmware upgrading procedure will be saved in the Event Log in both cases at the end of the operation.

7.4 RESET DEFAULT

The reset default sets the programming parameters of all devices in the system, including the control panel, to default.

The codes, keys and logs are not deleted.

Proceed as follows to carry out the partial reset

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance"** by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Reset Default**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. The message "**Are you sure?**" appears on the display of the keypad; Press ✓ to start the reset.
6. Press ↩ repeatedly to go back to the upper level menu.

7.5 RESET FACTORY SETTINGS

The reset factory settings procedure sets the control panel programming parameters to factory settings (inputs, outputs, times, zones, time scheduler, GSM parameters) and eliminates all previously acquired devices. The respective configurations are set to factory settings and the addresses are deleted.

Proceed as follows to carry out the global reset:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance"** by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Reset factory settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. The message "**Are you sure?**" appears on the display. Press ✓ to start the reset;
6. At the end, the control panel restarts, resetting the factory settings.

7.6 SYSTEM LOG

1068/005A Control panel

The System Log stores the last 500 events (setting, unsetting, alarm, tamper etc.) which concerned the system.

The events are stored from the most recent to the oldest, i.e. the most recent event is the one with the lowest identification number. The stored events move down by one position as a new event is added.

When the System Log reaches the maximum size (500 events), each new event will be written over the oldest stored event.

The System Log may be examined by the Master user and by the other users but may only be deleted by the Installer.

1068/010A Control panel

The System Log stores the last 1000 events (setting, unsetting, alarm, tamper etc.) which concerned the system.

The events are stored from the most recent to the oldest, i.e. the most recent event is the one with the lowest identification number. The stored events move down by one position as a new event is added.

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

The System Log may be examined by the Master user and by the other users but may only be deleted by the Installer.

The EN50131 Event log stores the last 500 events (tamper, failures, etc.) which concerned the system.

The events are stored from the most recent to the oldest, i.e. the most recent event is the one with the lowest identification number. The stored events move down by one position as a new event is added.

When the EN50131 Event log reaches the maximum size (500 events), each new event will be written over the oldest stored event.

The EN50131 Event log can be examined only by the Installer in the maintenance menu.

IMPORTANT!

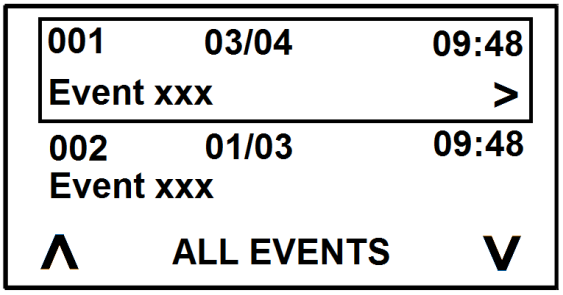
A user can only see the events related to the pertinent zones, i.e. the assigned zones.

The Master user is assigned to all zones and can always see all stored events.

Only the Installer user will be able to see technical events, such as faults and tampering.

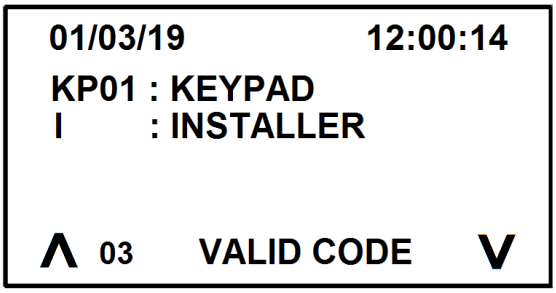
7.6.1 How to interpret viewed data

Event information is stored on the event Log and displayed as follows:



where:

- **001:** is the number of the event (001 is the most recent event, 500 is the oldest).
- **03/04:** is the date of the event.
- **09:48:** hours and minutes of the event.
- **Event xxx:** this is the type of occurred event.



where:

- **01/03/19:** it is the day, month and year of the event;
- **12:00:14:** hours, minutes and seconds of the event.
- **KP01: KEYPAD / I: INSTALLER:** detail of the individual event that occurred.

7.6.2 How to browse the System Log

Proceed as follows to browse the System Log:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**System log**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Read event log**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**All events**" by pressing the key associated with the ∨ or ∧ symbol; Press ✓ to confirm;
6. Select the event of which you want to have details by pressing the key associated with the ∨ or ∧ symbol.
7. Press ✓ to view details about the event;
8. Press ↩ repeatedly to go back to the upper level menu.
9. Select "**Event filter**" by pressing the key associated with the ∨ or ∧ symbol; Press ✓ to confirm.
10. Press the key associated with the ∨ or ∧ symbol to display the events according to the date or type of event;
11. Select the event of which you want to have details by pressing the key associated with the ∨ or ∧ symbol;
12. Press ✓ to view details about the event;
13. Press ↩ repeatedly to go back to the upper level menu.

7.6.3 How to browse the EN50131 Event log (available only with 1068/010A control panel)

Proceed as follows to browse the EN50131 Event log:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**EN50131 Event log**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Read event log**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**All events**" by pressing the key associated with the ∨ or ∧ symbol; Press ✓ to confirm;
7. Select the event of which you want to have details by pressing the key associated with the ∨ or ∧ symbol;
8. Press ✓ to view details about the event;
9. Press ↩ repeatedly to go back to the upper level menu;
10. Select "**Event filter**" by pressing the key associated with the ∨ or ∧ symbol; Press ✓ to confirm.
11. Press the key associated with the ∨ or ∧ symbol to display the events according to the date or type of event;
12. Select the event of which you want to have details by pressing the key associated with the ∨ or ∧ symbol;
13. Press ✓ to view details about the event;
14. Press ↩ repeatedly to go back to the upper level menu.

7.6.4 How to delete the System Log

IMPORTANT! The deletion operation cannot be undone.

Proceed as follows to delete the System Log:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**System log**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Erase event log**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. The message "**Are you sure?**" appears on the display. Press ✓ to confirm;
6. Press ↩ repeatedly to go back to the upper level menu.

7.6.5 How to delete the EN50131 Event log (available only with 1068/010A control panel)

IMPORTANT!
According to the provisions of the EN50131 standard, the "EN50131 Event log" cannot be deleted, but only consulted.

8 TABLES

8.1 VOCAL ALARM MESSAGES AND SMS

The following tables show all pre-recorded and unrecorded vocal messages for the expected events. These messages will be used when sending vocal messages and SMS.

You can customise them using the 1068set APP.

The maximum length of a message is 5 seconds.

Message	**Created for…**
HOLD UP	Introduction of hold-up code or input opening.
Intrusion	Intrusion input opening.
Pre-alarm	Pre-alarm input opening.
Set zones	Activation of one or more zones.
Unset zones	Deactivation of one or more zones.
Tampering	• Tamper input opening • Balanced / Double balanced input imbalance • Device tampering
Wrong code	Entry of invalid code or key for 21 times.
Emergency	Opening of the emergency input or use of the function key.
Fault start	Fault start.
Fault end	Fault end.
Loss of mains	Continuous lack of power network start.
Mains restored	Power network restored for at least 5 minutes.
Maintenance start	Start of maintenance.
Maintenance end	End of maintenance
Isolation/inhibition start	Start of an input isolation or inhibition.
Isolation/inhibition end	End of an input isolation or inhibition.
Battery fault start	Start of battery fault event.
Battery fault end	End of battery fault event.
Technological	Opening of a customised technological input.
SIM expiration date	SIM expiry date reached.
Fire *(available only whith 1068/010A control panel)*	Opening fire input.
Communicator failure *(available only whith 1068/010A control panel)*	Opening external communicator fault input.
Test message	Sending a test message.

Table 9 - Vocal messages and SMS for 1068/005A and 1068/010A control panel

8.2 ALARM SENDING TYPES

One or more sending modes can be selected according to the alarm type to be sent.

1068/005A Control panel

Event	Sending priority	Transmission mode				
		Vocal	IDP	IDP/IP	SMS	PUSH notification
Hold UP	0	■	■	■	■	■
Intrusion alarm	1	■	■	■	■	■
Pre-alarm	2	■	■	■	■	■
Zones activation/deactivation	3	■	■	■	■	■
Tampering	4	■	■	■	■	■
Wrong code	5	■	■	■	■	■
Emergency	6	■	■	■	■	■
Fault	7	■	■	■	■	■
Lack of mains/mains restored	8	■	■	■	■	■
Battery fault	9	■	■	■	■	■
Maintenance	10	■	■	■	■	■
Input isolation/inhibition	11	■	■	■	■	■
Technological event	12	■	■	■	■	■
SIM expiration date	13	■			■	■

1068/010A Control panel

Event	Sending priority	Transmission mode				
		Vocal	IDP	IDP/IP	SMS	PUSH notification
Hold UP	0	■	■	■	■	■
Fire	1	■	■	■	■	■
Intrusion alarm	2	■	■	■	■	■
Pre-alarm	3	■	■	■	■	■
Zones activation/deactivation	4	■	■	■	■	■
Tampering	5	■	■	■	■	■
Wrong code	6	■	■	■	■	■
Emergency	7	■	■	■	■	■
Fault	8	■	■	■	■	■
Lack of mains/mains restored	9	■	■	■	■	■
Battery fault	10	■	■	■	■	■
Maintenance	11	■	■	■	■	■
Input isolation/inhibition	12	■	■	■	■	■
Technological event	13	■	■	■	■	■
SIM expiration date	14	■			■	■

Multiple, simultaneous alarms will be send in order of priority (0 = maximum priority, 14 = minimum priority).

Table 10 - Alarm sending types

8.3 REMOTE CONTROL FUNCTIONS

These functions can be used by a supervisory institute to receive information from the control panel on dedicated equipment (analogue or digital numerical control panels) using analogue numerical protocols (IDP) or in digital mode via TCP/IP (IDP-IP).

The available functions are as follows:

- Sending of start and end events/alarms
- Sending of cyclical test calls

Below is a table associating events / alarms with the sent codes:

A	A	A	A	1	8	Q	E	E	E	G	G	C	C	C	S
Subscriber Code				FIXED		Qualification	Event			Group		Code or input ID			Cks

Where:

Block	Code	Description
Subscriber Code	xxxx	These are the last four digits of the subscriber code
Qualification	1	This indicates the beginning of an event or deactivation
	3	This indicates the end of an event or activation
Event	100	Emergency alarm from input. The input can be of control panel, expansion, keypad, reader or radio device. CCC indicates the logical number of the input.
	101	Emergency alarm from function key on wired keypad, wireless keypad or radio remote control. CCC indicates the device identification.
	110	Fire alarm from input (available only with 1068/010A control panel). CCC indicates the logical number of the input.
	120	Anti theft alarm from input. The input can be of control panel, expansion, keypad, reader or radio device. CCC indicates the logical number of the input.
	121	Hold-up alarm from input. CCC indicates the input.
	123	Anti theft alarm from function key on wired keypad, wireless keypad or radio remote control. CCC indicates the device identification.
	124	Hold-up alarm from code. CCC indicates the device.
	130	Intrusion alarm from any intrusion input customisation. CCC indicates the logical number of the input.
	137	Input tamper alarm. CCC indicates the logical number of the input.
	138	Input pre-alarm. CCC indicates the logical number of the input.
	145	Tamper alarm or control panel and/or peripheral wired Sab input. CCC indicates the device identification
	150	Input technological sustained event. CCC indicates the logical number of the input.
	151	Input timed technological event. CCC indicates the logical number of the input.
	301	Protracted loss of mains alarm. CCC at 0
	302	Battery fault. CCC indicates the device identification.
	307	Power supply failure alarm (+PS, +V1, +V2, +VBUS, +SR). CCC at 0.
	320	Input sirens failure. CCC indicates the logical number of the input.
	330	Control panel bus communication to wired peripheral device error alarm. CCC indicates the device identification.
	333	Peripheral device configuration failure. CCC always 0.
	343	Radio module/inteface failure. CCC always 0.
	344	Jamming alarm. CCC always 0.
	350	Communicator failure alarm (available only with 1068/010A control panel). CCC indicates the logical number of the input.
	353	IP interface failure alarm. CCC always 0.
	354	GSM telephone failure alarm. CCC always 0
	355	No supervision alarm (only with at least one radio module/inteface with devices). CCC indicates the device identification.

	380	Input detector failure. CCC indicates the logical number of the input.
	383	Radio tamper. CCC indicates the device identification.
	400	Setting/Unsetting from key. CCC indicates the key.
	401	Setting/unsetting from user code. CCC indicates the user.
	403	Setting/unsetting from Time Scheduler. CCC always 0.
	407	Setting/unsetting from remote with DTMF code or App. CCC indicates the user.
	408	Quick setting/unsetting from remote control. CCC indicates 99
	409	Setting/unsetting from key input. CCC indicates the logical number of the input.
	450	Forced setting. CCC indicates the user ID.
	454	EN zone setting not performed (activation lock). CCC indicates the device.
	458	Maintenance (installer working on site). CCC always 0.
	461	Wrong code alarm. CCC indicates the device identification.
	570	Input isolation. CCC indicates the logical number of the input.
	573	Input inhibition. CCC indicates the logical number of the input.
	601	Manual test call. CCC always 0.
	602	Cyclic test call. CCC always 0.
Group	00	The event refers to the entire system.
	01 ÷ 16	The event refers to zones 1 - 16.

Identification of user, key, input or device in the CCC field

Using the CCC Field	**Code**	**Description**
To identify a user	000	Event generated by the installer code
	001	Event generated by the technical manager code
	002	Event generated by the master code
	003 ÷ 018	Event generated by the user code 1-16
To identify a key	001 ÷ 016	Event generated by key 1-16
To identify an input	001 ÷ 021	Event generated by logic number input 1-21
To identify a device	000	Event generated by the control panel
	010	Event generated by the GSM module
	030	Event generated by IP interface
	040	Event generated by radio module/inteface
	060	Event generated by app
	101 ÷ 108	Event generated by the wired keypad 1-8
	201 ÷ 208	Event generated by the radio remote control 1-8
	301 ÷ 308	Event generated by reader 1-8
	401 ÷ 402	Event generated by expansion 1-2
	501 ÷ 528	Event generated by magnetic contact (DC) 1-28
	601 ÷ 628	Event generated by IR detector 1-28
	701 ÷ 704	Event generated by the wireless keypad 1-4
	801 ÷ 804	Event generated by the radio siren 1-4
Other uses	99	Setting event or prevention of setting without code
	000	Setting event or prevention of setting by time scheduler

8.4 FACTORY SETTINGS

8.4.1 System code

System code (for android 1068set App)	**99999999**

8.4.2 Zones

Zones number	**1**
Type of setting (No EN compliant mode)	**Standard**
Type of setting (EN compliant mode)	**Prevention of setting**

8.4.3 Users

1068/005A	1068/010A	Default	Name	Enabled	Assigned zones
Installer	**Installer**	0000	**Installer**	Power ON	SYSTEM
Tech. Manager	**Tech. Manager**	2222	**Tech. Manager**	Power ON	SYSTEM
Master	**Master**	1111	**Master**	Always	SYSTEM
User 1	**User 1**	0010	**…**	NO	1
User 2	**User 2**	0020	**…**	NO	1
User …	**User …**	0….	**…**	NO	1
User 16	**User …**	0160	**…**	NO	1
	User 32	0320	**…**	NO	1

1068/005A	1068/010A	Default
Hold UP	**Hold UP**	Disabled

8.4.4 Keys

1068/005A	Name	1068/010A	Name	Default	Type	Enabled (if acquired)	Assigned zones
Key 1	KE01: Key 1	**Key 1**	KE01: Key 1	Not present	Zone Status	X	Those enabled in the system
Key ...	…	**Key …**	…	Not present	Zone Status	X	Those enabled in the system
Key 16	KE16: Key 16	**Key 32**	KE32: Key 32	Not present	Zone Status	X	Those enabled in the system

8.4.5 General parameters and Times

Parameter	Default
Intrusion alarm time [EN compliant mode]	30 s
Intrusion alarm time [No EN compliant Mode]	60 s
Pre-alarm time	30 s
Tamper alarm time	30 s
Emergency time	30 s
Pulsed Commandable Time	3 s
Timed Technological Time	3 s
Courtesy light time	180 s
Door opener time	5 s
Call delay time	0 s
And inputs time	5 min
Loss of mains	1 min
Alarm count	10
GSM failure time	10 min
GSM network connection time	2 min
Time scheduler notice time	30 min
Battery test time	24 h

8.4.6 Control panel inputs

1068/005A Control panel

Attrib.	Isolable	YES				
	Assignment type	OR				
Zones assignment		1	1	1	1	1
Customisation [EN compliant mode]		First Entry/ Last Exit	Path	Immediate	Fault Detectors	Fault Sirens
Customisation [No EN compliant mode]		First Entry/ Last Exit	Immediate	Immediate	Immediate	Immediate
Type [EN compliant mode]		D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.
Type [No EN compliant mode]		NC	NC	NC	NC	NC
Name		…	…	…	…	…
Physical address		In1	In2	In3	In4	In5

1068/010A Control panel

Attrib.										
	Isolable	YES								
	Assign. type	OR								
Zones assignment		1	1	1	1	1	1	**1**	1	1	1
Customisation [EN compliant mode]		First Entry/ Last Exit	Path	Immediate	Fault Detectors	Fault Sirens	Immediate	Immediate	Immediate	Immediate	Immediate
Customisation [No EN compliant mode]		First Entry/ Last Exit	Immediate	Immediate	Immediate	Immediate	Immediate	Immediate	Immediate	Immediate	Immediate
Type [EN compliant mode]		D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.	D. Bal.
Type [No EN compliant mode]		N.C.	N.C.	N.C.	N.C.	N.C.	N.C.	N.C.	N.C.	N.C.	N.C.
Name		**…**	**…**	**…**	**…**	**…**	**…**	**…**	**…**	**…**	**…**
Physical address		In1	In2	In3	In4	In5	In6	In7	In8	In9	In10

8.4.7 Control panel outputs

1068/005A Control panel

Zones assignment	SYSTEM	SYSTEM	SYSTEM	SYSTEM
Customisation	Intrusion / Tamper	Intrusion / Tamper	Intrusion [No EN compliant mode] / Faults [EN compliant mode]	Zone status
Type	N.H.	N.H.	N.L.	N.H.
Name	**…**	**…**	**…**	**…**
Physical address	O1	O2	O3	O4

1068/010A Control panel

Zones assignment	SYSTEM	SYSTEM	SYSTEM	SYSTEM	SYSTEM	SYSTEM	SYSTEM
Customisation	Intrusion / Tamper	Intrusion / Tamper	Intrusion [No EN compliant mode] / Faults [EN compliant Mode]	Zone status	Intrusion	Intrusion	Intrusion
Type	N.H.	N.H.	N.L.	N.H.	N.H.	N.H.	N.H.
Name	**…**	**…**	**…**	**…**	**…**	**…**	**…**
Physical address	O1	O2	O3	O4	O5	O6	O7

8.4.8 Expansion module inputs

Attrib.	Isolable	YES							
	Assignment type	OR							
Zone assignment		1	1	1	1	1	1	1	1
Customisation		Immediate	Immediate	Immediate	Immediate	Immediate	Immediate	Immediate	Immediate
Type		N.C.	N.C.	N.C.	N.C.	N.C.	N.C.	N.C.	N.C.
Name		…	…	…	…	…	…	…	…
Physical address		In1	In2	In3	In4	In5	In6	In7	In8

8.4.9 Expansion outputs

Zones assignment	SYSTEM	SYSTEM	SYSTEM
Customisation	Intrusion	Intrusion	Intrusion
Type	N.L.	N.L.	N.L.
Name	…	…	…
Physical address	O1	O2	O3

8.4.10 Keypad inputs

Attrib.	Isolable	YES
	Assignment type	OR
Zone assignment		All
Customisation		Immediate
Type		Not used
Name		…
Physical address		In1

8.4.11 Radio module/interface inputs

For further details and information, refer to the dedicated manual.

8.4.12 Radio module/interface outputs (sirens)

For further details and information, refer to the dedicated manual.

8.4.13 Reader inputs

Attrib.	Isolable	YES	
	Assignment type	OR	
Zone assignment		System	System
Customisation		Immediate	Immediate
Type		Not used	Not used
Name		…	…
Physical address		In1	In2

8.4.14 Keypad parameters

Keypads	Assigned zones	Name	Exit time	Entry time
Keypad 1	System	…	NO	NO
Keypad …	System	…	NO	NO
Keypad 8	System	…	NO	NO

8.4.15 Reader- zones assignment

Readers	Name	LED 1 Assigned zones	LED 2 Assigned zones	LED 3 Assigned zones	Masking
Reader 1	…	1	---	---	Disabled
Reader …	…	1	---	---	Disabled
Reader 8	…	1	---	---	Disabled

8.4.16 Assignment of radio remote control keys

KEYS	ZONE	FUNCTION
Key 1	System	Set zones
Key 2	Not used	Not used
Key 3	Zone [1]	Partial setting
Key 4	System	Unsetting zones

8.4.17 Communicator parameters

Event	Hold UP	
	Instrusion	
	Pre-alarm	
	Zones On/Off	
	Tampering	
	Wrong code	
	Emergency	
	Fault start	
	Fault end	
	Loss of mains	
	Mains restored	
	Maintenance start	
	Maintenance end	
	Isolation/inhibition start	
	Isolation/inhibition end	
	Battery fault start	
	Battery fault end	
	Technologicals	
	SIM expiration date	
	Test message	
Sending type		Vocal
Telephone line		GSM
Zones assignment		SYSTEM

PARAMETER			**DEFAULT**
Vocal message sending mode			Base
GSM parameter	SIM PIN		
	SIM expiration date		01/2020
	Incoming SMS		Disabled
IP parameter	Ethernet		DHCP
	Connection type		Access point
	WiFi		DHCP
Periodical communication test			Disabled
Advanced	Answer Machine	GSM	Disabled
	IDP subscriber code - IDP/IP		Empty
	Call delay		Disabled
	Line enabling	GSM	Disabled
		IP	Enabled
	Sending mode		Base

8.4.18 Time scheduler

The time scheduler is deactivated by default.

8.5 TIME SCHEDULER CONFIGURATION

	Days						
Type	**Monday**	**Tuesday**	**Wednesday**	**Thursday**	**Friday**	**Saturday**	**Sunday**
Working day							
Pre-holiday							
Holiday							

Note: *only one type may be selected for each day.*

WORKING DAY COMMANDS		
Number	**Time**	**Type**
1	:	
2	:	
3	:	
4	:	
5	:	
6	:	
7	:	
8	:	
9	:	
10	:	
11	:	
12	:	
13	:	
14	:	
15	:	
16	:	

PRE-HOLIDAY DAY COMMANDS		
Type	**Time**	**Type**
1	:	
2	:	
3	:	
4	:	
5	:	
6	:	
7	:	
8	:	
9	:	
10	:	
11	:	
12	:	
13	:	
14	:	
15	:	
16	:	

HOLIDAY COMMANDS		
Number	**Time**	**Type**
1	:	
2	:	
3	:	
4	:	
5	:	
6	:	
7	:	
8	:	
9	:	
10	:	
11	:	
12	:	
13	:	
14	:	
15	:	
16	:	

9 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.

9.1 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 phase:

- They are OFF and therefore do not switch the following outputs O customisations:
  - INTRUSION
  - PRE-ALARM
  - TAMPER
  - INTRUSION_PRE-ALARM
  - INTRUSION_TAMPER
  - INTRUSION_TAMPER_PRE-AL
  - SYSTEM FAILURE
  - DETECTOR FAILURE
  - SIREN FAILURE
  - SYSTEM_DETECTOR_SIREN FAILURE
  - LOW BATTERY
  - FIRE (available only with 1068/010A control panel)
- All other output customisations remain unchanged when starting maintenance and can switch normally during maintenance;
- The phone dialer cannot forward calls, except for service calls.
  - Test calls
  - Low battery
  - Loss of mains
  - SIM expiration date
- The system cannot be activated
- The event log is not affected, i.e. all events that occur will continue to be logged.

9.1.1 Maintenance mode access

Maintenance mode is accessed if one of the following conditions occurs:

- The control panel tamper is opened when the installer has logged in (on the keypad or on the 1068set android App);
- The installer accesses the maintenance menu from the keypad;
- All the zones of the system are activated (an operation that is also allowed through APP), then all the zones are deactivated within 10 seconds, then the control panel tamper is opened within 10 minutes.
- Press the dedicated button on the "Maintenance" page of the 1068set App.

The maintenance status is indicated by:

- The turning on of the tamper icon on the home page of the keypads (only if the tamper is opened);
- The turning on of the DL3 LED in the control panel and the warning LEDs (yellow) on the keypad (only if the tamper is opened);
- The turning on of the maintenance icon on the home page of the keypads;
- The fast blinking of the RUN LED of the control panel.

When accessing maintenance mode:

- All the outputs indicated in the previous paragraph are deactivated;
- The memories of all inputs (alarm and tamper memories) and of all devices are reset to zero: fault memories (modules and power supplies), communication failure, tampering and jamming, so that the technician only views the actual status of any fault on the keypad;
- Any call cycles in progress are interrupted;
- The Event Log records the “start of maintenance”;
- The maintenance event (start), if scheduled, is sent via communicators.

9.1.2 End of maintenance

If you have started maintenance without opening the tamper, you can end it by doing one of the following actions:

- Exit the keypad maintenance menu
- Installer logout from keypad or 1068set App
- Dedicated key in the "Maintenance" page of the 1068set App

If you are in maintenance with at least one tamper open, you must close them all.

- As soon as all tampers are closed:
  - The tamper icon on the keypad home page turns off;
  - The DL3 LED in the control panel and the warning LEDs (yellow) on the keypads turn off;
  - The run LED will keep blinking fast;
  - The maintenance icon on the keypad home page remains on;
  - A 10-second timer is activated.
- After the 10 seconds:
  - An Installer logged on to the keypad or 1068set App is automatically redirected to the home page;
  - A connection to the control panel with 1068set App is automatically interrupted;
  - The system quits the maintenance mode;
  - The run LED stops blinking quickly;
  - The maintenance icon on the keypad home page turns off;
  - The maintenance event (end), if scheduled, is sent via communicators.

If the control panel tamper is reopened within 10 seconds, then the initial condition of permanent maintenance is restored.

When you quit the maintenance status:

- All those outputs that were deactivated and inhibited are re-piloted in a manner consistent with the current status of failures and tampering;
- After comparison with the status before the maintenance start, signals are sent through the communicators (if a failure or tampering WAS NOT already present at the start of maintenance, alarm events must be sent to the communicator, vice versa, if a fault is PRESENT when you start maintenance and it is no longer present when you end the maintenance, the end of fault events must be sent to the COMMUNICATOR).

9.2 ADDING A NEW BUS DEVICE

9.2.1 Procedure for acquiring bus devices (expansions, readers and radio interfaces)

	**IMPORTANT!** The instructions below assume that the devices have not yet been acquired. Otherwise, see paragraph *9.13.7 Wired device hardware reset.*

To acquire a new expansion device or reader, from keypad (acquired or of service), follow the instructions below:

1. If the device is already connected to the BUS, go directly to step 4, otherwise turn off the system completely;
2. Connect the new device to the bus and power the system;
3. The yellow LED of the new device blink slowly for about 10 second before changing the speed of blinking;
4. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm.
5. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select "**Acquisition**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. "ESC TO FINISH…" will appear on the display; press the programming button of the device to acquire it; its yellow LED will turn off;
9. The address assigned to the device will appear on the keypad display during assignment
10. Repeat step 8 on all devices to be acquired;
11. Press ↩ to return to the upper level menu.

To acquire an expansion device or reader, it must not already have an address in its memory.

To reset the address of a device you need to:

- Delete it from the appropriate keypad menu

or

- Use the "reset" procedure (paragraph *9.13.7 Wired device hardware reset).*

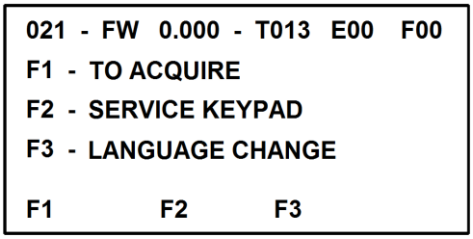
 It is now possible to configure the system.

	**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.

9.2.2 Keypad acquisition

To acquire a new keypad (from another acquired or service keypad), proceed as follows:

1. If the device is already connected to the BUS, go directly to step 4, otherwise turn off the system completely;
2. Connect the keypad to the bus and power the system;
3. Wait for the just connected keypad to display.



4. Press the key associated with the **F1** symbol on the keypad;
5. Enter the **INSTALLER** menu by entering the access code. Press to confirm;
6. Select "**System Settings**" by pressing the key associated with the or symbol. Press to confirm;
7. Select "**Maintenance**" by pressing the key associated with the or symbol. Press to confirm;
8. Select "**Acquisition**" by pressing the key associated with the or symbol. Press to confirm.
   "ESC TO FINISH" appears on the display.
9. Press the key associated with the **F1** symbol on the keypad;
10. Repeat step 8 on all keypads to be acquired;
11. Press to return to the upper level menu.

The keypad must not already have an address in its memory in order to be acquired.

To reset the address of a keypad:

- Delete it from the menu of another keypad;

or

- Use the "Reset" procedure.

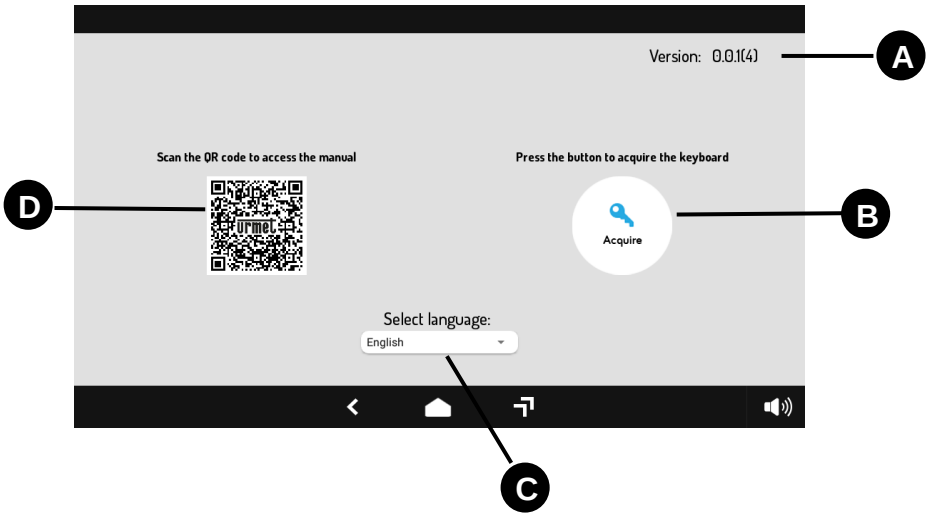
9.2.3 Touch keypad acquisition

Following the installation of the device or in the case of a reset to the factory parameters, the touch keypad will be in acquisition mode.

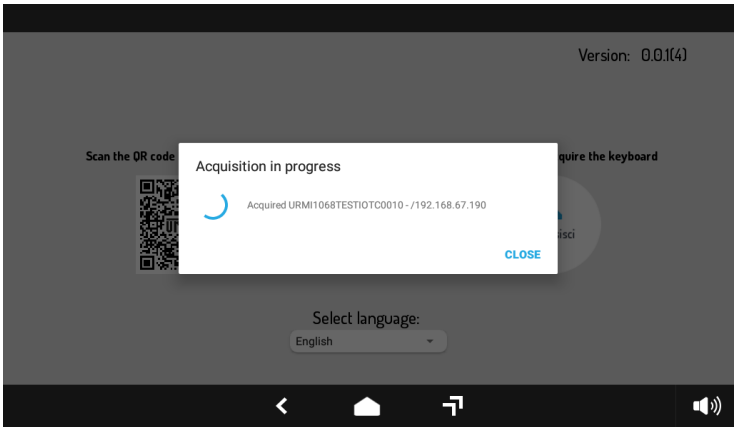
This screen will allow you to acquire an available control panel.

As below screenshot shown, the acquisition screen will present the following main components:

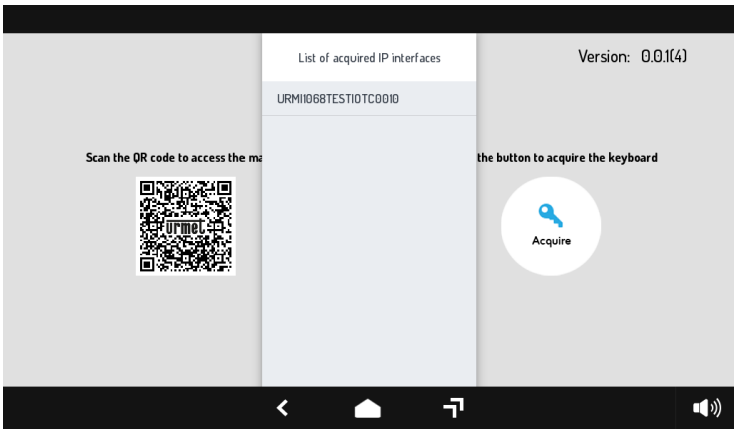
A. Current firmware version.
B. Key used to start the acquisition procedure.
C. Selectable drop-down that allows you to change the interface language (Italian, English, French or German).
D. QR code that allows the installer to access the product data sheet on the Urmet website, to then be able to select and download the document (Installation / Programming Manual) directly on his device.



Pressing the "**Acquire"** key will start the search in order to identify any systems present in the network.

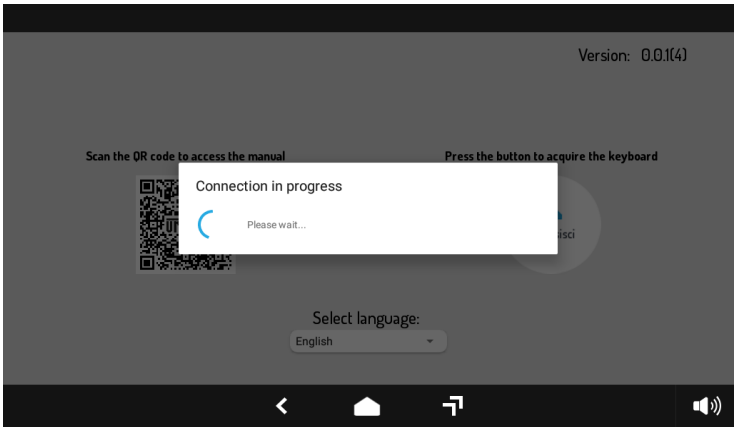


By pressing the "**CLOSE**" key, the list of identified interfaces will be displayed.

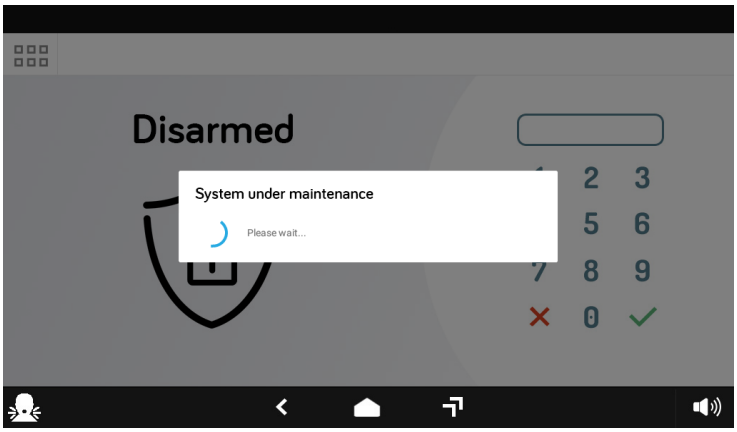


To acquire the touch keypad on the control panel it is necessary to set the control panel in Maintenance mode.
Then, select the interface you want to connect to from the keypad.
In this way, the keypad will communicate with the control panel and carry out the acquisition.

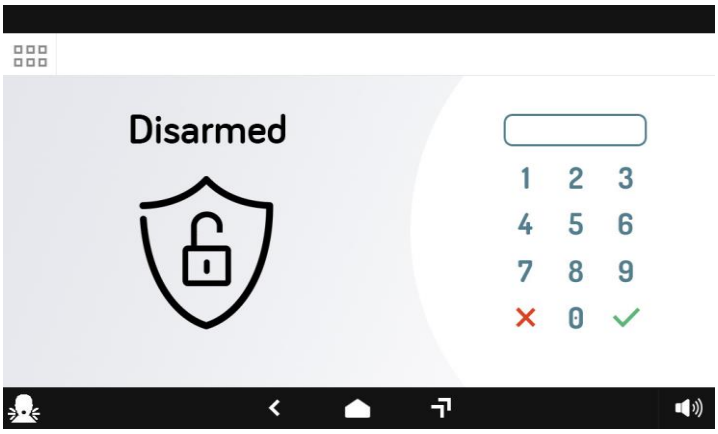
	IMPORTANT! For the operation of the device, the FW version of the 1068A series control panels must be 1.025 or higher.



If the system is still in Maintenance mode, the keypad will be inhibited.



To enable the keypad you need to exit Maintenance mode.
At the end of the acquisition, the main screen (Home page) of the keypad will be displayed.



9.3 REPLACING A RADIO DEVICE

It allows you to replace a device by assigning to the new one the same address and configuration of the previous one.

To replace a device, follow the instructions below:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Radio devices**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Substitution**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the device you want to replace by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. From the list that appears, select the device you want to replace by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. The message "**Are you sure?**" appears on the display. Press ✓ to confirm;
9. Press the acquisition button on the new device to acquire it with the address and configuration of the previous one;
10. Press ↩ to return to the upper level menu.

	**IMPORTANT!** In order for a radio device or reader to be replaced with another one, the two must be of the same type, otherwise an error will be reported.

9.4 REPLACING A BUS DEVICE

9.4.1 Replacing the Bus devices (expansions, readers and radio interfaces)

It allows you to replace a device by assigning to the new one the same address and configuration of the previous one.

To replace a device, follow the instructions below:

1. Switch off the system completely;
2. Disconnect the device to be replaced;
3. Connect the new device to the bus;
4. Then power up the system again. The yellow LED of the new device blink slowly for about 10 second before changing the speed of blinking.
5. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
6. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.
7. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Select "**Substitution**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
9. Select the device you want to replace by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
10. The message "**Are you sure?**" appears on the display. Press ✓ to confirm;
11. Press the programming button of the new device to acquire it with the address and configuration of the previous one; its yellow LED turns off.
12. Press ↩ to return to the upper level menu.

IMPORTANT! In order for an expansion device or reader to be replaced with another one, the two must be of the same type, otherwise an error will be reported

9.4.2 Replacing the keypad

To replace a keypad, follow the instructions below:

1. Access the maintenance mode without keypad;
2. Disconnect the damaged keypad;
3. Connect a new keypad and use it as a service keypad;
4. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
5. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select "**Substitution**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Select the device you want to replace by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
9. The message "**Are you sure?**" appears on the display. Press ✓ to confirm;
10. Disconnect the service keypad;
11. Reconnect it and acquire it.

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 must be disconnected (reset) before carrying out any reacquisition procedure.

9.5 IDENTIFYING A BUS DEVICE

9.5.1 Interrogating a bus device

In order to find the address of a device already acquired on the bus (readers and expansions), follow the instructions below:

1. Activate the maintenance mode 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.

A not acquired device does not show any blinking.

9.5.2 Searching for and identifying a device

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

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Devices identification**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.

Then examine all installed devices:

- For expansions: the one with the required address will have the yellow acquisition LED blinking fast;
- For readers: LEDs will blink quickly;
- For keypads: the device address and its software version will appear on the display.

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

9.6 DELETING A BUS DEVICE

To delete any existing device from the bus (keypads, readers or expansions) proceed as follows:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Deleting**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. 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;
6. Switch off the system completely;
7. Physically disconnect the device from the bus;
8. Then power up the system again.

The device will be available again to be acquired on the same control panel or on another one.

To restore the device removed to default parameters and reacquire it again, it is necessary to reset it as described in paragraph *7.4 Reset default*.

EN50131

9.7 DELETING 1068/017 RADIO INTERFACE OR 1068/011 RADIO MODULE

To delete any existing device from the bus (keypads, readers or expansions) proceed as follows:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Deleting**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the "**Radio expansions**" type 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;
6. Switch off the system completely;
7. Physically disconnect the interface from the bus and/or the module from the control panel;
8. Then power up the system again.

If the control panel is powered again without disconnecting the 1068/011 module from the control panel, the module is automatically acquired upon restart.

IMPORTANT! When deleting a radio interface, 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.

9.8 ENABLING/DISABLING THE 1068/011 RADIO MODULE

Proceed as follows to enable a radio module:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Radio devices**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Enable**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Press the key associated with the Enable symbol ☑.

6. Enable ☑ = parameter enabled ; Enable ☐ = parameter disabled.

8. Press ✓ to confirm;
9. Press ↩ to return to the upper level menu.

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 data of the last device acquired and emit an error signal (a long beep).

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.

9.9 ENABLING/DISABLING THE 1068/017 RADIO INTERFACE

Compared to the 1068/011 radio module, the 1068/017 radio interface cannot be enabled or disabled.

It is automatically enabled when it is acquired on the bus and disabled when deleted.

9.9.1 Radio connection test

The 1068/011 radio module or the 1068/017 radio interface, 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.

To check 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, <u>without securing it</u>.
   All the devices must be powered and already acquired.
2. Position the control panel in the definitive final position.
3. Access the **MASTER** / **INSTALLER** menu by entering the access code. Press ✓ to confirm.
4. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.
5. Select "**Test**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.
6. Select "**Radio devices**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm. “ESC TO FINISH” appears on the keypad display.
7. In presence of a Fieldbus module, you will be asked which type of expansion you want to work on, vice versa no.
8. Open the magnetic contacts (DC), pass in front of the detectors (IR), press the key 🔒 on the radio remote control (RC), press the key ⟳ on the wireless keypad (KP).
9. For each device communicating with the interface, the keypad will indicate a value from 0 to 9 depending on the how good the signal is.
10. The table below illustrates what the test results might be:

7 ÷ 9	Excellent connection
4 ÷ 6	Good connection
2 ÷ 3	Sufficient connection
0 ÷ 1	Insufficient connection

11. After completing the tests, press ↩ to finish.
12. 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, then repeat the test procedure from point 4.
13. 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.
14. Press ↩ repeatedly to go back to the main menu.

For further details and information, refer to the dedicated manual.

9.10 CONFIGURING RADIO PARAMETERS

The following parameters describe the steps for changing the default configuration of the radio module parameters.

9.10.1 Device supervision

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Radio devices**" by pressing the button associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Device Supervision**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select the supervision time by pressing the key associated with the symbol ◉ .
8. Press the key associated with the symbol on the display ◉. Press ✓ to confirm.
   - Disabled ○
   - 4h ◉
   - 6h ○
   - 8h ○
   - 10h ○
   - 12h ○

   Supervision ◉ = enabled ; Supervision ○ = NOT enabled
9. Press ↩ to return to the upper level menu.

Supervision	Functional notes
Disabled	The radio module does not control the presence or absence of radio devices belonging to it.
4 hours	The radio module 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	

9.10.2 Jamming

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Radio devices**" by pressing the button associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Jamming**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Press the key associated with the Enable symbol ☑ .

   Enable ☑ = parameter enabled ; Disable ☐ = parameter disabled.
8. Press ✓ to confirm;
9. Press ↩ to return to the upper level menu.

Jamming	Functional notes
Disabled	The radio module does not control the occupation of the radio band by devices foreign to the system.
Enabled	The radio module does control the occupation of the radio band by devices foreign to the system.

9.10.3 Enable

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Radio devices**" by pressing the button associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Enable**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Press the key associated with the Enable symbol ☑.

   Enable ☑ = parameter enabled ; Enable ☐ = parameter disabled.
8. Press ✓ to confirm;
9. Press ↩ to return to the upper level menu.

9.10.4 Module supervision

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Radio devices**" by pressing the button associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**Module Supervision**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Press the key associated with the Enable symbol ☑.

   Enable ☑ = parameter enabled ; Disable ☐ = parameter disabled.
8. Press ✓ to confirm;
9. Press ↩ to return to the upper level menu.

9.11 ACQUISITION OF A NEW RADIO DEVICE

EN50131

To acquire a new radio device, proceed as follows:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Radio devices**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Acquisition**" by pressing the key associated with the ∨ or ∧. Press ✓ to confirm;
6. Select "**Input devices" or "Dispositivi Output devices**" by pressing the key associated with the ∨ or ∧. Press ✓ to confirm. "ESC TO FINISH" appears on the display;
7. Press the acquisition key on the device to be acquired;
8. The address assigned to the device appears on the keypad display during acquisition;
9. Repeat step 7 on all devices to be acquired;
10. Press ↩ to return to the upper level menu.

⚠	**IMPORTANT!** Addresses are assigned progressively and by family; there is no need to follow a pre-established order. If you want the device addresses to follow a given logic, you must acquire them in that order.

9.12 DELETING A RADIO DEVICE

EN50131

Proceed as follows to delete any radio device:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Radio devices**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Deleting**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the type of device to delete by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. From the list that appears, select the device you want to delete by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Press ↩ to return to the upper level menu.

9.13 RESET FACTORY SETTINGS

The table below indicates the various possibilities for resetting the control panel and system devices to default values as needed.

	Reset software				Reset hardware		
	Partial	Total	Codes	Radio module	Installer code	Factory settings	Wired devices
PARAMETERS IN THE CONTROL PANEL MEMORY							
Control panel programming	■	■				■	
Wired device addresses		■				■	
Radio device addresses		■				■	
Installer Code		■	■		■	■	
Tech. Manager Code		■	■		■	■	
Master Code		■	■			■	
User codes		■	■			■	
Keys		■				■	
System log		■				■	
EN50131 Event log (available only with 1068/010A control panel)		■				■	
PARAMETERS IN THE WIRED DEVICE MEMORIES							
Device address		■					■
Device parameters	■	■					■
PARAMETERS IN THE RADIO MODULE MEMORY							
Acquisition of the radio devices		■		■			
Module parameters	■	■		■			

IMPORTANT! The reset operations are irreversible and therefore once carried out, it become necessary to reacquire and/or reprogram any devices involved.

9.13.1 Software partial reset

Reset the control panel programming to default.

The following are not deleted: the System Log, the codes, the keys, and the device acquisitions.

Proceed as follows to carry out the partial reset:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Reset Default**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press ✓ to confirm;
6. Press ↩ repeatedly to go back to the upper level menu.

It does not restart the system.

It resets the programming of:

- System general parameters
- Inputs
- Outputs
- Acquired wired expansions (acquisition is maintained)
- Possible radio module (the radio module maintains the acquisition of its devices)
- Radio devices acquired by the radio module
- Acquired wired keypads (acquisition is maintained)
- Acquired readers (acquisition is maintained)
- Time scheduler
- Zones
- Directory
- SMS
- GSM / GPRS
- IP

The programming of users and keys and their codes are maintained.

9.13.2 Codes software reset

To reset user codes, Master code, Installer code or Technical Manager code to their default value, proceed as follows:

1. Access the **MASTER / INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Users**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Default code**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the profile of which you want to reset the code by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Press ✓ to confirm;
8. Press ↩ repeatedly to go back to the upper level menu.

9.13.3 Radio module software reset

To reset the software of a radio module, follow the instructions below:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Radio Devices**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Reset factory settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Press ✓ to confirm;
7. Press ↩ repeatedly to go back to the upper level menu.

9.13.4 Installer hardware code reset

To reset the Installer code to its default value if you do not know the Master Code, restart the system with JP3 closed.

9.13.5 1068/013 interface hardware reset

Should a keypad not be present, to restore IP interface default values, restart the system with JP1 closed.

9.13.6 Hardware reset to factory settings

The hardware Reset can be used 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 factory settings. Remember that this method has the same effect as the Reset factory settings (see paragraph *7.5 Reset factory settings*) 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 *7.1 (How to view device addresses)* and reacquiring devices.

In reference to the radio module, it is also necessary to reacquire all the radio devices associated with it.

	**IMPORTANT!** Following the Hardware reset command, it is necessary to carry out the local reset of all the radio sirens of the system and then reacquire them.

To reset the hardware, restart the system with both JP1 and JP2 closed.

9.13.7 Wired device hardware reset

The deletion of any device in the system and connected to the bus must be done according to the procedure described in paragraph *9.6 Deleting a bus device*.

Only in special cases, for example if a device has already been acquired by another control panel or following “Hardware reset to factory settings" can the Devices reset been used.

	**IMPORTANT!** Remember that this method only deletes the data on the device. If the device is also acquired on the control panel, it will continue to be present there, generating and signalling a tamper alarm.

To cancel the address of any device and reset its programming to factory settings, follow the instructions below:

- Disconnect power from the device and reconnect it. The yellow LED will begin blinking slowly.
- Within 10 seconds, press and hold down the “PROG” button for about 5 seconds until the yellow LED blink at a different speed.
- Release the button. The Reset phase is concluded. The yellow LED will continue to flash until the device is reacquired.

9.13.8 Wired keypad hardware reset

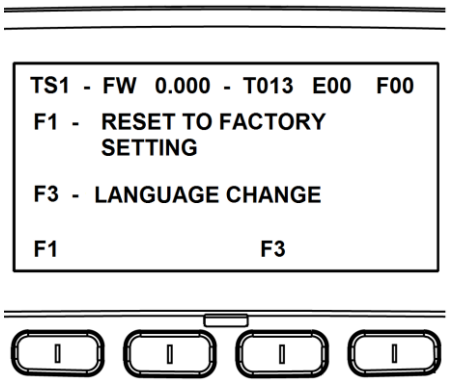
The deletion of any keypad in the system and connected to the bus must be done according to the procedure described in paragraph *9.6 Deleting a bus device*.

Only in special cases, for example if a device has already been acquired by another control panel or following a “Hardware reset to factory settings" can the Devices reset be used.

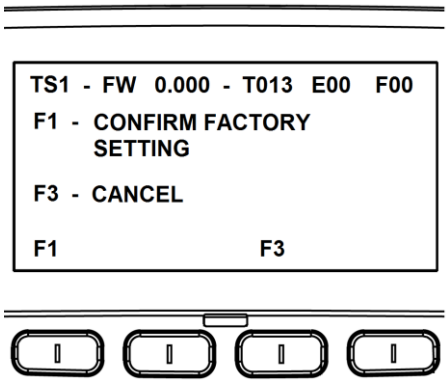
	**IMPORTANT!** Remember that this method only deletes the data on the device. If the device is also acquired on the control panel, it will continue to be present there, generating and signalling a tamper alarm.

To delete the address of a keypad and reset its programming to default, follow the instructions below:

- Disconnect the keypad from the power supply
- Open the keypad tamper
- Reconnect the keypad to the power supply
- Press the key associated with the **F1** symbol within 10 seconds



the page below will appear



- By pressing the key associated with the **F1** symbol the Reset of the parameters is confirmed, while by pressing the key associated with the **F3 “**Cancel**”** symbol, you will return to the previous screen.

9.13.9 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 *9.1 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. Perform a Battery Test.

IMPORTANT! The battery may only be replaced by trained and qualified personnel.

9.14 TURNING OFF THE ENTIRE SYSTEM

Whenever the entire system must be turned off, follow the instructions below:

1. Activate Maintenance status (see paragraph *9.1 Maintenance procedure*) and open the control panel.
2. Disconnect the mains power supply.
3. Disconnect the battery.

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.

10 TECHNICAL SPECIFICATIONS

10.1 1068/005A CONTROL PANEL

EN50131
GRADO 1

Nominal power voltage	230 V~ ; 50/60 Hz
Max absorption power at 230 V (1061/515)	0.6 A
Power unit output nominal voltage 1061/515 (*) - Type A power unit	14.4 V⎓
1061/515 power unit max current deliverable	1.5 A
Ripple max 1061/515	300 mV p.p. with I = 1A
Control panel operating voltage	10.5 V⎓ ÷ 16 V⎓
Overload protection tripping current	16 V⎓
Max current absorbed by control panel board at 14.4 V⎓	
(with relays energised, default condition)	110 mA stand-by with balanced inputs
(with relays de-energised)	80 mA with balanced inputs
Installable battery	12 V – 7.2 Ah
Battery charging nominal voltage	13.8 V⎓
Max. current supply to charge battery	600 mA
Max time for recharging battery to 80%	24 hours
Battery flat threshold	11.4 V
Automatic test battery	every 24 hours (with mains)
Nominal voltage on the + terminal	13.8 V⎓ ±1,5%
Max current deliverable from + terminal	1,1 A (with overload protection)
Nominal voltage on the +V1 terminals	13.8 V⎓ ±1,5%
Nominal voltage on the +V2 terminals	13.8 V⎓ ±1,5%
Nominal voltage on the +SR terminal	14.4 V⎓ ±1,5%
Max. current deliverable from +V1 terminals	0,75 A (with overload protection)
Max. current deliverable from +V2 terminals	0,75 A (with overload protection)
Max total current deliverable from the +SR terminals	0,2 A (with overload protection)
Ripple max on outputs + +V1 V2 +SR with flat battery	300 mVpp
Max current and voltage of relay contact switch of outputs U1-U2	1 A – 24 V⎓ with resistive load
Max current deliverable from electric output U3	0.5 A
Max current deliverable from electric output U4	55 mA
Tamperproof switch	1 A – 24 V⎓
Max total length of control panel -peripheral serial Bus line	400 m
Max length of the connection between each detector or actuator and the control panel	500 m
Max length of the connection between a fast detector (roller, inertial, ...) and the control panel	100 m
Max number possible code combinations	from 10.000 to 1.000.000
Number of possible combinations of electronic keys	more than 1099 billion
Number of possible combinations of proximity keys	more than 4 billion
Programmable entry time	1 s ÷ 5 min
Programmable exit time	1 s ÷ 5 min
Programmable alarm time	1 s ÷ 30 minutes (default 3 minutes)
Programmable tamper alarm time	1 s ÷ 30 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 and System log maintenance.	EEPROM
Operating temperature	-10 °C ÷ +40 °C
Max. relative humidity during operation	75%
Storage temperature	-20°C ÷ +60°C
Polluting degree	Grade 2
Overvoltage category	CAT II
Degree of protection of casing	IP40 / IK06
Dimensions (W x H x D)	290 x 275 x 95 mm
Weight (without battery)	1.3 Kg

(*) = Power supply unit in CAT II 2500 V. The power supply unit that, once installed, is subject to transient voltages higher than those of the design overvoltage category, requires additional protection from the transient voltages external to the equipment.

See paragraph *1.2.3 Maximum system size*, for more details.

10.2 1068/010A CONTROL PANEL

Nominal power voltage	230 V~ ; 50/60 Hz
Max absorption power at 230 V (1061/515)	0.6 A
Power unit output nominal voltage 1061/515 (*) - Type A power unit	14.4 V⎓
1061/515 power unit max current deliverable	1.5 A
Ripple max 1061/515	300 mV p.p. with I = 1A
Control panel operating voltage	10.5 V⎓ ÷ 16 V⎓
Overload protection tripping current	16 V⎓
Max current absorbed by control panel board at 14.4V⎓	
(with relays energised, default condition)	130 mA stand-by with balanced inputs
(with relays de-energised)	100 with balanced inputs
Installable battery	12 V – 7.2 Ah
Battery charging nominal voltage	13.8 V⎓
Max. current supply to charge battery	600 mA
Max time for recharging battery to 80%	24 hours
Battery flat threshold	11.4 V
Automatic test battery	every 24 hours (with mains)
Nominal voltage on the + terminal	13.8 V⎓ ±1.5%
Max current deliverable from + terminal	1,1 A (with overload protection)
Nominal voltage on the +V1 terminals	13.8 V⎓ ±1.5%
Nominal voltage on the +V2 terminals	13.8 V⎓ ±1.5%
Nominal voltage on the +SR terminal	14.4 V⎓ ±1.5%
Max. current deliverable from +V1 terminals	0,75 A (with overload protection)
Max. current deliverable from +V2 terminals	0,75 A (with overload protection)
Max total current deliverable from the +SR terminals	0,2 A (with overload protection)
Ripple max on outputs + +V1 V2 +SR with flat battery	300 mVpp
Max current and voltage of relay contact switch of outputs U1-U2	1 A – 24 V⎓ with resistive load
Max current deliverable from electric output U3	0.5 A
Max current deliverable from electric outputs U4 ÷ U7	55 mA
Tamperproof switch	1 A – 24 V⎓
Max total length of control panel -peripheral serial Bus line	400 m
Max length of the connection between each detector or actuator and the control panel	500 m
Max length of the connection between a fast detector (roller, inertial, ...) and the control panel	100 m
Max number possible code combinations	from 10.000 to 1.000.000
Number of possible combinations of electronic keys	more than 1099 billion
Number of possible combinations of proximity keys	more than 4 billion
Programmable entry time	1 s ÷ 5 min
Programmable exit time	1 s ÷ 5 min
Programmable alarm time	1 s ÷ 30 minutes (default 3 minutes)
Programmable tamper alarm time	1 s ÷ 30 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 and System log maintenance.	EEPROM
Operating temperature	-10 °C ÷ +40 °C
Max. relative humidity during operation	75%
Storage temperature	-20°C ÷ +60°C
Polluting degree	Grade 2
Overvoltage category	CAT II
Degree of protection of casing	IP40 / IK06
Dimensions (W x H x D)	290 x 275 x 95 mm
Weight (without battery)	1.3 Kg

(*) = Power supply unit in CAT II 2500 V. The power supply unit that, once installed, is subject to transient voltages higher than those of the design overvoltage category, requires additional protection from the transient voltages external to the equipment.

See paragraph *1.2.3 Maximum system size*, for more details.

10.3 1067/092 SUPPLEMENTARY POWER SUPPLY WITH REPEATER

Section - BUS IN

Mains power supply ..... 13.8 V⎓ (supplied by control panel BUS)
Expansion operating voltage ..... 9 V⎓ to 15 V⎓
Nominal current absorbed at 12 V⎓
(with relays energised, default condition) ..... 50 mA stand-by with balanced inputs
(with relays de-energised) ..... 40 mA with balanced inputs
Nominal voltage on the +V1 terminal ..... 13.2 V⎓ (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⎓ (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⎓ 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 detector or actuator and expansion ..... 500 m
Max length of the connection between a fast detector (roller, inertial..) and the expansion ..... 100 m

Supplementary power section and BUS OUT

Mains power supply ..... 100-240 V~ -15%+10% 50/60 Hz
Max absorption power at (MW RS-50-15) ..... 800 mA
MW RS-50-15**(*)** power output nominal voltage - Type A power supply ..... 14.4 V⎓
Max. deliverable current ..... 3.4 A
Ripple max. MW RS-50-15 ..... 120 mV p.p. with I = 3.4 A
Operating voltage of the electronic power supply/repeater ..... 9 V⎓ ÷ 15 V⎓
Max current absorbed by the electronic power supply/repeater ..... 100 mA
Installable battery ..... 12 V - 18 Ah
Nominal voltage of battery charger **Note 1**) ..... 13.8 V⎓
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
Automatic test battery (controlled by control panel) ..... every 24 hours (with mains)
Max current for external devices (keypads, detectors, sirens) taken from + (BUS OUT), +, + terminals
Grade 2 – with SP2 dialler and 12 hour autonomy ..... 1050 mA
(total 1150 mA, of which 100 mA for electronics)
Nominal voltage on the +SR terminal **Note 2**) ..... 14.4 V⎓
Max current deliverable from the +SR terminal ..... 200 mA (with overload protection)
Nominal voltage on the + (BUS OUT) terminal) ..... 13.8 V⎓ ±1.5%
Max. current deliverable from + (BUS OUT) terminal) ..... 1100 mA (with overload protection)
Nominal voltage on the + (BUS OUT) terminal) ..... 13.8 V⎓ ±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 ÷ +40°C
Average relative humidity during operation 75%
Storage temperature ..... -20°C ÷ +60°C
Degree of protection of casing ..... IP40 / IK02
Polluting degree ..... Grade 2
Overvoltage category ..... CAT II
Dimensions (W x H x D) ..... 435 x 320 x 93 mm
Weight (without battery) ..... 5.2 Kg

Note 1): if the battery is not connected to the head of the terminal +BT -BT there is no power.

Note 2): in case of blackout, the +SR does not supply voltage.

(*) = Power supply unit in CAT II 2500 V. The power supply unit that, once installed, is subject to transient voltages higher than those of the design overvoltage category, requires additional protection from the transient voltages external to the equipment.

10.4 1068/021 COMMAND KEYPAD LCD

Nominal power voltage ..... 13,8 V⎓ (taken through communication bus)
Keypad operating voltage ..... 9 V⎓ ÷ 15 V⎓
Nominal current absorbed at 13,8 V⎓:
in stand-by, only LED for presence mains supply ..... 17 mA
operative, with backlighting at minimum level ..... 22 mA
operative, with backlighting at maximum level and all LEDs ON ..... 93 mA
Max total length of control panel-peripheral -serial Bus line ..... 400 m
Max length of the connection between each detector and the keypad ..... 500 m
Max length of the connection between a fast detector (roller, inertial, ...) and the keypad ..... 100 m
Type of communication ..... Urmet serial protocol
Programmable input 1
Tamperproof switch ..... standard with clear channel signalling in the control panel
Protection against inserting false codes ..... Yes
Operating temperature range ..... -10 °C ÷ +40 °C
Max. relative humidity during operation 75%
Storage temperature ..... -20°C ÷ +60°C
Degree of protection of casing ..... IP40 / IK06
Weight ..... 210 g
Dimensions (W x H x D) ..... 141 x 117 x 29 mm

10.5 1067/334 – 1067/335 ELECTRONIC KEY READER

Nominal power voltage ..... 13.8 V⎓ (taken through bus)
Reader operating voltage ..... 9 V⎓ ÷ 15 V⎓
Nominal current absorbed at 12 V⎓ ..... 7 mA in stand-by
..... 10 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 detector and the reader ..... 500 m
Max length of the connection between a fast detector (roller, inertial, ...) and the reader ..... 100 m
Type of communication ..... Urmet serial protocol
Auxiliary inputs 2
Operating temperature ..... -10°C ÷ +40°C
Max. relative humidity during operation 75%
Storage temperature ..... -20°C ÷ +60°C
Degree of protection of casing ..... IP40 / IK02

10.6 1068/435 PROXIMITY READER

Nominal power voltage ..... 13.8 V⎓ (taken through communication bus)
Reader operating voltage ..... 9 V⎓ ÷ 15 V⎓
Nominal current absorbed at 13.8 V⎓ ..... 33 mA in stand-by
..... 36 mA (with all LEDs ON)
Max total length of control panel-peripheral -serial Bus line ..... 400 m
Max length of the connection between each detector and the reader ..... 500 m
Max length of the connection between a fast detector (roller, inertial, ...) and the reader ..... 100 m
Type of communication ..... Urmet serial protocol
Auxiliary inputs 2
Operating temperature range ..... -10°C ÷ +40°C
Max. relative humidity during operation 75%
Storage temperature ..... -20°C ÷ +60°C
Degree of protection of casing ..... IP40 / IK02

10.7 1067/008A 8-INPUT EXPANSION MODULE

Nominal power voltage	13.8 V⎓ (taken through bus)
Expansion operating voltage	9 V⎓ ÷ 15 V⎓
Nominal current absorbed at 12 V⎓	30 mA in stand-by (with energised relay, default condition)
	18 mA max with relay de-energised
Nominal voltage on the +V1 terminal	13.2 V⎓
Max current deliverable from +V1 terminal	500 mA
Nominal voltage on the +V2 terminals	13.2 V⎓
Max total current deliverable from the +V2 terminals	500 mA
Max current and voltage of relay contact switch of output U1	1 A – 24 V⎓ 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 detector and the expansion	500 m
Max length of the connection between a fast detector (roller, inertial, ...) and the expansion	100 m
Type of communication	Urmet serial protocol
Operating temperature	-10°C ÷ +40°C
Max. relative humidity during operation	75%
Storage temperature	-20°C ÷ +60°C

10.8 1068/458 GSM/GPRS MODULE WITH VOCAL SYNTHESIS

Nominal power voltage	13.8 V⎓ (taken from control panel)
Module operating voltage	9 V⎓ ÷ 15 V⎓
Nominal current absorbed in stand-by	35 mA
Current absorbed with active connection	170 mA max
Operating temperature	-10°C ÷ +40°C
Reference standard	EN50136-2
ATS category	SP2
ACK type	Pass-Through

10.9 1068/013 IP INTERFACE

Nominal power voltage	14 V⎓ (taken from control panel)
Power supply range	9 V⎓ ÷ 15 V⎓
Absorption at nominal voltage of 14 V⎓	60 mA
Logic signal level from/to control panel	3.3 V⎓
Ethernet baudrate	10Mbps
WiFi baudrate	54Mbps
Max. relative humidity during operation	75%
Operating temperature	-10°C ÷ +40°C

10.10 1068/002 IP INTERFACE

Nominal power voltage	13.8 V⎓
Operating voltage	10 V⎓ ÷ 14,5 V⎓
Nominal current absorbed at 13.8 V⎓ (without LAN connections)	48 mA
Max absorbed current at 13.8 V⎓ (PoE and LAN connections)	1.2 mA
PoE rated voltage	48 V⎓
PoE power	14 W
ETH2, ETH3, ETH4 connections	RJ45 10/100BaseT MDI/MDIX autosensing
ETH0-PoE connection	RJ45 PoE IEE 802.3af 10/100BaseT MDI/MDIX autosensing
Transfer mode	Store and forward
Cables type	100base-T CAT5 or higher UTP ETH0-PoE (≤ 30m) ETH2, ETH3, ETH4 (≤ 100m)
RJ45 Yellow LED	speed 10/100Mbps
RJ45 Green LED	Active Ethernet link
Dimensions (mm)	88 x 74 x 17

10.11 1068/027 7”TOUCH SCREEN KEYPAD

POE input voltage	48 - 54 V⎓
External power supply voltage	48 V⎓ - min. 15 W
Max consumption	12 W
S+, S- terminal outputs	25 mA @ 24 V⎓
Display	7” TFT
Touchscreen	Capacitive
Resolution	1024 x 600 px
Brightness	350 cd/m^2
Viewing Angle	160° / 160°
Operating Temperature	-5 ÷ 45°C
IPerHome CU Consumption	0,5 CU
Dimensions (LxHxP)	212 x 138 x 24 mm

Frequency bands

WiFi	2400 ÷ 2483,5 MHz
Bluetooth ver. 4.0	2400 ÷ 2483,5 MHz
Yokis	2400 ÷ 2483 MHz

Output power (Max)

WiFi	20 dBm
Bluetooth ver. 4.0	4 dBm
Yokis	10 dBm

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

The symbol of the crossed-out wheeled bin on the product or on its packaging indicates that this product must not be disposed of with your other household waste.

Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment.

The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment.

For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

URMET S.p.A.
10154 TORINO (ITALY)
VIA BOLOGNA 188/C
Telef. +39 011.24.00.000 (RIC.AUT.)
Fax +39 011.24.00.300 - 323

Area tecnica
servizio clienti +39 011.23.39.810
http://www.urmet.com
e-mail: info@urmet.com

MADE IN CHINA