EN 50131-1
EN 50131-3
EN 50131-6
EN 50131-10
EN 50130-4
EN 50130-5
EN 50136-1
EN 50136-2
CEB T031

PRIME

Anti-intrusion control panel and security systems

Programming manual

inim

End-User Licence Agreement (EULA)

This is a legally binding agreement between the authors of this software (Inim Electronics S.r.l.) and You (You means the licensee or anyone engaged by You or otherwise pertaining to You).

By installing, copying or otherwise using this software, You acknowledge that You have read, understand and agree to be bound by the terms of this agreement (EULA). If You do not agree with any of the terms or conditions of this agreement (EULA), You are not authorised to install or use this software for any purpose whatsoever.

All versions of this software are protected throughout the world by copyright and other intellectual property rights. All rights are property of Inim Electronics S.r.l.. You may not duplicate, sell, distribute or use this software save as provided under this End-User Licence Agreement, unless You obtain written consent from Inim Electronics S.r.l..

Any parties interested in using this software for non-personal purposes must contact Inim Electronics S.r.l..

Rights

This license grants the following rights: installation and use. It is allowed to install and use an unlimited number of copies of this product.

Reproduction and distribution

This End-User Licence Agreement hereby grants to You the right to reproduce and distribute an unlimited number of copies of this product; each copy must be in whole and accompanied by a copy of this agreement (EULA).

You may not embed this software in another software application or freeware, shareware or commercial product without first obtaining explicit consent from Inim Electronics S.r.l..

Other rights and restrictions

You are not permitted to reverse engineer, disassemble, decompile or modify this product or any portion thereof.

Separation of components

This software is Licensed as a single product; You are not permitted to separate and use any portion of it on more than one single workstation.

Transfer of the Software

You are permitted to transfer this product and Your rights under this End-User Licence Agreement on a permanent basis to another person or entity.

Licence Term

Our rights under this agreement (EULA) will terminate immediately if You fail to comply with any of the terms and conditions contained within. If this occurs, You must destroy the Software, and all copies of all and any part of it.

By using this software, You agree to be bound by the terms of this End-User Licence Agreement.

Copyright

With the exception of any explicit annotations, all rights and the copyright pertaining to the software in its entirety and its parts (including figures, photographs, animation, video, audio, music, text and code) and accompanying documentation are the exclusive property of Inim Electronics S.r.l..

This software is protected by International Copyright Laws and Agreements and must be considered in the same way as all other material which is subject to copyright laws.

Disclaimer of Warranties

Inim Electronics S.r.l. make no warranties of any kind, either statutory or otherwise in relation to this product. The software and all associated material is released without any undertakings of any kind, express or implied. You use this product at your own risk.

Limits of Liability

In no event shall the authors of this software be liable to You or to those claiming for You for any damage of any kind, whether direct or in direct (including but not limited to, damage or loss of any kind, loss of profits, business interruptions, loss or corruption of data) arising out of or in connection with the use of, or the impossibility to use, this product.

Contact www.inim.biz for further details.

Processing of personal data

Prime control panels, by attributing them to installers and users registered with the Inim Cloud service, can be managed through dedicated web pages and/or apps available to both the installer and the end user.

In order to allow management of the control panel via Inim Cloud an explicit request is required from the users to whom the control panel is to be associated.

As soon as a control panel is connected to a LAN or a GSM/LTE network, it will be available on the Inim Cloud, however, until the association is explicitly requested by a user the data exchanged are:

- purely technical (in order to allow an association to a user in the future) and do not include any personal data
- always encrypted

- free from any correlation with personal data that may already be present in the Inim Cloud

The control panel events log becomes available only after associating the control panel with the users and can be viewed chronologically from the moment of such an association.

If you do not want to manage the control panel via Inim Cloud and/or do not want to allow any type of connection to Inim Cloud in advance, simply disable the connection with the service via programming (refer to "*Enablement for programming*").

Table of contents

Chapter 1 General information

1.1 Manufacturer's details

Manufacturer: Inim Electronics S.r.l.
Production plant: Centobuchi, via Dei Lavoratori 10
63076 Monteprandone (AP), Italy
Tel.: +39 0735 705007
Fax: +39 0735 734912
E-mail info@inim.biz
Web: www.inim.biz

The persons authorized by the manufacturer to repair or replace the parts of this system have authorization to work only on devices marketed under the brand Inim Electronics.

1.2 Operator Qualifications

Installer

The installer is the person (or group of persons) who sets up and programs the entire security system in accordance with the purchaser's requirements and in respect of the safety laws in force. It is the responsibility of the installer to instruct the user on how to use the security system properly.

Under normal circumstances, the installer is not allowed to arm/disarm the system without previous authorization from the user. All the system partitions must be disarmed before accessing the parameter programming phase.

The access code of the installer is a level 3 access code (see "*Access Levels*").

User

The user or users are the occupants of the premises where the Prime anti-intrusion system is installed. The users can arm and disarm the system or parts of it after valid authentication.

As a result of the extreme flexibility of the system, the most frequent operations can be carried out without prior authorization. This operating method must be expressly requested by the purchaser who must be made aware of the risks that this way of operating entails (false alarms, accidental arm/disarm operations, etc).

Each user is associated with a system access code. The code programming process allows you to define the code hierarchy:

- **User**
- **Manager**
- **Master**

Each code, in accordance with its assigned level in the system-hierarchy (the "User" being the lowest level), is capable of carrying out the following operations on all other codes that are hierarchically inferior:

- enable/disable
- change PIN
- change some of the programming parameters

1.3 Access Levels

Specific legislation defines the following levels of access to the control panel, distinct from the limitations of system usability:

- **Level 1** - access by any person (e.g. passer-by)
- **Level 2** - access by a user
- **Level 3** - access by the installer or maintenance operator (expressly authorized by a user with level 2 access)
- **Level 4** - access by the manufacturer

1.4 Manuals

The manuals which are not supplied with the apparatus can be ordered, making reference to their respective codes, or downloaded from www.inim.biz.

Installation and programming guide

The guide, supplied with each control panel, provides all the instructions and illustrations necessary for fast installation and programming of the Prime system.

This leaflet provides a quick guide to first startup, together with the wiring diagrams for the necessary connections, a table for the peripheral addresses, a quick guide to system programming as well as the default values of the programming parameters.

Installation manual

The installation manual contains the technical specifications of all the system components and the instructions for their installation, including instructions with wiring diagrams for the various modules.

It also contains the instructions for system commissioning

It is the responsibility of the installer to follow all the manufacturer's instructions in order to ensure proper functioning of the system and, at the same time, to comply with all the warnings relating to the active and passive security of the installation.

Programming manual (this manual)

The Programming manual contains instructions for the configuration and programming of the Prime system, as well as the descriptions of all the parameters and options, regardless of the means chosen for the programming process (keypad, software, etc.).

It also contains the instructions for commissioning, maintenance and troubleshooting procedures.

Software program

The Prime/STUDIO software manual contains the description of the software and the instructions for its installation and use.

It is the responsibility of the person who programs the Prime system to follow the instructions carefully and to ensure they have complete knowledge of the software in order to proceed swiftly and properly with the configuration and programming procedures.

User's manual

This manual contains instructions relating to the user interface of the Prime control panel, its functions and use.

Supplied with every control panel, this manual must be given to the user who must be aware of and have fully understood all the system functions as well as the configuration set by the installer.

1.5 Documents for the users

Declarations of Performance, Declarations of Conformity and Certificates concerning to Inim Electronics S.r.l. products may be downloaded free of charge from the web address www.inim.biz, getting access to Extended Access and then selecting 'Certifications' or requested to the e-mail address info@inim.biz or requested by ordinary mail to the address shown in this manual.

Manuals can be downloaded free of charge from the web address www.inim.biz, after authentication of credentials and by directly by accessing the page of each product.

1.6 About this manual

Manual code: DCMPINE0PRIMEE

Revision: 170

1.7 Copyright

1.8 Terminology

Panel, control panel, device — Refer to the main supervisory unit and any constituent parts of the Prime security system.

Left, Right, Behind, Above, Below — Refer to the directions as perceived by the operator when directly in front of the mounted device.

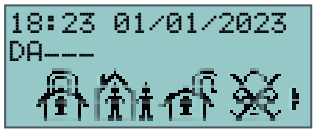
Qualified personnel — Persons whose training, expertise and knowledge of the products and laws regarding security systems, are able to create, in accordance with the requirements of the purchaser, the most suitable solution for the protected premises.

Select — Click on a specific element of the interface (drop-down menu, options box, graphic object, etc.).

Press — Means click-on a video button or push a key on the control-panel keypad.

1.9 Graphic conventions

The following images represent the display of a control panel with an LCD screen and relative signalling. For other types of displays, it is necessary to refer exclusively to the notifications which are shown and not to the image shown:



Note — The notes contain important information relating to the text.

Attention! — **The "Attention" prompts indicate that total or partial disregard of the procedure could damage the device or its peripherals.**

DANGER!

The DANGER warnings indicate that total or partial disregard of the procedure could injure the operator or persons in the vicinity.

Chapter 2 Programming the Prime system

The Prime system has been especially designed to be programmed either from a keypad (using one of the keypads connected to the control panel) or from a PC via Prime/STUDIO software.

All the options, functions and parameters of the control panels must be programmed solely by the installer or by qualified persons authorized by the installer.

The control panels are programmed at the factory with almost ready-to-go settings ("Factory settings") which, in the majority of installations, require the installer to make only minor changes in order to customize the system. For example, all the zones, keypads and readers are assigned to (belong to) partition 1, alarm and tamper events related to partition 1 activate the relay output which is monostable set at 3 minutes (Monostable time = 3 minutes), etc.

2.1 Programming via keypad

The programming of the control panel via one of the Prime system keypads can be carried out only after a valid access to the installer menu.
In order to access the installer menu from a keypad and thus have the possibility to read/write the control panel parameters, it is necessary to:

1. Ensure all the control panel partitions are disarmed.
2. Type-in the installer code Pin on a keypad then press **OK**.

If you are working on a Alien keypad, it is necessary to access the "Settings" section, type in the user code, and access the "Installer section" then type-in the installer code.

Note

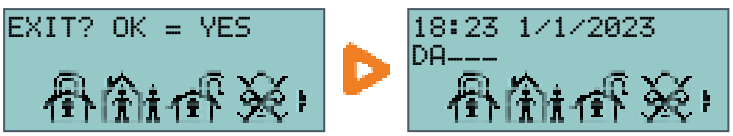
The PIN is "9999" at default.

3. The system will allow access to installer menu only after the entry of a valid PIN.

Once access to the installer menu is achieved, the system will:

- All the system keypads, except for the one the installer is working on, will be locked.
- The "PROGRAMMING" message will be shown on all the locked keypads.
- All outputs that do not have the home-automation attribute will be forced to stand-by.
- The events recognized by the control panel will be prevented from queuing calls, activating outputs and saving events to the events log.

To exit the installer menu, it is necessary to press **Esc** or **C** until the system asks: "EXIT? OK = YES", therefore press **OK**.



On exiting the installer menu, the control panel will:

- Apply all the new settings and values.
- Restart the I-BUS, reprogram and make all the peripherals fully operational.
- Restart the entire control panel processing phase thus allowing the queuing of phone calls, the activation of outputs and the storage of events.

2.2 Programming via Prime/STUDIO software

Programming the control panel and the system devices via the Prime/STUDIO software is possible only when the installation of the system is complete and the relative configuration has been downloaded to the PC in use.

1. Open a solution for a system (**Open** button).
2. Connect the apparatus to the PC in use.
3. Read the system configuration by downloading it to the PC by means of the **Read** button.
4. Select the first element to be programmed using the buttons on the left, then customize the programming parameters in the section that appears on the right.
5. To download the data to the control panel, click-on **Write** button.

Note

If an error occurs during the writing phase, it will be necessary to repeat the operation. Any data currently on the control panel will be overwritten.

6. Save the solution (**Save** button on the menu) or print out the details (**Print** button).

For a description of the Prime/STUDIO software and the instructions on how to use it, refer to the software manual.

2.3 Registration of the control panel to Inim Cloud

The registration of a control panel is an operation that allows its accessibility to all Inim Cloud service users. This accessibility is provided by the association of the control panel with the installer and users, who thereby will be able to reach the control panel via their Inim Cloud profile.

Following a correct registration procedure, the installer and users have a direct connection with the control panel for system management and programming operations.

An installer can view and program the control panels they are associated with through:

- their own Cloud web interface
- the Inim Tech Security App
- system programming and supervision software (Prime/STUDIO), by selecting the control panel from those listed in the **List of control panels available on the Cloud** field available in the "Communication ports" section of the settings menu

A user can view and manage the control panels they are associated with through:

- their own Cloud web interface
- the Inim Home App

Removing the control panel from the Cloud

Removal of the control panel from the Cloud can be carried out by the installer or by the user. This possibility is subject to the "Installer property" option programmed by the installer.

Following removal of the control panel from the Cloud, all codes are made available again when registering to the Cloud service.

In the case of removal, the installer can interact with the control panel as if it had never been registered to the Cloud. This is therefore the only possible way to allow a new installer to register the control panel and associate the first user (admin user).

2.3.1 Control panel registration via keypad for the installer

1. Connect the control panel to the Internet:
   - LAN connection, via PrimeLAN
   - Wi-Fi connection, via PrimeWiFi
   - GSM connection, by means of Nexus appropriately programmed with a valid APN associated with the SIM card in use
2. Access the installer menu, then the "Cloud enrollment" section:

Via keypad

Type-in Code (Installer), PROGRAMMING User functions, Activations, Cloud enrollment

Via Alien

Access the "Settings" section and then the "Installer" section, type-in the installer code and then access to the "User functions - Activations - Cloud enrollment" section.

3. Enter the 8-digit installer ID number.
   This number is available:
   - in one of the confirmation emails received during registration to the Cloud as an installer
   - in the installer personal profile section of www.inimcloud.com
   - in the "Programming" section of the Inim Tech Security App, via the ☰ button on the top left
4. The control panel will ask you to specify the owner using the "Inst. Ownership" option
   If the option is selected, the control panel is the ownership of the installer, otherwise it is the ownership of the "Admin" user.
5. After setting the above-mentioned option and pressing "**Ok**", the control panel will carry out the registration to Cloud and the keypad will display the string "WAIT".

Note

If the control panel date/time differs by more than 15 minutes from the exact date/time, the registration process may result negative .

6. The keypad will show the result of the procedure by displaying one of the following messages:

- "Account created!": the control panel has been successfully registered to Cloud
- "Communicat.Error": generic communication error.
  The possible causes may be:
  - no Internet connection
  - date of manufacture of the control panel is earlier than dd/mm/yyyy
  - date/time of control panel different, ahead or behind the exact date/time by more than 15 minutes
- "Already enrolled": the control panel is already registered to Cloud
- "Bad ID": the entered Installer ID code is wrong
- "Panel notEnabled": the control panel cannot be registered to Cloud

2.3.2 Registration of the control panel via web and user keypad

The following procedure requires that the user already has a Cloud account and that the control panel to be registered has been previously registered for the service by an installer.

1. Access the service through their user account.
2. Clicking on the button that manages your profile, accesses a page where you can set the parameters of your account and those of registered control panels.
   In the lower section, below the list of control panels, you have the "New INIM system" section.
3. The **Add** button will allow you start the registration process. The Cloud service will send an OTP (One Time Password) number consisting of 6 digits to the user.
   This number is also made available in the case of first access to the Cloud service as a user, following an invitation by the installer.

Note

This number has a limited time duration of 15 minutes.

4. Activate the "Cloud enrollment" option:

Via keypad

`Type-in Code (User), Activations, Cloud enrollment`

Via Alien

Access the "Menu" section, then "Activations", and then the "Cloud enrollment" option.

Enter the OTP password and wait for the outcome of the registration. The outcome of the procedure will be shown with one of the following messages:

- "Account created!": the control panel has been successfully registered to Cloud
- "Communicat.Error": generic communication error.
  The possible causes may be:
  - no Internet connection
  - date of manufacture of the control panel is earlier than dd/mm/yyyy
  - date/time of control panel different, ahead or behind the exact date/time by more than 15 minutes
- "Already enrolled": the control panel is already registered to Cloud
- "Bad/expired OTP": the entered password is incorrect or expired
- "Panel notEnabled": the control panel cannot be registered to Cloud.

2.3.3 Control panel registration via Inim Tech Security App

1. Connect the control panel to the Internet:
   - LAN connection, via PrimeLAN
   - Wi-Fi connection, via PrimeWiFi
   - GSM connection, by means of Nexus appropriately programmed with a valid APN associated with the SIM card in use
2. The control panel searches for the connection to the Cloud.
   As soon as it is found, the blue "**CLOUD**" LED will light up.
3. Activate the Inim Tech Security App and access the relevant QR-code scanning section.

4. The Prime control panel has a unique QR-code relating to the serial number of the control panel in use.
   This code can be found on the PCB of the motherboard, on the side of the metal enclosure or packing box.
   Use the App to scan this code.

Note

The QR-code of the control panel must be scanned once and only by the installer.

5. A 30 second window starts within which the installer must hold down the "FACT-SERV" button on the control panel board for at least 3 seconds (also indicated with the "CLOUD REG" label).

6. Enter a valid control panel installer code and enable, if necessary, the "Installer property" option.
   The App verifies the installer code provided. If the installer code is at default ("9999") the App proposes a code change.

Note The operations described above must be completed within 120 seconds.

7. The following automatic operations will start:
   - The control panel is associated with the installer on the Cloud
   - The control panel is enabled for complete programming.
   - The installer receives a control panel message registered to their account

At this point the control panel will be properly registered. You can then proceed with the association of the control panel to users who already have profiles on the Cloud service.

8. Associate the main user (admin) to the control panel.
   The App requires the installer to type in the e-mail address of the user. The address entered must be the same as that of the Cloud account of the user.

9. The admin user must accept their association via Inim Home.
   Once the operation is confirmed, a push notification will be sent to the App of the user.

Note For security reasons, the first user must complete the association operation within a maximum of 60 minutes

As soon as the association is completed, the installer will no longer have any ability to associate other users.

The installer can regain the ability to associate users with the control panel only when it is removed from the Cloud and subsequent re-association.

2.3.4 Control panel registration via Inim Home App

Main user (admin)

The following procedure requires that the user already has a Cloud account and that the control panel to be registered has been previously registered for the service by an installer.

1. Via the Inim Home App the admin user receives notification of the ongoing registration carried out by the installer.
2. The user must accept or reject the request within 60 minutes:
   - If the user refuses, the installer can re-propose the invite by accessing the specific section of the installer App.
   - If the user ignores the notification, after the set time has elapsed, the installer can send a new notification.
   - If the user accepts, a page will open on which the user will be asked to enter a control panel user code.
3. The App verifies the entered user code.
   If the code PIN is at default (from "0001" to "0050") the App will reject it and will repeat the PIN entry request.
4. If the PIN code is valid, the Cloud will forward a request to the control panel.
   - If the user is already set in programming by the installer (PIN code and partitions to operate on), the user has immediate access to the operations on the control panel.
   - If the PIN is valid but not associated with any user via programming, the system will assign the characteristics of the first available user profile to the user.

From this moment on, the installer will lose the right to invite other users.

At the same time, the newly enrolled user inherits the ability to invite other users for association with the control panel.

Secondary users

The operation can be carried out from the section of the Inim Home App reachable via the "Settings > Configuration" menu, by sharing one of the accessible control panels, and using the e-mail addresses of the accounts of the users to be invited.

1. The admin user must make a request to associate a secondary user.
2. Via the Inim Home App the secondary user receives notification of the ongoing registration carried out by the Main User.
3. The secondary user must accept or reject the request within a maximum of 60 minutes:
    - If the secondary user refuses the invite, the admin user can propose it again.
    - If the secondary user ignores the invite, after 60 minutes the admin user can send them a new request.
    - If the secondary user accepts the invite, the procedure described above for the admin user is repeated.
4. The App verifies the entered user code.
   If the code PIN is at default (from "0001" to "0050") the App will reject it and will repeat the PIN entry request.
5. If the PIN code is valid, the Cloud will forward a request to the control panel.
    - If the user is already set in programming by the installer (PIN code and partitions to operate on), the user has immediate access to the operations on the control panel.
    - If the PIN is valid but not associated with any user via programming, the system will assign the characteristics of the first available user profile to the user.

Secondary users do not have the ability to invite additional users.

Chapter 3 Programming the control panel

3.1 Configuration of a control panel

An installation managed by a Prime control panel requires different devices to be connected or installed directly on the control panel in order to enhance its functions. The configuration of a control panel consists not only in the programming of its parameters but also of the enrollment of these devices, the relative parameters of which can also be programmed.

3.2 Installer codes

The installer code allows the installer to access the programming phase of the Prime system. In fact, the system will request the PIN before allowing any programming from a keypad via the installer menu or before allowing reading or writing operations via the Prime/STUDIO software, that is, if it has not already been entered in the appropriate field.

The installer can set 2 installer codes (one personal and another) exclusively by accessing the installer menu via a keypad:

Via keypad

`Type in code` (Installer), `PROGRAMMING Installer code`

Table 3.1: Installer code parameters

ChangeInst. 1	Program the PIN of the primary installer code by entering it twice. The PIN is "9999" by default.
ChangeInst. 2	Program the PIN of the secondary installer code by entering it twice. The PIN is "9998" by default.
Inst.code access 2	Use keys ▣ and □ to enable/disable the sections of the installer menu that the secondary installer code can access.

Note

Code PINs must comprise 4, 5 or 6 digits.

In this section, the secondary installer code can access the Installer code PIN 2 section only.

Via software

Any reading operations from the system or writing of software solutions on the Prime system will be executed only after the installer code has been correctly entered.

This option is made available by clicking on the **Panel parameters** button in the section on the left and accessing the "Programming - Installer code" section on the right.

3.3 Prime control panel parameters

Table 3.2: Control panel definition

Parameter		Software section	Installer menu section
Control panel description	Edit field for the description of the control panel (max 50 alphanumeric characters).	Control panel parameters	–
Serial number	Section where you can view the univocal serial number of the control panel.		Other parameters, Serial number
Geolocation	Section where you can set the geographical coordinates of the installation. Pressing the "**...**" button on the left opens a window containing the map of the globe. Here, with a right click of the mouse it is possible to position the system and, after clicking on the "**+**" button, the "Latitude" and "Longitude" strings will show the selection coordinates.		–
"Cloud Mode"	If enabled, this option will apply a preset of some of the control panel parameters that would otherwise have to be programmed individually for connection to the Inim Cloud service. Refer to "*Preset for Cloud notifications*".		–
Date/Time	Editable field for the system date and time.		User functions, Set date/time
Set local time	This button sets the local time of the PC in use.		–
Write on control panel	This button writes the local time of the PC on the control panel.		–

Parameter		Software section	Installer menu section
Restart monostable outputs	If activated, each event which activates a monostable output refreshes the programmed "Monostable time".	Control panel parameters	Parameters RefreshMnstblOut
Does not arm if any of the zones are not ready	The control panel will not arm the partition if it detects any zones that are not in stand-by status. If there are zones with the "Auto-bypassable" or "NoArmIfNotReady" attribute amongst the open-zones (refer to "*Zones/Inputs*"), they will be shown on the keypad as Not ready. If the user goes ahead with the arming operation, these zones will be bypassed automatically and the partition will arm.		OpenZonesArmLock
Bypass tamper in the event of bypassed zones	If a zone is bypassed (disabled), it will also be unable to generate terminal tamper.		BypassAlsoTamper
Prevents the deletion of tamper memory by user code	No user will be allowed to delete of the following events: • terminal tamper • control panel open-tamper • control panel dislodgement-tamper • peripheral tamper • peripheral loss • false key		NoUserTamp.reset
Instant reset of wireless magnetic contact	If this option is enabled, reset of the magnetic reed sensor of wireless detectors will be signalled instantly (otherwise signalling has a maximum delay of 10 seconds).		Instant restoral
Lock installer code	If this option is enabled, all the control panel parameters with the exception of the installer PIN will reset to the factory default settings after reset.		LockInstall.Code
Automatic Daylight Saving Time (DST)	The control panel clock will go back automatically one hour at 03:00 the first Sunday in October, and it will go forward automatically one hour at 02:00 the last Sunday in March.		DayLightSav.time
Maintenance	You can start the maintenance session from the keypad without need of opening the control panel or moving the jumper. After exiting the Installer menu, you can operate on the system in the same way as when the control panel is placed in maintenance mode by means of the jumper. In order to place the control panel in "RUN" mode, this option must be disabled.		Maintenance
Check horn	The control panel will generate a "Sounder/flasher tamper" event when the passive horn disconnects from the relay (wire cutting tamper).		Tamper siren
Squawk	This option activates the sounder for a brief period during partition stay/away arming and disarming operations. This audible signal indicates that these operations have been executed successfully.		Squawk on arming
Sound alarm on keypad	If enabled, all the system keypads will emit an audible signal in the event of an alarm or tamper event on any one of the partitions they belong to.		Alarm on keypads

Parameter		Software section	Installer menu section
Enable control panel anti-dislodgement	This option, enabled by default, provides protection against tamper on the control panel (tear-off and tilt detection).		PanelTamp.enable
Clear memory on code recognition	If enabled, this option clears the alarm memory on recognition of a valid code.		ValidCode=Reset
Enable Wi-Fi	If enabled, activates the module for the Wi-Fi connection.		Parameters Enable Wi-Fi
Wireless supervision time	Parameter for the setting of the wireless-device monitoring time. On expiration of the set time any wireless devices that fail to respond will be signalled as lost. Accepted values: 12 to 250 minutes.		Other parameters. Wireless superv.
Mains fault signal delay	Parameter for the setting of the delay, expressed in minutes, between an "AC Mains failure" event and "AC Mains failure" event signalling. Accepted values: 0 to 250 minutes.		Mains fail.Delay
Low battery delay	Parameter for the setting of the delay, expressed in minutes, which will be applied before "LowBattery" events are actually signalled after detection. Accepted values: 0 to 250 minutes.		LowBattery delay
BUS speed	Selection of the BUS communication speed (38.4 / 125 / 250 kbps).		–
Cloud options	Parameter for selecting the communication channel with the Cloud: • Use LAN • Use Nexus If both are selected priority will be given to the LAN. If you do not wish to manage the control panel via Inim Cloud and/or do not wish to allow any type of connection to Inim Cloud in advance, simply disable these options.		Cloud options
Cloud port settings	Section that appears only if the "Allow cloud port configuration" option included in the Prime/STUDIO software settings is enabled. By means of the respective boxes, it is possible to type-in the cloud communication ports: • "Events cloud port", for the control-panel event transmission channel • "Management cloud port", for the commands channel The **Read** and **Write** buttons allow the installer to read operations from the control panel or to set entered data.		–
Enable context menu	Enabling this option, in the event of an alarm signalled by the control panel, the display of the control panel will show a request for entry of a valid user code. Following this entry, the system will carry out the following operations, depending on the options selected by the installer: • Switch off sounder/flashers • Stop call queue • Disarm • Delete alarm memories	-	QuickAlarmAction
LAN/Nexus Internet test	If enabled, every 5 minutes the control panel will perform automatically an internet connection test on the LAN/GSM channel which, in the event of failure, will force restart of the Wi-Fi connection.	-	LAN/NEXUS Internet test
AccessPoint WiFi	Option that enables the control panel to create a local Wi-Fi network.	-	AccessPoint WiFi
Automatic APN	This option activates an automatic search for the APN (Access Point Name) for Italian operators. The search is carried out at each startup of the control panel, at the end of each programming session and when the peripheral modules are inserted or disconnected.	GPRS parameters	Automatic APN

3.4 Preset for Cloud notifications

In order to make it easier for the installer to program a Prime control panel registered to the Inim Cloud service, the programming parameters regarding the Cloud service are preset at factory.

The Prime/STUDIO software has the "Customize Cloud Notifications" option which, if enabled, allows you to change the settings of these parameters.

The default programming involves a set of different types of events that must be communicated to the Cloud when they occur:

Table 3.3: Preset events for the Cloud

Event	Communication to Cloud in case of	
	Activation	Reset
Zone alarm	Yes	Yes
Terminal tamper	Yes	Yes

Event	Communication to Cloud in case of	
	Activation	Reset
Zone bypass	Yes	Yes
Effective arming mode on partition	Yes	No
Partition armed in Away mode	Yes	No
Partition disarmed	Yes	No
Overtime request on partition	Yes	No
Partition failed to arm	Yes	No
Thermostat on keypad	Yes	Yes
Activate scenario	Yes	No
Emergency button	Yes	No
Panic	Yes	No
Control panel Tamper	Yes	Yes
Zone fuse fault	Yes	Yes
I-BUS fuse fault	Yes	Yes
Battery inefficient	Yes	Yes
Mains failure	Yes	Yes
Expansion tamper	Yes	Yes
Keypad Tamper	Yes	Yes
Reader Tamper	Yes	Yes
Sounder flasher tamper	Yes	Yes
Nexus tamper	Yes	Yes
Video detector tamper	Yes	Yes
Expansion Loss	Yes	Yes
Keypad Loss	Yes	Yes
Reader Loss	Yes	Yes
Sounder/flasher loss	Yes	Yes
Nexus loss	Yes	Yes
Video detector loss	Yes	Yes
Jamming	Yes	Yes
Low battery wireless zone	Yes	Yes
Wireless zone loss	Yes	Yes
Valid Installer code	Yes	No
Invalid code	Yes	No
False key	Yes	No
Nexus fault	Yes	No
Input undergoing programming	Yes	Yes
Output fault	Yes	No
Low credit	Yes	No

3.5 Control panel language

The Prime system allows selection of the language the system uses for the strings in the User and Installer menus and for the descriptions of events, faults, etc.

Via keypad

`Type in Code` (Installer), `PROGRAMMING Language`

Use keys ▽ and △ to select the desired language and **OK** to confirm.

Obviously, after a change of language the descriptions of the various system elements such as the zones, partitions, outputs, codes, etc., will remain unchanged.

3.6 Firmware updating

Through a direct connection between the Prime/STUDIO software and the Prime control panel, it is possible to update the Prime board firmware to the latest revision available at moment of the software release.

Via software

Clicking on the **Firmware update** button on the menu on the top right opens a section with the available updates and the start procedure button.

Click on the button to start the updating of the control-panel peripherals and, on completion, just before the Prime update, you will be asked to confirm the operation.

Attention!

In order to avoid invalidating the procedure, do not switch off or disconnect the PC or control panel during the updating process.

The battery in the control panel must therefore be connected and fully efficient.

Prime/STUDIO solutions

Following the firmware update of a control panel, all programming data will be converted. However, there may be some dysfunctions due to the lack of alignment between the updated control panel revision and the revision referring to the Prime/STUDIO solution of the system being programmed.

It is therefore advisable to update the solution:

1. Click on the **Open solution** button.
2. On the window listing the saved solutions, select the solution to update.
3. Click on the **Conversion Wizard** button.
4. Follow the guided procedure the updated solution is generated.

Troubleshooting

- During the updating process, the keypad displays may show messages that are irrelevant.
- The maps on the Alien keypad may lose programming data.
  In this case it is necessary to update the Prime/STUDIO solution being used, by matching the firmware revisions and then restoring the maps via the USB of the keypad.
- Following the first update, the Alien keypads lose their settings and therefore must be recalibrated. Subsequent updates will not present similar problems.
- The Air2-Aria/W keypads are not to be updated if the control panel has not been previously put into service status.

Chapter 4 Programming inputs and outputs

4.1 Programming terminals

The terminals (with some exceptions) of the control panel, keypads and expansion boards can be configured as:

Table 4.1: Configuration of terminals

Configuration type	Software	Keypad
zone input		**I**
double zone input ("doubling")		**D**
output		**O**
Controlled output ("I/O", input-output)		**H**
unused		**-**

Attention!

For critical events or events of particular importance, it is advisable to use keypad terminals T1 and T2 as the signal outputs. The status of these outputs may switch (On to Off and vice versa) in the event of BUS reset.

Via keypad

1. Access the "Programming Terminals" section.

`Type-in Code` (Installer) , `PROGRAMMING Terminals` .

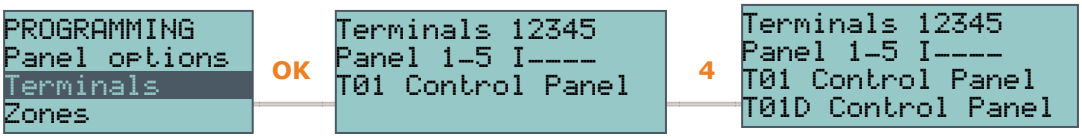


Table 4.2: Terminals viewing

Line	Display	View
1	Terminals 12345	the number of terminals on the selected device
2	Panel 1-5 I----	the selected terminal and the type of configuration
3	T01 Control Panel	the description of the selected terminal
4	T01D Control Panel	the description of the second zone of the selected terminal if this is set as a double zone or the string "Wireless" in the case of an expansion configured as such.

2. Use keys ▲ and ▼ to select the device whose terminals you wish to configure. The terminals are arranged as follows:
   - terminals from 1 to 5 on the control panel
   - terminals from 6 to 10 on the control panel
   - terminals on expansion boards
   - terminals on keypads

3. Use and to scroll across the terminals. The selected terminal will blink. The terminal setting is applied by pressing:
   - "**1**", to configure the terminal as an input ("I")
   - "**2**", to configure the terminal as an output ("O")
   - "**3**", to configure the terminal as a controlled output ("T")
   - "**4**", to configure the terminal as a double zone ("D")
   - "**5**", to configure the terminal as a Unused ("-")
   - "**6**", to enable/disable the terminal as wireless (only for expansion terminals)
4. After pressing the button that corresponds to the desired setting, it is necessary to press one of the buttons **OK**, , , and to configure its type.

If an "Unused" terminal is configured as "I", "O" ,"H" or "D" and the keypad emits an audible error signal, it means that you have exceeded the maximum number of terminals available on the control panel. If you wish to employ the terminal concerned, you must first configure another terminal as "Unused"

Press the **OK** button in correspondence with any terminal, provided that it is not an "Unused" terminal, to access directly the Type programming parameters of the selected terminal, be it a zone or an output.

Via software

By clicking on the **System Layout** button on the menu on the left, a graphical representation of the control panel board and a list of the configured peripherals will be shown in the section on the right.

The control panel and device terminals can be programmed in these sections and reached by right clicking in correspondence with the terminal symbol on the device image.

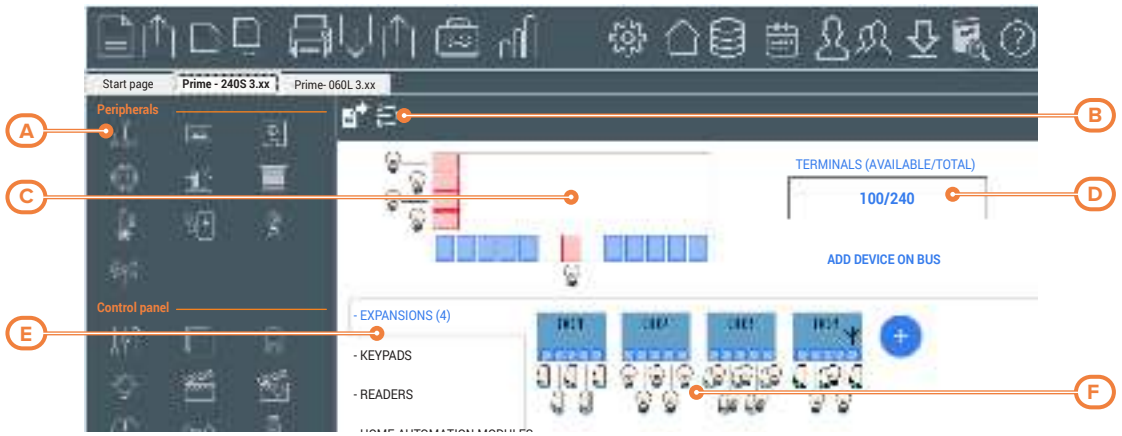


Table 4.3: Example of terminals undergoing programming

[A]	"System Layout" section button
[B]	Section menu bar
[C]	Control panel terminals
[D]	Number of terminals used out of the maximum number
[E]	List of peripheral categories with relative number of terminals used out of the maximum number
[F]	Terminals of the selected peripherals

By right clicking on any one of the PCBs you can assign a configuration common to all the terminals on the selected board. Right clicking on a single terminal allows it to be configured separately.

Double clicking on the icon of a terminal with an already assigned configuration will open a window where you can configure all the parameters of the selected terminal.

The section menu bar provides the **Rename the CCCs in sequential mode** button. This button starts an operation that reassigns the Contact-ID code of each zone in such a way that they are all in sequential order.

The section also provides a **Data export for supervisor** button for the creation of an interface file with monitoring software, such as Inim Electronics's SmartLook.

4.2 Zones/Inputs

The terminal the zone is connected to must be configured as an "input".

Via keypad

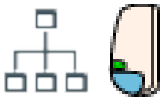
`Type in Code` (Installer), `PROGRAMMING Terminals`, select the terminal concerned configured as input ("**I**")

or

`Type in Code` (Installer) , `PROGRAMMING Zones` , select the zone concerned

This section allows the programming of the various parameters of the selected zone.

Via software



To program the zone, click on the **System Layout** button and, in the section on the right, select the device (control panel or peripheral) to which the terminal to be configured belongs.

Here, by right clicking on the icon of the terminal you can configure it as a "zone". Instead, by double clicking you access the programming phase.

or

Click-on the **Zones** button on the menu on the left, the section on the right will show a list of all the available zones and their parameters.

By selecting one of these items it is possible to set the parameters of the single zone by clicking on the button.

Zone type

For "Instant", "Route", "24 hour", "Automation", "Arm", "Disarm", "Switch", "OnArm/OffDisarm" and "Patrol" type zones, refer to the glossary (see "*Glossary*").

"Delayed" and "Delayed unhidden" zones are delayed both during entry and exit phases, in accordance with the output "Entry Time" and "Exit Time" settings (refer to "*Partition parameters*"). In particular, "Delayed unhidden" zones behave as follows:

- if violated when the system is disarmed, it will switch Off the blue LED on the keypad
- if the "View open zones" option is enabled, it will be shown on the keypad (refer to "*Keypad parameters*")
- it will not generate "Partition not ready" events
- on arming from a keypad, the zone will be visualized as a violated zone but, when the arming operation is confirmed, it will behave as a delayed zone and will not generate an alarm.
- if the "OpenZonesArmLock" option is enabled and the zone is violated, it will appear as a violated zone but, when the arming operation is confirmed, will behave as a delayed zone and will not generate an alarm (refer to "*Prime control panel parameters*")
- if the "OpenZonesArmLock" option is enabled, the zone is violated and instant arming is required, the zone will appear as a violated zone and when the partition arming operation is confirmed, the partitions the zone belongs to will not be armed.

Table 4.4: Zone parameters

Parameter		Software section	Installer menu section
Description	This is the editable label which identifies the zone. By default all the zones assume the description of the peripheral they refer to, followed by the respective terminal.	 Zones, selected zone	
Type	Checkbox for the selection of the zone type: • Instant • Delayed • Delayed unhidden • Route • 24 hour • Automation • Armed in Away mode • Disarm • Switch • OnArm/OffDisarm • Patrol		Zones, "zone"
Balancing	Dropdown box for the selection of the balancing type (the options vary in accordance with the zone type). Normally open (NO), Normally closed (NC), Single balancing, Double balancing, Double zone (without EOL), Double zone (with EOL).		
Detector type	Generic zone, Rollerblind, Shock, Anemometer, Temperature probe The selection determines the appearance of further parameters.		
Alarm cycles	Checkbox for the selection of the number of alarm cycles (between 1 and 14). If you select "Unlimited", the zone will operate as a "repetitive" zone.		
Wiring diagram	Button for to open a window showing the zone connection mode.		
Contact ID	Checkbox to indicate the Contact-ID code associated with the zone for the occurrence or restoral of events such as: • Zone alarm • Zone tamper • Zone bypass • Zone real-time		–
Configuration scheme	Button for to open a window showing the zone connection mode.		–
Real-time	Section for the adjustment of zone detection thresholds. The thresholds can be modified via the number boxes or by using the bar which indicates the levels by means of colours: • yellow - tamper/short • green - stand-by • red - alarm • orange - double zone with one zone in alarm status and the other in stand-by status Clocking-on the **Real-time** button makes a connection with the zone which feeds back information regarding the thresholds. The **OK** button saves the changes which will be written during the write phase.		–
Partitions	These are the partitions the zone belongs to. A zone configured as "Automation" cannot be assigned to any partition.		Zones, "zone"
Events button	At the bottom of the section are the buttons that directly access the programming section of the events associated with the selected zone.		Events

Table 4.5: Zone options

Parameter		Software section	Installer menu section
Interior	A zone that monitors the inside of the protected building. If a partition that a zone belongs to is armed in Stay mode, it will be unable to generate alarms.	 Zones, selected zone, options	Zones, "zone" Options
Auto-bypassable	A zone with this attribute will be bypassed automatically by the control panel if the partition it belongs to arms when the zone is not in standby status. The zone will be unbypassed automatically when it restores to standby or when the partition it belongs to is disarms.		
Unbypassable	A zone with this attribute cannot be bypassed, manually (by the user) or automatically (by the control panel).		
Chime	A zone with this attribute will generate "Chime on partition" events, if violated when the partitions it belongs to are disarmed. Keypads which have partitions in common with the chime zone will emit an audible signal when the "Chime on partition" event occurs. If all the partitions the zone belongs to are armed, the zone will operate as programmed.		
Test	A zone with this attribute cannot generate alarms (activate audible and visual signalling devices). However, any alarm events that occur will be saved to the events memory.		
No-Unbypassable	If this option is enabled, the zone will operate as an "Auto-bypassable" zone, with the difference that it will be automatically unbypassed only when the partition next disarms.		
NoArmIfNotReady	If this option is enabled, the zone, even if it is a 24H, automation or delayed zone, will not arm when it is not in stand-by status. If this option is selected for a 24H or technological zone, it can be used together with the control panel option: "Does not arm if any of the zones are not ready", for the management of the "anti-masking" function on duly capable detectors.		
Activate Entry Time 2	If this option is enabled, delayed zone will activate the second partition entry time. If this option is not enabled, delayed zones will activate the first partition entry time.		
Last exit zone	If this option is enabled and the zone passes from stand-by status to alarm status while the partition exit time is running, the exit time will be forced to 15 seconds. If the zone passes from alarm status to standby status, the exit time will be forced to 5 seconds.		
UnbypassOnDisarm	If this option is enabled, a zone which has been bypassed by a user, will be automatically unbypassed when the partition next disarms.		
Hold-up	Activation of a zone with this configuration generates an instant alarm even when the partition it belongs to is disarmed. However, audible and/or visual signalling devices will not be activated (silent alarm). Therefore, calls generated by the alarm will not be revealed audibly or visually on the keypad display and LEDs.		
Fault zone	If this option is enabled, violation of the zone will generate a zone alarm event and contribute to fault signalling (yellow LED on the keypad).		
Fire	The activation of this option forces the following programming settings on the relative zone: • the zone is a 24 hour type • the SIA-IP codes relating to fire events are associated with the events relating to the signals of this zone • to the events related to the signals of this zone, in case of use of an on-BUS sounder, the relative pattern is "fire"		

4.2.1 Detector type

In the case where the zone is associated with a detector, it is possible to set the type of detector (generic, roller blind, shock, anemometer, temperature probe) depending on the terminal in use:

Table 4.6: Zones - detector type

Zone	Generic	Roller blind	Shock	Anemometer	Temperature probe
Control panel terminals	any	any	any	None	None
Expansion terminals	any	T1, T2, T3, T4	T1, T2, T3, T4	T1, T2, T3, T4, T5	T1, T2, T3, T4, T5
Keypad terminals	any	any none for Alien/G	any none for Alien/G	none	None
Icon on software					

The control panel provides programming parameters for the terminal that vary in accordance with the type of detector selected:

Table 4.7: Detector parameters

Detector type	Parameter		Software section	Installer menu section
Generic	**Multi-pulse time**	This parameter applies only when the "Alarm pulse num." parameter (see below) is more than 1. This is the window during which a number of alarm pulses must be detected (each lasting as long as the programmed "Al.pulse Duration"). The number of alarm pulses must equal or exceed the value programmed for "Alarm pulses", before the system generates an alarm. This time window can be expressed in seconds or minutes.	Zones, selected zone, Device parameters "generic"	Zones, Generic zone
	Alarm pulses	This is the number of pulses (each lasting for the length of the "Al.pulseDuration") necessary to generate a zone alarm event. If this value is more than 1, the "Multi-pulse time" parameter must also be programmed.		
	Alarm pulse duration	This is the length of time (after detection of alarm conditions) the zone will allow before generating an alarm. Expressed in multiples of 15 milliseconds or 10 seconds.		
Roller blind	**Roller blind time**	This parameter applies only when the value of the "Roller blind pulses" parameter (see below) is more than 1. This is the time window during which a number of pulses, equal to the value set for "Rollerblind pulses", must be detected before a zone alarm is generated. This time window can be expressed in seconds or minutes.	Zones, selected zone, Device parameters "roller blind"	Zones, "roller blind zone"
	Roller blind pulses	This is the number of pulses necessary to generate a zone-alarm event. If this value is more than 1, you must also program the "Roller blind time" parameter.		
Shock	**Shock time**	This parameter applies only when the "Shock pulses" (see below) value is more than 1. This is the time window during which the system must detect a number of pulses equal to the value set for "Shock pulses" before generating a zone alarm. This time window can be expressed in seconds or minutes.	Zones, selected zone, Device parameters "shock"	Zones, "shock zone"
	Shock pulses	This is the number of pulses necessary to generate a zone-alarm event. If this value is more than 1, you must also program the "Shock time" parameter. If this value is 0, the alarm will be generated exclusively in accordance with the "Shock sensitivity" parameter.		
	Shock sensitivity	This is an empirical parameter which regulates the sensitivity of the sensor. Increasing this value decreases detection sensitivity.		
Anemometer	**InterventionTime**	Time expressed in seconds during which, if the set wind speed limit is exceeded, a zone alarm will be generated. If a speed greater than or equal to three times the set speed is detected, an alarm will generated instantly.	Zones, selected zone, Device parameters "anemometer"	Zones, "anemometer zone"
	Hysteresis speed	Hysteresis in Km/h of wind speed The value will be added to that of the limit and will constitute the real value for the zone alarm. If the terminal is already in alarm status, the calculated hysteresis value will instead be subtracted from the threshold limit to establish reset.		
	Wind speed	Wind speed threshold in Km/h above which, if it persists for more than the intervention time, a zone alarm will be generated.		

Detector type	Parameter		Software section	Installer menu section
Temperature probe	**InterventionTime**	Time expressed in tenths of a second during which, if the set temperature limit is exceeded, a zone alarm will be generated. If a temperature greater than or equal to three times the set temperature is detected, an alarm will be generated instantly.	Zones, selected zone, "temperature probe" device parameters	Zones, "temperature probe zone"
	Temperature hysteresis	Percentage of hysteresis calculated on the temperature limit. The calculated value will be added to that of the limit and will constitute the real value for the zone alarm. If the terminal is already in alarm status, the calculated hysteresis value will instead be subtracted from the threshold limit to establish reset.		
	Temperature limit	Threshold in tenths of a degree centigrade beyond which, if it persists for more than the intervention time, a zone alarm will be generated.		
	Associated thermostat	Box for the selection of one of the thermostats that can be managed by the control panel if it is desired to associate a chronothermostat function with the thermal probe.		

Note

The "anemometer" function is only available for Flex5/S expansion terminals with firmware revision above 1.01.
The "temperature probe" function is only available for Flex5/S expansion terminals with firmware revision above 1.02.

Calibration of a "Termperature probe" terminal

Via keypad

Type in code (Installer), PROGRAMMING User functions, View, Zone status, zone

By accessing this section it is possible to carry out a calibration of the terminal by tenth of a degree.

Use keys ◁ and ▷ in order to change the temperature reading.
Press and hold the "**0**" key for at least 2 seconds to reset the calibration of the terminal to default value.

The calibration function is not available from the user menu.

4.3 Outputs

Prime control panels always have 5 outputs available which are constituted by:

- relay output (terminals 1-2-3)
- open-collector output OC1 (terminal 5)
- open-collector output OC2 (terminal 6)
- supervised output AUX1 (terminal 11)
- supervised output AUX2 (terminal 23)

Furthermore, all terminals from T1 to T10 can be used as OC collectors.

The outputs configured on Flex5/SP and Flex5/SU expansion boards are open-collectors (OC).

The output on terminal T5 can be configured as a dimmer type output, to be used as an analog output (industrial standard 0-10V).

The 5 outputs on the Flex5/DAC expansion board can be configured as:

- Relay output
- Triac ON/OFF output (default setting)

- Triac dimmer output

The terminal pairs of the Flex5/DAC OUT1-OUT2 and OUT3-OUT4 are provided with the interlock function which is required in applications with, for example, roller blind motors. Activated via the option, which must be activated for both terminals of the pair, this function has the purpose of inhibiting the simultaneous active status of the associated terminals.

The outputs configured on the keypads are all open-collector outputs.

Table 4.8: Outputs - terminal type

Output	Generic (OC)	Relay	Dimmer
Control panel terminals	any	NO NC COM	None
Expansion terminals	any	None	T5
Flex5/DAC terminals	any	any	any
Keypad terminals	any	None	None
Icon on software			

Via keypad

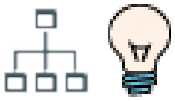
`Type in Code` (Installer), `PROGRAMMING Terminals`, select the terminal concerned configured as controlled output ("**T**")

or

`Type in Code` (Installer) , `PROGRAMMING Outputs` , select the output concerned

This section allows the programming of the various options of the selected output

Via software



To program the output, click on the **System Layout** button and, in the section on the right, select the device (control panel or peripheral) to which the terminal to be configured belongs. Here, by right clicking on the terminal icon you can configure it as an "output". Instead, by double clicking you access the programming phase.

or

Click on the **Outputs** button on the menu on the left, the section on the right will provide a list of all the available outputs and their parameters.

By selecting one of these items it is possible to set the parameters of the single output by clicking on the button.

Note

If the stand-by status of the output is determined by the occurrence of an event, the output will still not return to stand-by status during programming mode.

Table 4.9: Output parameters

Parameter		Software section	Installer menu section
Description	This is the editable output label (device description). By default each output, except for the 3 outputs on the control panel, acquires the description of the device where it is located followed by the relative terminal.	Outputs, selected outputs	`Outputs, "output"`
Category of output	Selection checkbox for operative category of the output. This category will be used by the system for grouping the outputs based on the use assigned by the installer: • generic • gate • lighting • roller blinds • garden sprinkler • climate • household appliances • signalling • fire • intrusion All the categories listed above, except "intrusion", can be assigned to outputs intended for "home automation" use.		
Monostable time	Checkbox where you can set the monostable time if the "Monostable" option is activated.		

Parameter		Software section	Installer menu section
ON icon **OFF icon**	Checkbox for the selection of one of the 80 icons available (refer to "*Available Icons*") that can be associated with the "Output activation / Output deactivation" shortcut assigned to the selected output.		–
Events	Clicking on the **Events** option in the table opens a window containing a list of events which, when they occur will activate the output. You can delete a single event by clicking on **Delete**.	 Outputs	–
Codes	Clicking on the **Codes** option in the table opens a window containing a list of user codes which can activate the output.		–
Normally closed	With this option active, the output is normally closed in stand-by status.	 Outputs, selected outputs, Options	Outputs, "output", Options,
Monostable	This option makes the output a "monostable" output.		
Buzzer - beep 1KHz	When the output is activated, it will generate a 1Khz signal. This can be used to drive a buzzer.		
Flasher - 0.5s ON and 0.5s OFF	When the output is activated, it will generate an intermittent signal (0.5 sec ON and 0.5 sec OFF). This can be used to drive a visual signalling device.		
Do not deactivate on reset	The output will not restore when the activating event ends.		
Switch	Each time an output activation command is executed, it is switched.		
Relay use	The output will operate as a relay output.		
Interlocked	If enabled, this option inhibits the contemporary activation of the associated terminals. It can be enabled only for terminal T01, which will automatically activate the option for the associated T02, and terminal T03, which will automatically activate the option for the associated T04.		

The options listed above allow you to indicate the output-function type.

Note

A declaration as to the type of output which is incoherent with the output itself may cause malfunction.

Monostable

When a "Monostable" output receives an activation signal, it will remain active (On) for the programmed time, regardless of the status of the event which caused its activation.

For some events there are conditions that can force the early deactivation of the activated monostable outputs.

Do not deactivate on reset

If the option is activated, the output will not reset when the event that refers to it ends. It is useful to activate the output with one event and deactivate it with another.

This option applies to "Bistable" outputs only. When a bistable output has this option enabled, its selection as an output when an event is restored generates the output reset and not its activation (refer to "*Programming events*").

This option is useful in situations that require the output to create "memory" of events, the occurrence of which continues to be signalled by the referenced output. In this case, the output is deactivated by a different event which restores it directly to standby (resets the output).

For example, set:

- for the AUX output this option
- on activation of the "AC Mains failure" event, the AUX output
- on reset of the "Valid Code" event for "CODE 1" AUX output

In the event of Mains failure the output will activate but will not deactivate when the Mains power restores. The output will be deactivated only when the "CODE 1" recognition event occurs.

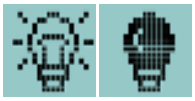
Switch

If this option is enabled, each time an output activation command is carried out the output will switch status. Therefore, if it is deactivated it will activate and vice versa.

A deactivation command will always carry out deactivation.

In order to use this feature with the shortcuts, it is therefore necessary to use the "Activate output" shortcut.

OFF icon



Exclusively via software, in the programming page of the single output, it is possible to select the ON and OFF icons, to be chosen from those available.

These icons will be shown on LCD keypads if On or Off shortcuts are programmed on any function key.

4.3.1 Home-automation outputs

The Prime system allows you to program the outputs for an installation with home automation functions. The outputs can be destined not only for "anti-intrusion" purposes, for example alarm signallers, but also for home-automation purposes like lighting or air conditioning.

To this end, these outputs, appropriately categorised, can be associated with user codes, or with keypads In particular, the installer can program the outputs which can be viewed and activated from a keypad without authentication (i.e. without entering a user code).

If the output is activated when the control panel enters the programming phase, it will not reset to stand-by.

Via keypad

The procedure for access to these outputs depends on the type of keypad in use:

- from a keypad with keys, activate the "Output management menu" shortcut (shortcut n. 21) associated with one of the buttons **F1**, ..., **F4**
- from a touchscreen keypad, access the "Commands" section, then the "Home automation" section.

Via Inim Home App

The "SmartHome" section is dedicated to the home-automation functions of the system.

Inside it are all the available outputs, divided in accordance with the category (lighting, generic, gates, sprinklers, air conditioning, household appliances, roller shutters).

Selecting an individual output, inside each of these sections, allows you to change its status.

Via software

Click-on the **Outputs** button on the menu on the left, the section on the right will provide the list of configured outputs. From the list shown, it is possible to indicate the outputs you want to use for home-automation systems:

- generic
- gate
- lighting
- roller blinds
- garden sprinkler
- climate
- household appliances
- signalling
- fire

Click on the **Keypads** button on the menu on the left, the section on the right will show a list of the configured keypads. On selection of one of the keypads, the section regarding "Details - Domotic outputs enabling" shows a list of the outputs available on the keypad. From the list shown, you can indicate the outputs you want to use for home-automation systems.

Outputs selected in this way can be activated by all persons with access to the keypad, without the need of authentication via entry of a user code.

4.3.2 Output scenarios

A scenario is a configuration of the status of several outputs (activation type, supplied voltage).

These scenarios can be used in the following ways:

- by means of the "Activate output scenario" shortcut (shortcut n.23), associated with the system peripherals
- combined with the activation and restoral of an event

The Prime control panel provides 50 output scenarios, each with a maximum of 30 outputs.

Programming occurs in two phases: the first is the definition of the scenarios, the second is the assignment to the activation and reset of the event.

Via software

Click-on the **Output scenarios** button on the menu on the left, the section on the right will show the list of the 50 available scenarios. By selecting one of them, it is possible to set (at the side of the list) each of the outputs available.

For each of these it is necessary to indicate the output (from those configured) and the activation type:

- **0/100** - percentage value for dimmer outputs or analogue outputs of an expansion
- **ON** - command that activates the output or, if it is a "switching" type output, changes its operating status.
- **OFF** - command that deactivates the output
- **Force ON**, command that activates the output
- **Toggle**, command that changes the activation status of the output
- **Open, 3/4 open**,**1/2 open, 1/4 open, Closed**, command that changes the status of the "roller shutter" type output

Scenarios on events

To assign one of the programmed scenarios to the each event, go to the programming section of the event.

The "Output scenarios" section provides two programming fields for the selection of the scenarios, one relating to activation of the event and the other to its restoral.

4.4 Double zone

The Prime system allows you to connect two different zones to a single terminal. This terminal must be configured as "Double zone input".

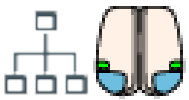
Via keypad

Type in code (Installer), PROGRAMMING Terminals, select the terminal in question configured as input ("**D**") and then select one of the two zones

or

Type-in Code (Installer), PROGRAMMING Zones, select the zone concerned and then select one of the two zones

Via software



To program the zone, click on the **System Layout** button and, in the section on the right, select the device (control panel or peripheral) to which the terminal to be configured belongs.

Here, by right clicking on the icon of the terminal you can configure it as a "double zone". Instead by double clicking you access the programming phase where the boards of "Zone 1" and "Zone 2" are available.

or

By clicking the **Zone**s button in the menu on the left, the section on the right will show a list of all the available zones and their parameters, including those programmed as "double zones". By selecting one of these items it is possible to set the parameters of the single zone by clicking on the button.

4.5 Supervised output (I/O terminal)

A "controlled" output is an output whose status is made known in real time.

Using a terminal configured as "I/O", the terminal combines the configurations of both input and output. By means of the terminal input configuration, the control panel can generate alarm and real time events, which can report the activation status of the output.

Via keypad

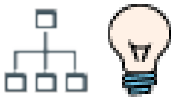
Type-in Code (Installer), PROGRAMMING Terminals, select the terminal in question configured as output ("**T**"), Input/output, select the section to be programmed between "Input" and "Output".

or

Type-in Code (Installer), PROGRAMMING Zones, select the I/O terminal in question in order to program its parameters as an input

Type-in Code (Installer), PROGRAMMING Outputs, select the I/O terminal in question in order to program on its parameters as an output

Via software



To program the output, click on the **System Layout** button and, in the section on the right, select the device (control panel or peripheral) to which the terminal to be configured belongs.

At this point, by right clicking on the icon of the terminal you can configure it as "I/O". By double clicking you access the programming phase of the available "Input" and "Output" boards.

or

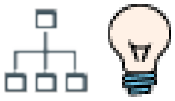
By clicking on **Zones** and **Outputs** on the menu on the left, the section on the right will show a list of the available zones and outputs, including those configured as "I/O" terminals. By selecting one of these items it is possible to set the parameters of the single zone by clicking on the button.

4.6 Virtual terminals

The virtual terminals can be used to manage automation and integration with external systems ("KNX" type), without need of wiring physical terminals.

These are "I/O" type terminals, however, they are purely logical and therefore cannot be wired to any device. They allow detection of the status of an output (virtual, activatable by various control panel events or manually by the user) through the relative (virtual) input whose management is similar to that of a physical terminal. Therefore, this type of input terminal has its own settings, alarm events and real time events. Balancing can only be "Normally Open" or "Normally Closed".

Via software



To program a virtual terminal click on the **System Layout** button and from the section on the right select the "Virtual terminals" option from the list of peripherals.

At this point, by right clicking on the icon of the terminal you can configure it as "I/O". By double clicking you access the programming phase of the available "Input" and "Output" boards.

or

By clicking on **Zones** and **Outputs** on the menu on the left, the section on the right will show a list of the available zones and outputs, including those configured as "virtual terminals". By selecting one of these items it is possible to set the parameters of the single zone by clicking on the button.

Note

The number of virtual terminals added to the system is subtracted from the total number of terminals of each control panel model.

4.7 Wireless terminals

The parameters necessary for the enrolling and programming of wireless terminals will be shown only if the expansion to which they belong has been configured as "Wireless".

These parameters vary depending on the type of wireless device to be configured.

4.7.1 Enrolling wireless devices

The final installation phase of each wireless device is the enrollment and configuration on the control panel.

This phase develops into a procedure that involves either the keypads or the software Prime/STUDIO and the devices to be enrolled.

1. Go to the expansion board field and then to the terminal concerned.
2. Configure the terminal as "Wireless":

Via keypad

`Type in Code` (Installer), `PROGRAMMING Terminals`, select the terminal concerned

Press the number button "**6**"; the word "Wireless" will appear on the last line of the display (pressing the button again will disable the wireless attribute on the terminal).

Via software

Right click on the expansion that was previously added to the configuration and select "Wireless" to configure it as such. The "Wireless" symbol will appear on the expansion image.

Note

If a terminal on the expansion board is configured as "wireless", all the remaining terminals must be configured as "wireless" terminals.

3. Enrolling the terminal:

Via keypad

`Type in Code` (Installer), `PROGRAMMING Terminals`, select the terminal concerned, `Wireless`, `Enroll device`

Enroll the terminal by selecting the type.

Via software

Double-clicking on the configured terminal will open a window where you can program the zone. The lower part of the window shows the "Wireless section", right-click and select the "Wireless" option. Select the type of device, in the "Type" field, then start the guided enrolling process by clicking-on the "Enroll" button.

Table 4.10: Wireless terminal types

Air2 device		Terminal	Via software		Via keypad
Air2-QIR200W		Single	Passive infrared detector		`Single T detector`
Air2-QDT200W		Double	Dual technology detector		`Dual T detector`
Air2-UT100/S		Single	Outdoor terminal		`OutdoorDetector`
Air2-FD100		Single	Smoke detector		`Smoke detector`
Air2-MC200/S		Double	Magnetic contact		`Cont.Magn.MC200`
Air2-MC300	Reed contact	Single	Magnetic contact		`Magnetic Contact`
	Terminal "T1"	Single	Terminal 1 Magnetic contact		`Terminal T1 MC`
	Terminal "T2"	Single	Terminal 2 Magnetic contact		`Terminal T2 MC`
Air2-MC300 outputs	Terminal "T1"	Single	Terminal 1 Magnetic contact		`Terminal T1 MC`
	Terminal "T2"	Single	Terminal 2 Magnetic contact		`Terminal T2 MC`
Air2-MC300 I/O	Terminal "T1"	Double	Terminal 1 Magnetic contact		`Terminal T1 MC`
	Terminal "T2"	Double	Terminal 2 Magnetic contact		`Terminal T2 MC`
Air2-QDT600W	Curtain detector	Double	Curtain detector		`Curtain detector`
	Detector direction	Double	Directional detector		`Curtain direction`

4. Press the **ENROLL** button on the Air2 device.
5. If the device to be enrolled is an output connected to a terminal of any device with an Air2-MC300 output terminal, you must enable the "Broadcast RF" zone option (refer to "*Wireless terminal parameters*").
   Once done, you must step back to the configuration of the terminal and configure it as an "OUTPUT".

Note

The 'Broadcast RF' option must be enabled for each terminal of the Air2-MC300 device concerned.

6. Enroll all remote controls in the same way as you would enroll keys, and select as the reader the one with the same address as the expansion.
7. Set the parameters of the zones, outputs and keypads.

4.7.2 Wireless terminal parameters

Table 4.11: Wireless detector parameters

Parameter		Software section	Installer menu section
Enroll	This section allows you to enroll a wireless detector which has not yet been enrolled on the terminal concerned.	Wireless expansion, Selected terminal, Wireless	Terminals, "terminal", Wireless Enroll device
Type	Type of device to be enrolled ("*Enrolling wireless devices*").		
Remove	Section to delete from the terminal in question.a previously enrolled wireless detector.		Delete device
Sensitivity	The "Wireless" section contains the parameters for adjustment of the detector sensitivity of the previously enrolled devices and their functions. These parameters vary depending on the type of wireless terminal.		Terminal type
Tamper on unused reed relays	Detects tamper on the Air2-MC300 magnetic-contact when both reeds are in stand-by status.	Wireless expansion, Selected terminal, Wireless, Options	–
Disable detector on partition disarming	In order to increase battery life, the infrared sensor will deactivate when the partitions it belongs to are disarmed and will only activate when the partitions it belongs to arm. When the detector is deactivated it will not generate alarms. When the partitions arm, there may be a delay of up to 3 minutes before the detector receives the activation command.		Terminals, "terminal", Options, TamReed/FollPir
Use detector LED	The red LED on the device provides visual signalling of alarm or tamper conditions on the device itself. This option will be enabled on all the terminals of the Air2 device.		Use sensor LED
Broadcast RF	This option assures the activation/deactivation of the output within four seconds of the control panel command. Valid only for terminals T1 and T2 of Air2-MC300 configured as outputs.		Broadcast RF
Bypass tamper	If this option is disabled, open/dislodgement tamper on Air2 devices will not generate the respective events.		DisableTamperWLS WLS
Disable wireless monitoring	Enabling this option (disabled by default), disables monitoring on the wireless detector. In the event of the loss of the specific detector, no event will be generated and no fault signal will be signalled on the keypad.		No superv. WLS

Detector sensitivity

Table 4.12: Wireless detector sensitivity

Terminal type	Parameter	Via software	via keypad
○ Infrared ○ Smoke detector	Detector sensibility: • PIR: from 1 (least sensitive) to 10 (most sensitive) • Smoke detector: from 0.08 dB/m to 0.15 dB/m (default)	Sensitivity	Sensitivity
○ Passive infrared detector ○ Outdoor terminal ○ Dual technology detector ○ Curtain detector	PIR detector sensitivity Varies from 1 (least sensitive) to 10 (most sensitive). The default setting is 6.	Sensitivity	Sensitivity
○ Dual technology detector ○ Curtain detector	Microwave detector sensitivity. Varies from 1 (least sensitive) to 10 (most sensitive). The default setting is 6.	Microwave sensitivity	MicrowaveSensit.
○ Dual technology detector ○ Curtain detector ○ Outdoor terminal	Tamper sensor sensitivity. Varies from 1 (least sensitive) to 10 (most sensitive). The default setting is 3.	Tamper sensitivity	Shock Sensit.

Terminal type	Parameter	Via software	via keypad
○ Dual technology detector ○ Curtain detector	Anti-mask detector sensitivity Varies from 1 (least sensitive) to 10 (most sensitive). The default setting is 3.	Anti-mask sensitivity	Shock Sensit.
○ Magnetic contact	Selection of the magnetic reed contact: • Magnet - long side, for detection using the long side of the magnetic contact. • Magnet short side - for detection on the short side of the magnetic contact. • Both magnets - for detection using both sides of the magnetic contact.	Reed relay type	MagnetLongSide MagnetShortSide BothMagnets
○ Magnetic contact	Shock detector sensitivity Varies from 1 (least sensitive) to 10 (most sensitive). The default setting is 1.	Shock sensor	Shock sensitiv.
○ Magnetic contact	Maximum angle within which the movement is not signalled, from 1 (minimum tilt) to 10 (about 90 ° from the resting position); 1 is the default preset value.	Tilt	Tilt
○ Magnetic contact	If the device is set to detect shock waves (bangs or vibration), this parameter refers to the time within which the shock waves must be detected. If the device is configured to detect tilting, this parameter refers to the time with which the angle variation will be signalled. from 1 to 125 (100msec or sec)	Shock/Tilt time	Time inclination
○ Passive infrared detector ○ Outdoor terminal ○ Dual technology detector ○ Curtain detector ○ Magnetic contact	Checkbox to disable the corresponding detector	Disabled	–

Real-time

For each configured wireless device the software provides a direct software- to- device connection. Once activated, the current values of the following characteristics are displayed:

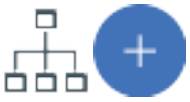
Reading level	The value read by each detector of the device is displayed on a bar which indicates the alarm threshold by means of a colour change from green to red.
Signal reception level	This series of notches represents the reception level of the wireless signal of the device as received by the Air2-BS200 transceiver.
Battery charge level	Percentage of the device battery charge.
RF analysis	Function to monitor the variation of the signal transmitted by the device and the background noise detected through time.

Chapter 5 Programming peripherals

5.1 Keypads

5.1.1 Enrolling keypads on BUS

Via software



Once the solution for the system to be designed has been opened, click on the **System Layout** button on the menu on the left. Then click on the "Add device to BUS" button in the section on the right.

A window will open where you can select the keypads to be configured and added to the configuration.

In the section on the left the number increases in correspondence with the keypads button.

To remove a keypad from the structure, it is necessary to access the programming section by clicking on the relative key on the menu on the left then, from the list shown, click on the **Delete** button in correspondence with the line of the keypad in question.

Via keypad

`Type in Code` (Installer), `PROGRAMMING Keypads, Enable/Disable`

This section allows you to add/remove keypads from the configuration, by means of keys ▣ and □.

5.1.2 Enrolling wireless keypads

The Prime system provides guided procedures (wizards) for the enrolling of wireless keypads.

Via software

Click on the **Keypads** button on the menu on the left, the section on the right will show a list of the configured keypads.

By selecting one of these keypads, the "Keypad type" parameter will allow the association of the "Wireless" attribute to the selected keypad. This operation visualizes:

- the **Enroll** button, which allows the start of the enrolling procedure.
- the "Wireless monitoring" section
  Pressing the **Start** button initializes the monitoring process on the variation of the signal transmitted by the device and background noise detected over time.

Via keypad

`Type in Code` (Installer), `PROGRAMMING keypads, ChoosePeripheral "keypad", Wireless`

Once the **OK** button is pressed, it is necessary to work through the menu options and enroll the keypad.

5.1.3 Keypad programming

Via software

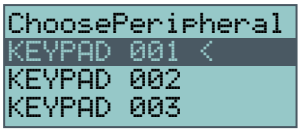
Click on the **Keypads** button on the menu on the left, to access two programming sections on the right:

- "Configured keypads", with a list of all the configured keypads. By selecting one of these items it is possible to set the parameters of the single keypad by clicking on the button.
- "Keypad parameters", section with parameters common to all the keypads.

Via keypad

`Type in code` (Installer), `PROGRAMMING Keypads, ChoosePeripheral`

This section provides a list of the available keypads.



Alongside the description of the keypads the following symbols may appear:

- "<", indicating the keypad in use
- "*", indicating a keypad configured on the I-BUS

From this list it is possible to select a keypad for the programming of parameters.

Keypad settings

The keypads of the Prime system also provide a section where you can set their parameters, for the customization and optimization of their use.

The complete description of the parameters in this section can be found in "*Keypad and display settings*" in the user manual.

5.1.4 Keypad parameters

Table 5.1: Parameters common to all keypads

Parameter		Software section	Installer menu section
Wrong PIN keypad lockout	If a wrong code is typed-in at a keypad more than 5 times in succession, the keypad will lock for 10 minutes. The count restarts from 10 minutes in the case of control panel reset or entry into programming.	Keypad parameters	Parameters Keypad lockout
View open zones	The keypad will show the descriptions of any zones not in standby status when the partitions disarm. Any auto-bypassable zones will be shown in negative.		View open zones
Show scenario	The second line on the keypad display, on the left side, will show the description of the active scenario.		Show scenario
Message repetitions on voice keypad	This refers to the number of times event messages are played on the keypad (only for keypads with speakers). The playback phase can be stopped by pressing any button.		Parameters, Other parameters, LocKpadMessTimes
Press key to end playback	If this option is enabled, message playback can be interrupted solely by pressing any button.		LocKpadMessTimes, "255"

Table 5.2: Parameters for single keypads

Parameter		Software section	Installer menu section
Description	Description of the keypad, customizable by the installer.	Configured keypads, selected keypad	Keypads, ChoosePeripheral, "keypad"
Keypad type	Checkbox for the selection of the keypad type: • Keypad with display and keys • Touch-screen keypad • Wireless keypad		–
Partitions	Section for the selection of the partitions the keypad can operate on.	Configured keypads, selected keypad, General	Keypads, ChoosePeripheral, "keypad"
Disable temperature visualization	If this option is enabled, the room temperature will not be flashed on the display. This option is valid only for keypads equipped with thermometers.	Configured keypads, selected keypad, General, Details, Other parameters	Keypads, ChoosePeripheral, "keypad", Options, Temperature off
Disable audible entry-time signal	This option enables/disables the buzzer during partition entry-time		NoEntryTimeSign.
Disable audible exit-time signal	This option enables/disables the buzzer during partition exit-time		NoExitTimeSignal

Parameter		Software section	Installer menu section
Audible signal on terminal T1 output	This option enables/disables the buzzer when the keypad terminal T1 is activated as an output.	Configured keypads, selected keypad, General, Details	Beep on output
Disable chime	This option enables/disables the buzzer that signals the violation of the bell zone relative to the keypad.		Disable chime
LED OFF in stand-by	If enabled, in the event of at least 40 seconds inactivity on the keypad, the respective LEDs will switch off.		LED OFF in stand-by
Bypass wireless supervision	If enabled, this option inhibits the monitoring function the control panel must perform on the wireless keypad.		NO Superv. WLS
Bypass tamper	If enabled, this option inhibits signalling on the control panel of wireless keypad tamper.		Disable tamp. WLS
Enablement of home-automation outputs	Section for the selection, from the outputs available, of outputs for "home-automation" purposes, accessible without code entry (refer to "*Home-automation outputs*").		-
Thermostats managed by keypad	This section lists all the potential thermal probes of the system, both isolated ones and those integrated in the keypads, with those in configuration highlighted. By means of the relative check boxes, it is possible to select which of the probes is reachable from the keypad being programmed.		Keypads, ChoosePeripheral, "keypad", TemperatureSens.
Thermostat on keypad	This key directly accesses the programming section of the "Thermostat ON" event	Configured keypads, selected keypad	Events, Thermostat ON
Valid code at keypad	This key directly accesses the programming section of the "Valid code at keypad" event		Events, Valid Code
Temperature adjustment	This parameter allows entry of the effective value of the room temperature detected by an external thermometer. This value replaces the one detected by the keypad and allows the correction of the temperature sensor on the keypad concerned (valid for keypads with temperature sensors only). The entered value must be expressed in °C decimals (for example, type in 252 if the temperature is 25.2 °C).	-	Other parameters, Temp. adjustment

Table 5.3: Shortcuts on single keypad

Parameter			Software section	Installer menu section
Shortcuts		For each key, from F1 to F12, it is possible to program the type of shortcut selectable from among all the available shortcuts. In the case of programming touch-screen keypads, positions F1 - F12 refer to the positions in the list available in the "Scenarios" section of the keypad being programmed.	Configured keypads, selected keypad, General, Details, Shortcut	Keypads, ChoosePeripheral, "keypad", F1/4KeyShortcuts
Shortcut parameter		It is necessary to specify a further parameter for each shortcut: • **Execute Arm/Disarm**, the parameter is one of the scenarios • **Activate output**, the parameter is an output • **Deactivate output**, the parameter is an output • **Activate output scenario**, the parameter is one of the scenarios • **Panic**, this parameter is one of the panic events		F1/4KeyShortcuts, "Fx", Type
Shortcut options	**Requires code**	If this option is enabled and a user selects the shortcut by pressing the relative function key, before activation of the shortcut occurs, the system will request entry of a user code . If the user code is valid the shortcut will be applied.		F1/4KeyShortcuts, "Fx", Options, Requires code
	Code entry in the event of security risk	If this option is enabled and the selected shortcut involves a scenario that disarms a partition, or switches a partition from Away mode to Stay mode, the security of the system will obviously be at risk, therefore, the system will request entry of a valid code.		SecurityRiskCode

Parameter			Software section	Installer menu section
	Requires confirmation	If this option is enabled when the user selects the shortcut via the relative function key, the system will request confirmation before actually activating the shortcut, confirmation is achieved by simply pressing the key. This option helps the user avoid accidental activations. This option is not valid on touch-screen keypads.		Confirm
Disable exit time signal		If this option is enabled and the application of an arming scenario is programmed for the relative shortcut, the keypad will not sound the exit time when the specific scenario is applied. This option is disabled by default.		NoExitTimeSignal
Disable entry time signal		If this option is enabled and the application of an arming scenario is programmed for the relative shortcut, the keypad will not sound the entry time when the specific scenario is applied. This option is disabled by default.		NoEntryTimeSign.

The "Listen-in" and "Arming status" shortcuts will have no effect if requested at a keypad.

In the case of programming touch-screen keypads, the only type of shortcut that functions is "Arm/disarm".

5.1.5 Graphic interface of the touch-screen keypads

Exclusively via software it is possible to program the graphic interface of the touch screen keypads and the graphic maps that can be viewed on it.

Once the keypad has been selected, it is necessary to select "Touch-screen keypad" as its type. Together with the "General" section common to all types of keypads, the following sections are shown:

- "Graphics", for the graphic interface setup (backgrounds, buttons, icons)
- "Maps", to configure the graphic maps accessible in the "Maps" section in the "APPs" section

In order to configure the modified parameters on the keypad, it is necessary to have a link between the PC to the USB port of the keypad.

Table 5.4: Touch-screen keypad parameters

Parameter	
Communication port	Selection of the connection port with the touch-screen from among those found by the PC.
Refresh	Button for the connection upgrades found by the PC.
Model	Selection of the touch-screen keypad model.
Available Skins	Selection of one of the themes available for the touch-screen graphics.
Background	Button to display only the background of the graphics in the image below.
All	Button to display the graphics complete with buttons in the image below.
Default	Button to visualize the default graphic for the selected theme.
Clean	Button to cancel the selected graphic.
Write skin	Button to set the selected skin on the keypad.
Write icons	Button to set the icons selected for the buttons on the keypad.

The image in the lower part of the 'Graphics' section allows the visualization of the graphic selected for the keypad.

It is possible to load an image from the PC by double-clicking on the background or button icons.

The requirements for the images are:

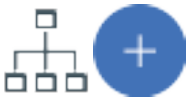
- for 4,3" display
  - - the background file must be a JPG file with a maximum size of 120 kbytes, 480x272 pixels
  - - each of the 8 main buttons must be a JPG file with a maximum size of 12 kbytes, 109x88 pixels
- for 7" display
  - - the background file must be a JPG file with a maximum size of 120 kbytes, 800x480 pixels

- - each of the 8 main buttons must be a JPG file with a maximum size of 12 kbytes, 109x88 pixels

5.2 Proximity readers

5.2.1 Enrolling readers

Via software



Once the solution for the system to be designed has been opened, click on the **System Layout** button on the menu on the left. Then click on the "Add device to BUS" button in the section on the right.

A window will open where it is possible to select the readers to configure and then add to the configuration.

In the section on the left the number increases in correspondence with the Readers button.

To remove a reader from the structure, access the programming section by clicking on the relative key in the menu on the left then, from the list displayed, click on the **Delete** button that corresponds to the line of the reader to be deleted.

Via keypad

`Type in code` (Installer), `PROGRAMMING Readers, Enable/disable`

In this section it is possible to add/remove readers from the configuration, by means of keys  and  .

5.2.2 Programming of proximity readers

Via software

Click on the **Proximity readers** button on the menu on the left to access two programming sections on the right:

- "Configured readers", with the list of all the configured readers, whether they are standalone peripherals or integrated into keypads.
  Selecting one of the options will allow you to configure the parameters of the single reader by clicking on the  button.
- "Reader parameters", section containing the parameters common to all the readers.

Via keypad

`Type in code` (Installer), `PROGRAMMING Readers, ChoosePeripheral`

In this section, it is possible to program the various parameters of each reader after selecting it, regardless of whether it is a standalone peripheral or integrated into a keypad.

5.2.3 Reader parameters

Table 5.5: Parameters common to all readers

Parameter		Software section	Installer menu section
Programming the proximity reader address	Section for the programming of the proximity reader addresses.	 Reader parameters	`Readers, Prog. address`
Address LED codes	Section for the visualization of how the addresses will be reproduced on the LEDs.		/
Reader Buzzers OFF	No reader buzzers will emit audible signals when the entry time, exit time, output time or pre-arm time is running.		`Parameters, ReaderBuzzersOFF`

Table 5.6: Parameters of single reader

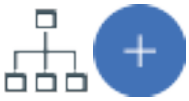
Parameter		Software section	Installer menu section
Description	This is the name used to identify the reader, customizable by the installer.	Configured readers, selected reader	Readers, Chooseperipheral, "reader"
Partitions	Section for the selection of the partitions the reader can operate on.		
Type	It is possible to assign a shortcut type, selectable from those available, to each of the LEDs (refer to "*Default Shortcuts*"). The type of activatable shortcut is to be chosen in accordance with the reader model, whether standalone or integrated, as the activation of some shortcuts depends on the presence of a keypad with a display.		
Parameter	It is necessary to specify a further parameter for each shortcut: • Execute Arm/Disarm, the parameter is one of the scenarios • Activate output, the parameter is an output • Deactivate output, the parameter is an output • Activate output scenario, the parameter is one of the scenarios • Panic, the parameter will be one of the panic events • Access shortcuts to menus and data viewing on keypad displays, the parameter is the reference access code	Configured readers, selected reader, Shortcut	Readers, ChoosePeripheral, "reader", Shortcut, Type
Valid key at reader	Button to access directly the programming section of the "Valid key at reader" event	Configured readers, selected reader	Events, ValidKeyAtReader

In the case of a reader simulated by the Air2-BS200 transceiver, the parameters of the wireless system will be available in the section reserved for wireless receivers.

5.3 Expansions

5.3.1 Enrolling expansions

Via software



Once the solution for the system to be designed has been opened, click on the **System Layout** button on the menu on the left. Then click on the "Add device to BUS" button in the section on the right.

A window will open for the selection of the expansions to be configured and then added to the configuration.

In the section on the left, the number is increased in correspondence with the expansions button.

To remove an expansion from the structure, access the programming section by clicking on the relative button in the menu on the left then, from the list displayed, click on the **Delete** button in correspondence with the line of the expansion in question.

Via keypad

Type-in Code (Installer PIN) , PROGRAMMING Expansions, Enablements

In this section it is possible to add/remove expansions from the configuration, by means of keys ▣ and □.

5.3.2 Programming the expansion boards

Via software

By clicking on the **Expansions** button on the menu on the left, the section on the right will show a list of the configured expansions.

Selecting one of the options will allow you configure the parameters of the single expansion by clicking on the ☜ button.

Via keypad

Type in Code (Installer), PROGRAMMING Expansions, ChoosePeripheral

This section allows the programming of the various options of the selected expansion.

5.3.3 Expansion parameters

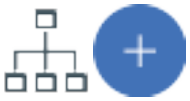
Table 5.7: Individual expansion parameters

Parameter		Software section	Installer menu section
Description	Description string of the expansion (to be customized by the installer).	Configured expansions, selected expansion	Expansions, ChoosePeripheral, "expansion"
Sound on output	This option that enables/disables the buzzer of the selected expansion when the relevant T1 terminal is activated as an output.		Expansions, ChoosePeripheral, "expansion", Options
Disable tamper protection	This option enables/disables tamper on the peripheral (enabled by default).		

5.4 Sounderflashers

5.4.1 Enrolling sounder/flashers

Via software



Once the solution for the system to be designed has been opened, click on the **System Layout** button on the menu on the left. Then click on the "Add device to BUS" button in the section on the right.

A window will open where it is possible to select the sounders/flashers to be configured and added to the configuration.

In the section on the left the number increases in correspondence with the sounders/flashers button.

To remove a sounder/flasher from the structure, click on the relative button on the menu on the left to access the programming section, then, from the list that appears, click on the **Delete** button that corresponds to the line of the sounder/flasher in question.

Via keypad

`Type in Code` (Installer), `PROGRAMMING Sounders/Flashers, Enable/Disable`

In this section it is possible to add/remove sounders/flashers from the configuration by means of keys ▣ and □.

5.4.2 Enrolling wireless sounder/flashers

The Prime system provides wizards for the enrolling of wireless sounder/flashers.

Via software

By clicking on the **Sounders** button in the menu on the left, it will be possible to select a sounder/flasher from the "Programming - Configured sounders/flashers" section.

The checkbox next to that of the sounder/flasher description allows the selection of the sounder/flasher type:

- Hardwired sounder/flasher
- Indoor wireless sounder/flasher
- Outdoor wireless sounder/flasher

If "wireless" is selected as the sounder/flasher type, the programming section will provide the **Learn** button that initializes the enrolling process.

Via keypad

`Type in Code` (Installer), `PROGRAMMING Sounders, ChoosePeripheral, "sounder/flasher", Wireless`

Once the **OK** button has been pressed, it is necessary to work through the menu steps to enroll the sounder/flasher.

5.4.3 Programming sounders/flashers

Via software

Clicking-on the **Sounders** button on the menu on the left accesses two programming sections on the right:

- "Configured sounders", with a list of all the configured sounder/flashers.
  By selecting one of these options it is possible to set the parameters of the single sounder/flasher by clicking on the button.
- "Sounder pattern", section with the programming parameters of the tone types (pattern).
  8 modifiable patterns are available.

Via keypad

`Type in code` (Installer), `PROGRAMMING Sounders, ChoosePeripheral`

This section provides a list of the available sounders/flashers. From this list it is possible to select a sounder/flasher in order to program the parameters.

Accessing the sounders section will, for each configured sounder, allow you to initially define

- "Description", editable field for the name of the sounder/flasher
- "Events", that is, a selection of the events that activate the sounder
- "Type of sounder", to indicate whether the selected sounder type is
  - wired, for on-BUS sounders
  - indoor wireless
  - outdoor wireless

5.5 On BUS sounder parameters

After selecting a 'wired' sounder connected to the control panel via BUS, the programming software will provide the following parameters:

Table 5.8: Single hardwired sounder/flasher parameters

Parameter		Software section
Read sounder/flasher	By clicking-on the **Read sounder** and **Write sounder** buttons it will be possible to program the sounder/flasher parameters.	 Configured sounder/flasher, Hardwired sounder/flasher, Sounder/Flasher parameters
Write sounder/flasher		
Default	Button to reset the factory default data	
I-BUS loss signal delay	This is the time the sounder/flasher must wait before signalling the loss of the I-BUS signal (expressed in minutes).	
Version	This is the firmware version of the sounder/flasher board.	
Sounder/Flasher address	Checkbox for the selection of the address of the sounder/flasher on the BUS.	
I-BUS loss **Activation of LED input** **Power failure** **Open cover signalling** **Foam tamper signalling** **Blow-torch tamper signalling** **Horn fault** **Battery status**	The check boxes in this section allow the association of one or more signals to each of the sounder/flasher events. The available signals are aligned with the wording of each event: • FAULT output • TAMPER output • Red STATUS LED • Green PRG LED • Flasher • Sounder	
Audible signalling	Selection of the type of sound produced by the magnetodynamic horn.	
Maximum sound (audible signal) time	This is the maximum time the sounder/flasher is allowed to emit the audible signal, however, the visual signals will continue until the device resets.	
STATUS LED ON	If this option is selected, the red STATUS LED will turn On solid.	
Flashes/minute	Selects the flash rate on the flasher.	
Enable flasher LED input	Option to allow blinking on the STATUS LED and PRG LED activated by the LED input.	
Monitor IBUS	If enabled, after control panel reset the BUS will be monitored for one minute, its status will be signalled by the green PRG LED: • On solid - BUS disconnected • 1 flash per second - BUS connected but sounder/flasher not enrolled • 2 flashes per second - BUS connected and sounder/flasher enrolled	

Parameter		Software section
TAMPER and FAULT outputs	This option allows the selection of the type of contact (normally open or closed) of the outputs during stand-by status.	
Temperature compensation	If the internal temperature of the sounder/flasher indicated in the "Real-time" section is incorrect, it is possible to use this section to set the real temperature value and correct the parameter via the **Compensation** button.	 Configured sounder/flasher, Hardwired sounder/flasher, Temperature compensation
Sounder/flasher LED activations	Each sounder/flasher LED (PRG or STATUS) provides 5 options which allow you to select the control panel event that will activate the LED.	 Configured sounder/flasher, hardwired sounder/flasher
Sounder/flasher cut off events	A maximum of 5 options allow you to select a control panel event that will deactivate the sounder and flasher.	
Inversion	If the option is disabled, the LED or sounder and flasher will switch off when activation of the event occurs. If the option is enabled, the LED or sounder and flasher will switch off when deactivation of the event occurs.	

5.5.1 Wireless sounder/flasher parameters

After the selection of a wireless sounder/flasher, the programming software provides the following parameters in addition to the parameters common to all "wired" sounder/flasher units:

Table 5.9: Single wireless sounder/flasher parameters

Parameter		Software section
Communication loss signalling	It is possible to select when the sounder/flasher is to activate in the event of communication loss with the control panel: • never • only when wireless jamming disturbs communication • each time communication is lost In the latter two cases it is necessary to indicate the "**Wireless supervision time**", in minutes, after which if the communication continues to be absent the sounder/flasher will activate. The activation type can be defined in the same section (selection of the sound, duration, flash sequence, activation of the STATUS and PRG LEDs).	 Configured sounder/flashers, selected sounder/flasher, Sounder/flasher parameters
Enable anti-tamper signalling	Options that enable the signalling of tamper or low battery charge	
Enable foam tamper signalling		
Enable battery inefficient signalling		
PRG/STATUS LED activation	Parameter to indicate the source (control panel or the sounder/flasher itself) of the activation of the PRG and STATUS LEDs. The selection of one of the two LED activation sources excludes the other.	
Default	Button to reset the factory default data	
Sounder/flasher LED activations	Each sounder/flasher LED (PRG or STATUS) provides 5 options which allow you to select the control panel event that will activate the LED.	 Configured sounder/flasher, selected sounder/flasher
Sounder/flasher cut off events	A maximum of 5 options allow you to select a control panel event that will deactivate the sounder and flasher.	
Inversion	If the option is disabled, the LED or sounder and flasher will switch off when activation of the event occurs. If the option is enabled, the LED or sounder and flasher will switch off when deactivation of the event occurs.	

5.5.2 Real-time on BUS sounder/flasher

For each of the configured sounder/flasher units, the software provides a direct software-to-sounder/flasher connection.

Clicking on the **Real-time** option displays the following real-time values of the sounderflasher:

Table 5.10: Single sounder/flasher parameters

Parameter		Software section
Battery voltage	Voltage of the internal battery of the sounder/flasher.	 Configured sounder/flasher, hardwired sounder/flasher, Real-time
Line voltage	Voltage detected on terminals "**+**" and "**-**" of the sounder/flasher.	
Temperature	Internal temperature of the sounder/flasher detected by the thermal probe.	
Foam left/right	Values detected by the anti-foam sensor (left/right).	
Tamper	Value detected by the open-panel tamper sensor.	

5.5.3 Real-time wireless sounder/flasher

Pressing the **Start** button initiates a 4-minute countdown during which the current values of various features of the wireless sounder are displayed.

Level / foam threshold
Level / tamper threshold

From the bars it is possible to read the values (from 1 to 100) detected by the antifoam and tamper sensors.

Using the boxes alongside, it is possible to modify the alarm threshold. The **Default** button resets the values to the factory settings.

Monitoring the wireless sounder/flasher

In this section, the monitoring window lists the parts of the sounder/flasher whose status is represented by icons/LED:

LED	Colour	Status
Tamper	Green	Sounder/flasher not in tamper status
	Red	Sounder/flasher in tamper status (open or dislodged)
Battery inefficient	Green	Battery charged
	Red	Battery charge low (below 40%)
Sounder active	Green	Audible signalling Off
	Red	Audible signalling On
Flasher active	Green	Visual signalling Off
	Red	Visual signalling On
STATUS LED ON	Green	STATUS LED off
	Red	STATUS LED On
PRG LED ON	Green	PRG LED off
	Red	PRG LED On
Signal reception level	This series of notches represents the reception level of the wireless signal of the device as received by the Air2-BS200 transceiver.	
Battery charge level	Percentage of charge of the sounder/flasher battery	

Monitoring wireless

This software section starts a monitoring phase on the variation of the signal transmitted by the device and background noise detected over time.

5.5.4 Programming the patterns

By selecting the system "Sounder" category, it is possible to program the patterns, sequences of visual and audible signalling, for all the sounders in the configuration.

Table 5.11: Pattern parameters

Parameter			Software section
Description	Description of the pattern to program.	• Burglary • Burglary low volume • Fire • Tamper • Pre-alarm • Automation • Squawk • Chime	 Configured sounder/flashers, Sounder/flasher pattern
Tone	Sound of the audible signal	5 types available	
Sounder duration	Sounder activation time	from 1 to 127 seconds or from 1 to 127 minutes	

Parameter			Software section
Volume	Sound level of the sounder/flasher.		
Flash type	Checkbox for the selection of the flash rate (number of flashes per minute).	• 36 flash/min • 46 flash/min • 56 flash/min • ON solid	
Flasher duration	Flasher activation time	from 1 to 127 seconds or from 1 to 127 minutes	
Activate sounder	Enable/Disable sounder activation		
Activate flasher	Enable/Disable flasher activation		
Activate STATUS LED	Enables/Disables the activation of the red STATUS LED.		
Activate PRG LED	Enables/Disables the activation of the PRG green LED output.		
Activate TAMPER output	Enable/Disable activation of TAMPER output		
Activate FAULT output	Enable/Disable activation of FAULT output		
Test	Buttons to start and stop a test on the pattern selected via the audio output of the PC in use and the image of the sounder/flasher on the left of the buttons.		
Stop			
Test sounder/flasher pattern	Buttons to start and stop a test on the selected pattern on the sounder/flasher selected from the list provided. This test requires an active connection with the control panel.		

Default

The pattern programming section has a dedicated button in its menu bar for the reinstatement of the pattern settings.

The following default patterns are available, each of which can be modified:

Description	Sounder/flasher	Sounder duration	Tone	Volume	Flasher	Flasher duration	Flash type	STATUS / PRG LED
Burglary	ON	3 minutes	1	high	ON	3 minutes	56	OFF
Burglary low volume	ON	3 minutes	1	medium / low	ON	3 minutes	56	OFF
Fire	ON	3 minutes	3	high	ON	3 minutes	56	OFF
Tamper	ON	3 minutes	1	high	ON	3 minutes	36	STATUS ON
Pre-alarm	ON	30 seconds	1	low	ON	30 seconds	36	OFF
Automation	ON	3 seconds	1	medium / low	OFF			PRG ON
Signalling	ON	1 second	5	low	ON	3 seconds	ON solid	OFF
Chime	ON	3 seconds	4	low	ON	3 seconds	ON solid	OFF
Total cut off	OFF	/	/	low	OFF	/	/	OFF

5.6 Wireless transceivers

The Prime/STUDIO software has a section that allows the viewing of all the enrolled wireless devices, and also the setting up of the programming parameters of the wireless transceivers.

Via software

Click on the **Wireless transceivers** button on the menu on the left, the section on the right will shows a page divided in sections, a section for each configured transceiver.

Each sub-section shows:

- the transceiver model
- the firmware version of the transceiver board
- the transceiver parameters
- a list of devices enrolled by the transceiver
  for each device it shows:
  - the Icon
  - the terminals (where present)
  - the serial number
  - the model

Table 5.12: Menu bar for wireless transceivers

Button		Function
	**Read**	Buttons for reading from and writing on the control panel the data relative the configuration of the wireless transceivers.
	**Write**	
	This button starts an operation which attenuates (6db) the wireless signal transmitted by the transceivers for 5 minutes. During this period the installer can carry out tests on the stability of the RF connection in conditions of poor signal levels.	
	**Clone remote-control keys**	This button starts the guided procedure for cloning the wireless keys enrolled by the transceiver of the selected board. The guide allows you to indicate which transceiver, from those selectable, the cloned keys will be assigned to.

5.6.1 Enrolling simulated wireless readers

During the enrolling phase the Air2-BS200 wireless transceiver is integrated into the Prime system, by simulating:

- a reader, with the address programmed via the module itself (ADD), by means of buttons P1 and P2 on the PCB;
- up to 10 expansion boards, at addresses ADD, ADD+1, ... ADD+9, to manage the terminals to be configured via the "System Layout" section of the Prime/STUDIO software.

Via software

Once the reading procedure has been completed at the control panel, by clicking on the **Proximity readers** button on the menu on the left, a list of configured readers will be provided in the section on the right.

The reader simulated by the Air2-BS200 transceiver is the one with the "ADD" address configured by the module itself.

Via keypad

`Type-in Code (Installer PIN) , PROGRAMMING Readers, ChoosePeripheral`

In the list of configured readers, the reader simulated by an Air2-BS200 has a "W" at the end of its description.

5.6.2 Enrolling simulated wireless expansions

Via software

To identify an expansion as "wireless", it must first be configured as described above, in the same way as the hardwired expansions.

Once configured, click on the **System Layout** button, the section on the right will show the diagram of the terminals of the entire system.

Right click on the expansion previously added to the configuration and select "Wireless" to classify it as such.

The "Wireless" symbol will appear on the expansion image. The configuration is completed by enrolling the wireless devices.

Via keypad

`Type in Code` (Installer), `PROGRAMMING Terminals`, select a terminal of an expansion

The "**6**" button button enables the wireless attribute on the terminal (and consequently on the entire expansion). The "Wireless" string will be shown on the bottom line of the display.

```
Terminals 12345
EXPAN. XYZ IIII
Expans. XYZ T01
Wireless
```

Pressing the "**6**" button again will disable the wireless attribute on the terminal (and consequently the entire expansion).

5.6.3 Programming transceivers

Table 5.13: Wireless transceiver parameters

Parameter		Software section	Installer menu section
Channel	Section for the selection of the wireless communication channel used by the transceiver that simulates the reader being programmed: • **Channel 001**, 868.1MHz • **Channel 002**, 868.3MHz • **Channel 003**, 868.5MHz	Home, Wireless transceivers, Parameters	`Readers, ChoosePeripheral, "reader", Channel`
Disable tamper protection	This option disables the tamper signal of the Air2-BS200 transceiver.		`Readers, ChoosePeripheral, "reader", Options, Disable Tamper`
Disable the Rolling Code	This option disables the use of a rolling-code algorithm for the transmission of wireless commands via the module Air2-BS200. If the same remote control is used on multiple systems, the disabling of this feature may be useful to the installer.		`Readers, ChoosePeripheral, "reader", Options, RollingCodeDisab`

5.6.4 Wireless device data check

The Prime/STUDIO software has a section where, after a direct connection to the control panel, it is possible to check the configuration of the wireless devices the control panel actually recognizes compared to the configuration set during programming.

Click-on the **Maintenance** button on the menu bar. The page on the right provides different sections, selectable from the menu, dedicated to different categories of wireless devices.

Click on the **Check consistency** button of each section to initiate a cross-check between the devices in the control panel configuration, those recognized as wireless and those present on the wireless transceiver.

The outcome of this check will be displayed with a list of devices and their respective configurations:

- "In configuration", for a device in the control panel configuration
- "Wireless", for a device recognized as a wireless device
- "On transceiver", for a device in the configuration of one of the wireless transceivers

If an inconsistency is highlighted, the process provides a **Fix** button which restores a coherent situation after a request for confirmation.

The following table lists the various configuration conditions of the devices the software detects and, in the case of inconsistent conditions, the correction proposed by the **Fix** button:

Table 5.14: Wireless configuration consistency

Device condition detected	Combination of configurations			Outcome	
	In configuration	Wireless	On transceiver	Test result	Correction
Device is not configured and not detected (potential configuration available)	No	No	No	Fix	Device unenrolled from each configuration
Device enrolled by the transceiver but not in the control panel configuration.	No	No	Yes	Fix	Wireless device both in the control panel and transceiver configurations
Wireless device detected but not in the control panel configuration	No	Yes	No	Fix	Device unenrolled from each configuration
Wireless device detected and enrolled by the wireless transceiver but not in the control panel configuration	No	Yes	Yes	Fix	Wireless device both in the control panel and transceiver configurations
Device wired and in configuration	Yes	No	No	Ok	/
Device in both the control panel and wireless transceiver configurations but not detected	Yes	No	Yes	Fix	Wireless device both in the control panel and transceiver configurations
Wireless device in the control panel configuration only	Yes	Yes	No	Fix	Device unenrolled from each configuration
Wireless device configured correctly	Yes	Yes	Yes	Ok	/

5.7 Temperature sensors and chronothermostats

The temperature sensors that can be connected to the Prime system are of different types:

- stand-alone module connected to the SenseTH100/H BUS
- Air2-SenseTH100/W wireless stand-alone module
- thermal probe integrated in a keypad connected to BUS
- NCT thermal probe connected to one of Flex5/S expansion terminals

A temperature module/probe, both wired or wireless, or even a keypad probe, are identified by the control panel during the programming phase with the chronothermostat function.

On the other hand, temperature probes connected to one of the terminals of an expansion module are enrolled as zones that can generate alarm or tamper events and must be programmed as such. Successively, it is possible to associate to these one of the thermostats to be configured (refer to "*Detector type*").

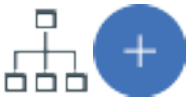
5.7.1 Enrolling temperature sensors

The enrolling of a temperature sensor varies depending on which device the sensor is connected to or a part of.

Stand-alone module

During the programming phase, a module/temperature probe, both wired and wireless, is identified by the control panel with the chronothermostat function.

Via software



Once the solution for the system to be designed has been opened, click on the **System Layout** button on the menu on the left. Then click on the "Add device to BUS" button in the section on the right.

A window will open where you can select the modules to be configured and add them to the configuration.

In the section on the left the number increases in correspondence with the button of the thermostats.

Click on the **Thermostats** button on the menu on the left, the section on the right will provide the list of configured thermostats.

Selecting one of the thermostats provides a box for the selection of the type of module/probe:

- Wired temperature probe, for the modules connected to the BUS
- Wired temperature probe, in this case the **Enroll** button appears, which allows the start of the enrolling process.

To remove a temperature sensor from the structure, it is necessary to access the programming section by clicking on the relative button in the menu on the left then, from the list shown, click on the **Delete** button in correspondence with the line of the sensor to be removed.

Via keypad

Type in code (Installer), PROGRAMMING TemperatureSens., Enable/disable

This section allows you to add/remove probes from the configuration by means of keys ▣ and □.

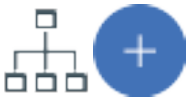
To set the module as "wireless" you need to access the section:

Type in Code (Installer), PROGRAMMING TemperatureProbe, ChoosePeripheral, "temperature sensor", Wireless

Once the **OK** button is pressed, it is necessary to work through the menu options and enroll the module.

Keypad probe

Via software



Once the solution for the system to be designed has been opened, click on the **System Layout** button on the menu on the left. Then click on the "Add device to BUS" button in the section on the right.

A window will open where you can select the keypads to be configured and added to the configuration.

In the section on the left, the number corresponding to the button of the keypads and thermostats increases.

Expansion probe Flex5/S

Via software

The probe can be reached by selecting one of the terminals configured as a zone, or by clicking the **Zone** button in the menu on the left in the section on the right.

In the zone programming section it is necessary to select the "Temperature sensor" item from the "Detector type" box.

Following are shown the respective parameters.

Via keypad

Type in Code (Installer), PROGRAMMANG Zones, "temperature sensor", Detector type, TemperatureProbe

5.7.2 Programming thermostats

Via software

Click on the **Thermostats** button on the menu on the left, the section on the right will provide the list of all the configured thermostats.

Selecting one of the options will allow you to configure the parameters of the single thermostat by clicking on the button.

Via keypad

From the installer menu, the parameters relating to the thermostats can be reached in accordance with the type of associated device.

- In the case of stand-alone module connected to the BUS or connected via wireless connection:

Type in Code (Installer), PROGRAMMING TemperatureSens., ChoosePeripheral

- In the case of a thermal probe integrated in a keypad:

Type in Code (Installer), PROGRAMMING Keypads, ChoosePeripheral

- In the case of a thermal probe connected to an expansion:

Type in Code (Installer), PROGRAMMING Terminals, "thermal probe terminal"

- If the terminal is associated with a thermostat, this can be reached via:

Type in Code (Installer), PROGRAMMING TemperatureSens., ChoosePeripheral

5.7.3 Chronothermostats parameters

Parameter			Software section	Installer menu section
Description	String that describes the temperature sensor, customizable by the installer		 Configured thermostats, selected thermostat	TemperatureProbe, ChoosePeripheral, "sensor", Description
Activatable outputs	In this section you can select the outputs that can be activated by the thermostat function relating to the probe being programmed. There are 4 outputs that can be activated when the thermostat is in "summer" mode and 4 when it is in "winter" mode.			/
Temperature hysteresis	Enter the value of the hysteresis of the sensor.	The entered value must be expressed in °C decimals (from a minimum of 0 to a maximum of 4).		Hysteresis
Programming the chronothermostat	Section relative to the programming of chronothermostat. You can program the thermostat and also adjust its temperature setting and operating times. The adjustment of the temperature (manual or operating time mode) is allowed by indicators on level bars. The **Read** button allows you to read the thermostat schedule and ambient temperature detected by the provided thermometer. The **Write** button allows you to set the schedule.			
Enroll	Button to start the procedure for enrolling wireless devices ("*Enrolling wireless devices*").		 Configured thermostats, wireless thermostat	Wireless
Use detector LED	The red LED indicates a communication in progress between the device and the control panel.			Terminals, "terminal",Options, Use sensor LED
Disable wireless monitoring	Enabling this option (disabled by default), disables monitoring on the wireless detector. In the event of the loss of the specific detector, no event will be generated and no fault signal will be signalled on the keypad.			No superv. WLS
Monitoring wireless	This software section starts a monitoring phase on the variation of the signal transmitted by the device and background noise detected over time.			

5.8 Home-automation and roller shutter modules

5.8.1 Enrolling Home-automation modules

Via software

Once the solution for the system to be designed has been opened, click on the **System Layout** button on the menu on the left. Then click on the "Add device to BUS" button in the section on the right.

A window will open where you can select the home-automation modules to be configured and added to the configuration..

In the section on the left the number is increased in correspondence with the button of the home-automation modules.

To remove a home-automation module from the structure, it is necessary to access the programming section by clicking on the corresponding button on the menu on the left then, from the list shown, click on the **Delete** button in correspondence with the line of the module to be removed.

Via keypad

Type-in Code (Installer), PROGRAMMING HomeAutom.module, Enable/disable

In this section it is possible to add/remove home-automation modules from the configuration, by means of keys and .

5.8.2 Programming of home-automation modules

Via software

Click on the **Project** button in the menu on the left then select one of the home-automation modules added to the configuration.
Clicking the right mouse button on the module icon makes it possible to set the required use of the module itself:

- Expansion module with 4 terminals (home-automation module)
- Roller-shutter module
- "Smart" roller-shutter module
- Roller-shutter module with 1 ON/OFF button
- Roller-shutter module with 1 long press button
- Roller-shutter module with no buttons
- Venetian blind module
- Light point 1 switch and 1 relay
- Light point 1 button and 1 relay
- Light point 2 switches and 2 relays
- Light point 2 buttons and 2 relays

Instead, clicking the right mouse button on a terminal of a module makes it possible to configure the terminal ("*Programming inputs and outputs*").

By clicking on the **Home-automation modules** button on the menu on the left, the section on the right will show the list of all the configured modules.

Selecting one of the options will allow you to configure the parameters of the single module by clicking on the button.

Via keypad

`Type in Code` (Installer), `PROGRAMMING Home-automation modules, ChoosePeripheral`
This section allows you to program the various options of the selected module.

5.8.3 Parameters of Home-automation modules

The parameters of a home-automation module are different, depending on the use for which the module has been programmed.

Parameter			Software section	Installer menu section
Description	This string identifies the home-automation module, customizable by the installer.		 Configured home-automation modules, selected module	HomeAutom.module, ChoosePeripheral, "module", Description
Generic Roller blind Lights	Option to enable the operating mode of the selected module.			/
Operating type	Checkbox for the selection of one of the operating modes. Depending on the type of operation, additional parameters are available:			/
	Roll up time	in mS, from 1 to 200 seconds		/
	Roll down time	in mS, from 1 to 200 seconds		/
	Additional roll up/roll down time	in mS, from 0 to 20 seconds		/
	Pulse time of Venetian blind rotation	in mS, from 1 to 10 seconds		/
	Number of Venetian blind pulses	from 0 to 4		/

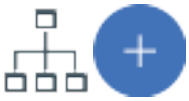
Note

In the case of programming the device to control roller-shutters, it is necessary to enter, as accurately as possible, the times for up/down and Venetian blinds movement.

5.9 Power supply stations

5.9.1 Enrolling power-supply stations

Via software



Once the solution for the system to be designed has been opened, click on the **System Layout** button on the menu on the left. Then click on the "Add device to BUS" button in the section on the right.

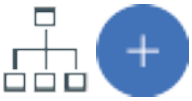
A window will open where you can select the power-supply stations to be configured and add them to the configuration.

In the section on the left, the number increases in correspondence with the power-supply stations button.

To remove a station from the structure, it is necessary to access the programming section by clicking on the corresponding button on the menu on the left then, from the list shown, click on the **Delete** button in correspondence with the line of the station to be removed.

5.9.2 Programming power-supply stations

Via software



By clicking on the **Pow. stations** button on the menu on the left, the section on the right will show a list of the configured stations.

By selecting one of these options and clicking on the button you access the section where you can set only the description of the power station.

Click on the **Project** button on the menu on the left and select one of the power-supply stations added to configuration.

As a control panel peripheral, the power supply station has two terminals that can be configured as outputs ("AUX1" and "AUX2"). These are programmed in the same way as the other outputs available on the system ("*Outputs*").

Chapter 6 Programming of Nexus

The Nexus programming phase allows the installer to select which actions the control panel will implement on receiving a command from a user via voice call or SMS message over the GSM network. Each command comprises a group of fully-programmable parameters.

Each time a user makes a request, via an appropriately formatted SMS text or voice call to the SIM card inside the Nexus, the control panel will be able to activate the respective shortcut, force activation of an event and signal confirmation of the successfully implemented command.

Via software

The following parameters can be programmed solely via the Prime/STUDIO software.

Click on the **Nexus** button on the menu on the left, then go to the section on the right to configure the parameters.

Note

Inim Electronics does not guarantee the total availability of all the GSM/GPRS functions described in this manual, due to the various combinations of GSM/GPRS service providers, SIM types and telephone models that may be in use.

6.1 SMS Commands

In the 'SMS Commands' section it is possible to program up to 30 SMS-activated commands.

To program each command, double click on the corresponding line to open a window for the configuration of the respective parameters.

Table 6.1: SMS command parameters

Parameter		Software section
Action	Identifies the number of the command in the table shown.	 SMS Commands
SMS text	This is the identification string to be included in the SMS command.	
Shortcut	This field allows you to select one of the following shortcuts that the control panel can activate: • Arm/Disarm • Stop alarms • Clear call queue • Delete memory • Activate output • Deactivate output • Inhibit (bypass) control panel zones • Activate (unbypass) control panel zones • Nexus status • Credit inquiry • GPRS client	
Shortcut parameter	Selection menu for the parameter relating to the shortcut.	
Shortcut 2	Selection menu for the shortcut which is to be activated after the one selected above.	
Shortcut 2 parameter	As per "Shortcut parameter" but valid for the "Shortcut 2" command.	
Confirm	Identifies the type of command feedback: • **SMS** - feedback will be provided by an SMS text to the phone number of the caller (command dispatcher). • **Ring** - feedback will be provided on the phone of the caller (command dispatcher). Positive outcome will be indicated by a "ring"; negative outcome by "silence". Confirmation via SMS text or feedback ring will occur only when the phone number that sent the command is not hidden. • **Buzzer** - feedback is provided by an audible signal on the Nexus buzzer. Positive outcome is indicated by three short audible signals; negative outcome is indicated by five long audible signals.	

Command via SMS message

Users who wish to activate a command via SMS text must enter the command details as follows:

<xxxxxx> <SMS Text>

where:

- <xxxxxx> stands for the PIN of a control panel user
- it is necessary to insert a space (" ") after the PIN
- <SMS Text> which is the command identifier, as previously described

Note

Avoid inserting spaces (" ") inside the <SMS text>.

Example

The command dispatcher wants the control panel to activate "Scenario 3", switch On the perimeter lights and confirm the operation via SMS text. Proceed as follows:

1. "SMS Text" - choose the desired description, for example "Night mode"
2. "Shortcut" - select the "Arm/Disarm" shortcut
3. "Shortcut option": "Scenario 3"
4. "Shortcut 2" - select the "Activate output" shortcut
5. "Shortcut option 2" - output associated with the perimeter lights
6. "Confirm" - SMS

When a user keys in the following SMS text on a mobile (cellular) phone:

123456 NightMode

where '123456' stands for the User's PIN and this message is sent to the number of the SIM card of the Nexus, the control panel will carry out the requested operations and will send an SMS message of confirmation to the mobile phone of the caller who dispatched the command:

NightMode: command done!

Default Commands

By default, commands are predefined and can be modified by the installer:

- "**CONNECT**" for a request for remote assistance via SMS text (future use).
- '**CREDIT**' for balance enquiries relating to the SIM card of the Nexus, the user will receive an SMS text indicating the remaining credit.
- '**STATUS**' for status enquiries relating to the Nexus, the user will receive an SMS text indicating the:
  - device name and firmware revision
  - network provider
  - signal reception level
  - device tamper status
  - BUS status
  - Balance (remaining credit)
  - scenario active (if present)
- "**EXC**" (or "**ESC**"), to inhibit the control panel zones
- "**INC**", to activate the control panel zones

For the last two commands, the message text must be:

<xxxxxx> EXC <zone description>

where:

- <xxxxxx> is the PIN of a control-panel user coded, followed by a blank space (" ")
- "EXC" (or "ESC" or "INC") is the command to be implemented on the zone, followed by a space ("")
- <zone description> is the name zone to be inhibited or activated

6.2 Caller ID commands

The 'Caller ID commands' section allows you to program up to 200 telephone numbers and the commands which will be implemented when each telephone number is recognized by the control panel.

If the phone number sends a call (voice), the command selected by the installer from those programmed in the 'SMS Commands' section will be activated.

Table 6.2: Call command parameters

Parameter		Software section
N°	Identifies the number of the command in the table shown.	Caller ID commands
Name	This is the identification string of the command.	
Telephone number	This is the telephone number which, during a call to the Nexus, will activate the command.	
Access Codes	This field is for the association of a user code (from 1 to 255) to the telephone number. The code determines which partitions the phone-number user can operate on.	

Parameter		Software section
Actions	This is the number that identifies the command option selected from the 30 commands programmed in the SMS Commands section.	
Reject call	If this option is enabled, when the phone number calls, the Nexus will reject the call after generating the requested command. If this option is disabled, when the phone number calls, the Nexus will not reject the call but will allow it to proceed in such a way that the control panel can activate (if duly programmed) the dialer after the programmed number of rings.	
Receive diverted SMS	If this option is enabled the selected number will be able to receive SMS messages diverted from the communicator which do not comply with the command-activation format. If the SMS message is a 'command', it cannot be diverted.	

6.3 Text for SMS messages

In the "Texts for SMS messages" section you can edit and program up to 50 SMS messages with 80 alphanumeric characters each.

These SMS texts can be associated with the events via the 'SMS number' option, included in the programming menu of single events.

This section, where the SMS messages are listed in a column, contains the following parameters for each message:

- **N°**, identifies the number of the SMS message.
- **Text**, editable field for the SMS text message. The number of characters available is also indicated.

6.4 Parameters of the Nexus communicator

In the 'General parameters' section, it is possible to program some functions relating to the management of the Nexus device, such as: low/remaining credit, input and output volume, disablement of tamper protection and the emergency signalling delay.

Table 6.3: General parameters of Nexus

Parameter			Software section	Installer menu section
Enable credit check		If this option is enabled, you must also program the interrogation method the Nexus will use to make residual-credit enquiries to the GSM provider. **Automatic** - the Nexus will make remaining credit enquiries to the GSM provider (regarding its own SIM) without need of programming any parameters. **Manual** - the interrogation parameters to the provider and reply must be set up manually.	General parameters, Remaining credit	–
Manual parameters	Request	**SMS** - the remaining credit inquiry will be made via an SMS text sent by the Nexus to the provider. **Call** - the remaining credit enquiry will be made via a call which will be diverted by the Nexus to the provider. **Network command** - the remaining credit enquiry will be made via a special command made available by the provider. **Credit request number** - this is the phone number or network command (made available by the GSM provider) for remaining credit inquiries. This field must be programmed regardless of the type of manual mode selected (SMS, Call or network command). **Credit request message** - this text will be sent to the number in order to obtain information regarding remaining credit.		–
Manual parameters	Answer via SMS	**Answer number** - this is the phone number (made available by the GSM provider) the remaining credit information will come from.This field must be programmed regardless of the selected manual mode (SMS, call or Network command). **Answer message** - part of the SMS answer message, to filter the credit information. It is necessary to type in the text which precedes the numeric value of the remaining credit.		–
Low credit threshold		The remaining credit limit, expressed in local currency. If credit drops below this limit, the Nexus Nexus communicator will signal 'Low credit'.		–
Credit request interval		This is the interval, expressed in hours, which must pass between one automatic credit-enquiry and the next.		–
Balancing		This option permits adjustments to the correlation between input volume/output volume.	General parameters, Volume settings	–
Input volume		This option allows you to program the volume of the input signal to the Nexus and, consequently, the volume of the signal received by the control panel.		–
Output volume		This option allows the programming of the volume of the output signal from the Nexus to recipient telephone devices.		–

Parameter		Software section	Installer menu section
Disable tamper	This option, if enabled, deactivates tamper signalling on the Nexus communicator.	General parameters, Other parameters	–
Emergency signalling delay	This is the delay, expressed in seconds, that the Nexus device applies before generating the 'Nexus lost' event.		–
Disable GPRS fault on keypad	If enabled, this option stops the control panel from signalling the occurrence of specific faults or GPRS connection trouble.		Parameters Disab.GPRS fault
Fault signaling on insufficient GSM cover	If enabled, this option determines the generation of the 'Nexus fault' event when the GSM cover is poor or insufficient. If disabled, poor GSM cover will not generate a fault event.		Low field enable

Note

The remaining credit control feature is subject to temporary or even permanent unavailability caused by changes in the implementation of the methods used by the GSM/GPRS service provider.

Inim Electronics provides device programming functions which may be capable of restoring this feature, by means of manual changes to the respective parameter settings.

6.5 GPRS connection parameters

The "GPRS Parameters" section provides the parameters necessary for setting up the GPRS connection for the remote GPRS connection with the control panel.

Table 6.4: GPRS parameters

Parameter		Software section
Access point name (APN)	Editable field for the name of the GPRS provider.	GPRS parameters
Advanced	This button opens a window for the user's name and password, sometimes required by the provider. If these details are not required, these fields can be left blank.	
Automatic APN	Option that activates automatic search mode of the APN.	

Automatic APN

For Italian operators there is a function that automatically searches for the APN (Access Point Name). By enabling the "Automatic APN" option, you can setup the search automatically. The APN search is carried out at each startup of the control panel, at the end of each programming session and in general when the peripheral modules are inserted or disconnected.

The first time it can take several minutes, however, during subsequent start-ups the time will be reduced to a few tens of seconds.

Following the setting of the automatic APN, the communicator can connect to the Cloud. Successful connection is verified by the lighting up of the blue LED ("CLOUD") on the main board.

Note

The CLOUD LED may light up for other connections types (LAN or Wi-Fi). If you wish to verify with certainty the successful connection via GPRS, it will be necessary to remove all other connection causes or carry out a check from the keypad.

Given the wide variety of SIM cards and services made available by each operator for each SIM, it is possible that the connection system may not be able to find the APN automatically. In this case it will be necessary to remove the "Automatic APN" option from the module programming and operate by setting the APN manually in the relevant field.

Below is a list of operators currently enabled for the automatic APN search.

- Tim
- Vodafone
- WindTRE
- Iliad

Chapter 7 Programming of PrimeLAN and PrimeWiFi

Programming of the PrimeLAN board is possible only via the Prime/STUDIO software.

Via software

The button on menu on the left **PrimeLAN settings** allows you to read and program the Ethernet interface board.

The programming data read is that of the board, the sent programming data will be saved to the memory of the board connected to the control panel and not to the control panel memory.

The programming of the PrimeWiFi board involves the configuration of the Wi-Fi network and the access point.

7.1 Programming IP parameters

Connectivity to the LAN network is subject to the configuration of the network itself.

The manufacturer strongly recommends that you contact the network administrator for the correct configuration.

Table 7.1: IP connection

Parameter		Software section	Installer menu section	User menu section
IP Address **Subnet mask** **Gateway** **DNS** **Communication port**	Connection parameters	IP connection parameters, Connection parameters	Other parameters, IP parameters	Settings, IP Par. and Wi-Fi IP parameters
Web server port **SSL port**			–	–
Obtain an IP address automatically	If this option is enabled the above items are not required. The protocol used is DHCP.		Parameters Enable DHCP	Parameters Enable DHCP
Enable UPnP	This option enables UPnP protocol which automatically activates "port-forwarding" through the network router of the communication, web and SSL ports.		–	–
Domain **User name** **Password**	If you have a dynamic public IP address, you may find it useful to use a domain name which will allow you to trace the LAN board at all times. Prime supports the service offered by: • dyndns.org • freedns.afraid.org • no-ip.com • camsec.net • inimdns.biz By registering at one of these addresses, you will obtain the access data required in this programming section:	IP Connection parameters, DNS dynamic	–	–
Update every	This interval (expressed in seconds) will be applied by the LAN when updating the association of the selected domain with the public IP address.		–	–
Check DDNS account	This button start the DDNS account verification (for "inimdns.biz" service only).		–	–
Enable NTP synchronization	If enabled, the Prime control panel clock will be synchronized with NTP protocol, therefore, it will be necessary to indicate: • **Server** • **Update every** - this is the time, expressed in seconds, that elapses between successive time updates.	IP connection parameters, Configure NTP client	–	–

Parameter		Software section	Installer menu section	User menu section
Enable Modbus	If enabled, the Modbus/IP service on the LAN board will be activated; in this case it is necessary to indicate: • **Port** • **Access Codes**	Connection parameters, Modbus	–	–
This section allows the programming of the parameters of the IP connection test.		IP connection parameters, IP connection test parameters	–	–
IP address **Port**	Pv4 Address and port connection attempts are directed to.		–	–
Range	Time, expressed in seconds, between connection tests. If "0" is set, the connection test will be disabled.		–	–
Number of attempts	Number of connection attempts for each test.		–	–

7.2 Connection to a LAN network

The Prime control panel can connect to a LAN network, both cabled via an Ethernet port, or via Wi-Fi through the optional PrimeWiFi module, and therefore have access to a local or Internet network.

Note

The connectivity to the Prime control panel LAN is subject to the configuration of the network itself. The manufacturer strongly recommends that you contact the network administrator for the correct configuration.

The connection of the control panel and configuration of its settings can be carried out by the user from the user menu, which can be accessed via:

- LCD keypad
- keypad with touch-screen, after accessing the 'Settings - Alphanumeric display' section from the home page that operates as an LCD display

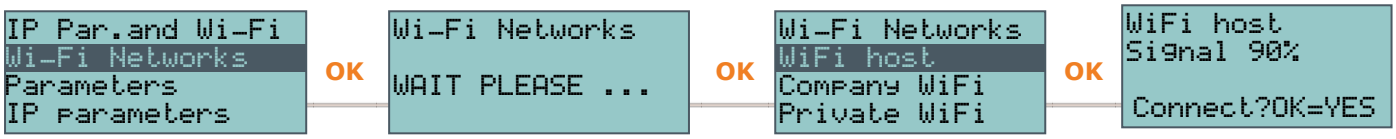
For the programmer it is possible to set the network parameters also thanks to the software, but only if there is a direct connection between the control panel and the PC.

Via keypad

Type-in Code (User), Settings, IP Par.and Wi-Fi

This section provides the following sub-sections:

- **Wi-Fi Networks** - by pressing the **OK** button the control panel will start scanning for available networks, those found will be listed in order in accordance with their signal strength.
  At this point the user can select a network and make the connection using the **OK** button, after entering the respective password, if required.



- **Parameters**:
  - **Enable DHCP** - if enabled, the IP connection parameters will be obtained automatically, in accordance with DHCP protocol.
  - **Enable Wi-Fi** - if enabled, the PrimeWiFi module will activate for the Wi-Fi connection.
  - **Test Internet** - if enabled, the control panel will automatically carry out an Internet connection test every 5 minutes, if failed, the system will force the restart of the Wi-Fi connection.

    Once the option has been selected, it is enabled using the "■" button and disabled using "□". The **OK** button confirms any changes to the options.
- **IP Parameters** - this section is for the network parameter settings (IP address, subnet mask, gateway, DNS, communication port).

1. Use keys and to select the parameter then press **OK**.
2. Using the "left" and "right" arrow keys select the field you wish to change then, by means of the number keys, edit the number.
   Insert the octets inclusive of zeros (e.g.: 192168001010 per 192.168.1.10).
3. Press **OK** to confirm and exit.

After modifying these parameters, and in general, on exiting the "Settings" menu item, the control panel may restart completely.

7.3 Network connection test

You can start the Internet/Cloud connectivity test via your user menu.

Via keypad

`Type-in Code` (User), `Settings`, `Connection test`

This test starts the following checks in succession:

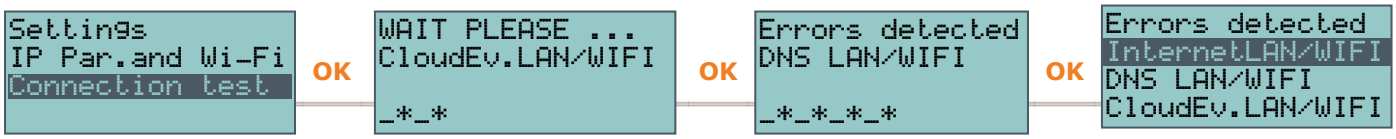
- Internet connection test via LAN/Wi-Fi network
- Internet connection test via GSM communicator
- DNS resolution test via LAN/Wi-Fi network
- DNS resolution test via GSM communicator
- Cloud "Events" channel connection test via LAN/Wi-Fi network
- Cloud "Events" channel connection test via GSM communicator
- Cloud "Commands" channel connection test via LAN/Wi-Fi network
- Cloud "Commands" channel connection test via GSM communicator

During the execution of the test, the first line of the display will show the wording 'Wait' while the second line of the display shows the description of the test currently in progress.

On completion of each test, the keypad display shows the test result on the fourth line:

- an asterisk ("*") if the test is completed successfully;
- a dash ("_") if the test fails.

On completion of all the tests, if communication is successful, the following message will be shown on the first two lines: "Test carried out successfully" otherwise the generic wording "Errors detected Press OK" will be shown. When the **OK** button is pressed, any failed tests will be listed.



Note

If the Ethernet connector is disconnected or if the Nexus GSM communicator is not present or does not respond, or if there is a GSM communicator model without IP communication capacity, the tests relating to these communication channels will not be carried out.
If a PrimeLAN module is present on the control panel, the test relating to the LAN channels will be started regardless of whether the Ethernet connector is connected or not to a network.

7.4 Access point Wi-Fi

The Prime control panel can be equipped with the Wi-Fi 'Access Point' function, which allows you to connect directly to the control panel via a Wi-Fi network created by the control panel itself.

If the control panel options 'AccessPoint WiFi' and 'Enable Wi-Fi' ("*Prime control panel parameters*") are both active and a PrimeWiFi module is installed, when the control panel is turned on, the latter will create a network with the following credentials:

- SSID: 'INIM_Prime_' + last 4 digits of the control panel serial number
- password: serial number of the control panel

The "AccessPoint WiFi" option is active by default and resets to enabled status whenever the factory parameters are restored.
The 'Enable Wi-Fi' option is not active by default.

By default, the 'Enable DHCP' option ("*Programming IP parameters*") is active. With this option active, the control panel Wi-Fi access point is able to automatically assign an IP address to the device in use connected to it and this address will be assigned in the 192.168.1.xxx class.

If the 'Enable DHCP' option is not active, the device from which you are connecting must be manually set to an address of 192.168.1.xxx class, but different from that of the control panel.

7.4.1 Connecting to the control panel as "Access point"

Via software

Via the Prime/STUDIO software it is possible to program the control panel through the Wi-Fi that has been generated.

1. Activate the access point function of the control panel.
   When the function is activated, the blue "**CLOUD**" LED will flash.
2. Start the Prime/STUDIO software application and access the "Settings, Communication port" section of the menu.
3. Select the "LAN/WiFi" connection in the "Communication type" field.
4. In the "IP Address" section, type in the credentials of the network generated by the control panel in the "IP address" and "Password" fields ("*Access point Wi-Fi*").
5. Click on **OK** to start the connection.

As an alternative to the procedure indicated above, it is possible to set the Wi-Fi network and connect to it by following the quick guide made available through the appropriate menu button on the left.

Note

At the end of programming, the control panel will restart completely and with it the Wi-Fi card. In this case it may be necessary to reconnect to the Wi-Fi network generated by the control panel.

7.5 Programming e-mails

The use of the optional PrimeLAN board provides the user with the possibility of sending e-mails with attachments relating to the control panel events.

The sending of e-mails on activation or restoral of events depends on the activation of the 'Memory' option of each event.

Table 7.2: E-mail parameters

Parameter		Software section
Subject	This is the "Subject" field of e-mails, the PrimeLAN board will use this parameter as the subject for all types of events. Depending on the configuration of the e-mail messages, the "Subject" field can be integrated with a general indication of the type of event or a customized text	E-mail parameters, Parameters
Sender	This is the e-mail address of the sender.	
Mail Server	Address of the SMTP server of outgoing post.	
Port	This is the out port of the post server (SMTP).	
Account	This field is for the selection of a domain for which an automatic configuration of the parameters can be obtained by pressing **Preconfigure**.	
SSL Method	Checkbox for the selection of the SSL protocol	
Timeout (s)	Selection field for the maximum time (from 60 to 300 seconds) within which the control panel must send an email to the post server.	
Authentication request	Checkbox for the selection of the authentication type	
User name **Password**	Authentication credentials of the SMTP server selected above	
Id. **Name** **Address**	Section for the creation of the address book, with the data of the recipients of the e-mail messages. This data can be programmed both in this section and during the assignment of the recipients to the e-mail message. It is possible to save up to 20 e-mail contacts.	E-mail parameters, Address book

Following are the parameters that allow you to configure the e-mail messages, setting the text and associating it with the occurrence of events and certain recipients:

Table 7.3: Email message configuration

Parameter		Software section
Event type	Selection field for the selection of type of events to be programmed. The application will show all the programmable events for the selected type.	 Email configuration
Activation / Restoral	The "Activation" and "Restoral" sections are the same and are intended, respectively, for the programming of the dispatch of e-mails when the event occurs (Activation) and when the event ends (Restoral).	
Sel	If you click on the respective check boxes of events with this option enabled, you can program simultaneously the recipient contacts, text and attachments, as described in the following paragraphs. If you right click on the header on this column, you will be able to carry out selections/deselections which involve all the control panel events or all the events of the same type.	
Re: (events log)	If this option is enabled, the message text of the event will be saved to the control panel memory. If you right click on the header on this column, you will can carry out selections/deselections which involve all the control panel events or all the events of the same type.	
Recipients	Double click on the respective check box to access the e-mail addresses in the contact list. The **Contacts** window allows you to select and change the e-mail addresses of the recipients. There are 3 buttons: • **Apply** - this option allows you to add or delete the recipients of the selected event only. • **Apply to events of the selected group** - this option allows you to add or delete the recipients of all events of the same type as the selected event. • **Apply to all the selected control panel events** - this option allows you to add or delete the recipient contacts for all the selected control panel events.	
Subject	For each event, this option allows you to edit the information provided with the subject of the e-mail in addition to what is indicated in "*E-mail parameters*". Double-clicking on the checkbox of the relevant event accesses the **Message subject** field where you can edit a text: • if this text filed is left empty, the e-mail subject will also contain the generic type of event • if a text is entered, the subject will also include the text specified for the single event The 3 buttons **Apply**, **Apply to events of the selected group** and **Apply to all the selected control panel events** have the same functions as previously described. The **Set default for selected** button automatically configures the object in the format: "event type - reference". If the mouse arrow is positioned on the text body, the contents will be shown as a tooltip.	
Text body	This option allows you to edit the text body of the e-mail for each event. Double click on the respective event field to access the message **Text body** window where you can write a text of up to 512 characters on several lines. You can also add links for direct access to web pages or LAN devices (for example, IP cameras), in this case, you must always include "http://". The 3 buttons **Apply**, **Apply to events of the selected group** and **Apply to all the selected control panel events** have the same functions as previously described. If the mouse arrow is positioned on the text body, the contents will be shown as a tooltip.	
Attachment	This allows you to attach a document/file to the e-mail for each event. A double click on the checkbox of the selected event accesses the **Explore** window where you can load or cancel the selected file from the SD-card. The 3 buttons **Apply**, **Apply to events of the selected group** and **Apply to all the selected control panel events** have the same functions as previously described.	
Camera	It is possible to associate a camera to each event. A double click on the relative field of the selected event will open the **Select Onvif camera** window. This window will allow you to select a camera from those configured and select two presets for it. The presets can be selected from those listed after updating the dedicated section (refer to Onvif cameras). The 3 buttons **Apply**, **Apply to events of the selected group** and **Apply to all the selected control panel events** have the same functions as previously described.	
Record on SD	If enabled, the recorded frames will be saved to the SD card that is inserted into the Prime board.	

7.6 Onvif Camera

Remote PTZ control and preset audio/video profiles allow hassle-free user interaction with ONVIF protocol cameras.

The Prime board provides support for JPEG and MJPEG streams for surveillance cameras and allows users to retrieve and view video recordings and snapshots. Interaction with ONVIF cameras allows viewing of recorded images (videos and snapshots) previous to and after the occurrence of an event.

The frames are sent as attachments to emails associated with events or are stored for viewing using a web interface or Inim Electronics application, through the 'Camera' section.

To do this it is necessary to:

1. program the ONVIF camera (using its own presets), provide it with the PTZ presets necessary for viewing the zone under surveillance and recorded video
2. associate a camera with the occurrence (activation or restoral) of an event through the Email configuration section
3. activate the **Record on SD** option for the viewing of recorded frames through a web interface

4. using the Prime/STUDIO software, configure the ONVIF camera by clicking-on the **Prime settings** button and then going to the "Programming - ONVIF camera management" section on the right.

This section provides a pane containing the list of the configured cameras. At the side of this is another section containing the parameters relative to the selected camera:

Table 7.4: ONVIF camera parameters

Parameter		Software section
	Buttons for the addition of a new camera or for the deletion of the selected camera.	ONVIF camera management
Include Security Header in messages	This option, if enabled, includes the "Security Header" in the SOAP messages for the communication with Onvif devices.	
Description	This is the description of the selected camera.	ONVIF camera management, Camera
IP address **Port** **User name** **Password**	Parameter that permits access to the selected camera.	
https	If selected, a secure HTTPS connection will be used.	
Multimedial profile	Field for the selection of one of the multimedia profiles of the camera. These profiles are listed following a read operation requested by pressing the button. The button opens a window showing all the available profiles and where you can edit the 'Token' and name of each one. The window provides two buttons: • - for manual entry of a profile in the list • - for deletion of the selected profile	
Pan - Tilt - Zoom	This field indicates whether the selected camera is equipped with PTZ (Pan, Tilt, Zoom) capabilities.	
Preset available for the selected profile	This section lists all the presets relating to the profile selected in the previously mentioned programming field. These presets are listed following a read operation requested by pressing the button. The button opens a window showing all the available presets and where you can edit the 'Token' and name of each one. The window provides two buttons: • - for manual entry of a preset in the list • - for deletion of the selected preset	
URI Snapshot **URI Stream**	This field allows you to view the addresses (URIs) of frames shots and audio/video streams. These addresses are listed following read operation requested by pressing the button.	
Sampling frequency	This is the time that must elapse between two successive frame shots (max. 60 seconds).	
Number of frames pre/post event	This is the number of frames (from 0 to 5) which will be saved to the memory before/after the occurrence of the event the camera is associated with.	
Images	The image in the lower part of the section reproduces the instant frame of the camera selected after pressing the button. Clicking on the image itself opens window for the viewing of video footage in real-time, control of the camera functions and display of the available presets.	

7.7 Programming KNX interface

By clicking on the **Prime settings** button on the menu on the left, you will access the 'Programming KNX' section.

This section contains three further sections, one for setting the parameters of the KNX gateway and communicating with it, the other boards for translating of signals to and from the KNX system.

Table 7.5: KNX gateway parameters

Parameter		Software section
Enable KNX function	This option enables communication between Prime and KNX systems.	Programming KNX, General settings
IP address / UDP Port / Group address of the KNX gateway	Check boxes for setting the KNX-IP interface gateway data.	
Control panel code	Check box to indicate the Prime user code for commands and actions from KNX devices.	
Polling time	Time interval in seconds of interrogation of the Prime control panel.	
KeepAlive time	Time interval in seconds between two successive supervision signals of the KNX gateway.	
Enable SYNC function	Option that enables the SYNC function. If enabled, it is necessary to enter the address and bit in the appropriate checkboxes.	

Control panel code

When necessary for the security system, it is useful for the installer to create an additional Prime user equipped with a PIN code, capable of carrying out commands and actions from KNX devices even when validation from the Prime control panel is required.

SYNC function

By activating this option, the Prime board sends an update of the control panel statuses to the KNX system either automatically, whenever the connection with the system is lost, or manually, on receipt of the specified telegram.

From control panel to KNX

This section allows you to define which panel events must be communicated to the KNX system via commands or actions and to translate these into "KNX telegrams".

These events (maximum of 3000) are added to the list below via the appropriate button  .

Table 7.6: Signals from control panel to KNX system

Parameter		Software section
Value	Checkbox to indicate the event type.	Programming KNX, From control panel to KNX
Element	Checkbox to indicate the parameter of the type of event that defines the event itself.	
Element category	Checkbox to indicate the category of the element that defines the event.	
KNX telegram	Check boxes to enter the KNX telegram to be sent following the corresponding event.	
Activation/Restoral	Fields for the datapoint value relating to the telegram to be transmitted on activation and restoral.	
...	Button to open the "Add KNX telegram" window.	
Delete	Button to delete the corresponding event from the list	

KNX solutions

The 'Add KNX telegram' window, which is opened by the button '**...**', provides the **Open** button to open '.esf' format files, the solution files of KNX programming software.

Once one of these solutions has been selected the window will show a tree structure with the various elements of the KNX system and the relative telegrams. A double click on one of these items allows you to import the telegram into the appropriate field.

From KNX to control panel

This section allows you to define which signals from the KNX system in the form of 'KNX telegrams' must be communicated to the control panel and which actions must be performed.

These events are added to the list below via the appropriate button  for a maximum of 3000 actions.

Table 7.7: Signals from KNX system to Prime control panel

Parameter		Software section
KNX Event	Field for the insertion KNX telegram, signal from the KNX system corresponding to an event.	Programming KNX, From KNX to control panel
...	Button to open the "Add KNX telegram" window.	
Actions on control panel	Check box to indicate the action to be activated on the Prime control panel.	
Element /Mode	Action parameter.	
Execute if bit=0	Options that activate the action on the control panel depending on the bit associated with the signal from the KNX.	
Execute if bit=1		
Execute anyway		
Execute as a bit		
Delete	Button to delete the corresponding event from the list	

The activation of an action in the Prime control panel triggered by a signal from a KNX system depends on the value of the bit that accompanies each telegram and on the selection of one of the "execute" parameters indicated above. Following is an explanatory table:

Table 7.8: Actions on control panel from KNX system

Action		Execute if bit=0		Execute if bit=1		Execute anyway		Execute as a bit	
on control panel	**Mode**	**bit=0**	**bit=1**	**bit=0**	**bit=1**	**bit=0**	**bit=1**	**bit=0**	**bit=1**
Arm in Stay mode	**Away mode**	Activation action	No action	No action	**Activation action**	Activation action	Activation action	Activation "Disarm"	Activation action
	Stay Arm	Activation action	No action	No action	**Activation action**	Activation action	Activation action	Activation "Disarm"	Activation action
	Instant mode	Activation action	No action	No action	**Activation action**	Activation action	Activation action	Activation "Disarm"	Activation action
	Disarm	Activation action	No action	No action	**Activation action**	Activation action	Activation action	No action	Activation action
	Reset	Activation action	No action	No action	**Activation action**	Activation action	Activation action	No action	Activation action
Zone bypass	**Bypass**	Activation action	No action	No action	**Activation action**	Activation action	Activation action	Activation "Unbypass"	Activation action
	Unbypass	Activation action	No action	No action	**Activation action**	Activation action	Activation action	Activation "Bypass"	Activation action
Activate exit	**Activation**	Activation action	No action	No action	**Activation action**	Activation action	Activation action	Activation "Deactivation"	Activation action
	Deactivation	Activation action	No action	No action	**Activation action**	Activation action	Activation action	Activation "Activation"	Activation action
Activation scenario	**Activation**	Activation action	No action	No action	**Activation action**	Activation action	Activation action	No action	Activation action

7.8 Programming CIAS devices

Clicking on the **Prime settings** button on the menu on the left accesses the "CIAS devices" programming section on the right.

This section provides the parameters of the CIAS devices that interface with the Prime system undergoing programming.

There are 8 subsections, each relating to a "group", i.e. a set of devices connected to a further CIAS device which acts as a bridge with the control panel via a LAN network.

Table 7.9: CIAS group parameters

Parameter		Software section
Description	Group description string	CIAS devices, Group x
Polling time	Polling time interval of the Prime control panel (x 100 msec).	
IP address **Port**	Check boxes for setting the CIAS interface gateway data.	
Maintenance polling tool	Time interval in seconds between two polling phases (queries) to detect the maintenance status of a group, a condition that occurs when a technician connects via PC. To detect maintenance status, it is necessary to make queries on the group with a longer interval time in respect to queries to detect the alarm status of the device. In the relative "Activate output" box, it is possible to select the output to activate if maintenance status is detected.	
Connection timeout	Maximum time, in seconds, before reporting that the device group is no longer responding to polling (queries). In the relative "Activate output" box, it is possible to select the output to activate if the response from the group does not arrive within the maximum time.	

For each group, the list of devices belonging to the group concerned is shown in the lower section.

Devices can be added to this list by means of the "**+1**", "**+5**", "**+10**" buttons, up to a maximum of 127 devices, or they can be deleted by means of the respective "**Delete**" button or the "**Empty all**" button for total deletion.

Each device has the following parameters:

Table 7.10: CIAS devices parameters

Parameter		Software section
Address	Address with which the device is enrolled in the group.	CIAS devices, Group x
Device	Device description string.	
Alarm **Pre-alarm** **Tamper** **Fault**	Checkboxes for the selection of the output which is to be activated in the event of verification of the relative device status.	
Timeout **Timeout type** **Output to be activated**	For each individual device it is possible to indicate a maximum period in which it must respond to a query from the control panel ("Seconds") or a maximum number of "No responses". This number corresponds to that indicated in the "Timeout" box. If this limit is exceeded, the control panel will activate the output indicated in the "Output to activate" box.	

The "**Load programming**" and "**Save programming**" buttons at the top allow loading to Prime/STUDIO of any programming present in the groups, or to send the one in progress.

With the "**Statistics**" key it is possible to access a report regarding the operation of polling (queries) with the CIAS devices. Here it is possible to find the latest statuses detected by each device and the minimum and maximum query/polling times.

The "**Advanced**" button opens a window for the setting of the advanced CIAS parameters:

- "Maximum waiting time for detector response", time to wait for each device to respond to polling (query). If this time elapses and there is no response, the system will go to the next device.
- "Maximum waiting time for the response of the maintenance tool", time to verify the persistence of maintenance, once detected on a device.

Note

The default values in the "Advanced" window are those ideal for the system and should not be changed unless absolutely necessary.

Chapter 8 Programming the telephone

The Prime system provides for the programming of all the telephone parameters, both for the telephone numbers to be called when events occur, and for the telephone line parameters.

Via software

Clicking on the **Telephone** button on the menu on the left accesses two sections on the right.

- **Telephone numbers**, where all the available telephone numbers and their parameters are listed. Selecting one of these items allows you to set the parameters of the single scenario by clicking on the button.
- **Telephone parameters**, where it is possible to set the parameters of the telephone line and telephone dialers.

Via keypad

`Type in code` (Installer PIN), `PROGRAMMING Telephone`

In this section it is possible to program both the parameters of each selected telephone number and some parameters of the telephone line.
Other parameters are available in the sections:

`Type-in Code` (Installer), `PROGRAMMING Parameters` or also `Other parameters`

8.1 Telephone numbers

Table 8.1: Parameters of single phone number

Parameter		Software section	Installer menu section
Description	This is an editable field for the code user's phone number, to be customized by the installer.	Telephone numbers, selected number	`Telephone, Selected number, "number"`
Telephone number	Editable field for the contact number (maximum 20 digits). Accepts also "," (= 2 second pause), "*" and "#".		
Type	Telephone number type: • **None** - the selected number can receive SMS text messages only • **Voice** - the selected number can receive voice calls and SMS text messages If the number refers to the Alarm Receiving Centre, assigns the **ARC** protocol (reporting format): • Ademco 10bps, Ademco 14bps, Franklin 20bps, Radionics 40bps, Scantronic 10bps, CONTACT-ID, SIA-IP		
Account code	This is the 4-character alphanumeric code which identifies the caller in reports to the Alarm Receiving Centre.		
Channel	Checkbox for the selection of the channel on which the call can be routed: • PSTN • GSM		
Encryption	This field allows you to select the SIA-IP protocol encryption type: • None • AES 128 bit • AES 192 bit • AES 256 bit After selecting the type is is necessary to indicate the encryption key.		

Parameter		Software section	Installer menu section
Receive SMS	This option allows the telephone number to receive an SMS message from the GSM module, as well as all other event-related communications.		Telephone, Selected number, "number", Options
Toggle channel on	This option, in the event of call failure on a channel, enables the control panel to carry out call attempts on an alternative channel and then try again on the original channel and continue on both channels alternately for the set the number of attempts.		
Enable SIA-IP polling	If a phone number is a "SIA-IP" type number, this option enables the polling function.		
SIA-IP	If a phone number is configured as "SIA-IP", you must program the IP address and the SIA-IP receiver port in this section.		–
(LAN) port Port (Nexus)	Port used for SIA-IP communication via LAN / Nexus		–
Partitions	You can associate each phone number with specific partitions. By selecting the partitions, you can enable/disable users (who have at least one of these partitions in common with the phone number) to modify the number concerned.		Telephone, Selected number, "number"
Failed call	A key is available that directly accesses the programming section of the failed call.event.		Events, Failed call

'SIA-IP' type

If a phone number is a "SIA-IP" type, the IP address and port of the SIA-IP receiver must be entered in the receiver number field in the "Number" section, using the following format:

xxxyyyzzzttt,ppppp

where:

- "xxxyyyzzzttt" are the 4 octets of the IP address (standard IPv4), each of which should be written with 3 figures and, if necessary, "0" filler characters and no separation points.
- "ppppp" is the port and should be written with 5 figures and, if necessary, "0" filler characters.

Polling SIA-IP

If a telephone number is a "SIA-IP" type number, it is possible to enable the "polling" function. In this way, from this number the control panel sends a periodic signal to the receiver SIA-IP server, which can verify proper functioning of the transmission. The parameters of the polling periodicity are available in the "Telephone parameters" section (refer to Telephone line).

Account code

Depending on the protocol, the account code can be exclusively numeric or can accept also the letters "A", "B", "C", "D", "E", "F", available on keys "**2**" and "**3**".

8.2 Telephone line

Table 8.2: Telephone parameters

Parameter		Software section	Installer menu section
Dial-tone check	The control panel will engage the phone line and check for the "dial tone"; if present, the control panel will start dialing.	Telephone parameters - Telephone line parameters	Parameters Dial tone check
Pulse dialing	The control panel will dial using pulse tone.		Pulse dialing
Telephone line fault alert	If a "telephone line fault" event occurs, the control panel will flash the respective icon on the keypad displays.		Line down signal
Double call	The control panel will override the answerphone function. Option available only for PSTN calls.		Double call
Number of rings for answerphone	This value determines the number of rings the system allows before picking up an incoming call (from 1 to 15).		Telephone Number of rings
Ring sensitivity	This is the numerical value that determines the sensitivity to the recognition of the rings of a phone call to the control panel. This value is set at 60 by default. Accepted values: 1 to 120.		Other parameters, Ring sensitivity
Call all voice/digital/SIA-IP numbers	If several voice calls (digital or SIA-IP) generated by the an event are waiting in the outgoing call queue, the control panel will attempt to send voice calls to all the numbers of this type.	Telephone parameters, Telephone dialer parameters	Parameters Call allVoxNums Call all TLVNums Call all SIA-IP
Access DTMF menu without code	When the control panel makes voice calls, it will allow access to the user menu over-the-phone using the parameters and enablements of the last user code of the control panel model (code 30, 50 or 100).		DTMF withoutCode
Start message after dialing	The control panel will start the voice message 5 seconds after dialing the respective contact number.		BypassVoiceCheck

Parameter		Software section	Installer menu section
Confirm call with "*"	The control panel will consider the voice call successful when the recipient presses the "*****" key on the phone keypad.		Confirm with *
UTC Time on SIA-IP	Calls to SIA-IP type numbers will contain the date and time in "UTC" format (Coordinated Universal Time).		UTC timeOnSIA-IP
Increase DTMF sensitivity	Option that increase the sensitivity of incoming DTMF tones.		DTMF sensitivity
No SIA strings **No SIA-IP strings**	The descriptive strings will not be sent in SIA/SIA-IP protocol.		NoStrings SiaProt NoStrings SIA-IP
Arm/Disarm inverted on C.ID	Partition arming events using CONTACT-ID protocol will send the "New event/Event activation" code when the partition arms, and the "Event ended/Event restore" code when the partition disarms.		CONT-IDInversion
Generates one call only for each event	If this option is enabled, it blocks all the calls programmed for an event after the first successful call. If the options "Call all voice/digital/SIA-IP numbers" are enables, then the latter have priority.		SingleCallEachEv
Stop calls on disarm with no alarm	The control panel will not carry out the calls programmed for disarm operations when there are no active alarms or alarm memories present.		Disab.Tel.Disarm
Message repetition number	This value determines the number of times the voice message will be played during the call (from 1 to 15).		Telephone Message repeats
Number of attempts	This value determines the number of calls attempts the system will make before deleting the contact number from the call queue (from 1 to 15).		Max.num.attempts
Delay on line-down signal	This parameter allows you to program the delay, expressed in seconds or minutes, which will be applied before "Line Down" events is signalled.		Other parameters, LinedownDelay
Telephone-voice volume output	This parameter allows you to select the volume of the outgoing voice messages played during a phone call. Accepted values: 10 to 100 minutes.	Telephone parameters	OverThePhoneVol.
Incoming Telephone volume	This parameter allows you to select the volume level of the incoming phone signal. This is a useful parameter for the understanding of DTMF tones. Accepted values: 1 to 80 minutes.		Tel. input Gain
SIA-IP polling interval	Field for the interval between two consecutive polling signals (expressed in seconds).		-
Disabled	Option that disables the polling function for all phone numbers.		

8.2.1 Telephone line adjustment

The "Outgoing voice volume" and "Incoming voice volume" parameters can be used to correct the voice functions of the dialer and DTMF tones. The values of these parameters affect each other, therefore, and a good result is always a compromise.

If you are not using a GSM interface, you should:

- Adjust one parameter at a time and carry out tests to verify the result.
- Increase/decrease the values in small steps (for example, from 25 to 22 and not from 25 to 15).
- If the DTMF tones are not recognized, or are recognized with difficulty, decrease the value of the "Outgoing voice volume" parameter (in small steps of 2 or 3 units) and verify the effect. If there is no improvement, increase the value of the "Incoming voice volume" parameter until an acceptable level is achieved.
- Do not increase the "Incoming voice volume" parameter excessively, as an excessive value may cause incorrect interpretation of DTMF tones.
- If the volume of the telephone messages is low, increase the "Outgoing voice volume" (in small steps of 1 or 2 units) and verify the effect. An excessive value of the "Outgoing voice volume" parameter may cause incorrect interpretation of DTMF tones.

In most cases, the value of the "Outgoing voice volume" parameter is between 15 and 25, whereas, the value of the "Incoming voice volume" parameter is between 20 and 30.

Chapter 9 Programming arming scenarios

The programming of the arming scenarios (configurations of the arming mode of the Prime system partitions) can be carried out either via software or from a keypad.

Via software

Click-on the **Arming scenarios** button on the menu on the left, the section on the right will provide a list of all the available scenarios and their parameters. Selecting one of these items allows you to set the parameters of the single scenario by clicking on the button.

Via keypad

Type in code (Installer), PROGRAMMING Arming scenarios

This section allows you to program the various options of the selected scenario.

9.1 Scenario parameters

Table 9.1: Parameters of single scenario

Parameter		Software section	Installer menu section
Description	Editable field for the description of the scenario.	 Arming scenario, selected scenario	ArmingScenario, "scenario"
Icon	This section allows you to select the icon you wish to assign to the scenario, by indicating the icon number (refer to "*Keypad shortcut and icon*").		
Output	The selected output will be activated when the scenario is applied (via keypad, reader, phone, etc.). It is possible to use a scenario solely to activate an output (leaving all actions on the areas null) thus having the possibility to display different icons on the keypads to activate different outputs, inheriting the desired icon from the scenarios.		
Partitions	This section allows you to configure the arm/disarm scenarios of all the partitions managed by the control panel. • "-" the current operating mode of the partition will not be changed. • Away - the partition will arm in Away mode (interior and perimeter). • Stay - the partition will arm in Stay mode (perimeter only). • Instant - the partition will arm in Instant mode (perimeter only with zero delay). • Disarm - the partition will disarm.		
Activate scenario	At the bottom of the section is a key that directly accesses the programming section of the event that applies the selected scenario.		Events, ScenarioON

Chapter 10 Programming partitions

The programming of the partitions of the Prime system can be performed either via software or from a keypad.

Via software

Click-on the **Partitions** button on the menu on the left, the section on the right will show a list of all the available partitions and their parameters. By selecting one of these items it is possible to set the parameters of the single partition by clicking on the button.

Via keypad

Type in code (Installer), PROGRAMMING Partitions

This section allows the programming of the various options of the selected partition.

10.1 Partition parameters

Table 10.1: Parameters for single partitions

Parameter		Software section	Installer menu section
Description	This is the editable partition label (description).	 Partitions, selected partition	Partitions, "partition"
Exit time	This is the Exit time window (programmable in seconds or minutes) If you set "0" in this field, there will be no Exit time. Therefore, any delayed zones belonging to the partition will generate alarms instantly if they are not in stand-by status when the partition is armed.		
Entry Time	This is the Entry time window (programmable in seconds or minutes). If you set "0" in this field, there will be no Entry time. Therefore, any delayed zones belonging to the partition will generate alarms instantly if violated when the partition is armed.		
Entry Time 2	This is the window for the second Entry time.		
Pre-arm time	This setting is the delay, expressed in minutes, which precedes automatic-arming on a partition.		
Patrol time	This is the time window for patrol operations (programmable in minutes).		
Timers	Select the timer you want to associate with the automatic-arming operations.		
Autoreset memory on arming	If enabled, the partition alarm and tamper memory will reset automatically when the partition arms.		Partitions, "partition", Options, AutoresetMemories
Auto-arm in stay mode	If enabled, the partition will arm in "Stay" mode at the programmed time. If disabled, the partition will arm in "Away" mode at the programmed time.		Autoarm.STAYmode
Clear call queue on disarm	If enabled, the call queue will clear when the partition disarms.		StopTelOn Disarm
Events button	At the bottom of the section are the buttons that directly access the programming section of the events associated with the selected partition.		Events

Automatic arming/disarming

The association of a timer with a partition will allow it to arm or disarm automatically at the ON/OFF times set on the timer.

This function must be enabled or disabled for each individual partition.

Type in code (User), Activations, Auto-arm

This section lists the partitions on which to activate or not automatic arm/disarm operations by means of the ▣ and □ buttons.
Forced auto-arm operations may occur, generated by events active at the time of the auto-arm operation.

Chapter 11 Programming timers

Each timer can be set as "Ordinary" or as "Astronomical".

Ordinary Timer

For each "ordinary" timer it is possible to set:

- two scheduled activation times ("ON") for each day of the week.
- two scheduled deactivation times ("OFF") for each day of the week.
- Up to 15 exceptions
- the assigned partitions of the codes and keypads that have access to the programming process of the timers via the user menu

A timer can be associated with:

- a **Partition** - if the timer is enabled and the partition is enabled for automatic-arming operations (refer to "*Activations*" in the User's Manual), the partition will arm when the timer is active (ON) and will disarm when the timer switches OFF.
- a **Code** - if the timer is enabled, the code will be authorized to operate on the system only when the timer is active (ON).
- a **Key** - if the timer is enabled, the key will be authorized to operate on the system only when the timer is active (ON).

Astronomical timer

The programming of an "astronomical" timer, using the control panel "astronomical clock" function, refers to sunrise and sunset times. It is possible to set:

- a switch-on time ("ON") referring to the time of sunset
- a switch-off time ("OFF") referring to the time of sunrise

Note

The timers must be enabled/disabled by the user (refer to "*Activations*" in the User's Manual). On exiting the programming session all the timers will be automatically re-enabled, therefore, if the user previously disabled any of the timers, then these must be re-enabled.

Via software

Click-on the **Timer** button on the menu on the left, the section on the right will provide a list of all the available timers and their parameters. Selecting one of these items allows you to set the parameters of the single timer by clicking on the button.
The software program allows you to set up 15 setting exceptions for each timer. Each exception allows you to define an interval period (of even one day) within which you can set an activation time and a deactivation time valid for all the days of the interval. The system does not accept intervals which go over the end of the year. Therefore, it is impossible to program an interval such as 12th December to 5th January. In such situations, you must program 2 "timer exceptions", one from 12th to 31st December and the other from the 1st to 5th January, both with the same On and Off settings.
The exceptions have priority over the days of the week. For example, If a "timer exception", let's say 1st May, falls on a Tuesday the settings programmed for 1st May will be applied.

Via keypad

`Type in code` (Installer), `PROGRAMMING Timers`
This section allows you to program the various options of the selected timer.

Note

The exceptions cannot be programmed via keypad.

11.1 Timer parameters

Table 11.1: Single "ordinary"timer parameters

Parameter		Software section	Installer menu section
Description	This is an editable field for the description of the timer.	Timer, selected timer	–
Monday / ... / Sunday	You can program two "ON" and "OFF" time frames for each day of the week. During the week, the timer will activate in accordance with each "ON" indication and deactivate in accordance with each "OFF" indication, regardless of the number of times "ON" and "OFF" indications occur and also regardless of whether the indications belong to the same day of the week.		Timers, "timer"
Partition filter for user-codes	This section indicates the partitions associated with the codes and keypads which have access to timer programming through the user menu.		
Exceptions	Each exception allows you to define a time frame, expressed in days, within which you can set an "ON" time and an "OFF" (deactivation) time valid for all the days included in the time frame. Exceptions always have priority over the days of the week.		–
Timer event	A key is provided that directly accesses the programming section of the activation event of the selected timer.		Events, Activated timer

Note

It is also possible to program only activation or only reset of a timer.
The field not used for programming purposes must be set as "--:--".

Table 11.2: Single "astronomical" timer parameters

Parameter		Software section
Description	This is an editable field for the description of the timer.	Timer, selected timer
Minutes of deviation in respect to sunset	This parameter allows you to set an advance in minutes (if the value is negative) or a delay (if the value is positive) in respect to the moment calculated for sunset.	
Minutes of deviation in respect to sunrise	This parameter allows you to set an advance in minutes (if the value is negative) or a delay (if the value is positive) in respect to the moment calculated for sunrise.	

Once all the above data have been set, the following will be obtained:

- upon reaching the time calculated by the control panel as "sunrise", added to the deviation programmed for sunrise, the timer will switch to "OFF" status and the related event will be reset (if not already)
- upon reaching the time calculated by the control panel as "sunset", added to the deviation programmed for sunset, the timer will switch to "ON" status and the related event will be activated (if not already)

Note

In order for the control panel to make a correct calculation of the moments of sunrise and sunset, the correct geographical coordinates of the system must be set (refer to "Geolocation", in "*Prime control panel parameters*").

Activation of the control panel "Automatic daylight saving time" option ("*Prime control panel parameters*") does not affect the sunrise and sunset times obtained by means of the astronomical clock.

The control panel does not perform partition auto-arming programmed on the basis of astronomical timers.

Chapter 12 Programming user codes

Programming of the user codes involves both the authorizations of the user the code is associated with, and the code itself with its parameters (hierarchical level, PIN, etc.).

Via software

Click-on the **Codes** button on the menu on the left, the section on the right will provide a list of all the available user codes and their parameters. Selecting one of these items allows you to set the parameters of the single code by clicking on the button.

Via keypad

`Type in code` (Installer), `PROGRAMMING Codes`

This section allows you to program the various options of the selected user code.

12.1 Change user PIN

The user code PINs must be numeric and comprise 4 to 6 digits.

The PIN of the user code n. 1 is "0001" at default. The PINs of the successive user codes are "0002", "0003", etc. up to "0150" for the Prime060S and Prime060L control panel model, up to "0200" for Prime120L, up to "0300" for Prime240L and up to "0500" for Prime500L.

Via software

Click on the **Codes** button on the menu on the left, the section on the right will provide the "Change User PIN" subsection where you can change the PIN of the selected code.

The new Code PIN can be created in the "New PIN" field in two different ways:

- **Old PIN** - this method allows you to substitute the old code PIN (to be entered in the upper edit field) with a new PIN (to be entered in the lower edit field).
- **Master or Manager User PIN** - this method, using a Master or Manager user PIN (to be entered in the upper edit field) allows you to substitute the old code PIN with a new one (to be entered in the lower edit field on the right).

Changes will be valid only after the **Change PIN** button has been pressed.

Via keypad

`Type in code` (User), `Change PIN`

This section allows you to change the User Code PIN used for access and also the PINs of all other users with a lower rank in the system hierarchy.

1. Using keys and select the user code you want to change.
2. Type-in the new PIN (4, 5 or 6 digits) using keys "**0**", ..., "**9**" then press **OK**.
3. Type-in the new PIN again using keys "**0**", ..., "**9**" and press **OK** to save.

`Type in Code` (Installer) ,`PROGRAMMING Default settings, Only PIN default`

This section will allow you to reset all PINs of the user codes to default.

Via touch-screen keypad

From the touch-screen keypad, access the "Settings" section, enter a valid user code, then access the "Date/Time – Change PIN – Change tel. num." section, then the "Change PIN" section.

Select the code from those available on the list. In the section that follows it is possible to change the code by means of the buttons displayed on the screen and confirm changes by pressing the **OK** button.

12.2 Code PINs Database

The Prime/STUDIO software provides a section for the saving of code PINs in a database for their eventual retrieval during control panel resetting or reprogramming phases.

This function allows you to read or rewrite on the solution in progress the PINs of all the codes previously registered in the control panel without them being shown to the installer or operator.

An encryption algorithm hides from the installer the sensitive data of the codes contained both in the Prime/STUDIO solution and in the programming storage database.

Via software

1. Click the **PIN/Key** button on the menu on the left.
2. Enter a valid user code that is qualified as "Master" and enabled on all partitions in the "Master Code" programming field.
3. Select the "PIN" page for the PINs of registered codes.

4. During the PIN reading phase, click on the "Read from control panel" button to load the PINs from the control panel or click on the "Read from database" button to load them from an existing database.
   The software reads the PINs and matches them to the codes without making them visible (instead "****" will be shown).

During the PIN saving phase, click on the "Write on control panel" button to load the PINs on the control panel or click on the "Read from database" button to load them from an existing database.

12.3 Access to user menu

Via software

By clicking-on the **Codes** button in the menu on the left and selecting one of the options, you can view the "Access to User menu" subsection in the section on the right.

The selection checkbox will be shown on the system keypads immediately after user code access has been validated.

- **Icons, function key shortcuts** - displays the icons of the codes corresponding to the function keys. At this point, the user can press the function keys and activate the respective shortcut.
- **Shortcut text** - displays the descriptions of the user shortcuts associated with the function keys. The descriptions of the shortcuts will be shown in the place of the respective shortcuts icons.
- **Standard user menu** - accesses the user-menu scroll list containing all the operations the user is enabled to perform. At this point, the user can scroll the list and select the required operation.

Via keypad

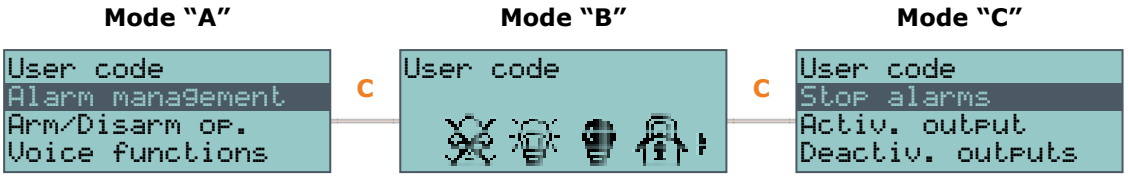
Type-in Code (Installer) , PROGRAMMING Codes, "code", Options .

This section provides the "Text Menu" and "User Menu" options.

The combination of these two options allows immediate display on the keypad screens immediately after user code validation. Refer to the following table.

Table 12.1: Combinations "text menu" and "user menu"

Mode	Text menu	User menu	View
A	Disabled	Enabled	Access to the user-menu (shown as a list of operations the user is enabled to perform); at this point the user can scroll the list using and and select the required option.
B	Disabled	Disabled	Visualization of the user-icons associated with function keys **F1**, ..., **F4**; at this point the user can press the required function key and activate the associated shortcut.
C	Enabled	Disabled	Shows the descriptions of the personalized user-icons associated with function keys. The shortcut descriptions will be shown instead of the shortcut icons, at this point the user can use and to scroll the list of shortcut descriptions and select the shortcut, which can be activated by means of the**OK** key.
D	Enabled	Enabled	As per mode "C"



In all methods of access (A, B and C), the **C** button allows the user to access/view the other cases in succession.

12.4 User code parameters

Table 12.2: Single code parameters

Parameter		Software section	Installer menu section
Description	This is an editable programming field for the code user's name.	Codes, selected code	Codes, "code"
Partitions	Section for the selection of the partitions the code is assigned to.		
Type	Programming field for the assignment of the level in the code hierarchy of the selected user. The default level of code number 1 is “Master”; the default level of all the other codes is “User”.	Codes, selected code, Options	
Partition filter	If this option is enabled, the code concerned can change the parameters only of codes of a lower level in the code hierarchy whose partitions are a subset of its own partitions. For example, if a code is configured as “Master” with “Partition filter” and is assigned to partitions 1, 3, 5 and 7, it will be able to enable/disable or change the PIN of a “User” code assigned to partitions 1 and 5 but not the PIN of a “User” code assigned to partitions 1, 2, and 3.		Codes, "code", Options
Fixed length	Fixed length - if enabled, the user will be able to arm and disarm the control panel simply by typing in their PIN without need of pressing the **OK** button. If all the partitions the user controls are disarmed, it will arm them, otherwise it will disarm them If this option is enabled, the user of the code concerned can access their menu only after pressing **OK** and typing-in their PIN.		
Voice guide	If enabled on a keypad with a speaker, the voice guide (after PIN entry followed by **OK**) will announce the shortcut descriptions relating to the entered user-code and the respective number keys on the keypad.	Codes, selected code, Enablement details, Options	AnnounceShortcut
Patrol	If enabled, the code will be a “Patrol” code.		
Remote access	If enabled, the code PIN can be used to operate the system over-the-phone. If the code PIN is entered on a remote telephone keypad, only the shortcuts associated with keys 0 to 9 can be used to: • Arm/Disarm • Stop alarms • Clear call queue • Delete memory • Activate output • Deactivate output • Listen-in • Arming status		
Recognized valid user code	A key is available that directly accesses the programming section of the system arming event of the selected code.	Codes, selected code	Events, Valid Code

Table 12.3: Code enablements

Parameter		Software section	Installer menu section
Enablements	This section allows you to enable/disable access to the various sections of the User Menu. For details regarding the sections of the user menu, refer to the *User Manual*.	Codes, selected code, Enablement details	Codes, "code" Enablements
Enablement of outputs	This section allows you to enable/disable each output the code is authorized to control manually via the user menu.		Assigned outputs
0/9 key shortcuts	This section allows you to assign a shortcut to each of the number keys ("**0**", ..., "**9**") on the control-panel keypad (with the eventual respective parameter) which will activate when the key is pressed.	Codes, selected code, Shortcut details	0/9 Key shortcuts
Shortcuts activated via function keys	In this section you can associate a shortcut (and eventual parameter) with each of the function keys ("**F1**", ..., "**F4**") to be activated when the key is pressed (refer to "*Shortcuts by default*").		F1/4KeyShortcuts
Timer	This section allows you to assign a timer to the code. The code will be operative only at the pre-set times.	Codes, selected code, Enablement details	Timers

Chapter 13 Programming events

The programming of events includes the programming of actions that the control panel must carry out at the occurrence of events. The control panel recognizes all of the events described in this paragraph and, in accordance with programming, is capable of generating pre-programmed actions for each event, both when the event occurs and when it restores/ends.

The actions are:

- activation of outputs
- activation/deactivation of outputs
- event notification via telephone call
- send SMS text messages
- event storage
- management of voice messages
- management of the option of each event
- activation of event related shortcuts
- Roll up/Roll down of roller shutters

Telephone notifications (calls) are queued and sent out in chronological order. However, some events may need to be notified immediately (for example, use of a code under duress), therefore, such events can be given priority by selecting the "Priority" option.

Event notification via e-mail requires the use of the LAN board (refer to "*Programming of PrimeLAN and PrimeWiFi*").

Notification of events via predefined SMS messages requires the use of a Nexus (refer to "*Text for SMS messages*").

Note

If a list of phone calls is programmed for the notification of an event as well as SMS messages, the SMS messages will be sent before the phone calls.

The following table shows the events the control panel recognizes ("*Event type*"), the number of events for each type, the activation and reset modes of each event and if the event is a pulse type event.

Via software

Click on the **Events** button on the menu on the left to access the various sections on the right:

- **Events list**, this section is where all the available events and their parameters are listed.
  The programming field above "Event type" performs a filter on the display of events, in accordance with the type.
  Selecting one of these items allows you to set the parameters of the single event by clicking on the button.
- **Event maintenance**, this section groups together all the fast programming functions of the events.
- **Configure other outputs**, this section allows you to configure the set of outputs selectable for each individual event in the "Other outputs" section.
- **Output scenarios**, this section allows you program the scenarios of the outputs that are to be associated with activation and reset of each event.

Via keypad

`Type in code` (Installer PIN), `PROGRAMMING Events`

This section allows you to program the various options of each selected event.

1. Using the and buttons select the event type and press **OK**.
2. Using the and buttons select the single event from the previously selected type and then press **OK**.
3. Select:

- **Activation**, to program the actions to be carried out when the event occurs.
- **Restoral**, to program the actions to be carried out when the event ends.

4. Set the parameters relating to the event activation or reset actions.

13.1 Events parameters

Table 13.1: Single event parameters

Parameter		Software section	Installer menu section
Activation / Restoral	The actions are arranged on lines in a table, each with a checkbox for its activation when the event occurs and a checkbox for the activation of the action when the event restores.	Events list, selected event, Actions	Events, "Event type", "event", Activation / Restoral
Tel. number "x"	This section allows you to select the phone numbers to call on event activation/reset.		TelephoneNumbers
Output	Checkboxes for the selection of the output to be activated on activation/restoration of each event.		Outputs
Notification to Cloud	If the control panel is registered to the Cloud service, a notification is sent when each event is activated/restored.		–
Activate periodic event	When the event occurs, the system will generate Periodic event number 1.		Options StartPeriodicEv.
Clear call queue	When the event occurs, the system will cancel the outgoing call queue.		Clear call queue
Memory	If this option is enabled, activation/restoral of the event will be saved to the events log.		Event ON to log/Event OFF to log
Voice message on keyp. 001	Activation of message playback on the keypad must be set on the keypad at address "001" on activation/restoral of the selected event.		Local Message ON (for activation) LocalMessage OFF (for reset)
Output scenarios	This section provides boxes for the selection of one of the 50 output scenarios, a field for event activation and one for event reset.		–
Shortcut on event	This programming field is for the selection of a control panel operation that will be activated automatically when the event occurs (refer to "*Shortcut on event*"). This field is followed by a further two fields for the definition of the respective parameters.	Events list, selected event	–
Activate roller shutter	Activation command selection checkboxes (outputs and activation type) that occur when the event occurs.		–
Sounder/flasher pattern	If a sounder/flasher is included in the outputs, its activation will occur in accordance with the selected pattern.		Types of tones
Silent event	If the event occurs, the system will generate silent calls which will not be signalled on the keypads.		Options Silent event
Force call to alternative channel	All telephone calls programmed for the event will be diverted to the channel that is the alternative of the one indicated by the **Channel** parameter in the programming of each telephone number (refer to "*Telephone numbers*").		ForceAlt.Channel
Priority event	Calls associated with this type of event have priority over all other calls. Therefore, if a priority event occurs, any ongoing calls will be interrupted and the priority-event call will be sent immediately.		Priority
Enable SMS mess.	When the event occurs, the control panel will send an SMS message to all the duly enabled telephone numbers (refer to "*Telephone numbers*", parameter "*Receive SMS*").	Events list, selected event, Nexus	Enable SMS
Automatic SMS	If enabled, the dispatched SMS message will consist of the event description contained in the Events log.		Automatic SMS
SMS number	If the "Automatic SMS" option is not activated, the SMS message, selected from the 50 available on the Nexus, will be sent (refer to "*Text for SMS messages*").		–

Parameter		Software section	Installer menu section
Configure object	At the bottom of the section is a button that accesses directly the programming section of the object (system component) associated with the selected event.		–
Other outputs	This section allows you to activate additional outputs (besides the one programmed for the "Outputs" parameter) in connection with the verification or restoral of the event.	Events list, selected event, Other outputs	Events, "Event type", "event", Activation/Restoral, Other outputs
Maximum number of events	Box for entering the maximum number of events to be notified within a given time window. If different from "0" it is possible to set the time window (1, 2, 4, 8 or 16 hours), or activate the "Do not disturb at night (from 23:00 to 07:00)" option.	List of events, selected event, Maximum limit of events for a time window	–

Note

The "Force call to alternative channel" option is valid only with Nexus installed.

Output

For the conditions of Zone alarm, Terminal tamper, Partition alarm, Partition in Stay-mode alarm and Partition tamper, if a monostable output is programmed in the "Outputs" parameter, the event will reset when, at the end of the monostable time, the event has actually returned to stand-by status.

If the event status returns to stand-by while the monostable time is running, the event itself will not be restored.

Note

If the output has the "Do not deactivate on reset" option enabled (refer to "*Outputs*") and is programmed to restore when the event occurs, it will be deactivated when the event occurs.

Other outputs

The section for the selection of additional outputs provides a list of outputs.

These outputs were in turn selected from the list of all the outputs configured via another programming section. In this further section, common to all events, there are 16 outputs for activating the event and 8 for restoring it.

Via software

By clicking on the **Events** button on the menu on the left, the **Configure other outputs** page will be shown in the section on the right and will provide a list of the outputs for use as "Other outputs" with a selection checkbox for each one.

Via keypad

Type-in Code (Installer), PROGRAMMING Events, "event type", "event", Activation/Restoral, Other outputs

In this section, it is necessary to first select one of the additional outputs and then associate it with one of the configured outputs.

Sounder/flasher pattern

This section deals with the selection of the audible and visual signals emitted by the sounder/flashers when these are programmed in the "Outputs" and "Other outputs" sections.

This is a parameter of the event, therefore, if several sounder/flashers have been programmed in relation to a specific event, they will all emit the programmed tone when the event occurs. If a sounder/flasher has been programmed in relation to respond to several events, it will emit the last tone type setting received in order of time.

Limitation of notifications

The Prime/STUDIO software allows limitation of the number of notifications of the occurrence of a single event within a given time window. This limitation will be applied to the:

- sending of events to the Inim Cloud service
- generation of phone-calls
- generation of SIA-IP notifications
- activation of the outputs connected to the event (both individual and belonging to scenarios)

The limitation of events does not apply to the:

- activation of on event shortcuts
- events log

The software requires the "Maximum number of events", i.e. the maximum allowed number of notified occurrences of the same event within a time window, to be defined and which starts from the first notification. Within the successive time window, the number of reportable events allowed will decrease by one until it reaches the value "0". At the end of the relevant time interval, the parameter will reset completely.

It is also possible to activate the "do not disturb during the night" option. With this option activated, the event will not produce any notification if the maximum number is reached previously within the set time interval and will repeat itself during the night (from 11pm to 7am) before the number is reset.

13.2 Voice and digital dialer for the event

The programming of a single event also includes the association of the occurrence of the event with a voice message, a combination of 3 voice messages, and a message with a digital protocol.

Voice message

Each event can be associated with 3 voice messages, selected from the message list (refer to "*Voice messages*"):

- Message type
- Message A
- Message B

This feature allows you to create messages which will be played during event-related voice calls to contact numbers, both at the start and end of the event.

The choice of the messages to be programmed and the replace sequence of these, depend on the setting of the "AutomaticDialer" option.

The following table shows the voice-message sequence in accordance with the previously mentioned parameters and options.

Table 13.2: Event-related messages

	"Automatic dialer" option enabled	"Automatic dialer" option disabled
Message type	Plays the message relating to the event type (e.g. "zone alarm", "Mains failure"). This message should not be changed.	You can select any message from 1 to 219
Message A	Blank message, editable	
Message B	Contains event details, for events which are not distinctive (e.g. the "zone alarm" event indicates the zone concerned).	
Event Activation Sequence	1. Message type + 260 2. Message A 3. Message B 4. "Location" (244)	1. Message type 2. Message B 3. "Location" (244)
Sequence in the event of Restoral	1. "Restoral" (97) 2. Message type 3. Message A 4. Message B 5. "Location" (244)	1. Message A 2. Message B 3. "Location" (244)

Note

If an event is programmed with the "Automatic dialer" option enabled, the "Message type" parameter will identify messages from 420 to 484, that is, messages containing descriptions of the event types.

Table 13.3: Voice dialer parameters

Parameter		Software section	Installer menu section
Automatic dialer	If this option is enabled, the system will configure an optimal sequence of the messages for the activation/restoral of the event. It is however possible to choose different messages from those available, but the option activated in this way imposes a limited choice depending on the type of event.	 Events list, selected event, Voice dialer	Events, "Event type", "event", Activation/Restoral, Options, AutomaticDialler
Send address	Option that adds the message corresponding to the recorded address to the message sequence.		Send address
Message type **Message A** **Message B**	Section for the selection of the messages.		Events, "Event type", "event", Activation/Restoral, Message type Message A Message B
	Button to listen to the combined message.		–

Digital message

The digital message associated with the occurrence of the event follows the protocols in accordance with the following parameters:

Table 13.4: Voice dialer parameters

Parameter		Software section	Installer menu section
Class code	This is the CONTACT-ID reporting format Class-Code which corresponds to the event.	Events list, selected event, Digital dialer	Events, "Event type", "event", Activation/Restoral, Class code
Event Code on Activation/Restoral	This is the 2-character alphanumeric code, which corresponds to the activation/restoral of the event sent the alarm receiving centre (ARC).		Event code
SIA protocol	If the event is associated with calls using SIA protocol or SIA-IP, this parameter allows you to program the event code in accordance with SIA standard by selecting it from the list.		SIA Codes

Event code

For zone and terminal events (alarm, tamper, bypass), the "CCC" field of the CONTACT-ID protocol counts the number of physical terminals.

SIA Codes

An explanatory table of all the SIA codes is provided in the support manual for the installer and programmer.

13.3 Shortcut on event

Exclusively via software, it is possible to program for each event the shortcut that will be activated on the activation of the event itself.

These shortcuts function differently from those which can be activated by the user (refer to "*Shortcuts by default*") and allow the control panel to activate automatically determined operations when the event occurs.

Via software

Click-on the **Events** button on the menu on the left, then from the "Programming section on the right select the single event to be programmed.

The "Shortcut functions" section provides check boxes that allow the selection of the shortcut and definition of the relative parameter:

Table 13.5: Shortcut on event

Shortcut	Function	Parameter
Activate scenario	Shortcut that activates the scenario selected in the checkbox alongside.	One of the 30 shortcuts available
Activate output	Shortcut that activates/deactivates the output selected in the checkbox alongside.	One of the configured outputs
Deactivate output		
Zone bypass	Shortcut that deactivates/activates the zone selected in the checkbox alongside.	One of the configured zones
Unbypass zone		
Disable code	Shortcut that deactivates/activates the code selected in the checkbox alongside.	One of the available codes
Enable code		
Disable key	Shortcut that deactivates/activates the key selected in the checkbox alongside.	One of the available keys
Enable key		
Delete alarm memory	Shortcut that deactivates the outputs relative to zone/partition alarm and tamper events and deletes the partition and system alarm and tamper memories. This shortcut operates on the partitions selected for the scenario.	One of the 30 shortcuts available

13.4 Maintenance of events

Table 13.6: Single event parameters

Parameter		Software section	Installer menu section
Reset CONTACT-ID default	Button to reset the default values of the digital communicator for all the events.	Event maintenance	Default settings, CONTACTIDDefault
Delete activation/restoral outputs	The sections with a **Delete** button allow you to delete all the outputs associated with the activation/restore actions of each event.		–
Delete activation/reset notifications to Cloud	Sections with a **Delete** button for the deletion of all notifications to cloud service set for the activation/reset of each event.		–
Delete activation/restoral calls	The sections with a **Delete** button allow you to delete all the phone calls associated with the activation/restore actions of each event.		–

Parameter		Software section	Installer menu section
Delete voice message playbacks on activation/reset	The sections with a **Delete** button allow you to delete all the voice message on keypad playbacks associated with the activation/restore actions of each event.		–
Reset SIA protocols to default	This section provides a **Reset default** button that resets the default settings of SIA protocol codes for all the events.		Default settings, SIA defaults
Delete shortcuts on event	This section provides a **Delete Shortcuts** button that cancels the "Shortcut on event" parameters on all the events.		–

13.5 Periodic events

The Prime control panel provides 4 periodic events.

Programming of these events includes the date and time of the first activation and the periodicity.

The activation of the first periodic event can be driven by other events (see the "Activate periodic event" option, "*Events parameters*").

Table 13.7: Periodic event parameters

Parameter		Software section	Installer menu section
Periodic event	Programming field for the date and time of the first "Periodic Event" You can write the setting on the control panel by means of the **Write on control panel** button.	Control panel parameters, Periodic event	Other parameters, Periodic ev., Periodic ev. "x" Time per. Event
Periodic event Interval	This parameter allows you to set the interval between "Periodic events" (expressed in minutes or hours). To disable the "Periodic event" completely, set "0".		PeriodicInterval Options, PeriodicEv. InMin
Continuous periodic event	If enabled, the system will generate the corresponding periodic event regardless of its initial date/time. The event will be generated when the programming session is exited, or when the system starts up, and will be generated continuously when the set period expires.		Options, Per.Ev. Continuous
Write on control panel	This button writes the setting on the control panel.		–

Note

Set the date and time of first occurrence following the current date and time of the control panel.

13.6 Programmable events

A group of events is available for installer programming. Event activation and restoral depend on a combination of other control panel events based on logical operations, counters and timers.

On account of their enhanced flexibility, special attention is required during the programming and testing phases of the programmable events. The effects of the programmable events must always be rigorously tested.

Each programmable event consists of a mathematical-logic formula of events, timers and counters. The programming structure consists of:

- 30 events programmable for Prime060S and Prime060L, 50 for Prime120L and 60 for Prime240L and Prime500L control panels
- 40 timers
- 10 counters

Via software

Click on the **Events** button on the menu on the left then, from the "Events list" on the right, select the "Programmable event" option in the "Event type" field.

All the available programmable events will appear in the list below. Selecting an event accesses its programming section. The menu bar of this section provides the **Equation** button which opens a window where you can define the event.

This window is divided into two sections:

- Equation
- Timers and counter details

Table 13.8: Programmable event

[A]	Section for the compilation of the logical expression.
[B]	Section for the definition of the timers and counters.
[C]	Selection field and button for the inclusion of the verified control-panel event to be included in the equation. The restoral of the event is included using the event followed by the "NOT" operator.
[D]	Selection field and button for the inclusion of the timer.
[E]	Selection field and button for the inclusion of the counter.
[F]	Selection field and button for the inclusion of the button.
[G]	Button for entering the logical operators in the expression.
[H]	Buttons for the deletion of the entire expression or the last element of the expression.
[I]	Field for the visualization of the expression.
[J]	Button for the commutation of the visualization mode of the equation (parameters/descriptions of parameters).
[K]	Field for the addition of eventual notes..

Equation

The logical expression of the event includes various parameters, which may have a "real" value (either "1" or "active" - as in the case of a verified event) or a "false" value (either "0" or "not active" - as in the case of a restored event):

Timers

A timer is a logical expression element (it may have an "active" or "non active" value). It is characterized by an interval, therefore, you must specify an interval (in seconds) for each timer you wish to include.

You can select up to four "Start events" (i.e. control panel events which trigger the timer) and up to four "Reset events" (i.e. control panel events which interrupt the timer). You can specify the "Edge" for each of the eight events, that is, the status passage of the selected event ("Activation", "Reset" or "Both").

The last two options allow you to choose when the timer will be "active":

- **Timer active on Start event**. The timer will become "active" on start, that is, when a start event occurs, and will remain "active" for the sat time. The timer will become "non active" when the set time expires or when a reset event occurs.
- **Timer active with delay**. The timer will remain "non active" on start, that is, when a start event occurs and will remain "non active" for the specified time. The timer will become "active" when the specified time expires.

Note

A timer with the "timer active with delay" option enabled will remain "active" until a reset event makes it "non active" again.

Counters

A counter is a logical expression element. It is characterized by an increasing value ("Count"). The counter will have a "non active" value until it reaches the set value, which will take the counter to the "active" value.

You can select up to four "Start events" (i.e. control panel events which increase the counter value) and up to four "Reset events" (i.e. control panel events which annul the counter). You can specify the "Edge" for each of the eight events, that is, the status passage of the selected event ("Activation", "Reset" or "Both").

It is necessary to define an "Autoreset" time that will zero the count when, between two successive increases, a superior time elapses. If you do not desire an "Autoreset" time, you must set the time at "65535", already set by default, in order to ensure that the count never expires.

Note

You should not set an "Autoreset" value of less than 5 seconds.

Once the event programming process is complete and the event is sent to the control panel, the event programming values will be checked for errors.

13.6.1 Examples of programmable events

If you want to generate an alarm (i.e. activate sounder/flashers and calls) when only two PIRs (DET1 and DET2) go into alarm status within a pre-set time.

1. T0000; timer 1 will activate when the "Zone alarm DET1" Start event activates for 30 seconds
2. T0001; timer 2 will activate when the start event of the "Zone alarm DET2" S activates for 30 seconds
3. Both conditions must occur together (AND)

   T0000 AND T0001

4. Therefore, it is necessary to program the activation of the sounder/flasher and telephone calls for the event organized in this way.
5. If the programmable event activates an on-BUS sounder/flasher, associate its deactivation with an event.

If you wish to activate an output for 40 seconds when key 17 is used to arm partition 1, and to disarm and the same output when the partition disarms.

1. T0000; associate timer 1 with the activation of the Start event of key 17 recognition
2. T0000; timer 1 with a 40 second timeout, "timer active with delay" option enabled
3. T0000; associate timer 1 with the restoral of the reset event of partition 1
4. Programmable event 1 must be programmed as:

   T0000

5. Select the output you want to activate in concurrence with the programmable event
6. If the programmable event activates an on-BUS sounder/flasher, associate its deactivation with an event.

If you wish to receive a phone call when a zone q, which belongs to partitions 1 and 2, is violated and one of the two partitions is armed

The automation zone q always generates the zone alarm event (even when the partitions are disarmed). However, the programmable event will occur only when the zone q is in alarm status and at least one of the two partitions is armed.

1. Configure zone q as "automation" belonging to partitions 1 and 2
2. Remove all the outputs and phone calls associated with the "Alarm zone q" event
3. The programmable event must be programmed as "Alarm zone q" AND ("Partition 1 armed in away mode" OR "Partition 2 armed in away mode"):

   E0010 AND (E7215 OR E7216)

4. Associate the programmable event with the phone call you wish to receive

If you wish to activate a telephone call after 3 consecutive wrong code entries (with a maximum of 120 seconds between each entry).

1. C0000; counter 1 will activate on activation of the "False code" Start event, with a count of 3, 120 second autoreset time
2. The programmable event must be programmed as:

   C0000

3. Associate the programmable event with the phone call you wish to receive

If you wish to activate a telephone call and output when at least two detectors out of 5 go into alarm status.

1. The programmable event must be programmed as (“Alarm zone 1” + “Alarm zone 2” + “Alarm zone 3” + “Alarm zone 4” + “Alarm zone 5”)>=2

   (E0000 + E0001 + E0002 + E0003 + E0004) >= V0002

2. Associate the programmable event with the phone call you wish to receive and the output you wish to activate.

Chapter 14 Programming keys

Key programming consists of setting the parameters of the keys and remote-control devices for user access to the partitions protected by the Prime system.

Each digital key and remote-control device must be enrolled separately on the system in order to allow it to operate.

14.1 Enrolling keys

The enrolling procedure is carried out in this section, as follows:

Via keypad

`Type in code` (Installer), `PROGRAMMING Keys, Enroll`

1. The readers present in the control panel configuration will be shown. Select the reader for enrolling the keys, then press **OK**, if you select a reader simulated by a transceiver, a "W" will be shown at the end of the description.
2. Select the digital key you wish to enroll and press **OK**; if you are using a non-simulated proximity reader, all the LEDs will begin to blink to indicate that it is ready to enroll the key.
3. The keypad will indicate the current description of the key concerned.
4. Hold the digital key in the vicinity of the reader and then move it away. In the case of a wireless keyfob, press simultaneously keys **3** and **4**.
5. The keypad will emit a beep to confirm that the key has been successfully enrolled. If you are using one of the proximity readers, the red LED will go On.
6. The digital key description on the display will pass to the next key automatically. This method (from step 4.) allows you to enroll as many digital keys as the system requires.
7. Once you have completed the enrolling process, press "**Esc**" or "**C**".

Note

All the enrolled keys will be enabled to operate the system immediately.

Delete keys

`Type in code` (Installer), `PROGRAMMING Keys, Delete key`

This section allows you to delete enrolled digital keys from the system configuration. The enrolled digital keys can be found in the list with the ▣ symbol.

1. Use keys ▽ and △ to select the enrolled digital keys to be deleted.
2. Press □ to delete the selected key.
3. Press **OK** to confirm and exit.

Through an appropriate section of the installer menu it is also possible to delete all the enrolled keys at once. This section can be reached as follows:

`Type in code` (Installer), `PROGRAMMING Default settings, Only keysDefault`

Key enablements

`Type in code` (Installer), `PROGRAMMING Keys, Enable/disable`

This section allows you to enable/disable the digital keys. These operations are not irreversible:

1. Use keys and to select the key in question.
2. Use keys and to enable/disable the selected key.
3. Press **OK** to confirm and exit.

14.2 Key PINs Database

Each key has a PIN, an integral part of the key itself, which is transferred to the control panel during the key programming process. It cannot be set by the user and is considered sensitive data.

The Prime/STUDIO software provides a section for the saving of code PINs in a database for their eventual retrieval during control panel resetting or reprogramming phases.

This function allows you to read or rewrite on the solution in progress the PINs of all the keys previously registered on the control panel without them being shown to the installer or operator.

An encryption algorithm hides from the installer the sensitive data of the codes contained both in the Prime/STUDIO solution and in the programming storage database.

Via software

1. Click the **PIN/Key** button on the menu on the left.
2. Enter a valid user code that is qualified as "Master" and enabled on all partitions in the "Master Code" programming field.
3. Select the "Keys" page for the PINs of registered codes.

4. During the PIN reading phase, click on the "Read from control panel" button to load the PINs from the control panel or click on the "Read from database" button to load them from an existing database.
   The software reads the PINs and matches them to the codes without making them visible (instead "****" will be shown).

5. During the PIN saving phase, click on the "Write on control panel" button to load the PINs on the control panel or click on the "Read from database" button to load them from an existing database.

14.3 Key parameters

Via software

Click-on the **Keys** button on the menu on the left, the section on the right will provide a list of all the available keys and their parameters. By selecting one of these items it is possible to set the parameters of the single key by clicking on the button.

Via keypad

`Type in code` (Installer), `PROGRAMMING` `Keys`, "`key`", `Key parameters`

This section allows you to program the various options of the selected key.

Table 14.1: Parameters for single key

Parameter		Software section	Installer menu section
Description	This is an editable field for the key name/description.	 Keys, selected key	
Partitions	This section allows the installer to establish which partitions the key can control.		
Timers	This section allows you to associate a timer with the key in order to filter the operability of the key on a time basis.		
Shortcut	In this section it is possible to set the shortcuts (with any related parameter) that the key can activate at a reader. Each shortcut is associated with the lighting-up of a specific reader LED: • F1 - red LED • F2 - blue LED • F3 - green LED • F4 - yellow LED In the case of wireless keys, the shortcuts are activated by pressing the buttons the remote control device: • Shortcut 1 - pressing the F1 button • Shortcut 2 - pressing the F2 button • Shortcut 3 - pressing the F3 button • Shortcut 4 - pressing the F4 button • Shortcut 5 - pressing the F1 button for 2 seconds ('super key') • Shortcut 6 - pressing the F2 button for 2 seconds ('super key') • Shortcut 7 - pressing the F3 button for 2 seconds ('super key') • Shortcut 8 - pressing the F4 button for 2 seconds ('super key')		Keys, "key", Key parameters
Parameter	It is necessary to specify a further parameter for each shortcut: • "Execute Arm/Disarm", the parameter is one of the scenarios • "Activate output", the parameter is an output • "Deactivate output", the parameter is an output • "Activate output scenario", the parameter is one of the scenarios • "Panic", the parameter will be one of the panic events • Access shortcuts to menus and data viewing on keypad displays, the parameter is the reference access code		
Patrol	The key will be a "Patrol" key.	 Keys, selected key, Options	Keys, "key", Change key, Options
Maintenance	The key will be able to block outputs associated with alarm/tamper events for the time that it is held in the vicinity of a reader.		
Wireless	This option indicates whether the previously enrolled key is a wireless key or not.		
Use key shortcuts only	If a key is held in the vicinity of a reader, only the key shortcuts will be indicated and not the reader shortcuts.		Use keyShortcuts
Total disarming disabled	If a key is held in the vicinity of a reader when some partitions are armed, the Disarm option will be inhibited (all LEDs Off).		DisarmNotAllowed
Valid key	A key is available that allows direct access to the programming section of the access to the system event via a valid key.	 Keys, selected key	Events, Valid key

Shortcut visualization

If a digital key is held in the vicinity of a reader, the LEDs will run through a series of visual signals with the following meanings:

Table 14.2: Readers - LED visualization

LED On sequence		Option: Use key shortcuts only	
		enabled	**disabled**
1	Red LED On	Key shortcut F1	shortcut associated with the red LED on the reader
2	Blue LED On	Key shortcut F2	shortcut associated with the blue LED on the reader
3	Green LED On	Key shortcut F3	shortcut associated with the green LED on the reader
4	Yellow LED On	Key shortcut F4	shortcut associated with the yellow LED on the reader

LED On sequence		Option: Use key shortcuts only	
		enabled	disabled
5	All LEDs On	This sequence does not occur	Key shortcut F1
6	All LEDs Off	Option: Total disarming disabled	
		enabled	disabled
		No request to arm all the partitions common to both the key and reader.	Request to disarm all the partitions common to both the key and reader.

Note

The "Use only key shortcut" and "Total disarm disabled" options have no effect for wireless keyfobs.
If the key shortcut is a "Go to menu" type shortcut and the key is read at a keypad reader, the requested menu will be shown on the display with the credentials of the code that were programmed as a parameter of the shortcut.

Chapter 15 Voice messages

The Prime provides a programming section for the recording and playback of all voice messages.

The Table in the Appendix shows all the pre- recorded messages provided by the SmartLogos30M voice board ("*Pre-recorded messages*").

Via software

By clicking-on the **Voice messages** button on the menu on the left, the section on the right will give access to several sections:

- **Messages list**, this section is where all the available voice messages and their parameters are listed.
  The "Message category" box at the top implements a filter on the display of messages, depending on the category it belongs to.
  Selecting one of these options makes it possible to set up the single message by clicking on the button or to listen to it by means of the relative button  .
- **Voice board maintenance**, section for formatting the SmartLogos30M voice board.

The menu bar of these sections has the following buttons:

Table 15.1: Voice messages, menu bar

Button		Function
	**Import**	Keys to import/export the voice message programming
	**Export**	
	**Execute Text to speech**	Button to apply the text to speech setting to the selected messages. The texts entered in the "Text to speech" section will be converted into audio files and associated with all the messages selected in the table.
	**Configure Text to speech**	Button to open a window where the "text to speech" settings can be changed
	**Invert selection**	Button to invert the selection of the messages
	**Delete**	Button to delete the selected messages

Via keypad

`Type-in Code` (Installer), `PROGRAMMING Messages`

This programming field allows the selection of the single message. Afterwards it will possible to listen to, record or delete the recording.

15.1 Voice message parameters

Table 15.2: Single voice message parameters

Parameter		Software section
Nr.	Message index inside the voice board memory.	 Messages list
Description	This is an editable field for the message description.	
Type of coding	Type of coding for the message: • No Message, no playback, no recording • High quality, for superior recording/playback quality • Average quality, for recording/playback quality compatible to phone-line quality	
Quality	Checkbox to indicate the recording quality of the associated audio file.	
Time	This is the duration of the associated audio file (expressed in seconds).	
Text to speech	Text of the associated audio file	
Message category	This is the message type the selected message belongs to.	 Messages list, selected message
Note	This field allows you to edit the text you wish to associate with the message.	
Recorder	This section provides software for the playback and recording of audio files. Through which it is possible to edit the audio file associated with the message: • Load an audio file (.wav) • Play the loaded audio file • Record a new audio file • Reset the selected file to default	
Good/Average Quality	Button for the selection of the sound quality of the audio file.	
Text to speech	This section allows you to edit the text which will be converted to an audio file and associated with the message. The conversion and association with the message will occur after the execution of text to speech (in this section this can be done using the record button).	

Via keypad

`Type-in Code` (Installer), `PROGRAMMING Messages`, `"message"`, `Record`

Before recording a voice message it is necessary to select:

- **No Message** - no recording or playback
- **High quality**, for superior recording/playback quality
- **Average quality**, for recording/playback quality compatible to phone-line quality.

High quality messages occupy twice the memory space of average quality messages of the same length.

The recording phase will start when the **OK** button is pressed, the recording time (in seconds) will be indicated by a second counter on the display. To stop the record/playback operation manually press **OK**, otherwise, it will end automatically when the pre-set time expires.

`Type-in Code` (Installer), `PROGRAMMING Messages`, `"message"`, `Play`

Message playback section. The volume can be adjusted during the playback phase by means of keys ▽ and △.

`Type-in Code` (Installer), `PROGRAMMING Messages`, `"message"`, `Delete`

Section for the deletion of the message. The control panel will ask for confirmation before deleting the message by means of the **OK** button.

15.2 Voice board maintenance

Table 15.3: Voice board maintenance operations

Parameter		Software section
Read all messages from the control panel	Button that allows the reading from the control panel of all the messages on the voice board.	Voice board maintenance 
Write all messages on the control panel	Button that allows the writing on the control panel of all the programmed voice messages.	
Check SmartLogos30M board	Button to start a check on the voice board and obtain information regarding its firmware version.	Voice board maintenance, Formatting the SmartLogos30M board
Formatting the voice board	Button to start the formatting process of the voice board in order to align the firmware version with that of the control panel. The following formatting options are available: • Preserve previously-recorded messages • Format using default messages	

Chapter 16 Keypad shortcut and icon

The Prime provides two programming sections to edit the shortcut icons that appear on the keypad display in correspondence to keys **F1**, ..., **F12**.

The basic icons and association with the shortcuts at default are shown in the table in "*Default Shortcuts*".

16.1 Icons

Via software

Click on the **Icon** button on the menu on the left, the section on the right will provide a grid with the 80 available icons. Of these the last 30 are "blank" icon spaces.

Selecting one of these blank spaces opens a page where it is possible to edit:

- **Description**, the descriptive string associated with the icon.
- The graphics of the icon can be changed using digital graphic tools.

16.2 Association shortcut-icon

Via software

Click on the **Association shortcut-icon** button on the menu on the left, the section on the right will provide a grid with all the 38 available shortcuts and their associated icons.

The selection of one of these icons opens a section in the lower part of the screen showing all the 80 icons and their descriptions. Clicking on any one of these associates it with the selected shortcut.

Via keypad

1. Accessing the "Shortcuts" section:

Type-in Code (Installer), PROGRAMMING Shortcuts

2. Use keys and to select the shortcut then press **OK**.
   Set the parameters:
   - **Description** - this is the descriptive string of the shortcut which can be customized by the installer.
   - **Icon**, this allows the selection of the icon associated with the shortcut, by indicating the icon number
3. Use keys and to scroll across the digits of the number.
4. Use the number keys to edit the number.
5. Press **OK** to confirm and exit.

Chapter 17 Events log

Via software

Click-on the **Events log** button on the menu on the left, the section on the right will allow the viewing of all the events saved to the control panel via a table, in which each row refers to a single event and the columns show the related data.

Table 17.1: Events log via software

Parameter		Note
Num.	Number which indicates the chronological order of the events in the log.	You can group the events into categories by dragging the header of the required category to the grey line above the columns.
Date/Time	Event date and time	
Event	Type of event	
Filter	Parameters for further event details.	
Agent		
Location		
Category	Logic grouping of events	
Num.	Number which indicates the chronological order of the events in the log.	
Date/Time	Event date and time	
	Button to download the events log from the control panel.	These buttons are active only when you are working on a solution or a database. In particular, the **Save** button is enabled after a reading from the control panel.
	Print button for the events log	
	Button to save the contents of the events log to the database.	
	Button to load the contents of the events log from the database. A from-to period will be requested, if no particular period is specified the entire contents of the Events Log will be loaded.	
	Button to delete the Events log from the database. A from-to period will be requested, if no particular period is specified the entire contents of the Events Log will be deleted.	

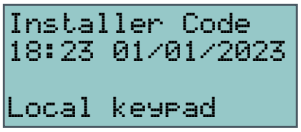
Via keypad

`Type-in Code` (Installer), `PROGRAMMING User functions, View`

This section allows you to display the event log on the keypad, also through the subdivision of these:

- Events log - allows the viewing of all the events saved to the log.
- Alarms log - allows the viewing of all the events relating to zone/partition alarm and tamper saved to the log.
- Faults log - allows the viewing of all the fault events saved to the log.
- Arm/Disarm ops. - allows the viewing of all the arm/disarm operations saved to the log.

Press keys ▽ and △ to scroll the chronological events list. For some events, pressing the ▷ button accesses the partition details. For example, the details of an "Arm" command will show the code and keypad concerned and, by pressing the ▷, the list of partitions involved.



Via touch-screen keypad

Access the “Intrusion” section and enter the user code. You will be provided with the “Events log”.

All the events saved to the log will be displayed one at a time. However, the up/down keys will allow you to scroll the entire list of events. Each event shows the relative details and, where possible, allows you to view the partitions involved by means of the **PARTITIONS** button.

Chapter 18 Default settings

The operations necessary for the reset of factory data vary and can be carried out by the installer in accordance with the method used to access the control panel:

- the **CLOUD REG** and **RESET** buttons on the control panel PCB
- the keypad, via the installer menu
- Prime/STUDIO software

Attention!

Reset of the factory default programming data deletes all the previously programmed parameter settings.

Note

Reset of the factory default programming data does not cancel the connection of the control panel to the Cloud.

Via PCB

1. Press and hold the **CLOUD REG** button on the motherboard.
2. Press and release the **RESET** button on the motherboard.
3. Wait 5 seconds then release the **CLOUD REG** button.

Within 70 seconds the control panel will reset the parameters factory default values, enroll all the peripherals currently on the I-BUS and, if at least one keypad is connected, will ask you to select the Language.

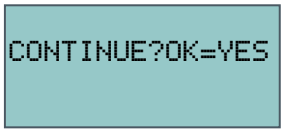
Reset to factory default data will not delete the events log.

Via keypad

Type in Code (Installer) ›PROGRAMMING Default settings

In this section it is possible to reset to factory values all the control panel parameters, auto-learn zone balancing values, auto-enroll I-BUS peripherals and reset the event codes of CONTACT-ID reporting format.

Following each of these operations, the control panel will ask for confirmation by pressing the **OK** button.



Via software

The Prime/STUDIO software program allows reset of the control panel default values only for the following parameters:

- digital dialer parameters
- "CCC" field of CONTACT-ID protocol of the zones
- SIA protocol parameters

Furthermore, the software allows you, through the "Events maintenance" section, to delete the following elements that have been associated with the activation or reset of events:

- call queue
- notifications to Cloud
- outputs
- playback on keypad

Table 18.1: Reset operations

Parameter		Software section	Installer menu section
Full reset	If you select this option, the control panel will reset all programming data to factory default settings.	-	Default settings, Factory data
Learn zone balancing	If you select this option, the control panel will gather and save the balancing settings of all the zones automatically (Patent Pending).	-	Learn zone bal.
Enroll peripherals	If you select this option, the control panel will reconfigure the IBUS and enroll in the new configuration all the peripherals that respond to the auto-enroll peripheral command.	-	Auto enrolPeriph
Reset CONTACT-ID event codes	If you select this option, the control panel will reset all the event codes used for the CONTACT-ID protocol to factory default (refer to "*Voice and digital dialer for the event*").	Events maintenance, Reset to default CONTACT-ID protocols	CONTACTIDDefault
Reassign the CCC in sequential mode	If you select this option, the control panel (after requesting confirmation) will implement incremental numbering (from "1") in the "CCC" field of the CONTACT-ID protocol for the events relative to the zone.		CONT-ID enumer.
Reset SIA protocols to default	If you select this option, the control panel (after requesting confirmation) will reset to factory default all the SIA parameters of all events.	Events maintenance, Reset SIA default	SIA defaults
Delete events programming	Pressing the **OK** button will delete all the control panel events, both on activation and restoral: • all outputs • all calls • all options • all shortcuts on event	-	DeletePrg.events
Wireless data reset	Pressing the **OK** button will delete all the data relating to the Air2-BS200 transceiver. The data relating to the detectors and wireless remote-control devices will not be deleted, nor will the devices simulated by the transceiver be removed from the configuration.	-	WLS data reset
Reset PIN codes	Pressing the **OK** button will delete all the programmed User PIN codes and will reset the default codes.	-	Reset PIN default
Reset keys	Pressing the **OK** button will delete all the enrolled keys.	-	Only keysDefault
Global restore	Selection of this function will reset the control panel to its initial condition, thus cancelling any operations carried out for its activation of the control panel itself and the selection of the language used.	-	Global restore

18.1 Auto-learn balancing

This option allows the control panel to learn the balancing settings of all the zones automatically.

Note

This function is a registered patent.

The balancing settings which are acquired correctly are:

- Normally Open
- Normally Closed
- Balancing (Single balancing)
- Double balancing
- Roller blind with EOL

The balancing settings which are not acquired accurately are:

- Roller blind without EOL (which is classified as a normally-closed generic zone)
- Double zone without EOL (which is classified as a normally-closed generic zone)
- Double zone with EOL (which is classified as a generic zone with Double balancing)

In order to allow accurate acquisition of the balancing settings of all the zones, you must:

1. Wire and select the balancing settings of all the zones.
2. Ensure, as far as possible, that all the zones are in stand-by status
3. Activate the "Learn zone bal." option.

Via keypad

Type in code (Installer), PROGRAMMING Default settings, Learn zone bal.

4. Verify that the operation has been carried properly and that all the settings are accurate (if any zones are not in stand-by status during this process their balancing will not be acquired accurately).
5. Set manually any inaccurate zone balancing settings.

Chapter 19 User functions for the installer

The installer menu on the keypad contains a section that provides the installer with the functions shared with the user.

Via keypad

1. Access the "User Functions" section of the installer menu:

`Type-in Code (Installer) , PROGRAMMING User functions .`

The options available are:

- Activations
- View
- Outputs ON/OFF
- Set date/time

2. Use keys ▽ and △ to select the required function then press **OK**.

Activations

This section provides the "Cloud enrollment" option for connection of the Prime control panel to the Inim Electronics cloud services.

View

- **Events log** - allows the viewing of all the events saved to the log.
- **Alarms log** - allows the viewing of all the events relating to zone/partition alarm and tamper saved to the log.
- **Faults log** - allows the viewing of all the fault events saved to the log.
- **Arm/Disarm ops.** - allows the viewing of all the arm/disarm operations saved to the log.
- **Nexus status** - allows viewing (on the display) the following parameters of the 2G/3G/4G communicator:

Table 19.1: View Nexus status from keypad

Line	Display	View

1	TELECOM C G	• mobile network provider (on the left side)
		• "--" indicates that the GSM card is present in the control panel
		• "C" means that data transfer is in progress
		• data network technology (on the right side)
		  ◦ G, GPRS service
		  ◦ 3G, UMTS service
		  ◦ H, HSPA service
		  ◦ 4G, LTE service

2	GSM signal 01	GSM signal reception (value between 1 and 100)
3	Remaining cred. 11	Credit balance, at the last operation (expressed in the local currency)
4	No signal	Faults present, in this case it is necessary to access the "View-Faults" section for details.

- **System voltage** - allows you to view the supplied voltage and current:
  - measured on the battery
  - power-supply of the control panel
  - measured on all 3 "AUX x" terminals of the control panel
  - measured on terminal "+" of the I-BUS
- **Zone status** - allows the viewing of the status of all the zones. Use keys ▽ and △ to scroll the list of accessible zones. The display shows the following zone parameters:

Table 19.2: View zone status from keypad

Line	Display	Generic zone	Wireless zone	Smoke detector	Thermal probe
1	FD living room LivingThermometer	Zone description			
2	Standby Unbypsed Normal value	Zone status (“Standby”, “Alarm”, “Short-circuit”, “Tamper”) and its activation status (“unbypassed” - capable of generating alarms, or “bypassed” - incapable of generating alarms)			“Normal value” or “Threshold exceeded” respectively if the temperature is below the alarm threshold or not.
3	Lev.07 000 mdB/m Temper. 25.5°C	-	Level of wireless signal (from 0 to 7)	Level of wireless signal and level of smoke present in the sensing chamber, expressed in mdB/m	Temperature read by the probe connected to the terminal with precision of a tenth of a degree centigrade
4	Res 12345 Ohm Dust level 000%	Resistance read from the terminal	-	Level of contamination present in the smoke detection chamber of a smoke detector (%)	Resistance read by the probe

Note

If the resistance value has reached the maximum readable, the string will show the writing “> 20000 Ohm”.
It is advisable to clean the smoke detector if the contamination value exceeds 90%.

- **Faults ongoing** - allows the viewing of any ongoing faults.
- **Panel version** - allows the viewing of the firmware version and model of the Prime control panel.

Outputs ON/OFF

Allows manual activation/deactivation of the outputs by means of keys ■ and □.

Write date/time

Allows the setting of the date and time of the control panel (refer to "*Prime control panel parameters*").

Via software

The Prime/STUDIO software program provides a section which, during a direct connection to a Sol control panel, allows monitoring of the entire system in real time and access to some of the above-mentioned parameters.
Select the “Monitoring” option from the menu bar.
A window containing various sections will open. The sections can be selected by means of tags, each referring to a different part of the system (refer to "*Monitoring the control panel*").

Chapter 20 Compliance with rules in force

In order to guarantee compliance with the regulations in force, you must adhere to the following guidelines:

Anti-dislodgement of control panel

The protection against control panel tamper ("*Prime control panel parameters*") must be enabled.

Zones

Zones programmed as "24 hour", "Fire" or "Automation" purposes do not comply with the EN 50131-1 and EN 50131-3 standards, as they are not covered by the standards themselves.

Zones programmed as "Arm", "Disarm", "Switch" or "Follow" comply only when activated by keyswitches with more than 10,000 code combinations.

An input is set up for system fault management.

For zones with the "Fault zone" option enabled, it is necessary to eliminate from the relative alarm event the programming of an external sounder/flasher in the "Outputs" parameter. You can program indoor sounder/flashers via the "Other outputs" option.

If a zone is categorized as "Hold-up", the description of the zone must contain the word "hold-up" and, if SIA-IP or Contact-ID communications are set, the alarm events generated must be categorized with the relative attribute and must have the option of "Priority event".

The "Hold-up" zone must always have the "Unlimited" option in the count of "Alarm cycles". You must enable the "Priority" option for any alarm events associated with "Hold-up" zones.

If a zone is categorized as "Fault" the "Alarm Pulse Duration" time must be at least 10 seconds. Furthermore, the description of the zone must contain the word "fault", and, if SIA-IP or Contact-ID communications are set, the alarm events generated must be categorized with the relative attribute.

All the zones characterized as "Intrusion", "Hold-up" and "Tampering" must have a minimum alarm pulse of 400ms (option "Al.pulseDuration" in the zone programming page).

Zone balancing

The lines relating to the intrusion-detection zones must be configured as "Double balancing" with double EOL resistors, or as Single balancing with single EOL resistor. They must also be equipped with devices which protect them against the forced-opening of their casings.

Events

"Failed to arm" and "Forced arming" events must be saved to the Events log.

All "Force arming" events must have the "Event ON to log" and "Event OFF to log" options activated.

Tamper events

Terminal tamper, peripheral tamper and control-panel tamper events must trigger audible signals (sounder signals) for a period of not less than 3 minutes.

The output activated by the previously mentioned tamper events must be different from the output activated by alarms signals.

PIN

All Code PINs must have 6 digits.

Timers

If a Timer is used for automatic-arming operations, the Pre-arm times must be programmed separately for each partition (the pre-arm time must not be set at "0").

The timer cannot be used for arm/disarm operations. Any operation of this type attributable to the control-panel timers cannot be certifiable.

Devices anti-tamper

Joy, Aria/HG, nCode/G and Concept/G keypads must be equipped with enabled tamper-protection devices.

The following devices must be mounted inside the enclosure of the control panels, if possible, or must be equipped with a device that protects them against the forced-opening of their casings (EN50131 grade 2) and dislodgement (EN50131 grade 3):

- nBy/K, nBy/X readers
- Flex2R/2T, Flex5/DAC, Flex5/R, Flex5/SU expansions
- Nexus communicators
- IB200/U isolators

Air2-Aria/W keypads must be equipped with enabled tamper-protection devices.

Flex5/R

If used in compliance with EN 50131-1 and EN 50131-3, it can drive visual/audible signalling devices only. Other types of operating modes are not considered certified in accordance with

the EN 50131 series.

Flex2R/2T

If used in accordance with EN 50131-1 and EN 50131-3, the input terminals can only be of the intrusion/robbery type and the outputs used can only be for driving visual/audible signalling devices. Other types of operating modes are not considered certified in accordance with the EN 50131 series.

Flex5/R, Flex2R/2T

The modules must be located inside a fireproof metal or plastic enclosure with flammability class UL 94-V0.

Sounder/flashers

The system must include a self-powered outdoor sounder/flasher for the signalling of intrusion-alarm events.

Telephone dialer/communicator

The telephone dialer must be enabled.

If a digital telephone dialer is used for transmissions or a voice dialer with a SmartLogos30M board, a channel and a phone number must be reserved for the following events:

- All events generated by zones with the "Hold-up" attribute.
- All events generated by: "Instant", "Delayed", "Delayed unhidden" and "Route"
- All events generated by terminal, peripheral and control panel tamper.
- All faults detected by the control panel

20.1 EN50131 grade 2 options and parameters

Compliance with EN50131 Grade 2 is guaranteed by observing the following guidelines.

Options

Table 20.1: EN50131 grade 2 - Enablement of options

Parameter		Status	Software section	Installer menu section
Wrong PIN keypad lockout	"*Keypad parameters*"	**Enabled**	Keypad parameters	Parameters Keypad lockout
Does not arm if any of the zones are not ready	"*Prime control panel parameters*"	**Enabled**	Control panel parameters	OpenZonesArmLock
Prevents the deletion of tamper memory by user code		**Enabled**		NoUserTamp.reset
Reader LED OFF	The readers LEDs will remain OFF when there are no keys near the readers themselves. As soon as a key is held near a reader and then immediately moved away, the reader will show the status of the LEDs for 30 seconds, after which it will switch OFF all the LEDs again. During this 30 second phase, the user can hold the key in the vicinity of the reader and select the desired shortcut indicated by LEDs.	**Enabled**	Regulatory compatibility, Parameters 50131	50131ReadLedOFF
Hide status	The status of the partitions will be hidden. If a valid code is entered at a keypad, the real-time status will be indicated on the keypad concerned for 30 seconds. If partitions are armed, the real-time status of the system will be hidden from non-authorized users. If the partitions are disarmed, the LEDs will function normally, the status icons will be present and the alarm and tamper events will be visible.	**Enabled**		50131NasconStato
Hide icons	If partitions are armed, the status icons will be hidden from non-authorized users. If a valid code is entered at a keypad, the status of the icons will be shown for 30 seconds. The keypad will show the real-time status of the icons when all the keypad partitions are disarmed.	**Enabled**		50131NasconIcone
Alarm delay	If an instant-zone alarm occurs on a partition while entry time is running, the associated actions (calls, output activation, save to log, etc.) will not be generated until 30 seconds after the expiry of the entry time. If the partition (or partitions) are disarmed during this period, the associated actions will not be generated, however, the keypads will indicate the violation of the instant zone.	**Enabled**		50131AllarRitard
Fault memory LED	If the control panel detects a fault, the yellow LED on the keypads will go On and will remain On even after the fault clears. To switch the yellow LED Off, clear all activating causes and reset the partition.	**Enabled**		50131LedGuastMem
Do not arm with low battery on keyfob	In the event of a request to arm a scenario from a remote-control device (keyfob), with a low battery and which has not been authorized to arm/disarm with such a battery level, activation will not be applied.	**Enabled**		50131Batt.chiave

Parameter		Status	Software section	Installer menu section
Reader Buzzers OFF	"*Reader parameters*"	**Disabled**	Reader parameters	ReaderBuzzer OFF
Bypass tamper in the event of bypassed zones	"*Prime control panel parameters*"	**Disabled**	Control panel parameters	BypassAlsoTamper
Enable context menu		**Disabled**	-	Other parameters, QuickAlarmAction
Overload AUX	A load of over 1.5A detected on the "+AUX" terminal	**Enabled**	Regulatory compatibility Forced arming faults	Other parameters, FaultForNotReady Zone fuse fault
Overload BUS	A load of over 3.5A has been detected on the "+" terminal of the I-BUS of the motherboard.	**Enabled**		IBUS fuse fault
Low battery	The backup battery is low	**Enabled**		Low battery
Mains failure	The primary power supply 230V~ fails	**Enabled**		Mains failure
Telephone line down	The land line is not working	**Enabled**		Tel. line down
Jamming	Wireless interference detected	**Enabled**		Jamming
Low battery wireless	The battery of a least one wireless detector must be replaced	**Enabled**		Low battery WLS
Wireless zone loss	Loss of at least one wireless detector has been signalled (supervisory time expired)	**Enabled**		WLS zone loss
Loss or tamper ongoing	This warning groups together the following events: • Control panel open • Keypad Tamper • Reader Tamper • Sounder flasher tamper • Keypad Loss • Reader Loss • Sounder loss	**Enabled**		LossTamp.ongoing
Requires code	"*Keypad parameters*"	**Enabled**	Configured keypads, selected keypad, General, Details	Authentication
Clear call queue on disarm	"*Partition parameters*"	**Disabled**	Partitions, selected partition	Partitions, "Partition", StopTelOn Disarm

Parameters

The "Alarm Cycles" parameter of each zone must be set between 3 and 10.
The "Mains fail.Delay" parameter must be set at no more than 1 minute.
The "Entry Time" of each partition must be set at a maximum of 45 seconds.
You must enable the "Priority" option for any alarm events associated with "Hold-up" zones.
"Failed to arm" and "Forced arming" events must be saved to the Events log.
The programmed "LowBattery delay" must not be programmed at more than 5 minutes.

20.2 EN50131-3 and EN50131-6 grade 3

The Prime/STUDIO software provides a section for a configuration of the control panel that complies with grade 3 of 50131 regulations.

However, total respect of the said regulations is obtained by appropriately setting also the other options related to grade 2. For this purpose refer to "*EN50131 grade 2 options and parameters*".

Options

Table 20.2: EN50131 grade 3 parameters

Parameter		Status	Software section	Installer menu section
This section allows you to select which faults or events, other than zones in alarm status, will be signalled as system security-risk conditions when the partition arms.			Regulatory compatibility Forced arming faults	Other parameters, FaultForNotReady
Nexus fault	The Nexus device signals a fault	**Enabled**		Nexus fault
Faults on zones	Violation has occurred on one or more zones with the "Fault zone" option enabled.	**Enabled**		Faults on zones
Sounder faults	Fault present on one of the sounder/flashers	**Enabled**		Sounder faults
General power-supply faults	Fault present on the power supply or one of the power sources	**Enabled**		Power faults
Keypad faults	Fault present on one of the keypads	**Enabled**		Keypad faults
IP connection lost	The IP connectivity test is enabled and the test has failed	**Enabled**		IP conn. lost
50131 Grade 3 Compatibility	This option activates a presetting on the control panel which adheres to grade 3 of EN50131. • only the installer code can be used to delete fault memories • the readers lock for 10 minutes after 5 consecutive attempts to use a false key • the keypads lock for 10 minutes after 5 consecutive attempts to type in a false code (valid only when the "Lock keypad" option is enabled) • bypassed zones are automatically unbypassed when the system disarms • in the presence of ongoing faults and lost peripherals, arming operations will require installer code entry	**Enabled**	Regulatory compatibility, Parameters 50131	Parameters 50131, Grade 3
Show scenario	The second line on the keypad display, on the left side, will show the description of the active scenario.	**Enabled**	Keypad parameters	Show scenario

Detectors with anti-masking protection

If the installation uses detectors with an anti-masking function, each anti-masking signal must be managed as follows:

- Prepare an input terminal for the anti-masking signal connection.
- "Description" parameter: assign an explanatory description to the signal
- Enable "Zone fault" option
- Enable the "Do not arm if zones are not ready" ("*Prime control panel parameters*")

ATS4

Use an ATS4 notification appliance:

- protocol: SIA-IP with encryption
- interface: LAN (integrated on the motherboard) or PrimeLAN

Chapter 21 Graphic map configuration

The Prime monitoring functions are based on graphic maps which can accessed by the end-user through an Alien keypad or web interface. The user, by means of access to a graphic map, can view the supervised partition and also access the security system functions.

The Alien keypad can manage up to 10 maps (revisions below 2.00 can manage up to 5 maps) and the web interface up to 20. Each map supports up to 20 objects/buttons represented by icons.

Note

In order to use the graphic maps it is necessary to use an SDcard in micro-SD format.

The card must inserted into the slot on the Alien keypad, for the configuration and access to the Alien keypad maps, or inserted into the slot on the Prime Ethernet interface board for the web accessible maps.

The programming of the maps of an Alien keypad is uniquely linked to the SDcard used. Changing the SDcard or using it in several keypads causes the programming to be completely lost and can cause keypad malfunction.

Via software

Exclusively using the Prime/STUDIO software, access to the map configuration is achieved through the sections:

- **Graphic maps of the Alien keypad** - click on the **Keypads** button on the menu on the left, from the section on the right select the "Touch-screen" keypad type to access the "Maps" section.

- **Graphic maps of the web interface** - click-on the **PrimeLAN settings** button on the menu on the left then go to the "Programming - Graphic maps" section on the right.

A field, located in the centre of both sections, shows the images of the current maps.

Above this is a bar with the icons of the objects to be inserted and the buttons to edit the current map.

To the left of this you will find the graphic-map tree with the objects inserted.

New map

The construction of a new map is carried out as follows:

1. Add a new map by clicking on the button.
2. Associate an image with the map by selecting a file by means of the button.
3. Insert an object from among those available on the icons bar.
   The objects are inserted by clicking on the respective icon on the bar and then by clicking on the point on the map where you wish to place it.
4. Load the configured map in the control panel by means of the button.

If, instead, you intend to change the maps that are already programmed in the control panel, you must first read the configuration by means of the button and then implement the changes.

Table 21.1: Map configuration buttons

Keys	Alien Programming	Programming Web interface
Object icons		
	Left-clicking on any one of the icons positioned on the map will highlight the icon which will then be shown in a frame that allows you to resize or reposition it. Right-clicking on any one of the icons positioned on the map or map tree on the left allows the deletion of the object concerned or modification of its settings; in this case a window will open showing all the editable settings (refer to "*Map object settings*").	
	Button to show or hide the map tree located to the left of the displayed map.	
	Buttons for the addition of a new map in the last position on the map tree or for the deletion of the last map on the map tree.	
	Button for the insertion or overwriting of the background image of the current map. The name of the current image file is indicated in the lower section.	

Keys	Alien Programming	Programming Web interface
	The selection of several icons by means of these buttons will allow you to create their alignment.	
	By selecting several icons, with these buttons it is possible to change their dimensions by assigning them the dimensions of the first icon selected (width, height or both).	
	Not available	The selection of an icon, by means of these buttons, will allow you to resize and reposition the icon so that it occupies a quarter of the image.
	Button to read the configured maps from the keypad or from the Prime so that they can be modified.	
	Button to write on the keypad or on the Prime the newly configured or modified maps after a reading.	

Table 21.2: Map object settings

Section	Parameter		Note
Size and position	**Height, Width, Position X and Y**	Number fields for the dimensions of the object icon and its position on the map.	
	String	Field for the string that appears over the icon.	For Alien only
		Button for the definition of the colour of the string.	
Control panel	Selection checkbox for the selection of the part of the anti-intrusion system the icon refers to.		Zone, partition, output, scenario, keypad
Map link	Field for the selection of the map the link refers to. For web interfaces it is possible to indicate the home page.		
Web cam	**URL** **jpeg, m-jpeg**	Configuration parameters for the webcam.	For the web interface only.
Images	Section containing the icons which replace the current icons in the event of status change of the represented object. For keypad maps, it is possible to indicate the strings that will appear (when the occurrence requires) below the current string, indicated previously mentioned.		
		Button to select the image that will replace the default image.	
		Button for the deletion of the selected image.	For the web interface only.
		Button for the definition of the colour of the string.	For Alien only
		Button to reset the factory default images	
Options	**Command selection window**	If enabled, touching the icon on the map will open a window on the display for command selection.	For Alien only. The commands implement a status change on the object. The type of status depends on the type of object: Arming type - for a "Partition status" object Activation/Enablement status - for a "Zone" object Activation/Enablement status - for an "Output" object Activation/Enablement status - for a "Scenario" object
	Command with authorization request	If enabled, the keypad will request user-code entry before activating the command associated with the icon.	
	Switch/Invert	If enabled, touching the icon on the map will immediately switch/invert the status of the object it represents. The "Partition status" object requires further indications relating to the arming type which is to be switched to Away status (totally disarmed).	
	Immediate command	If enabled, touching the icon on the map will almost immediately activate the command. The command can be selected from the drop-down menu which appears.	
	View status	If enabled, this option allows the visualization on the display of status changes on an object by means of changes on the icon, in accordance with the configuration selected in the "Image" section.	
		Button to reset the factory default settings.	

Chapter 22 Programming example

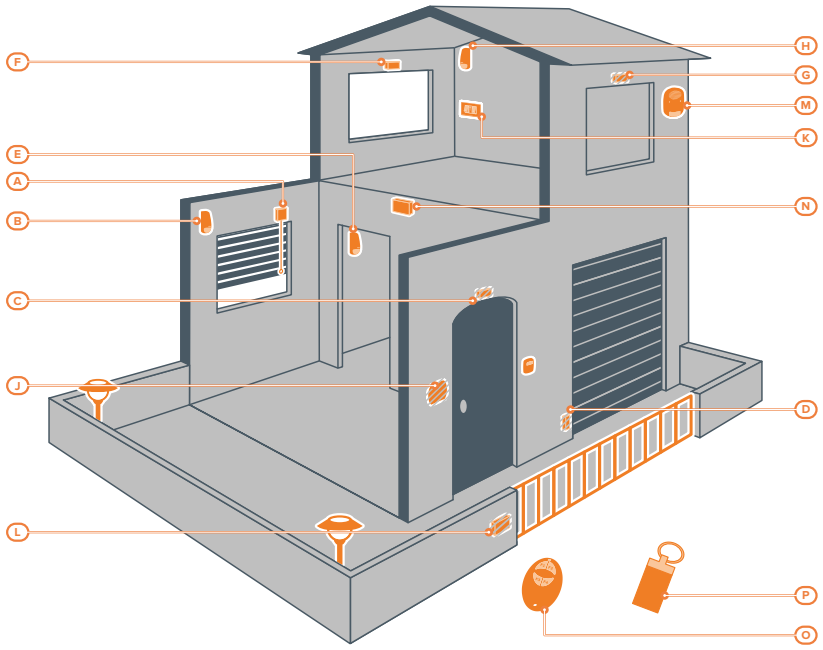
This example describes the installation of a Prime system in a residential building.

It explains the basic programming procedure that must be carried out on the installed devices and aims at staying as close as possible to the control-panel default programming.

Ideally this procedure directly follows the instructions given in the installation manual for the first startup of the system

Table 22.1: Installation example

[A]	Roller blind detector
[B]	Motion detector entrance
[C]	Magnetic contact entrance door
[D]	Magnetic contact garage shutter
[E]	Motion detector living room
[F]	Magnetic contact window 1 bedroom
[G]	Magnetic contact window 2 bedroom
[H]	Motion detector bedroom
[I]	Reader entrance door
[J]	Keypad
[K]	Reader bedroom
[L]	Expansion
[M]	Sounder/flasher
[N]	Wireless transceiver
[O]	Wireless keyfob
[P]	Key



Start programming

1. Start the programming session

Via keypad

`Type-in Code` (Installer) , `PROGRAMMING`

Via software

Start a new solution by selecting the control panel model such as the one in the installation.

Click-on the **Settings** button on the menu bar, set up the connection to the control panel .

In order to have the system configuration available, perform a read operation using the **Read** button

Programming partitions

2. Change the descriptions of the partitions:
   - Partition 1 - “Ground floor”
   - Partition 2 - “First floor”

Via keypad

`PROGRAMMING Partitions, "Partition 00x", Description`

Via software

Click on the **Partitions** button on the menu on the left, the section on the right will show the list of available partitions.

Here, by selecting the partition to configure, it is possible to change the parameter “Description”.

Programming zones

3. Program the zones (all connected to the control panel):

Via keypad

`PROGRAMMING Terminals`, select the terminal concerned

or

PROGRAMMING Zones, select the zone associated with the terminal concerned

Via software

To program the zone, select the **Terminals** button. The section on the right will show the graphic representation (map) of the terminals of the entire system.

By double clicking on the terminal concerned you will enter the terminal programming phase.

Table 22.2: Zone parameters

Device	Description	Partition	Zone type	Option	Balancing	Detector type
[A]	Roller blind detector	Ground floor	Instant	None	Normally closed	Roller blind
[B]	Motion detector entrance	Ground floor	Delayed	Interior	Normally closed	Generic zone
[C]	Magnetic contact entrance door	Ground floor	Delayed	None	Normally closed	Generic zone
[D]	Magnetic contact garage shutter	Ground floor	Instant	None	Normally closed	Generic zone
[E]	Motion detector living room	Ground floor	Instant	None	Normally closed	Generic zone
[F]	Magnetic contact window 1 bedroom	First floor	Instant	None	Normally closed	Generic zone
[G]	Magnetic contact window 2 bedroom	First floor	Instant	None	Normally closed	Generic zone
[H]	Motion detector bedroom	First floor	Instant	None	Normally closed	Generic zone

Programming scenarios

4. Add a third partial arming scenario (Stay mode) to the default scenarios (Scenario 1 "Away mode" and Scenario 2 "Disarm") of both partitions.

Via keypad

PROGRAMMING Arming scenarios, "SCENARIO 003", Partitions, "partition", Stay

Via software

Click on the **Arming scenarios** button on the menu on the left, the section on the right will show the list of available scenarios.

Here, select scenario 3, set "Stay mode" for the "Ground floor" and "First floor" partitions.

Programming readers

5. Associate the "Ground floor" and "First floor" partitions with the readers, and scenario 3 Stay mode (arm partially) to the default scenarios:

Via keypad

PROGRAMMING Readers, ChoosePeripheral, "READER 00x", Partitions

In this section you can enable the "Ground floor" and "First floor" partitions.

PROGRAMMING Readers, ChoosePeripheral, "READER 00x", Shortcut

In this section you can select the shortcut associated with the red and blue LEDs by first selecting the "Arm/disarm" type then the scenario to associate with the LED.

Via software

Click on the **Readers** button, the section on the right will show all the configured readers.

At this point, clicking on the button accesses a section where you can select the partitions to associate with the reader and configure the shortcut of the red and blue LEDs.

Table 22.3: Reader parameters

Device	Description	Partitions	Red LED shortcut	Blue LED shortcut
[I]	Reader entrance door	Ground floor First floor	Default	Default
[J]	Keypad (integrated reader)	Ground floor First floor	Default	Execute "Scenario 3" arming mode
[K]	Reader bedroom	Ground floor First floor	Execute "Scenario 3" arming mode	None

Programming keypad

6. Associate the keypad with the "Ground floor" and "First floor" partitions.

Via keypad

PROGRAMMING Keypads, ChoosePeripheral, KEYP. 001", Partitions

In this section you can enable the "Ground floor" and "First floor" partitions.

Via software

Click on the **Keypads** button, the section on the right will show the configured keypad.

Here you can associate the keypad with the partitions.

Programming expansions

7. To program the devices connected to the expansion terminals:

Via keypad

PROGRAMMING Terminals, select the terminal concerned

Press the **2** button to configure the terminal as an output. Press **OK** to access the programming menu.

Via software

To program the zone, select the **Terminals** button. The section on the right will show the graphic representation (map) of the terminals of the entire system.

Right clicking-on the expansion terminal will allow you to configure it as an output, after which a double click will access the terminal programming phase.

Table 22.4: Expansion parameters

Device	Terminal	Description	Type	Output options	Monostable time
[L]	1	Cancel	Output	Monostable	30 seconds
	2	Garden lights	Output	Monostable Switch	60 minutes

Programming keys

8. Associate the keys (*[O]* and *[P]*) with the "Ground floor" and "First floor" partitions:

Via keypad

PROGRAMMING Keys, Change key, "Key 00x", Partitions

In this section you can enable the "Ground floor" and "First floor" partitions.

Via software

Click on the **Keys** button, in the section on the right you will be able to view the keys and the partitions to associate with them.

9. Enroll the keys, using one of the proximity readers and/or a keypad.

Via keypad

PROGRAMMING Keys, Enroll, "Reader 00x", "Key 00x"

Hold the key in the vicinity of the reader and then move it away. The keypad you are working on will emit a beep to confirm that the key has been enrolled.

Programming wireless keyfobs

10. Associate the shortcuts for the arm/disarm commands and control of expansion outputs to the keyfob command buttons *[O]*

Via keypad

PROGRAMMING Keys, Key parameters, "Key 00x", Shortcut

This section will allow you to associate the shortcuts that are not default shortcuts, specifically "Activate output" shortcuts. to buttons**F3** and **F4** then select the respective outputs on the expansion.

Via software

Click on the **Keys** button then, on the section on the right, select the key corresponding to the remote control by clicking on the corresponding button .

The "Shortcuts" section will allow you to associate the shortcuts with the buttons.

Table 22.5: Expansion parameters

Device	Button	Shortcut	Parameter	Default
[O]	F1	Arm/Disarm	Scenario 1 "Away"	Yes
	F2	Arm/Disarm	Scenario 2 "Disarm"	Yes
	F3	Activate output	Cancel	No
	F4	Activate output	Garden lights	No

11. Enroll the wireless keyfob via the simulated reader of the transceiver (*[N]*, identified on the keypad by the letter "W").

Via keypad

PROGRAMMING Keys, Enroll, "READER 00x W", "Key 00x"

At this point you have 3 minutes to enroll the wireless keyfob by pressing simultaneously buttons **F3** and **F4**.

The positive outcome of the operation will be signalled by 3 blinks on the green LED of the wireless keyfob and a long audible signal on the buzzer.

Closing the programming session

12. Close the programming session after saving the modified data.

Via keypad

Press the **Esc** several times until the following message appears on the display:

EXIT? OK = YES

On pressing **OK** you will automatically exit the programming session, save the programmed data and reboot of the control panel.

Via software

Using the **Write** button carry out a write operation.

At the end of this operation the control panel will reboot and it will possible to close the software solution in progress.

Chapter 23 Monitoring the control panel

The Prime/STUDIO software program provides a section which, during a direct connection to a control panel (refer to the Software manual), allows monitoring of the entire system in real time.

Click-on the **Monitoring** button on the menu bar. The section on the right provides various sections selectable by means of tabs with headers, each one concerning different parts of the system and monitoring functions.

Some of these functions are also reachable from the keypad.

23.1 Remote keypads

Via software

Click on the **Monitoring** button on the menu bar, then go to the "Remote Keypad" section.

In this section is divided in two parts. The left hand side shows all the keypads available for the system, but only those currently connected to the control panel are highlighted (in colour).

By clicking on one of the keypads in the field on the right, its exact replica will be visualized, it is possible therefore not only to view the display and the status of its LED, but also to issue commands by means of the buttons on the image.

Also available is the **Refresh** button, which updates the connection with the control panel, thus renewing the images in the window.

23.2 Control panel status

Via software

Click on the **Monitoring** button on the menu bar, then go to the "Control panel status" section.

A section will open where you can view the real-time status of the control panel.

A list of the basic functions of the control panel, the system parts and components will be shown and also information regarding the proper functionality of the system or any ongoing faults.

23.3 Monitoring Partitions

Via software

Click on the **Monitoring** button on the menu bar, then go to the "Partitions" section.

The top of this section shows a series of icons which represent all the partitions that group together the system zones. These icons show the arming status of the partition based on colour:

red - armed in Away mode

blue - armed in instant mode

orange - armed in Stay mode

green - disarmed

If necessary, these icons can also report the alarm or tamper status of one of their zones by showing the appropriate icon (refer to "*Monitoring terminals*").

By clicking on one of the partition icons, in the "Controls" section it is possible to view the partition status, its arming status, tamper conditions and whether the "auto-arm" function has been enabled (refer to "*Partition parameters*").

The "Actions" section is also available where, once a valid user code has been entered, it is possible to change the arming status of the partition or carry out reset.

23.4 Monitoring terminals

Via software

Click on the **Monitoring** button on the menu bar, then go to the "Zones/Outputs" section.
On selecting a partition from the section at the top, the section will divide into two parts:
the left side will show the list of all the zones of the selected partition
the right side will show the list of all the system outputs
Both sections will show the status of the elements listed in accordance with the icons present:

Table 23.1: Terminal status icons

Icon	Status
	Zone operating normally and in stand-by status
	Zone in alarm status
	Zone with alarm memory
	Zone tamper in progress
	Zone with tamper memory
	Zone in test mode.
	Zone disabled
	Output activated
	Output deactivated

The lists also provide a button to enable or disable the related zone, as well as a button to activate or deactivate the related output. These operations are allowed only after entry of a valid user code authorized to carry out these operations.

Via keypad

`Type-in Code (Installer) , PROGRAMMING User functions, View, Zone status`

23.5 Monitoring timers

Via software

Click on the **Monitoring** button on the menu bar, then go to the "Timer" section.
This section provides a grid containing all the available timer icons.
The status of each icon reflects the status of the respective timer and indicates, in real-time, whether it is enabled or not, or whether it is currently On (operating).

23.6 Monitoring peripheral devices

Via software

Click on the **Monitoring** button on the menu bar, then go to the "Peripherals" section.
In this section it is possible to monitor the devices connected to the I-BUS, divided according to type:

- Keypads
- Readers
- Expansions
- Home-automation modules
- Thermostats
- Sounders/Flashers
- Isolators

- DAC peripherals
- Nexus
- Power supply stations

By selecting an item from this list, in the section alongside, all the peripherals of the selected type will be visualized, represented by icons.

There are two keys to obtain specific information for each device (address, firmware version, operating voltage, presence of faults, etc.):

- **Update**, for a data update
- **Continuous**, for continuous reading of the data in real time

In addition, via tooltip (passing over the icon with the mouse pointer) the device model is provided and if it is present or not.

23.7 Monitoring sounder/flashers

The monitoring phase on the sounder/flashers, both wireless and on the I-BUS, provides feedback relating to the status sounder/flashers and their descriptions.

Via software

Click on the **Monitoring** button on the menu bar, then go to the "Peripherals, Sounder/flashers" section.

The information relative to each sounder/flasher is shown after the respective icon. If the sounder/flasher is configured the icon will not be blanked out and will be accompanied by its description and the status, fault and tamper icons, as follows:

Table 23.2: Sounder/flasher icons

Category	Icon	Notification
Alarms		Sounder/flasher loss
		Sounder active
		Flasher active
		STATUS LED On
		PRG LED On
		Sounder flasher tamper
		Foam tamper protection activated
		Wire cutting
		Blow torch protection activated
Faults		Sounder broken
		Low battery
		Battery fault

Category	Icon	Notification
Status	IN LED	LED input activated
	OUT FAULT	Output FAULT active
	OUT TMP	Output TAMPER active
		Sounder/flasher undergoing programming

Wireless sounders

The programming section of the wireless sounder/flashers allows you view their status.

Via software

Click on the **Sounder/flashers** button on the menu on the left, the "Programming, Configured sounders/flashers" section on the right will show a list of configured sounder/flashers. By selecting a sounder/flasher with the "Wireless" attribute, the "Real time" sub-section will allow you to view the sounder/flasher status.

In this section, the monitoring window lists the parts of the sounder/flasher whose status is represented by icons/LED:

Table 23.3: Wireless sounder/flasher status LEDs

LED		Status
Tamper	Green	Sounder/flasher not in tamper status
	Red	Sounder/flasher in tamper status (open or dislodged)
Antifoam	Green	Foam level below alarm signalling threshold
	Red	Foam level above alarm signalling threshold
Battery fault	Green	Battery charged
	Red	Battery charge low (below 40%)
Sounder active	Green	Audible signalling Off
	Red	Audible signalling On
Flasher active	Green	Visual signalling Off
	Red	Visual signalling On
STATUS LED ON	Green	STATUS LED off
	Red	STATUS LED On
PRG LED ON	Green	PRG LED off
	Red	PRG LED On
Signal reception level		This series of notches represents the reception level of the wireless signal of the device as received by the Air2-BS200 transceiver.
Battery charge level		Percentage of charge of the sounder/flasher battery

Instead, the "Wireless monitoring" sub-section provides the **Start** button that starts a monitoring on the variation of the signal transmitted by the device and background noise detected over time.

23.8 Monitoring Flex5/DAC expansion

The software monitoring function allows you to view the status of the outputs of all the connected Flex5/DAC expansions and to work on them.

Via software

Click on the **Monitoring** button on the menu bar, then go to the "Peripherals, DAC peripheral" section.

In this section you must first select the expansion, form those configured, by entering the relative address in the appropriate field. After clicking-on the **Start monitoring** button this section will show the following:

- Status of each of the 5 outputs on the expansion:
  - power absorbed by the load, phase shift or power factor and current for alternating current loads at mains voltage

- percentage of the supplied power with respect to the maximum possible, measured exclusively for dimmable loads

- Buttons for the activation or deactivation of each single output or to change the voltage supplied to the dimmer output (this operation is allowed only after the entry of a valid user code)
- Voltage supplied to the expansion

23.9 Monitoring the power supply

The software has a section for monitoring the power supplies, through LEDs with the relative colours and values shown in the readings.

Via software

Click on the **Monitoring** button on the menu bar, then go to the "Peripherals, Power" section.
After clicking-on the **Start monitoring** button this section will show:

- data relating to the power supplied to the control panel
  - primary power supply
  - power and secondary power supply
  - power supply module
  - battery
- the data relating to the power the control panel supplies to the devices in the field:
  - voltages and currents on the "**AUXx**" terminals
  - voltage and current on the I-BUS

23.10 Monitoring wireless devices

Via software

Click on the **Monitoring** button on the menu bar, then go to the "Wireless devices" section.
After clicking-on the **Update** button, this section shows a list of all the wireless devices connected to the control panel.
The monitoring-operation provides the following feedback for each device:

- an index of the reception quality of the wireless signal
- the percentage of the battery charge

The colour of the values shown also indicates the level of both the signal index and the charge (red-orange-green).

23.11 Walk test

This section provides a quick and easy way of testing all the configured inputs.
After initializing the Walk test, all the operator need to do is walk through the protected partitions and then check the detection capacity of the inputs via the system keypad or Prime/STUDIO software application.

Via keypad

Type-in Code (Installer) , PROGRAMMING Walk test .
Access to this section opens the full list of configured zones on the keypad display.
As these input zones are violated by the operator carrying out the walk test, they will be cleared from the list and the keypad will emit a long beep.
The system can be considered as having passed the test when all the items disappear from the list.

Via software

Click-on the **Monitoring** button on the menu bar, then go to the "Programming, Sounder/flashers" section.
The list of zones and the **Start Walk test** button will be shown.
Once the test starts, the operator can walk through the entire area protected by the system and verify the correctness of the detection capacity of the inputs by means of the information reported in this section, marking the violated areas with a red dot and the time of the violation.
The **Print Walk test** button allows the so0ftware to print the test results.

Appendix A Default programming

Keypads	• keypad "1" enabled • all keypads belong to partition 1 • 12 programmed shortcuts: Execute Arming Scenario 1 - Execute Arming Scenario 2 - Delete telephone calls - Delete memory - Zone activation menu (bypasses) - View alarm log - View faults - Time/date setting - Voice function menu - Intercom call - Thermostat menu - Keypad settings menu • all thermostats enabled on all keypads
nBy stand-alone readers	• belong to partition 1 • shortcut programmed on the red LED: Execute Arming Scenario 1
Partitions	• entry time and exit time 30 seconds • Autoreset memories on arming • clear call queue on disarming
Terminals	• terminals on control panel: inputs • terminals on expansion boards: inputs • terminals on keypads: unused
Zones	• belong to partition 1 • have N.C. balancing (normally closed) • zones T1 and T2 on the control panel are delayed; all other zones are instant • unlimited alarm cycles (repetitive)
Outputs	• the output relay is monostable, normally closes, monostable time at 3 minutes • the output relay is "Intrusion" type • all other outputs are "generic" • "AUX1" and "AUX2" outputs of the control panel are normally closed • "AUX1" and "AUX2" outputs of all power-supply stations are normally closed
Virtual terminals	• all virtual terminals are input/output, "technological" and associated with partition 1
Expansions	• all expansions have anti-tamper disabled
Scenarios	• scenario 1: Away arm partition 1 • scenario 2: Disarm partition 1
Codes	• user code 1 belongs to all partitions • all other codes do not belong to any partition • only Code 1 is "Master" user • enabled on all sections of the user menu • 8 programmed shortcuts (F1-F4 keys): Clear call queue phone - Output 2 activation - Output 2 deactivation - View Zone status - View System status - Enable answerphone - Activate output scenario - Settings menu • 6 programmed shortcuts (keys from 1 to 6): Listen-in – Execute arming scenario 1 – Execute arming scenario 2 – Stop alarms – Activate Output 2 – Deactivate Output 2 • voice guide enabled • all terminals configured as "output" or "I/O" are associated with all codes
Keys	• belong to partition 1 • Maintenance option enabled
Telephone	• numbers 1 to 6 in the contacts list have the voice attribute (user) • contact numbers 7 and 8 in the phone book are for alarm receiving centres CONTACT-ID • contact number 9 in the phone book has the voice attribute (for the installer)

Zone alarm/tamper events	• relay output activated • "Other outputs / Sounder/flasher 1" activated • on activation of the event, calls contact numbers 1 to 8 • on restoral of the event, calls contact numbers 7 to 8
Zone bypass events	• calls to contact numbers 7 and 8
Partition Arming/Disarming events	• calls to contact numbers 7 and 8
Partition Arming/Disarming events	• calls to contact numbers 7 and 8
Emergency button (Panic) events	• on activation of the event, calls contact numbers 1 to 8
Open-panel/Panel dislodgement events and tamper on peripheral events	• relay output activated • "Other outputs / Sounder/flasher 1" activated • on activation of the event, calls contact numbers 1 to 8 • on restoral of the event, calls contact numbers 7 to 8
Blown fuse, A.C. mains failure, peripheral loss and low battery events	• activated Output 1 • calls to contact number 9 (voice call to installer)
Sounders/Flashers	• causes shutdown on the sounder and the flasher: Reset memories on partition (Partition 1)
Cloud	• both the LAN network and the GSM communicator are enabled for connection
Wi-Fi	• the Wi-Fi card is enabled to function as an "Access point"
Timer	• all system timers are enabled to function as "ordinary" and not as "astronomical"

Appendix B Default Shortcuts

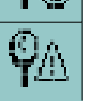
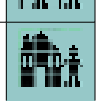
Shortcut			on keypad			on code		on reader		on keys	on event
description	function	parameter	n.	Icon	String	via keypad	over the phone	stand alone	via keypad		
Arm/Disarm	Applies a pre-set scenario	which scenario	**1**		Arm/Disarm	Available	Available	Available	Available	Available	Available Activate scenario
Stop alarms	Shortcut that deactivates instantly the outputs relative to alarm and tamper events and deletes the partition and system alarm and tamper memories.		**2**		Stop alarms	Available	Available	Available	Available	Available	Not available
Clear call queue	Cancels the entire call queue and stops ongoing calls (if any).		**3**		Clear call queue	Available	Available	Available	Available	Available	Not available
Delete memory	Deletes memory of system and partition alarm and tamper events.		**4**		Delete memory	Available	Available	Available	Available	Available	Available
Activate output	Activates one of the programmed outputs.	which output	**5**		Activ. output	Available	Available	Available	Available	Available	Available
Deactivate output	Deactivates one of the programmed outputs.	which output	**6**		Deactiv. output	Available	Available	Available	Available	Available	Available
Overtime	Delays partition auto-arming time by 30 minutes.		**7**		Overtime	Available	Available	Available	Available	Available	Not available
Settings menu	Accesses the user menu section: Settings	Reference code (on reader and key)	**8**		Settings menu	Available	Not available	Not available	Available	Available	Not available
StartVoiceNotifier	Plays a recorded voice message which announces the shortcuts assigned to the number keys.		**9**		Voice menu	Available (only for number keys)	Available	Not available	Not available	Not available	Not available
Listen-in	Allows listen-in sessions via phone by means of a microphone on one of the available keypads.	Keypad	**10**		Listen-in	Not available	Available	Not available	Not available	Not available	Not available
Intercom Call	Accesses the user menu section: Voice functions / Intercom	Reference code (on reader and key)	**11**		Intercom call	Available	Not available	Not available	Available	Available	Not available
Arm/Disarm menu	Accesses the user menu section: Arm/Disarm op.	Reference code (on reader and key)	**12**		Arm/Disarm menu	Available	Not available	Not available	Available	Available	Not available
Alarm management menu	Accesses the user menu section: Alarm management	Reference code (on reader and key)	**13**		Alarm menu	Available	Not available	Not available	Available	Available	Not available
Voice functions menu	Accesses the user menu section: Voice functions	Reference code (on reader and key)	**14**		Voice func. menu	Available	Not available	Not available	Available	Available	Not available
Activations menu	Accesses the user menu section: Activations	Reference code (on reader and key)	**15**		Activations menu	Available	Not available	Not available	Available	Available	Not available
Nexus status menu	Accesses the user menu section: View / Nexus status	Reference code (on reader and key)	**16**		Nexus status menu	Available	Not available	Not available	Available	Available	Not available
Arming status	Plays a voice announcement regarding the armed/disarmed status of partitions.	Reference code (on reader and key)	**17**		Arming status	Available	Available	Not available	Not available	Not available	Not available
Keypad settings	Accesses the user menu section: Keypad settings	Reference code (on reader and key)	**18**		Keypad sett.menu	Available	Not available	Not available	Available	Available	Not available
Zone activations menu	Accesses the user menu section: Activations / Zones	Reference code (on reader and key)	**19**		ZoneBypass menu	Available	Not available	Not available	Available	Available	Not available

Shortcut			on keypad			on code		on reader		on keys	on event
description	function	parameter	n.	Icon	String	via keypad	over the phone	stand alone	via keypad		
Voice memo	Accesses the user menu section: Voice functions	Reference code (on reader and key)	**20**		Voice memo	Available	Not available	Not available	Available	Available	Not available
ON/OFF output menu	Accesses the user menu section: Home-automation commands	Reference code (on reader and key)	**21**		Output control	Available	Not available	Not available	Available	Available	Not available
Enable/Disable answerphone	Accesses the user menu section: Activations / Answerphone	Reference code (on reader and key)	**22**		Enab.answerphone	Available	Not available	Not available	Available	Available	Not available
Activate output scenarios	Activate one of the programmed output scenarios	which scenario	**23**		Output scenario	Available	Available	Not available	Not available	Not available	Not available
Enable codes	Accesses the user menu section: Activations / Codes	Reference code (on reader and key)	**24**		Enable codes	Available	Not available	Not available	Available	Available	Not available
Enable keys	Accesses the user menu section: Activations / Keys	Reference code (on reader and key)	**25**		Enable keys	Available	Not available	Not available	Available	Available	Not available
Enable timers	Accesses the user menu section: Activations / Timers	Reference code (on reader and key)	**26**		Enable timers	Available	Not available	Not available	Available	Available	Not available
Enable auto-arming	Accesses the user menu section: Activations / Auto-arming	Reference code (on reader and key)	**27**		Enab. auto-arm	Available	Not available	Not available	Available	Available	Not available
View events log	Accesses the user menu section: View / Events log	Reference code (on reader and key)	**28**		View events log	Available	Not available	Not available	Available	Available	Not available
View alarms log	Accesses the user menu section: View / Alarms log	Reference code (on reader and key)	**29**		View alarm log	Available	Not available	Not available	Available	Available	Not available
View faults log	Accesses the user menu section: View / Faults log	Reference code (on reader and key)	**30**		View faults log	Available	Not available	Not available	Available	Available	Not available
View arm/disarm operations	Accesses the user menu section: View / Arm/Disarm op.	Reference code (on reader and key)	**31**		View arm ops log	Available	Not available	Not available	Available	Available	Not available
View system status	Accesses the user menu section: View / System status	Reference code (on reader and key)	**32**		ViewSystemStatus	Available	Not available	Not available	Available	Available	Not available
View zone status	Accesses the user menu section: View / Zone status	Reference code (on reader and key)	**33**		View zone status	Available	Not available	Not available	Available	Available	Not available
Change PIN code	Accesses the user menu section: Change PIN	Reference code (on reader and key)	**34**		Change PIN	Available	Not available	Not available	Available	Available	Not available
Time/Date	Accesses the user menu section: Set date/time	Reference code (on reader and key)	**35**		Time/Date	Available	Not available	Not available	Available	Available	Not available
View faults	Accesses the user menu section: View / Faults present	Reference code (on reader and key)	**36**		View faults	Available	Not available	Not available	Available	Available	Not available
Thermostat menu	Accesses the user menu section: Thermostat	Reference code (on reader and key)	**37**		Thermostat menu	Available	Not available	Not available	Available	Available	Not available
Panic	Activates a "Panic" event	which panic event	**38**		Panic	Available	Available	Not available	Available	Available	Not available
Zone bypass	Bypasses one of the configured zones	which zone			Not available	Not available	Not available	Not available	Not available	Not available	Available
Unbypass zone	Unbypasses one of the configured zones	which zone			Not available	Not available	Not available	Not available	Not available	Not available	Available
Disable code	Disables one of the configured codes	which code			Not available	Not available	Not available	Not available	Not available	Not available	Available
Enable code	Enables one of the configured codes	which code			Not available	Not available	Not available	Not available	Not available	Not available	Available
Disable key	Disables one of the configured keys	which key			Not available	Not available	Not available	Not available	Not available	Not available	Available
Enable key	Enables one of the configured keys	which key			Not available	Not available	Not available	Not available	Not available	Not available	Available

Shortcut			on keypad			on code		on reader			
description	function	parameter	n.	Icon	String	via keypad	over the phone	stand alone	via keypad	on keys	on event
Activate thermostat	Activates the thermostat in the selected operating mode	which thermostat which mode	Not available			Not available	Not available	Not available	Not available	Not available	Available
Deactivate thermostat	Deactivates the thermostat	which thermostat	Not available			Not available	Not available	Not available	Not available	Not available	Available
Dimmer up	Increases the voltage value on a dimmer output by 5%	which output	Not available			Not available	Not available	Not available	Not available	Not available	Available
Dimmer down	Decreases the voltage value on a dimmer output by 5%	which output	Not available			Not available	Not available	Not available	Not available	Not available	Available

Appendix C Available Icons

The following Table shows the icons provided at default. The icons can be customized to suit the keypad shortcuts.

no.	Icon	no.	Icon	no.	Icon	no.	Icon	no.	Icon	no.	Icon
1		11		21		31		41		51	
2		12		22		32		42		52	
3		13		23		33		43		53	
4		14		24		34		44		54	
5		15		25		35		45			
6		16		26		36		46			
7		17		27		37		47			
8		18		28		38		48			
9		19		29		39		49			
10		20		30		40		50			

Appendix D Event type

Name		Occurs when...	Restores when ...	Number of events	Pulse events
Zone alarm	Zone alarm	A zone generates an alarm	A zone restores	One event for each zone	no
Terminal tamper	Terminal tamper	A terminal detects tamper (short-circuit or wire cutting)	A terminal restores	One event for each terminal	no
Partition alarm	Partition alarm	A 24h zone which belongs to the partition generates an alarm, or a zone which belongs to the partition generates an alarm during Away mode.	All the zones belonging to the partition restore (reset).	One event for each partition	no
Alarm partition armed in Stay mode	StayPartit.alarm	A zone which belongs to a partition armed in Stay or Instant mode, generates an alarm.	All the zones belonging to the partition restore (reset).	One event for each partition	no
Partition tamper	Partition tamper	A zone which belongs to the partition detects tamper (short-circuit or wire cutting).	All the zones belonging to the partition restore (reset).	One event for each partition	no
Zone bypass	Zone bypass	A zone is inhibited	A zone is enabled (switched On)	One event for each zone	no
Real time zone	Real-time zone	The electrical status of a zone switches from standby to alarm.	The electrical status of a zone switches from alarm to standby.	One event for each zone	no
		The event is independent of the zone type and the armed/disarmed status of the partitions.			
Partition not-ready-to-arm	Partit.not ready	A zone which belongs to the partition is not in stand-by status.	All the zones belonging to the partition are in standby status.	One event for each partition	no
Away arming request on partition	Away arm request	A request is made to arm the interior and perimeter zones of the partition	A request is made to disarm the partition	One event for each partition	Yes
Stay arming request on partition	Stay arm request	A request is made to arm the partition in Stay mode (perimeter zones only) or in Instant mode	A request is made to disarm the partition	One event for each partition	Yes
Effective arming mode on partition	Partit.AwayArmed	The partition interior and perimeter zones have been armed effectively	The partition will be disarmed	One event for each partition	no
Partition armed in Away mode	Partit.stayArmed	The partition has been armed effectively in Stay or Instant mode	The partition will be disarmed	One event for each partition	no
Disarm partition	Partit. disarmed	The partition will be disarmed	The partition will be armed	One event for each partition	no
Reset partition memories	Partition reset	A request is made to reset the partition		One event for each partition	Yes
Partition exit time	Exit time	The partition exit time starts running	The partition exit time expires	One event for each partition	no
Partition entry time	Entry time	The partition entry time is running	The partition entry time expires	One event for each partition	no
Partition pre-arm time	Pre-arm time	The partition pre-arm time is running	The partition pre-arm time expires	One event for each partition	no
Overtime request on partition	Overtime request	A request for overtime relating to the partition is made		One event for each partition	Yes
Partition bell	Chime	A chime zone belonging to the partition is violated		One event for each partition	Yes
Forced arming on partition	Forced arming	At the time of an arming command, relating to one or more partitions, there are open zones on the partition/partitions involved, or there are other conditions present which lower system security, nonetheless, the user arms the system.		One event for each partition	Yes
Partition failed to arm	Failed to arm	If partition arming is requested whilst: there is at least one open/violated zone and the option "NoArm.ZonesOpen" is enabled or when one or more of the events described in "LossTamp.ongoing" is present		One event for each partition	Yes
Recognized valid user code	Valid code	A user-code PIN entered at a keypad is recognized as valid		One event for each code	Yes
Valid key	Valid key	A key used at a reader is recognized as valid on the reader		One event for each key	Yes
Valid code at keypad	ValidCodeAtKeyp.	An entered user-code PIN is recognized as valid on the keypad		One event for each keypad	Yes
Valid key at reader	ValidKeyAtReader	A key used at a reader is recognized as valid on the reader		One event for each reader	Yes

Name		Occurs when...	Restores when ...	Number of events	Pulse events
Valid user-code on partition	Partition code	An entered user-code PIN is recognized as valid on the partition		One event for each partition	Yes
Valid key on partition	Partition key	A key used at a reader is recognized as valid on the partition		One event for each partition	Yes
Failed call	Failed call	All attempts to call a specific phone number have failed	One call to the phone number has been successful	One event for each contact phone number	no
Timer activated	Timer activated	The timer is enabled (On)	The timer is disabled (Off)	One event for each timer	no
Thermostat on keypad	Thermostat ON	The activation conditions programmed for the keypad thermostat occur.	The deactivation conditions programmed for the keypad thermostat occur.	One event for each keypad	no
Activate scenario	Scenario ON	The status of all the partitions correspond exactly to the configured scenario.	The status of at least one of the partitions does not correspond to the configured scenario.	One event for each scenario	no
Programmable event	ProgrammableEvt	Refer to "*Programmable events*"			no
Emergency button	Emergency button	One of the emergency-buttons is pressed		One event for each emergency-button	Yes
Panic	Panic Ev.	The "Panic" shortcut has been activated.		15	Yes
Periodic event	Periodic event	The Periodic Event occurs		4	Yes
Control panel Tamper	Panel tamper	Tamper has been detected on the control panel	The tamper event has been restored	1	no
Zone fuse fault	Zone fuse fault	The zone protection fuse on the control panel is not operational (blown)	The zone protection fuse on the control panel restores	1	no
I-BUS fuse fault	IBUS fuse fault	The I-BUS protection fuse is not operational (blown)	The I-BUS protection fuse restores	1	no
Battery inefficient	Low battery	The backup battery is low	The backup battery is charged	1	no
AC Mains failure	Mains failure	The primary power supply 230V~ fails	The primary power supply 230V~ is restored	1	no
Expansion tamper	Expansion tamper	An expansion board signals tamper conditions	Tamper conditions clear on all the system expansion boards	1	no
Keypad Tamper	Keypad tamper	A keypad signals tamper conditions	Tamper conditions clear on all the system keypads	1	no
Reader Tamper	Reader tamper	A reader signals tamper conditions	Tamper conditions clear on all the system readers	1	no
Sounder flasher tamper	Sound.flash.Tamp	Tamper is detected on a sounder/flasher connected to the BUS	All the sounder/flashers connected to the BUS reset tamper	1	no
2G/3G/4G communicator tamper	2G/3G/4G tamper	The 2G/3G/4G communicator signals tamper	Tamper conditions clear on the 2G/3G/4G communicator	1	no
Expansion Loss	Expansion loss	An expansion board cannot be found on the BUS	All expansion boards can be found on the BUS	1	no
Keypad Loss	Keypad loss	A keypad cannot be found on the BUS	All keypads can be found on the BUS	1	no
Reader Loss	Reader loss	A reader cannot be found on the BUS	All readers can be found on the BUS	1	no
Sounder/flasher loss	Sound.flash.Loss	A sounder/flasher device connected to the BUS is not present	All sounder/flasher devices connected to the BUS are present	1	no
2G/3G/4G communicator loss	2G/3G/4G loss	The control panel cannot find the 2G/3G/4G communicator	The 2G/3G/4G communicator can be found on the BUS	1	no
Jamming	Jamming	Wireless interference detected	Wireless interference cleared	1	no
Low battery on wireless zone	Low battery WLS	The battery of a least one wireless detector is running low	All the wireless detectors are running with sufficient power	1	no
Wireless zone loss	WLS zone loss	Loss of at least one wireless detector has been signalled (supervisory time expired)	All the wireless detector are present	1	no
Valid Installer code	Installer code	An Installer PIN entered at a keypad is recognized as valid		1	Yes
Invalid code	Invalid code	An invalid code PIN is entered at a keypad		1	Yes
False key	False key	An invalid key is used at a reader		1	Yes
2G/3G/4G communicator fault	2G/3G/4G fault	The 2G/3G/4G communicator device signals a fault (refer to the User manual)	Fault conditions clear	1	no
Telephone line down	Tel. line down	The land line is not working	The land line restores	1	no
Hard reset	Hard reset	The control panel re-initializes. The system clock may be wrong or not working properly.		1	Yes
Call queue full	Call queue full	There are no more slots left in the outgoing call queue		1	Yes
Successful call	Successful call	The call is answered		1	Yes
Input undergoing programming	Programming	Access to system programming is authorized	End of system programming	1	no
Ongoing call	Ongoing call	A call is sent	A call ends	1	no
SMS message not delivered	SMSMessageFailed	Nexus failed to send SMS message		1	Yes

Name		Occurs when...	Restores when ...	Number of events	Pulse events
Output fault	Output fault	An output fails to switch status as commanded		1	Yes
Low credit	Low credit	The credit remaining on the SIM card inserted in the Nexus is below the minimum credit threshold.	The remaining credit is above the minimum credit threshold.	1	no
Date and time change	Time modified	There is a change in the date and time. This event will be recorded together with the date/time before the change.	There is a change in the date and time. This event will be recorded together with the date/time after the change.	1	no
Resistance internal battery	Int. Resistance	The internal resistance of the battery has exceeded the $R_{i\ max}$ value.	The internal resistance of the battery returns to below the $R_{i\ max}$ value.	1	no
Short-circuit on battery	Battery shorted	A short-circuit condition has been detected on the battery connection terminals	The short-circuit condition is no longer present	1	no
Battery disconnection	Battery disconn.	The backup battery is disconnected	The backup battery is connected	1	no
Power-supply overload	PwSupplyOverload	Output overload is detected on the power-supply unit	The electrical load returns below the allowed limit	1	no
Overheating on power-supply unit	PwSupply Overheat	The temperature of the power-supply unit has exceeded the allowed limit	The temperature of the power-supply unit is normal	1	no
Earth fault	Earth fault	Leakage to ground is present	The leakage to ground condition is no longer detected	1	no
Overvoltage output "x"	Overvoltage "x"	A voltage of over 14.5V has been detected on terminal "**+AUX**" corresponding to number "x" on the motherboard.	The normal voltage on the terminal has been restored.	one for each output "**+AUX**" of the motherboard	no
Overvoltage BUS	Overvolt. BUS	A voltage higher than 14.5V has been detected on the "**+**" terminal of the BUS of the motherboard.	The normal voltage on the terminal has been restored.	1	no
Low voltage output "x"	Undervoltage "x"	A voltage below 9.8V has been detected on terminal "**+AUX**" corresponding to number "x" on the motherboard	The normal voltage on the terminal has been restored.	one for each output "**+AUX**" of the motherboard	no
Low voltage output BUS	Undervoltage BUS	A voltage below 9.8V has been detected on I-BUS terminal "**+**" on the motherboard.	The normal voltage on the terminal has been restored.	1	no
Short-circuit output "x"	Short circuit "x"	A short-circuit has been detected on terminal "**+AUX**" corresponding to number "x" on the LIVPWR100 board	The short-circuit is no longer present.	one for each output "**+AUX**" of the motherboard	no
Short-circuit output BUS	Short circuit BUS	A short-circuit has been detected on I-BUS terminal "**+**" on the motherboard.	The short-circuit is no longer present.	1	no
Overload output "x"	Overload "x"	A load of over 1.5A has been detected on terminal "**+AUX**" corresponding to number "x" on the motherboard	The terminal restores to normal.	one for each output "**+AUX**" of the motherboard	no
Overload output BUS	Overload BUS	A load of over 3.5A has been detected on I-BUS terminal "**+**" on the motherboard.	The terminal restores to normal.	1	no
Failed communication with power-supply unit	NoCommunPwSupply	The power supply unit fails to communicate with the control panel	Communication between the power supply unit and the control panel restores.	1	no
Telephone call on Number 1 in progress	Tel. on number 1	A call has been sent to phone number 1	The call has ended (even in the event of negative outcome)	1	no
Telephone call on Number 15 in progress	Tel.on number 15	A call has been sent to phone number 15	The call has ended (even in the event of negative outcome)	1	no
IP connection on LAN/WiFi lost	IP conn. LAN loss	The IP connectivity test on LAN/WiFi is enabled and the test has failed.	A connection attempt has been successful.	1	no
GPRS connection lost	IP conn. lost	The 2G/3G/4G communicator has detected GPRS connectivity trouble.	The GPRS connectivity is restored.	1	no
Dust in smoke detector chamber	Detector dusty	The smoke chamber of at least one or more smoke detectors is contaminated by dirt or dust. Refer to the instructions supplied with the detector for information regarding the respective threshold.	All smoke sensors have stopped signalling the presence of dust.	1	no
General alarm	Alarm	Any one of the zones has generated an alarm signal.	All the zones have reset the alarm signal.	1	no
General tamper	Tamper	Any one of the zones has generated a tamper signal.	All the zones have reset the tamper signal.	1	no
Failed SIA-IP polling	SiaIPPollingFail	The polling signal enabled by the SIA-IP server has stopped.	The polling signal has resumed.	1	no
Temperature detector tamper	Temp.SensorTamp.	For future use			
Roller blind board tamper	HomAut.mod tamp.	One of the home-automation modules has been tampered.	Tamper conditions clear on all the system home-automation modules	1	no
Tamper on the power-supply station	PowerStationTamp	One of the power-supply stations has been tampered.	Tamper conditions clear on all the power stations	1	no
Temperature detector loss	Temp.Sensor loss	For future use			
Roller blind board lost	HomAut. mod loss	One of the home-automation modules is not present.	All home-automation modules can be found on the BUS	1	no

Name		Occurs when...	Restores when ...	Number of events	Pulse events
Power-supply station loss	PowerStationLoss	One of the power-supply stations is not present	All the power-supply stations can be found on the BUS	1	no
IP connection on GSM lost	IP conn.GSM lost	The IP connectivity test on GSM is enabled and the test has failed.	A connection attempt has been successful.	1	no
Low battery on keyfob	Low batt. keyfob	One of the keyfobs in the configuration signals low battery voltage	All the keyfobs have effective battery voltage	1	no
Remote-control key enablement with low battery	Keyfob enable	A remote -control device has been unlocked and enabled for arming/disarming operations even with low battery.		1	Yes
Commissioning	Maintenance	The control panel enters Maintenance status.	The control panel returns in normal operating status.	1	no

Appendix E Combination of outputs triggered by events

This appendix explains the behaviour of the outputs programmed in the "Outputs" and "Other outputs" parameters of each event together with the activation and deactivation modes ("Tone types" parameter) of the sounder/flashers on the BUS.

Output typology

Symbol/Initials	Description
TM	Output on terminal/Relay/OC1/OC2 - monostable
TB	Output on terminal/Relay/OC1/OC2 - bistable
SM	Sounder/flasher output with limited flasher time
SB	Sounder/flasher output with unlimited flasher time

Functioning and deactivation of the outputs

Symbol/Initials	Description
A	These outputs will deactivate if a Stop alarm, Reset partition or Disarm operation is carried out while the monostable time of the main output is running.
B	These outputs will deactivate only when the event clears after expiry of the monostable time of the main output.
C	These outputs, due to the continuous flasher function, will not deactivate automatically. In order to deactivate the SB flashers of the sounder/flasher after expiry of the monostable time applied to the main output, you must: trigger an event which applies a Stop pattern to the SB flashers reset the partition
D	These outputs will deactivate only when the event clears.
E	These outputs will deactivate if, when an event is active, a Stop alarm operation, reset or disarm partition command operation is carried out.
F	These outputs, due to the continuous flasher function, will not deactivate automatically. In order to deactivate the SB flashers of the device on termination of the event, you must: trigger an event which applies a Stop pattern to the SB flashers reset the partition
G	These outputs will deactivate when the respective monostable time expires

Output combinations

Event groups	Principal output				Other outputs			
	TM	**TB**	**SM**	**SB**	**TM**	**TB**	**SM**	**SB**
Zone Alarm terminal tamper partition alarm partition tamper	**A G**				**A G**	**A B**	**A G**	**A C**
		D E			**E G**	**D G**	**E G**	**F**
			A G		**A G**	**A B**	**A G**	**A C**
				F	**E G**	**D G**	**E G**	**F**
Control panel open Dislodged panel Expansion tamper/loss Keypad tamper/loss Reader tamper/loss Sounder/flasher tamper/loss Jamming Wireless zone loss Telephone line down	**A G**				**A G**	**A D**	**A G**	**A C**
		D E			**E G**	**D G**	**E G**	**C**
			A G		**A G**	**A B**	**A G**	**A C**
				F	**E G**	**D G**	**E G**	**C**
other events	**G**				**G**	**B**	**G**	**C**
		D			**G**	**D**	**G**	**F**
			G		**G**	**B**	**G**	**C**
				F	**G**	**C**	**G**	**C**

Appendix F Pre-recorded messages

The SmartLogos30M voice board is supplied by Inim Electronics with 500 voice message slots, 291 of which are pre-recorded. The messages are arranged in such way as to produce event-related voice calls which clearly describe the related event.

The following Table shows the message numbers and their purpose, together with the respective recording time.

Type	Number	Default message	Message duration (seconds)	
			High quality	Average quality
Available user-messages	1 – 100	''	169 (for all 100 messages)	271 (for all 100 messages)
Not available	101 - 165	''		
Arming scenarios	166	Scenario 1	2.5	4
	167	Scenario 2	2.5	4
	168	Scenario 3	2.5	4
	169	Scenario 4	2.5	4
	170	Scenario 5	2.5	4
	171	Scenario 6	2.5	4
	172	Scenario 7	2.5	4
	173	Scenario 8	2.5	4
	174	Scenario 9	2.5	4
	175	Scenario 10	2.5	4
	176	Scenario 11	2.5	4
	177	Scenario 12	2.5	4
	178	Scenario 13	2.5	4
	179	Scenario 14	2.5	4
	180	Scenario 15	2.5	4
	181	Scenario 16	2.5	4
	182	Scenario 17	2.5	4
	183	Scenario 18	2.5	4
	184	Scenario 19	2.5	4
	185	Scenario 20	2.5	4
	186	Scenario 21	2.5	4
	187	Scenario 22	2.5	4
	188	Scenario 23	2.5	4
	189	Scenario 24	2.5	4
	190	Scenario 25	2.5	4
	191	Scenario 26	2.5	4
	192	Scenario 27	2.5	4
	193	Scenario 28	2.5	4
	194	Scenario 29	2.5	4
	195	Scenario 30	2.5	4
Shortcut	196	Armed in Away mode	2.5	4
	197	Stop alarm	2.5	4
	198	Stop call queue	2.5	4
	199	Delete memory	2.5	4
	200	Activate output	2.5	4
	201	Deactivate output	2.5	4
	202	Overtime request	2.5	4
	203	Request maintenance	2.5	4
	204	StartVoiceNotifier	2.5	4
	205	Listen-in	2.5	4
	206	Intercom Call	2.5	4
	207	Arm/Disarm menu	2.5	4
	208	Alarm management menu	2.5	4
	209	Voice functions	2.5	4
	210	Activations menu	2.5	4
	211	Nexus status	2.5	4
	212	System status	2.5	4

Type	Number	Default message	Message duration (seconds)	
			High quality	Average quality
	213	Keypad settings	2.5	4
	214	Zone bypass menu	2.5	4
	215	Voice memo	2.5	4
	216	ON/OFF output menu	2.5	4
	217	Enable/Disable answerphone	2.5	4
	218	Enable teleservice	2.5	4
	219	Enable codes	2.5	4
	220	Enable keys	2.5	4
	221	Enable timers	2.5	4
	222	Enable auto-arming	2.5	4
	223	View events log	2.5	4
	224	View alarms log	2.5	4
	225	View faults log	2.5	4
	226	View arm/disarm operations	2.5	4
	227	View battery status	2.5	4
	228	View zone status	2.5	4
	229	Change PIN	2.5	4
	230	Date/Time settings	2.5	4
	231	View faults	2.5	4
Not available	232 - 240	''		
Generic messages	241	Reset	1.25	2
	242	To	0.63	1
	243	Press	1.25	2
	244	Location	6.25	10
	245	Zero	2.5	4
	246	One	2.5	4
	247	Two	2.5	4
	248	Three	2.5	4
	249	Four	2.5	4
	250	Five	2.5	4
	251	Six	2.5	4
	252	Seven	2.5	4
	253	Eight	2.5	4
	254	Nine	2.5	4
Partition status	255	Away mode	3.13	5
	256	Armed in Stay mode	3.13	5
	257	Instant mode	3.13	5
	258	Disarm	3.13	5
Menu	259	To go back to previous menu press *	3.13	5
Activation / Deactivation	260	To activate	1.88	3
	261	To deactivate	1.88	3
Type-in user-code PIN	262	Type-in user-code PIN followed by #	2.5	4
Outputs	263	Relay	2.5	4
	264	Output 1	2.5	4
	265	Output 2	2.5	4
Not available	266 - 270	''		
Zone / Terminal	271	Zone 1	3.13	5
	272	Zone 2	3.13	5
	273	Zone 3	3.13	5
	274	Zone 4	3.13	5
	275	Zone 5	3.13	5
	276	Zone 6	3.13	5
	277	Zone 7	3.13	5
	278	Zone 8	3.13	5
	279	Zone 9	3.13	5
	280	Zone 10	3.13	5
	281	Zone 11	3.13	5
	282	Zone 12	3.13	5
	283	Zone 13	3.13	5
	284	Zone 14	3.13	5
	285	Zone 15	3.13	5
	286	Zone 16	3.13	5
	287	Zone 17	3.13	5
	288	Zone 18	3.13	5
	289	Zone 19	3.13	5
	290	Zone 20	3.13	5
	291	Zone 21	3.13	5
	292	Zone 22	3.13	5
	293	Zone 23	3.13	5
	294	Zone 24	3.13	5

Type	Number	Default message	Message duration (seconds)	
			High quality	Average quality
	295	Zone 25	3.13	5
	296	Zone 26	3.13	5
	297	Zone 27	3.13	5
	298	Zone 28	3.13	5
	299	Zone 29	3.13	5
	300	Zone 30	3.13	5
	301	Zone 31	3.13	5
	302	Zone 32	3.13	5
	303	Zone 33	3.13	5
	304	Zone 34	3.13	5
	305	Zone 35	3.13	5
	306	Zone 36	3.13	5
	307	Zone 37	3.13	5
	308	Zone 38	3.13	5
	309	Zone 39	3.13	5
	310	Zone 40	3.13	5
	311	Zone 41	3.13	5
	312	Zone 42	3.13	5
	313	Zone 43	3.13	5
	314	Zone 44	3.13	5
	315	Zone 45	3.13	5
	316	Zone 46	3.13	5
	317	Zone 47	3.13	5
	318	Zone 48	3.13	5
	319	Zone 49	3.13	5
	320	Zone 50	3.13	5
	321	Zone 51	3.13	5
	322	Zone 52	3.13	5
	323	Zone 53	3.13	5
	324	Zone 54	3.13	5
	325	Zone 55	3.13	5
	326	Zone 56	3.13	5
	327	Zone 57	3.13	5
	328	Zone 58	3.13	5
	329	Zone 59	3.13	5
	330	Zone 60	3.13	5
	331	Zone 61	3.13	5
	332	Zone 62	3.13	5
	333	Zone 63	3.13	5
	334	Zone 64	3.13	5
	335	Zone 65	3.13	5
	336	Zone 66	3.13	5
	337	Zone 67	3.13	5
	338	Zone 68	3.13	5
	339	Zone 69	3.13	5
	340	Zone 70	3.13	5
	341	Zone 71	3.13	5
	342	Zone 72	3.13	5
	343	Zone 73	3.13	5
	344	Zone 74	3.13	5
	345	Zone 75	3.13	5
	346	Zone 76	3.13	5
	347	Zone 77	3.13	5
	348	Zone 78	3.13	5
	349	Zone 79	3.13	5
	350	Zone 80	3.13	5
	351	Zone 81	3.13	5
	352	Zone 82	3.13	5
	353	Zone 83	3.13	5
	354	Zone 84	3.13	5
	355	Zone 85	3.13	5
	356	Zone 86	3.13	5
	357	Zone 87	3.13	5
	358	Zone 88	3.13	5
	359	Zone 89	3.13	5
	360	Zone 90	3.13	5
	361	Zone 91	3.13	5
	362	Zone 92	3.13	5
	363	Zone 93	3.13	5

Type	Number	Default message	Message duration (seconds)	
			High quality	Average quality
	364	Zone 94	3.13	5
	365	Zone 95	3.13	5
	366	Zone 96	3.13	5
	367	Zone 97	3.13	5
	368	Zone 98	3.13	5
	369	Zone 99	3.13	5
	370	Zone 100	3.13	5
Partition	371	Partition 1	3.13	5
	372	Partition 2	3.13	5
	373	Partition 3	3.13	5
	374	Partition 4	3.13	5
	375	Partition 5	3.13	5
	376	Partition 6	3.13	5
	377	Partition 7	3.13	5
	378	Partition 8	3.13	5
	379	Partition 9	3.13	5
	380	Partition 10	3.13	5
	381	Partition 11	3.13	5
	382	Partition 12	3.13	5
	383	Partition 13	3.13	5
	384	Partition 14	3.13	5
	385	Partition 15	3.13	5
Codes	386	Code 1	2.5	4
	387	Code 2	2.5	4
	388	Code 3	2.5	4
	389	Code 4	2.5	4
	390	Code 5	2.5	4
	391	Code 6	2.5	4
	392	Code 7	2.5	4
	393	Code 8	2.5	4
	394	Code 9	2.5	4
	395	Code 10	2.5	4
Keys	396	Key 1	2.5	4
	397	Key 2	2.5	4
	398	Key 3	2.5	4
	399	Key 4	2.5	4
	400	Key 5	2.5	4
	401	Key 6	2.5	4
	402	Key 7	2.5	4
	403	Key 8	2.5	4
	404	Key 9	2.5	4
	405	Key 10	2.5	4
Keypads	406	Keypad 1	2.5	4
	407	Keypad 2	2.5	4
	408	Keypad 3	2.5	4
	409	Keypad 4	2.5	4
	410	Keypad 5	2.5	4
Readers	411	Reader 1	2.5	4
	412	Reader 2	2.5	4
	413	Reader 3	2.5	4
	414	Reader 4	2.5	4
	415	Reader 5	2.5	4
Function keys / Emergency	416	Fire	2.5	4
	417	Ambulance	2.5	4
	418	Police	2.5	4
Not available	419	''		
Event type	420	Zone alarm	2.5	4
	421	Terminal tamper	2.5	4
	422	Partition alarm	2.5	4
	423	Stay alarm	2.5	4
	424	Partition tamper	2.5	4
	425	Zone bypass	2.5	4
	426	Real time zone	2.5	4
	427	Partition not-ready-to-arm	2.5	4
	428	Away arm request	2.5	4
	429	Stay arm request	2.5	4
	430	Armed in Away mode	2.5	4
	431	Armed in Stay mode	2.5	4
	432	Reset partition	2.5	4
	433	Partition armed, leave partition	2.5	4

Type	Number	Default message	Message duration (seconds)	
			High quality	Average quality
	434	Disarm partition	2.5	4
	435	Pre-arm alert	2.5	4
	436	Overtime request	2.5	4
	437	Welcome	2.5	4
	438	Forced arming	2.5	4
	439	Failed to arm	2.5	4
	440	Valid user-code	2.5	4
	441	Valid key	2.5	4
	442	Valid code at keypad	2.5	4
	443	Valid key at reader	2.5	4
	444	Valid user-code on partition	2.5	4
	445	Valid key on partition	2.5	4
	446	Failed call	2.5	4
	447	Timer activated	2.5	4
	448	Thermostat	2.5	4
	449	Scenario	2.5	4
	450	Programmable event	2.5	4
	451	Emergency	2.5	4
	452	Open-panel tamper	2.5	4
	453	Dislodged-panel tamper	2.5	4
	454	Zone fuse fault	2.5	4
	455	I-BUS fuse fault	2.5	4
	456	Battery inefficient	2.5	4
	457	Mains failure	2.5	4
	458	Expansion tamper	2.5	4
	459	Keypad Tamper	2.5	4
	460	Reader Tamper	2.5	4
	461	Sounder flasher tamper	2.5	4
	462	Nexus tamper	2.5	4
	463	Expansion Loss	2.5	4
	464	Keypad Loss	2.5	4
	465	Reader Loss	2.5	4
	466	Sounder/flasher loss	2.5	4
	467	Nexus loss	2.5	4
	468	Jamming	2.5	4
	469	Low battery wireless zone	2.5	4
	470	Wireless zone loss	2.5	4
	471	Valid Installer code	2.5	4
	472	Invalid code		
	473	False key		
	474	Nexus fault		
	475	Telephone line down		
	476	Periodic test event		
	477	Hard reset		
	478	Call queue full		
	479	Successful call		
	480	Start programming		
	481	Ongoing call		
	482	Failed to send message		
	483	Output fault		
	484	Low GSM credit		
Not available	485	''		
Voicemail slots	486 – 500	''	37.5 (for all 15 messages)	60 (for all 15 messages)

Notes

Notes

Notes

Evolving Security

Inim Electronics S.r.l.

Centobuchi, via Dei Lavoratori 10
63076 Monteprandone (AP), Italy
Tel. +39 0735 705007 _ Fax +39 0735 704912

info@inim.biz _ www.inim.biz

ISO 9001 Quality Management
certified by BSI with certificate number FM530352

DCMPINE0PRIMEE-170-20230713