### Types of Central Unit

**With GSM**
- SAS-W1.1E  
  - SAS-W1.1E
- SAS-W1.1F  
  - SAS-W1.1F

**Basic**
- SAS-W2.1E  
  - SAS-W2.1E
- SAS-W2.1F  
  - SAS-W2.1F
Contents

1 Introduction .................................................................................................................. 5
  1.1 Where to find the information .................................................................................. 5
  1.2 Conformity ................................................................................................................ 5
  1.3 Disclaimer .................................................................................................................. 5
  1.4 Trademarks and copyrights ....................................................................................... 5

Use the system .................................................................................................................. 6

2 Command interface ....................................................................................................... 6
  2.1 Display ....................................................................................................................... 6
    2.1.1 Meaning of the icons ............................................................................................. 6
    2.1.2 Authentication ..................................................................................................... 7
    2.1.3 Main user menu .................................................................................................. 7
    2.1.4 Status of the individual zones ............................................................................. 8
  2.2 LEDs .......................................................................................................................... 8
  2.3 Command interface ................................................................................................... 9
    2.3.1 Using the keyboard ............................................................................................ 9
  2.4 Authentication .......................................................................................................... 9
    2.4.1 User ID ............................................................................................................... 9
    2.4.2 Password .......................................................................................................... 9
  2.5 Authorisation level ..................................................................................................... 10

3 Arming and disarming the system ............................................................................... 11
  3.1 Arming or disarming using the keypad ...................................................................... 11
    3.1.1 Rapid arming or disarming ................................................................................ 11
    3.1.2 Global arming .................................................................................................... 12
    3.1.3 Global disarming ............................................................................................... 12
    3.1.4 Partial arming .................................................................................................... 13
    3.1.5 Partial disarming ............................................................................................... 13
  3.2 Arming or disarming using the remote control ......................................................... 13
  3.3 Arming using Forced Block ...................................................................................... 13
  3.4 Reset .......................................................................................................................... 14

4 Panic and burglary ....................................................................................................... 15
  4.1 Activating the panic alarm ....................................................................................... 15
    4.1.1 Activation using the keypad ............................................................................... 15
    4.1.2 Activation using the remote control .................................................................. 15
  4.2 Activate the burglar alarm ....................................................................................... 15
    4.2.1 Activation using the remote control .................................................................. 15

5 Alarms and event memories ......................................................................................... 16
  5.1 Alarm priority .......................................................................................................... 16
  5.2 How to block an alarm ........................................................................................... 16
  5.3 Events history ......................................................................................................... 17
    5.3.1 View events ...................................................................................................... 17
    5.3.2 Interpreting a stored event ................................................................................ 17

6 Remote commands ..................................................................................................... 20
  6.1 Telephone commands with DTMF tones .................................................................. 20
  6.2 SMS Commands ....................................................................................................... 21

7 System status ............................................................................................................... 22

8 Central unit settings ................................................................................................... 24
  8.1 Adjust display ........................................................................................................... 24
  8.2 Audio Settings ......................................................................................................... 24
8.2.1 Beep volume .................................................................................................................. 24
8.2.2 Sound Feedback ............................................................................................................. 25
8.2.3 Alarms .............................................................................................................................. 25
8.3 Setting date and time .......................................................................................................... 26
8.4 Change PIN ......................................................................................................................... 27
8.5 Operating method and change language ............................................................................ 27
8.6 Customize quick entry ........................................................................................................ 28

Install and configure the system .......................................................................................... 30

9 Main characteristics ............................................................................................................ 30
9.1 Main functions of the central unit ..................................................................................... 30
9.2 System capacity ................................................................................................................ 30

10 Designing a system ............................................................................................................ 31
10.1 Information on radio waves ............................................................................................. 31
10.2 Use the zones ..................................................................................................................... 31
10.2.1 Zone types ..................................................................................................................... 31
10.2.2 Subdivision into zones ................................................................................................. 32

11 Installing the central unit .................................................................................................. 33
11.1 Workspaces ...................................................................................................................... 33
11.2 Commissioning ................................................................................................................ 33
11.2.1 Reading operational sequences .................................................................................... 33
11.2.2 First start-up .................................................................................................................. 33
11.3 Status of the system ......................................................................................................... 37
11.3.1 Arm / disarm the system .............................................................................................. 38
11.3.2 Display alarm zones ..................................................................................................... 39
11.4 Authentication ................................................................................................................... 39
11.5 General and alarm reports ............................................................................................... 41

12 Programming ...................................................................................................................... 42
12.1 System creation ................................................................................................................ 42
12.2 Programming zones and sensors ................................................................................... 42
12.2.1 To programme a new zone: ......................................................................................... 42
12.2.2 To modify or delete a zone: .......................................................................................... 42
12.2.3 To programme a sensor: .............................................................................................. 43
12.3 Programming system devices ........................................................................................ 44
12.3.1 Remote Control Programming .................................................................................... 44
12.4 Programming external sirens .......................................................................................... 48
12.4.1 Possible parameters ...................................................................................................... 48
12.4.2 Zones Filters ............................................................................................................... 49
12.4.3 Alarms .......................................................................................................................... 49
12.4.4 Events ........................................................................................................................... 49
12.5 Repeater programming .................................................................................................... 50
12.5.1 Possible parameters ...................................................................................................... 50
12.6 Telephone contact programming .................................................................................. 50
12.6.1 Customised message .................................................................................................... 52
12.6.2 Phone message sending sequence .............................................................................. 53
12.6.3 Receiving telephone calls from the central unit ........................................................... 53
12.7 Home automation free@home ....................................................................................... 53
12.7.1 Version .......................................................................................................................... 53
12.7.2 Key .................................................................................................................................. 54
12.7.3 GTW Reset .................................................................................................................... 54
12.8 System test ....................................................................................................................... 54
12.9 User management ............................................................................................................. 56
1 INTRODUCTION

Thank you for purchasing the BUSCH-/ABB-secure@home central unit. This manual contains all of the information that the user needs for day-to-day use of the central unit and the intrusion alarm system, including configuration and maintenance procedures.

1.1 Where to find the information

This manual contains all of the information to use, configure and maintain the central unit. It also provides suggestions for planning a security system, includes a list of the technical specifications of the central unit and sets out the procedures for isolating the system and resolving any faults. The configuration section is exclusively intended for use by the technician who installs the system.

1.2 Conformity

The central unit has been designed and built according to quality and safety standards provided for in the regulations and laws in force. Conformity with qualitative requirements is confirmed by the inclusion of the CE mark in accordance with regulation 1999/05/EC.

Warning! Installation must only be performed by a qualified electrician.

When installing the system, current national electrical regulations regarding the installation site must be complied with. It should be noted that the conformity referred to above and the performance of the product may be compromised by:

- incorrect electrical power supply;
- incorrect installation or incorrect, improper or otherwise inconsistent use of the instructions provided in the installation and use manual or in the instructions provided with the devices;
- replacement of original parts or accessories with other types that have not been approved by the manufacturer, or performed by unauthorised personnel.

In the event of opting for non-conforming configurations, the product labels confirming conformity must be modified or removed.

1.3 Disclaimer

All the information in this document has been collected and checked with care. However, ABB and BUSCH-JAEGER cannot be held liable for any printing errors or technical inaccuracies. ABB and BUSCH-JAEGER reserve the right to improve or change the products described in this manual at any time and without prior notice. This manual may also contain references or information about products or services that are not yet on the market. The inclusion of such references or information does not in any way imply that ABB and BUSCH-JAEGER intend to market such products or services.

1.4 Trademarks and copyrights

All trademarks mentioned in the document belong to their respective owners.
© Copyright ABB S.p.A. 2018 - All rights reserved.
© Copyright BUSCH-JAEGER GmbH. 2018 - All rights reserved.
USE THE SYSTEM

This section contains all of the information that the user needs for day-to-day use of the central unit and the intrusion alarm system, including some configuration procedures.

2 COMMAND INTERFACE

2.1 Display

The liquid crystal display screen shows all of the information relevant to the configuration of the central unit and operation of the system. It may contain up to 8 lines of text with up to 20 characters each, or a series of icons, or a combination of text and icons.

The display is normally off, and lights up when a key is pressed.

When idle, the screen displays the following information:

- Status of the system (armed/disarmed/partially armed (Note1))
- 2 icons to indicate, from left to right, the status of the central unit power supply and the GSM connection.

Pressing the ↗ key once will bring up detailed information on the status of the individual zones, while pressing it a second time:

- central unit FW release number
- physical address (8 digits) of the central unit
- date - time
- connection to ABB-free@home
- battery level

Note 1:
Armed All zones are armed using the same method
Disarmed All zones are disarmed
Partially armed Not all zones are armed or they are armed in a non-uniform manner

2.1.1 Meaning of the icons

<table>
<thead>
<tr>
<th>Status of Intrusion alarm system</th>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td>![Icon]</td>
<td>The connection to the GSM telephone network is working. The signal strength is displayed using the bars (1 to 3).</td>
</tr>
<tr>
<td></td>
<td>![Icon]</td>
<td>GSM telephone network not identified, SIM Card not installed, not identified, expired or not active.</td>
</tr>
<tr>
<td></td>
<td>![Icon]</td>
<td>System disarmed.</td>
</tr>
<tr>
<td></td>
<td>![Icon]</td>
<td>System armed in &quot;Notification&quot; mode.</td>
</tr>
</tbody>
</table>
2.1.2 Authentication

To perform the authentication process when the window is idle:

1. Press the ok key on the key pad. A window will appear showing the level 2 users set up for the system

   ![Select user screen]

   2. Select the user from the list and enter the PIN. The numbers entered will be hidden

   3. Press the ✓ key to confirm. If the PIN entered is not 5 digits long, the ✓ key will not be accepted. If the user enters the wrong PIN, a tampering alarm is generated on the tenth attempt.

   4. If the authentication process is successful, the main user menu appears.

2.1.3 Main user menu

The screen is laid out as shown below. When the user accesses this screen, the central unit automatically switches to the "Arm/disarm" icon

![Arm/Disarm icon]

The ⬅ key allows you to leave the screen and return to the idle screen. The ➤ ◀ arrows allow you to navigate to select the desired icon and, therefore, function.
### 2.1.4 Status of the individual zones

The status of the zones can be accessed by pressing the ▼ key on the idle screen: each zone can assume the statuses - and therefore the icons - described in the "Intrusion alarm system" section of the **Meaning of the icons** table - par. 2.1.1.

### 2.2 LEDs

4 LEDs are located beside the display, on the right.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Battery Fault" /></td>
<td>Indicates that the central unit battery is faulty.</td>
</tr>
<tr>
<td><img src="image" alt="Mandatory Notifications" /></td>
<td>Indicates that mandatory notifications have been stored and not yet viewed. Visible when the system is deactivated.</td>
</tr>
<tr>
<td><img src="image" alt="Alarm" /></td>
<td>Signals an alarm (intrusion, tampering). Does not signal burglar alarms. Only visible to authenticated users.</td>
</tr>
<tr>
<td><img src="image" alt="System Jamming" /></td>
<td>Signals system jamming.</td>
</tr>
</tbody>
</table>

In the event of a fault or an alarm, the relevant LED will come on and stay on, unless the network power supply is not working and only battery power supply is available. If this is the case, the LEDs will flash slowly (2 seconds on, 6 seconds off) to save power. The notification LED will switch off automatically when all of the pending faults have been viewed by scrolling through the various screens using the F2 key and returning to the main screen. In the event of alarms (tampering or intrusion), the LED will only switch off following the restoration operation.
2.3 Command interface

2.3.1 Using the keyboard

The central unit is configured with the aid of the keyboard that allows you to navigate through the voices of the menu, enter digits and letters.

The keyboard consists of 17 keys:

- ▲ It allows you to navigate between menu items and icons.
- ▼
- ▶ Confirm the value entered or selected.
  Pressed in any displayed menu, saves the data and moves to the upper menu level.
- 1 2 3
- 4 5 6
- 7 8 9
- 0
- Alphanumeric keys that allow you to enter numbers or letters.
- ← Return to the previous page.
- ● Remove a setting.

2.4 Authentication

In order to access the menus and operate the central unit, authentication is required via an ID and password, both of which are numerical. The ID and password are stored as codes. Each user is also assigned specific privileges that determine what they can do. There are no preset factory users. The duration of the work session is 3 minutes for level 2 users and 1 hour for level 3 users.

2.4.1 User ID

The user ID is a 1 digit numerical code, between 0 and 9, assigned in order by the system ID 0 is reserved for a level 3 user (installer), ID 1 is for a level 2 user (user) or a level 4 user (Maintenance personnel).
At least one level 3 user and one level 2 user must be set for each system.

2.4.2 Password

The password (PIN) consists of 5 digits and is chosen freely by the user. The PIN can only be modified by its owner, using a specific procedure.
### 2.5 Authorisation level

The authorisation level determines what individual users can and cannot do after authentication. There are three levels of authorisation:

- **Level 2** classifies the users who use the intrusion alarm system on a daily basis.

- **Level 3, Installer**: can set up or modify the configuration of the system. There can only be one installer per system. To use the system, a level 3 user must be authorised in advance by a level 2 user.

- **Level 4**. Refers to users who can update or change the central unit firmware. Because this operation is critical to the proper functioning of the system, it is required to enable users who have already gone through the authentication process using their login details to be authenticated again on a specific basis.

The star (*) identifies the maintainer, pay attention before deleting this user!

Level 3 Installer users and level 2 Superusers correspond to the authorisation levels of the same names provided for in regulation EN 50131-1.

The table below outlines the permissions granted to each authorisation level.

<table>
<thead>
<tr>
<th>Function</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>User</td>
</tr>
<tr>
<td>Global arming</td>
<td>■</td>
</tr>
<tr>
<td>Only permitted arming</td>
<td>■</td>
</tr>
<tr>
<td>Total disarming</td>
<td>■</td>
</tr>
<tr>
<td>Only permitted disarming</td>
<td>■</td>
</tr>
<tr>
<td>I&amp;HAS restoration</td>
<td>■</td>
</tr>
<tr>
<td>Check I&amp;HAS functions</td>
<td>■</td>
</tr>
<tr>
<td>Event register interrogation</td>
<td>■</td>
</tr>
<tr>
<td>Inhibition / isolation / override (based on level)</td>
<td>■</td>
</tr>
<tr>
<td>Addition / changes to individual authorisation codes (changes can only be made to your own code)</td>
<td>■</td>
</tr>
<tr>
<td>Addition / removal of users and level 2 codes</td>
<td>■</td>
</tr>
<tr>
<td>Addition / changes to specific site data</td>
<td>■</td>
</tr>
<tr>
<td>Changes / replacement of firmware</td>
<td>■</td>
</tr>
</tbody>
</table>
3 ARMING AND DISARMING THE SYSTEM

This chapter sets out the procedures for arming and disarming the intrusion alarm system using the keypad and remote control. It also explains the procedures to be implemented if the central unit rejects the arming operation due to faults detected in the system or the individual components. For remote arming or disarming see chapter Remote commands.

3.1 Arming or disarming using the keypad

3.1.1 Rapid arming or disarming

Total arming or disarming of the system can be performed, or customisable partial arming/disarming by pressing the ▲ key on the main screen.

If multiple users are set up, select a user from the list and enter the PIN or, if there is only one user, enter the PIN directly as requested.

A video will appear showing an icon that can be selected directly based on this criterion:

- System with one or more zones armed: disarming icon (as shown in the figure below).

![Disarm icon](image1)

Press OK. The central unit will beep 3 times and the intrusion alarm system will be disarmed.

- All zones disarmed: global Away mode arming icon appears (as shown in the figure below)

![Arm icon](image2)

Press OK The central unit will beep 1 time and the intrusion alarm system will be armed.

- In both cases: in addition to the other option, a further 2 icons of customized insertions (Favourite 1 and Favourite 2)

If you wish to select the other option, use the arrows to move and confirm using the OK key.

The rapid arming command can be customised: in this case the central unit performs this configuration instead of the pre-defined configuration (global away mode arming).
3.1.2 Global arming

The global arming of the intrusion system can only be performed by Users (PIN level 2) and by the Installer (PIN level 3 - if authorised by a level 2 User) that has permission on all the zones.

To arm the entire intrusion system using the keypad:
1. Log in as a level 2 user
   
   ![Arm/Disarm icon]

2. The central unit will automatically display the "Arm/Disarm" icon. Press OK. Select all zones
   
   ![All zones]

3. Then press OK
   
   ![Arm Away]

4. Using the arrow keys, select:
   - **Arm Away** to arm the system in Arm Away mode,
   - **Arm Stay** to arm the system in Arm Stay mode,
   - **Notification** to arm the system in Notification mode,
   and confirm your selection using the **ok** key.

   The central unit will beep 3 times and the intrusion alarm zones will be armed.

   If any event reports are stored in the memory, the zones will not be armed. Instead, the first unseen event in the memory will be displayed. Select System or Devices to view all events, or the Force Block item to arm the alarm system anyway (for more information see the following paragraph Forced Block Arming).

3.1.3 Global disarming

Global disarming of the intrusion system can only be performed by Users (PIN level 2) and by the Installer (PIN level 3 - if authorised by a level 2 User) that has permission on all the zones.

To disarm the entire intrusion alarm system using the keypad:
1. Repeat points 1 and 2 from the previous paragraph
2. Select "Disarmed".

   The central unit will beep 1 time and the intrusion alarm system will be disarmed.
3.1.4 Partial arming

The partial arming of the intrusion system can only be performed by Users (PIN level 2) and by the Installer (PIN level 3 - if authorised by a level 2 User) on the zones for which they have been authorized.

To partially arm the intrusion system using the keypad:
1. Repeat points 1 and 2 from the previous paragraph
2. Only the enabled zones will appear. Select the zone that you wish to arm. If a specific name has been given to the zone during programming, this will appear instead of the generic names Zone A, Zone B, etc.
3. Using the arrow keys, select:
   - **Away mode** to arm the system in Away mode,
   - **Home mode** to arm the system in Home mode,
   - **Notification** to arm the system in Notification mode,

and confirm your selection using the **ok** key.

The central unit will beep 3 time and the intrusion alarm zones will be armed.

If you wish to arm other zones, repeat the entire procedure for each zone to be armed.

3.1.5 Partial disarming

Partial disarming of the intrusion system can be performed by Users (PIN level 2) and by the Installer (PIN level 3 - if authorised by a level 2 User) on the zones for which they have been authorized.

To partially disarm the intrusion alarm system using the keypad:
1. Repeat points 1 and 2 from the previous paragraph
2. Select the zone that you wish to disarm. If a specific name has been given to the zone during programming, this will appear instead of the generic names Zone A, Zone B, etc.
3. Select “disarmed”

The central unit will beep 1 time and the selected zones will be disarmed.

3.2 Arming or disarming using the remote control

There are two types of remote control:

- Programmable remote control: this can be customised, and so there is not pre-set key to arm or disarm the entire system.
- Pre-programmed remote control: specific functions are assigned to the keys

Refer to the manual of each remote control for a guide to arming and disarming the system.

3.3 Arming using Forced Block

The intrusion alarm system will not arm in the following cases:

- Detector that is active or faulty.
- Active anti-burglar device.
- Movement detector obstructed or with limited range.
- Tampering.
- Power supply fault (network or battery).
- Faulty siren.
- Problems communicating with the devices.
- Problems with the alarm transmission system (GSM).
- Arming performed using remote control with low batteries
- Other faults
A detector is active if it is signalling an alarm status. For example, the magnetic contact on a door or window is open. An anti-burglar device is active if it is signalling a burglary attempt. E.g. a remote control when the burglary button is pressed.

However, a level 2 user can override the block for the zones they are authorised for and arm the intrusion alarm system. By overriding the block, the central unit will ignore any causes preventing normal arming of the system and will proceed with the arming.

**WARNING!**

Block override is an emergency measure to allow partial operation of the intrusion alarm system. It is important to understand that due to the issues detected, the protection offered by the system is reduced to a greater or lesser extent. The issues that caused the block must therefore be resolved as quickly as possible to restore full system operation.

### 3.4 Reset

If the alarm system cannot be armed due to potential inhibitions caused by technical alarms, faults or tampering alarms affecting the detectors, e.g. jamming-supervision, the status of the central unit or the individual zone should be reset. The function allows you to stop the persistent fault report caused by failure to transmit the "all clear" signal (e.g. a technical impulsive alarm such as a smoke alarm, flooding alarm, central unit battery, etc.).

The reset operation is recorded in the events log.

To reset the system or an individual zone, proceed as follows:

1. Log in as a level 2 user

2. Select Status and Events and press OK

3. Select Status and press OK

4. Select Alarm Reset: select System to reset the entire system, or the individual zone to be reset. When the system is reset, all counters relating to multiple alarms will be set to zero.
4 PANIC AND BURGLARY

This chapter outlines the procedures for activating the panic and burglar alarms. The panic alarm is generated voluntarily by the user when a potential danger is presumed. One example is the threatening presence of an unknown person. The panic alarm sounds the sirens, as a deterrent, but does not cause telephone messages to be sent.

The burglar alarm is generated voluntarily by the user when they are the victim of a burglary. This type of alarm does not cause the sirens to sound, to prevent the burglar from reacting. Instead it disarms the system if armed, and causes telephone alarm reports to be sent.

4.1 Activating the panic alarm

4.1.1 Activation using the keypad

To activate the Panic event, proceed as follows:

1. Log in as a level 2 user
2. Use the arrow keys to select the Panic icon and press ok. To stop the sirens before the programmed time has elapsed, disarm the system.

4.1.2 Activation using the remote control

Press the remote control button programmed to activate the Panic event. To stop the alarm by interrupting the programmed siren sound, press the remote control button programmed to disarm the system. See the remote control manual for more details.

4.2 Activate the burglar alarm

When the burglar alarm is activated, all other alarms that may be active are blocked, the system is deactivated if armed, and the burglar alarm voice telephone calls are activated.

4.2.1 Activation using the remote control

Press the remote control button programmed to activate the Burglary event.

To stop the alarm, press the remote control button programmed to deactivate the alarm.
5 ALARMS AND EVENT MEMORIES

5.1 Alarm priority

In the event of multiple simultaneous alarms of different types, only the highest priority alarm will sound. In the event of alarms with the same priority level, the first one to be triggered will sound. The table below shows the priority level of various types of alarms, where 1 represents maximum priority:

<table>
<thead>
<tr>
<th>Type of alarm</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion</td>
<td>1</td>
</tr>
<tr>
<td>Tampering</td>
<td>2</td>
</tr>
<tr>
<td>Supervision</td>
<td>3</td>
</tr>
<tr>
<td>Low battery</td>
<td>4</td>
</tr>
<tr>
<td>System</td>
<td>5</td>
</tr>
<tr>
<td>Panic</td>
<td>6</td>
</tr>
<tr>
<td>Technical</td>
<td>7</td>
</tr>
</tbody>
</table>

5.2 How to block an alarm

An alarm can be blocked by disarming the alarm system using the keypad, remote control or remotely. When an alarm is blocked, the sound signals (sirens) and phone reports (voice message and SMS) will stop.

Total disarming blocks all types of alarms, while partial disarming may or may not block the alarm, as shown in the table below:

<table>
<thead>
<tr>
<th>Type of alarm</th>
<th>Disarming</th>
<th>Zone not in alarm mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total</td>
<td>Alarm zone</td>
</tr>
<tr>
<td>Intrusion</td>
<td>Alarm block</td>
<td>Alarm block</td>
</tr>
<tr>
<td>Tampering</td>
<td>Alarm block</td>
<td>Alarm block</td>
</tr>
<tr>
<td>System (1)</td>
<td>Alarm block</td>
<td>Alarm block</td>
</tr>
<tr>
<td>Panic (1)</td>
<td>Alarm block</td>
<td>Alarm block</td>
</tr>
<tr>
<td>Technical (1)</td>
<td>Alarm block</td>
<td>Alarm block</td>
</tr>
</tbody>
</table>

(1) Also valid in relation to a zone that has already been disarmed

All alarms are stored in the mandatory events memory. An analysis of this memory will reveal the details of the alarm (when it happened, type of alarm, what device generated the alarm report, etc.).
5.3 Events history

Events are recorded in the central unit in two separate memory blocks:

- Mandatory, which may contain up to 250 separate events.
- Optional, which may contain up to 128 separate events.

When the maximum block capacity is reached, the new event overwrites the oldest event in the memory.

5.3.1 View events

To view events, proceed as follows:

1. Log in as a level 2 user

2. Select Status and events and press OK

3. Select 2 Critical events to examine the main events, 3 to examine the secondary events.

4. The detailed events screen will open. The events are displayed in order of most recent to oldest.
   Use the > and < keys to scroll through the events.
   To read the information relating to the event, see the Interpreting a stored event paragraph.

5.3.2 Interpreting a stored event

The data relating to the event is shown on one or more screens. The first screen appears similar to this:

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info 4</td>
<td>[n/t]</td>
<td></td>
</tr>
<tr>
<td>Info 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;Recent</td>
<td>Past&gt;</td>
<td></td>
</tr>
</tbody>
</table>

where:
- [n/t] indicates the progressive number of the event (n) and the total number (t) of events in the memory.
- Date is the date on which the event occurred.
- Time is the time that the event occurred.
- **Info 4 ... Info 7** provides additional information that varies according to the type of event and that is specified in the tables below.
- ➤ and ◀ allows you to scroll forward and backward through the events

### Main events (mandatory)

<table>
<thead>
<tr>
<th>Event type</th>
<th>Info 4</th>
<th>Info 5</th>
<th>Info 6</th>
<th>Info 7</th>
<th>Second screen (Inf)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>System / Zone armed</td>
<td>Name or ID of the user who armed the system</td>
<td>Device used for the operation</td>
<td>Previous zone status</td>
<td>Status following arming</td>
</tr>
<tr>
<td>Disarming</td>
<td>Disarmed system / zone</td>
<td>Name or ID of the user who disarmed the system</td>
<td>Device used for the operation</td>
<td>Previous zone status</td>
<td>Status following disarming</td>
</tr>
<tr>
<td>Burglar alarm</td>
<td></td>
<td>Name or ID of the user who performed the operation</td>
<td>Device used for the operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion alarm</td>
<td></td>
<td>Type of Sensor</td>
<td>Sensor Position</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tampering alarm</td>
<td></td>
<td>Type of Sensor</td>
<td>Sensor Position</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervision</td>
<td></td>
<td>Type of Sensor</td>
<td>Sensor Position</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radio jamming alarm</td>
<td></td>
<td>Central unit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tampering</td>
<td></td>
<td>Central unit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detector exclusion</td>
<td></td>
<td>Type of Sensor</td>
<td>Position</td>
<td>User ID</td>
<td></td>
</tr>
<tr>
<td>Block override</td>
<td></td>
<td>Arming</td>
<td>User name or ID</td>
<td>Device used</td>
<td></td>
</tr>
<tr>
<td>Fault – Fault type</td>
<td></td>
<td>Type of Sensor</td>
<td>Position</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low battery</td>
<td></td>
<td>Type of Sensor</td>
<td>Position</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 2 user</td>
<td></td>
<td>New User L. 2-3</td>
<td>PIN Lev3 Index</td>
<td>PIN Lev2 Index</td>
<td></td>
</tr>
<tr>
<td>added by level 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date and time</td>
<td></td>
<td>User ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Num. Variation</td>
<td></td>
<td>User ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central unit SW</td>
<td></td>
<td>User ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central unit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>start-up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Periodic GSM</td>
<td></td>
<td>Tel. ID (1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>inspections</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>power supply</td>
<td></td>
<td>Battery Level</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network power supply return</td>
<td>Battery Level</td>
<td>No 230V</td>
<td>Network time OFF minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------</td>
<td>---------</td>
<td>-------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice call</td>
<td>Alarm type</td>
<td>Telephone ID calls (1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send SMS</td>
<td>Alarm type</td>
<td>telephone IDs recipients</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(1) In bold if the call was successful, i.e. the recipient picked up; normal if the call was unsuccessful.

<table>
<thead>
<tr>
<th>Event type</th>
<th>Info 4</th>
<th>Info 5</th>
<th>Info 6</th>
<th>Info 7</th>
<th>Second screen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion pre-alarm</td>
<td>Type of Sensor</td>
<td>Position</td>
<td>Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login</td>
<td>User ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logout</td>
<td>User ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
6 REMOTE COMMANDS

If enabled, it is possible to interact with the central unit remotely with GSM using telephone lines and DTMF tones or SMS messages. The central unit must be equipped with an active SIM Card.

6.1 Telephone commands with DTMF tones

The central unit telephone number can be called from any telephone, as long as DTMF tones can be sent. The telephone number used to place the call need to be included among the numbers stored by the central unit. Caller authentication and privileges to operate the central unit are guaranteed using the same ID-password system used to perform authentication on the central unit keypad. Phone sessions last a maximum of 1 minute before the arming is interrupted by the central unit. During this time, the user can send any commands it wants to the central unit.

To send commands using DTMF tones:
1. Dial the telephone number of the central unit (the one on the SIM Card installed in the central unit).
2. The central unit will respond with the voice message “Enter User and press asterisk”. Use the telephone keypad to input a level 2 or 3 user ID (1 digit) and press the * key to confirm.
3. The central unit will respond with the voice message “Enter PIN and press asterisk”. Use the keypad to enter the telephone password (5 digits) combined with the ID code sent previously and press the * key to confirm.
4. If the ID-password pair is incorrect, the central unit will respond with the voice message “Incorrect user” and repeat the procedure from point 1. After 5 failed authentication attempts, the phone call will be interrupted and the episode will be stored in the events log as “Tampering from telephone no. xxxxxxxxxxx”. If the number is hidden, the caller will not be recorded in the log.

If the authentication process is successful, the central unit will respond with the voice message “Enter command and press asterisk”. Use the keypad to enter the command code (2 digits) specified in the table below and press the * key to confirm.

<table>
<thead>
<tr>
<th>List of DTMF Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Function</strong></td>
</tr>
<tr>
<td>Anti-intrusion (all of the zones for which the user placing the call is authorised)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Command 1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Command 2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Command 3</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Command 4</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Command 5</td>
</tr>
</tbody>
</table>
5. If the command is not recognised, the central unit will respond with the voice message "Incorrect command" and repeat the procedure from point 5.
   If the command is recognised, the central unit will respond with the voice message "Confirm?" Press the * key to confirm.

6. The central unit will execute the command and send a confirmation voice message: "Command executed".
   The central unit will repeat the procedure from point 5 to accept other commands. If no other commands need to be sent, hang up the telephone to end the communication, or enter the next command. Communication is automatically interrupted after one minute.

**WARNING!**

In the case of non-optimal GSM signal, the control unit may not correctly detect DTMF tones. When this happens, the control unit doesn’t respond with any voice message or requests to re-enter ID and PIN.

If you intend to use telephone commands with DTMF tones, it’s recommended to install the control unit in a position with good reception of the GSM signal.

### 6.2 SMS Commands

In order to accept SMS commands, the number placing the call must be included among those stored in the central unit, and obviously must not be hidden. If the number is not included in the list, or is hidden, the central unit will ignore the request.

Privileges to operate the central unit are guaranteed using the same ID-password system used to perform authentication on the central unit keypad. All commands require authentication, with the exception of status requests and the scene.

Level 2 users can send SMS commands.

Commands are sent using coded SMS messages, to which the central unit replies with a response SMS or clear confirmation, unless it has been specifically instructed not to send a response.

A separate SMS must be sent for each command.

The general structure of the command is:

```
[command] [what] [mode] [user + PIN]
```

<table>
<thead>
<tr>
<th>Command</th>
<th>What</th>
<th>Mode</th>
<th>User + PIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arm</td>
<td>System</td>
<td>Home-mode</td>
<td>6-digits numerical code</td>
</tr>
<tr>
<td></td>
<td>Zone name</td>
<td>Away-mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Notification</td>
<td></td>
</tr>
<tr>
<td>Disarm</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Zone name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scene # (1-10)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The answer/confirmation SMS is as follows:

- Zone A (*) Away-mode
- Zone B Away-mode
- Zone C Home-mode
Zone D  Home-mode

- The star (*) indicates a zone anomaly: the detail of the anomaly is explicated in the central unit or by connecting to free@home;
- Up to 4 zones, the control unit sends 1 SMS;
- Beyond the 4 zones, the control unit sends 2 SMS;
- The technological zone (24h) will not be listed as it is always active.

When an unknown or incorrect SMS is sent, the control unit answers with an example SMS of the correct syntax, as follows:

Example:
Arm ZoneA Home-mode 111111
Disarm ZoneA 111111
Scene 1

7 SYSTEM STATUS

To check the status of the central unit and the radio connections:

1. Log in as a level 2 user

2. Select Status and events log and press OK

3. Status Selector

   1. Select Central unit
      The following information is displayed on the central unit:
      - **Tamper**: OK = tamper off / On
      - **Modem** (GSM): Signal Level / NO SIM
      - **Battery**: NO = no battery / voltage and battery temperature
- **Network:** Yes / NO
- **Address:** the hexadecimal address of the central unit.

  Pressing the > key opens a new window in which the current quality of radio communications and the occupation of the radio channel (Duty Cycle, should not exceed 1 el time) are shown in the last 15 minutes, in the last hour and in the last 24 hours. If there is no data, the message "Not available" appears.

2. Select Zones and Sensors: the various zones are displayed and within each zone information on the status of the programmed sensors is displayed.
3. System Devices: displays the status of system devices such as Sirens and Repeaters.
4. Alarm Reset: allows you to remove all the anomalies displayed in the status of both the system and the sensors if they have been resolved: for example, the operation clears the notification of "Alarm Mem" but does not remove an anomaly of the type "ma-nomination" if it remains on the device.
5. Postponed sync: Displays the list of sensors, if any, on which a change of one or more radio parameters has been made while waiting for this change to be actually implemented on the sensor. If the list is not empty, a type symbol 🕵️ appears in the top right of the display in the rest window.
8 CENTRAL UNIT SETTINGS

This chapter sets out the procedures for setting the central unit date and time, display lighting, audible feedback and the sound of the internal siren (buzzer).

8.1 Adjust display

1. Log in as a level 2 user.
2. Use the arrow keys to select the Options icon and press ok.
3. Press 1 Adjust display
4. Use the arrow keys to move and select Yes or No using the arrow keys to activate or deactivate "automatic off". When "automatic off" is activated, the display illumination switches off 60 seconds after the last key was pressed.
5. Select Yes/no to activate sound feedback for the keys.
6. Select Yes to completely switch off the buzzer sound for any alarm event.

8.2 Audio Settings

8.2.1 Beep volume

To adjust the sound feedback for the keys and the internal buzzer, perform points 1 and 2 from the previous paragraph and press Audio settings:

Press 1 Beep volume

Set the feedback volume for the keys of select No to switch it off.
Set "Switch off Buzzer" to Yes if you want to fully switch off the internal siren sound.

### 8.2.2 Sound Feedback

To adjust the sound feedback, perform points 1 and 2 from the previous paragraph and press Audio settings:

Press 2 Sound feedback and then press the number of the command for which you wish to configure sound feedback. The options are:

- **1 Arming** partial or total system arming
- **2 Disarming** (total or partial) disarming of the anti-intrusion system.
- **3 Arming fault**

A new screen appears

You can now choose how many (if any) beeps to activate for the command:

- **Local** includes the central unit keypad, remote control and connector.
- **Remote** the sound feedback emitted when the event is caused by f@h, GSM, or a timed command.

You can select the number of beeps that will be emitted (from 0 to 3) for each type of feedback.

### 8.2.3 Alarms

To adjust the central unit buzzer in the event of alarms, perform points 1 and 2 from the previous paragraph and press Audio settings:

Press 3 Internal Siren and then Set Reactions.

Press the number of the alarm for which you wish to configure sound feedback. The options are:
- **Away mode**, i.e. the intrusion alarm with the anti-intrusion system armed in away mode. This section also includes the **Panic and system tampering (when system is armed) and zone (always)** alarm.

- **Home mode**, i.e. the intrusion alarm with the anti-intrusion system armed in home mode.

- **Notification mode**, i.e. the intrusion alarm with the anti-intrusion system armed in notification mode.

- **Technological**, i.e. any of the technological alarms configured (flooding, gas leak, etc.), including when the anti-intrusion alarm system is deactivated.

A new screen appears:

![Type of sound](options.png)

A value can be selected using the arrow keys. The following parameters can be configured:

- **Sound type**; beep or continuous sound

- **Sound duration**, i.e. for how long the central unit buzzer should sound. (0-30sec-1-2-3-4-5-6-7-8-9min).

- Default: 3 min for Away mode and Home model intrusion alarms, 30 seconds for Pre-alarm and technological alarm.

**Zones filter**: allows you to select the zones to be taken into account in the event of an alarm (only for intrusion alarms and sensor tempering alarms). Factory settings include all zones. If the alarm occurs in an excluded zone, the internal siren will not be triggered.

### 8.3 Setting date and time

Setting the date and time is fundamental for correct storage of events in the log according to times.
The central unit automatically handles the summer time/winter time switchover and vice versa.

To set the date and time:

1. Log in as a level 2 user

![Options](options.png)

2. Use the arrow keys to select the Options icon and press ok.
3. Press 3 Change Date and time

4. Enter data and time using the numerical keys; use the arrow keys to move. Confirm the date and time entered by pressing ok

8.4 Change PIN
To change your PIN:

1. Log in as a level 2 user.

2. Use the arrow keys to select the Options icon and press ok.

3. Press 4 Change Pin

4. Set the current PIN, the new PIN (2 twice) and press OK to save

8.5 Operating method and change language
To change the operating method:

1. Log in as a level 2 user.
2. Use the arrow keys to select the Options icon and press ok.
3. Press 5 Operating Method

- Exclude
  i. Select "Force Block" to exclude the option: when Force Block is Excluded, the central unit performs the system activation function without requesting further confirmation in the event of one or more system faults.
  ii. Select Led Notice to exclude the yellow “Notifications” triangle and consequent need to reset. If disabled, the LED will never switch on, even if there are stored notifications, or notifications that still have not been viewed by the user.
  iii. Select All to exclude both Force Block and LED.
  iv. Select None to keep the pre-defined settings.

WARNING!
Exclusion of the Force Block and exclusion of the LED do not comply with the EN 50131-1 standard.

- Language: select the desired language

WARNING!
Language selection only comes into effect after the central unit has been restarted

8.6 Customize quick entry

To set a customised rapid arming command:
1. Log in as a level 2 user.
2. Use the arrow keys to select the Options icon and press ok.

3. Press 6: Favorite: opens a screen
4. Select the favourite you want to modify (1/2) and press OK

```
Favorite
Zone A
Away mode arming>
Zone B
Home mode arming>
Zone C
<No action>
```

5. For each system zone, choose the type of arming from among the following:
   - Away mode
   - Home mode
   - Notification
   - Disarmed
   - No action
   
   For each zone, the initial default is: **Away mode**

This custom setting, once saved, will be executed every time a "Quick Entry" command is executed instead of the default settings (Favorite1 = weapon all zones in Indoor mode, Favorite2 = weapon all zones in Pre-alarm mode).
INSTALL AND CONFIGURE THE SYSTEM

This section of the manual contains all of the information to use, configure and maintain the alarm central unit. It also provides suggestions for planning an Intrusion alarm system, includes a list of the technical specifications of the central unit and sets out the procedures for isolating the system and resolving any faults.

This section is intended for use by the technician who installs the system.

9 MAIN CHARACTERISTICS

9.1 Main functions of the central unit

The central unit communicates with the other system devices via radio-frequency and provides the user with the following functions:

- management of anti-intrusion and domestic security devices;
- management of panic reports;
- external device implementation commands;
- alarm notifications, via voice messages or SMS, to the programmed telephone numbers;
- system remote control via SMS or DTMF tone commands;
- integration of the Home Automation Busch-/ABB-free@home system

9.2 System capacity

The central unit manages up to 8 programmable zones, each of which can contain up to a maximum of 64 detectors, for an overall total of 64 across the system. The number of actual zones is determined during the central unit configuration phase.

Zones can be individually programmed as follows:

- intrusion alarm - up to a maximum of 7 zones
- technological alarms (smoke, flooding, gas) - 1 zone active on a 24h basis;

The central unit manages up to:

- 4 external sirens;
- 4 signal repeaters; (1)
- 16 remote control devices to activate or deactivate the intrusion alarm system; (1)
- 12 programmable telephone numbers to which alarm reports and events can be sent.

(1) the signal repeaters devices are not IMQ-Security Systems certified
10 DESIGNING A SYSTEM

Designing an intrusion and security alarm system using battery-powered radio devices is easy, provided that you follow some simple instructions. A good design ensures easy installation and proper functioning of the system. This chapter provides all of the information required to reach these objectives.

10.1 Information on radio waves

The systems that use radio waves to connect devices offer the significant benefit of being able to install and connect the various pieces of equipment without needing to perform complex wiring operations. One disadvantage is that greater care is required when positioning the devices, in order to obtain the best radio connection.

The quality of a radio connection is directly proportional to the power of the signal that reaches the device. This power is affected by the distance between the devices (the power of the radio signal decreases with each square of distance) and any signal absorption phenomena caused by obstacles along the radio wave route.

<table>
<thead>
<tr>
<th>Remaining power after crossing</th>
<th>Material crossed</th>
</tr>
</thead>
<tbody>
<tr>
<td>90-100%</td>
<td>Wooden or plastic furniture, synthetic materials (e.g. plexiglass), glass, perforated bricks, plasterboard</td>
</tr>
<tr>
<td>65-85%</td>
<td>Solid bricks, marble, fish tanks</td>
</tr>
<tr>
<td>10-60%</td>
<td>Reinforced concrete, metal structures (household appliances, pipes, railings)</td>
</tr>
<tr>
<td>0-10%</td>
<td>Metal sheets, mirrors</td>
</tr>
</tbody>
</table>

10.2 Use the zones

The zones serve to group the detectors together based on function, for improved use of the system. During the configuration phase, both the number of zones and their type can be determined.

10.2.1 Zone types

Zones can be programmed as follows:
- intrusion alarm: groups together the detectors that signal intrusion attempts and that must only be enabled when needed, typically when the area to be protected is unattended;
- active on a 24h basis: groups together the detectors that must always be on to provide reports relating to security, e.g. flooding detectors, smoke detectors, gas detectors and technological detectors in general;

The intrusion alarm zones can be configured in Notification mode, Home mode or Away mode. Notification and Home modes assume that the areas are not fully unattended, and therefore no signal of any kind is activated (external sirens and telephone messages).

In the event of an alarm in Away mode, on the other hand, all reports provided for by the system will be activated. All of these actions can be configured.
**WARNING!**
The technical zone (24h) and Pre-alarm and Internal Alarm modes do not comply with the EN 50131-1 standard. The functions relating to domestic security, for example flooding detectors, smoke detectors, gas detectors and technological detectors in general, and the Home Automation functions, are not covered by EN 50131 1 and EN 50131 3 standards.

### 10.2.2 Subdivision into zones

Subdivision of the intrusion alarm system into zones allows greater flexibility in terms of management and meeting user needs. For example, perimeter detectors (e.g. window and door opening) can be associated with one zone, and passive infra-red detectors with another. This way, the user can activate just the first zone at night, for when they are asleep, and both when the leave the house unattended. This setting signals intrusion attempts while the user sleeps, but allows people to move freely as required within the house. The option to activate and deactivate various zones is also very useful if there is a garage, a shop, an office or a laboratory adjacent to the house. In such cases, the option of associating the various areas with different zones makes it possible to protect them selectively, via a single system, arming the anti-intrusion function when nobody is present.
11 INSTALLING THE CENTRAL UNIT

Refer to the specific "Installation sheet" rapid guide for information on installing and securing the central unit.

11.1 Workspaces

The central unit manages 2 separate workspaces: the end user's workspace and the installer's workspace. Two specific authentications are required to access these two spaces: a level 2 authentication and a level 3 authentication.

As standard, the first log-in must always be performed by a level 2 user, followed by a level 3 user for the functions that require it.

When a level 2 user logs in, the menu described in paragraph 2.1.3 Main user menu appears.

When you access the installer section the specific screen for the environment appears:

11.2 Commissioning

11.2.1 Reading operational sequences

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sequence number</td>
</tr>
<tr>
<td>2</td>
<td>Screenshot</td>
</tr>
<tr>
<td>3</td>
<td>Selected / highlighted line</td>
</tr>
<tr>
<td>4</td>
<td>Interactive area on the central unit (keys alphanumeric, arrows, etc.).</td>
</tr>
</tbody>
</table>

11.2.2 First start-up

At the first start of the central unit or following a reset, it is necessary to proceed with configuration (language setting, creation of users, acquisition of security devices, creation of zones, etc.).

The following procedure lets you program the system:
Important, keep the installer PIN carefully!

⚠️ For security reasons, if the PIN is lost, the entire system will have to be reset and any settings will be lost.

INFO: Sequence 3 is displayed only when the secure@home central unit is connected, via a BUS cable, to a free@home System Access Point.

INFO: For the insertion of the battery and configuration of the device, refer to the relative instruction sheet.
INFO: The image represents a generic device. The configuration can be performed on all the secure@home devices.

INFO: The configuration steps may vary according to the characteristics of the installed security device.

INFO: Step 8 is applicable only for anti-intrusion sensors. Safety sensors (smoke, flooding) are automatically assigned to an H24 active zone. System devices (remote controls, sirens, repeaters, etc.) are not assigned to any specific zone.

Once the zone has been created and the safety device assigned to it the central unit returns to screen number 5.
INFO: It is possible to acquire a new device by inserting Battery into a new sensor and following the procedures indicated in screen 5 to 8, otherwise select “Finish Setup” to complete the installation.
Perfect radio signal.

Good radio signal.

Insufficient radio signal: move the sensor to improve communication or add a wireless repeater.

Fault (tampering, blinding, failure, etc.): check the sensor.

To find out the details of the installed device, select the corresponding item (ex: "01 IR Garage") and confirm with the key.

Sensor details:
- F6B4C0B2 - 20 dbm
- Sensor type: INFO
- Internal IR
- Last rx
- Date time

To return to screen 14 and continue with the programming, go back using the button.

11.3 Status of the system

Once the programming is finished, you can view the Home Page:
<table>
<thead>
<tr>
<th>Status of</th>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| 1        | ![Icon] | On the Idle screen you will be able to view one of the following messages:  
**All zones armed**: all zones are armed in the same way.  
**All zones disarmed**: all zones are disarmed.  
**Mixed armed**: the zones are armed in different modes or some are disarmed. |
| 2        | ![Icon] | The battery icon displayed may indicate one of the following statuses:  
**Battery connected and charging**: the central unit is connected to the 220V network.  
**Battery not connected**: the central unit is connected to the 220V network.  
**No network**: the control panel is battery powered (with indication of the charge level). |
| 3        | ![Icon] | The GSM icon indicates, with the number of bars, the level or the lack of signal.  
**Perfect GSM signal**.  
**Good GSM signal**.  
**Low GSM signal**.  
**No GSM signal**. |

### 11.3.1 Arm / disarm the system

From the Idle Screen it is possible to arm / disarm the system quickly by pressing the button ⬆️:

INFO: The default GLOBAL ARM will put the entire system in Arm Away mode, until a preferred mode / combination of zone activation is defined, associated with this command.
11.3.2 Display alarm zones

From the Idle Screen it is possible to view the actual status of the configured zones by pressing the button 

- **Notification Mode**: any intrusion alarm is notified silently (for example with push notifications or SMS), without using the indoor and outdoor sirens.

- **Home Mode**: any intrusion alarm is signaled only through the indoor siren, embedded in the Central Unit, and notifications (for example push or SMS), excluding the use of outdoor sirens.

- **Away Mode**: in case of alarm, all the signals provided by the system will be activated, including the indoor and outdoor sirens.

Scrolling further down, you get to the page that shows the system status.

**INFO**: If you need to scroll more pages, press and hold the key to scroll down quickly and get faster to the last page.


If necessary, install the updated version.

11.4 Authentication

For general information on authentication, refer to chapter 2.4.

**WARNING!**

- In working mode, no level 3 user can access the system unless authorised by a level 2 user.

1. Press the ok key on the key pad. A window will appear showing the level 2 users set up for the system;
2. Select the user from the list and enter the PIN. The digits entered appear as asterisks (*).
3. Press the ok key to confirm. If the PIN entered is not 5 digits long, the ok key will not be accepted. If the user enters the wrong PIN, a tampering alarm is generated on the tenth attempt.
4. If the authentication process is successful, the main user menu screen appears (described in chapter 2.3).
5. Select the icon and enter a valid PIN to access the Installer screen.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Zones and Sensors" /></td>
<td>Zones and Sensors. This provides access to the zones and sensors programming menu</td>
</tr>
<tr>
<td><img src="image" alt="System Test" /></td>
<td>System test. Provides access to the system test menu.</td>
</tr>
<tr>
<td><img src="image" alt="System Devices" /></td>
<td>System devices This provides access to the main system device programming menu (remote controls, keypads, sirens, repeaters)</td>
</tr>
<tr>
<td><img src="image" alt="Maintenance" /></td>
<td>Maintenance. This provides access to the system maintenance menu (access only granted to a level 4 user)</td>
</tr>
<tr>
<td><img src="image" alt="User Management" /></td>
<td>User management: this allows management of system users, setting their PINs, permissions and access restrictions</td>
</tr>
<tr>
<td><img src="image" alt="Contacts" /></td>
<td>Contacts: this allows the telephone numbers to be programmed and the associated events to be defined.</td>
</tr>
<tr>
<td><img src="image" alt="Remote Access" /></td>
<td>Remote access: this sets out the parameters for arming via Home Automation f@h</td>
</tr>
<tr>
<td><img src="image" alt="Arm/Disarm" /></td>
<td>Arm/Disarm: to arm/disarm the system or individual zones.</td>
</tr>
<tr>
<td><img src="image" alt="Exit" /></td>
<td>Exit. Exit the main menu and return the central unit to idle mode.</td>
</tr>
</tbody>
</table>
## 11.5 General and alarm reports

The central unit manages alarm situations or faults using the following reports:

<table>
<thead>
<tr>
<th>Cause</th>
<th>LED or device buzzer</th>
<th>Central unit</th>
<th>Siren</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification alarm</td>
<td>■ (1)</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Home mode alarm</td>
<td>■ (1)</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Away mode alarm</td>
<td>■ (1)</td>
<td>■ ■ ■ ■ ■ ■</td>
<td></td>
</tr>
<tr>
<td>System tampering alarm with external system activated</td>
<td>■ ■ ■ ■ ■ ■</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System tampering alarm with external system deactivated</td>
<td>□ ■ ■ ■</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensor tampering alarm with external system activated</td>
<td>■ ■ ■ ■ □ □</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensor tampering alarm with Internal/Pre-alarm system de-activated or activated</td>
<td>■ □ □ □ □</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jamming alarm</td>
<td>■ ■ ■ □ □</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Panic alarm</td>
<td>■ ■ □</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Burglar alarm</td>
<td>□ □</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assistance alarm</td>
<td>□ □</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fire alarm</td>
<td>□ □ □ □ □</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gas alarm</td>
<td>□ □ □ □ □</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flooding alarm</td>
<td>□ □ □ □ □</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technological alarm</td>
<td>□ □ □ □ □</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No GSM</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No 230 V network</td>
<td>■</td>
<td>□ □</td>
<td></td>
</tr>
<tr>
<td>230 V network return</td>
<td>■</td>
<td>□ □</td>
<td></td>
</tr>
<tr>
<td>Device battery low</td>
<td>□ □</td>
<td>□ □</td>
<td></td>
</tr>
<tr>
<td>Device fault</td>
<td>□ □</td>
<td>□ □</td>
<td></td>
</tr>
<tr>
<td>Central unit battery low</td>
<td>■ ■</td>
<td>□ □</td>
<td></td>
</tr>
<tr>
<td>Technical support with</td>
<td>□ □</td>
<td>□ □</td>
<td></td>
</tr>
<tr>
<td>Radio fault</td>
<td>■</td>
<td>□ □</td>
<td></td>
</tr>
<tr>
<td>Home mode anti-theft arming</td>
<td>■ □ □ □ □ □</td>
<td>□ □ □ □ □ □ □</td>
<td></td>
</tr>
<tr>
<td>Away mode anti-theft arming</td>
<td>■ ■ ■ □ □ □</td>
<td>□ □ □ □ □ □ □</td>
<td></td>
</tr>
<tr>
<td>Notification mode anti-theft arming</td>
<td>■ □ □ □ □ □</td>
<td>□ □ □ □ □ □ □</td>
<td></td>
</tr>
<tr>
<td>Anti-theft disarming</td>
<td>■ ■ ■ □ □ □</td>
<td>□ □ □ □ □ □ □</td>
<td></td>
</tr>
</tbody>
</table>

- ■ factory-enabled report compliant with EN 50131-1 regulations.
- □ optional programmable report
- (1) if included on the device
12 PROGRAMMING

At the time of first log-in, the guided sequence of steps (Wizard) set out in the Quick Guide manual for the Central unit allows the system to be programmed for the first time.

This initial configuration can in any case be increased or modified from the installer screen:

The icons are described in paragraph 11.2.1 Authentication.

12.1 System creation

The system creation process consists of acquiring and programming the various devices (detectors, repeaters, remote controls and sirens) and services (telephones, DTMF) required to create and configure users and for the final system test.

During the work system, the menus can be navigated in reverse by pressing the left arrow key, without needing to log in for each operation.

WARNING!
If you inadvertently leave the main menu and return to the idle system screen, you will need to log in again.

12.2 Programming zones and sensors

12.2.1 To programme a new zone:

1. Access the installer screen and log in as a level 3 user
2. Select the Zones and Sensors icon
3. The list of zones already created on the system and the Technological zone (always available) will appear.
4. Select New Zone
5. Modify the default sticker (optional)

12.2.2 To modify or delete a zone:

Select the desired zone.
A video appears offering the option to view the sensors programmed for the zone.
Select:
- Rename to modify the zone label
- Delete to delete the zone
12.2.3 To programme a sensor:

- Repeat points 1-3 of paragraph 12.2.1
- Select New Device: the central unit is waiting, get the central unit to discover the detector by following the instructions included with the device: the detector continues to wait for the parameters for 5 minutes before going into "low power consumption" mode

![New Device Waiting for the device...](image)

- When the device has been obtained, the following video will appear:

```
Label: [                   ]
Address: F831CB41
Type: External IR
Signal: -36 dbm
```

The list of parameters spans multiple pages. Use the arrow keys to scroll the pages. The parameters displayed in normal characters, rather than in bold, are read-only. These are:
- **Address**: hexadecimal address of the detector.
- **Type**: generic name of the detector.
- **Signal**: detector radio signal level, measured in dBm (decibel mW).
- **Repeater**: ID of the repeater used, if the detector does not communicate with the central unit directly, but rather via the repeater. "Not set" means that the detector communicates directly with the central unit.

Configure the parameters. The table in the subsequent paragraph lists all of the parameters for the detectors, their meaning and their possible values. Use the arrows to select the desired value from among the available values.

- Press Save or ok key to save the configuration.
- Associate the sensor with a zone.

**WARNING!**
The technological sensors are automatically assigned by the system to a technological zone.

12.2.3.1 Parameters for detectors

The table lists the possible parameters shared by the various detectors. The additional specific parameters for a type of detector are shown in the manual for that detector.
### Parameter | Meaning | Possible values
--- | --- | ---
**Label** | Serves to better identify the detector. A descriptive and unique name is recommended, e.g. KITCHEN, LIVING ROOM, BATHROOM, PORCH etc. | Alphanumerical characters, maximum length 10 characters.

**Exclude** | Exclude the detector (the central unit will ignore any of its alarm reports), while maintaining the configuration. Corresponds to the Isolation function, as defined in the EN 50131-1 standard. | YES, NO

**Supervision** | Select the frequency at which the central unit states that the detector functions. | NO, 15, 45 (1)

**Delay (2)** | Delay time between alarm system arming and activation of alarms when leaving the protected areas, or delay time between intrusion detection and alarm reports when a protected area is entered. Allows you to leave the protected areas after arming the alarm using a command device without triggering the report or to enter the protected areas and disarm the alarm system located within those areas. The entry delay time must only be applied to detectors that cover the route between the entry point (door, garage shutter, etc.) and the command device. | NO, 15, 30, 60, 90. If NO is selected, the alarm report is immediate. (2)

The underlined values are the factory settings.

(1) Frequencies other than 15 minutes do not comply with regulation 50131-6 par. 4.5.1.

(2) Settings based on time delays other than 0 do not comply with the EN 50131-1 and EN 50131-3 regulations.

(3) Subsequent amendments to parameters outside of this interval are stored on the control panel and received by the detector when the first useful transmission is performed: notification of this situation is provided via the icon in the top right of the display.

### 12.3 Programming system devices

This menu allows you to programme remote controls, sirens and repeaters.

Access the Programming menu and log in as a level 3 user.

#### 12.3.1 Remote Control Programming

**WARNING!** Transmissions from the remote control to the central unit are encrypted, and have a variable code that has 65536 possible combinations for each individual command transmitted.

Select the “system devices” icon and then “remote controls”:

Select “New device” and press OK
Get the central unit to discover the remote control by following the instructions included with the device. At this point the remote control configuration can be set; this is different for the 2 types.

12.3.1.1 Numerical remote control configuration

All 5 keys for this type of remote control (codes SAD-W2.1F and SAD-W2.11F) can be configured at the user’s discretion.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Factory configuration</th>
<th>Customisable</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Key 1</td>
<td>Panic</td>
<td>Key Yes / LED No</td>
</tr>
<tr>
<td>2</td>
<td>Key 2</td>
<td>Global Away mode arming</td>
<td>Key Yes / LED Yes</td>
</tr>
<tr>
<td>3</td>
<td>Key 3</td>
<td>Global Home mode arming</td>
<td>Key Yes / LED Yes</td>
</tr>
<tr>
<td>4</td>
<td>Key 4</td>
<td>Status Request</td>
<td>Key Yes / LED Yes</td>
</tr>
<tr>
<td>5</td>
<td>Key 5</td>
<td>Global disarming</td>
<td>Key Yes / LED Yes</td>
</tr>
</tbody>
</table>

Select the numerical remote control from the list and press the OK key. A window opens that enables a function to be associated with each button.

Go to the Key and set the desired function using the <> arrows. The possible functions are:

<table>
<thead>
<tr>
<th>Type of Association</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zones</td>
<td>The button arms/disarms one or more zones</td>
</tr>
<tr>
<td>Functions</td>
<td>Performs one of the functions listed below</td>
</tr>
<tr>
<td>N.A.</td>
<td>Not set</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Environment</th>
<th>Functions</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety</td>
<td>Burglar</td>
<td>Triggers a silent alarm</td>
</tr>
<tr>
<td></td>
<td>Panic</td>
<td>Starts up an audible alarm</td>
</tr>
<tr>
<td></td>
<td>Assistance</td>
<td>Activates an assistance event</td>
</tr>
</tbody>
</table>
By selecting **Zones**, another screen will appear that allows you to configure the selected action. Use the arrow keys and the OK key to save.

**Cyclical** this applies to any zone set using the “arming” type in any of the three available methods. This does not apply when the “disarming” type is selected. The cyclical mode is not available for special functions.

![WARNING!](image)

The arming block is not active in the Cyclical case; as such this does not comply with the EN 50131-1 standard.

**Zones**: The following mode options can be selected for each zone: arming, disarming or None (not set)

<table>
<thead>
<tr>
<th>Display notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Away mode</td>
<td>Away mode arming</td>
</tr>
<tr>
<td>Home mode</td>
<td>Home mode arming</td>
</tr>
<tr>
<td>Notification mode</td>
<td>Notification mode arming</td>
</tr>
<tr>
<td>Disarm</td>
<td>Disarm</td>
</tr>
<tr>
<td>Not set</td>
<td>No Action</td>
</tr>
</tbody>
</table>

**Configure the LEDs.** LEDs 2-5 can be configured to visually indicate the status of one or more zones, while LED 1 (Service) cannot be configured. The LED can light up with three different predefined, non-configurable colours:

<table>
<thead>
<tr>
<th>Colour</th>
<th>LED Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Disarmed zone(s)</td>
</tr>
<tr>
<td>Red</td>
<td>Armed zone(s)</td>
</tr>
<tr>
<td>Amber</td>
<td>Arming block (*)</td>
</tr>
</tbody>
</table>

If multiple zones refer to the same LED, the following rule applies: all disarmed - green, one or more armed - red. The zones associated with the LED can be set using multiple selection.

### 12.3.1.2 Pre-configured remote control configuration

All functions on this type of remote control (codes SAD-W1.1F and SAD-W1.11F) are pre-configured. Only the ![Panic key](image) and ![Away mode Key](image) keys can be customised.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Factory configuration</th>
<th>Customisable</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Panic key" /></td>
<td>Panic key</td>
<td>Panic</td>
<td>Key Yes / LED No</td>
</tr>
<tr>
<td><img src="image" alt="Away mode Key" /></td>
<td>Away mode Key</td>
<td>Global arming in away mode</td>
<td>Key No / LED No</td>
</tr>
<tr>
<td><img src="image" alt="Home mode Key" /></td>
<td>Home mode Key</td>
<td>Global arming in home mode</td>
<td>Key No / LED No</td>
</tr>
</tbody>
</table>
To configure the customisable keys, select the remote control from the list and press the OK key. A window opens that enables the user to assign a function.

Go to the key to be customised and set the desired function using the <> arrows. The possible functions are:

<table>
<thead>
<tr>
<th>Key</th>
<th>Type of Association</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key +</td>
<td>Functions</td>
<td>Panic / Assistance / Burglar</td>
</tr>
<tr>
<td>Key +</td>
<td>Zones</td>
<td>The button arms/disarms one or more zones</td>
</tr>
<tr>
<td></td>
<td>Status Request</td>
<td>Execute status request</td>
</tr>
<tr>
<td></td>
<td>Not assigned</td>
<td></td>
</tr>
</tbody>
</table>

The defaults appear in bold.

By selecting Zones, another screen will appear that allows you to configure the selected action. Use the arrow keys and the OK key to save.

**Cyclical** applies to any zone set with “arming” type using any of the three possible methods. This does not apply when the “disarming” type is selected.

**Zones**: The following mode options can be selected for each zone: arming, disarming or None (not set).

<table>
<thead>
<tr>
<th>Display notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Away mode</td>
<td>Away mode arming</td>
</tr>
<tr>
<td>Home mode</td>
<td>Home mode arming</td>
</tr>
<tr>
<td>Notification mode</td>
<td>Notification mode arming</td>
</tr>
<tr>
<td>Disarmed</td>
<td>Disarming</td>
</tr>
<tr>
<td>Not set</td>
<td>No Action</td>
</tr>
</tbody>
</table>

The LEDs cannot be programmed and have the following meaning:
### Colour | LED Meaning
--- | ---
LED 2 | Red On if the system is armed in Away mode
LED 3 | Red On if the system is armed in Home mode
LED 4 | Off if key 4 = Status request, otherwise shows the status of the zones associated with key 4.
LED 5 | On Green if the system is disarmed

#### 12.4 Programming external sirens

The system can handle up to 4 sirens. To programme the sirens:

1. Access the Programming menu and log in as a level 3 user.
2. Select the “system devices” icon
3. Press 2 External sirens and the following video will appear:

![Video](No Device)


#### 12.4.1 Possible parameters

- **Supervision**: Allows you to select the frequency at which the central unit checks that the siren is working. (No/15/45). The parameter set is the time interval between one check and another.

- **Exclude**: Yes/No. Enables exclusion of the external siren

- **Anti-masking**: Yes/No. enables the anti-jamming protection to be excluded.

- **Tamper**: Yes/No. When set to YES, the Siren sounds in the event of central unit tampering (or jamming), otherwise this is ignored.

- **Technological Alarm**: Yes/No. When set to NO, the technological alarms will not sound, even if the parameters in the Alarms - Technological type field are set.
12.4.2 Zones Filters
Allows customised filters to be set for the siren, or the zone (or zones) where the siren is assigned, to for the conditions to be set under which the alarm siren sounds. The options are: All zones, or a sub-set of zones.

12.4.3 Alarms
Allows operating parameters such as type of sound, duration etc. of the alarm event siren to be modified.

(*) Alarms include: Away intrusion alarm, zone tampering alarm, Panic and System tampering alarms if the “system tampering” parameter is set to Yes.
Various parameters can be set for the various alarms. To configure the parameters of a certain type of alarm, use the arrow keys to move to the corresponding one, select it and press OK to save.

The following parameters can be modified in the window that opens:

<table>
<thead>
<tr>
<th>Alarm type / event</th>
<th>Sound</th>
<th>Frequency</th>
<th>Burst</th>
<th>LEDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1 alarms</td>
<td>Sweep / Bitonal/ None</td>
<td>High/Low</td>
<td>10s / 30 s / 3 m / 9 m **</td>
<td>YES / NO</td>
</tr>
<tr>
<td>Alarm 2 Technological</td>
<td>Sweep / Bitonal/ None</td>
<td>High/Low</td>
<td>10s / 30 s / 3 m / 9 m</td>
<td>YES / NO</td>
</tr>
<tr>
<td>External Activation</td>
<td>1 long beep / 3 short beeps / none</td>
<td>1 long flash / 3 short / NO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deactivation</td>
<td>1 long beep / 3 short beeps / none</td>
<td>1 long flash / 3 short / NO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(**) To ensure compliance with EN 50131 1 and EN 50131 3 standards, siren activation time must be greater than 90 seconds and less than 15 minutes (without prejudice to local or national regulations to the contrary).

Factory settings are indicated in **bold**. To change a parameter, use the arrow keys to move to it and press the OK key to confirm the selection.

**WARNING!**  
The low frequency Sweep, high frequency Bitonal and low frequency Bitonal type sounds do not comply with the EN 50131-1 standard.

12.4.4 Events
Allows the siren operating parameters to be modified for alarm system arming and disarming events, using a procedure similar to the previous Alarms.
12.5 **Repeater programming**

The system can handle up to 4 repeaters. To program the Repeater:

1. Enter the programming menu, authenticating yourself as a Level 3 user.
2. Select the "system devices" icon
3. Enter 3 for the Repeater and the following video will appear:

![No Device
New Device](image)


12.5.1 **Possible parameters**

- **Name.** Allows you to set a label.
- **Exclude:** Yes/No. Allows you to exclude the repeater.
- **Supervision.** It allows to select the frequency with which the control unit ensures that the repeater functions (No/15/45). The parameter that is set is the time interval between one control and the other.

12.6 **Telephone contact programming**

Function only available on central unit versions with GSM.

The system can handle up to 12 phone numbers. To programme a phone number:

1. Log in as an Installer and select Contacts.

![Contacts
1 Contact 1
2 Contact 2](image)

2. Select Add Contact
3. Assign a name to the telephone number for easier identification. The name can be up to 16 alphanumerical characters long.
   - Use the keypad to enter the telephone number. The maximum length is 16 digits.
   - Press the ok key: the following video will appear

   - Interruptible: if set to Yes, it means that if the voice call is successfully answered, the next number will not be called.
   - Audio Message: refers to the customised message to be added to the pre-defined voice message.
   - Events:
     - Select Events and, for each event, choose between
       - SMS Only
       - Voice Call Only
       - Voice Call + SMS
       - None (default except for the first 3 events)

   - The events that can be programmed are:

<table>
<thead>
<tr>
<th>Event</th>
<th>Type of sending</th>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion</td>
<td>VOICE / SMS</td>
<td>Alarm zone</td>
</tr>
<tr>
<td>Tampering</td>
<td>VOICE / SMS</td>
<td>Alarm zone</td>
</tr>
<tr>
<td>Central unit Tampering</td>
<td>VOICE / SMS</td>
<td></td>
</tr>
<tr>
<td>Burglar</td>
<td>VOICE / SMS</td>
<td></td>
</tr>
<tr>
<td>Assistance</td>
<td>VOICE / SMS</td>
<td></td>
</tr>
<tr>
<td>Fire</td>
<td>VOICE / SMS</td>
<td>Technological zone</td>
</tr>
<tr>
<td>Gas</td>
<td>VOICE / SMS</td>
<td>Technological zone</td>
</tr>
<tr>
<td>Flooding</td>
<td>VOICE / SMS</td>
<td></td>
</tr>
</tbody>
</table>
Technical support  VOICE / SMS
No 230V (*)  VOICE / SMS
230V return  VOICE / SMS
Technological  VOICE / SMS  Technological zone
Contact ON  VOICE / SMS  Technological zone
Periodic GSM inspections  VOICE (**)  Technological zone
Low Battery  VOICE / SMS
Central unit Battery  VOICE / SMS
Input  VOICE / SMS
Disarming  VOICE / SMS
Jamming  VOICE / SMS
Hardware Fault  VOICE / SMS
Radio Fault  VOICE / SMS

VOICE indicates a voice message, SMS indicates a text message.
(*) after 15 minutes of continuous power outage (maximum delayed allowed under EN50131-1 and EN50131-3 standards is 60 min.)
(**) Performed once a day (6pm). Removal of the event on all telephones invalidates the EN50136-2 standard.

WARNING!

SMS delivery time is determined by the telephone operator network service. As such, there is no guarantee that it will be delivered promptly.

12.6.1 Customised message

Select Record message. The list of messages will appear. Up to 9 different messages can be recorded, each 14 seconds long.

If programmed, the personal message can be played after the specific pre-recorded message that the central unit sends after an event.

The message should always indicate where the reported event occurred. E.g. a generic customised message might say ”in Mario Rossi’s house, via Roma 15, Milan”.

Select the number corresponding to the message that you wish to record. The recording window will open.
Press the OK key to start recording. After about 2 seconds, the scroll bar appears to indicate the progressive recording time.

Press the OK key again to interrupt recording.

To check the quality of the recording, use the Test System > Telephones menu to send the voice message.

12.6.2 Phone message sending sequence

SMSs are immediately sent to all configured numbers.

Voice calls follow these rules:

- The numbers programmed for voice calls are called in order.
- If the phone number is busy and there is no answer after 4 rings, the central unit cancels the call and moves on to the next phone number on the list.
- Once the first cycle of calls is complete (all of the active telephone numbers), the central unit will attempt to call back the numbers that did not respond. The central unit will perform 3 call cycles for the numbers that did not respond, before interrupting the message sending sequence.
- The voice message is repeated 3 times before the central unit terminates the call.

The message sent consists of a pre-recorded part specific to the event that triggered the voice call, and a variable part, which follows the first part. This may be a customised recorded message or, if no customised message has been recorded, the generic message "at the anti-theft system".

12.6.3 Receiving telephone calls from the central unit

When connecting by phone to the central unit, tones are always accepted, even if the number placing the call does not correspond to one of the 12 numbers on the list.

12.7 Home automation free@home

This section shows how to check the status and parameters of the free@home gateway. To configure free@home, refer to the specific manual for the system.

12.7.1 Version

1. To check the version
2. Access the Programming menu and log in as a level 3 user.
3. Select the "free@home pairing" icon
4. **Press 1 Version:** information on the free@home FW version will appear

```
Ver.: 0.1.249
```

### 12.7.2 Key

Perform points 1 and 2 from the previous paragraph and press 2 Key. A video opens showing 32 "digits" that uniquely identify the gateway on the central unit. These codes are sent just once, to the free@home system, as shown in the free@home programming manual: press OK to perform the operation.

### 12.7.3 GTW Reset

Allows the free@home gateway to be reset. The procedure lasts approximately 1 minute.

### 12.8 System test

The entire system is tested at the end of the installation and then regularly, at least once every 6 months, to ensure that all devices and functions are operating correctly. It is also possible to test a single subset, or a select number of subsets, to check that they are working properly. Partial testing is useful in the event of limited modifications to the system that only affect one device or one function.

When using the Test system function, the system may be inactive for 10 minutes, after which it returns to normal functioning. Each time a test is performed, e.g. a detector sends a response signal to the central unit, the countdown is reset to 10 minutes.

System testing occurs at a reduced level of 6 dB, as required under the EN50131-5-3 standard.

To test the alarm system:
1. Log in and go to the Test System screen.
2. Press OK.

```
System test
1 Sensors
2 External sirens
3 Contacts
```

Select the subsystem that you wish to test, and enter the corresponding number. If the subsystem does not contain devices, the selection will be ignored.

3. Based on the subsystem selected, new windows will open and it may be necessary to perform actions to activate the relevant devices.

#### Sensors

After selecting 1 Sensors as a subsystem, select the zone and activate the various detectors as appropriate, e.g. by moving past IR detectors, opening and closing doors and windows for magnetic contacts, spilling water for flooding detectors etc.
All of the possible detectors are listed for each zone, together with the signal strength upon receipt, indicated using three bars, as shown in the figure. By using the arrow keys to highlight the position of the detector and pressing the OK key, a new detailed window appears, displaying the following information for diagnostic purposes:

- Hexadecimal address of the detector.
- Signal level.
- Detector type.
- Detector status. The abbreviations mean:
  - M.AL detector in alarm mode
  - ON detector contact open
  - OFF detector contact close
  - MAN. anti-opening tampering
  - RIM. anti-removal tampering
  - BATT battery dead
  - GST general fault
  - SVIS supervision fault
  - ESCL detector excluded (corresponds to “detector isolated” as provided for in EN 50131 standard)
- Receipt date and time.

**External sirens**

After selecting Sirens as a subsystem, select the relevant device from the list and press the OK key.

In the new window in the Test line: select the type of sound and press OK: The selected siren will sound as selected, at a medium volume, for 10 seconds, and its LEDs will flash.

**Contacts**

When you select contacts, a list of all available telephone numbers will appear. The configured numbers are marked with the ► symbol.

Select the relevant telephone number and press the OK key. Select the desired test type (Voice Call or SMS) and press OK.
12.9 User management

This function can be performed by a level 3 user. They can create new users, change their PIN or delete existing users. For more information on the user log-in criteria and the associated privileges, see the First Start-Up and Authorisation Levels paragraphs.

When the menu is opened, a list of existing users will appear:

```
Select user
User 1
User 2
New user
Change PIN
```

This function can be performed by a level 3 user. They can create new users, change their PIN or delete existing users. For more information on the user log-in criteria and the associated privileges, see the First Start-Up and Authorisation Levels paragraphs.

To create a new user, select New User, press OK and select the level from the following window (2-User / 3-Installer / 4-Maintenance) and press OK.

- Label: Assign a name to the user (e.g. name, surname or both) for easier identification. The name can be up to 16 alphanumerical characters long. Characters are entered using the keypad. Move the cursor using the arrows above the character to delete a wrong character, and enter the correct character or space to delete it.
- PIN: enter a 5 digit password of your choice.
- Enter the PIN again to confirm consistency
- Zones: these are the zones that the relevant user can operate in. The default settings allow the new user to operate in all zones. Use the arrow keys to move to the relevant zones and add them.

Press the ok key to save the new user.

12.9.1 Change a user

To change a user:
- Log in and Enter User Management.
- Select the user. A window will appear; here you can modify their profile or the zones in which they can operate.
- Press OK to confirm.

12.9.2 Deleting a user

To delete a user:
- Log in and Enter User Management.
- Select a user and select Delete PIN from the next window.
- Press OK to confirm.
The PIN ID will appear (number 2 in the example figure) and you will be asked to confirm deletion. Use the arrow keys to confirm deletion (YES) or cancel it (NO). The chosen option will be highlighted in black. Press the OK key to confirm the selection.
13 MAINTENANCE

13.1 Power management

13.1.1 Battery

The central unit constantly monitors battery power. If it falls below:
- 6.9 Vc.c. the central unit will recharge it;
- 5.5 Vc.c. the central unit will report a “Dead battery” event and switch off all power. The RTC calendar will continue to update. When network power is restored, the central unit will restart the system;
- 1.5 Vc.c. the central unit will report a “Battery fault” event and the battery LED will come on.

13.1.2 Electrical power network

If there is no electrical power supply (230 Vc.a.):
- The central unit display backlight will switch off immediately (the display will switch back on if the keypad is used).
- Gateway Home Automation will be deactivated (intelligent shut-down, after checking that all nodes are without power).
- Management of the GSM module will be based on the battery charge level.
- After 15 minutes of continuous power outage, the central unit will report a network power outage event.
- The USB terminal will remain active.

When network power is restored, the GSM module will resume full functioning. After 15 minutes of uninterrupted network power, the central unit will report restoration of network power. The 15 minute time interval may be modified via programming.

13.2 Placing system in maintenance mode

To place the system in maintenance mode, simply activate the Test system function. To exit maintenance mode, simply exit the menu.

13.2.1 Replacing the central unit battery

To replace the central unit battery:
1. Place the system in maintenance mode.
2. Remove the central unit from its support frame and secure it in maintenance position.
3. Open the battery compartment and remove the dead battery.
4. Replace it with the new battery and close the battery compartment.
5. Remove the central unit from the maintenance position and secure it in its support frame.
6. Exit system in maintenance mode.

⚠️ WARNING! Dead batteries must be replaced with identical ones, which meet UL94HB flammability standards or above.
13.2.2 SIM Replacement
To replace the SIM, place the system in maintenance mode and check the installation sheet contained in the central unit packaging.

13.2.3 Replacing the detector battery
To replace the detector battery:
1. Put the system into service.
2. Open the detector, replace the used battery and close it again according to the instructions provided in the sensor manual.
3. Perform a system test on the detector to verify its proper operation.

13.2.4 Replacing the remote control battery
To replace the battery of a remote control
1. Open the remote control, replace the battery and close it again according to the instructions provided in the device manual.
2. Enter the System Test menu and press any key on the remote control.
3. In the rest window and check that the device is working properly.

13.2.5 Replacing the siren battery
1. Enter the System Test menu and perform the siren test procedure as described in the dedicated section.
2. From now on, you have 5 minutes to open the siren without causing it to sound tampered with.
3. Open the siren according to the instructions in the manual, replace the old battery and close it again.
4. Afterwards, perform a siren test procedure again to check that it is working properly.

13.2.6 Central unit reset
To restore factory settings for the central unit, deleting all programming operations and configurations performed:
5. Log in as a level 2 user, go to the installer screen and log in as a level 3 user: select the Maintenance icon.
6. Log in as a level 4 user. If no level 4 users exist, the central unit will ask you to create one.
7. When the screen appears, press 2 Factory reset.

After a factory reset, the central unit generates a new encryption key.

**WARNING!**
The central unit reset operation cannot be reversed, and involves a new, full configuration of the system.

13.2.7 Adding devices
To add new devices after the system has been activated, following the instructions for programming the various devices contained in the Programming chapter.
13.2.8 Deleting devices

To delete a device that is no longer needed:
1. Log in as a level 2 user, go to the installer screen and log in as a level 3 user: select Programming.
2. Select the zone and type of device that you wish to remove, and press OK.
3. A detailed window will appear, allowing you to check that you have selected the correct device.
4. If you have selected the correct device, scroll through all parameters, select "Remove" at the bottom of the list and press OK to delete.
5. The control system will ask you to confirm the deletion. Select YES to remove the device or NO to avoid removing it, and confirm your selection by pressing the OK key.
6. Press ESC to leave the menu.

13.2.9 Replacing devices

To replace a device, first delete the old device from the system and then add it again.

WARNING!
Deleting a device will result in all configuration parameters being lost. Before definitively deleting a device, make a note of its parameter values, listed in the detailed window.
Then, when you add the new device, use the noted values to programme the parameters.

13.2.10 Central unit firmware update

To update the central unit firmware:
2. Double click on SAS_Wx_FW_ABB-secure@home_VXXX.cab to extract the FILENAME.uc3
3. Save the FILENAME.uc3 on a USB key.

WARNING!
The USB key must be formatted as FAT 32
The FILENAME.uc3 must be the only file on the USB key

4. Log in as a level 2 user, go to the installer screen and log in as a level 3 user: select the Maintenance icon.
5. Log in as a level 4 user. If no level 4 users exist, the central unit will ask you to create one.
6. When a new screen appears, press 1 Update FW from USB
7. Remove the central unit from its support frame.
8. Put the USB key with the new firmware in the USB port at the back of the central unit and press the OK key.
9. The central unit will load the new firmware and a message will appear at the end, stating whether the operation was successful.
10. Remove the USB key and secure the central unit in the support frame.
11. Exit system in maintenance mode.
The update file comes from ABB with a Digital signature. The Digital Signatures Ensures that firmware came from ABB and protect the firmware from alteration after publication. To verify that the Signature is valid follow these steps:

1. Click with the right mouse button on the received .cab file.
2. Choose Properties and click the Digital Signatures tab.
3. Choose ABB Asea Brown Boveri and click the Details button.
4. A new windows, like the following, opens. In the top line you can see that the certificate is valid.

## 14 PROBLEM SOLVING

<table>
<thead>
<tr>
<th>Problem</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon ![ ]</td>
<td>No SIM Card</td>
<td>Put in a SIM Card</td>
</tr>
<tr>
<td></td>
<td>SIM Card present, but not making contact.</td>
<td>Put the SIM Card in properly, after cleaning its contact points.</td>
</tr>
<tr>
<td></td>
<td>SIM Card Credit has run out.</td>
<td>Top up the SIM Card, if it can be topped up.</td>
</tr>
<tr>
<td></td>
<td>GSM Network not detected.</td>
<td>Check that there is network coverage.</td>
</tr>
<tr>
<td>Flashing battery icon</td>
<td>Battery is not connected.</td>
<td>Connect the battery or check that it is connected.</td>
</tr>
<tr>
<td>![ ]</td>
<td>Battery dead</td>
<td>Check that there is network power and wait for the battery to recharge if the report persists, replace the battery.</td>
</tr>
<tr>
<td>![ LED on ]</td>
<td>Battery faulty</td>
<td>Replace the battery</td>
</tr>
<tr>
<td>![ LED on ]</td>
<td>Radio channel jamming</td>
<td>Check whether an electronic device or electromagnetic source of disturbance is blocking radio communication between the central unit and the devices.</td>
</tr>
<tr>
<td>![ LED on ]</td>
<td>There are alarm reports that have not yet been viewed.</td>
<td>View reports</td>
</tr>
<tr>
<td>LED on</td>
<td>There are mandatory notifications that have not yet been viewed.</td>
<td>View notifications</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Forgotten PIN</td>
<td>Delete the user and create a new user</td>
<td></td>
</tr>
<tr>
<td>When the system is activated, Force Block must be executed.</td>
<td>Doors or windows are open.</td>
<td>Check that all doors and windows are closed</td>
</tr>
<tr>
<td></td>
<td>The sensor or siren battery level is low.</td>
<td>Replace batteries.</td>
</tr>
<tr>
<td></td>
<td>Tampering has occurred.</td>
<td>Check where the tampering occurred and, if possible, remedy the situation</td>
</tr>
<tr>
<td></td>
<td>The phone network is not working properly.</td>
<td>Check that the SIM Card has credit and that there is a phone network signal</td>
</tr>
</tbody>
</table>
# CENTRAL UNIT TECHNICAL SPECIFICATIONS

<table>
<thead>
<tr>
<th>MODEL</th>
<th>Busch-/ABB-secure@home central unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIELD OF APPLICATION</td>
<td>Security, anti-intrusion and Home Automation</td>
</tr>
<tr>
<td>PERFORMANCE LEVEL</td>
<td>Security level</td>
</tr>
<tr>
<td></td>
<td>2 - Models with GSM</td>
</tr>
<tr>
<td></td>
<td>1 - Models with GSM</td>
</tr>
<tr>
<td></td>
<td>Environmental category</td>
</tr>
<tr>
<td></td>
<td>Notification requirements</td>
</tr>
<tr>
<td>COMMUNICATION TECHNOLOGY</td>
<td>Between radio devices</td>
</tr>
<tr>
<td></td>
<td>FM 868.3 MHz bidirectional transmission</td>
</tr>
<tr>
<td></td>
<td>300 m free field range</td>
</tr>
<tr>
<td></td>
<td>Telephone network (just certain models)</td>
</tr>
<tr>
<td></td>
<td>GSM Dual band module (900 MHz / 1800 MHz)</td>
</tr>
<tr>
<td></td>
<td>Max transmission power 2 W</td>
</tr>
<tr>
<td></td>
<td>Internal antenna</td>
</tr>
<tr>
<td></td>
<td>With wired devices</td>
</tr>
<tr>
<td></td>
<td>RS485 interface, 3-wire terminal box</td>
</tr>
<tr>
<td></td>
<td>Home Automation</td>
</tr>
<tr>
<td></td>
<td>ABB-free@home on 2 wire bus</td>
</tr>
<tr>
<td></td>
<td>With PC</td>
</tr>
<tr>
<td></td>
<td>Type A USB port</td>
</tr>
<tr>
<td></td>
<td>Type B USB port</td>
</tr>
<tr>
<td></td>
<td>Alarm Transmission System (ATS)</td>
</tr>
<tr>
<td></td>
<td>SP2 Category (EN50136-2) ack: pass-through</td>
</tr>
<tr>
<td>ELECTRICAL SPECIFICATIONS</td>
<td>Generator</td>
</tr>
<tr>
<td></td>
<td>230 Vc.a. ± 10% 0/60 Hz frequency</td>
</tr>
<tr>
<td></td>
<td>Type A Feeder</td>
</tr>
<tr>
<td></td>
<td>Current</td>
</tr>
<tr>
<td></td>
<td>Stand by: 45 mA – In alarm mode 85 mA</td>
</tr>
<tr>
<td></td>
<td>Buffer battery</td>
</tr>
<tr>
<td></td>
<td>NiMh, 6 V, 1600 mAh rechargeable battery</td>
</tr>
<tr>
<td></td>
<td>Ensures compliance with the EN 50131-1 standard par. 9</td>
</tr>
<tr>
<td>PHYSICAL SPECIFICATIONS</td>
<td>Protection class</td>
</tr>
<tr>
<td></td>
<td>IP20</td>
</tr>
<tr>
<td></td>
<td>Dimensions (L x H x P)</td>
</tr>
<tr>
<td></td>
<td>272 x 187 x 48 mm</td>
</tr>
<tr>
<td></td>
<td>Weight</td>
</tr>
<tr>
<td></td>
<td>0.85 kg</td>
</tr>
<tr>
<td>CONDITIONS FOR USE</td>
<td>Environmental category</td>
</tr>
<tr>
<td></td>
<td>I (internal)</td>
</tr>
<tr>
<td></td>
<td>Operating temperature</td>
</tr>
<tr>
<td></td>
<td>-5...+45 °C (*)</td>
</tr>
<tr>
<td></td>
<td>Relative humidity</td>
</tr>
<tr>
<td></td>
<td>Average 75% non-condensing, peak 90%</td>
</tr>
<tr>
<td></td>
<td>Installation</td>
</tr>
<tr>
<td></td>
<td>Wall-mounted</td>
</tr>
<tr>
<td>SPECIFIC FUNCTIONALITY</td>
<td>CPU</td>
</tr>
<tr>
<td></td>
<td>Microprocessor</td>
</tr>
<tr>
<td></td>
<td>64 kB RAM and 128 kB Flash memory</td>
</tr>
<tr>
<td></td>
<td>Graphic display</td>
</tr>
<tr>
<td></td>
<td>Backlit LCD 128 x 64 pixel</td>
</tr>
<tr>
<td></td>
<td>Keypad</td>
</tr>
<tr>
<td></td>
<td>Capacitive with 17 keys</td>
</tr>
<tr>
<td></td>
<td>Audible warning device</td>
</tr>
<tr>
<td></td>
<td>Self-powered piezoelectric siren for internal use</td>
</tr>
<tr>
<td></td>
<td>85 dB power at 1 m</td>
</tr>
</tbody>
</table>
**16 CYBER SECURITY DISCLAIMER**

This product is designed to be connected to and to communicate information and data via a network interface. It is customer’s sole responsibility to provide and continuously ensure a secure connection between the product and customer network or any other network (as the case may be). Customer shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

**16.1 Network Manager**

Network Manager products are designed to be connected and to communicate information and data via a network interface, which should be connected to a secure network. It is your sole responsibility to provide and continuously ensure a secure connection between the product and your network or any other network (as the case may be) and to establish and maintain appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, etc.) to protect the Network Manager product, the network, its system and interfaces against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB and its affiliates are not liable for damages and/or losses related to such security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

Although ABB provides functionality testing on the products and updates that we release, you should institute your own testing program for any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third party software updates or patches, hardware change out, etc.) to ensure that the security measures that you have implemented have not been compromised and system functionality in your environment is as expected.