XT-iP GPRS Control Panel

Description

The XT-iP is a fully wireless alarm system. It can be powered by standalone batteries or connected to a power supply. This panel is intended mainly for residential and commercial markets.

With the Motion Viewers™ and Videofied® range of products, the XT-IP panel provides video verification in case of intrusion.

The XT-iP panel has three wired programmable inputs and two wired programmable outputs. Thanks to the Mapping feature, the programmable inputs can be configured to trigger a video.

For specific applications, the XT-iP alarm system offers the possibility to increase its Radio and/or GPRS performances through the connection of externally wired antennas.

Technology

The XT-iP alarm panel, like all Videofied devices, uses the S2View® patented technology. Which is an interactive wireless and AES encrypted technology ensuring signal integrity and optimal security.

The reliability of the signal is guaranteed thanks to the two-way radio frequency transmissions with all the peripherals of the Videofied® product line.

The integrated antennas allow the system to be totally wireless, thus preventing from the system beeing inelegant and cumbersome, and eliminating the installation problems.

The jamming detection feature identifies any intentional jamming from a third party. On the other hand, the supervision feature consists of transmitting signals between every device of the system and the alarm panel XT-iP. Through the supervision, the detectors transmit every 8 minutes a presence signal.

The entire RSI VIDEO TECHNOLOGIES team wishes you a successful installation.
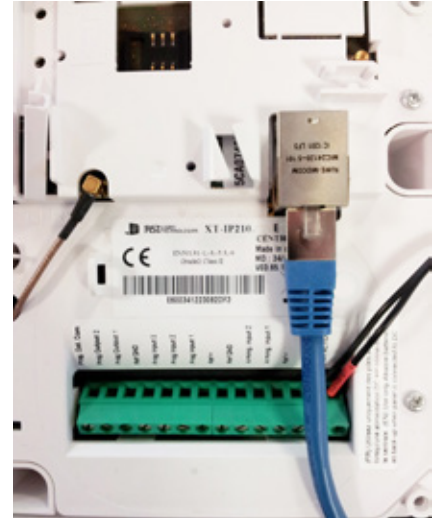
1.1 RJ45 cable connection

Connect the RJ45 cable to the Ethernet port.

When the panel attempts a transmission via Ethernet, a red LED on the connector will flash. This will allow the installer to check whether the panel is connected to a valid network.

Do not touch the RJ45 cable when the panel is powered.

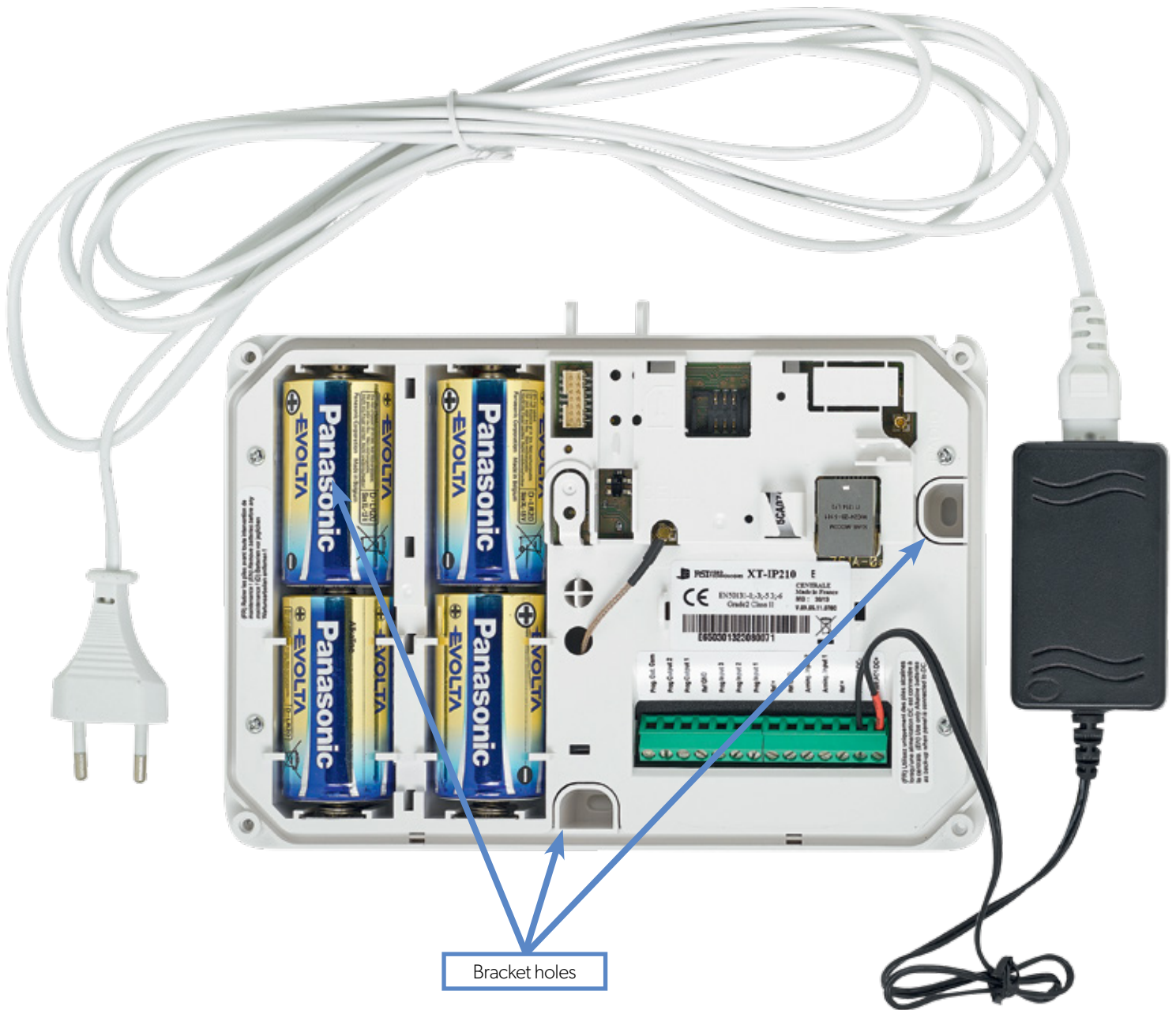## 1.2 SIM Card Installation

Before removing the front cover from its box, put the SIM card on the plastic base (take care to respect the right orientation).

DO NOT insert or remove the SIM card while the panel is powered.

1.3 Panel mounting

Bracket holes
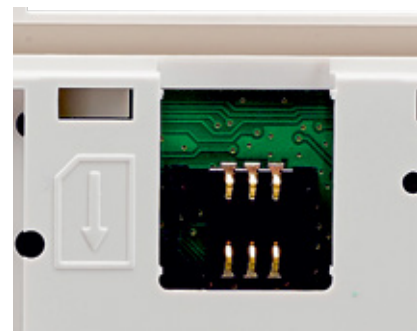
Fix the back casing on the wall using the three mounting holes illustrated above.

Mounting the panel is not required for programming.

1.4 Powering and initialization

• Connect the mains power supply and insert the 4 alkaline backup batteries.
• Press and hold the PROGRAMMING BUTTON for 10 seconds, until the indicator LED blinks twice.
• The panel is now reset, a CMA, XMA or XMB has to be enrolled to configure the panel.

| Alkaline batteries | Programming button | Ethernet Connector | Mains Power Supply |
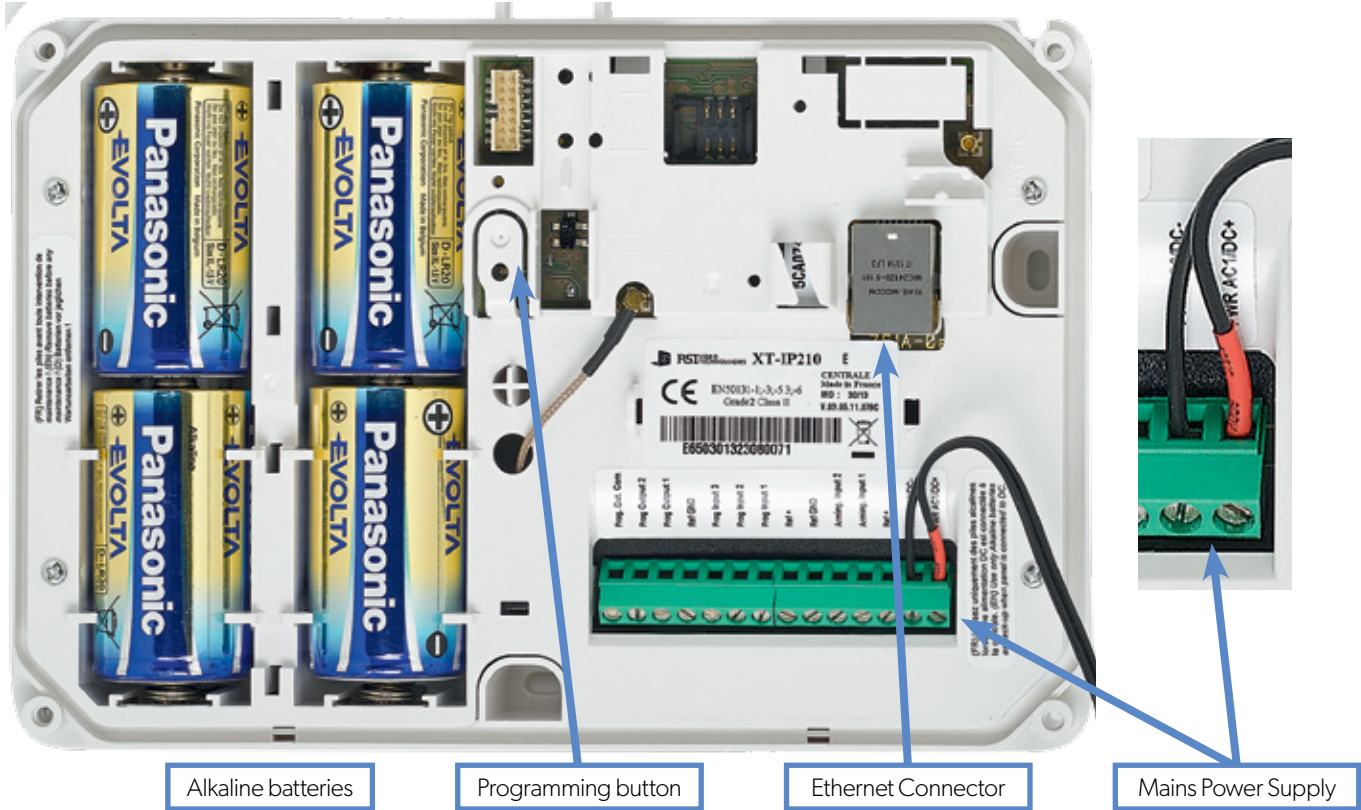
> Providing that **Ethernet connectivity is not used**, the XT-iP panel can be powered by 4 LSH20 Lithium, instead of mains power supply with alkaline backup batteries.

1.5 Pairing the remote keypad

• Press briefly the XT-iP programming button and release for the enrollment of a programming keypad. The indicator LED will blink once.

• Insert all 3 **LS14500 Lithium batteries** into the keypad.

• Do not mount the keypad. It will displays one of the following screens:

RSI (c) 2013
videofied.com   **or**   <=========XX=========>

• **Press on both** CLR and ESC NO **keys at the same time** and release. The indicator LED on the keypad will blink rapidly. Wait for the keypad to pair.

• **If the keypad doesn't pair up with the panel** and shows «XX», it certainly means that it is still paired to another system and needs to be reset. Take the batteries out, and press repeatedly on the keypad tamper switch for 30 sec to 1 minute. Then proceed to the above steps.

The XT-iP panel can be used as standard standalone alarm system but it can also be connected to an existing alarm system capable of latching a 9-12Vcc* voltage used for its arming/disarming.

2.1 Standalone Mode
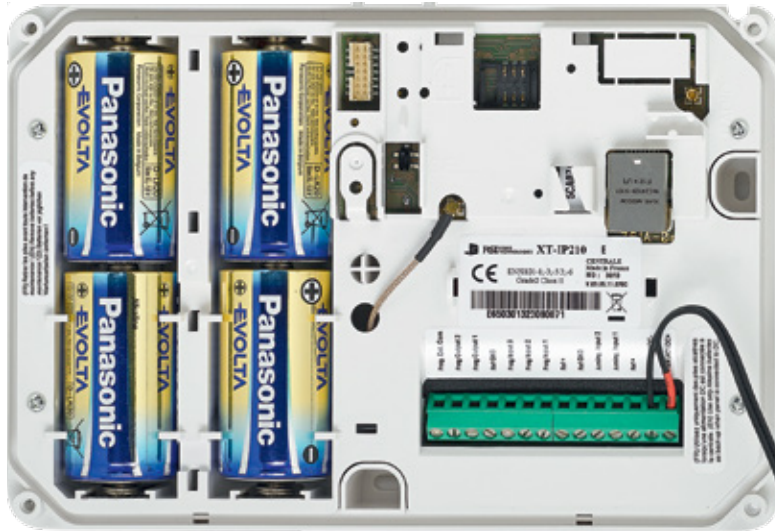
In this functioning mode, the XT-iP panel works as a standard hybrid alarm system with 25 wireless peripherals and 3 programmable inputs. It is a totally standalone alarm system.

2.2 XTENDER Mode (From the host)

Existing Host panel

Arming O/P 2
Arming O/P 1
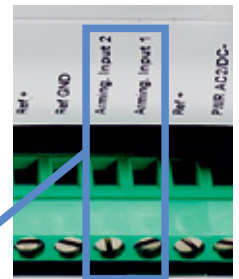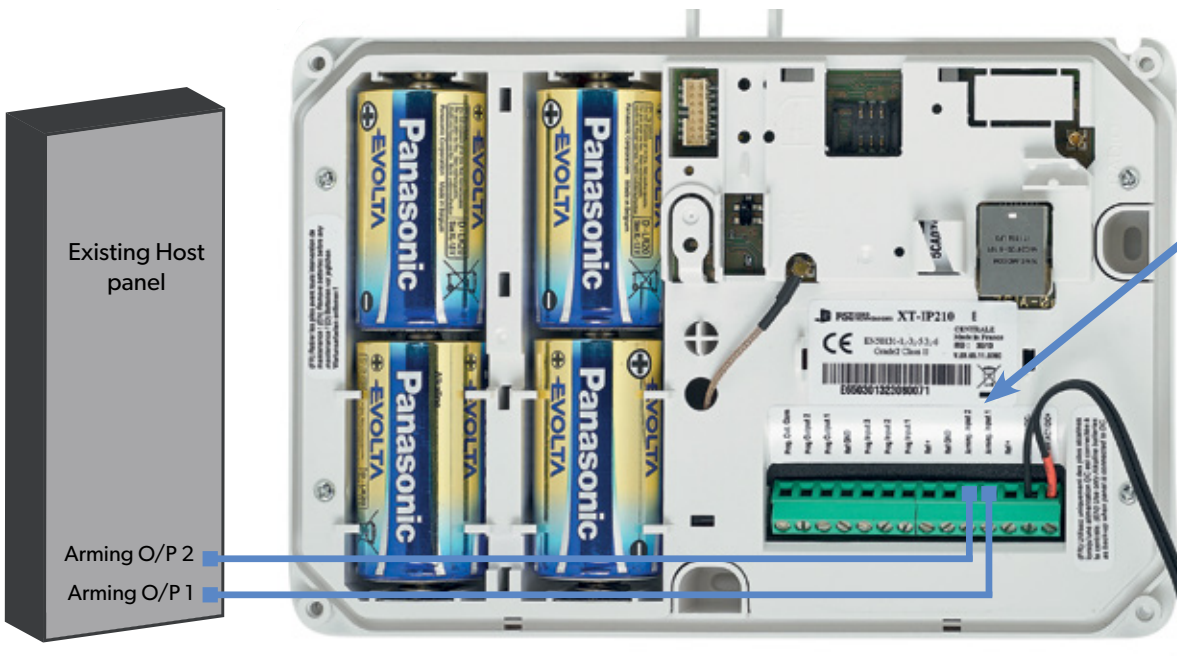
When the XT-iP panel is used in XTENDER mode, the system will only be able to arm and disarm by latching 9-12Vcc to its arming inputs Arming Input 1 and/or Arming Input 2.

When the voltage switches to 0V, the panel will disarm automatically.

On a programmed panel, you can choose between standalone and XTENDER modes from the menu :

CONFIGURATION (LVL 4) > **GENERAL PARAMETERS** > **XTENDER**

When using an XT-iP in XTENDER mode, the panel has to be powered by the mains power supply.

Keypad Display

Actions and comments

KEYPAD 1
RECORDED

OK or YES

< - LANGUAGE : - >
ENGLISH (UK)

↶   ↷   for language selection
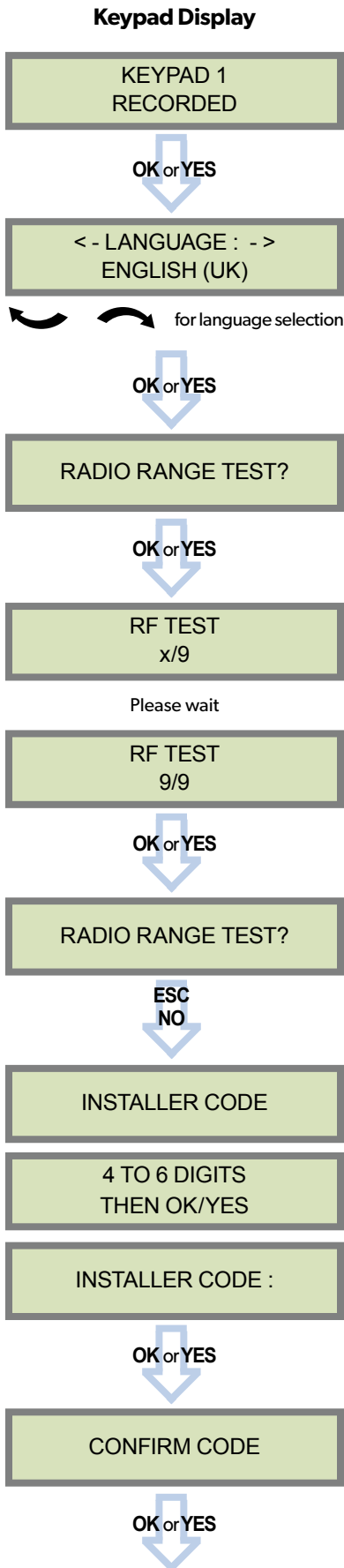
The system can also be programmed in : french, italian, german, dutch, spanish, swedish, portuguese, danish, czech and polish.

The language can be changed at any time once the panel is programmed in the MAINTENANCE menu.

OK or YES

RADIO RANGE TEST?

OK or YES

RF TEST
x/9

Please wait

RF TEST
9/9

OK or YES

RADIO RANGE TEST?

ESC
NO

INSTALLER CODE

4 TO 6 DIGITS
THEN OK/YES

INSTALLER CODE :

OK or YES

CONFIRM CODE

OK or YES

The Radio Range test must be run during the device learning process in order to ensure proper pairing with the control panel. This test measures the strength of communication between the device and the control panel. The keypad will display a real time radio range value on a scale of 9.

To receive the most accurate results you must run the radio range test for at least 30 seconds.

Result must be 8 out of 9 or better for reliable transmission.

Using the Alphanumeric Keypad, enter the Installer Code of your choice.

The Installer Code will be used for all future maintenance and configuration.

This code is important to keep track of.

There is no back door or Default codes to the system

Please refer to the restriction rules for codes (Chapter 4.4). Some codes are already used by default and therefore cannot be used.

Keypad display

Actions and comments

CODE NAME :

OK or YES

ACCESS 1
REGISTERED

Please wait

ADJUSTING DATE
AND TIME

DATE (YEAR):
12/ /

To set the year

OK or YES

DATE (MONTH):
13/01/

To set the month

OK or YES

You may proceed in the same way for:
Day, **Hour** and **Minutes.**

13/10/14 10:47
ENTRY COMPLETE !

CONNECTED TO
MONITOR. STATION?

OK or YES

ESC
NO

ACCOUNT NUMBER :

ACCOUNT NUMBER :
567001

OK or YES

You may name the installer code using the Alphanumeric Keypad.

If using automatic setting (called installer default list), enter the name of the list.

Warning : If the wrong installers list name is used it cannot be set later, the system must be defaulted.

Leaving the name blank by pressing **ESC NO**, it will be named 'ACCESS 1' by default.

Use the Alphanumeric Keypad to enter in a 4-8 digit account number provided by the Central Station.

Keypad display

Actions and comments
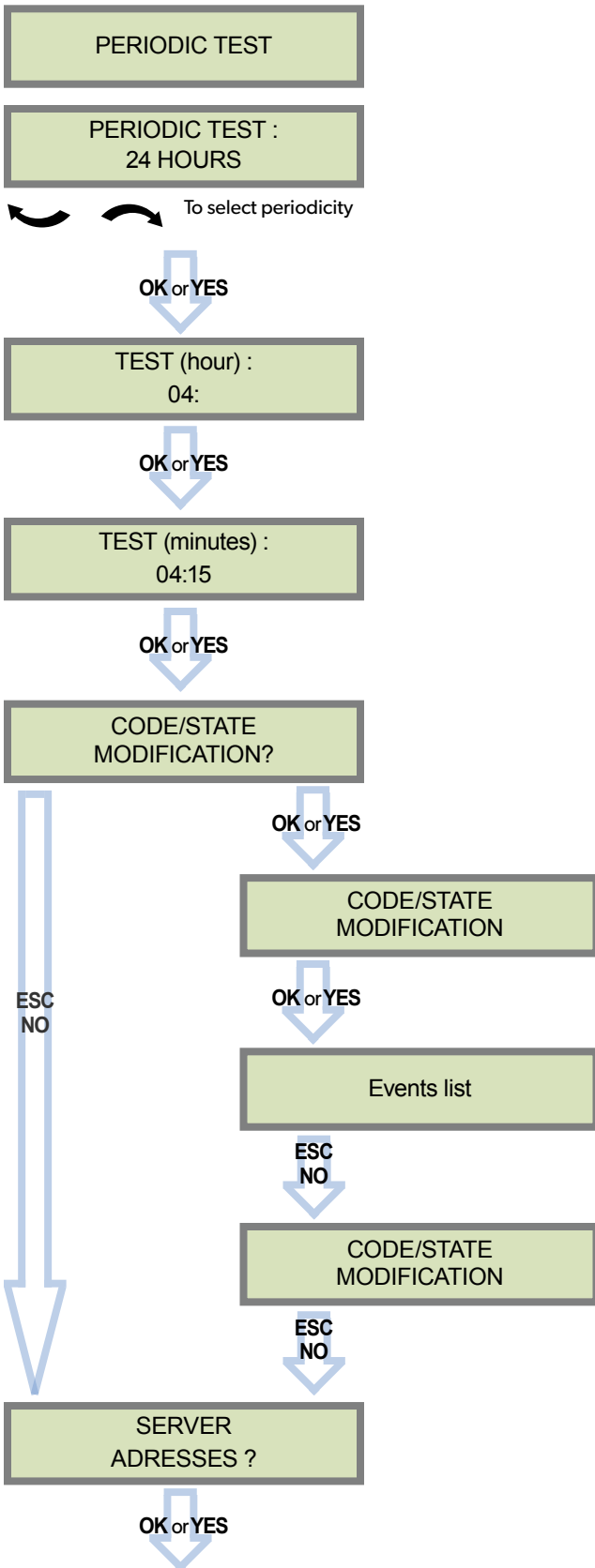
PERIODIC TEST

Test Periodicity: 1 hour, 12 hours, 24 hours, 48 hours, 7 days or no tests.

PERIODIC TEST :
24 HOURS

We suggest a 24 hours periodic test call.

To select periodicity

OK or **YES**

TEST (hour) :
04:

OK or **YES**

TEST (minutes) :
04:15

OK or **YES**

CODE/STATE
MODIFICATION?

OK or **YES**

CODE/STATE
MODIFICATION

The CODE/STATE MODIF. menu is to configure the transmitted events to the monitoring station, use the arrow keys to toggle between events and **OK or YES** to modify.

OK or **YES**

ALARM: event transmitted upon occurrence.

Events list

ALARM/END: event is transmitted on occurrence and on event restoral.

ESC
NO

NOT TRANSMITTED: event is not transmitted, however it will appear on the keypad.

ESC
NO

CODE/STATE
MODIFICATION

Please liaise with your Monitoring Station to ensure that the requested events to transmit are correctly set.

ESC
NO

SERVER
ADRESSES ?

OK or **YES**

IP1 ADDRESS
0.0.0.0

DOMAIN NAME 1

PORT 1
888

ESC
NO

SERVER
ADRESSES ?

ESC
NO

STRATEGY:
ETH+2G3G

OK or YES

2G3G
PARAMETERS ?

OK or YES

APN CODE
internet-entrepr

USER NAME
orange

PASSWORD
orange

ESC
NO

2G3G
PARAMETERS ?

ESC
NO

2G3G LEVEL ?

OK or YES

TEST IN PROGRESS
END = OK/YES

2G3G LEVEL
5/5

OK or YES

2G3G LEVEL ?

ESC
NO

The **IP1 address**, **Domain name 1** and/or **Port 1** are provided by the monitoring station. *Leave Port details at 888 unless otherwise instructed.*

Press **OK or YES** to enter/modify the parameter then **OK or YES** for validation.

WARNING : You will use either an **IP adress** or a **Domain name** but **not both**, leave the **Domain name** blank if an **IP adress** has already been entered.

Press on the right arrow to configure IP/Domain name 2 and PORT2 (for the back-up server), and IP/Domain name TMT and PORT TMT (to configure remote maintenance server).

How the alarms and videos are transmitted to the monitoring station ?
ETH+2G3G : Ethernet transmission with GPRS backup.
2G3G : GPRS transmission only (if the Ethernet connection is not used).
ETH : Ethernet transmission only (only if GPRS is not used).
Warning : the transmission mode "Ethernet only" is not recommended.

The **APN Code** (Access Point Name), **User Name** and **Password** are supplied by the mobile operator. Please make sure you have entered the code exactly as indicated by your local SIM card operator.

Press **OK or YES** to enter/modify the parameter then **OK or YES** for validation.

Note: When entering your SIM card settings, both APN codes, username and password fields are case sensitive! It makes a difference between UPPER and lower case letters.
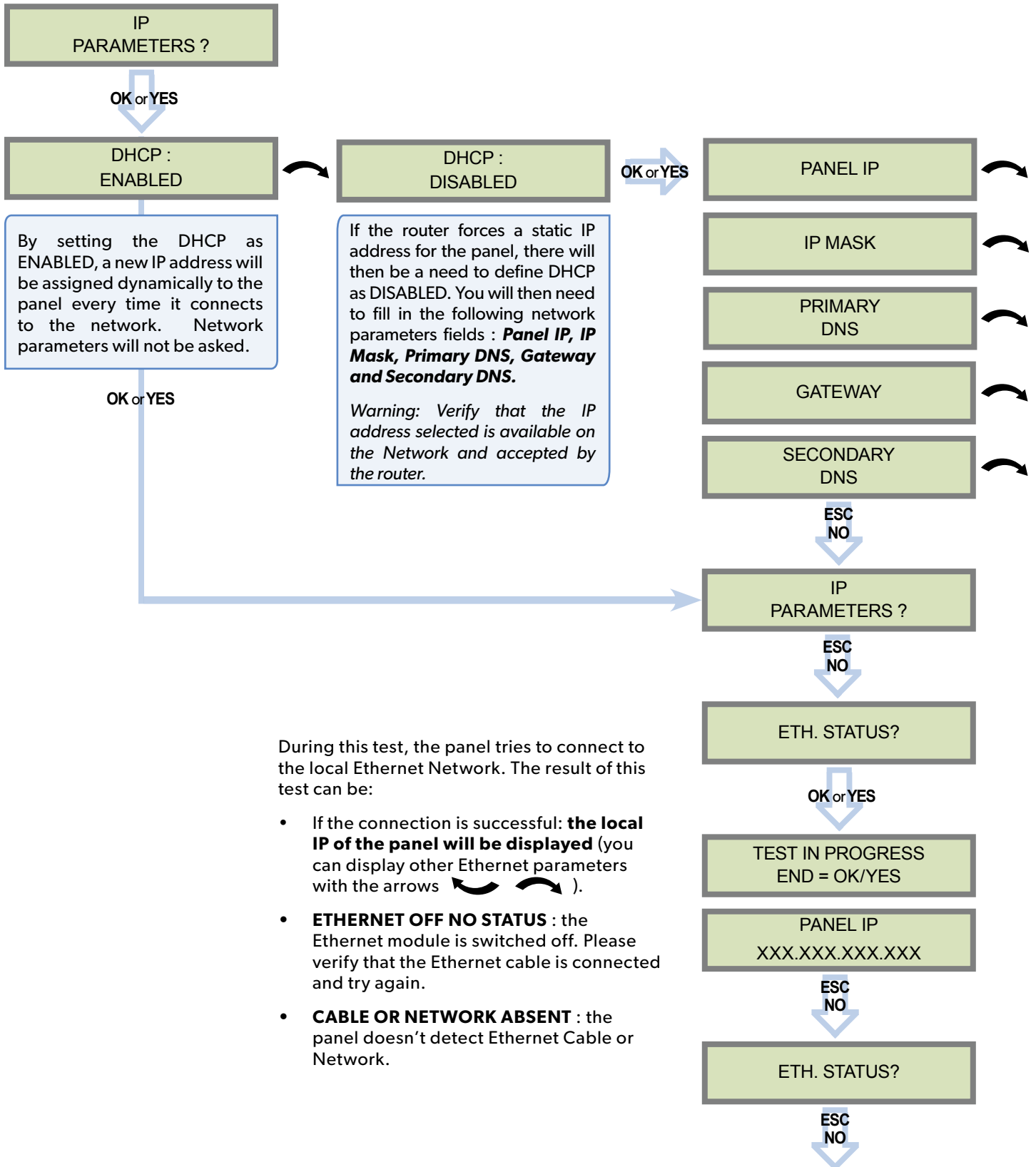
To switch between UPPER and lower case, use the M/m key from CMA keypad or hold a digit key (0-9) for XMA/XMB.

Once the 2G3G test completed, the keypad will display one of the following results :

- A level between 0/5 and 5/5.

- A GPRS Error code (please see Chapter 7 : 2G3G errors codes and contact your technical support).

If the screens shuts down, press any key to light it up except **OK or YES**, **ESC NO** or **CLR**.

The 2G3G level test can last several minutes. Do not interrupt the test or remove the SIM card during the test.

IMPORTANT : Videofied will require a 3/5 grade or better for reliable transmission of Video alarms.

ETHERNET parameters configuration

IP
PARAMETERS ?

OK or **YES**

DHCP :
ENABLED

DHCP :
DISABLED

OK or **YES**

PANEL IP

IP MASK

By setting the DHCP as ENABLED, a new IP address will be assigned dynamically to the panel every time it connects to the network.   Network parameters will not be asked.

If the router forces a static IP address for the panel, there will then be a need to define DHCP as DISABLED. You will then need to fill in the following network parameters fields : *Panel IP, IP Mask, Primary DNS, Gateway and Secondary DNS.*

Warning: Verify that the IP address selected is available on the Network and accepted by the router.

PRIMARY
DNS

GATEWAY

OK or **YES**

SECONDARY
DNS

**ESC
NO**

IP
PARAMETERS ?

**ESC
NO**

During this test, the panel tries to connect to the local Ethernet Network. The result of this test can be:

ETH. STATUS?

OK or **YES**

- If the connection is successful: **the local IP of the panel will be displayed** (you can display other Ethernet parameters with the arrows   ).

TEST IN PROGRESS
END = OK/YES

- **ETHERNET OFF NO STATUS** : the Ethernet module is switched off. Please verify that the Ethernet cable is connected and try again.

PANEL IP
XXX.XXX.XXX.XXX

**ESC
NO**

- **CABLE OR NETWORK ABSENT** : the panel doesn't detect Ethernet Cable or Network.

ETH. STATUS?

**ESC
NO**

COMPATIBILITY
EN 50131 NORMS ?

For full compatibility with EN50131, press **OK or YES**.

Otherwise, press **ESC NO.**

OK or **YES**   **ESC NO**

AREAS CONFIGURATION

Press **ESC NO** to default the area names.

Enter the name of the area 1 and **OK or YES**.

Repeat the procedure for areas 2,3 and 4.

For further details, please refer to chapter 4.3.

OK or **YES**

AREA 1 NAME :

Your choice will depend on how you are arming the system :

Standalone : Will make the XT-iP a completely independant system controlled by arming and disarming using Videofied peripheral devices(keyfobs, keypads, badge,readers).

OK or **YES**

ARMING PROFILE :
STANDALONE

ARMING PROFILE :
FROM THE HOST

From the host : Will make the XT-iP panel a piggyback/xtender system that will only arm and disarm off the latching of 9-12V on the arming inputs 1 & 2.

OK or **YES**

Please go to page 14 if you chose
FROM THE HOST

EXIT DELAY :
45 sec

Other values are available: 2 min, 1 min, 45 sec.

For the selection

OK or **YES**

ENTRY DELAY :
15 sec

Other values are available: 2 minutes, 1 minutes, 45 seconds, 30 seconds or 15 seconds.

For the selection

Please go to page 15 if you chose
STANDALONE

XTENDER mode configuration

```
ARMING PROFILE :
FROM THE HOST
```

OK or YES

```
ARMING MODE
```

```
MODE :          MODE :
SLOW            FAST
```

OK or YES

```
ENTRY DELAY
```

```
VALUE (0-255) :
(000) : _
```

OK or YES

```
TRANSMISSION DELAY
```

```
VALUE (0-600) :
(000) : _
```

OK or YES

```
ARMING CONFIRMATION
```

```
VALUE (0-240) :
(0) : _
```
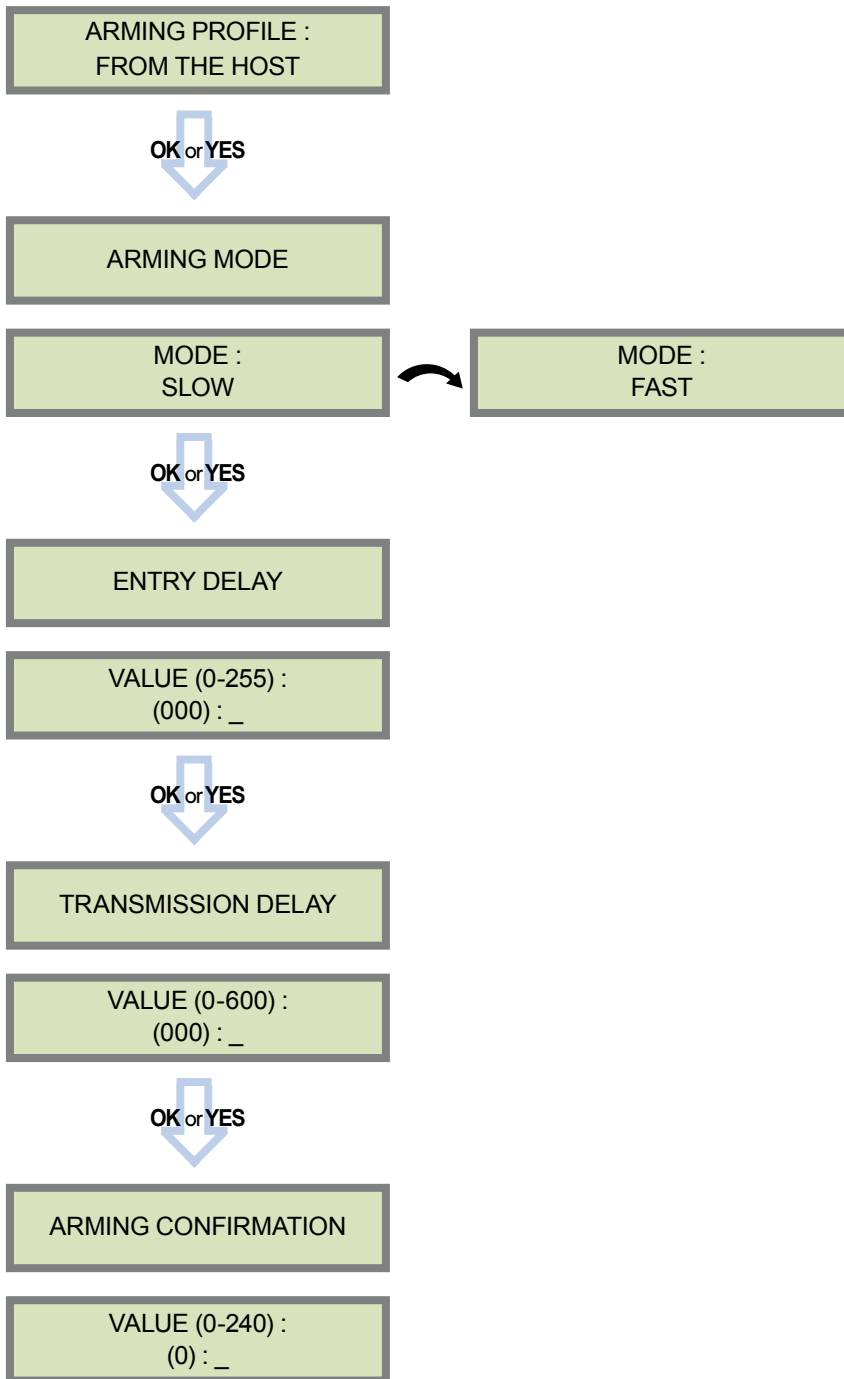
MODE SLOW : : The panel will arm each device one at a time saving battery life. We recommend this mode.

MODE FAST : The panel will arm all devices at the same time. This mode increases significantly the battery consumption.

OK or YES to choose the parameter.

Enter the value for your Entry Delay up to 255 seconds and press **OK or YES.**

Note : In From the Host mode, the entry/exit delay are dealt by the master system.

The transmission delay value sets the delay between the detection of an event and its transmission to the monitoring center.

Except when specifically required, please enter 0.

Enter the value you would like for the Transmission Delay and press **OK or YES.**

Arming Confirmation is the number of seconds the system will wait to arm after voltage is latched on the arming input. This feature can be used as an exit delay, we suggest you to enter the same value as your master system exit delay.

Enter the value you would like for the Arming Confirmation and press **OK or YES.**

For further information about the programmable inputs and outputs, please consult the following application notes available on our support website:
240-XT - APP NOTE - XTENDER CONFIGURATION MODE

RECORDING
DEVICES

PRESS PROGRAM
BUTTON OF DEVICE

ENTERING A NEW DEVICE ?

ESC
NO

BADGE ENTERED ?

OK or **YES**

ESC
NO

RECORDING A
NEW BADGE ?

ESC
NO

END OF
CONFIGURATION
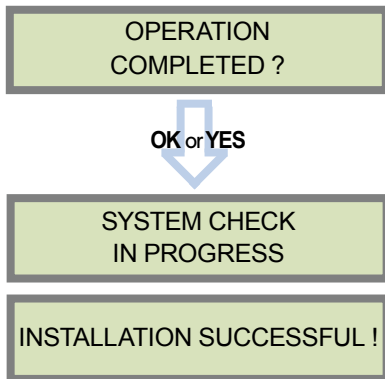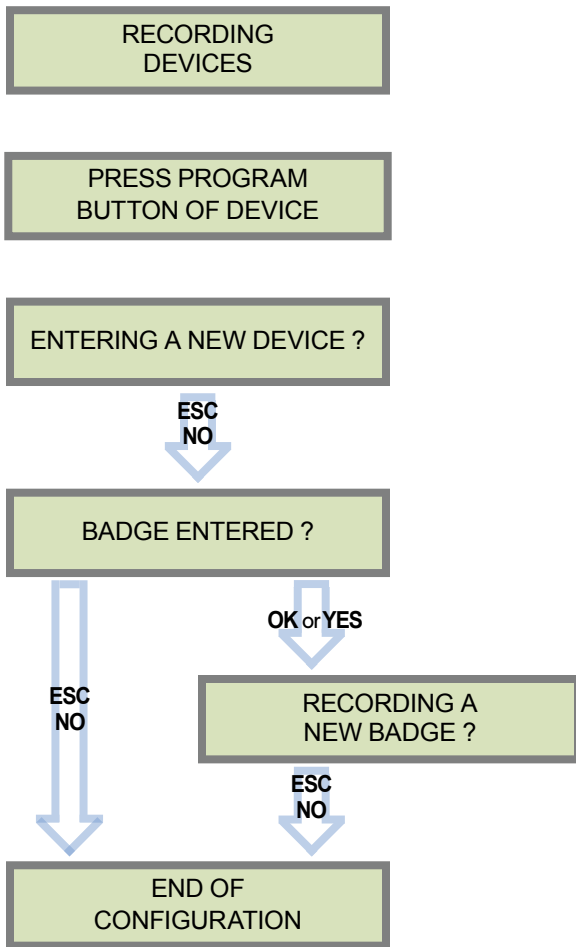
Each device has a unique programming button or a specific manipulation. Please refer to the Installation Sheet for the device you would like to program.

Please check the radio level of each device on its final location. The result must be 8 out of 9 as a minimum (Please refer to the Radio Range section, page 8 for further details).

Each system can embrace a maximum of 25 devices, **programming keypad included.**

Press **OK or YES** to enter a new device or **ESC NO** to move to the next step.

After initial programming has been completed, the system cannot be armed or disarmed until a user code or badge is entered (the installer code cannot arm or disarm the system).

Press **OK or YES** to register one or more badges. **ESC NO** if you're not using any badges.

If you wish to use an user code, please skip this step and when initial programming is completed go to the BADGES/ACCESS CODES menu (please refer to chapter 4.4 for further details).

Badges and codes are limited to 19 for user (level 2 or 3) + 1 installer code.

OPERATION
COMPLETED ?

OK or **YES**

SYSTEM CHECK
IN PROGRESS

INSTALLATION SUCCESSFUL !

Before completing programming make sure that all tampers are depressed by verifying that each device is closed and the indicator LEDs are off.

After initial programming has been completed, make use of the menu overview document (available on our technical support website), to see full programming options.

4.1 Get to Access level 4

Tue 29/10   11:23 DISARMED   LVL:1

→

ACCESS LEVEL 1

OK or **YES** ⇨

ACCESS LEVEL LEVEL : 1

→ → →

ACCESS LEVEL LEVEL : 4

OK or **YES** ⇩

BADGE OR CODE

OK or **YES**
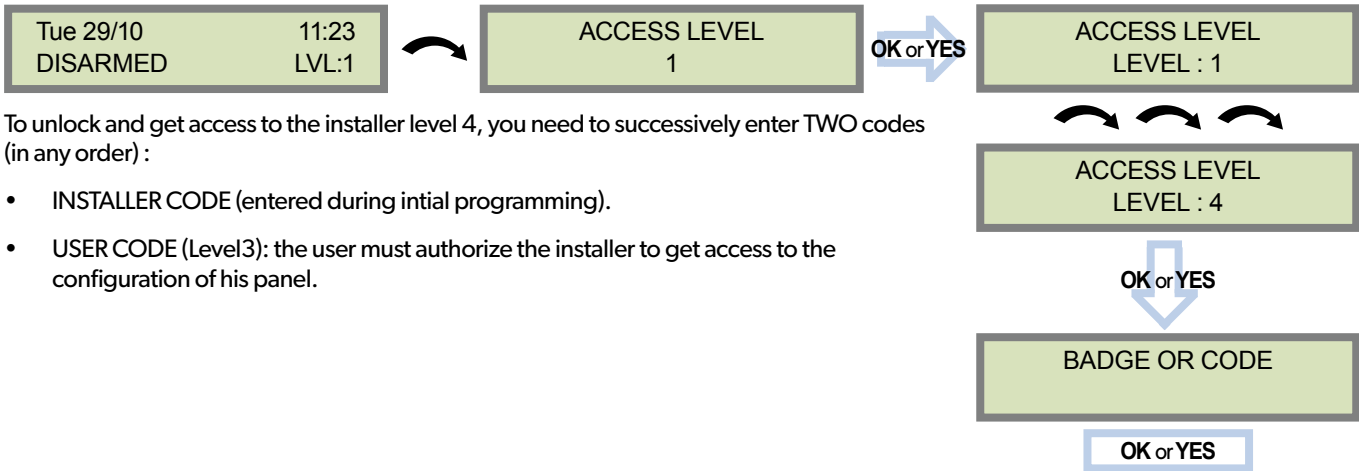
To unlock and get access to the installer level 4, you need to successively enter TWO codes (in any order) :

• INSTALLER CODE (entered during intial programming).

• USER CODE (Level3): the user must authorize the installer to get access to the configuration of his panel.

4.2 How to Arm/Disarm the System

When in the standby mode, the system can be armed with the embedded or remote keypad , the remote keyfob and/or the embedded or remote badge reader.

	Full arming with user code	Full arming with badge	Special Arming 1	Special Arming 2
With remote keypad	Enter your user code and press **OK or YES**	Present your badge on the keypad (XMB model only)	Press 🏠 / 🏠 enter your user code and press **OK or YES**	Press 🏠 / 🏠 enter your user code and press **OK or YES**
With remote badge reader BR250	N/A	Present your badge on the badge reader	N/A	N/A
With remote keyfob	N/A	N/A	Press 🔳	Press 🔳

4.3 Arming and Siren Mode Configuration

• Use the   to go to menu :

CONFIGURATION (LEVEL 4) -> **SPECIAL ARMING MODES** -> **FULL ARM, SP1 or SP2** use direction arrows to select the arming mode you want to modify and **OK / YES.**

• **There are 3 different arming modes :**

    FULL ARM : Arming of all areas and all devices. Use a badge or a user code and press **OK** / 🔒 on the XMA/XMB keypad or the **YES** key on the CMA keypad.

    SP1 : Partial Arming (1) is enabled by entering the user code and pressing ⌂ on the XMA/XMB keypad, the 🏠 key on the CMA keypad or 1️⃣ on the remote keyfob RC.

    SP1 : Partial Arming (2) is enabled by pressing the ⌂ key on a XMA/XMB keypad, 2️⃣ on a CMA keypad, or 2️⃣ on the remote keyfob RC.

For each arming mode, it is possible to specify how each of the 4 areas will be armed and how the system will behave during an alarm.

Areas :	1	2	3	4	Each time you press the corresponding number, the system will toggle the arming state for the respective area.
State :	A	A	A	A	Press **OK / YES** after this configuration step. The system will then display what siren mode will be in effect for this special profile. Select the siren mode using the direction arrows then press **OK / YES.**

A	**Armed**
D	**Disarmed**
P	**Perimeter** (by default : all opening contacts*)
E	**External** (by default : all opening contacts with external access*)

Siren	Immediate triggering of all sirens
Delay Beeps	Entry/Exit delay beeps, then triggering of all sirens
Silent	No Sirens, No Beeps
Without Siren	Beeps on the keypad only

* You can set your devices as : External, Perimeter, ou External +Perimeter. Please go to the menu:

CONFIGURATION (LVL 4) -> AREAS AND DEVICES -> DEVICES -> DEVICES CONFIGURATION -> DEVICE TYPE

When in the 'Arm From Host' mode, the Videofied system will only arm and disarm when 9-12v is supplied and sustained. When both arming inputs are supplied voltage at the same time the Videofied Keypad display will show 'SYSTEM ARMED. When only one arming input is supplied voltage the Videofied Keypad display will show 'PART LVL #'

•   Arming Input 1 will arm/disarm Areas 1 & 2 – Area 1 is delayed by default
•   Arming Input 2 will arm/disarm Areas 3 & 4– Area 3 is delayed by default

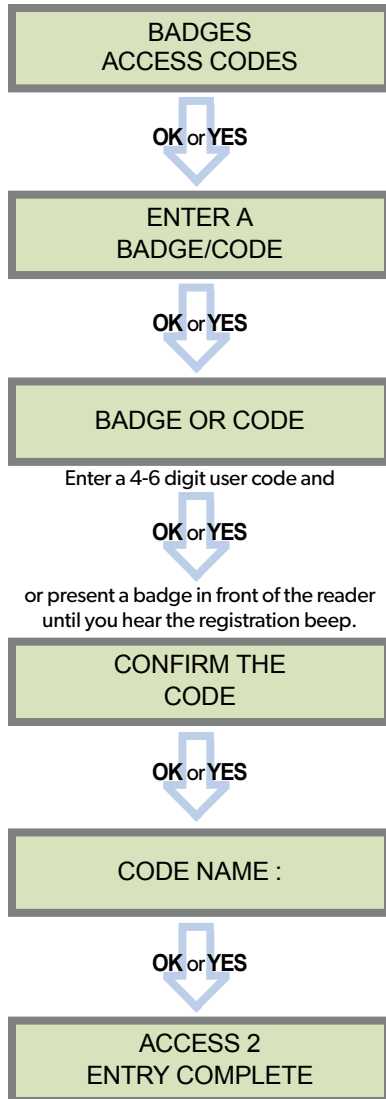## 4.4 Manage badges and access codes

Access Level

Access Level	Definition & Rights
LVL 1	Standby Level
LVL 2	**Restricted USER level,** where it is only possible to arm/disarm the system.
LVL 3	**USER level,** where it is possible to arm/disarm the system, check the event log, test the devices. Modifications of the settings are not possible at this level. User **Level 3** can create **Level 2** or **Level 3** access codes or badges.
LVL 4	**INSTALLER level,** where it is possible to modify the setup of the panel. To access **Level 4**, the approval of a **Level 3** oe **Level 2** user is required. Installer **Level 4** can creat the first **Level 3** access code only.

Codes and badges created after the installer code will automatically set to Access Level 3.
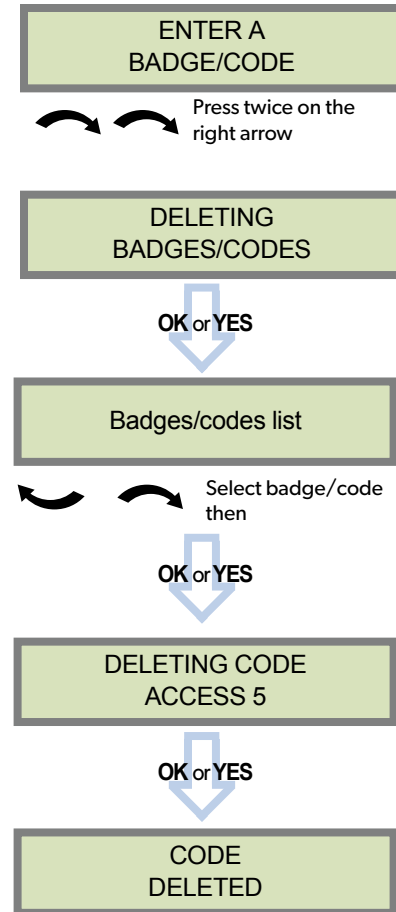
How to return to the LVL1?

- After 1 min of no use of the keypad and no tests running, the display returns to the standby display and LVL1.

- When standby display, if the **ESC NO** key is held during 5s, the level is changed to LVL1.

Enter a new end user Badge/Code

BADGES
ACCESS CODES

OK or YES

ENTER A
BADGE/CODE

OK or YES

BADGE OR CODE

Enter a 4-6 digit user code and

OK or YES

or present a badge in front of the reader
until you hear the registration beep.

CONFIRM THE
CODE

OK or YES

CODE NAME :

OK or YES

ACCESS 2
ENTRY COMPLETE

Delete an end user Badge/Code

ENTER A
BADGE/CODE

Press twice on the
right arrow

DELETING
BADGES/CODES

OK or YES

Badges/codes list

Select badge/code
then

OK or YES

DELETING CODE
ACCESS 5

OK or YES

CODE
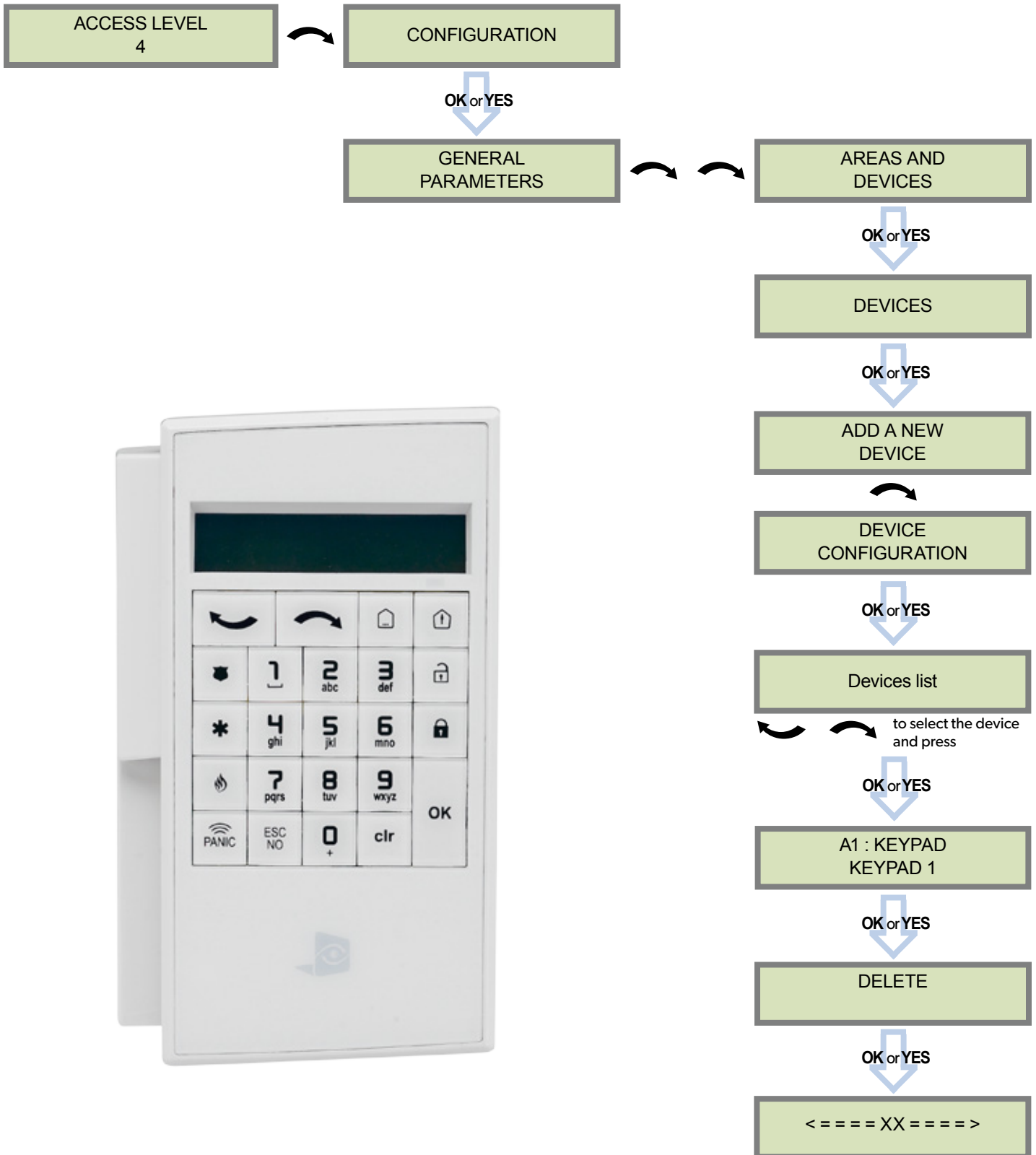DELETED

Reserved Codes

The XT-iP system can accept up to 19 (+1 installer code) Badges or Access codes in any combination.

The table presents the reserved code possibilities that cannot be used.

A total of 186 codes are forbidden.

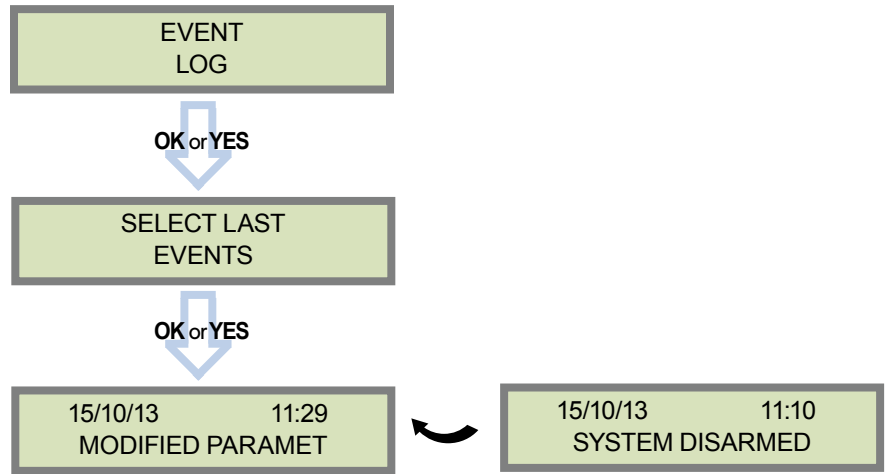| Reserved Codes |
| --- |
| 000000 |
| From 9998 to 9999 |
| From 99998 to 99999 |
| From 999898 to 999999 |
| From 314157 to 314159 |
| All codes +1 |
| All codes +2 |
| All codes -1 |
| All codes -2 |

4.5 Delete the keypad or any other device

ACCESS LEVEL 4	→	CONFIGURATION

OK or **YES** ⬇

GENERAL PARAMETERS	→ →	AREAS AND DEVICES

OK or **YES** ⬇

DEVICES

OK or **YES** ⬇

ADD A NEW DEVICE

↷

DEVICE CONFIGURATION

OK or **YES** ⬇

Devices list

↶ ↷ to select the device and press

OK or **YES** ⬇

A1 : KEYPAD KEYPAD 1

OK or **YES** ⬇

DELETE

OK or **YES** ⬇

< = = = = X X = = = = >

You can now remove the batteries from the device

4.6 Read the event log

When user disarms the system, the keypad indicates the last event.

In case of the user needs to read the full log file, use the keypad to go in EVENT LOG, press **OK or YES** on SELECT LAST EVENTS and use arrow to list the events.

```
┌─────────────────────────────┐
│           EVENT             │
│            LOG              │
└─────────────────────────────┘
```

OK or **YES**

```
┌─────────────────────────────┐
│        SELECT LAST          │
│          EVENTS             │
└─────────────────────────────┘
```

OK or **YES**

```
┌─────────────────────────────┐        ┌─────────────────────────────┐
│  15/10/13          11:29    │        │  15/10/13          11:10    │
│     MODIFIED PARAMET        │        │     SYSTEM DISARMED         │
└─────────────────────────────┘        └─────────────────────────────┘
```

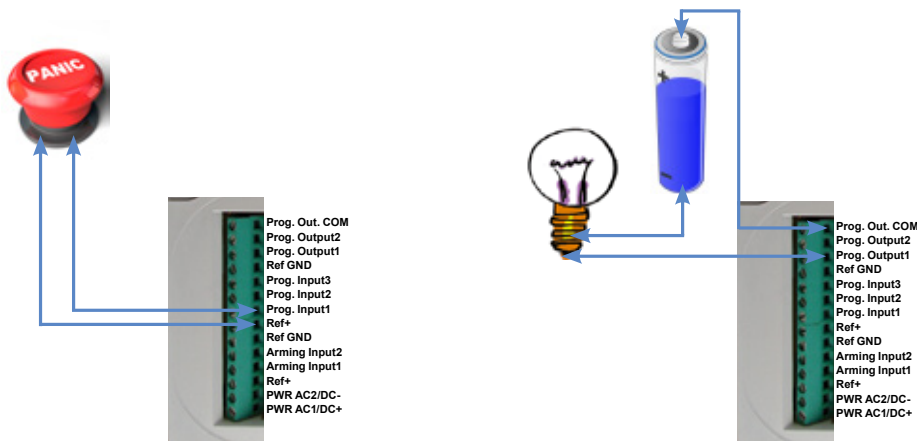Press **OK or YES** for more information about an event

4.7 Programmable inputs and outputs

The XT-iP control panel has 3 programmable inputs and 2 programmable outputs. Please note that we advise to connect the panels to a power supply when using programmable inputs. These functions allow the linking of Videofied® security systems to auxiliary equipment such as panic buttons, pepper spray, smoke generator, hard-wired door contact, light curtain, etc.

PROGRAMMABLE INPUT 1, PROGRAMMABLE INPUT 2 and PROGRAMMABLE INPUT 3 are triggered by voltage between 9V and 15V and an intensity between 1,5mA (@9V) and 3mA (@15V). If a dry contact is used to trigger the programmable inputs, the REF+output can be used to supply this dry contact.

PROGRAMMABLE OUTPUT 1 and PROGRAMMABLE OUTPUT 2 can be triggered either by a panel event, by a peripheral device or by an external event such as a programmable input or a arming input.

The XT-iP control panel also offer a mapping feature. Mapping option allows the input to generate a video-clip via a MotionViewer when a programmable input is triggered and/or when an event occurs.


Prog. Out. COM
Prog. Output2
Prog. Output1
Ref GND
Prog. Input3
Prog. Input2
Prog. Input1
Ref+
Ref GND
Arming Input2
Arming Input1
Ref+
PWR AC2/DC-
PWR AC1/DC+

Prog. Out. COM
Prog. Output2
Prog. Output1
Ref GND
Prog. Input3
Prog. Input2
Prog. Input1
Ref+
Ref GND
Arming Input2
Arming Input1
Ref+
PWR AC2/DC-
PWR AC1/DC+

For further information about the programmable inputs and outputs, please consult the following application notes available on our support website:
240-XV-XT - PROG INPUTS - APP NOTE
240-XV-XT - PROG OUTPUTS - APP NOTE

4.8 Golden rules

1. Area 1 is always **delayed.**When you register a keypad or a badge reader into an area, that area will automatically be delayed.

2. **Never position** a panel next to **a high voltage electrical cabinet** .

3. Press CLR to erase a typing mistake.

4. Never register the same device twice (delete from the system first).

5. Registration of **up to 25 devices** (including the keypad).

6. Respect indoor infrared devices installation height (**2m10 to 2m30)**.

7. Outdoor cameras have to be installed at **2m60 to 3 meters height**. Those devices needs to to protect an access and not a zone.

8. Do not fix the keypad at the beginning of the installation as it will need to be portable during programming.

9. **Always clean** the lens of the cameras after the installation (Use a clean, dry cloth, taking care not to exert pressure on the lens).

10. To switch between UPPER and lower case, use the M/m key from the CMA keypad or hold a digit key (0 to 9) for XMA/XMB.

11. Internal components are fragile, be careful opening or closing the panel.

12. LCD screen goes dark after 30 seconds of inactivity, press an arrow or numeric key to light it up.

13. Use only batteries provided by RSI (panel and siren : Alkaline batteries).

14. Infrared detectors should never be installed in stairs or close to stairs (false alarm risks).

15. A colon display [:] means that the parameter can be changed.

To configure Ethernet parameters, using the direction arrows, go to the menu :

Lvl. 4

CONFIGURATION	OK or YES	GENERAL PARAMETERS	OK or YES	ETHERNET
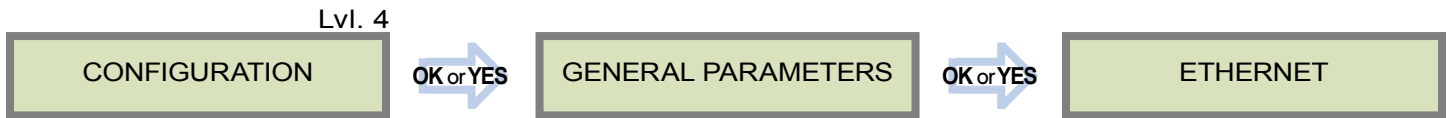
To configure or modify Ethernet Parameters, go to:

- **IP Parameters**:

If you wish to use the Ethernet transmission mode, two options are available:

1. **DHCP Enable**: IP address is assigned by the DHCP service on the network. (Dynamic IP address). This is the default option.
2. **DHCP Disable**: IP address must be defined in Ethernet parameters. IP address will NOT be automatically obtained from DHCP service on the network. Each connection from the panel to the network (alarms transmission), the XT-iP will have the same connection parameters. You must first connect to the router in order to get the network parameters and all available IP addresses. The following parameters must be filled in the IP PARAMETERS sub-menu: PANEL IP, IP MASK, GATEWAY, PRIMARY DNS, SECONDARY DNS.

- **Constant Ethernet**:

Three options are available:

1. **"Auto" Mode** - We recommend this mode. If main powered, the panel will be connected constantly to the local Network. In case of an alarm, the alarm will be sent in few seconds to the monitoring station. When the main power is cut, the Ethernet module will switch off after a delay (DELAY BEFORE OFF – 30 by default) in order to save battery life. In case of an alarm, the panel will at first connect to the local Network. It adds few seconds to the total process of sending an alarm.
   You can set the delay in this menu :
   CONFIGURATION (NIV 4) -> **GENERAL PARAMETERS** -> **ETHERNET** -> **CONSTANT ETH.** -> **DELAY BEFORE OFF**.

2. **"ON" Mode** - The panel will be connected constantly to the local Network. This option will impact back-up battery life.

3. **"OFF" Mode** - For each transmission of alarm and video, the panel will connect to the local Network.

- **PING reply, Time Out Server, Max Seg. Size:**
   - PING REPLY: Enables ping response.
   - Time Out Server: In case of disconnection to the local Network, the panel will try after that time to re-connect.
   - Max Seg. Size: Maximum size of packet sent.

The XT-iP panel can be configured to enable or disable the transmission of events like alarms or defaults.

The installer can modify the default sending settings for those events, although it will end the EN50131 standard compliance.

These are the default transmitted events :
DEVICE (intrusions) ALERT (Panic Buttons) PANEL LOW BATT. TAMPER DEVICE LOW BATT. PERIODIC TEST DURESS CODE FIRE MEDICAL ASSIST. ETHERNET CABLE

The following events are not sent by default :
PANEL RESET AC POWER LOSS (AC Power supply) PHONELINE FAULT RADIO JAMMING SUPERVISION 5 WRONG CODES ALARM CANCEL ARM/DISARM (On/Off)

There is 3 different transmission states :
ALARM : event transmitted upon occurrence
ALARM/END : event is transmitted on occurrence and on event restoral
NOT TRANSMITTED : event is not transmitted, however it will appear on the keypad.

Example :

If the monitoring station system is set to receive arms and disarms, the **ARM / DISARM** parameter must be changed from **NOT TRANSMITTED** to **ALARM / END**.

How to modify the transmission state

• **At initial programming, right after the PERIODIC TEST CALL step:**

CODE/STATE
MODIFICATION   Press **OK or YES** to access **EVENT TRANS. MODIFICATION** menu.

• **After initial programming, using a remote keypad :**

Use the arrows   to access :

CONFIGURATION (level 4) -> **CONFIGURATION MONITOR. STATION** -> **FRONTEL SECURITY PARAMETERS** -> **EVENT TRANS. MODIFICATION**

Then use the arrows   to determine the event to modify. Press **OK or YES** to edit.

IMPORTANT: The PIN of the SIM card has to be deactivated or 00000.

The following is a list of error codes that can appear after the 2G3G test.

2G3G LEVEL :
ERROR XXX

In case of 2G3G (GPRS) errors during initial programming, we strongly suggest to continue with the installation and perform the 2G3G (GPRS) level test again once achieved.

This error checklist is provided for information purposes only.

This is not a comprehensive list, but it is representative of most cases. Some events or codes are subject to change by SIM card operators.

However, the GPRS level test errors results in the majority of cases have the following causes :

• **SIM Card activation Delay:**

Some operators require an additional delay up to 48 hours to activate automatic data transmission. Please check with your operator prior to installation.

• **APN CODE, USERNAME and PASSWORD :**

The GPRS (2G3G) settings are supplied by the operator. Please make sure you have entered the code exactly as indicated by your local SIM card operator.

Note: When entering your SIM card settings, both APN codes, username and password fields are case sensitive! (It makes a difference between UPPER and lower case letters).

To switch between UPPER and lower case, use the M/m key from CMA keypad or hold a digit key (0-9) for XMA/XMB.

• **Insufficient GPRS Network:**

When the panel is unable to find any signal, proceed to GPRS level test in another location on site. You can also find the network state or condition of use by directly contacting your local operator.

Codes	Errors
03 ou 04	No network coverage or no SIM card inserted
003	SIM card not detected/not inserted
010	SIM not inserted
011	PIN code necessary -> *PIN code must be deactivated*
012	PUK code necessary, SIM card blocked
013	Default SIM card
014	SIM card busy
015	Error on SIM
030, 043, 057, 102, 132, …	• No network coverage • Typographical error in the APN Code, username, password • SIM card not activated

Notes de sécurité / (EN) Security notes / (DE) Hinweise zur Sicherheit

Français
- *Retirez les piles avant toute opération de maintenance !*
- *Attention ! Il y a un risque d'explosion si l'une des piles utilisées est remplacée par une pile de type incorrect !*
- *Respectez la polarité lors de la mise en place des piles !*
- *Ne jetez pas les piles usagées ! Ramenez-les à votre installateur ou à un point de collecte spécialisé.*

English
- *Remove battery before any maintenance !*
- *WARNING, there is a risk of explosion if a battery is replaced by an incorrect type!*
- *Observe polarity when setting up the batteries!*
- *Do not throw used batteries! Bring them to your installer or a collection point.*

Deutsch
- *Batterien vor jeglichen Wartungsarbeiten entfernen!*
- *Vorsicht, es besteht Explosionsgefahr, wenn eine Batterie durch eine Batterie falschen Typs ersetzt wird!*
- *Achten Sie beim Einsetzen der Batterien auf die Polung!*
- *Entsorgen Sie Batterien nicht im normalen Haushaltsmüll! Bringen Sie Ihre verbrauchten Batterien zu den öffentlichen Sammelstellen.*

Electrical data

Power requirements (option 1)

Power supply Type B	9-12VDC / 1,2A
Low voltage limit	5,15V
Backup	6V with 4 x 1,5 V D Alkaline batteries /LR20
Low battery limit	4,2V
Battery life (average)	1 year
Average current consumption (over 1h)	450µA
Max current	1,2A

RF S^{2}View® Technology

Radio type	Bidirectional RF
Operating frequency	868/915/920 MHz
Transmission security	AES algorithm encryption
Radio jam detection	Yes
Supervision	Yes
Antenna	Integrated
External radio antenna	Yes via MMCX connector

Tamper detection

Tamper	Wall and cover tamper detection

Programmable wired input

Number	3
«Dry» contact	Yes
Input voltage	12 VDC (15VDC max)

Programmable wired outputs

Number	2
Max switching voltage	60VDC /30VAC
Max switching current	4A
Max switching power	120 VA

Approvals

EN50131-1: 2007 - Grade 2 – Class II
EN50131-3:2009 - Grade 2   &   **RTC 50131-3**:2009
EN50131-4:2009 Grade 2   &   **RTC 50131-4**:2009
EN50131-5-3:2005 - Grade 2
EN50131-6:2008 Grade 2 –Type B &   **RTC 50131-6**:2008
NF C 48-212:2004
NF EN50130-4:1995; A1:1998; A2:2003
NF EN50130-5: 1998 Class II

GPRS Transmission

Communicator

Communicator type	GPRS/Ethernet
Security Protocol	Frontel
IP Stack	TCP/IP
Video transmission	By Frontel protocol to central monitoring station
GPRS antenna	Integrated
External GPRS antenna	Yes via MMCX connector

Video

Video format	MPEG
Video size	Depending on camera type
Video length	10 seconds

Miscellaneous

Programming	With remote Keypad
Remote Devices per system	25 maximum
Access Badges/codes	20 maximum
Special arming mode	4
Number of Areas	4
History / Event log	4,000 events stored on flash memory

Box

Physical and Environmental Datas

Operating temperature	-10°/+40°C
Maximum relative humidity	75%, non-condensing
Material	ABS—ULV0
Dimensions	225 mm x 180 mm x 55mm (LxWxD)
Weight	520gr (without batteries) / 1600gr (with batteries)

Installation/Mounting

Control Panel/Base
Two screws secures control panel cover to base; Three screws secure control panel base to the wall