



Description

The XTO is a fully wireless alarm system. It can be powered by standalone batteries or connected to a power supply. This panel has been designed for outdoor installations, with its weatherproof casing and extended operating temperature range.

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

The XTO 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 XTO alarm system offers the possibility to increase its Radio and/or GPRS performances through the connection of externally wired antennas.

Technology

The XTO 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 being 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 XTO. Through the supervision, the detectors transmit every 8 minutes a presence signal.

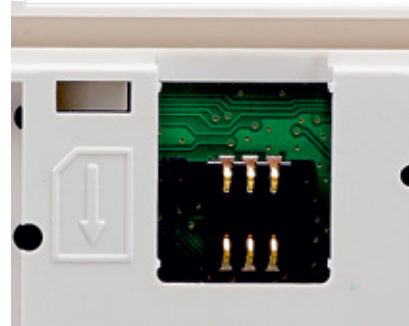
The entire RSI VIDEO TECHNOLOGIES team wishes you a successful installation.

Introduction.....	2
Summary.....	3
1. XTO Panel setup.....	4
1.1 SIM card installation.....	4
1.2 Panel Bracket Mounting.....	4
1.3 Powering and initialization.....	5
1.4 Pairing the keypad.....	6
1.5 Panel Mounting.....	6
2. XTENDER Mode.....	7
3. XTO Panel programming.....	8
XTENDER mode configuration.....	13
4. XTO features guide.....	16
4.1 Get to access level 4.....	16
4.2 How to Arm/Disarm the system.....	16
4.3 How to enable the External RF Antenna.....	16
4.4 Arming and Siren Mode Configuration.....	17
4.5 Manage badges and access codes.....	18
4.6 Delete the keypad or any other device.....	20
4.7 Read the event log.....	21
4.8 Programmable inputs and outputs.....	21
4.9 Golden rules.....	22
5. Transmitted events list.....	23
6. 2G3G error codes.....	24
7. Technical specification and security notes.....	25

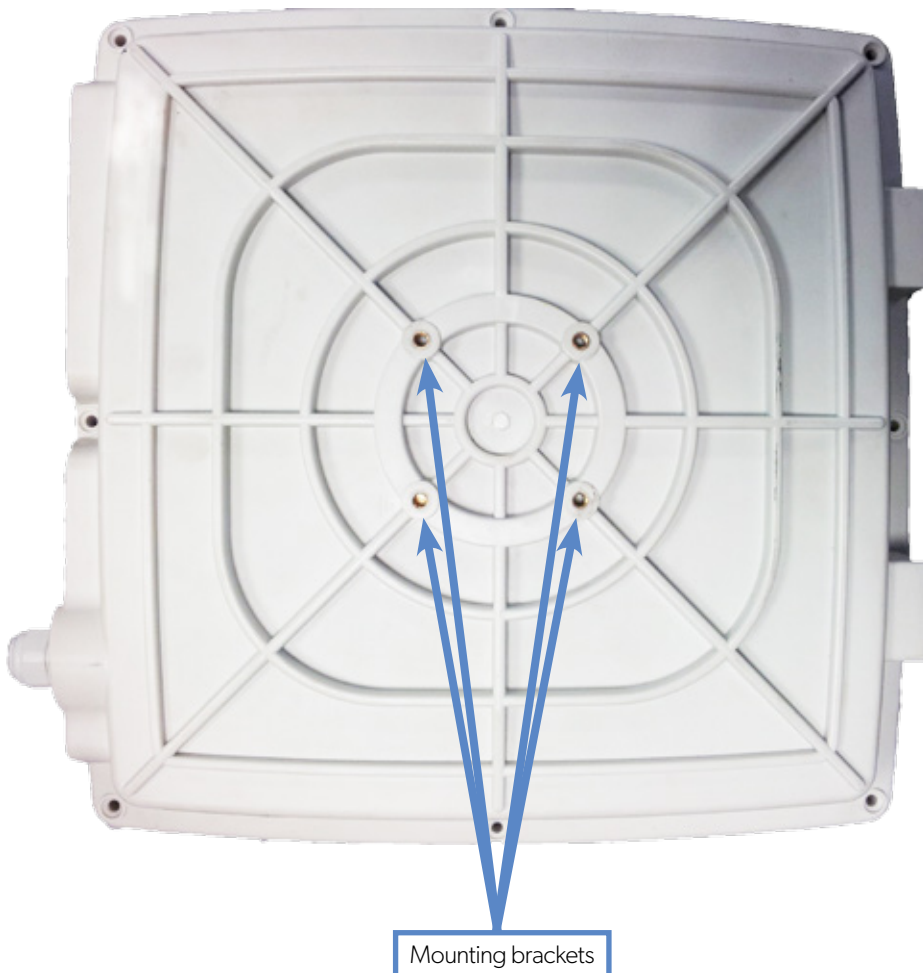
1.1 SIM Card Installation

Before removing the front cover from its box, Put the SIM card on the plastic base (Take care to respect the right direction).

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



1.2 Panel Bracket Mounting



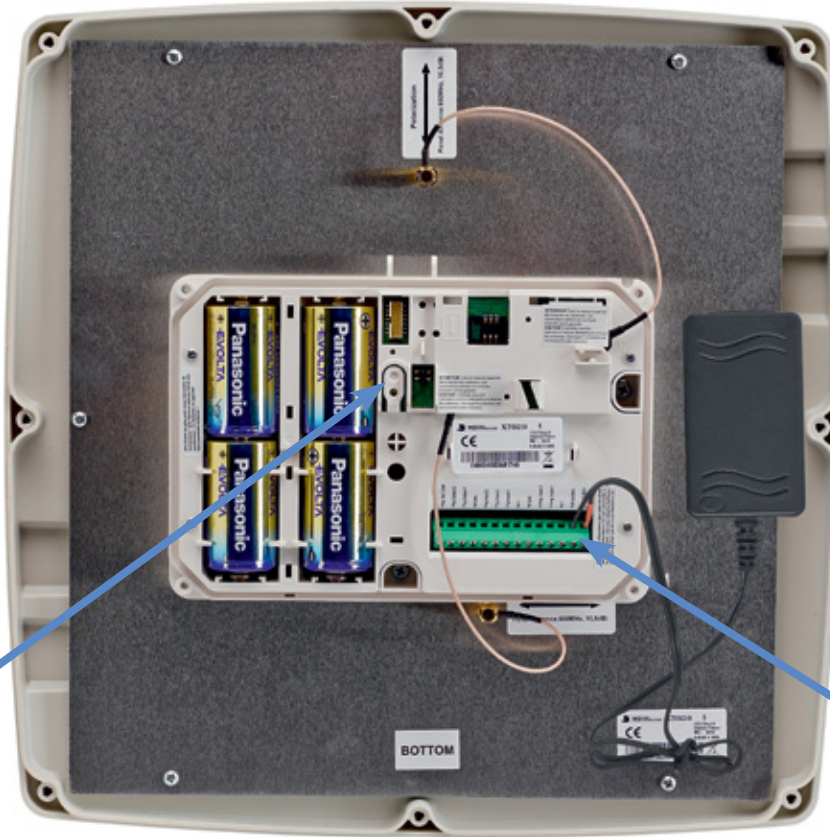
The four screwholes here opposite are intended to mount L shaped bracket, the latter being used to attach the panel to the wall or a pole.

Mounting the panel is not required for programming

1.3 Powering and initialization

Option 1

THE CONTROL PANEL **MUST BE CONNECTED TO AN EXTERNAL POWER SUPPLY (OPTION 1)** WHEN USING THE **RINGTONE FEATURE OR SMARTPHONE APP.**



- The panel is powered either with a mains power supply with 4 backup LR20 Alkaline batteries (Option 1 recommended) or with 4 LSH20 Lithium batteries (Option 2).
- 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.



Programming button

Mains power supply

Option 2



1.4 Pairing the remote keypad

- Press the XTO programming button and release for the enrollment of a programming keypad.
- Insert all **LS14500 Lithium batteries** into the keypad.
- **Do not mount the keypad.** It will display one of the following screens:

RSI (c) 2013
videofied.com

or

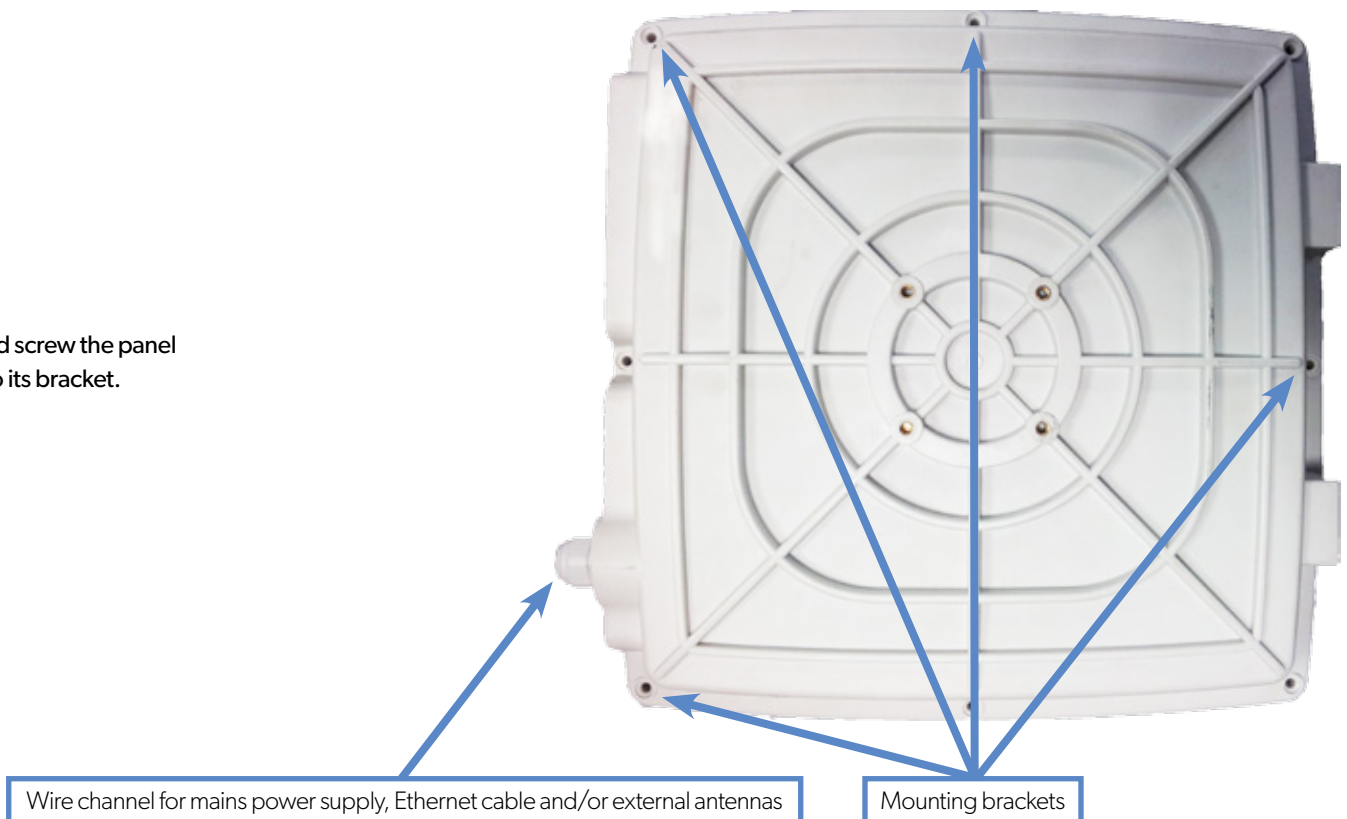
<=====XX=====>

- **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. Then proceed to the above steps.



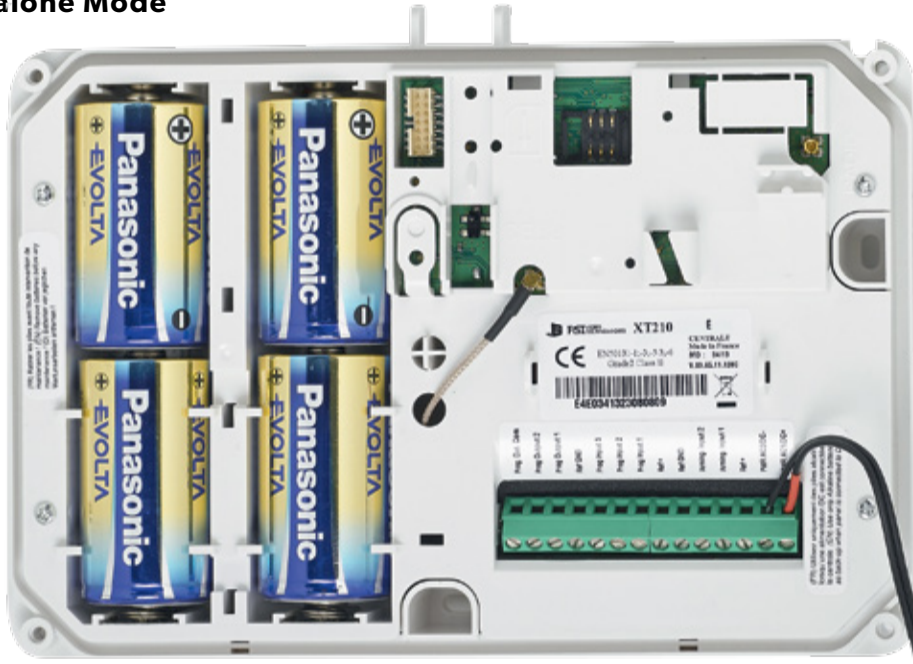
1.5 Panel Mounting

Place and screw the panel casing to its bracket.



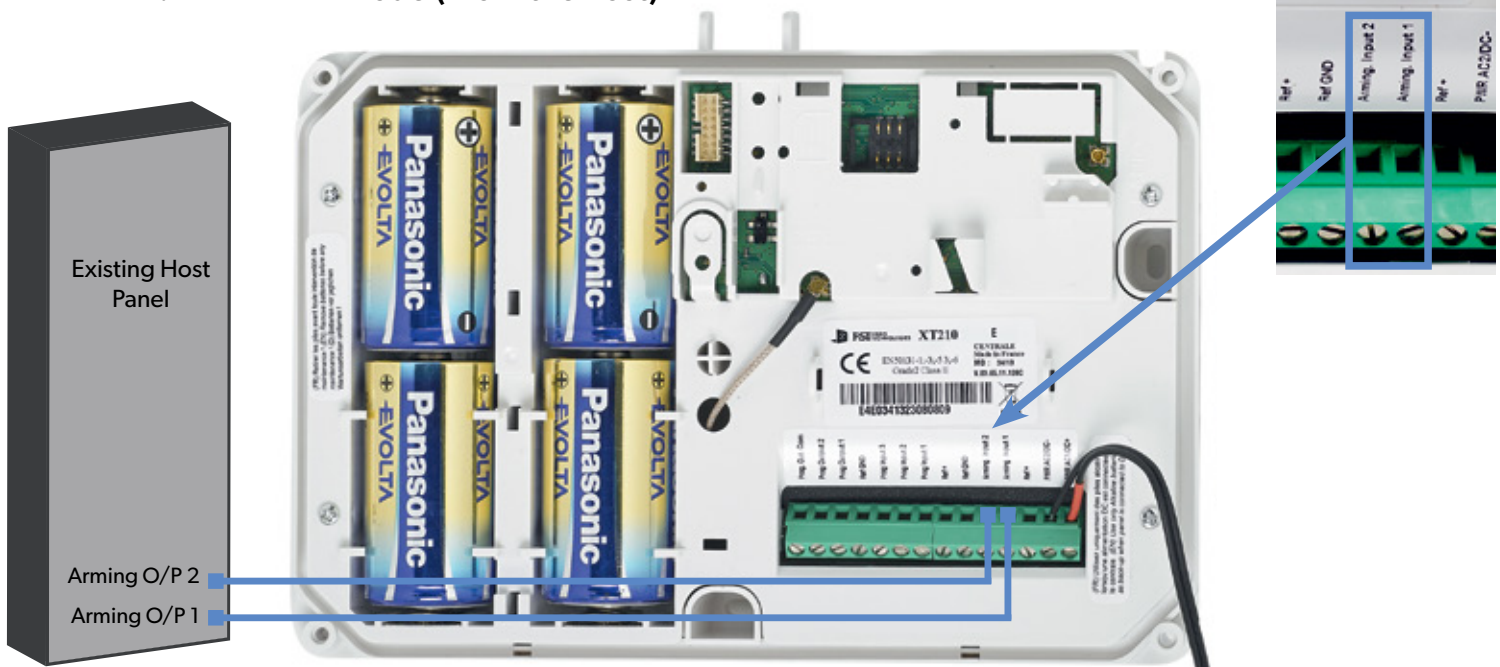
The XTO panel can be used as standard standalone alarm system but it can also be connected to an existing alarm system capable of latching a 9-12Vcc* voltage used for its arming/disarming.

2.1 Standalone Mode



In this functioning mode, the XTO 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)



When the XTO 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.

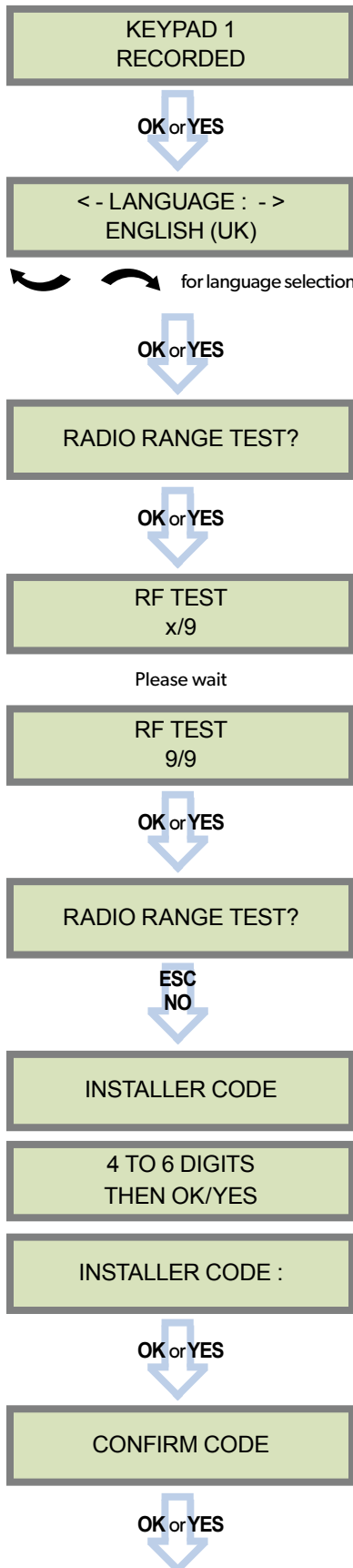
On a programed panel, you can choose between standalone and XTENDER modes from the menu :

CONFIGURATION (LVL 4) > GENERAL PARAMETERS > XTENDER

**When using an XTO in XTENDER mode, the panel has to be powered by the mains power supply.*

Keypad Display

Actions and comments



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.

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 rule 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

ACCOUNT NUMBER :

ACCOUNT NUMBER :
567001

OK or YES

ESC
NO

You may name the installer code using the Alphanumeric Keypad.

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

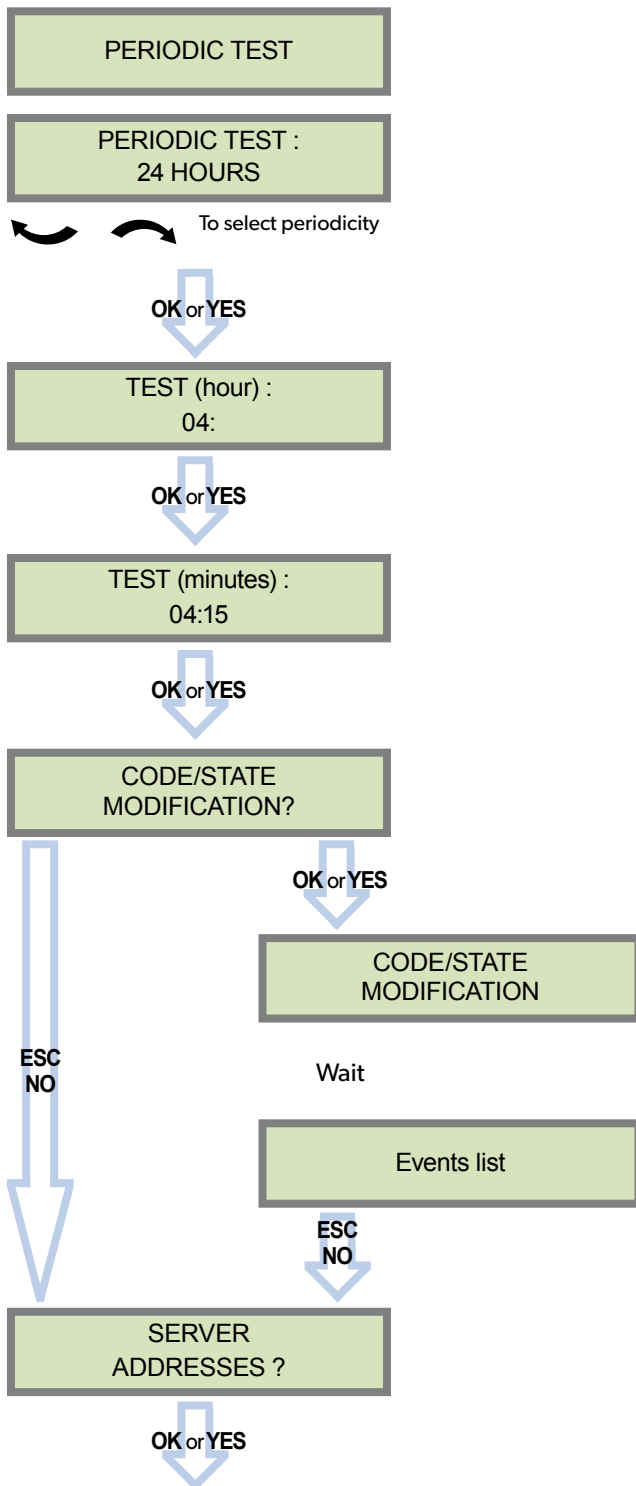
Warning : If the wrong installers list name is used it cannot be set later, the system must be defaulted.

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



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

We suggest a 24 hours periodic test call.

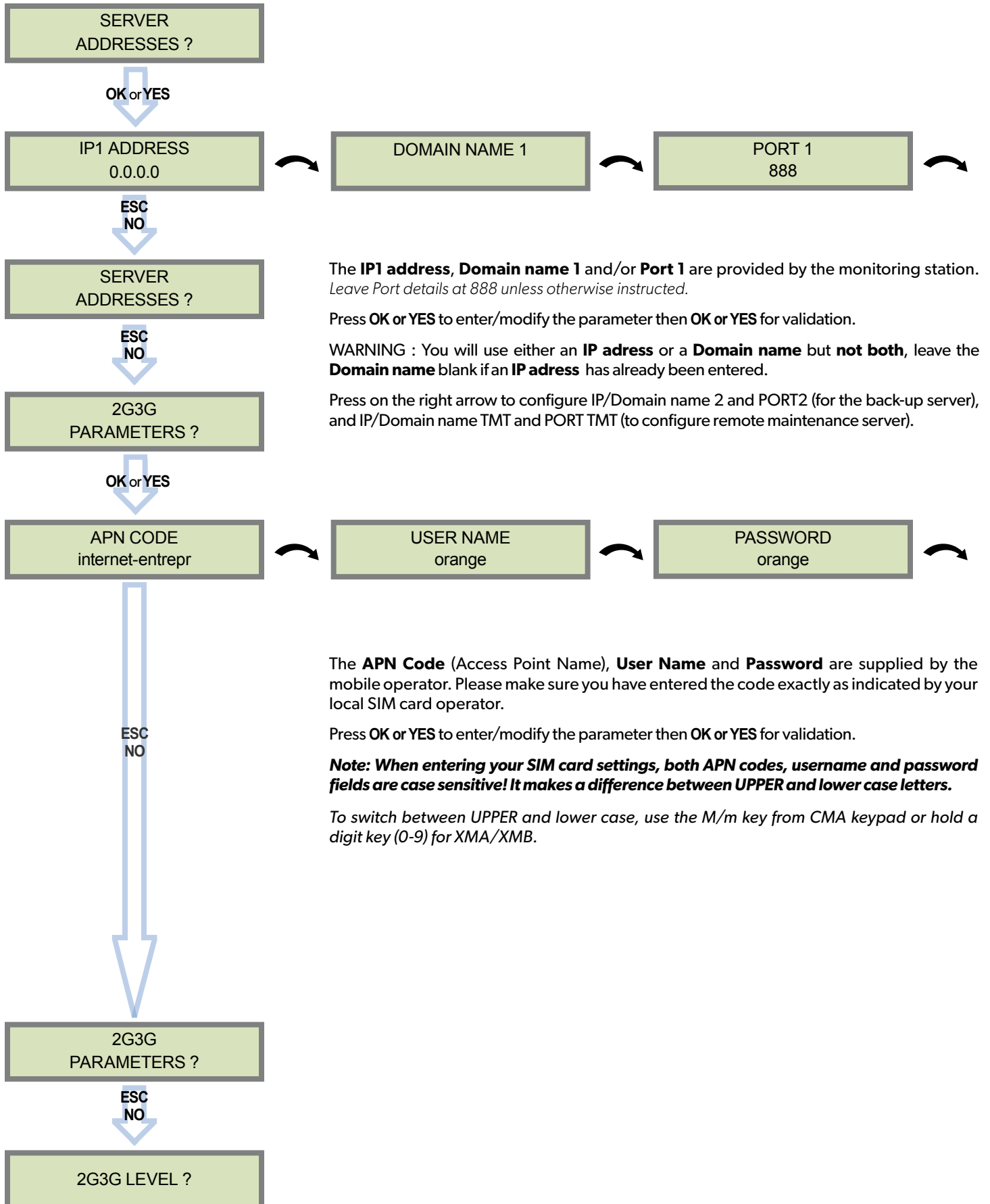
The CODE/STATE MODIF. menu is to configure the transmitted events to the monitoring station, use the arrow keys to toggle between events and **OK or YES** to modify.

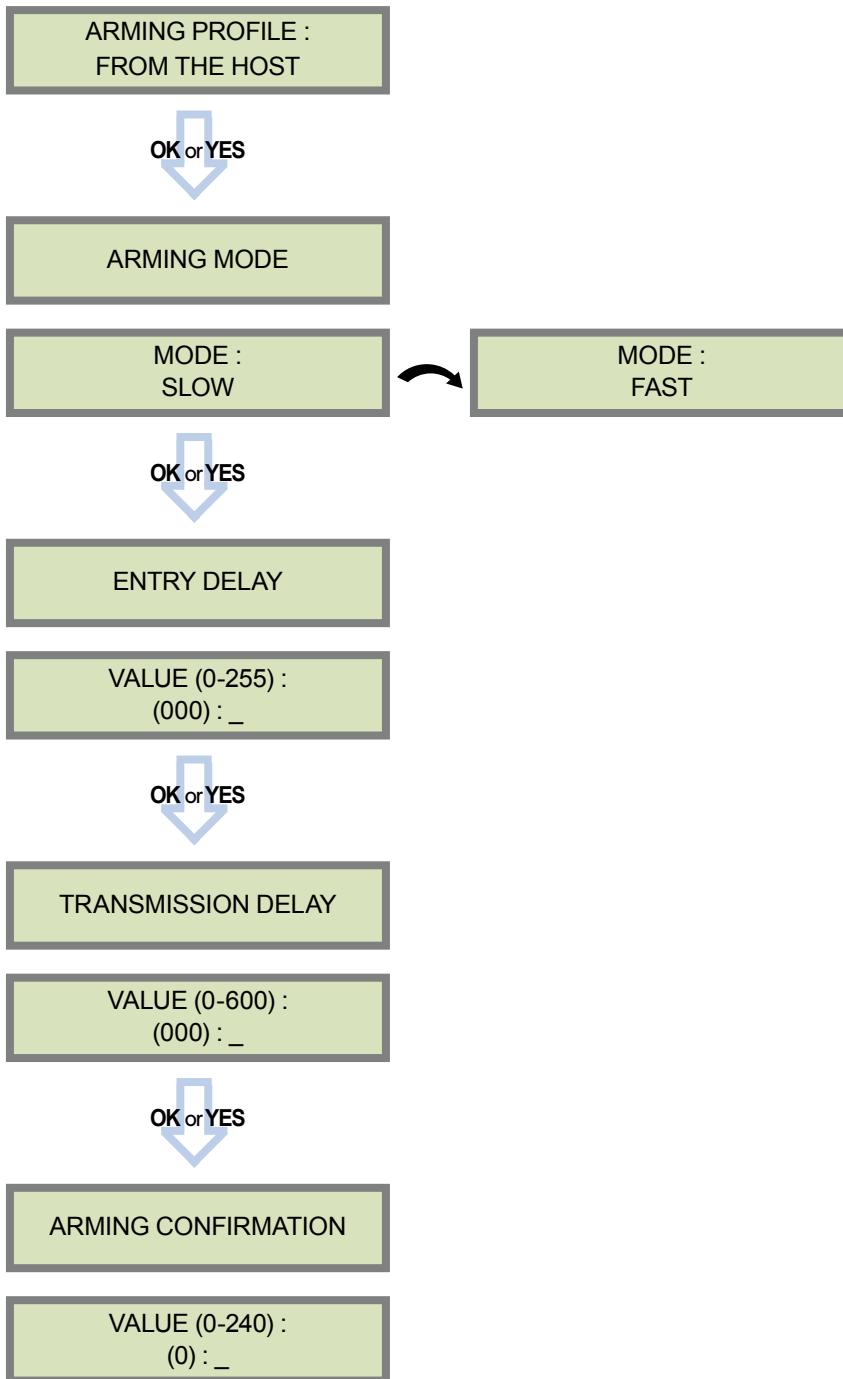
ALARM: event transmitted upon occurrence.

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

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

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



XTENDER mode configuration

MODE SLOW : The panel will arm each device one at a time saving battery life. This mode is recommended.

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 set the delay between the detection of an event and its transmission to the monitoring center.

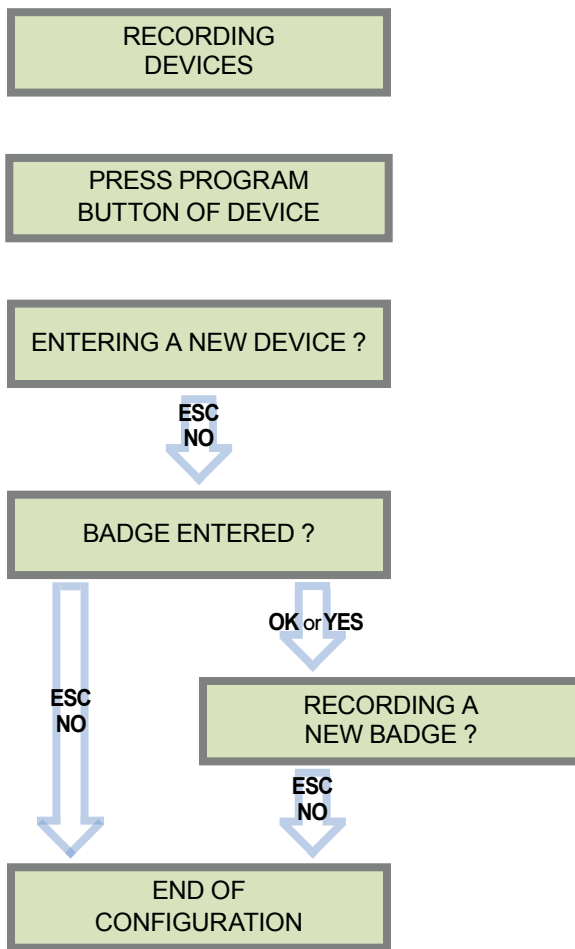
Except when specifically required, please enter 0.

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



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.**

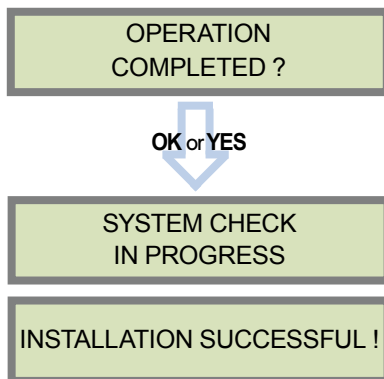
Press **OK** or **YES** to enter a new device or **ESC NO** to move to the next step.

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 once the system configuration done go to the BADGES/ACCESS CODES menu (please refer to chapter 4.4 for further details).

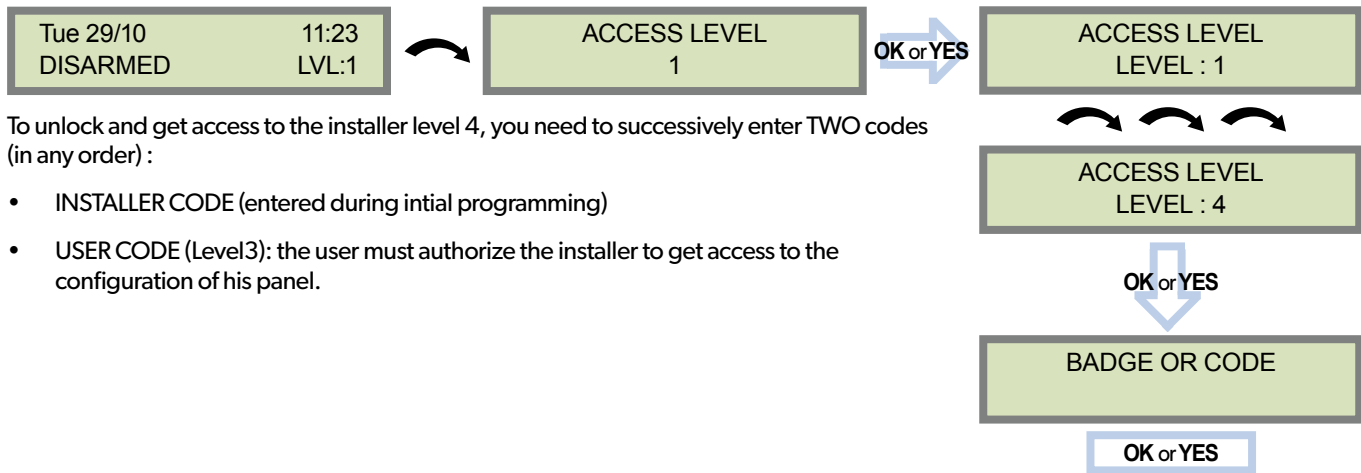
Badges and codes are limited to 19 for user (level 2 or 3) + 1 installer code.



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



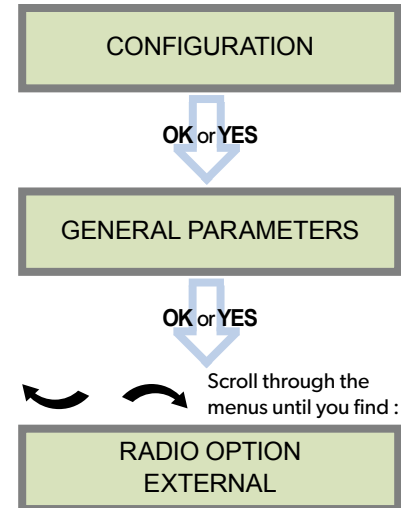
4.2 How to Arm/Disarm the System

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 personal 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 How to enable the External RF Antenna

The XTO control panels have built in High Gain RF and GPRS antennas. The GPRS external comes pre-activated and hooked up, while the RF antenna is hooked up but needs to be activated in Configuration after you have completed initial programming. The following steps will walk you through how to enable the High Gain RF antenna after initial programming.







4.4 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  on the remote keyfob RC.

SP2 : Partial Arming (2) is enabled by pressing the  key on a XMA/XMB keypad,  on a CMA keypad, or  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

State : A A A A

Each time you press the corresponding number, the system will toggle the arming state for the respective area.

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

4.5 Manage badges and access codes

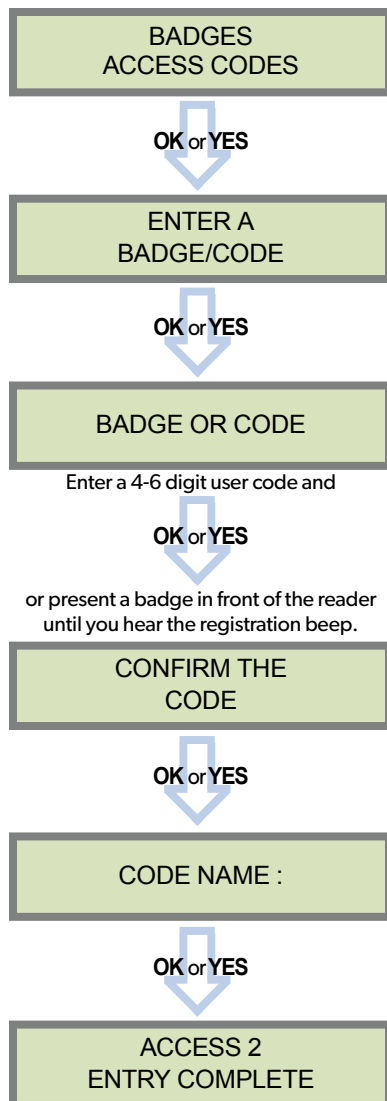
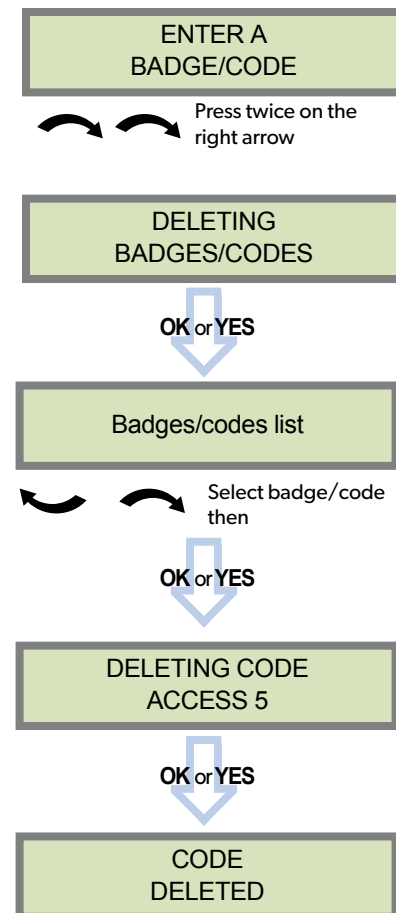
Access Level

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 or Level 2 user is required. Installer Level 4 can create the first Level 3 access code only.

Codes and badges get rights access to one of the 4 available levels of access.

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**Delete an end user Badge/Code****Reserved Codes**

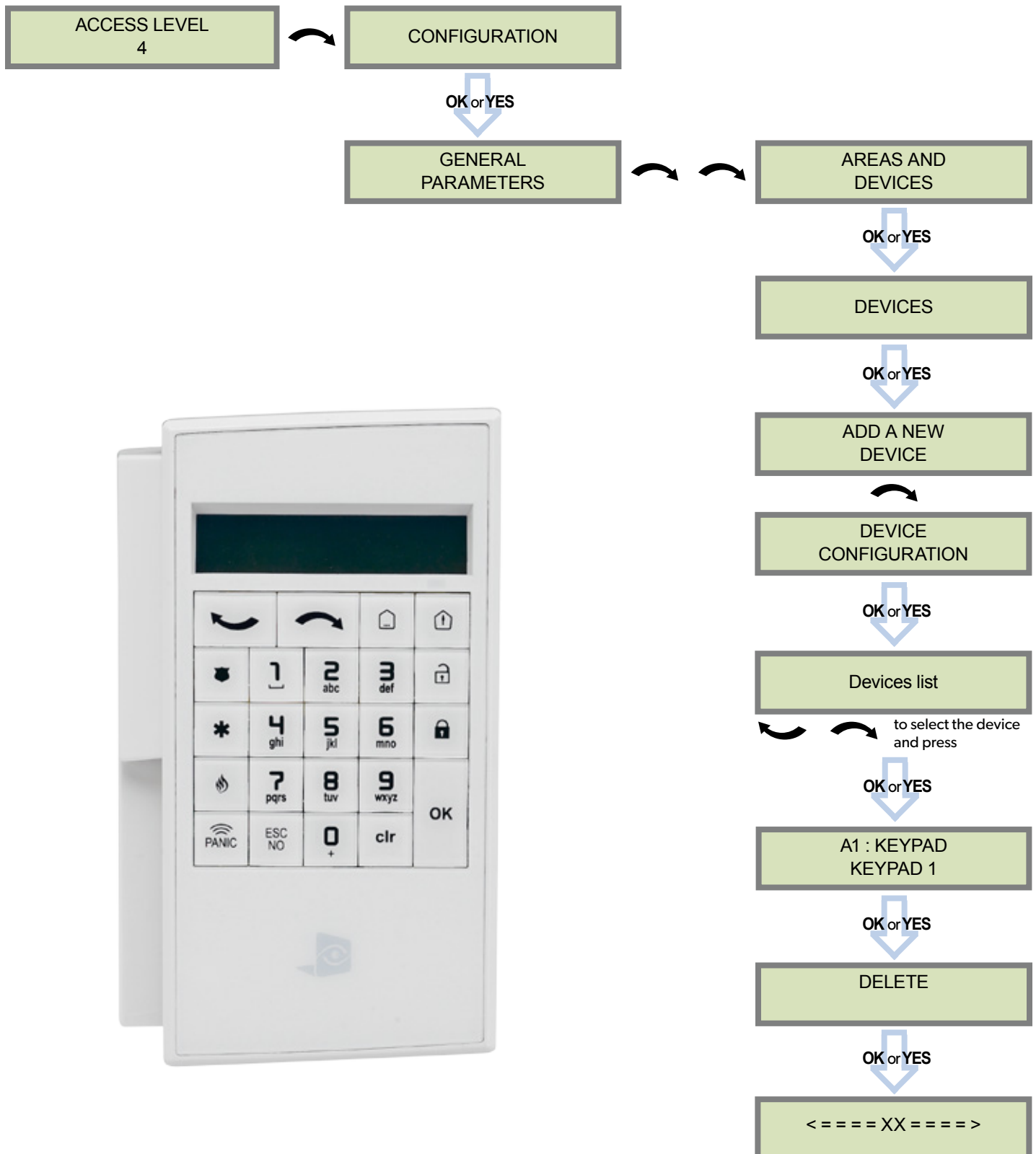
The XTO system can accept up to 19 (+1 installer code) Badges or Access codes in any combination.

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

4.6 Delete the keypad or any other device

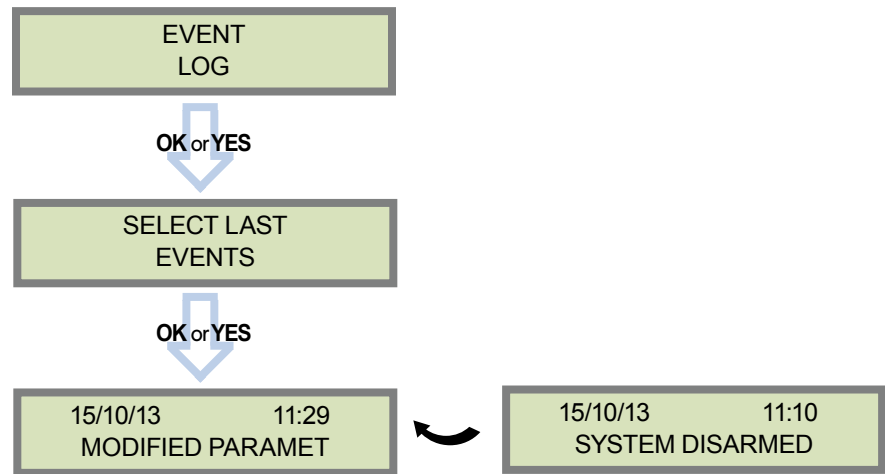


You can now remove the batteries from the device

4.7 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.



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

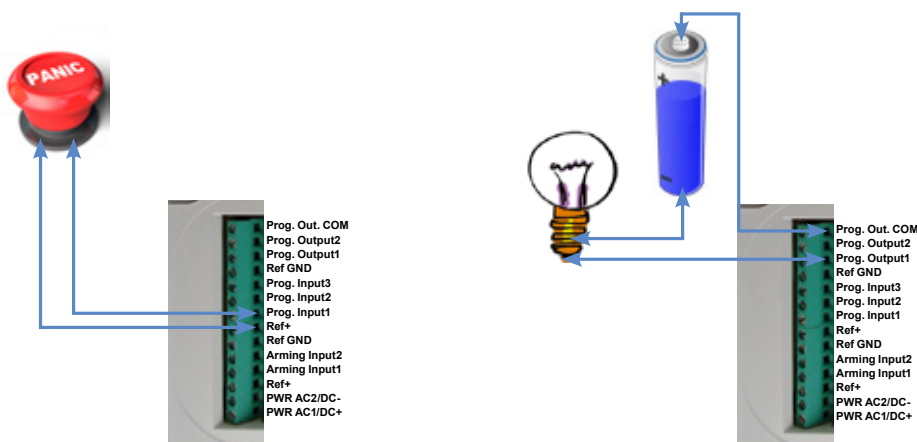
4.8 Programmable inputs and outputs

The XTO 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 XTO 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.



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 need 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.

The XTO 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 :	The following events are not sent by default :
DEVICE (intrusions) ALERT (Panic Buttons) PANEL LOW BATT. TAMPER DEVICE LOW BATT. PERIODIC TEST DURESS CODE FIRE MEDICAL ASSIST. ETHERNET CABLE AC POWER LOSS (AC Power supply)	PANEL RESET PHONELINE FAULT RADIO JAMMING SUPERVISION 5 WRONG CODES ALARM CANCEL ARM/DISARM (On/Off) ZONE BYPASS (bypass function enabling/dsiabling) SWINGER SHUTDOWN

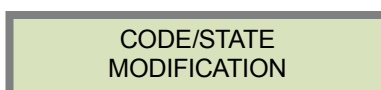
There is 3 different transmission states :
ALARM : event transmitted upon occurrence
ALARM/END : event is transmitted on occurrence and on event restoral
NOT TRANSMITTED : event is not transmitted, however it will appear on the keypad.

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:



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** > **MONITORING 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.

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 -> <i>PIN code must be deactivated</i>
012	PUK code necessary, SIM card blocked
013	Default SIM card
014	SIM card busy
015	Error on SIM
030, 043, 057, 102, 132, ...	<ul style="list-style-type: none"> No network coverage Typographical error in the APN Code, username, password SIM card not activated

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.

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

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.

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.

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 S²View® 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 &
EN50131-4: 2009 Grade 2 &
EN50131-5-3: 2005 - Grade 2
EN50131-6: 2008 Grade 2 –Type B &
NF C 48-212: 2004
NF EN50130-4: 1995; A1:1998; A2:2003
NF EN50130-5: 1998 Class II

RTC 50131-3: 2009
RTC 50131-4: 2009

RTC 50131-6: 2008

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	-28°/+60°C
Maximum relative humidity	95%, non-condensing
Material	ABS—ULV0
Dimensions	391 mm x 391 mm x 76mm (LxWxD)

Installation/Mounting

Control Panel/Base	Seven screws oncover for base closing; four screws on panel base for brackets mounting
--------------------	--



EMEA SALES

23, avenue du Général Leclerc
 92340 BOURG-LA-REINE
 FRANCE
 E-Mail : emeasales@rsivideotech.com

North American Headquarters

1375 Willow Lake Blvd, Suite 103
 Vadnais Heights, MN 55110
 USA
 E-Mail : usasales@rsivideotech.com

