INSTALLATION MANUAL

XTO-IP ALARM PANEL

DOC. - REF. 230-XTO-IP
MODIF. DATE : JANUARY 2016
FIRMWARE VERSION : XLP.05.21.00.XXX AND LATER

MADE IN FRANCE

Description

The XTO-iP 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-iP panel provides video verification in case of intrusion.

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

Technology

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

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

SUMMARY

Introduction....2

Summary....3

1. XTO-iP panel setup....4
   1.1 SIM card installation....4
   1.2 Ethernet cable connection....4
   1.3 Panel bracket mounting....4
   1.4 Powering and initialization....5
   1.5 Pairing the keypad....6
   1.6 Cover locking....6

2. XTENDER mode....7

3. XTO-iP panel programming....8
   ETHERNET parameters configuration....12
   XTENDER mode configuration....14

4. XTO-iP 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....17
   4.4 Arming and Siren Mode Configuration....18
   4.5 Manage badges and access codes....19
   4.6 Delete the keypad or any other device....21
   4.7 Read the event log....22
   4.8 Programmable inputs and outputs....22
   4.9 Golden rules....23

5. Ethernet parameters....24

6. Transmitted events list....25

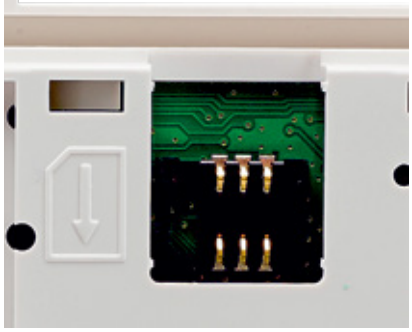
7. 2G3G error codes....26

8. Technical specification and security notes....27

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.



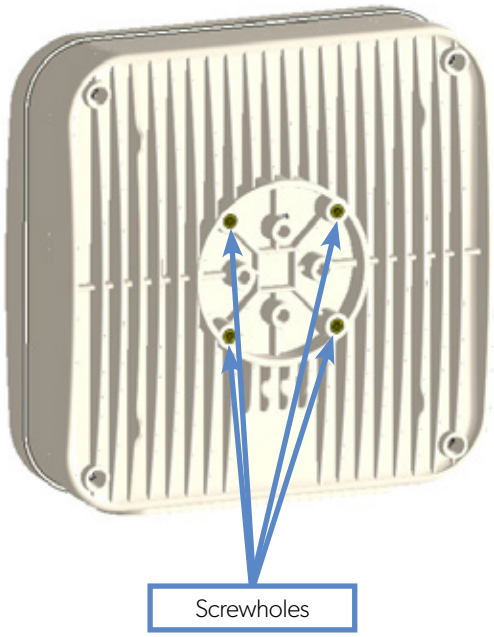
1.2 RJ45 cable connection

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.

1.3 Panel bracket mounting

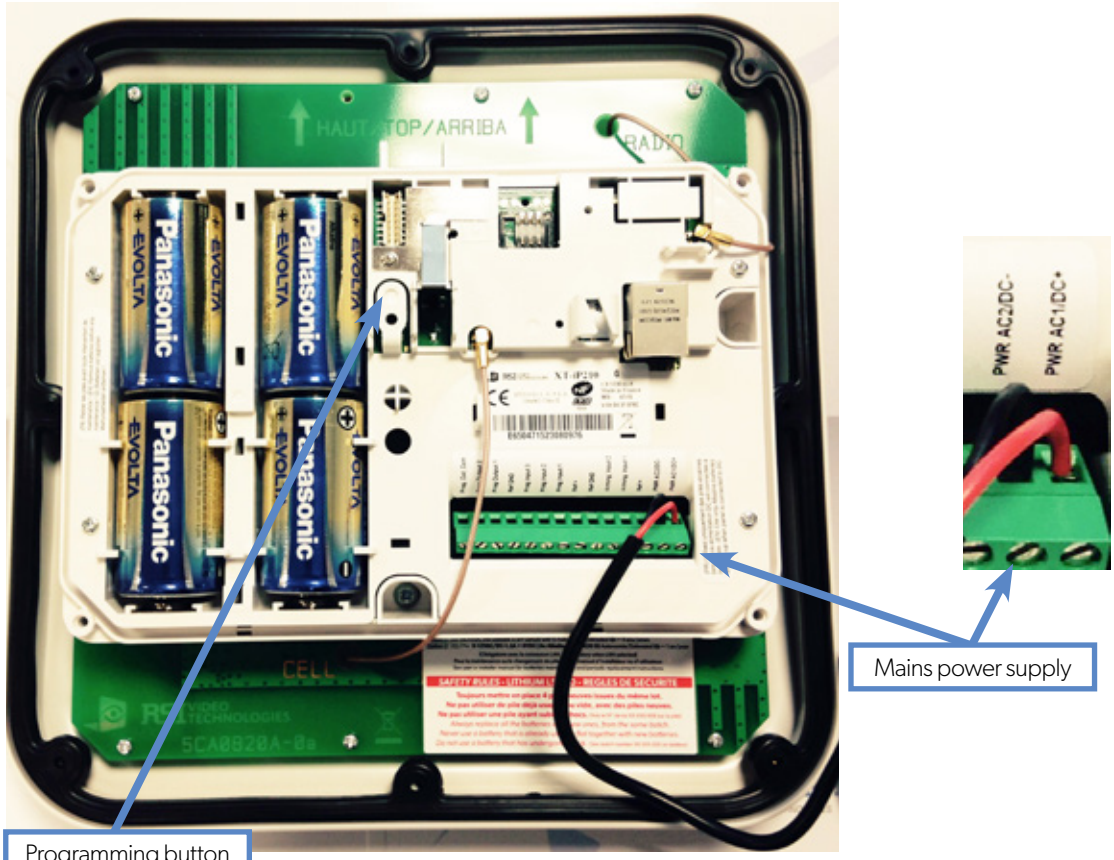


The four screwholes here opposite are intended to mount the bracket, the latter beeing used to attach the panel to the wall or a pole.

Mounting the panel is not required for programming.

1.4 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**.*

Option 2

- 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).
- Always replace all 4 batteries at once. Mixing new and used batteries can severely damage the panel (risk of explosion).
- 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.

1.4 Pairing the remote keypad

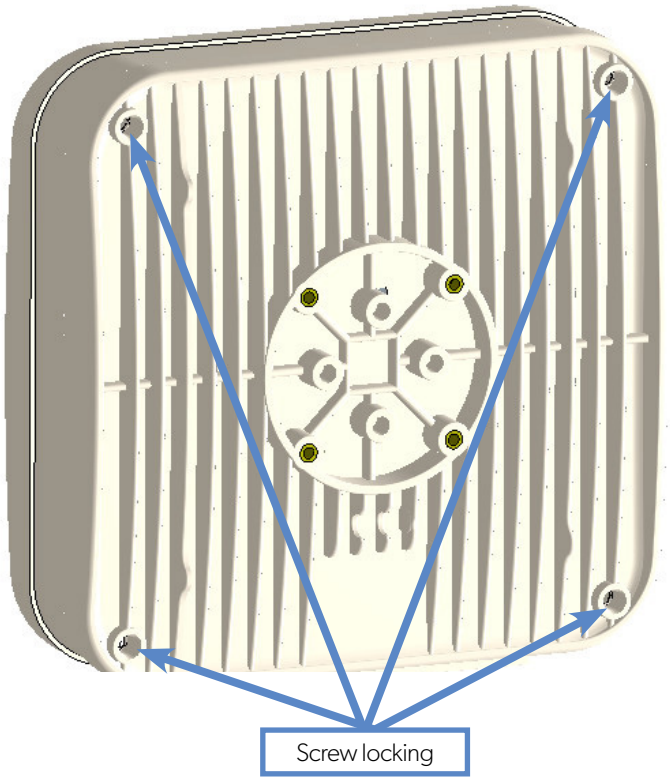
- Press the XTO programming button and release for the enrollment of a programming keypad.
- Insert all **LS14500 Lithium batteries** into the keypad.
- **Do not mount the keypad.** It will display one of the following screens:

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.

1.6 Cover locking

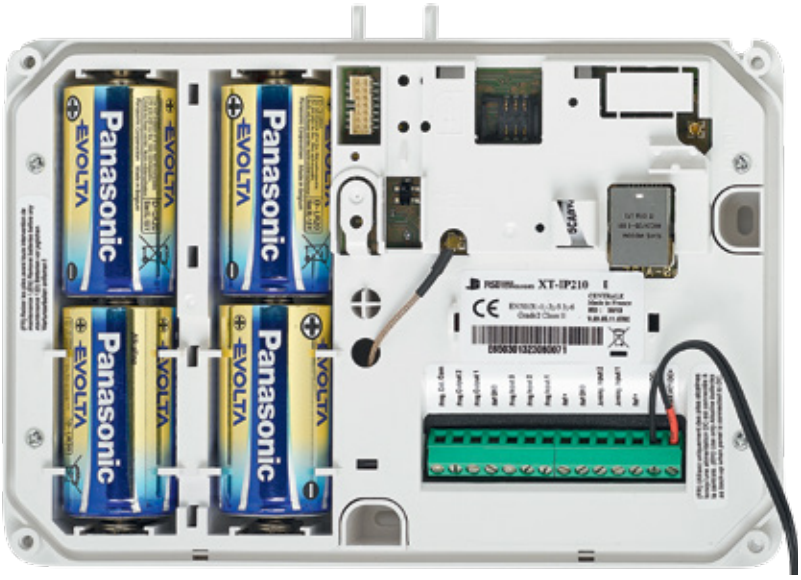
Place and screw the cover on its support.



2. XTENDER MODE

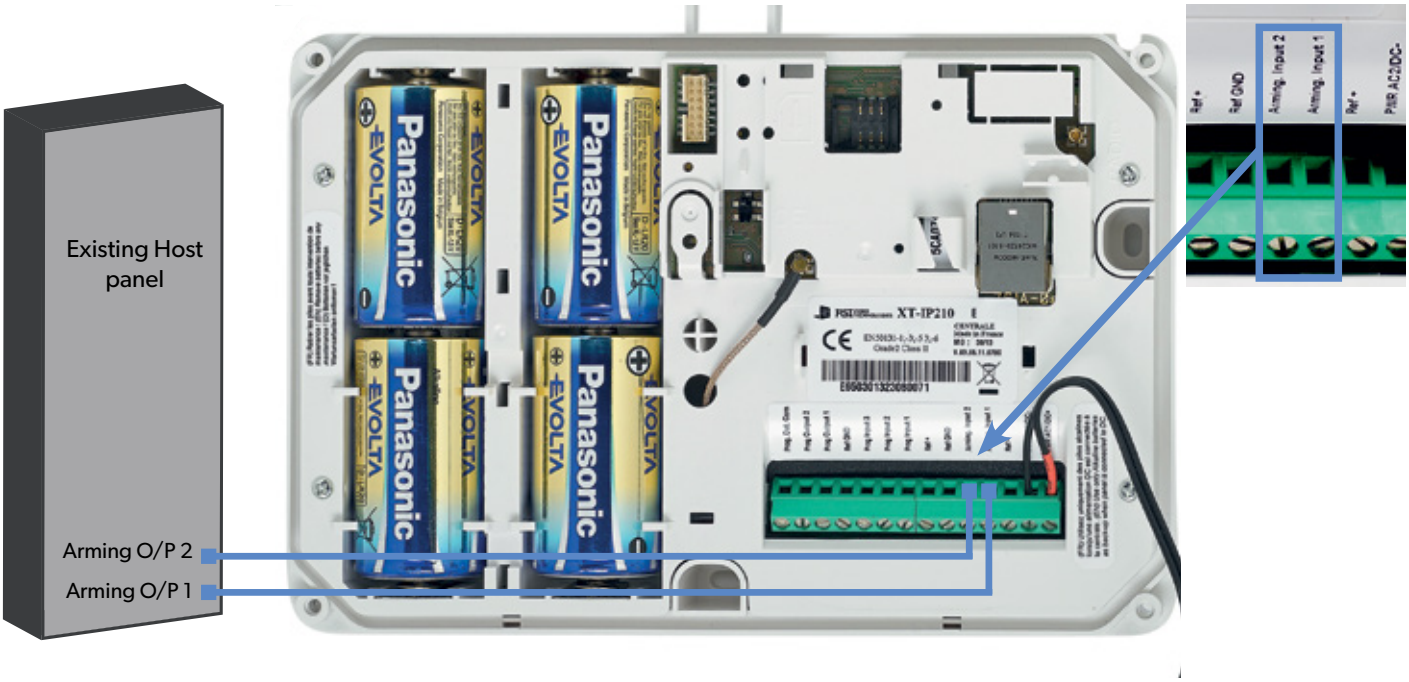
The XTO-iP panel can be used as standard standalone alarm system but it can also be connected to an existing alarm system capable of latching a 9-12Vcc* voltage used for its arming/disarming.

2.1 Standalone mode



In this functioning mode, the XTO panel works as a standard hybrid alarm system with 25 wireless peripherals and 3 programmable inputs.
It is a fully standalone alarm system.

2.2 XTENDER mode



When the XTO-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 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
KEYPAD 1 RECORDED	
OK or YES	
< - LANGUAGE : - > ENGLISH (UK)	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.
for language selection	
OK or YES	
RADIO RANGE TEST?	
OK or YES	
RF TEST x/9	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.
Please wait	
RF TEST 9/9	**Result must be 8 out of 9 or better for reliable transmission.**
OK or YES	
RADIO RANGE TEST?	
ESC NO	
INSTALLER CODE	
4 TO 6 DIGITS THEN OK/YES	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 4.5). Some codes are already used by default and therefore cannot be used.
INSTALLER CODE :	
OK or YES	
CONFIRM CODE	
OK or YES	

Keypad display

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?

ESC
NO

OK or **YES**

ACCOUNT NUMBER :

ACCOUNT NUMBER :
567001

OK or **YES**

Actions and comments

You may name the installer code using the Alphanumeric Keypad.

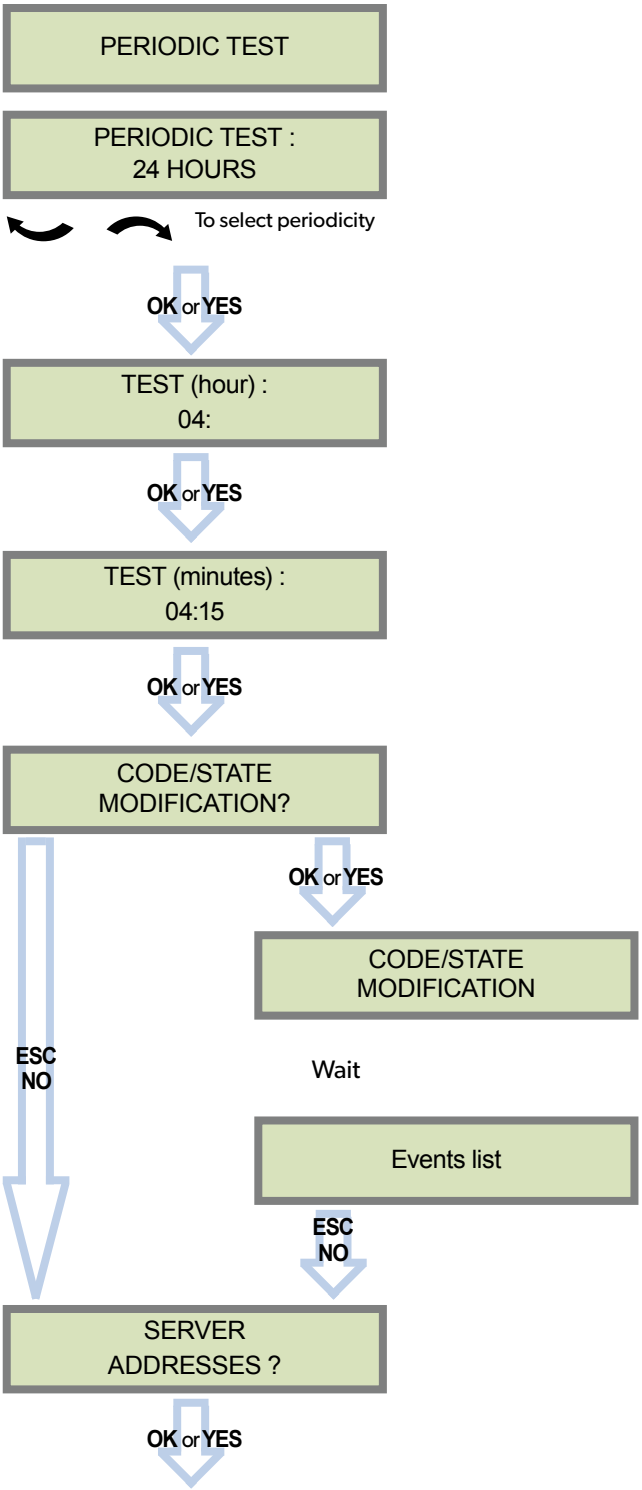
If using automatic setting (called installer default list), enter the name of the list.

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.

IP1 ADDRESS
0.0.0.0

DOMAIN NAME 1

PORT 1
888

ESC
NO

SERVER
ADDRESSES ?

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 address** or a **Domain name** but **not both**, leave the **Domain name** blank if an **IP address** 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).

ESC
NO

STRATEGY:
ETH+2G3G

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.

OK or YES

2G3G
PARAMETERS ?

OK or YES

APN CODE
internet-entrepr

USER NAME
orange

PASSWORD
orange

ESC
NO

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.

2G3G
PARAMETERS ?

ESC
NO

2G3G LEVEL ?

OK or YES

TEST IN PROGRESS
END = OK/YES

2G3G LEVEL
5/5

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 6 : 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.

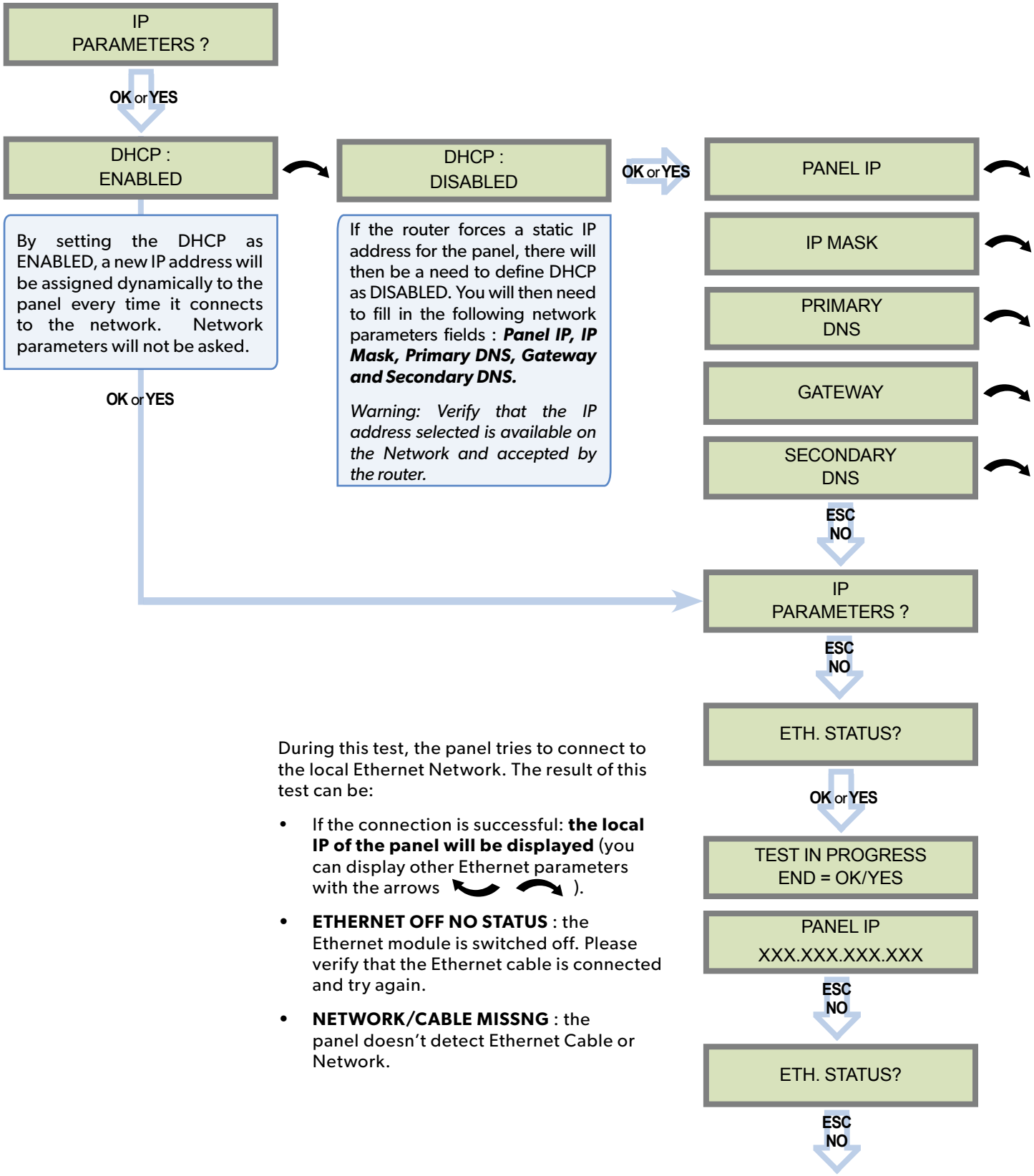
IMPORTANT : Videofied will require a 3/5 grade or better for reliable transmission of Video alarms.

OK or YES

2G3G LEVEL ?

ESC
NO

ETHERNET parameters configuration



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

- If the connection is successful: **the local IP of the panel will be displayed** (you can display other Ethernet parameters with the arrows).
- **ETHERNET OFF NO STATUS** : the Ethernet module is switched off. Please verify that the Ethernet cable is connected and try again.
- **NETWORK/CABLE MISSNG** : the panel doesn't detect Ethernet Cable or Network.

COMPATIBILITY
EN 50131 NORMS ?

OK or YES — ESC NO

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

Otherwise, press **ESC NO.**

AREAS CONFIGURATION

OK or YES

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 4.4.

AREA 1 NAME :

OK or YES

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

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

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

ARMING PROFILE :
STANDALONE

ARMING PROFILE :
FROM THE HOST

Please go to page 14 if you chose **FROM THE HOST**

OK or YES

EXIT DELAY :
45 sec

For the selection

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

OK or YES

ENTRY DELAY :
15 sec

For the selection

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

Please go to page 15 if you chose **STANDALONE**

XTENDER mode configuration

ARMING PROFILE :
FROM THE HOST

OK or YES

ARMING MODE

MODE :
SLOW

MODE :
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.

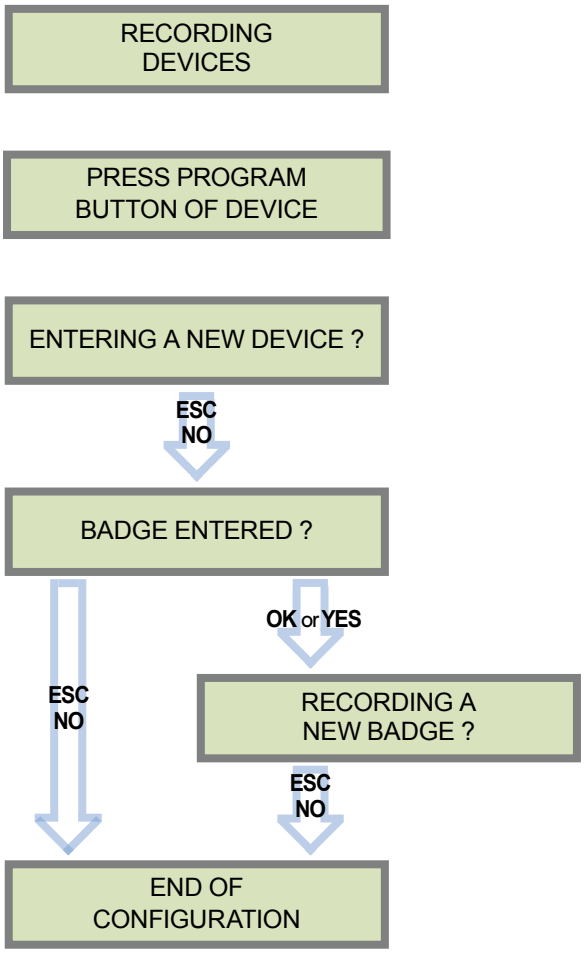
Enter the value you would like for the Transmission Delay and press **OK or YES.**

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

3. XTO-IP PANEL PROGRAMMING



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.

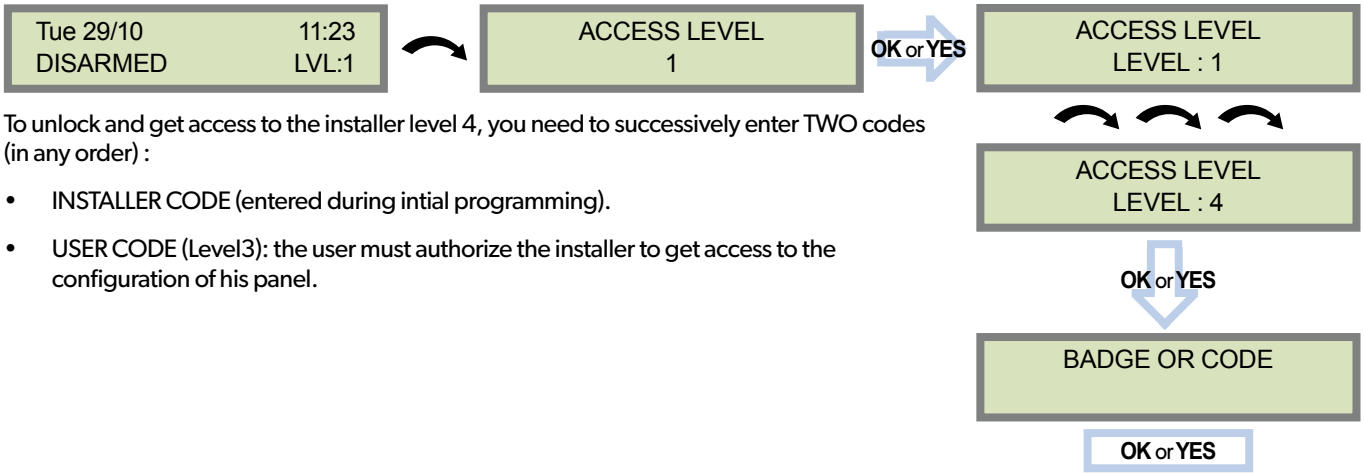
If you wish to use an user code, please skip this step and when initial programming is completed go to the BADGES/ACCESS CODES menu (please refer to chapter 4.5 for further details).

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

Before completing programming make sure that no device is tampered. Each device must be closed and its LED indicator shall be turned 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



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.

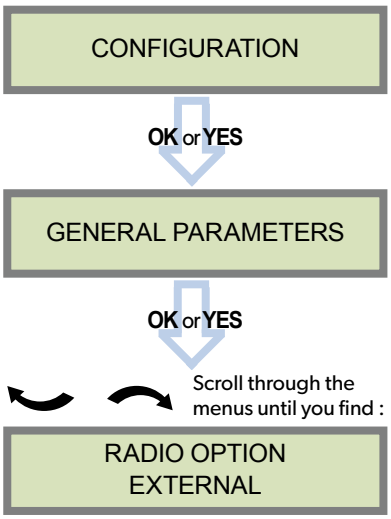
4.2 How to Arm/Disarm the System

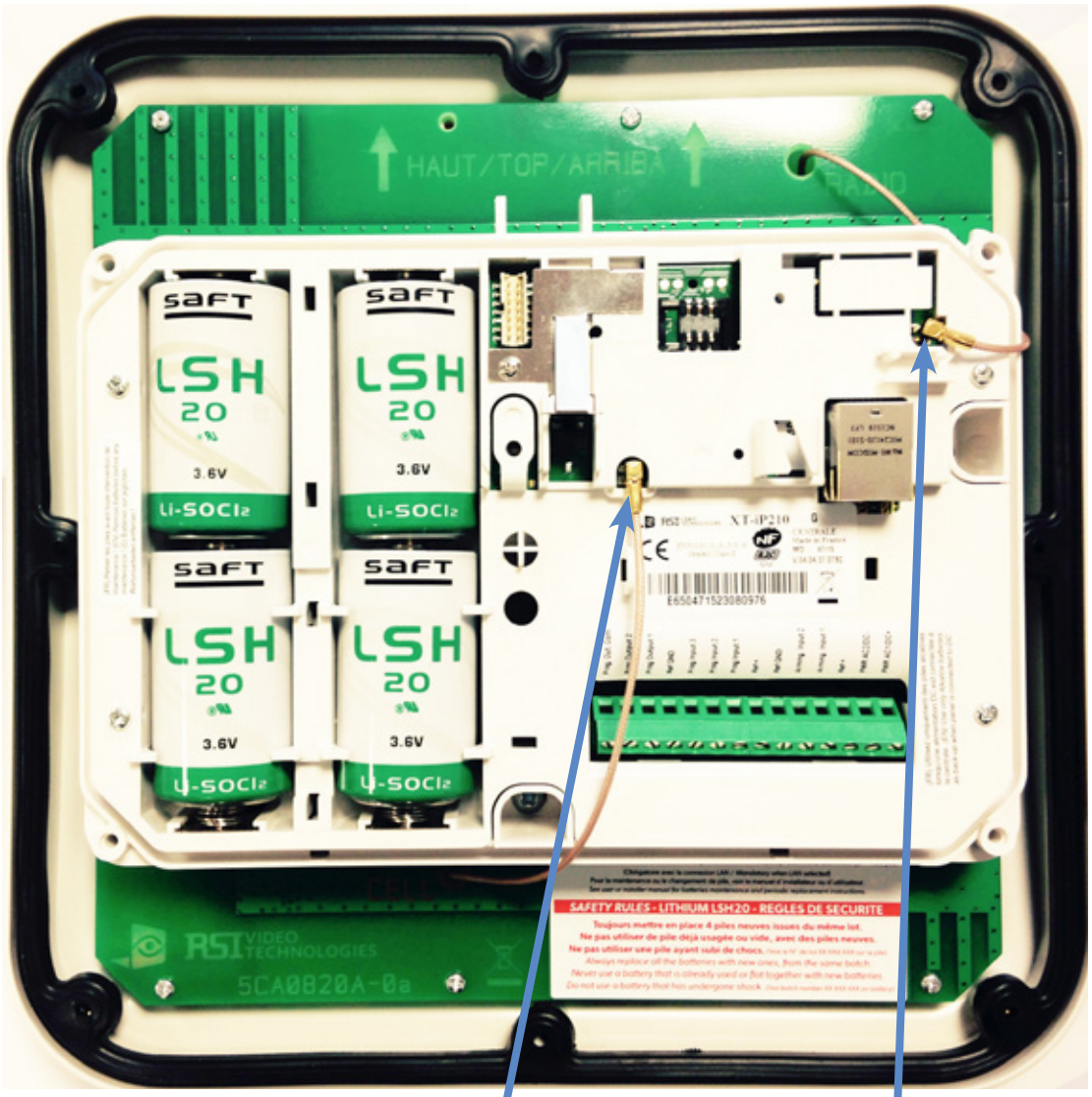
When in standby mode, the system can be armed with the remote keypad, the remote keyfob and/or the remote badge reader.

	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 / press **OK or YES** and enter your user code
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) > S**PECIAL 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** oe **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

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

Up to 19 codes (or badges) can be registered into the panel with the engineer code.

A code has 4 to 6 digits (0 to 9).

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

Those codes are used for maintenance or as panic/duress codes.

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 user codes +1
All user codes +2
All user codes -1
All user codes -2

When a code is created (1000 for example), the 2 next codes and previous codes (0998, 0999, 1001 and 1002) will be automatically reserved.

The +1 code (1001) is used for disarming under duress.

The +2 code (1002) is used for panic.

The -1 and -2 codes (0998 et 0999) are reserved to prevent conflicts when creating a new user code.

4.6 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

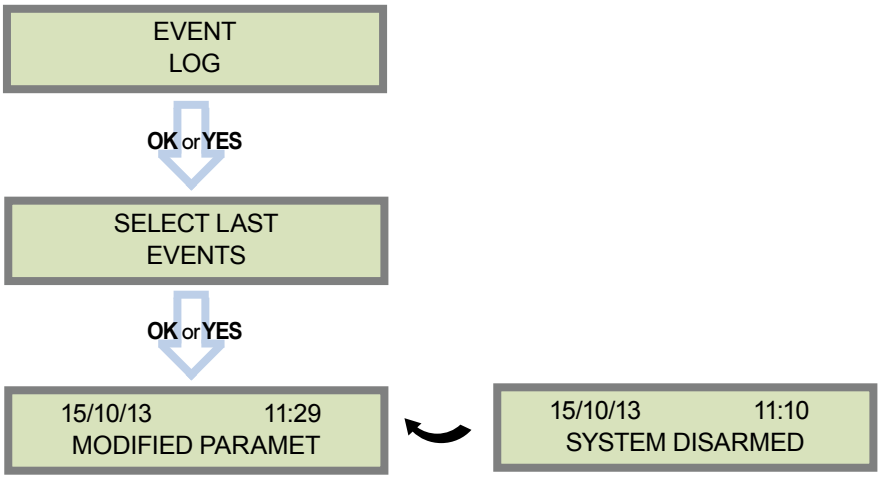
< = = = = XX = = = = >

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

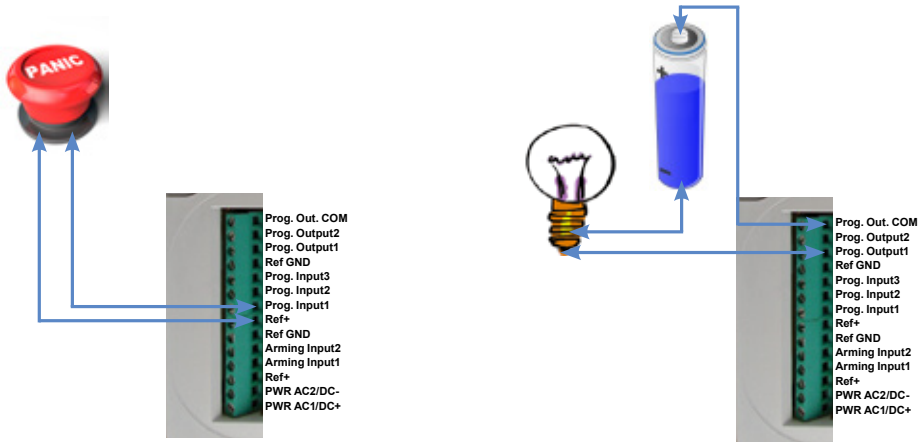
4.8 Programmable inputs and outputs

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.



IMPORTANT :

Ces sorties ne peuvent connectées qu'à des circuits Très Basses Tension de Sécurité (TBTS) soit au maximum 30VAC ou 60VDC.

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

4.9 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 Videofied (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.

5. ETHERNET PARAMETERS

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 (LVL 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.

6. TRANSMITTED EVENTS LIST

The XTO-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
AC POWER LOSS (AC Power supply)

The following events are not sent by default :
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:**

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** > **MONITORING PARAMETERS** > **EVENT TRANS. MODIFICATION**

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

7. 2G3G ERROR CODES

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 *-> 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

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.

FCC Regulatory Information for USA and CANADA

FCC Part 15.21 Changes or modifications made to this equipment not expressly approved by RSI Video Technologies may void the FCC authorization to operate this equipment.

FCC Part 15.105 Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference

to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

> Reorient or relocate the receiving antenna.
> Increase the separation between the equipment and receiver.
> Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
> Consult the dealer or an experienced radio/TV technician for help.

Radio frequency radiation exposure information according 2.1091 / 2.1093 / OET bulletin 65

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé.
Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada.
Operation is subject to the following two conditions:

1 This device may not cause harmful interference, and
2 This device must accept any interference received, including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes:

1 L'appareil ne doit pas produire de brouillage, et
2 L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

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.*

STANDARDS & CERTIFICATIONS

868MHz (XTO-iP 210)

Compliant with the annex IV from the R&TTE 1999/5/CE Directive

915MHz (XTO-iP 630)

USA FCC (Part 15C , 22H, 24E and 27)
Canada IC (RSS-210 Issue 8, RSS-132, RSS-133 and RSS-139)

920MHz (XTO-iP 730)

Australia C-Tick
(AS/NZS4268, , AS/CHS42 and AS/NZS 60950)

This symbol on the product or on its packaging indicates that this product should not be treated as household waste. It must be handed over to the applicable collection point for the recycling of electrical and electronic equipment. By ensuring this product is disposed of correctly, you will help prevent potential negative consequences for the environment and human health. The recycling of materials will help to conserve natural resources. For more information about recycling of this product, please contact your local municipality, your waste disposal service or the company that installed the product.

The EC declaration of conformity of this product is available by flashing this QR code.

ELECTRICAL DATA

Power requirements (option 1)	
Power supply Type B	9-12VDC / 1,2A
Low voltage limit	5.15 V
Backup	6V with 4 x 1,5 V D Alkaline batteries /LR20
Low battery limit	4.2 V
Battery life (average)	1 year
Average current consumption	450µA (over 1h)
Max current	1.2 A
Power supply (option 2)	
Power supply Type C	14,4V with 4x3,6V Lithium batteries /LSH20
Low battery limit	12 V
Battery life (average)	4 years

RF S2View® technology	
Radio type	Bidirectional RF
Operating frequency	868MHz - XTO-iP 210 (Europe, South Africa, Asia) 915MHz - FHSS - XTO-iP 620 (USA, Canada, South America) 920MHz - FHSS - XTO-iP 730 (Australia, South America)
Transmission security	AES encryption algorithm
Radio jam detection	Yes
Supervision	Yes
Radio Antenna	integrated
External RF antenna	Yes via MMCX connector

Tamper	
Autoprotection	Cover tamper

Programmable wired inputs	
Number	3
Input voltage	12 V_{DC} (15 V_{DC} max)

Programmable wired outputs	
Number	2
Max switching voltage	24V_{DC} /30V_{AC}
Max switching current	1 A
Max switching power	30 W

TRANSMISSION

Communicator	
Communicator type	2G3G/Ethernet
Security protocol	Frontel
IP stack	TCP/IP
Video transmission	By Frontel protocol to central monitoring station or App servers
2G3G Antenna	Integrated
External 2G3G antenna	Yes via MMCX connector

Video	
Video Format	WMV or MPEG
Images per second	5
Image size	320x240 or 640x480 pixels
Video length	4 to 12 seconds

Miscellaneous	
Programming	Keypad
Max number of devices	24
Max number of codes/badges	19
Arming modes	4
Areas	4
Event log	4000 events stored on flash memory
Events memory storage delay	Infinite

BOX

Physical and Environmental Data	
Operating temperature	-28°/+60°C
Maximum relative humidity	95%, sans condensation
International Protection Marking	IP65 / IK06
Material	ABS—ULV0

Installation / Mounting	
Control panel / Base	4 screws to close the cover 4 screws on panel base for brackets mounting

Dimensions	
Panel	272 mm x 276 mm x 96mm

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