videofied
Made by RSI VIDEO TECHNOLOGIES

XTO-IP 240/740 LTE-M Control Panel

INSTALLATION MANAL

DOC. - REF. 230-XTO-IP
MODIF. DATE : FEBRUARY 2016
FIRMWARE VERSION : XLP.04.04.00.XXX AND LATER

Description

The XTO-IP is a fully wireless alarm system. It is powered by standalone Lithium batteries. 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.

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.

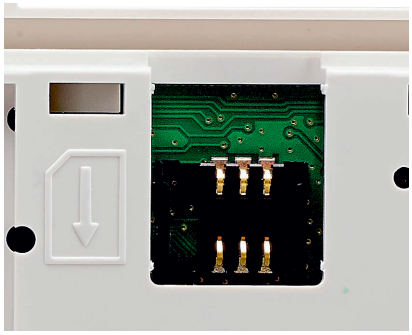
The jamming detection feature identifies any intentional jamming from a third party. On the other hand, the supervision feature consists of transmitting signals between every device of the system and the alarm panel XTO-IP. Through the supervision, the detectors transmit every 8 minutes a presence signal.

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

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 the bracket, the latter beeing used to attach the panel to the wall or a pole.

Mounting the panel is not required for programming.

1.3 Powering and initialization

- The panel is powered either with **4 LSH20 Lithium batteries**.
- 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

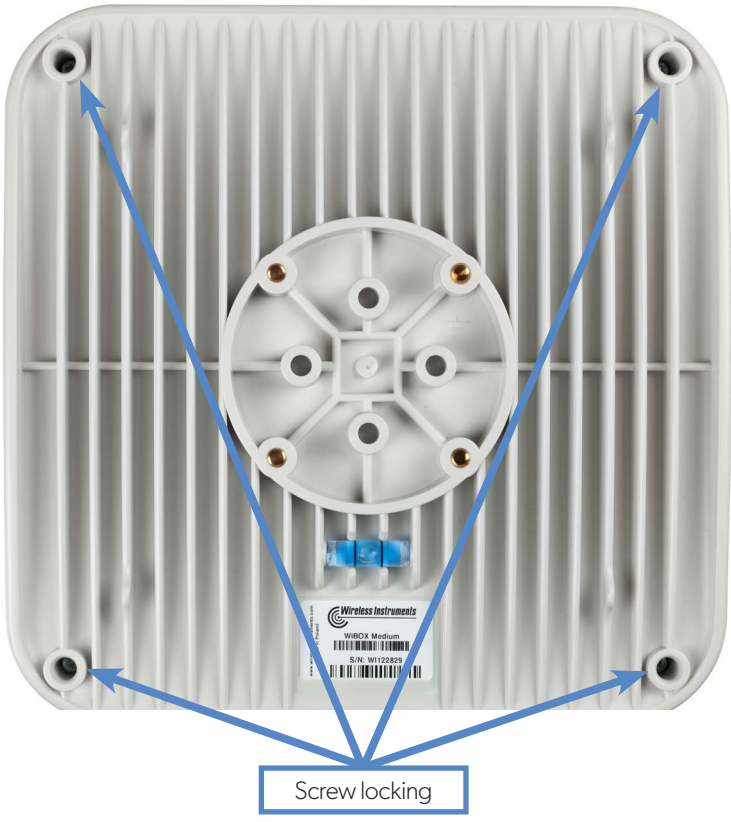
- Press the XTO programming button and release for the enrollment of a programming keypad.
- Insert all **LS14500 Lithium batteries** into the keypad.
- **Do not mount the keypad.** It will display one of the following screens:

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.

1.5 Cover locking

Place and screw the cover on its support.



Keypad Display

KEYPAD 1
RECORDED

OK or **YES**

< - LANGUAGE : - >
ENGLISH (UK)

for language selection

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**

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 rules for codes (Chapter 4.5). Some codes are already used by default and therefore cannot be used.

Keypad display

Actions and comments

You may name the installer code using the Alphanumeric Keypad.

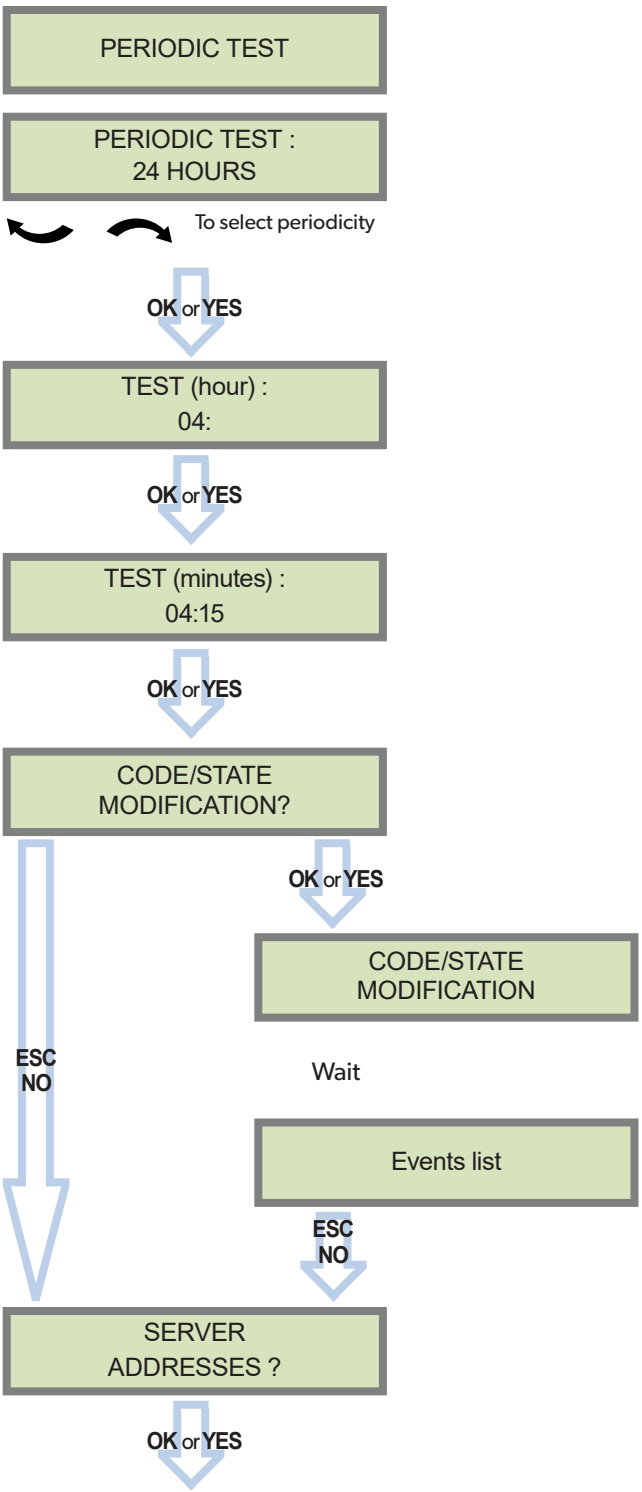
If using automatic setting (called installer default list), enter the name of the list.

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.

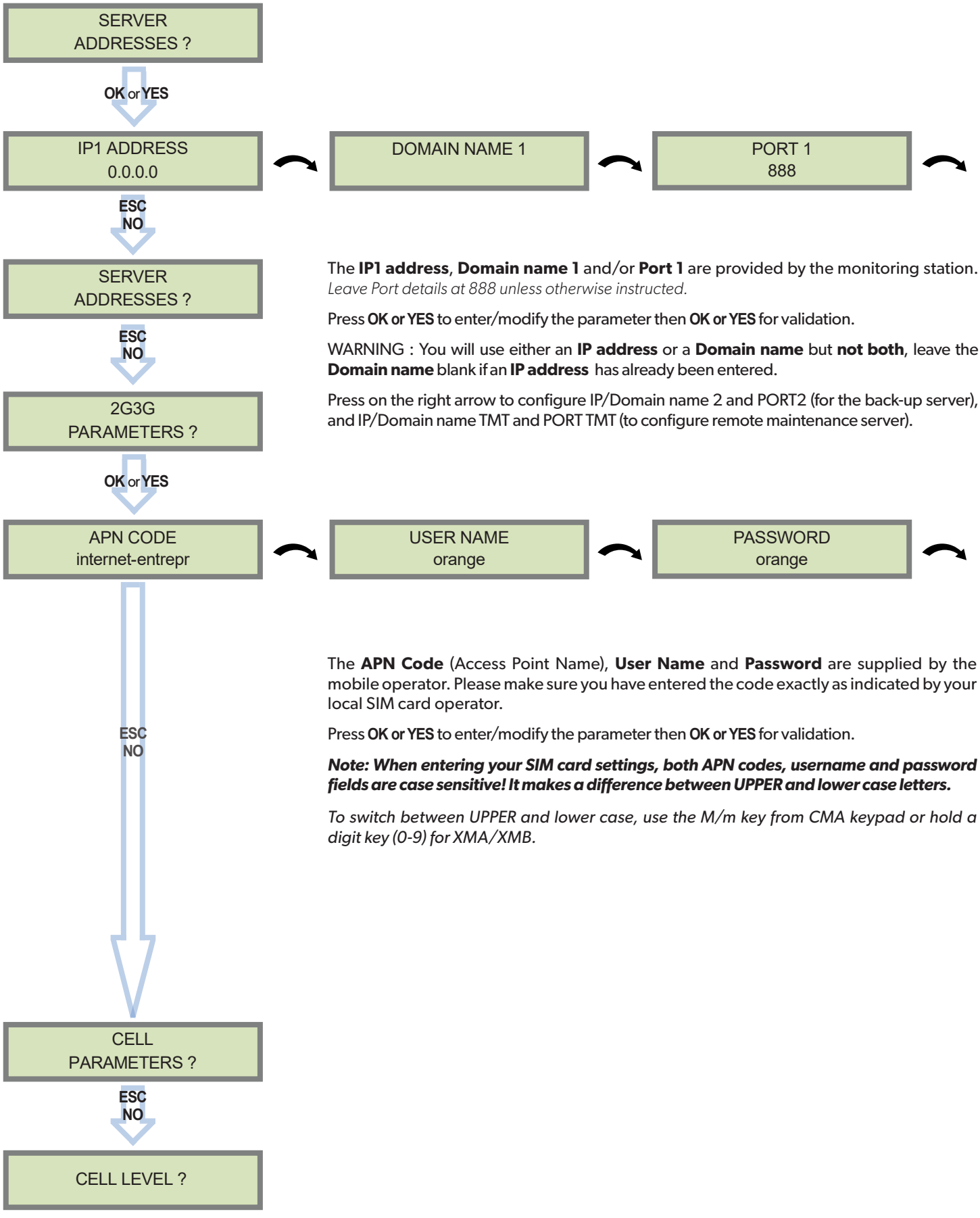
The CODE/STATE MODIF. menu is to configure the transmitted events to the monitoring station, use the arrow keys to toggle between events and **OK or YES** to modify.

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.



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.

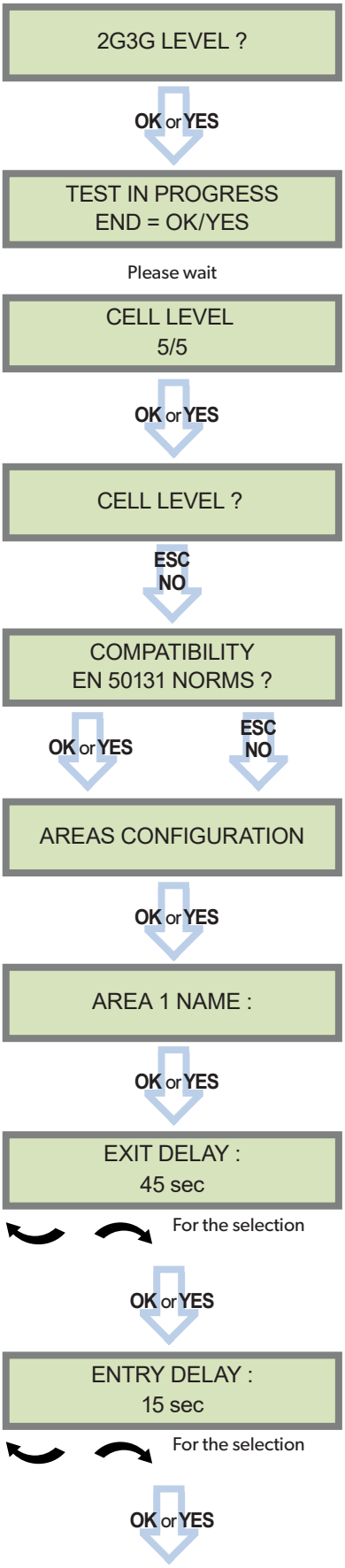
Press on the right arrow to configure IP/Domain name 2 and PORT2 (for the back-up server), and IP/Domain name TMT and PORT TMT (to configure remote maintenance server).

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 CELL test completed, the keypad will display one of the following results :

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

- A Cellular Error code (please see Chapter 6 : CELL 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** ou **CLR**.

The CELL 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.

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

Otherwise, press **ESC NO**.

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

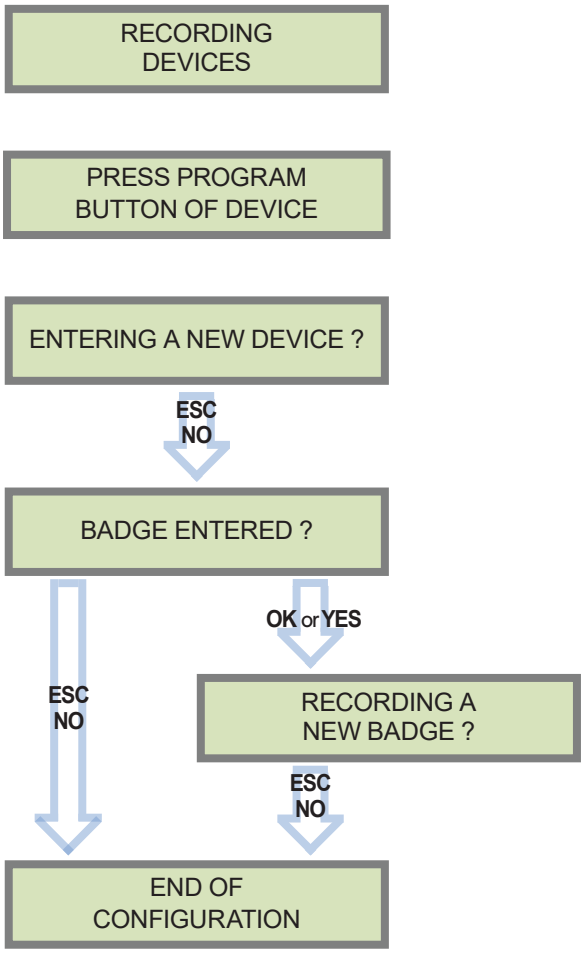
Enter the name of the area 1 and **OK or YES**.

Repeat the procedure for areas 2,3 and 4.

For further details, please refer to chapter 4.3.

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

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



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.

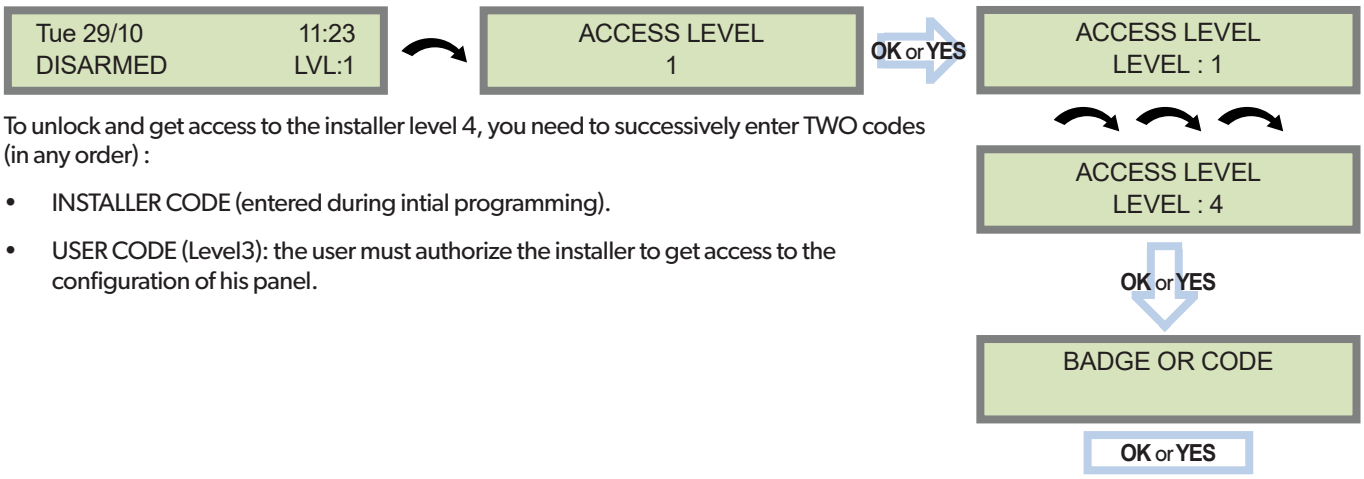
If you wish to use an user code, please skip this step and when initial programming is completed go to the BADGES/ACCESS CODES menu (please refer to chapter 4.5 for further details).

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.

3.1 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.

3.2 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 1 / enter your user code and press **OK or YES**	Press 2 / 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 1	Press 2

3.3 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 — 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

3.4 Manage badges and access codes

Access Level

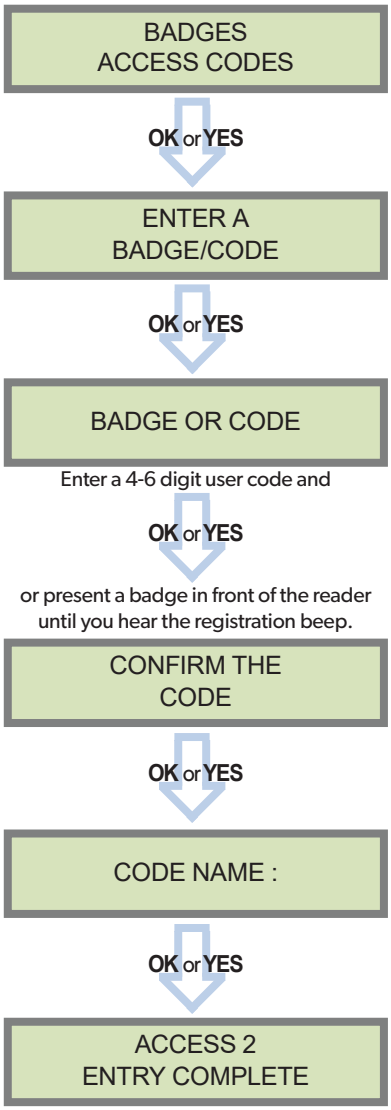
Access Level	Definition & Rights
LVL 1	Standby Level
LVL 2	**Restricted USER level,** where it is only possible to arm/disarm the system.
LVL 3	**USER level,** where it is possible to arm/disarm the system, check the event log, test the devices. Modifications of the settings are not possible at this 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 create the first **Level 3** access code only.

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

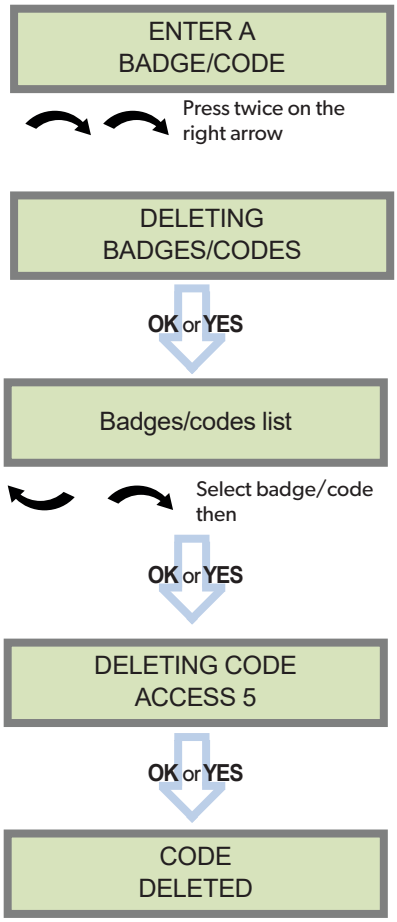
How to return to the LVL1?

- 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

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.

3.5 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

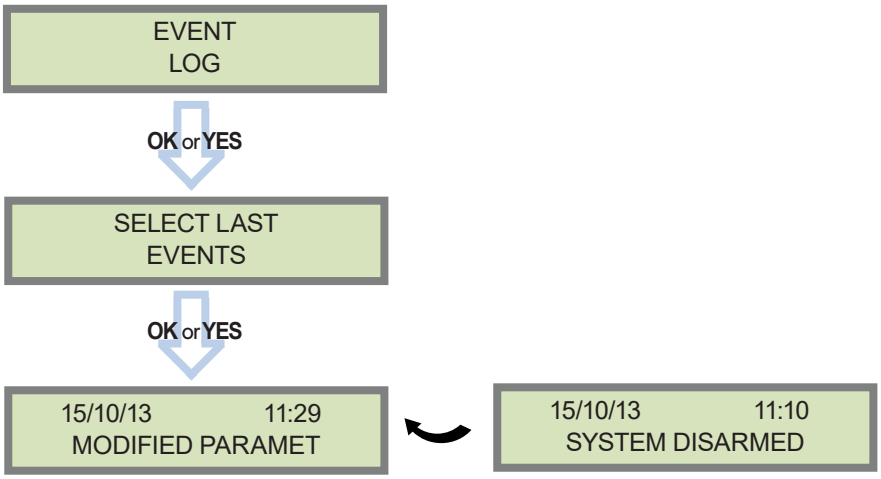
< = = = = XX = = = = >

You can now remove the batteries from the device

3.6 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.



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

3.7 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.

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.

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.

CELL LEVEL :
ERROR XXX

In case of Cellular errors during initial programming, we strongly suggest to continue with the installation and perform the CELL 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 CELL 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 CELL 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 CELL Network:**

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

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 supply	
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 240 (Europe, South Africa, Asia) America) 920MHz - FHSS - XTO-IP 740 (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

STANDARDS & CERTIFICATIONS

XTO-iP240	
Compliant with the annex IV from the R&TTE 1999/5/CE Directive	
XTO-iP740	
Australia A-Tick (AS/NZS4268, AS/CHS42 & AS/NZS 60950)	

TRANSMISSION

Communicator	
Communicator type	2G, 4G LAN Ethernet (240) 4G LAN Ethernet (740)
2G frequencies	850 / 900 / 1800 / 1900 MHz
4G frequencies	2100(B1), 1800(B3), 900(B8), 800(B20), 700(B28)(XTO-IP 240) 2100(B1), 1800(B3), 850(B5), 900(B8), 700(B28) (XTO-iP 740)
Security protocol	Frontel
IP stack	TCP/IP
Video transmission	By Frontel protocol to central monitoring station or App servers
Cellular Antenna	Integrated
External Cellular 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	-25°/70°C
Maximum relative humidity	95%, sans condensation
International Protection Marking	IP54 / 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

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.

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

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