

INSTALLATION MANUAL

Doc. - Ref. R800-27467A

Last modification date : July 2022

Firmware version : XLP.04.10.09.80078C XT-IP240 and later



Description

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

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

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

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

Technology

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

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

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

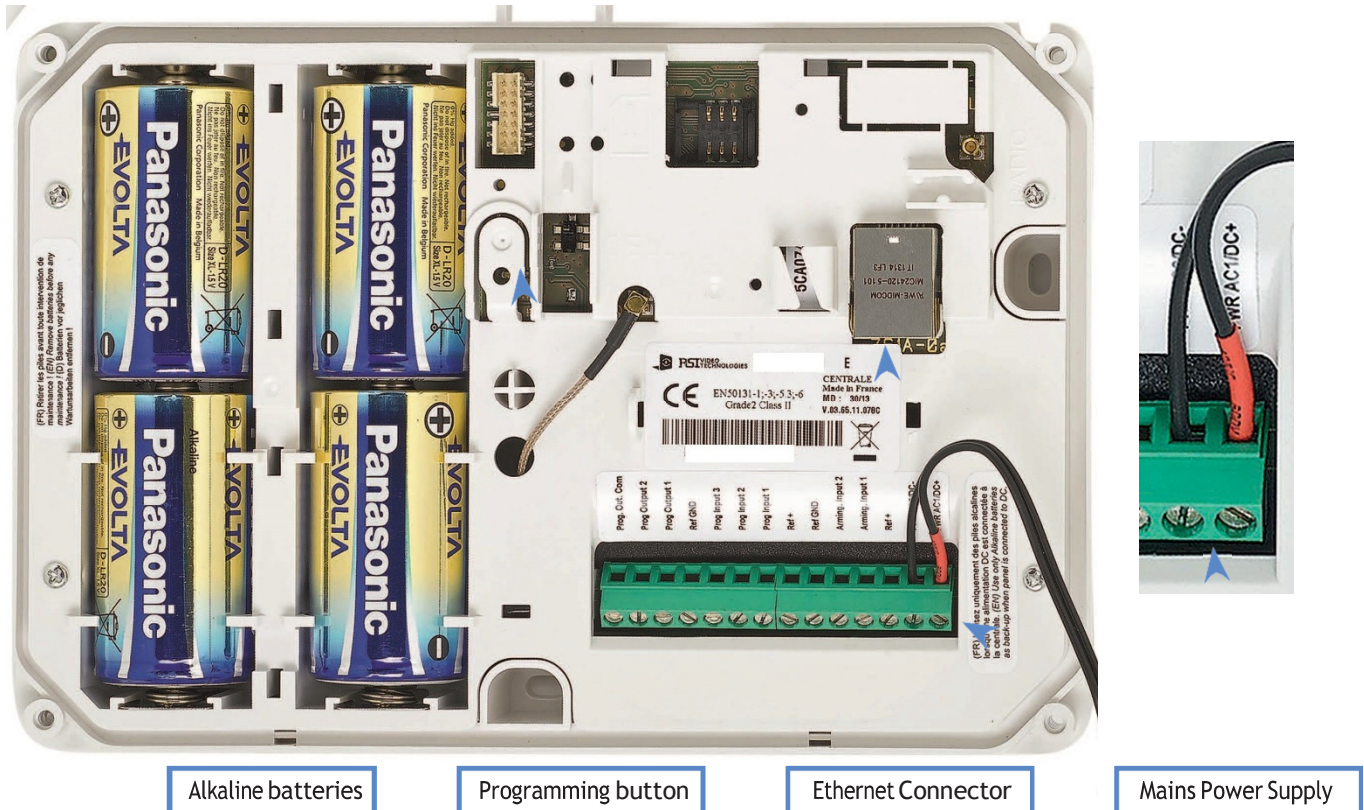
The jamming detection feature identifies any intentional jamming from a third party. On the other hand, the supervision feature consists of transmitting signals between every device of the system and the alarm panel XT-IP. Through the supervision, the detectors transmit every 8 minutes a presence signal.

When ETH + CELL is chosen for communication the system employs a strategy to alternate attempts to connect to the Primary and Secondary Central Station Receiver between Ethernet and Cellular communication. Each method will attempt reporting to the Primary Receiver twice followed by the Secondary Receiver twice. This sequence is repeated once for a total of 8 attempt to each receiver before the system attempts no additional communication for the current event. A new event during or after this sequence will restart the attempts from the beginning.

Introduction.....	2
Summary.....	3
1. XT-IP Panel setup.....	4
1.1 RJ45 cable connection.....	4
1.2 SIM card installation.....	4
1.3 Panel mounting.....	5
1.4 Powering and initialization.....	6
1.5 Pairing the remote keypad.....	6
2. XTENDER Mode.....	7
3. XT-IP Panel programming.....	8
ETHERNET parameters configuration.....	12
XTENDER mode configuration.....	14
4. XT-IP features guide.....	16
4.1 Get to access level 4.....	16
4.2 How to Arm/Disarm the system.....	16
4.3 Arming and Siren Mode Configuration.....	17
4.4 Manage badges and access codes.....	18
4.5 Delete the keypad or any other device.....	20
4.6 Read the event log.....	21
4.7 Programmable inputs and outputs.....	21
4.8 Golden rules.....	22
5. Ethernet parameters.....	23
6. Transmitted events list.....	24
7. Cell error codes.....	25
8. Technical specification and security notes.....	26

1.4 Powering and initialization

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



Providing that **Ethernet connectivity is not used**, the XT-IP panel can be powered by 4 LSH20 Lithium, instead of mains power supply with alkaline backup batteries.

1.5 Pairing the remote keypad

- Press briefly the XT-IP programming button and release for the enrollment of a programming keypad. The indicator LED will blink once.
- Insert all 3 **LS14500 Lithium batteries** into the keypad.
- Do not mount the keypad. It will displays one of the following screens:

RSI (c) 2013
videofied.com

or

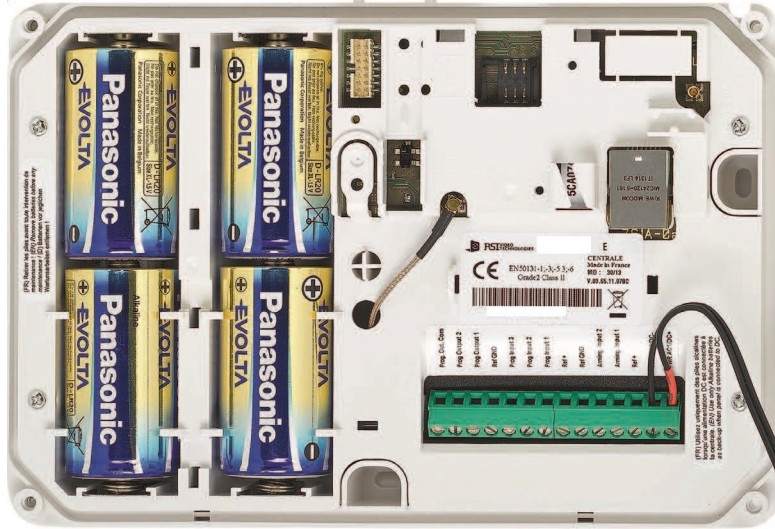
←-----XX-----→

- **Press on both CLR and ESC NO keys at the same time** and release. The indicator LED on the keypad will blink rapidly. Wait for the keypad to pair.
- **If the keypad doesn't pair up with the panel** and shows «XX», it certainly means that it is still paired to another system and needs to be reset. Take the batteries out, and press repeatedly on the keypad tamper switch for 30 sec to 1 minute. Then proceed to the above steps.



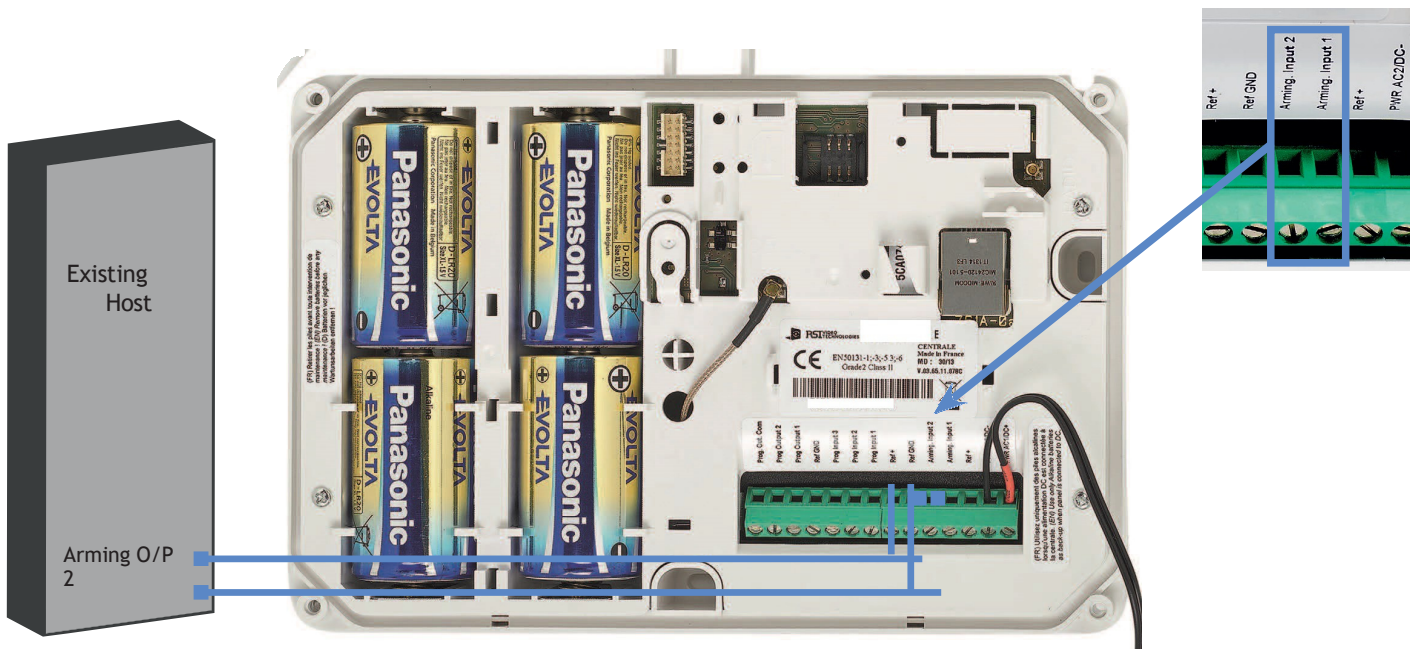
The XT-IP panel can be used as standard standalone alarm system but it can also be connected to an existing alarm system capable of latching a 9-12Vcc* voltage used for its arming/disarming.

2.1 Standalone Mode



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

2.2 XTENDER Mode (From the host)



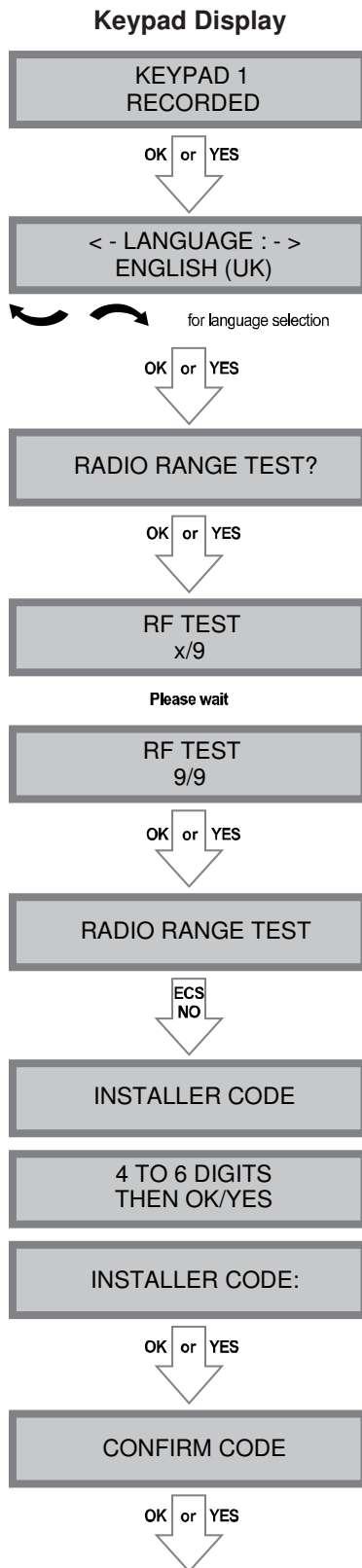
When the XT-IP panel is used in XTENDER mode, the system will only be able to arm and disarm by latching 9-12Vcc to its arming inputs Arming Input 1 and/or Arming Input 2.

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

On a programmed panel, you can choose between standalone and XTENDER modes from the menu:
CONFIGURATION (LVL 4) > GENERAL PARAMETERS > XTENDER

**When using an XT-IP in XTENDER mode, the panel must be powered by the mains power supply.*

The XT-Series control panels include a Scheduling feature capable of auto-arming and disarming the system following a seven day revolving schedule for the specified days and times. Refer to the Scheduling Feature Manual p/n R800-27841 for additional information and Programming instructions.



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 3.4). Some codes are already used by default and therefore cannot be used.

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?

OK or YES

ESC
NO

ACCOUNT NUMBER :

ACCOUNT NUMBER :
567001

OK or YES

Actions and comments

You may name the installer code using the Alphanumeric Keypad.

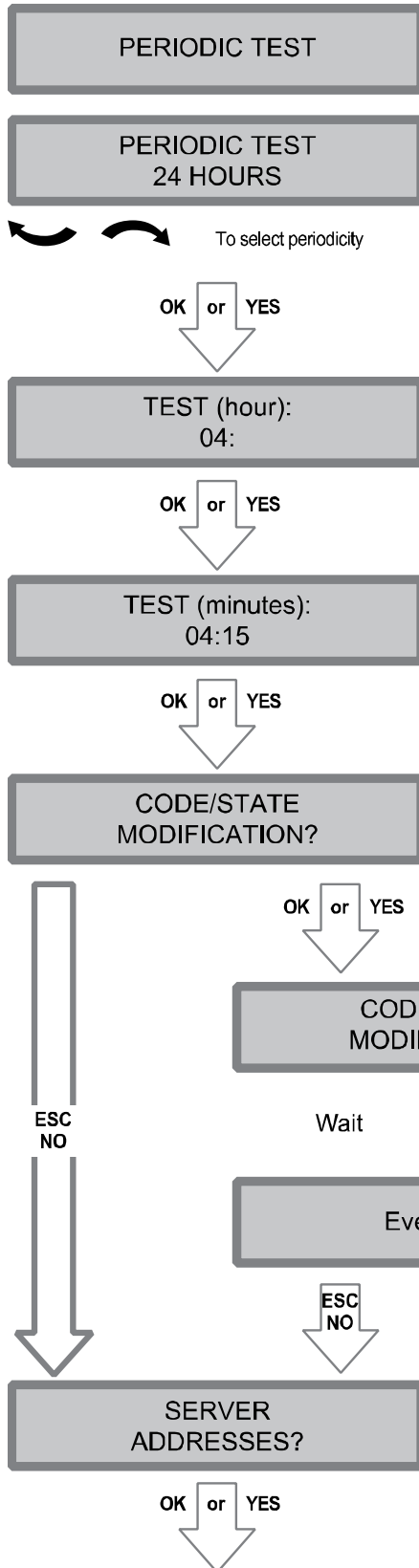
If using automatic setting (called installer default list), enter the name of the list.

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.

Note: A 24 hours periodic test call is recommended.

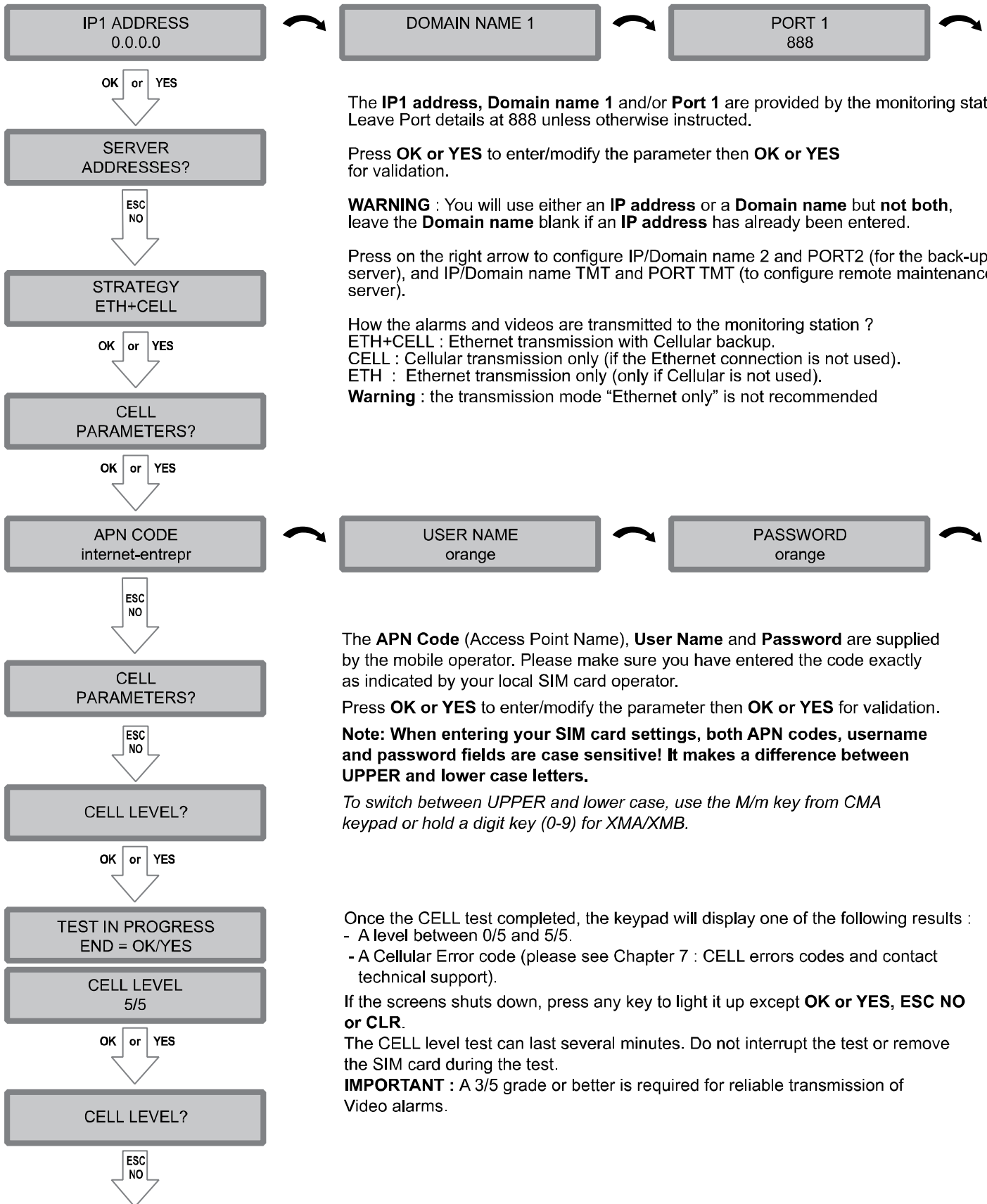
The CODE/STATE MODIF. menu is to configure the transmitted events to the monitoring station, use the arrow keys to toggle between events and **OK or YES** to modify.

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).

How the alarms and videos are transmitted to the monitoring station ?
 ETH+CELL : Ethernet transmission with Cellular backup.
 CELL : Cellular transmission only (if the Ethernet connection is not used).
 ETH : Ethernet transmission only (only if Cellular is not used).

Warning : the transmission mode "Ethernet only" is not recommended

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

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

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

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

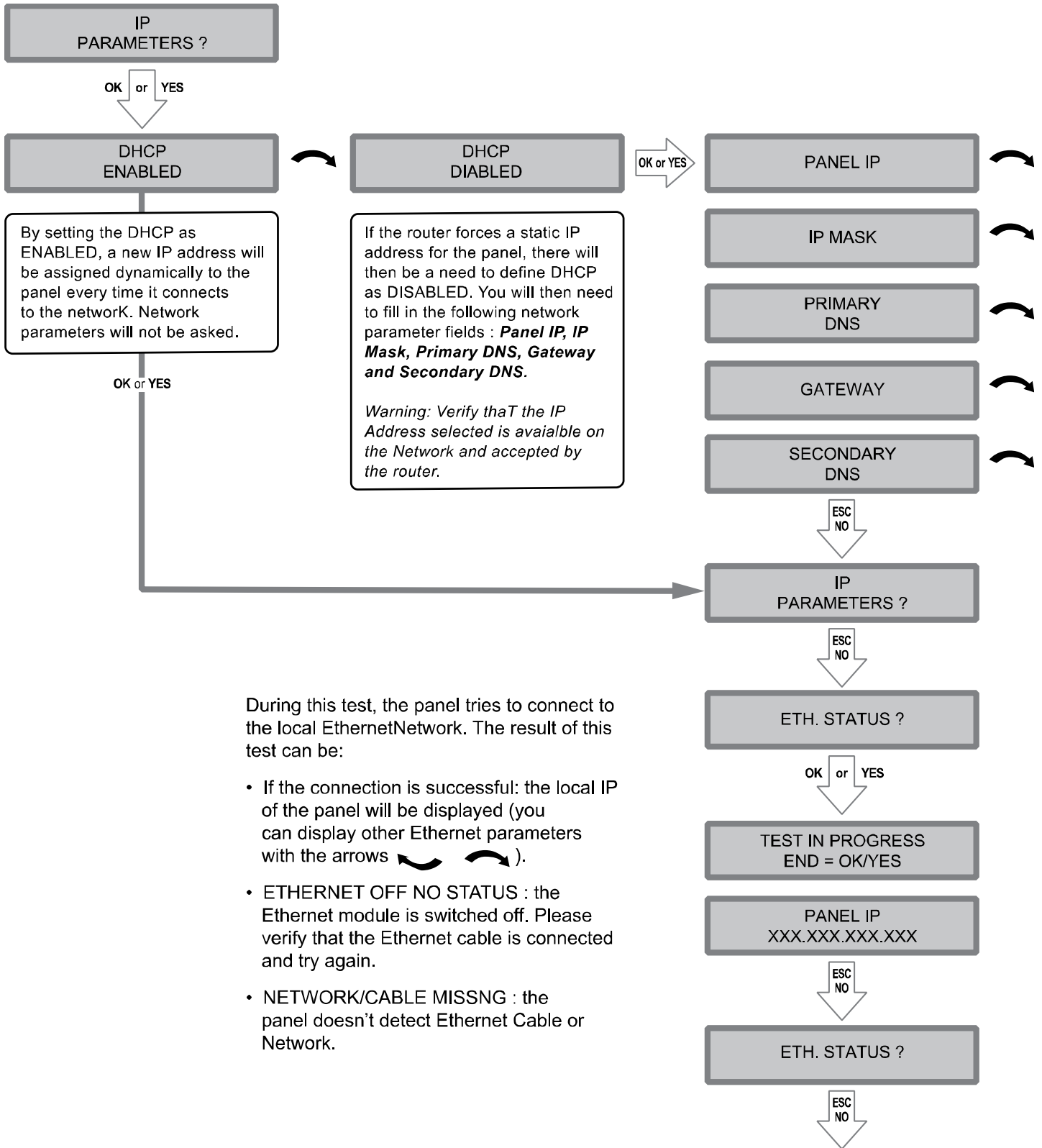
Once the CELL test completed, the keypad will display one of the following results :
 - A level between 0/5 and 5/5.
 - A Cellular Error code (please see Chapter 7 : CELL errors codes and contact technical support).

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

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

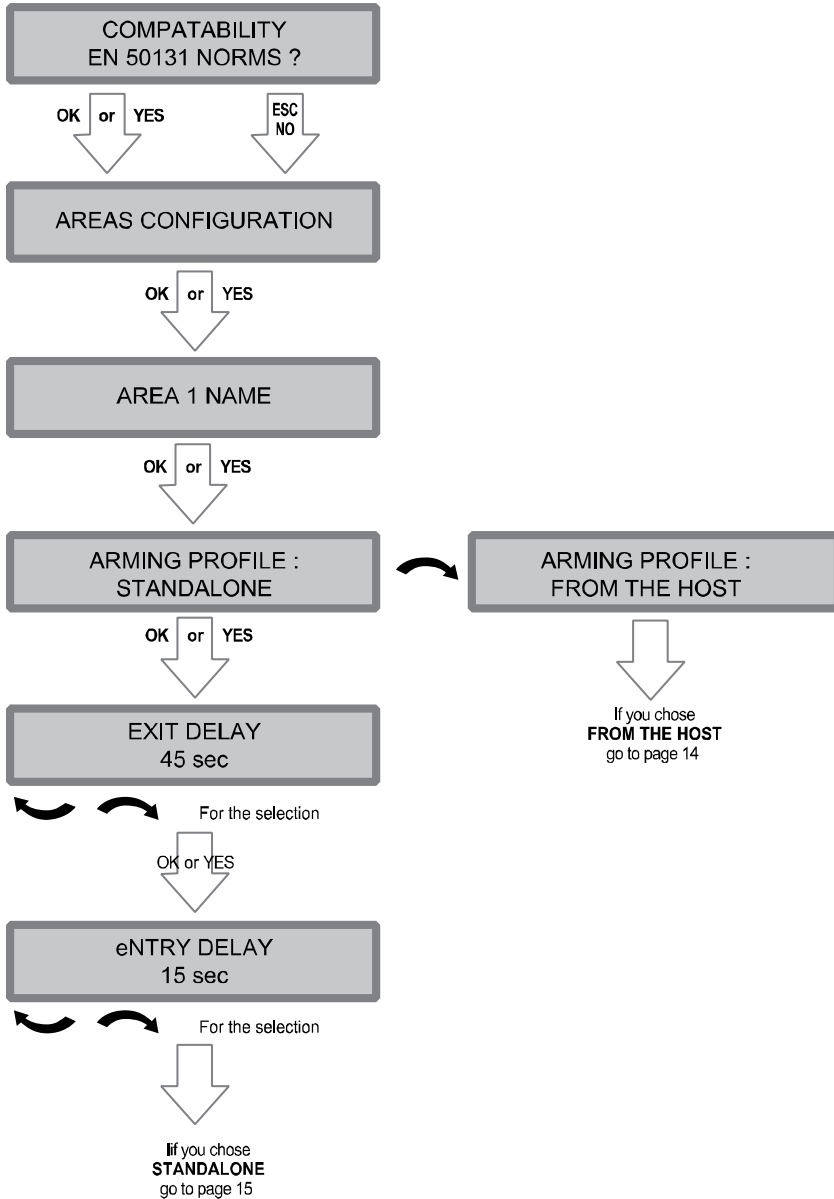
IMPORTANT : A 3/5 grade or better is required for reliable transmission of Video alarms.

ETHERNET parameters configuration



During this test, the panel tries to connect to the local EthernetNetwork. 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.



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.

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

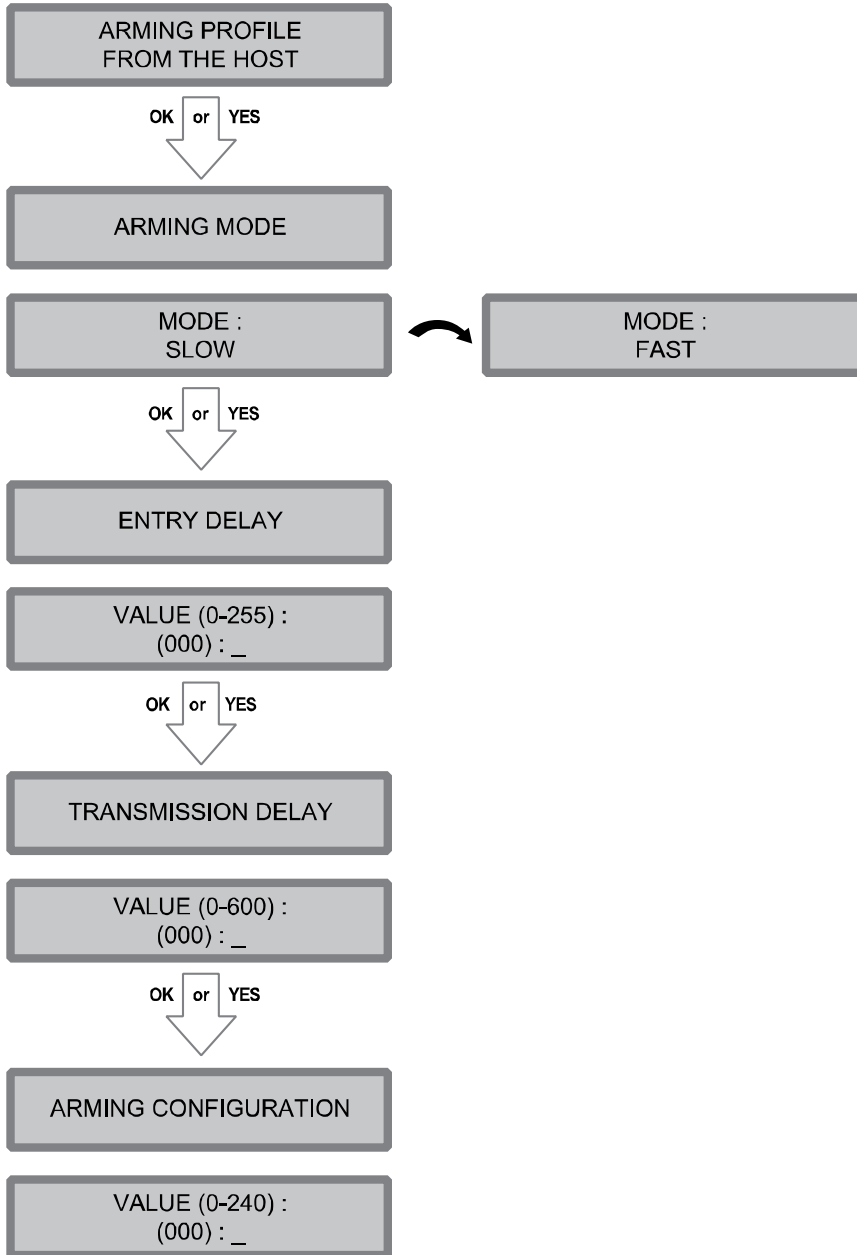
Standalone : Will make the XT-IP a completely independant system controlled by arming and disarming using Videofied peripheral devices(keyfobs, keypads, badge,readers).

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

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

XTENDER mode configuration



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.

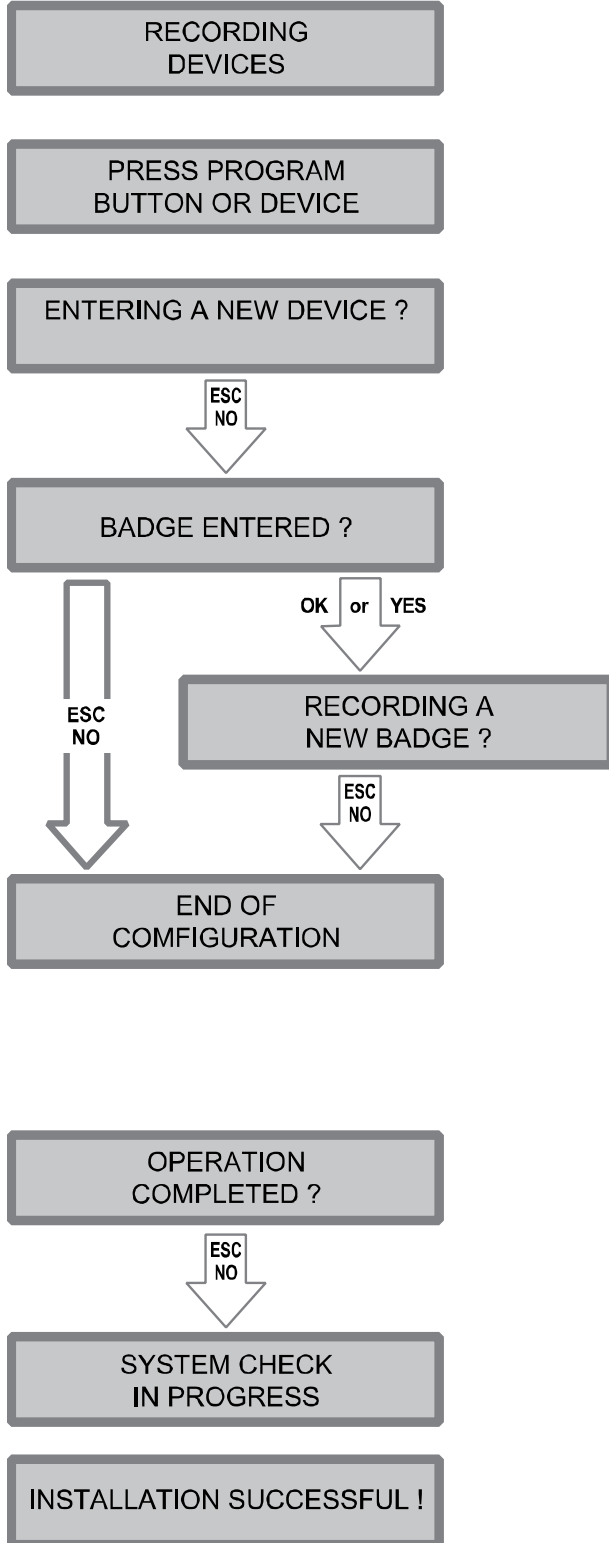
Enter the value you would like for the Transmission Delay and press **OK or YES**.

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*

Keypad Display



Actions and comments

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 a minimum (Please refer to the Radio Range section, page 8 for further details).

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

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

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

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

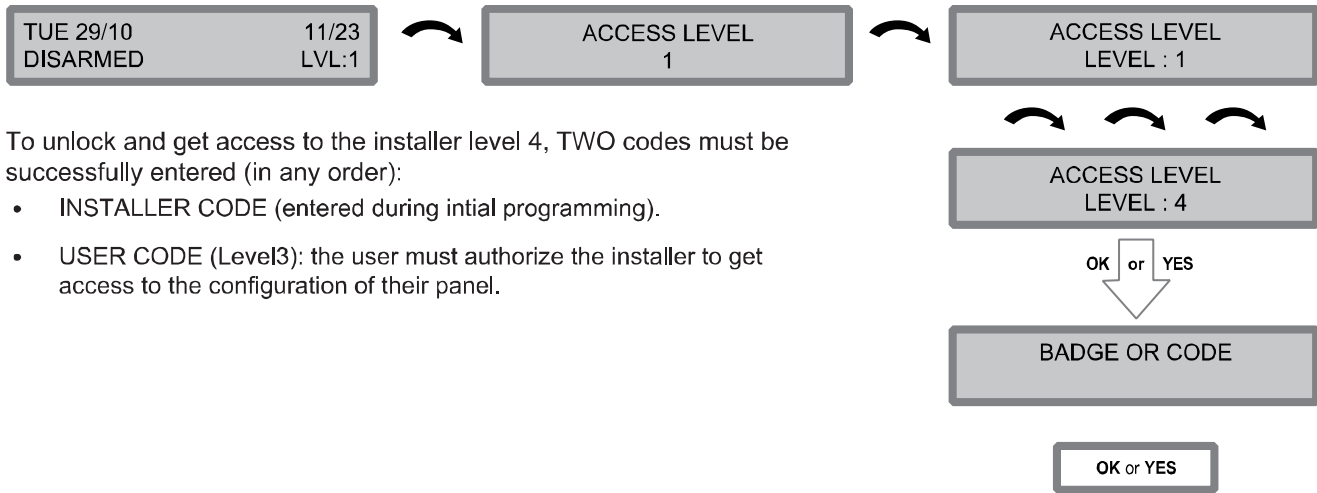
If you wish to use an user code, please skip this step and when initial programming is completed go to the BADGES/ACCESS CODES menu (please refer to chapter 4.4 for further details).

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

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, TWO codes must be successfully entered (in any order):

- INSTALLER CODE (entered during initial programming).
- USER CODE (Level3): the user must authorize the installer to get access to the configuration of their 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.

Note: In the event that 5 invalid Code entries have been made, the system will enter a 90 second lockout period.


	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 BR	N/A	Present your badge on the badge reader	N/A	N/A
With remote keyfob	N/A	N/A	Press	Press




4.3 Arming and Siren Mode Configuration

• Use the   to go to menu :

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

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

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

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

4.4 Manage badges and access codes

Access Level

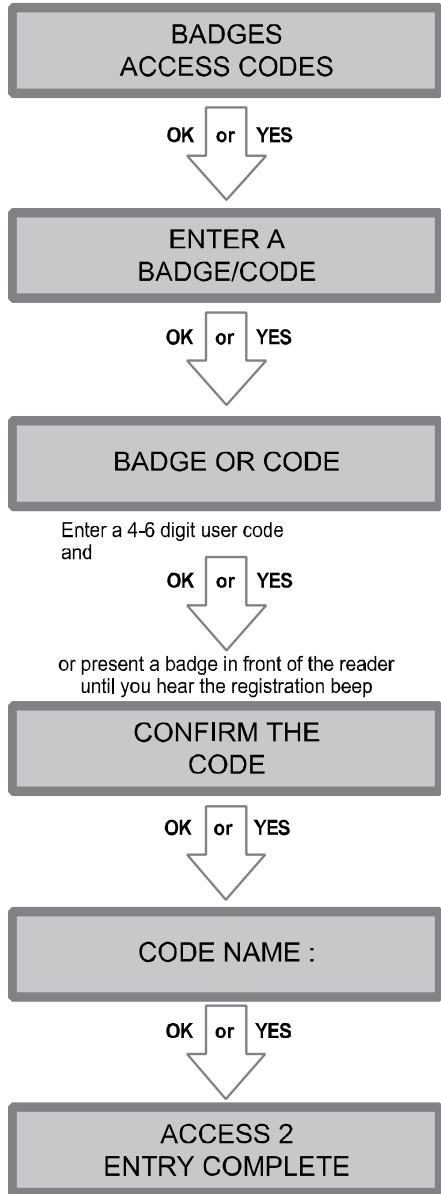
Access Level	Definition & Rights
LVL 1	Standby Level
LVL 2	Restricted USER level , where it is only possible to arm/disarm the system.
LVL 3	USER level , where it is possible to arm/disarm the system, check the event log, test the devices. Modifications of the settings are not possible at this level. 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 or Level 2 user is required. Installer Level 4 can create the first Level 3 access code only.

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

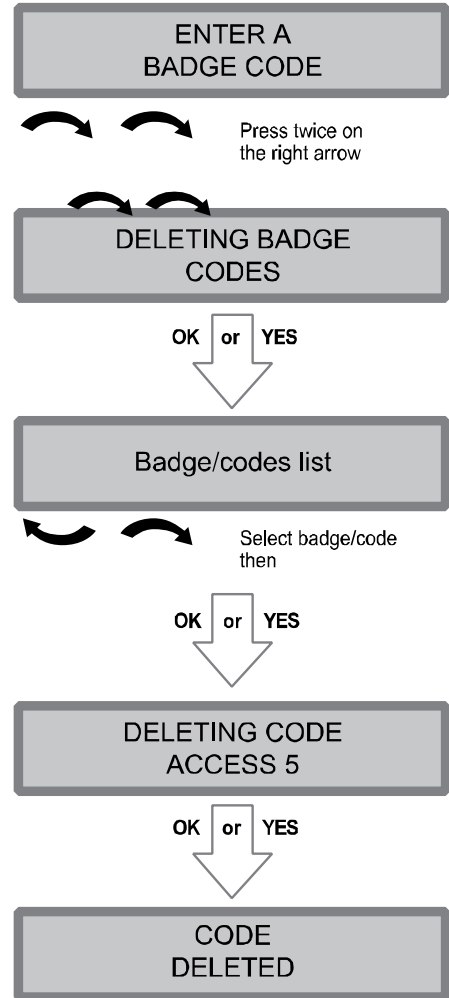
How to return to the LVL1?

- After 1 min of no use of the keypad and no tests running, the display returns to the standby display and LVL1.
- When standby display, if the **ESC NO** key is held during 5s, the level is changed to LVL1.

Enter a new end user Badge/Code



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

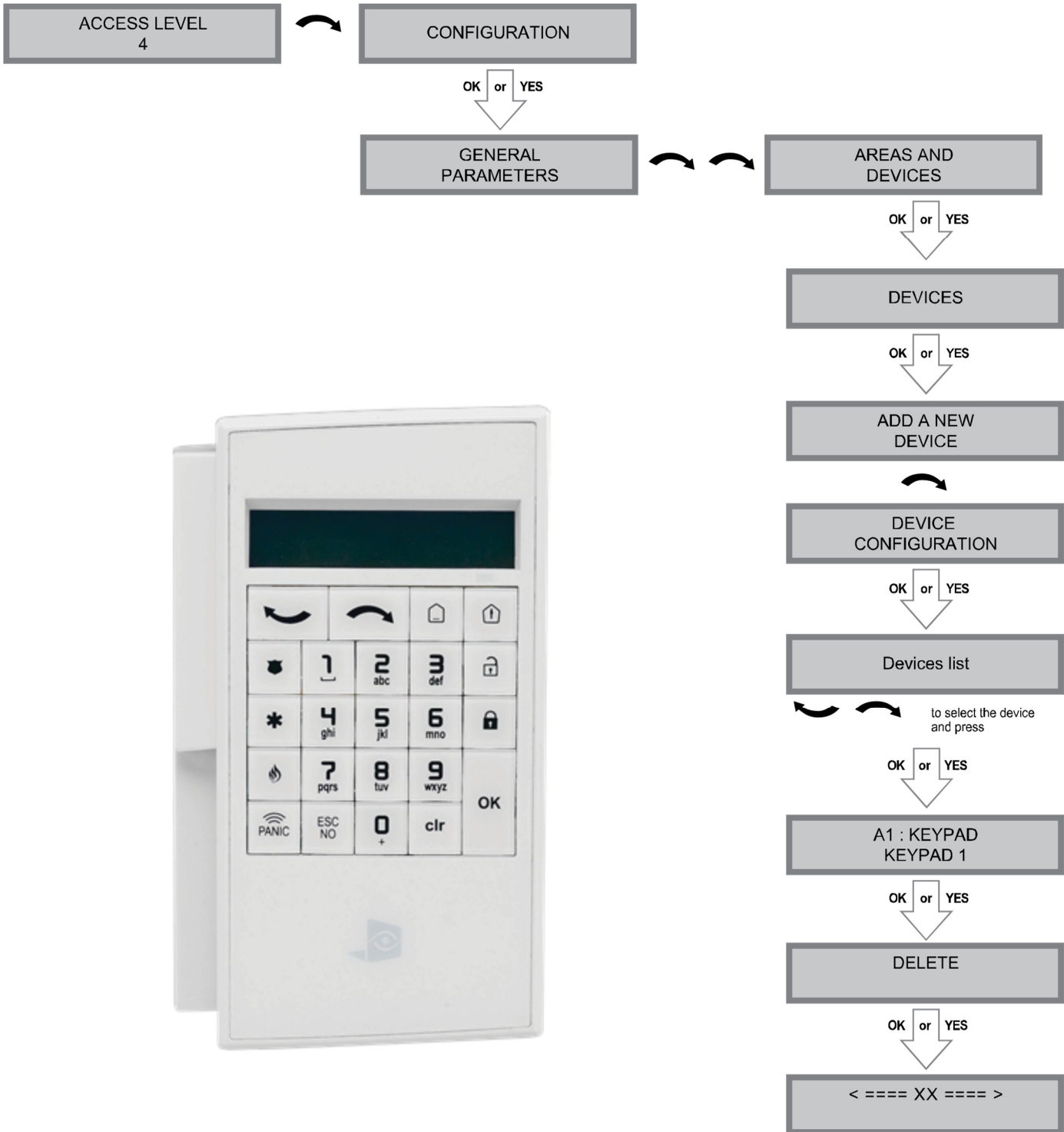
When a code is created (1000 for example), the 2 next codes and previous codes (0998, 0999, 1001 and 1002) will be automatically reserved.

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.

4.5 Delete the keypad or any other device

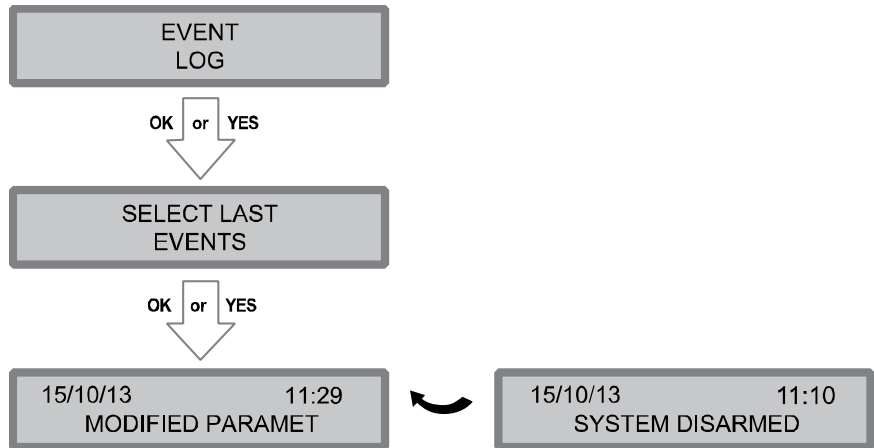


You can now remove the batteries from the device

4.6 Read the event log

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

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



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

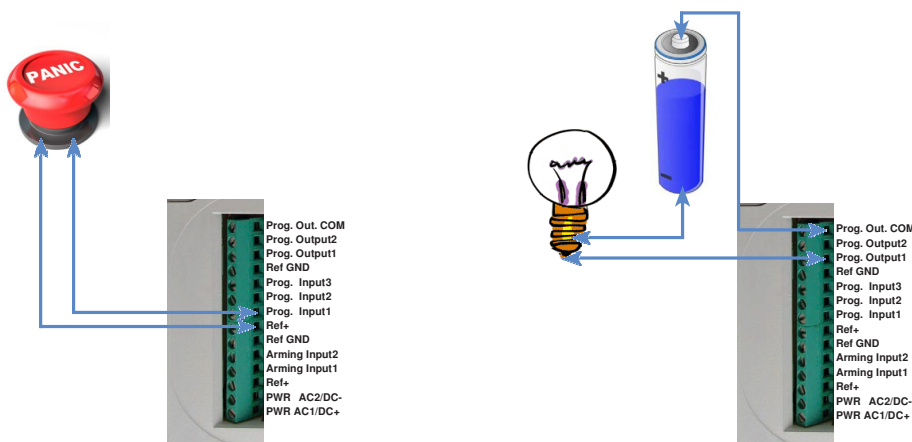
4.7 Programmable inputs and outputs

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

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

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

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



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**. Press CLR to erase a typing mistake.
- 4 Never register the same device twice (delete from the system first). Registration of **up to 25 devices** (including the keypad).
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 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.

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



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.

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

Events are displayed and transmitted in order of occurrence and there is no prioritization of signal transmission to the Central Monitoring Station.

When ETH + CELL is chosen for communication, the system will make alternate attempts to connect to the Primary and Secondary Central Station Receiver between Ethernet and Cellular communication. Depending on the profile loaded, the panel will try to reach alternatively the Primary or the Secondary receivers using Ethernet or Cellular. These attempts can be repeated several times and will stop once a Receiver is reached or cease once all attempts failed. A new event during or after this sequence will restart the attempts from the beginning.

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:

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 Cellular (cell) 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, ...	<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 Cellular (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 Cellular (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 Cellular Network:**

When the panel is unable to find any signal, proceed to Cellular (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 out used batteries! Bring them to your installer or a collection point.

Deutsch

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

Electrical Data

Power requirements

Power supply Type B	9-12VDC / 1.2A
Low Voltage limit	5.15V
Backup	6V with 4 x 1.5V Alkaline batteries / LR20
Low battery limit	4.2V
Battery life (average)	1 year
Current Consumption	1.2A transmit (maximum) 450µA standby

Power Requirements (Option 2)

Power supply Type C	14.4V with 4x3,6V Lithium batteries / LSH20
Low battery level	12V
Average Battery life	4 years

RF S²View[®] technology

Radio type	Bidirectional RF
Operating frequency	868MHz - XT-IP 240 (Europe, South Africa, Asia) 920MHz - FHSS - XT-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 detection

Tamper	Wall and Cover tamper detection
--------	---------------------------------

Mode of Operation

Pass Through

Approvals

EN 50131-1:2006+A1;A2	EN 50136-1:2012
EN 50131-3:2009	EN 50136-2:2013
EN 50131-4:2009	EN 50130-5:2011
EN 50131-5-3:2017	EN 61000-6-3:2007
EN 50131-6:2017	EN 61000-3-2:2014
EN 50131-10:2014	EN 61000-3-3:2013
ATS Class: SP3, DP2	



WEEE Directive 2012/19/EU Waste of Electrical and Electronic Equipment Directive Disposal Information

Do not dispose this device and contained batteries with general household waste. For proper treatment, recovery and recycling, please take the device and contained batteries to designated collection points. Disposing of this device and of contained batteries correctly will help save valuable resources and prevent any potential negative effects on consequences for the environment and human health and the environment, which could otherwise arise from inappropriate waste handling.

Cellular Transmission

Communicator

Communicator type	2G, 4G LAN Ethernet (XT-IP 240) 4G LAN Ethernet (XT-IP 740)
2G frequencies	850 / 900 / 1800 / 1900 MHz
4G frequencies	(XT-IP 240) 2100(B1), 1800(B3), 900(B8), 800(B20), 700(B28) (XT-IP 740) 2100(B1), 1800(B3), 850(B5), 900(B8), 700(B28))
Security protocol	Frontel
IP stack	TCP/IP
Video transmission	Frontel protocol to central monitoring station or App
Cellular Antenna	Integrated
External Cellular antenna	Yes via MMCX connector

Video

Video Format	MPEG
Images per second	5
Image size	Dependent upon camera type
Video length	10 seconds

Miscellaneous

Programming	With Remote Keypad
Remote devices/system	25 Maximum
Access Badges/codes	20 Maximum
Arming modes	4
Areas	4
History / Event log	4000 events stored on flash memory
Events memory storage delay	Infinite

Box

Physical and Environmental Data

Operating temperature	-10°/40°C
Maximum relative humidity	75%, sans condensation
International Protection	IP54 / IK06
Marking	
Material	ABS—ULV0
Dimensions	225 mm x 180 mm x 55mm
Weight	520g (without batteries) 1,600g (with batteries)

Installation / Mounting

Control panel / Base	2 screws secure control panel cover to base 3 screws secure control panel base to the wall
----------------------	---



resideo

For more information
www.resideo.com

RSI Video Technologies 25, rue Jacobi-Netter
67200 Strasbourg France
Phone: 33-3-90-20-66-30
R800-27467A 7/22 Rev. A
© 2022 Resideo Technologies, Inc



VIDEOFIED
by resideo