



Complete Setup and Programming Guide for XT-IP and XTO-IP Control Panels



* A Videofied alphanumeric keypad is required
for programming and maintenance *



CMA



XMB



WMB

<u>Table of Contents</u>	Page
FCC_____	3
Installation Guidelines_____	4
Introduction_____	5
Programming buttons and Golden rules_____	6
Initial programming_____	7-14
Entering Badges and User Codes_____	15
Change to level 4 (installer level)_____	16
Enabling and Disabling Monitoring_____	17
Ethernet Parameters overview_____	18
Disabling Eth comms and Useful codes_____	19
Perform 2G3G level_____	20
Testing Device RF Leve (radio range)_____	21
How to enable external antenna_____	22
2G3G antenna replacement_____	23
Arming Input Wiring Diagram_____	24
SP1 & SP2_____	25
Scheduling_____	26
Calendar Management_____	27
App settings_____	28-31
Partitioning_____	32-39
Replacing batteries_____	40
Inputs and Outputs_____	41-43
Troubleshooting	
Walk test / ETH status / Lost installer code / Radio protocols_____	44
Default devices / OMV tampers _____	45
Motion sensitivity / Keypad <--XX-->/ Change SIM / Smoke detector__	46
Outdoor installation guidelines_____	47

Menu structure (Flow chart)

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.*

Radiofrequency 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.

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.*

Cet appareil est conforme à la Partie 15 des réglementations de la FCC et avec la norme RSS-210 de l'Industrie Canadienne.

Son fonctionnement est soumis aux deux conditions suivantes : (1) Cet appareil ne doit pas causer d'interférences nuisibles et

(2) Cet appareil doit accepter toute interférence reçue, y compris les interférences pouvant entraîner un fonctionnement indésirable.

Basic Setup Guidelines for Installation and Programming

Pre-Setup

- 1) Obtain the account number and IP / Domain addresses from the Central Station.
- 2) If using Cellular communication for primary or backup, activate the SIM card through your cellular provider. (and get the APN code from your SIM card provider)
 - a. *Do these steps at least 1 day before the install.

System Programming and Setup

- 1) Setup and program the system in the office or in your vehicle. ADD ALL THE DEVICES. (Pages 7-14)
- 2) Add user codes and or badges after initial programming. (Pages 15)
- 3) Monitoring should be disabled so that signals are not sent until you are ready to send them. (Page 12)

Deploying the System on Site

- 1) Place the panel where you want to mount it and run the Ethernet cable. In Maintenance run the ETH. STATUS test to make sure you are receiving an IP. If you are using cellular as backup or primary make sure you get 3/5 or better when running the 2G3G Level Test in maintenance. If not, you will need to move the panel and run the test again.* (Page 20)
- 2) Deploying Devices: Run the RF test for your keypad, walk to each of the locations with the keypad where a device will be mounted (basically for this test you are replacing all your devices with your keypad). If you get a 9/9 for your RF test, then the location is suitable to mount your device. If not, find a suitable place to get optimal signal.* (Page 21)
 - a. If you are not getting an appropriate 2G3G or RF level, you can add an external antenna for either signal. Enabling External Antenna: (Page 22)
- 3) Re-enable monitoring before you send signals (Page 17)
 - a. If you are currently using TMT2 you can now take still pictures from each MotionViewer using the software. If in doubt on how to operate TMT2 or to get it please contact 1300 46 44 55
- 4) Once you have everything mounted, arm the system and trip one MotionViewer at a time. Make sure you stand in front of each MotionViewer for 10 seconds so the central station has some video to look at.
- 5) After you have sent signals to central station, call to verify.

The following pages will go through each one of these steps and, if you have any issues please consult the troubleshooting section Pages 44-47. If you still cannot resolve the issue, please feel free to call technical support on 1300 46 44 55

Sleeping mode and wake-up on the XMA/WMB:

The keypad backlight will go out after 30 seconds of inactivity. The first touch on the keypad will wake up the keypad and will register as a command to the control panel. It is recommended to wake up the keypad with the right arrow.

Introduction:

Description:

The XT-IP series control panel is a Videofied wireless, battery operated hybrid alarm system. It is designed for residential, small business and commercial security applications. The XT-IP series provides integrated Video Verification and features dual communication paths: Ethernet and 2G3G.

The XT-IP series has programmable inputs and outputs. XT-IP series also features mapping where an external input can be used to generate a video clip from a MotionViewer.

Internal RF range and 2G3G range can be enhanced using external antennas.

Supervised Wireless Technology:

The XT-IP, along with all Videofied devices, uses the patented S2View® - Spread Spectrum, Videofied, Interactive, AES Encrypted Wireless technology, providing optimum signal integrity and security.

The bi-directional RF communication path between all devices and the system control panel guarantees high signal reliability. Integrated antennas eliminate protruding wires or rods, which are difficult to install, unsightly to consumers and potentially troublesome if damaged.

The panel supervises every device (excluding the remote key fob) to validate current open/close state, tamper condition, serial number, date of manufacture, firmware revision, and battery status.

In order for an installation to be UL compliant you must follow the specifications in the table below:

Type	Specifications	Location in Manual
Audio	When a MotionViewer is installed on the sytem you may not have the siren sound for less than 60 seconds	
Audio	If no MotionViewer is installed on the system you may not have the siren sound for less than 240 seconds	
Delays	When a MotionViewer is installed on the sytem the Entry delay must be 45 seconds	

Useful information

Programming button locations:

Outdoor detector
DCV 750/751



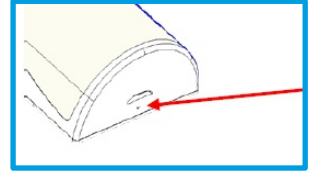
Outdoor detector
OMV 722



Indoor detector
DCV 700/701



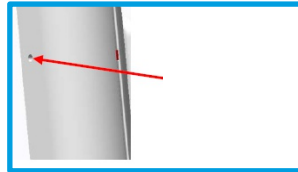
Indoor detector
IMV 701/702



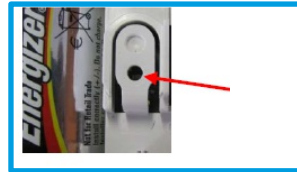
Door contact / univ. trans.
CT 700/701/711



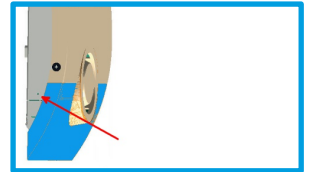
Door contact
IDC 701/702



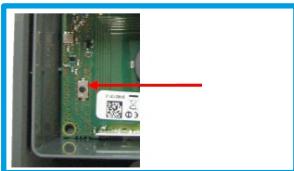
Siren
SE 750/751



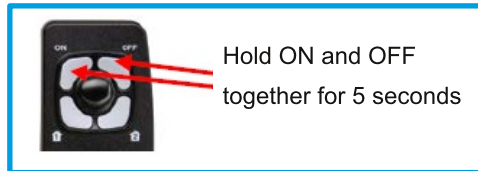
Siren
OSX 712



Badge reader
BR 700/701



Remote control
RC 700/701



Golden rules:

- Once you power a device / panel, make sure you don't take power off. Surely you can recover if you take power off, however by ensuring power is always ON your job will be quicker and easier. Pay special attention to the panel as one mounting hole is under a battery placement.
- Pair ALL your devices when the keypad displays "Press program button of device". Failure to do so could mean to start all over again (in certain circumstances).
- Don't default the panel (press and hold its programming button for 10 seconds) unless you know what you are doing...
- If you **Need** to default the panel, make sure you delete all the devices from it, failure to do so will make those "non-deleted" devices harder to pair later on.
- Disable monitoring before taking the SIM card out or putting the SIM card in, failure to do so can damage the modem and also may waste about 20 minutes of your time later on.
- Read the manual.

SETUP MANUAL FOR XT-IP SERIES 2G3G PANEL

THIS SYSTEM REQUIRES A KEYPAD FOR PROGRAMMING

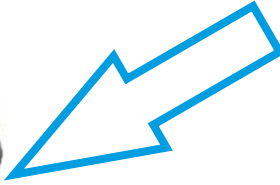
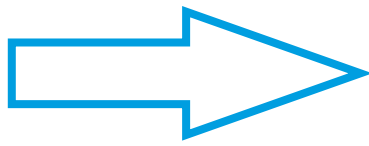
****TO TRANSMIT ALARMS AND VIDEO VIA ETHERNET, THE SYSTEM REQUIRES AN EXTERNAL POWER SUPPLY WITH 4 ALKALINE BATTERIES FOR BACK-UP****

XT Initial Programming



Open the Control Panel

Using a #1 Philips screwdriver, remove the 2 screws holding the cover on



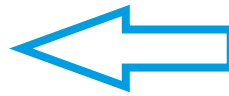
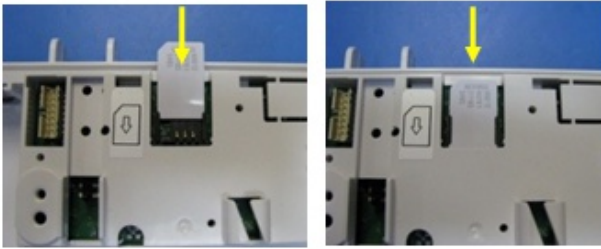
The cover will fold off the panel like a book with the curved side acting like the binding. The same technique is used when placing the cover back onto the unit.



When removing the XTO cover, pull straight off, do not slide it.

*The SIM card must **NOT** be inserted or removed while the modem is powered*

Disabling monitoring will ensure the modem is off

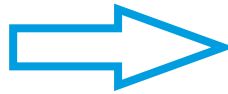


Install the SIM card

Slide SIM card into the slot. Make sure it is aligned correctly. The SIM card is not required if you plan to use Ethernet only.

Connect the RJ45 (Ethernet cable) to the panel

Plug the RJ45 cable into the Ethernet jack on the control panel. The cable can be routed back through the wire channel to make sure it does not get pinched.



Important:

When the panel attempts a transmission via Ethernet a red LED will flash.



Obtaining WMB / XMB Keypad Special Characters

Keys	1 st Press	2 nd Press	3 rd Press	4 th Press	5 th Press	6 th Press	7 th Press	8 th Press	9 th Press	10 th Press	11 th Press	12 th Press	13 th Press	14 th Press
1	'Space'	1	.	-	@	\$,	'	?		:	:	~	N/A
0	+	0	-	*	#	=	/	%	&	¥	<	>	()

Obtaining CMA Keypad Special Characters

Key	1 st press	2 nd press	3 rd press	4 th press	5 th press	6 th press	7 th press	8 th press	9 th press	10 th press	11 th press
1	"space"	.	.	'	?	!	:	:	#	1	
0	-	+	=	/	¥	_	<	>	()	0
@	@	\$	%	&	*	#					

Powering the Panel

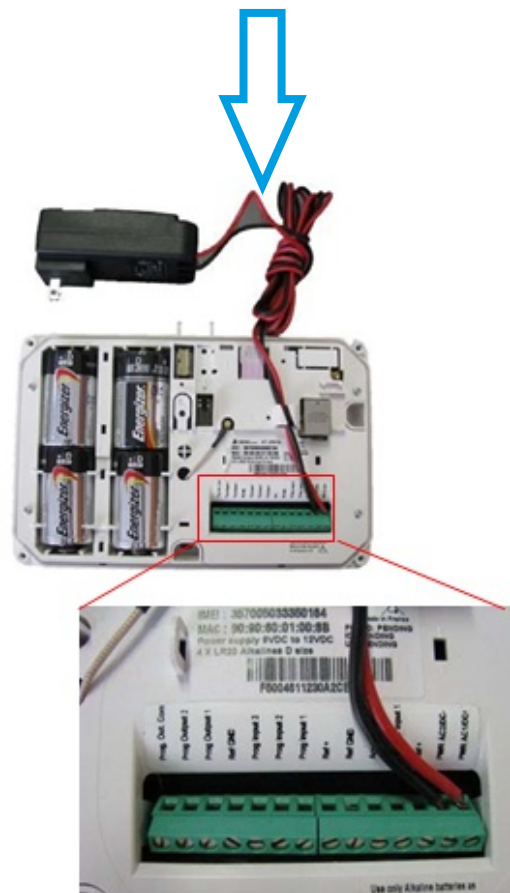
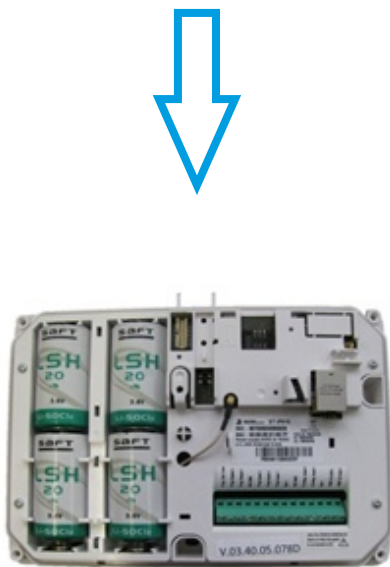
****THE CONTROL PANEL MUST BE CONNECTED TO AN EXTERNAL POWER SUPPLY WHEN ETHERNET FEATURE IS ACTIVE****

Option 1: PP1	Option 2
4 x LSH20 SAFT Lithium D-Cell	4 x E95VP Alkaline D-Cell + 12v 2amp DC Class 2 power supply (not supplied)
Used for Standalone or Xtender mode without Programmable Inputs, Programmable Outputs, Ethernet, or SMS	Used for Standalone or Xtender mode where Programmable Inputs/Mapping, Programmable Outputs, Ethernet connection, or SMS will be used
LSH20 Specifications: Operating Temp: -60°C to +110°C Storage Temp: Dry, Ventilated, 30°C Max	E95VP Specifications: Operating Temp: -17°C to 54°C

LSH20 Technical Specifications	
Nominal Voltage	3.6 V
Open Circuit Voltage	3.67 V
Nominal Capacity	9.3 Ah

E95VP Technical Specifications	
Nominal Capacity	8900 mA hours
Nominal Voltage	1.5 V

Power Supply Requirements	
Output Voltage (volts)	12
Output Current (mA)	2000
Certifications	Class 2 (For UL Compliance)



WARNINGS:

- DO NOT USE ALKALINE BATTERIES IF INSTALLING AN XTIP / XTOIP 2G3G BELOW 0°C, YOU MUST USE OPTION 1: PP1
- DO NOT INSTALL A TRANSFORMER WHEN USING OPTION 1 (LITHIUM BATTERIES)

XT-IP Programming

Reset the XTIP Panel:

Press and hold programming button (1) for 10 sec until the indicator LED blinks twice



Press and instantly release the programming button (1). The indicator LED will blink once. The panel is now in 'Learn Mode' for the CMA/XMA/W MB keypad.



Insert all the batteries into the keypad and press both the ESC/NO and CLR keys at the same time and release. The indicator LED on the keypad will blink rapidly.



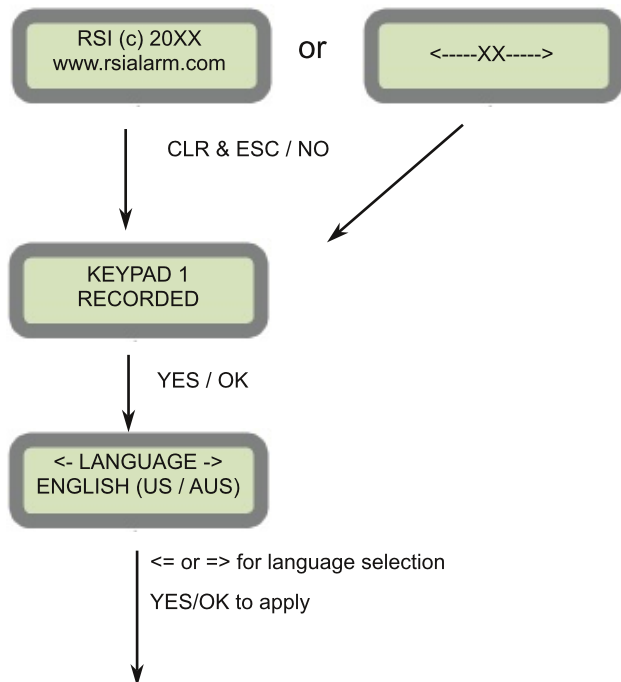
Other languages are available by scrolling with arrows. ENGLISH (UK), ENGLISH (US/AUS), FRENCH, ITALIANO, NEDERLANDS, DEUTSCH, CASTELLANO, SVENSKA, PORTUGUES, FRANCAIS Press YES/OK for the selected one.

There is no **NEED** to reset the panel if it is new (you can skip this step)

If the system is **NOT** new you may reset it **AFTER** deleting all your devices from it

****NOTE:** if you are having issues pairing the keypad to the panel, refer to the troubleshooting section

Programming Keypad



* This guide will display ENGLISH (US / AUS) language only *

The Radio Range test must be run during device recording to ensure proper pairing with the control panel. This test the number of successful pings between the device and the control panel. The keypad will display a real time RF level for the device that is being tested. This test will run until stopped and should be run for at least 15 seconds to receive accurate results.
 The RF level must be 9/9 for reliable transmission. (if it goes back to 8/9 it would NOT be reliable)

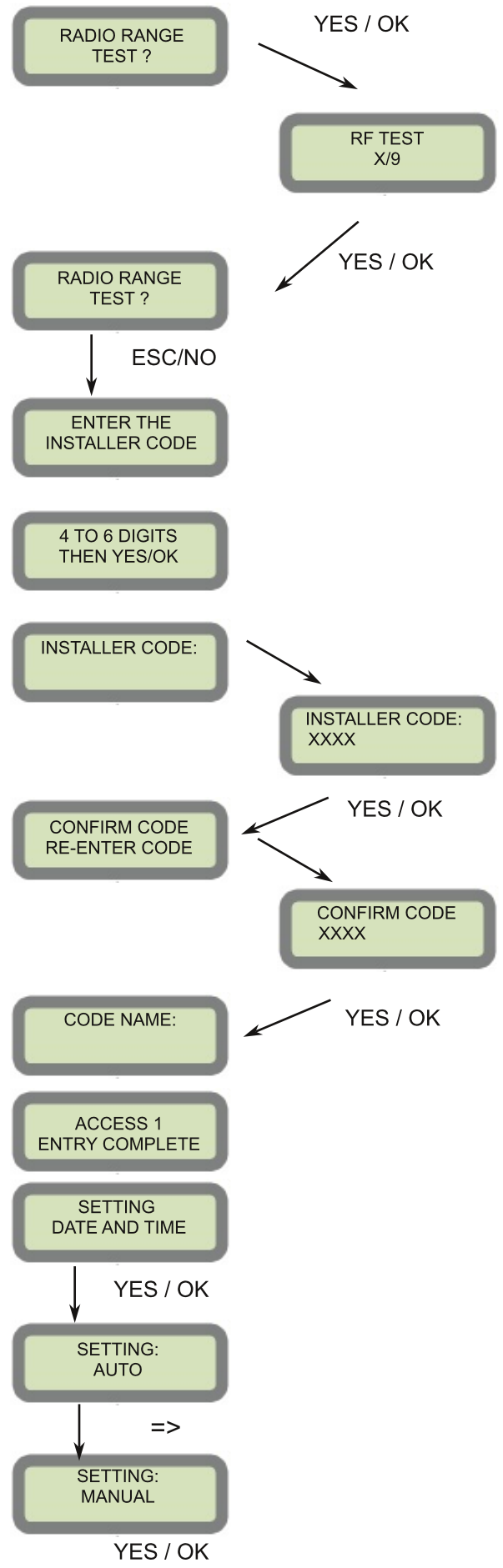
Wait while the screen changes

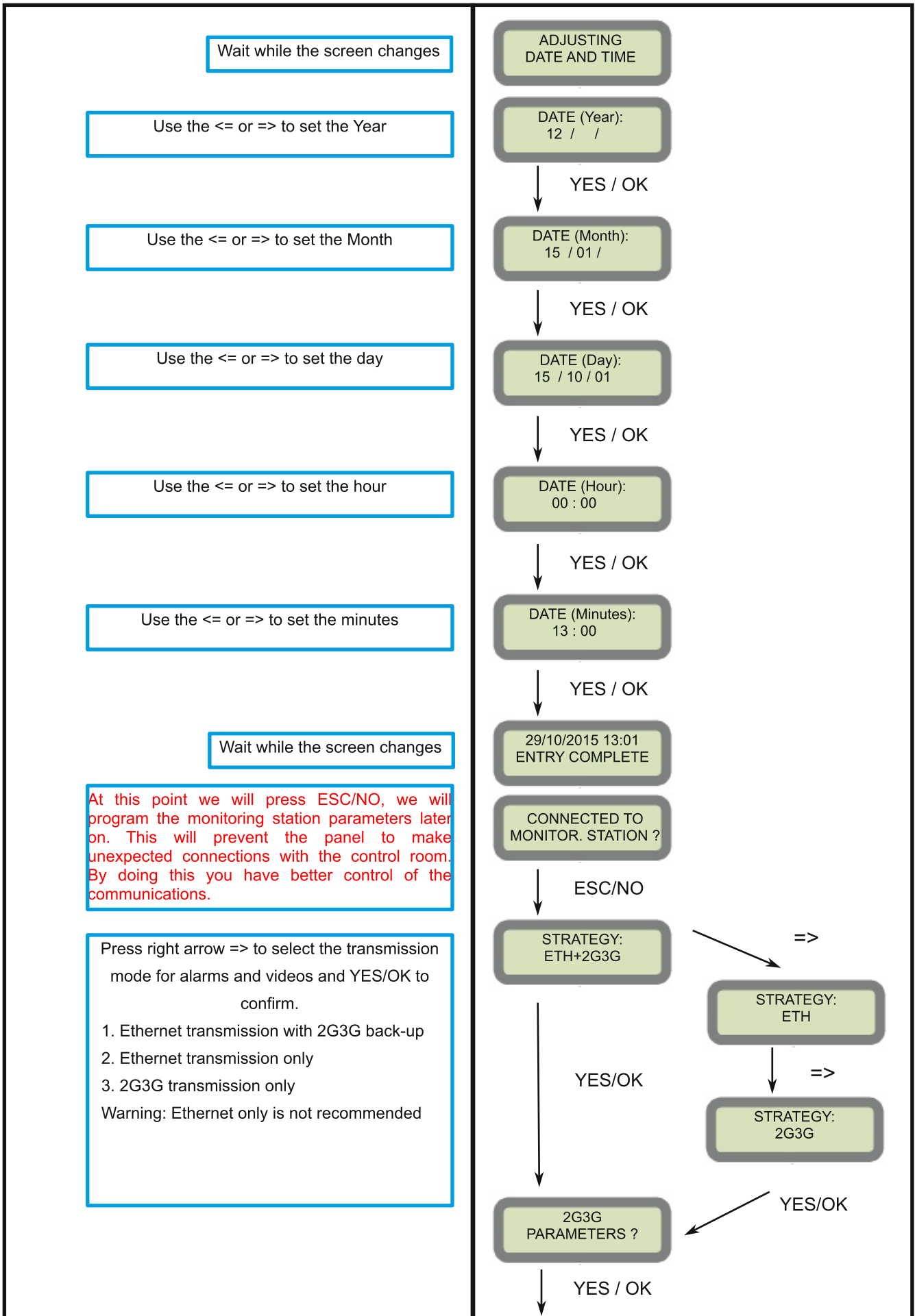
From here until the end of initial programming you will not be able to step back to a previous parameter. All parameters can be changed after initial programming has been completed.

Use the Alphanumeric Keypad to enter the Installer Code
***This code is important to keep track of.** There is no back door to the system

You may name the installer code using the Alphanumeric Keypad. If you leave the name blank it will default to 'ACCESS 1'

Wait while the screen changes





Your APN code is given to you by your SIM card provider.
 As a reference, a Telstra SIM usually has "telstra.internet" or "telstra.wap" APN code.
 The dot (.) is found by pressing the number 1 a few times.
 Press and hold a key to toggle between upper and lower case

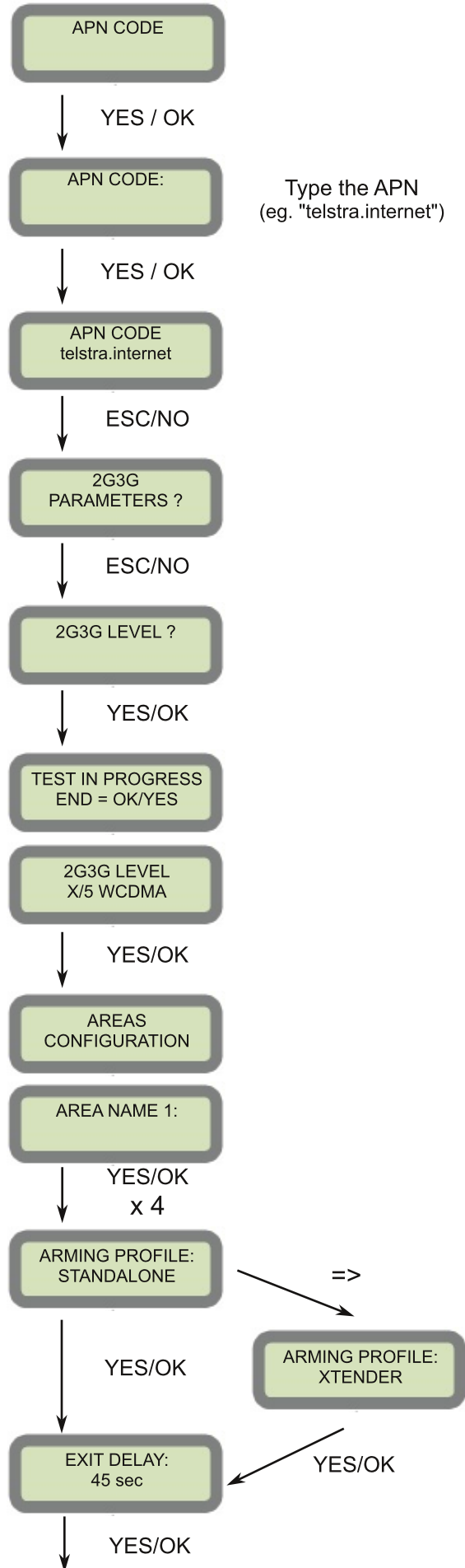
During the 2G3G level the system will attempt to access the mobile network.
 The system will display either a signal level out of 5 (3/5 is the minimum required), an error code or will go to sleep.
 Please go to troubleshooting section if you receive an error code or if the keypad goes to sleep.

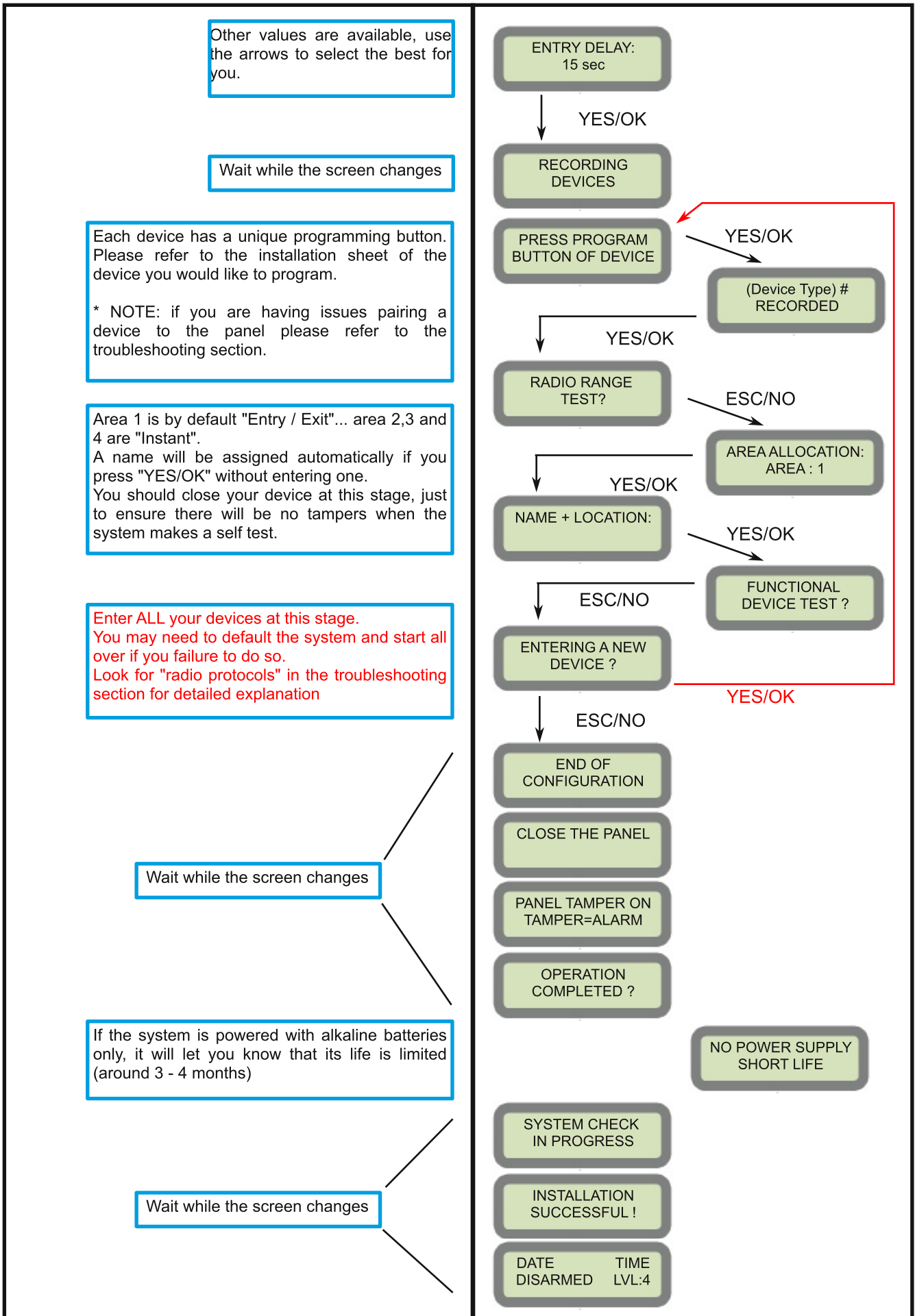
Wait while the screen changes

There are 4 areas in the system. Press YES/OK in all 4 areas

Arming profile option depends on how you want to arm the system:
XTENDER: Will make the XT IP730 a piggyback / xtender system that arms and disarms off the latching of 9-12v on the arming inputs.
STANDALONE: Will make the XT IP730 a standalone system, arm and disarm it by using Videofied peripheral devices (keypad, badge readers, remote control)

Other values are available, use the arrows to select the best for you.





Entering a Badge or Access code for user Arming/Disarming

After initial programming has been completed, you are not able to arm and disarm the system until you enter a user code or badge (the installer code can't arm and disarm the system). Codes can be 4-6 digits and the 4th. digit must be 2 values higher or lower than any other code on the system:

Example: User code 1234, next code can't be 1235, 1236, 1233, 1232. These are reserved for Silent Duress and Audible Duress. The XT system can accept up to 19 Badges or Access codes in any combination.

You must start from "Disarmed LVL:4", if you don't know how to get there follow the steps in the next section.

Enter the user code, it will show as " **** " on the display

Use the keypad to name the badge or code or leave it blank for the default name: ACCESS #.

If you are entering any additional codes press YES/OK. If you have completed entering Badges and Codes press and hold ESC/NO for 5 seconds to return to the main menu.

DATE TIME
DISARMED LVL:4

<= <=

BADGES
ACCESS CODES

YES/OK

ENTER A
BADGE / CODE

YES/OK

BADGE OR CODE

YES/OK

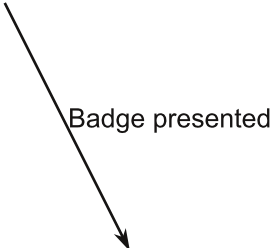
RE-ENTER
THE CODE

Code and YES/OK

CODE NAME:

YES/OK

NAME OF BADGE:



ENTRY COMPLETE

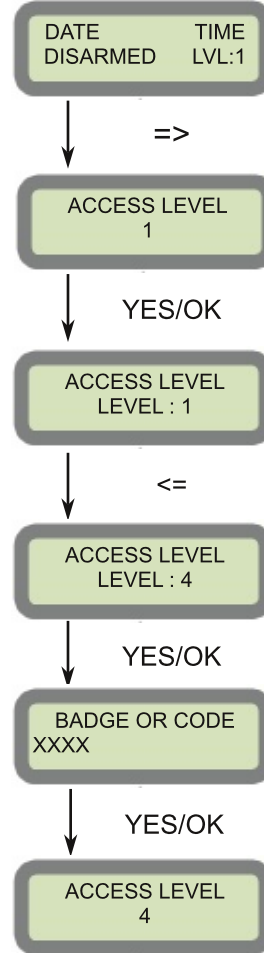


ENTER A
BADGE / CODE

Change access level to 4 (installer level)

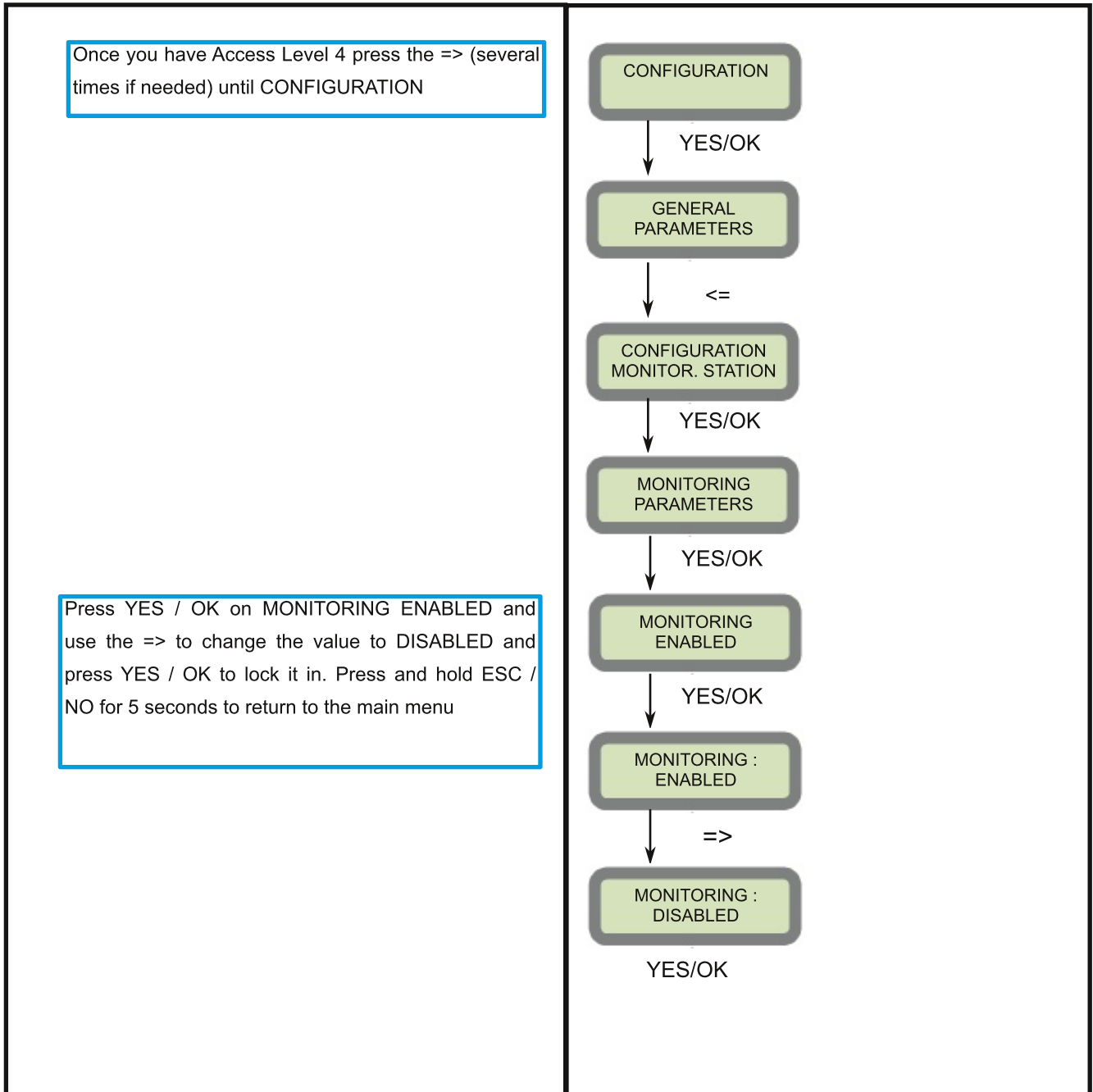
There are a few things that you *need* to remember when using the Videofied system... one is this procedure and your installer code.

In order to get full access to the configuration you have to be "access level 4".



How to Disable / Enable Monitoring

Disabling monitoring can be a useful tool in many situations. Before mounting devices and moving the panel to find a good 2G3G level, disabling monitoring will ensure that you have access to programming and that unnecessary signals are not sent to the monitoring station. When performing maintenance on the system disabling monitoring until the issue has been resolved will ensure that you will have access to programming throughout your troubleshooting.



Ethernet Parameters overview:

To configure or modify Ethernet Parameters, go to:

CONFIGURATION (Level 4) + [YES/OK] >> GENERAL PARAMETERS + [YES/OK] >> ETHERNET + [YES/OK]

* IP Parameters

1. **DHCP Enable** - IP address is assigned by the DHCP service on the network.
2. **DHCP Disable** - IP address must be defined in Ethernet parameters. IP address will NOT be automaticall obtained from DHCP service on the network.

* Constant Ethernet:

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.
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 the panel will connect to the local network and disconnect once it is done.

* **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:** Size of the packet sent

Disabling Ethernet communication

If you are not using Ethernet it is **IMPORTANT** to completely disable it as it is enabled by default.

Failure to do so will affect your battery life and also will fill the event log of the panel with useless information, so if, in the future, you or your client want to have a look at the internal log of the system you will not find the information you are looking for.

The internal log of the system is a valuable tool to give answers to you or your client of the activity of the alarm system.

CONFIGURATION ->CONFIGURATION MONITOR.STATION->MONITORING PARAMETERS-> CALLING PROFILE->STRATEGY-> set to 2G3G only.

CONFIGURATION->CONFIGURATION MONITOR.STATION->TMT PARAMETERS-> CALLING PROFILE TMT FRONTEL->STRATEGY-> set to 2G3G only

CONFIGURATION->GENERAL PARAMETERS->ETHERNET->CONSTANT ETH->set to OFF

Useful codes

Special code	Communication Type	Function	Available since firmware release
999999	GPRS/2G3G	One-shot GPRS/2G3G remote maintenance session request to TMT IP address/Domain Name.	XLP.03.08.01.xx
999997	All	Power supply detection	XLP.03.00.00.xx
999996	Ethernet	One-shot Ethernet remote maintenance session request to TMT IP address/Domain Name.	XLP.03.00.00.xx
999992	Ethernet	One-shot alarm test on IP address 1 / Domain name 1 via Ethernet .	XLP.03.20.00.xx
999991	GPRS/2G3G	One-shot alarm test on IP address 1 / Domain name 1 via GPRS/2G3G .	XLP.03.20.00.xx
999990	All	Ringtone Status (Enabled/Disabled).	XLP.03.21.03.xx
999980	WLAN	SSID WLAN network display.	XLP.03.01.00.xx
999983	WLAN	One-shot alarm test on IP address 1 / Domain name 1 via WLAN .	XLP.07.00.65.xx
999984	WLAN	One-shot WLAN remote maintenance session request to TMT IP address/Domain Name.	XLP.07.00.65.xx

Perform a 2G3G level

Once you have Access Level 3 or 4 press the => (several times if needed) until MAINTENANCE

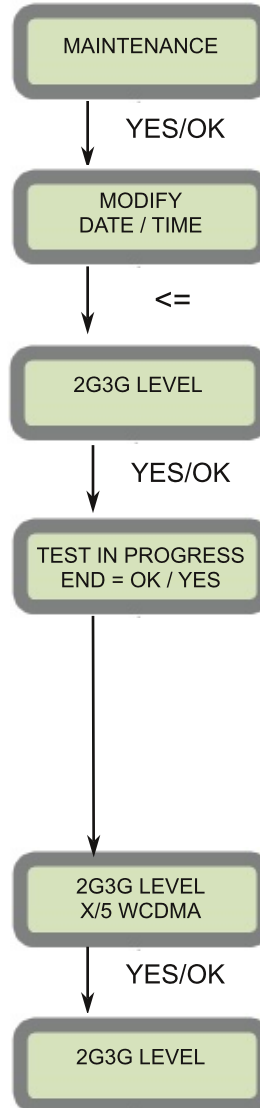
Press the <= arrow (a few times) until you see 2G3G LEVEL

Wait until one of the following:

a) Keypad goes to sleep or error message: in this case there is a problem with the SIM card, APN code, Power on the system (eg. low batteries and no external power supply) or faulty modem. If keypad went to sleep you should stop the test and fix the problem, no need to keep waiting anymore.

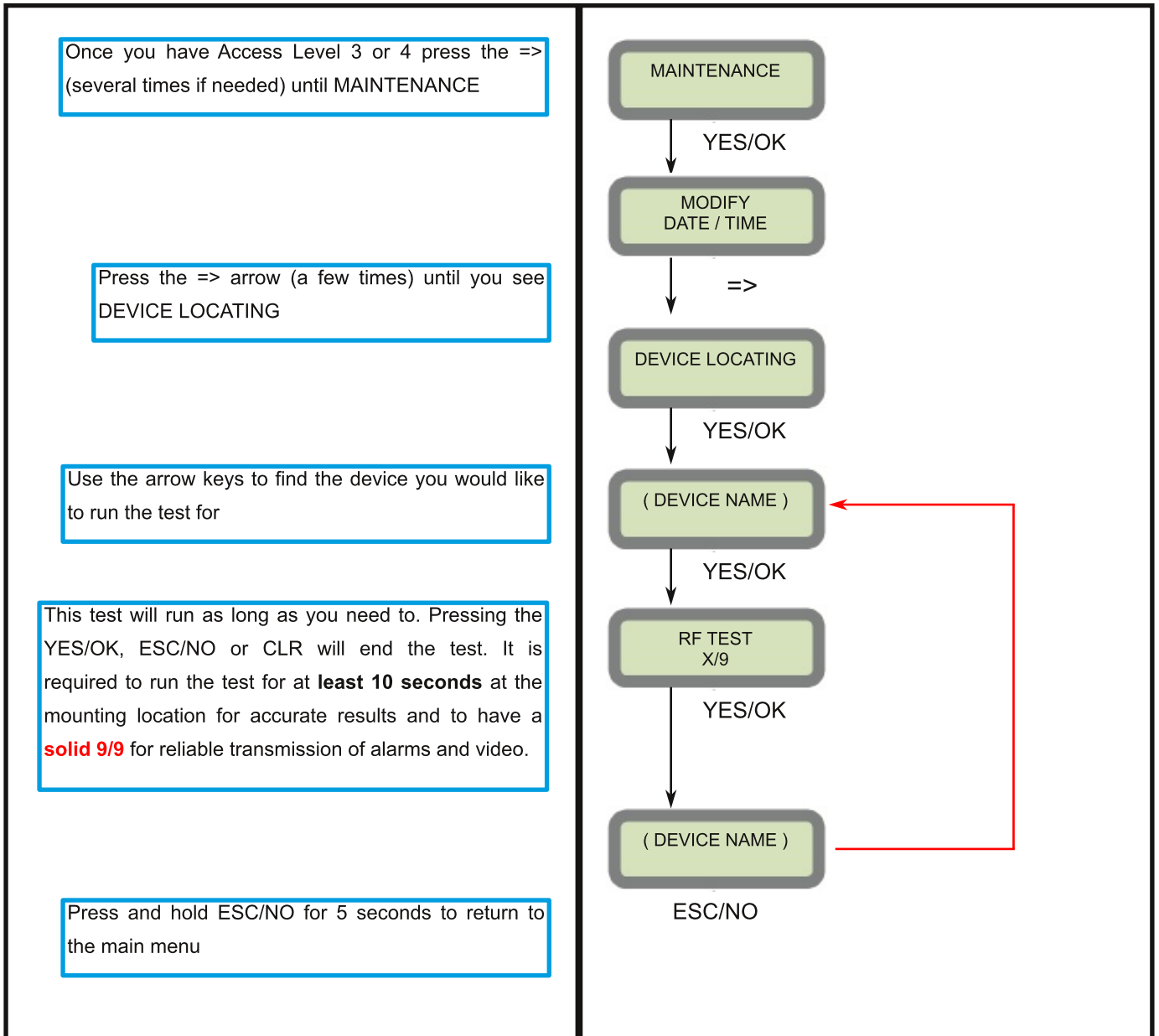
b) You receive a reading out of 5 (0/5 - 5/5)... minimum reading for commissioning is 3/5.

Press and hold ESC / NO for 5 seconds to return to the main screen



How to test the radio range of the devices (RF test)

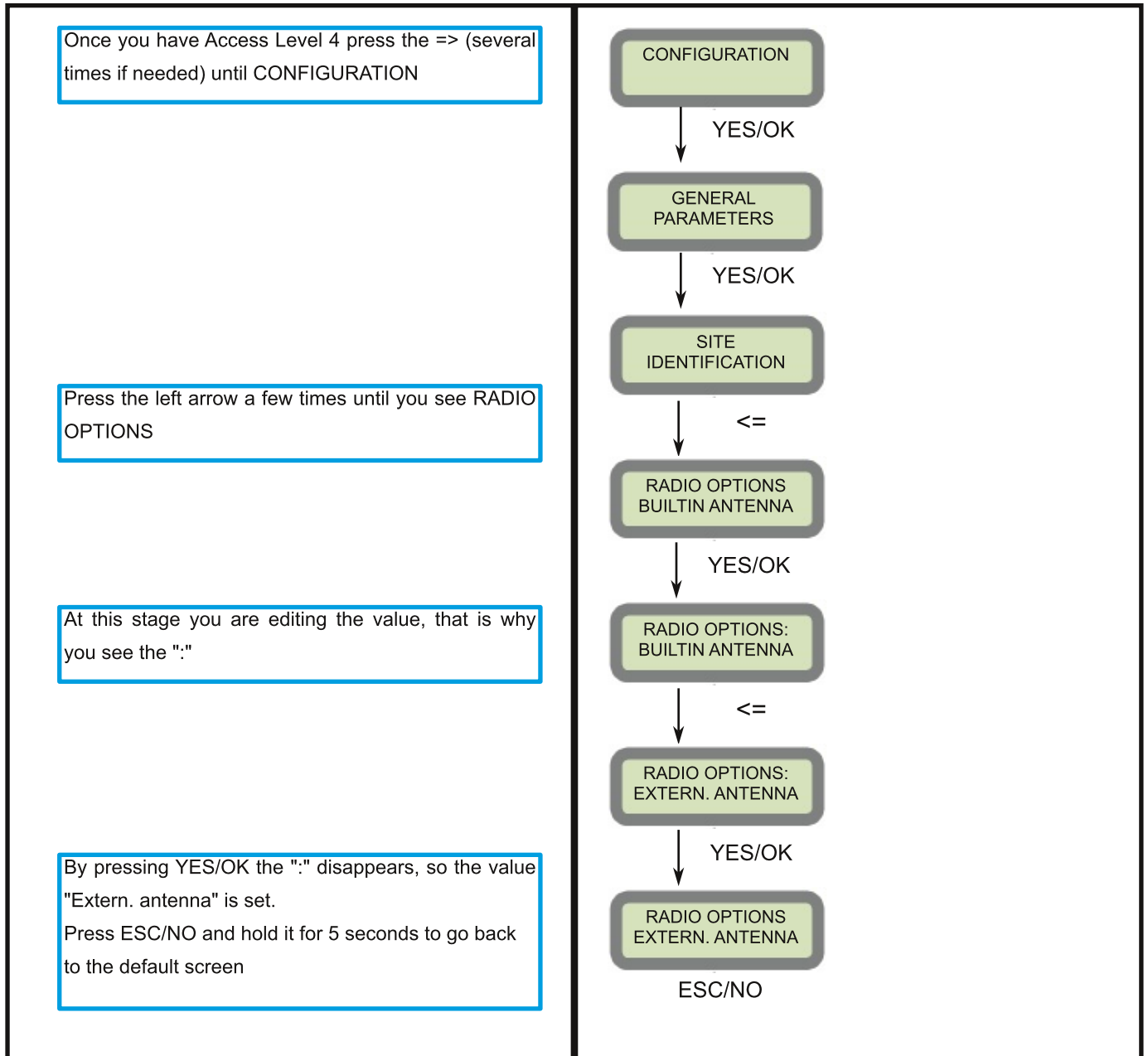
Running the RF test during the mounting of devices is key to a successful Videofied installation. This test will ensure that all devices have adequate communication with the control panel. All Videofied devices are bi-directional which allows the system to ping the device and expect a response. The number of successful responses out of 9 will be displayed on the keypad for the device you are running the test for.



How to enable external RF antenna

You must follow this procedure if you are adding a High Gain RF antenna to an XT-IP 730 or if you are using an XTO system.

The XTO control panels have built in High Gain RF and 2G3G antennas. The 2G3G external comes pre-activated and hooked up, while the RF antenna is hooked up but needs to be activated after you have completed the initial programming.



2G3G antenna disconnection

WARNING !

Use caution while disconnecting the antenna. Damaged connector is NOT covered under warranty

Step 1:

Gently press the antenna cable with your finger, there should be a gap between your finger and the golden connector of about 5 mm.



Step 2:

Insert a flat screwdriver under the cable, the screwdriver head should be larger than the distance between the cable and the plastic below... A 5-6 mm head should be enough



Step 3:

Turn the screwdriver so the screwdriver head pushes up the cable, your finger should prevent the cable from going up so all the upward force is applied to the connector. The antenna should disconnect from the panel without much effort. Make sure all the force is upwards, any wiggle to the side and you are risking breaking the soldering on the board.

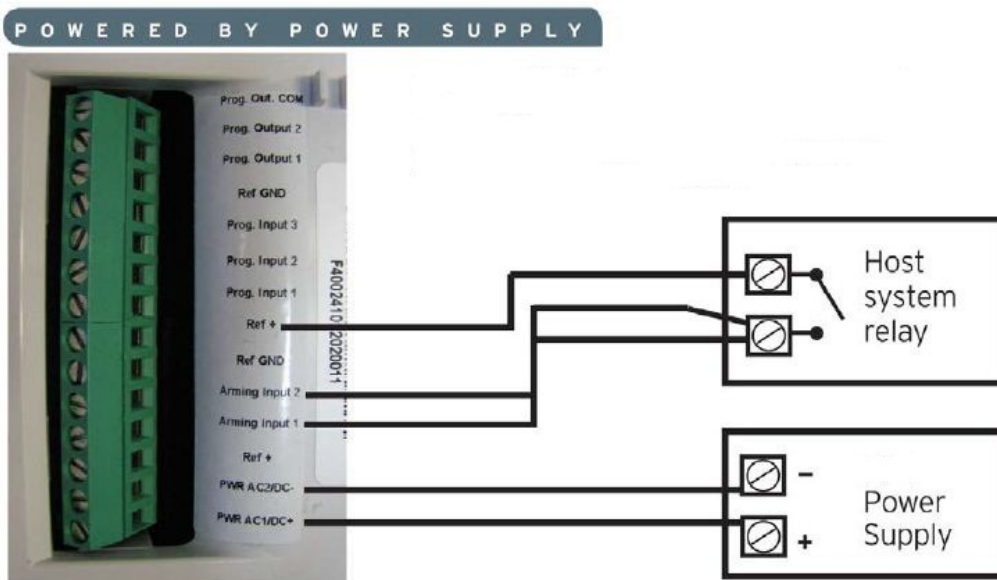
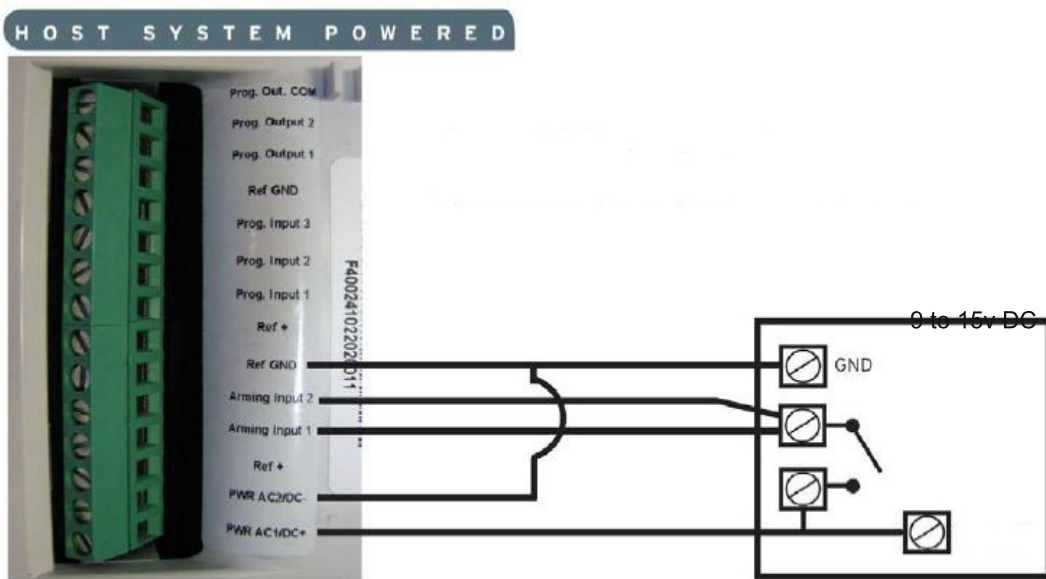


Arming Input Wiring Diagram (Arming profile: From the host)

When in the "Arm From Host" mode the Videofied system will only arm and disarm when 9-15 v 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 will display "PART LVL #"

Arming Input 1 will arm/disarm Areas 1 & 2

Arming Input 2 will arm/disarm Areas 3 & 4



SP1 and SP2 (Stay arming)

Special Program 1 and Special Program 2 are used for arming different areas of the Videofied system.

The most common application is to use it as "stay arming". With the use of SP1 and SP2 the system has 3 possible ways to be armed (SP1, SP2 and fully armed).

Simple scenario (SP1 only)

Imagine a home with 4 x internal and 4 x external detectors and the user wants to arm the external detectors while he is in the house. The user wants one external detector and one internal detector to be entry/exit delayed devices.

How to program it ?

- The entry/exit indoor detector in Area 1 (by default: entry/exit delayed)
- All instant indoor detectors in Area 2 (by default: instant)
- The entry/exit outdoor detector in Area 3 (by default: instant)
- All instant outdoor detectors in Area 4 (by default: instant)
- Make Area 3 entry/exit (Configuration/Areas and Devices/ Areas/Area3/Area mode: delayed)
- Program SP1 (Configuration/Special Arming Modes/Alarm Stay/DDAA)

Complex scenario (SP1 and SP2)

Imagine a home with 4 x internal and 4 x external detectors and the user wants to arm the external detectors while he is in the house, the user also wants to arm everything except the bedroom at night. The user wants one external detector to be entry/exit device.

How to program it ?

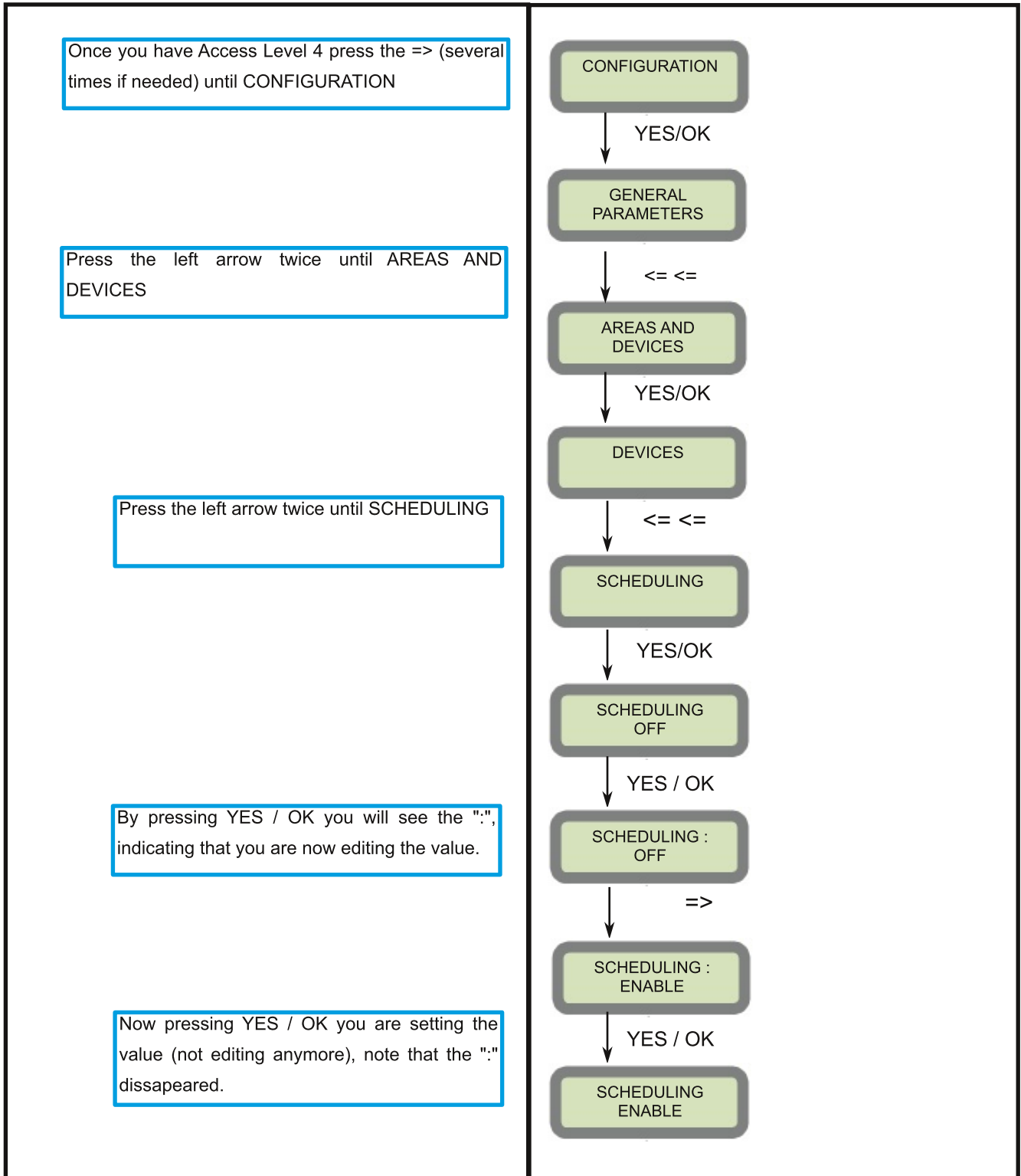
- The entry/exit outdoor detector in Area 1 (by default: entry/exit delayed)
- Bedroom indoor detector in Area 2 (by default: instant)
- All the rest of the indoor detectors in Area 3 (by default: instant)
- All the rest of outdoor detectors in Area 4 (by default: instant)
- Area 1 is already entry/exit area, and Areas 2,3 and 4 are instant by default... so nothing needs to be done there.
- Program SP1 (Configuration/Special Arming Modes/Alarm Stay/ADDA), so only outdoor detectors are armed.
- Program SP2 (Configuration/Special Arming Modes/Alarm SP2/ADAA), so everything except the bedroom is armed

Enabling scheduling

The scheduling defines the capability for the panel to ARM and/or DISARM itself following a weekly calendar.

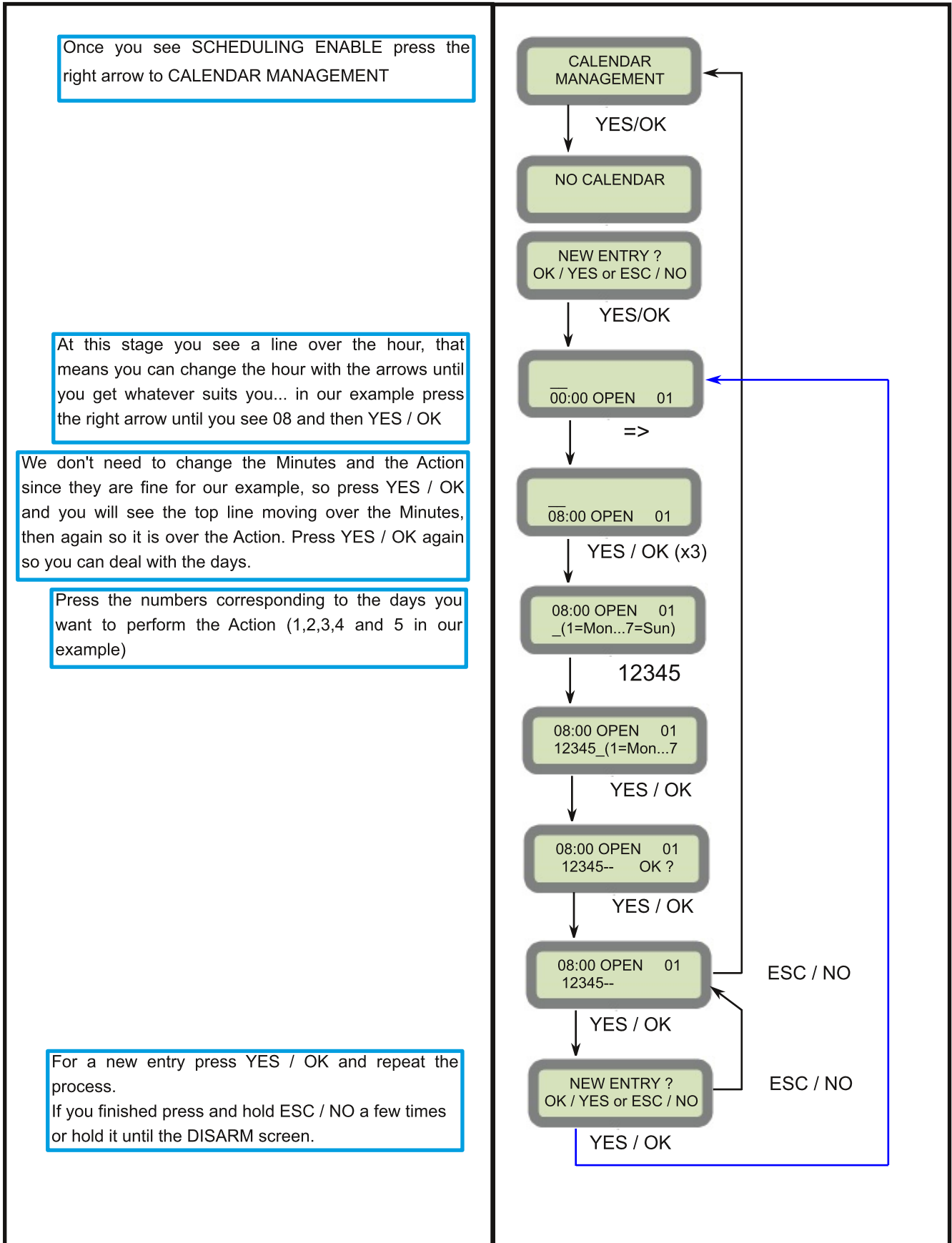
Below is an example of programming an automatic DISARMING Mon - Fri at 08:00.

Once you understand the procedure you can adjust the days / times and actions to suit your requirements... you can have up to 99 entries.



Calendar management

This is where you set up the Hour, Minutes, Action and Day/s (in that order).



Setting up the VideoApp4All

IMPORTANT (conditions for the app to work):

- It is mandatory to connect your panel to an external power supply.
- Your SIM card must be able to receive SMS's
- You have to request the creation of your account to 1300 46 4455 (if you don't have one)

The panel will be ready once you complete these 5 steps (in no particular order)

- Enable Frontel Comfort (or APP)
- Enable ringtone feature
- Enable SMS reception
- Create a client account through the web portal
- Enter an SMS access code

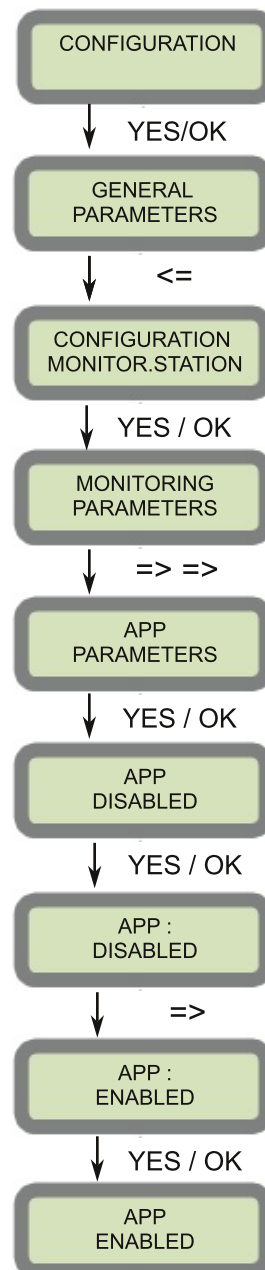
- Enable Frontel Comfort (or APP)

Once you have Access Level 4 press the => (several times if needed) until CONFIGURATION

By default this is set as "APP ENABLED", so usually there is no need to get in here. Also, by default, the Domain 3 and Domain 4 with their ports are also pre-programmed but just in case you accidentally delete them here are the details:

IP3 = 0.0.0.0
Domain 3 = vid-3.va4a.com
Port 3 = 2001

IP4 = 0.0.0.0
Domain 4 = vid-4.va4a.com
Port 4 = 2002



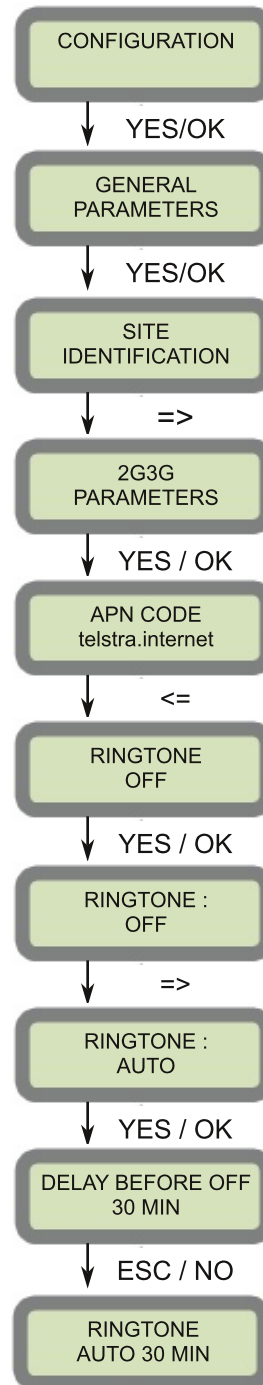
- Enable ringtone feature

Once you have Access Level 4 press the => (several times if needed) until CONFIGURATION

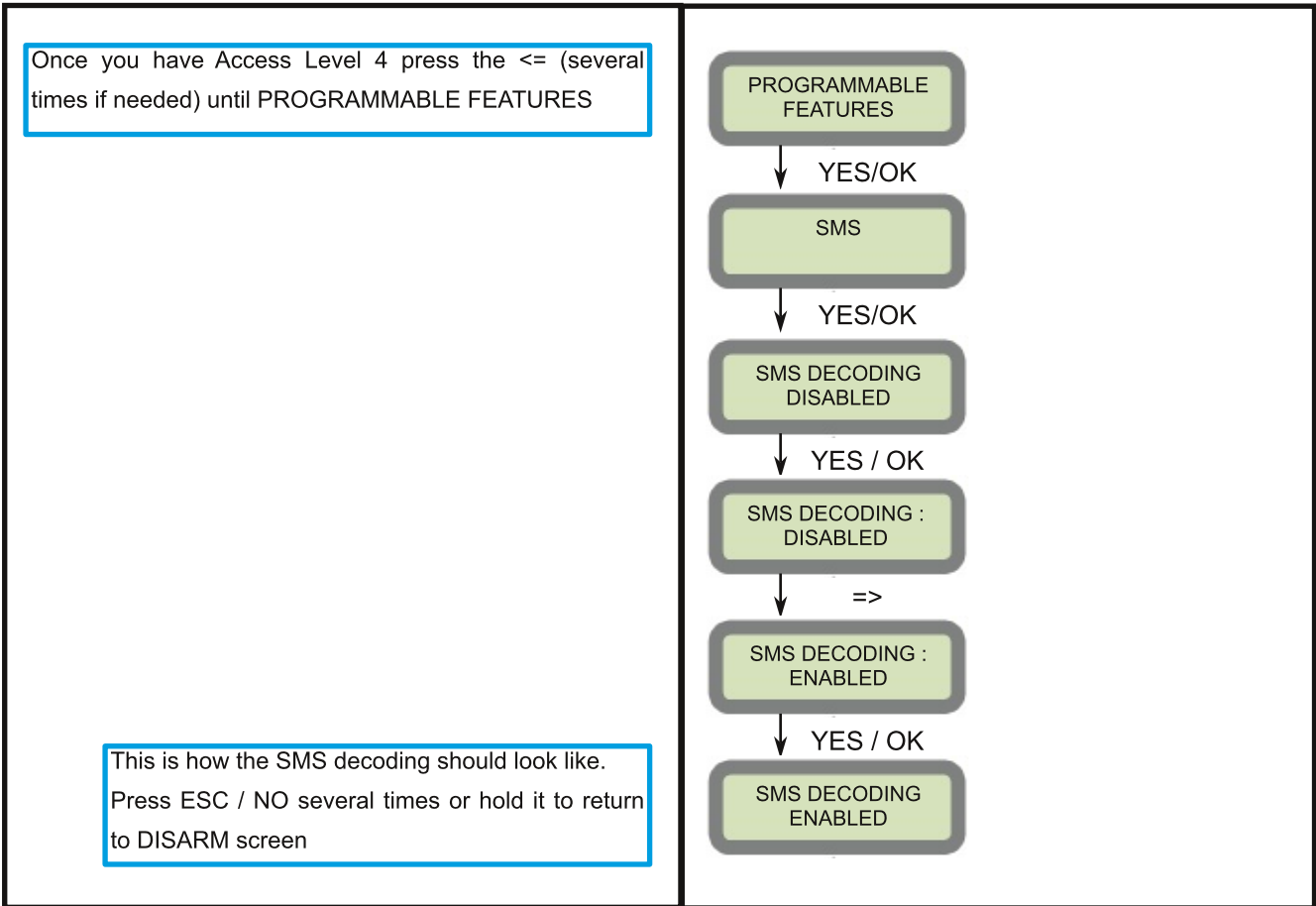
Press the right arrow a few times until you see 2G3G PARAMETERS

The APN code shown is just an example.

This is how the Ringtone should look like.
Press ESC / NO several times or hold it to return to DISARM screen



- Enable SMS reception



- Create a Web Portal account

- Log in with your email and your password to the web portal <http://rsiweb.swingmobility.com>
 - Click on **Create** to start an user account.
 - Enter the user e-mail address, the company name or the user last name and / or his first name
 - Click on **New Panel**
 - Enter the panel name (like: "Home"), the panel SIM card phone number and the full serial number
 - Click on **Save** to confirm the account creation
 - To add another user to the same panel click on **New Account** (optional)
- Your user will receive an e-mail containing teh password to connect to the smartphone app
- Enable a rate plan... click on the button on the upper-right corner, the icon will switch to green and now your user should be able to use the app.



Disabled



Enabled

- Enter an SMS access code

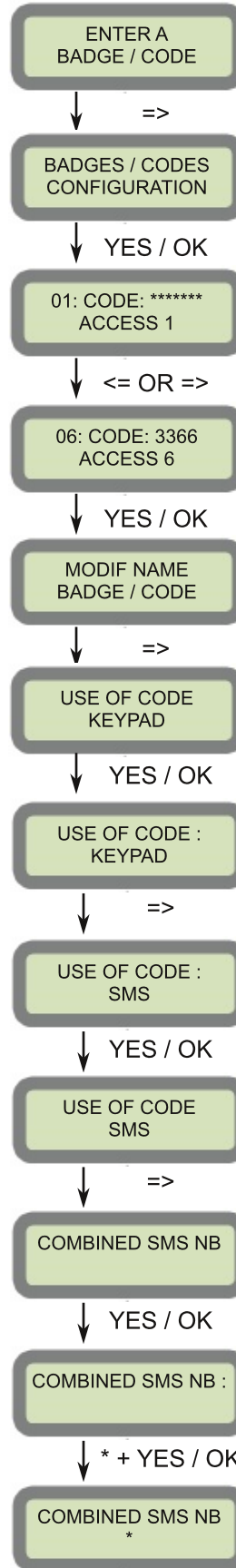
Enter an access code normally (as on page 15)

Press the left or right arrow several times until you get the latest code you entered which will be for SMS usage.

Code position (6), number (3366) and name (Access 6) is shown only as an example.

Press the right arrow several times until you see "USE OF CODE, KEYPAD"

An asterisk (*) will grant access to the panel from any phone number.
If you want to restrict access to a specific phone number add the country code at the beginning.
(+61 for AUS, 0412 345 678 becomes +61412345678).
Press ESC / NO several times or hold it to return to DISARM screen



Partitioning

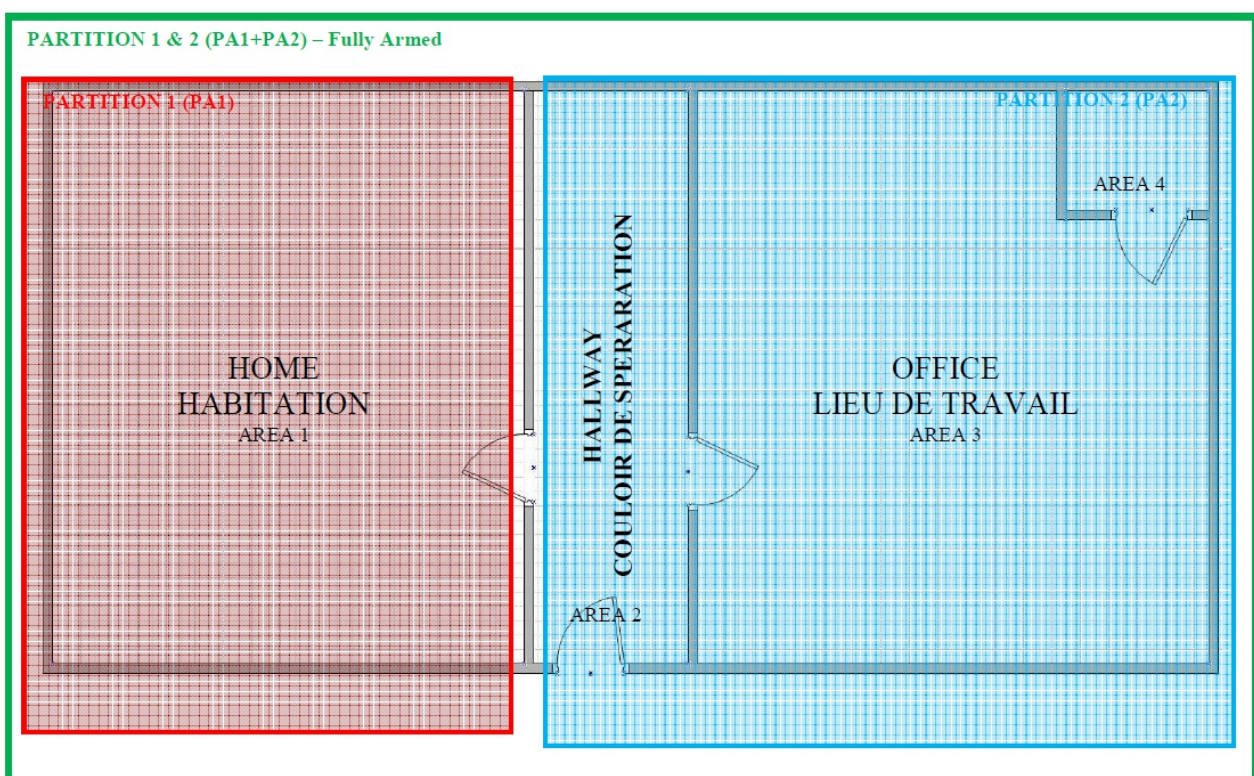
Introduction

Partitioning allows for the independent arming of two separate groups of areas with one control panel.

Each of these partitions can be managed for arming and disarming with a dedicated keyfob, badge or code.

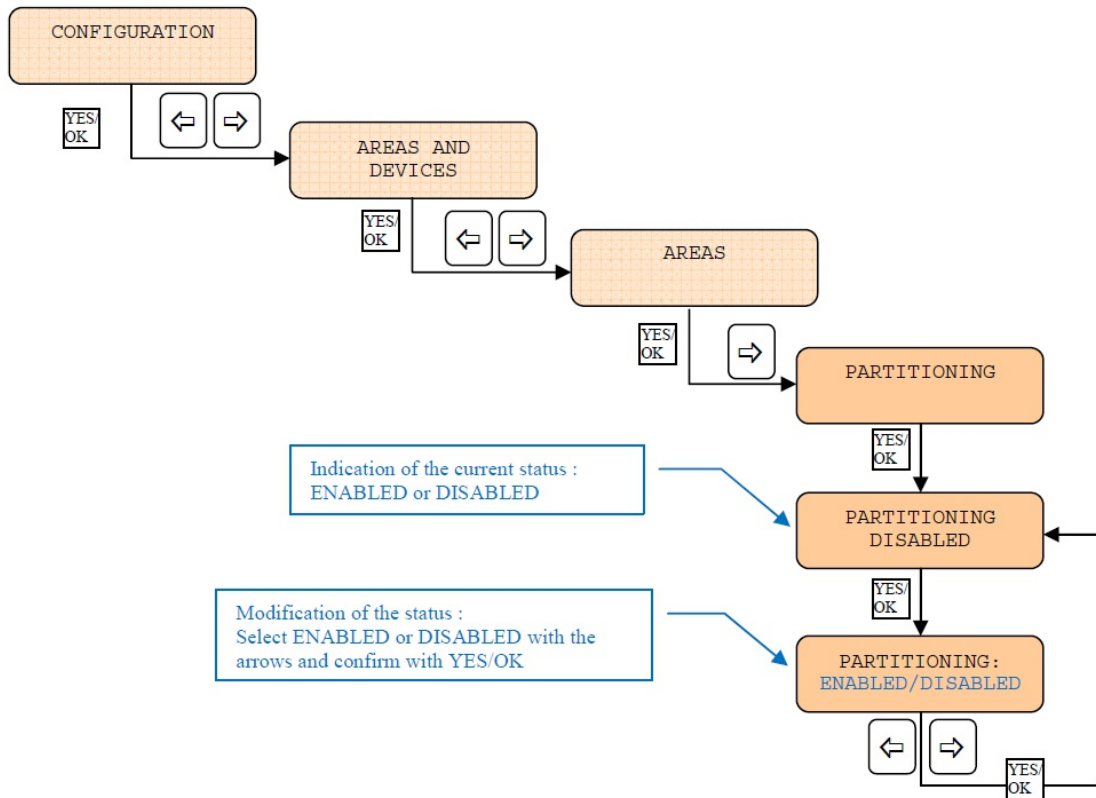
For example: Protect your workplace and place of residence without using two separate alarm systems.

Arm the residential part of the property (PA1) while working, the office (PA2) when you are home or arming both premises at the same time (PA1 + PA2)





1. Enabling / Disabling Partitioning

To enable / disable partitioning you must have control panel firmware XLP.03.65.02.XXX or newer on your control panel and at least one XMA/XMB/WMB keypad learned into the system. System firmware can be found by pressing the number "0" six times ("000000") + YES / OK on the keypad



* By default partitioning is set to DISABLED.

* The following icons  will be displayed on the keypad. The user can toggle between both by pressing the  key on the keypad.

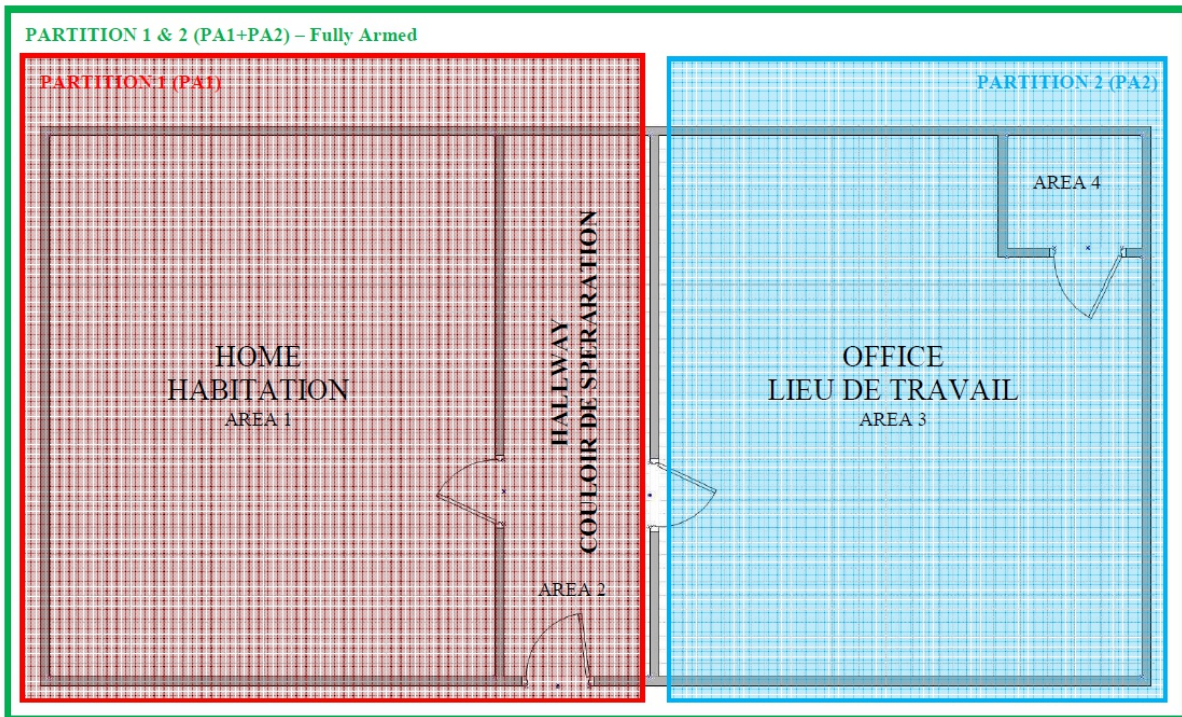
* SP1 and SP2 can't be used while using partitions

2. Assigning Areas to the partitions

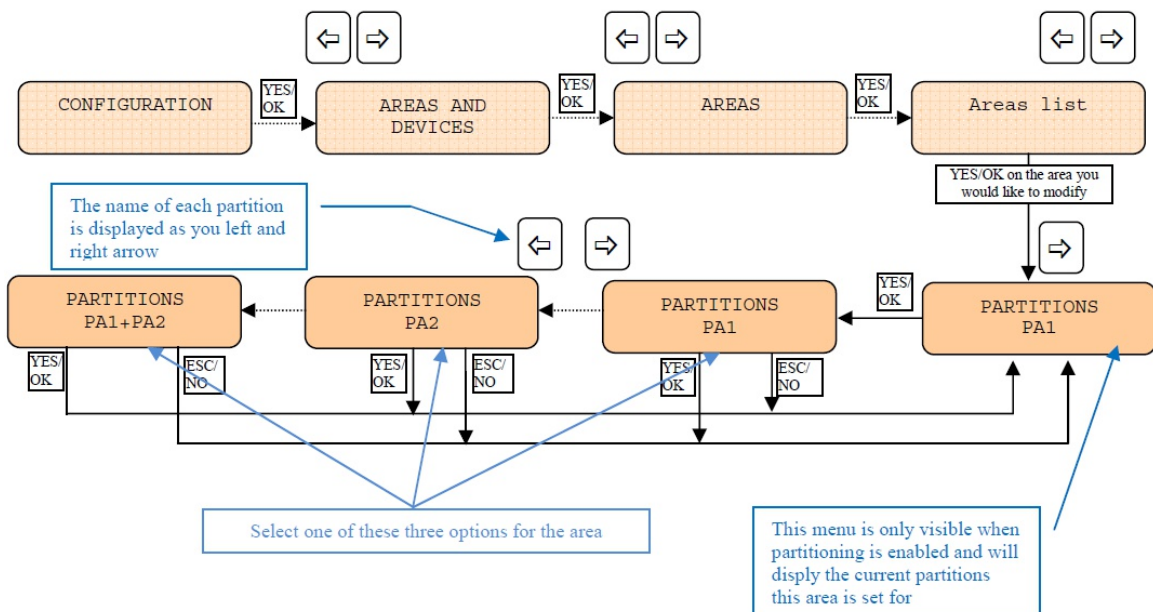
There are 4 distinctive areas that devices can be placed in. Areas are designed to define a logical separation of devices in physical areas. Example: Area 1 contains all home devices, Area 2 all hallway devices, Area 3 all office devices and Area 4 all workroom devices. Partitioning mode allows you to assign each area to one or both partitions.

By default:

- * Partition 1 (PA1) includes Area 1 (delayed) & Area 2 (instant)
- * Partition 2 (PA2) includes Area 3 (delayed) & Area 4 (instant)



Allocating an area to PA1 or PA2:



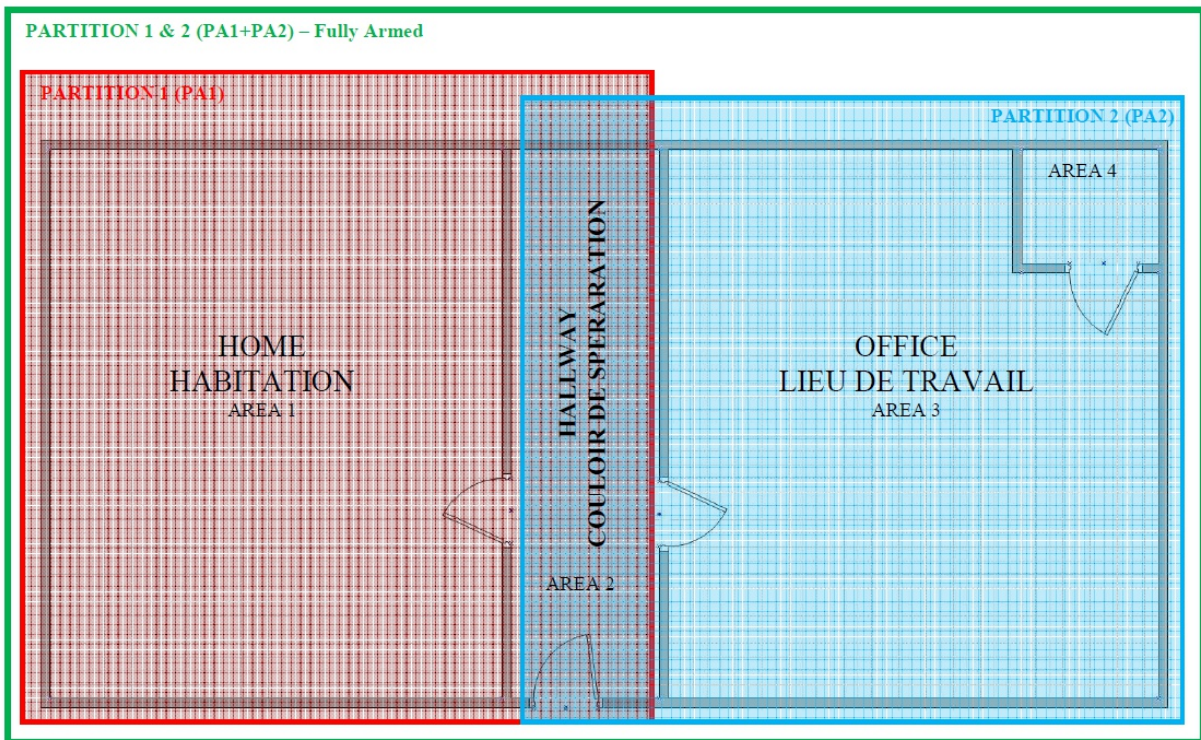
3. Assigning and Area to both partitions:

An area can be assigned to both partitions if needed.

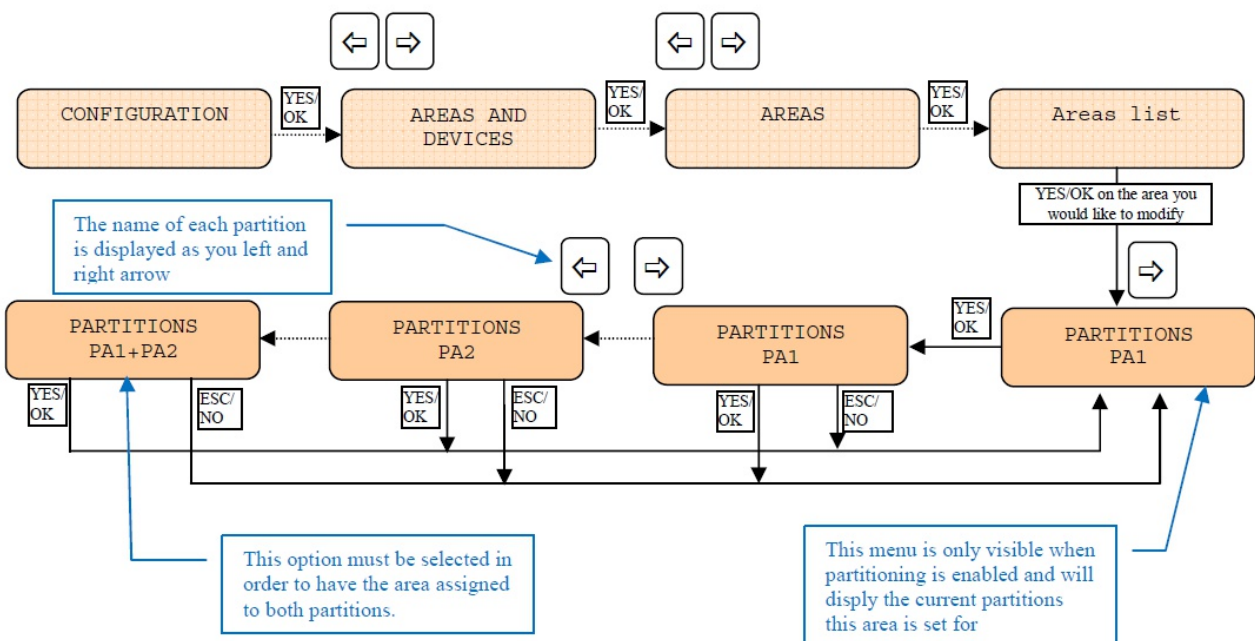
Example:

- * Area 1 and 2 can be assigned to PA1
- * Area 2, 3 and 4 can be assigned to PA2

Area 2 is common to PA1 and PA2



Allocating common area to PA1 and PA2:

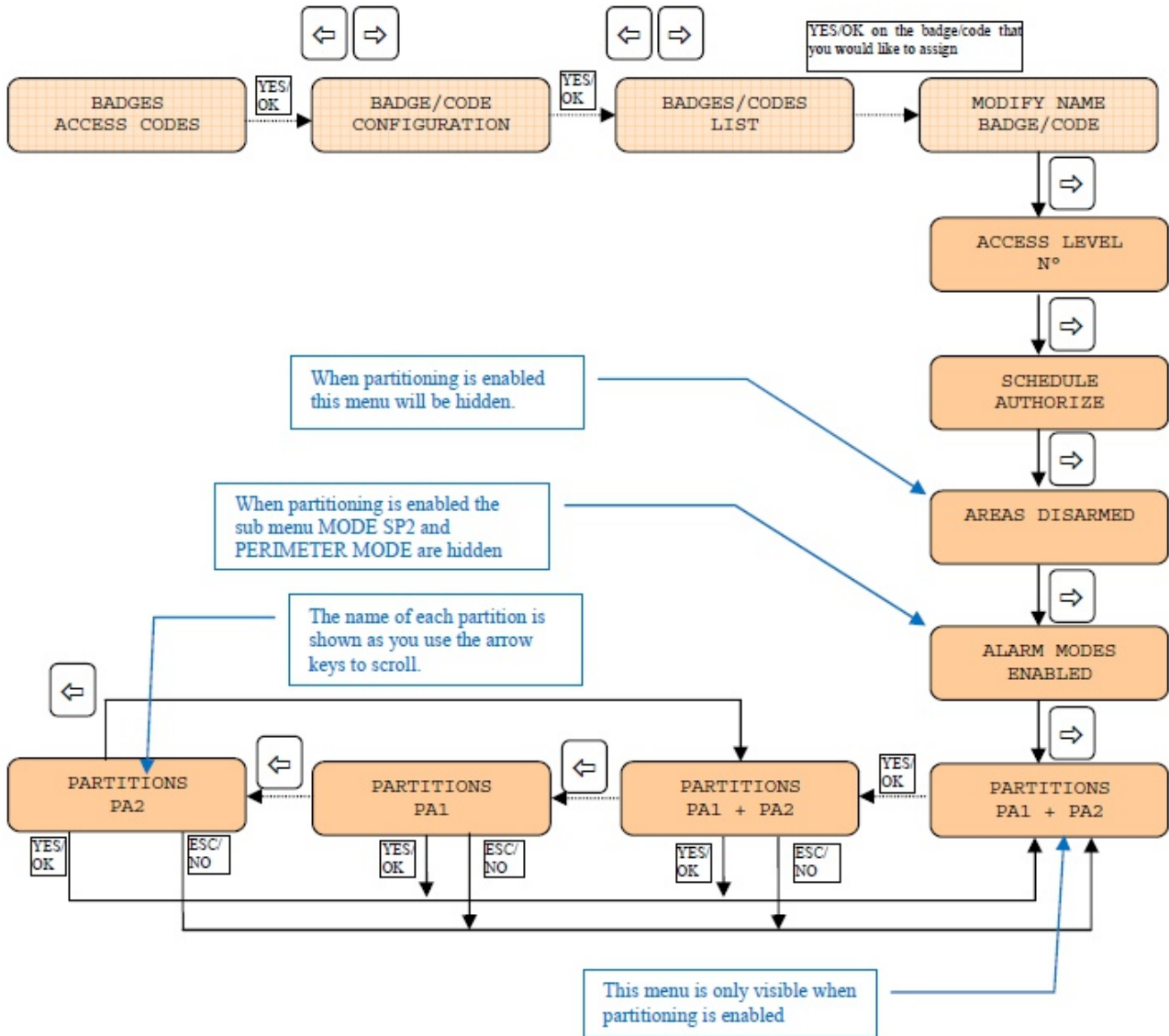


4. Assigning badges, codes or keyfobs to the partitions

When a user code/badge is assigned to one partition, all arming or disarming orders will only concern the partition where it has been assigned.

Allocating the user code/badge to the partition

Each user's code/badge can be assigned to one or both partitions.



By default all user codes/badges are enabled for both partitions

WARNING:

*** When PARTITIONING is enabled:**

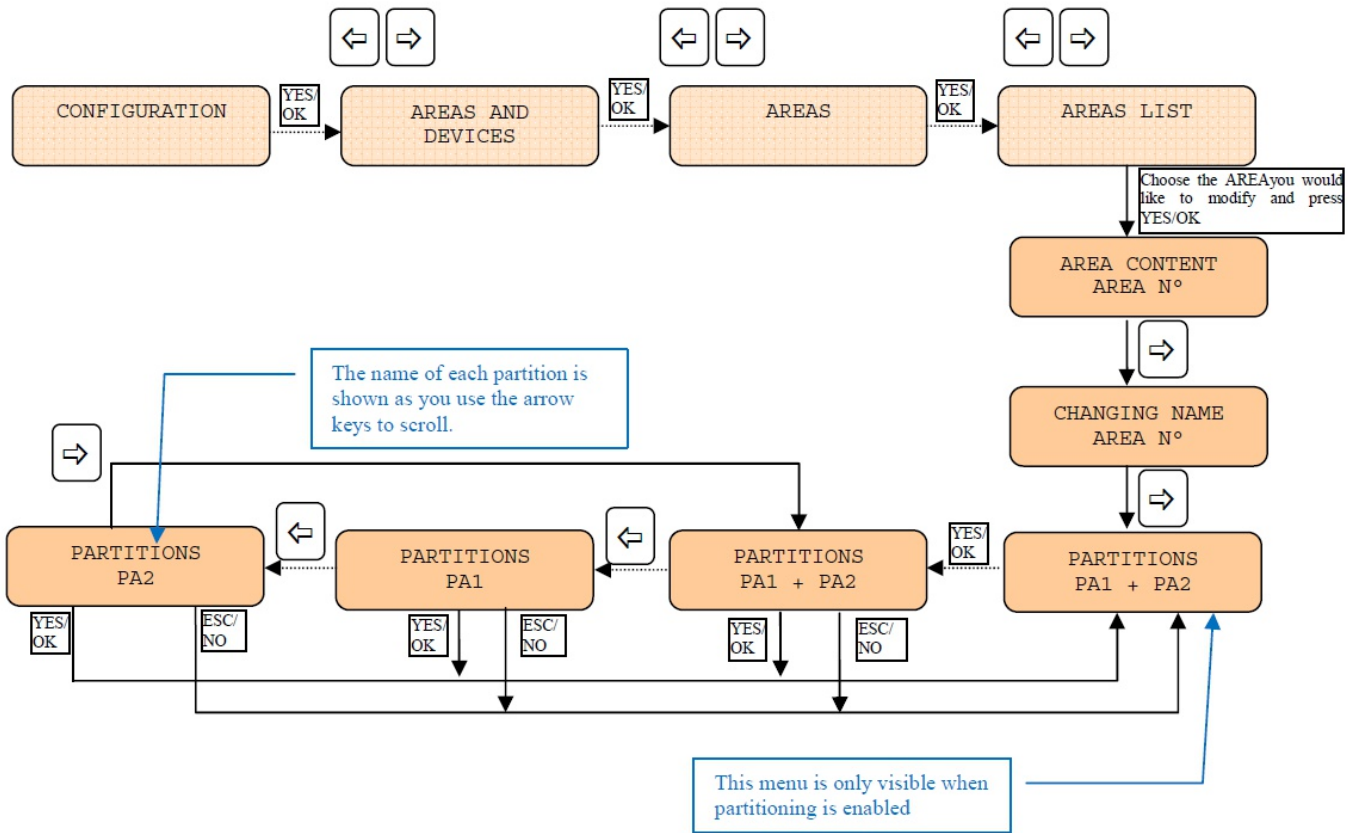
AREAS DISARMED is hidden. If there are settings for this parameter they will not be used for the code/badge.

*** When PARTITIONING is disabled:**

A user code/badge that has been previously assigned to one partition will automatically be set to arm all areas and not only areas of the previously programmed partition.

Allocating Keyfobs to the partitions:

* Each keyfob can be assigned to one or both partitions



When a keyfob is assigned to one partition: all arming and disarming orders will only concern the partition where it has been assigned.

By default the keyfobs are assigned to both partitions

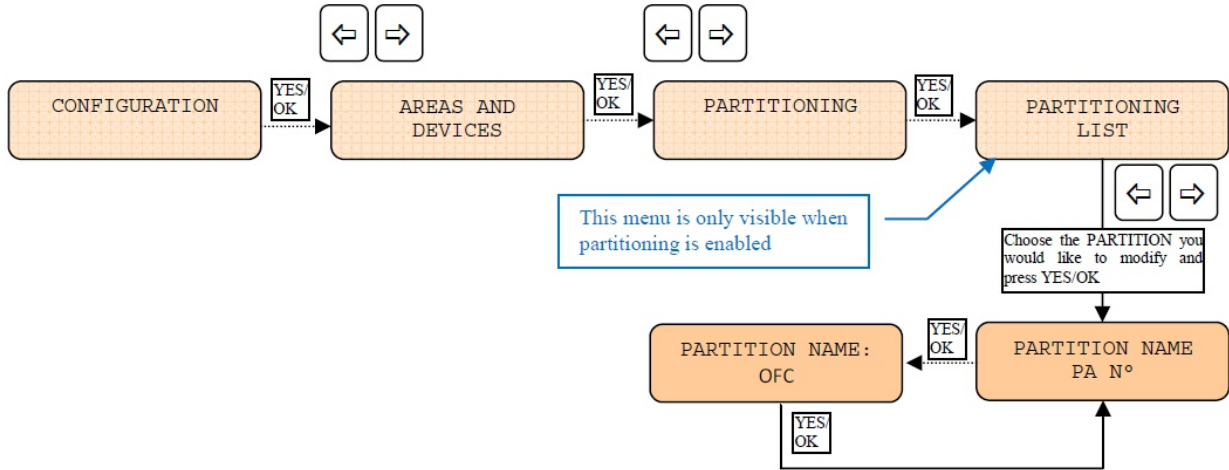
WARNING:

When a keyfob has been assigned to one partition and the PARTITIONING is disabled, the concerned keyfob will arm / disarm all areas and not only areas of the previously concerned partition

5. Naming Partitions

- * Partitions can be named to define the location of the partition.
- * Partition names are limited to 3 characters

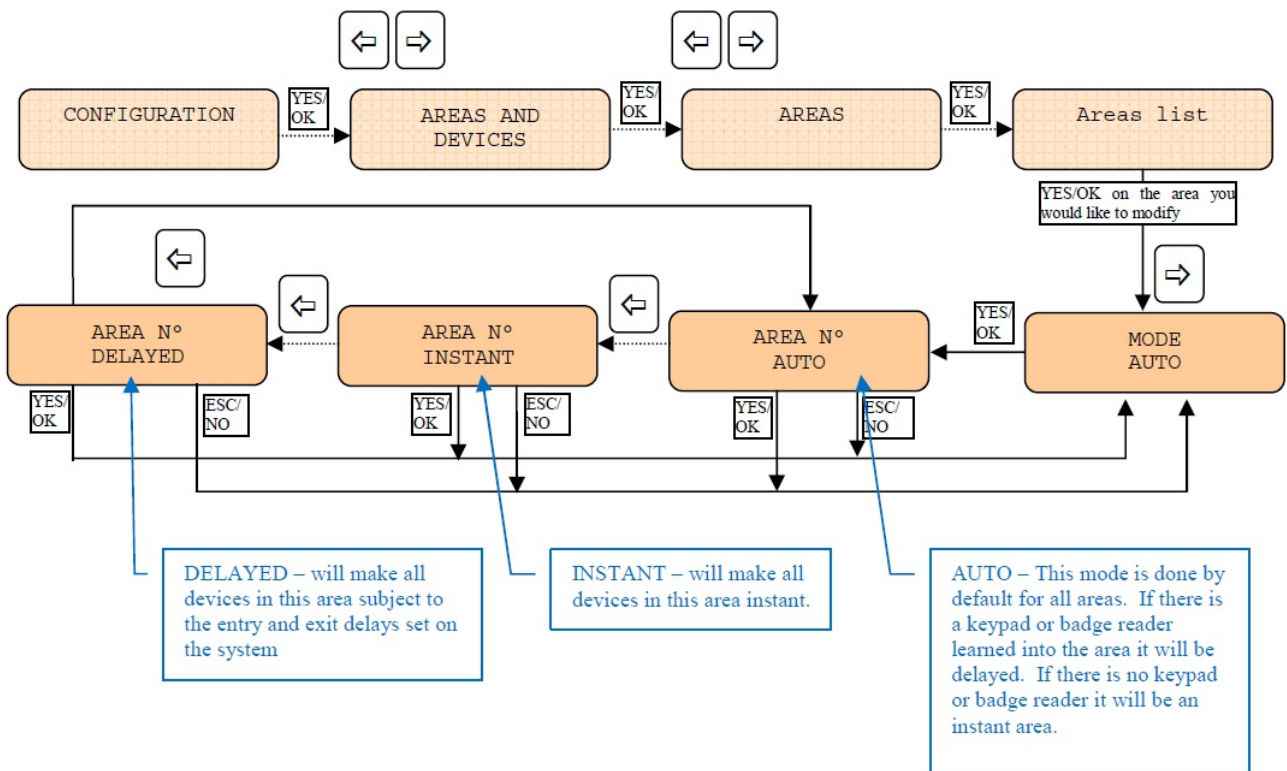
Example: OFC for Office or HME for Home



6. Configuring Entry and Exit Delays

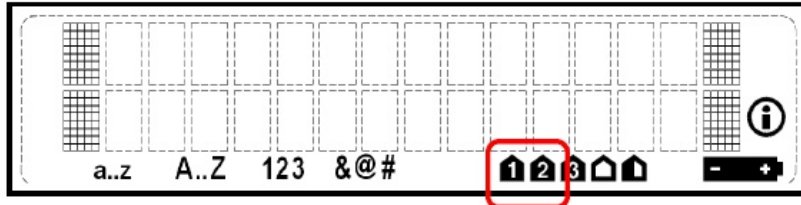
- * Areas are configured for entry and exit delay through one of two methods:
 - Automatic - System detects the presence of an entry/exit device (keypad, badge reader) and adds entry/exit delay to all devices in that area.
 - Manual - Installer selected area behaviour between instant or delay

* This feature can be set whether Partitioning is enabled or disabled.



6. Arming and Disarming Partitions (XMA/XMB/WMB)

- * The keypads offer full support of the partitioning feature.
- * With these keypads, the user, with full rights on both partitions, is able to select the partition to be armed or disarmed.
- * The LCD of the new keypad includes icons that will be used to identify the current selected partition.



Selecting a partition:

Press to toggle the choice of partition (1 or 2 or 12). This selection is recorded in the memory of the keypad avoiding a new selection by the user in case the selected is the same.

WARNING:

The selection of the partition is not available when partitioning is disabled.

7. Partitioning status on keypad display

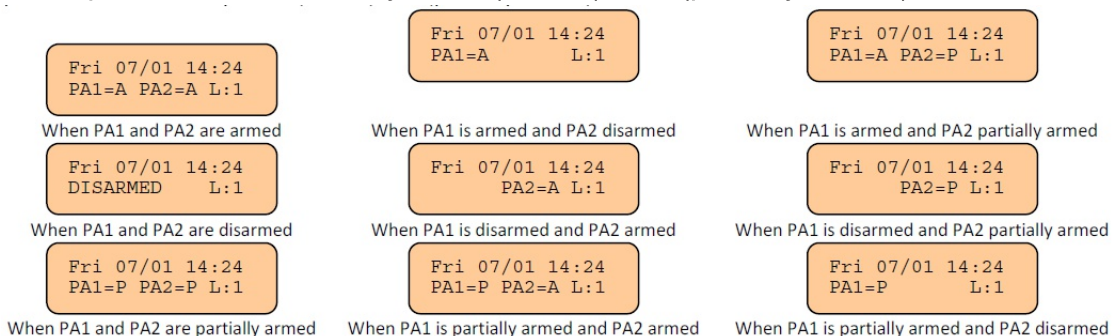
- * When partitioning is enabled, the keypad will display the current status of each partition.

Display when partitioning is disabled:



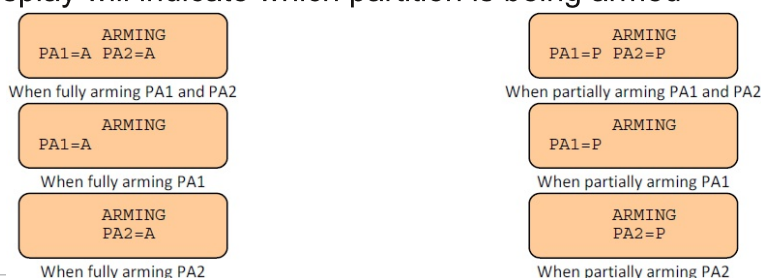
Display when partitioning is enabled:

The keypad display will show when a partition is armed or partially armed. In this case, the name of the partition is followed by the A (armed) or P (partially armed) indicator.



Display during arming process when partitioning is enabled:

When arming the display will indicate which partition is being armed



Replacing batteries

As much as you can, it is advisable to keep power at all times on devices and panel... otherwise you may need to do additional troubleshooting on the system.

If the batteries are flat and the panel / devices don't show signs of life, just change the batteries and then make sure all is working as it should ("Maintenance => Display faulty devices" is a good place to start).

If the batteries still have power then keep the power and do the following:

- On the panel:

- * Disable the monitoring and open the lid.
- * If the panel has external power supply, make sure that the panel senses it by pressing "999997 + YES / OK"... if it says "Power supply connected" then you can just change the batteries straight away, once done, close the lid and enable monitoring again.
- * Add a temporary power supply, even a 12 v battery should keep the panel alive for a few minutes while you change the batteries. Do this even if the batteries are lithium, a short temporary external power supply won't affect the panel or the lithium batteries.

- On the devices:

- * Disable monitoring (or Maintenance => Replace batteries)
- * Change batteries one by one instead of all of them at once, this will ensure the device will still be powered.
- * If the device holds only one battery, just change it and check the device afterwards.

Input configuration

- Change the Level to "Level 4", then right arrow to "CONFIGURATION" and "YES / OK"
- Once you see "GENERAL PARAMETERS" press "YES / OK" and right arrow a few times until you see "PROGRAMMABLE INPUTS", press "YES / OK".
- if you want to program the INPUT 1 then press "YES / OK"
- if you want to program the INPUT 2 then press the right arrow and then "YES / OK"

Below is a description of the settings of each Input:

Transmission:

ENABLED: Will transmit the event no matter the panel status.

DISABLED: No transmission will be sent.

ONLY IF ARMED: Will transmit the event only when the system is fully armed.

Alarm Mode:

ALARM: Appearance of the alarm only.

ALARM/END: Appearance and restoral of the event.

Input type:

NORMALLY OPEN: The external wired device is "open circuit" while in non alarm state.

NORMALLY CLOSED: The external wired device is in "closed circuit" while in non alarm state. If using this setting, the panel must be externally powered.

Event type:

Usually set to "INTRUSION", it indicates what event will be generated when this input triggers. Choose the event that suits you.

Input name: Is the name that the control room will see when this input is triggered (if looking at Alarm Viewer).

Siren mode:

SIREN: Activation of all sirens on the system

WITHOUT SIREN: Only keypads and badge readers will sound

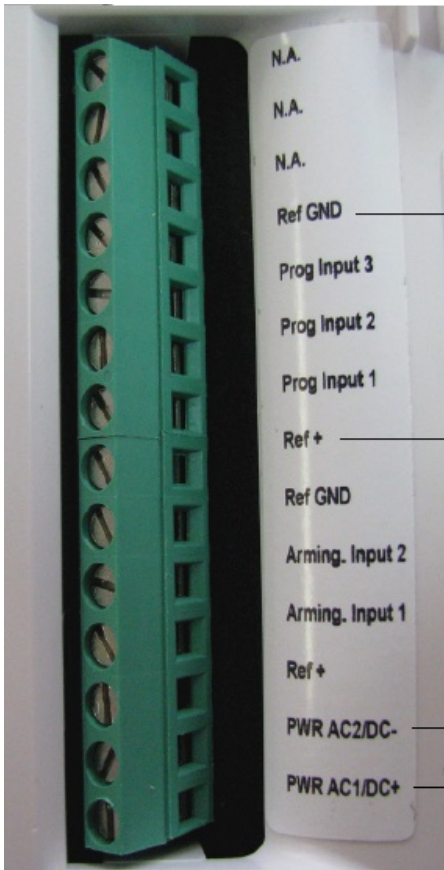
SILENT: No activation of any sound.

DELAY BEEPS: Sounding of delay beeps then full siren

Mapping:

DISABLED: Feature disabled.

* choice of detector *: This is a 1 to 1 relationship between MotionViewer and the programmable input. When the input is triggered it will force the chosen MotionViewer to take a 10 second video no matter the current status of the MotionViewer. We suggest that this is only used when using the event types "INTRUSION" and "PANIC" or the video won't automatically download to the control room.

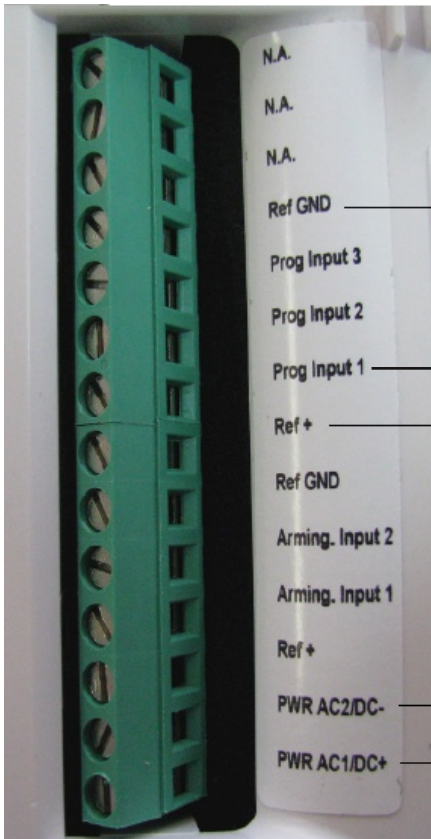


When using an external hardwired device that is powered, the ground (negative) wire must be hooked up here.

When using a dry contact one wire must be hooked up here, to provide voltage to the INPUT (as that is how the INPUT is triggered).

When using input NORMALLY CLOSED you must use 9v to 12v DC external power.

Example of a panic button.



- (GND)
+ 12 v DC

Output configuration

- Change the Level to "Level 4", then right arrow to "CONFIGURATION" and "YES / OK"
- Once you see "GENERAL PARAMETERS" press "YES / OK" and right arrow a few times until you see "PROGRAMMABLE OUTPUTS", press "YES / OK".
- if you want to program the OUTPUT 1 then press "YES / OK"
- for the other outputs press the right arrow and then "YES / OK"

Below is a description of the settings of each Output:

Status:

- ENABLED: Will activate the output based on the configuration
- DISABLED: Output will not be triggered

Lenght activation: (0 - 900 sec)

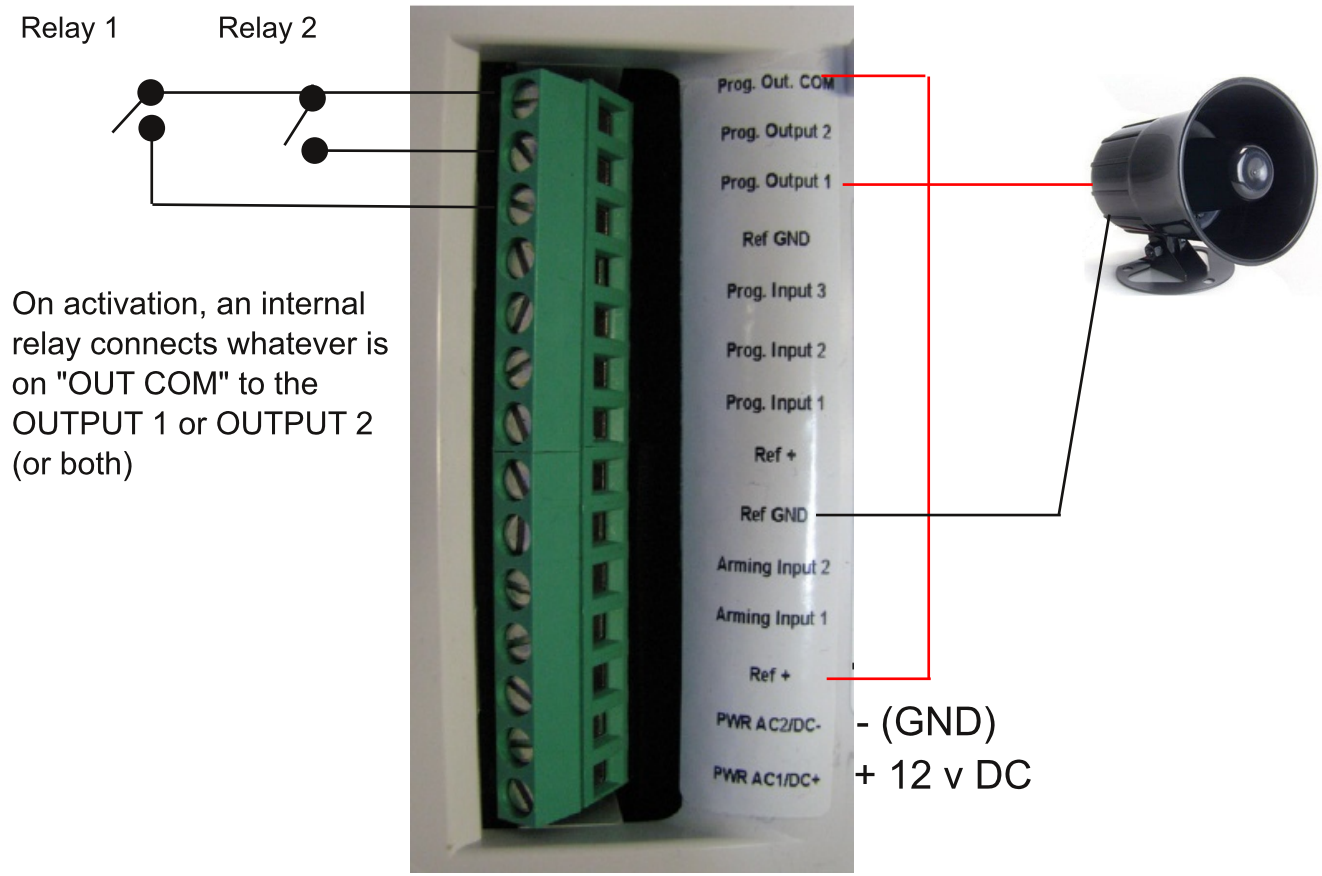
Remote controlled:

- ENABLED: Allows the output to be controlled by Frontel software (from control room)
- DISABLED: Doesn't allow the output to be controlled by Frontel software

Event type:

Usually set to "INTRUSION", it indicates under which condition the Output will be triggered. Choose the event that suits you.

Output name: Allows you to name the programmable output for identification



Troubleshooting and Maintenance

Some of the most common operations were already mentioned on this manual, for those please refer to its corresponding page:

- * **Perform a 2G3G level** = Page 20
- * **Test communications** = Use the "useful codes" on page 19, if all your tests are ok then you are ready for real transmissions.
- * **Locate devices and perform radio range test** = Page 21

* **Walk test (aka. Functional test devices):**

Go to Maintenance (you need to be level 3 or 4) and press "YES / OK" then press a few times the right arrow until you see "FUNCTIONAL TEST DEVICES" and press "YES / OK". The panel will put all detectors and reed switches in a "walk test mode"... they will pretend the system is armed and they will show a red light if they are in ALARM... (no light means no alarm).

This feature is useful to make sure the detectors are triggering when someone appears on their field of view, if you don't see the red light it could mean that you may need to adjust your detector position.

Another handy use of this function is when you use an CT (reed switch acting as universal transmitter) or IUT connected to another device, it will tell you if the device is currently in alarm or not.

* **Ethernet status:**

This should show you an IP address, otherwise you need to check your IP parameters (under "CONFIGURATION" => "GENERAL PARAMETERS" => "ETHERNET PARAMETERS"), cable or router settings (?)

* **Lost installer code:**

There is no default code. There are 2 ways to recover from a lost installer code:

- If the panel can connect to the control room, they have the ability to read the panel configuration and give you the installer code.
- You will need to default the panel and start all over again, with the additional difficulty of defaulting all your devices as well.

* **Radio protocols**

Videofied use 2 radio protocols (the older and the newer). Devices that have been launched recently can operate with both as they are backwards compatible, however some devices have only the old protocol at this stage (RSI developers are working so all device models will work on the newer protocol). The protocol to use is decided once you finish the initial configuration of the system... if the panel only see devices able to use the newer protocol it will be locked on it, otherwise it will be locked into the old protocol.

What are the practical consequences of this ?

If you finish the initial configuration and you have all newer protocol devices the panel will be locked into it, and if later on you want to add an old protocol device (like an RC701)... you won't be able to do it. (unless you delete all your devices, default the panel, start all over again and make sure you add the RC701 while on the initial configuration stage).

* How to default devices

In some cases you need to default the devices... the most common scenario is when a device has been paired to "system A" and you want to use it on "system B" without deleting it from the original system.

When the panel power up after a default it will generate a security key, and that key will be shared with all the peripherals belonging to it. The device will not pair with another system as the security key will not match, in order to delete the security key from the device you need to default the device.

- 1) Take batteries out of the device
- 2) Locate and press the tamper of the device several times (10-15). Skip this step for OMV's.
- 3) Press the programming button of the device several times (10-15). For keypads, press all the keys.
- 4) Press and hold the tamper (keep OMV's the upright position)
- 5) Make sure the panel is in "learning mode", either the keypad says "Press program button of device" or, if you are adding the first keypad, press the programming button of the panel once briefly, you should see a quick 1 flash. **DO NOT HOLD THE PROGRAMMING BUTTON OF THE PANEL** as it will default it.
- 6) Place 1 battery, let the device start. It's LED will flash briefly but should NOT stay ON (otherwise you are not holding the tamper and will need to start the procedure again)
- 7) Press the programming button of the device, its LED should flash and pair to the system... if it doesn't, don't despair, the procedure can take a few times to get the result. Start again.
- 8) Once the device has paired you can release the tamper, place the rest of the batteries and keep going as usual.

* Tamper's on OMV's

Tampers on the OMV are triggered by an accelerometer, so the device is "aware" of its position. It is recommended to add the device to the panel while in the upright position. Once all are mounted you must arm the system (making sure no movement is detected) and acknowledge any tamper from an OMV with "Continue", this will tell the OMV that its current position is the right position for the job. You can then disarm the system and a tamper signal will be triggered if anyone moves the OMV in the future.

- Disabling the tamper:

In some cases you may want to disable the tamper on the OMV... to do so:

1. Delete the OMV from the device configuration menu.
2. Press and hold the OMV initialization button for 5 seconds. The red LED will turn on for 2 seconds to confirm the setting.
3. Pair the OMV back with your panel.

- To enable the tamper again:

1. Delete the OMV from the device configuration menu.
2. Press and hold the OMV initialization button for 5 seconds. The red LED will turn on for 2 seconds to confirm the setting.
3. Press and hold the init button for 5 seconds. The red LED will turn on for 2 seconds, off for half a second and back on for 2 seconds.
4. Pair the OMV back with your panel.

*** How to adjust sensitivity on a detector**

You can adjust the sensitivity of a detector by changing its name.

- \$9 = Maximum sensitivity
- \$8 = Improved sensitivity
- \$0 = Normal sensitivity (same as nothing !)
- \$1 = Decreased sensitivity
- \$2 = Minimal sensitivity

By adding those 2 characters at the end of the detector name you will be changing the sensitivity

*** Keypad shows <----xx---->**

It means it lost comms with the panel

- a) Briefly press programming button on the panel to see if you get one flash, if not panel has no power.
- b) Move the keypad close to the panel and press CLR and ESC on the keypad to see if it pairs back.
- c) Default the keypad with the procedure described in page 45

*** Changing the SIM card**

It is not necessary (or advisable) to power off the system in order to change the SIM card. Just ensure the modem is off by disabling monitoring and turning the "ringtone" feature OFF (see page 29), once that is done you can safely change the SIM card.

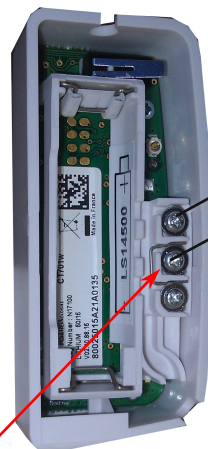
*** Adding a smoke detector (with CT or IUT)**

There is no Videofied smoke detectors for Australia, however you can combine an Australian compliant smoke detector with outputs and a CT or IUT (reed switch or Universal Transmitter).

Inside the CT you will find 3 screws, and there will be a wire connecting two of them... you need to move that wire and connect the smoke detector as the picture below

CT from factory

Adapted to be a universal transmitter



Notice the wire link

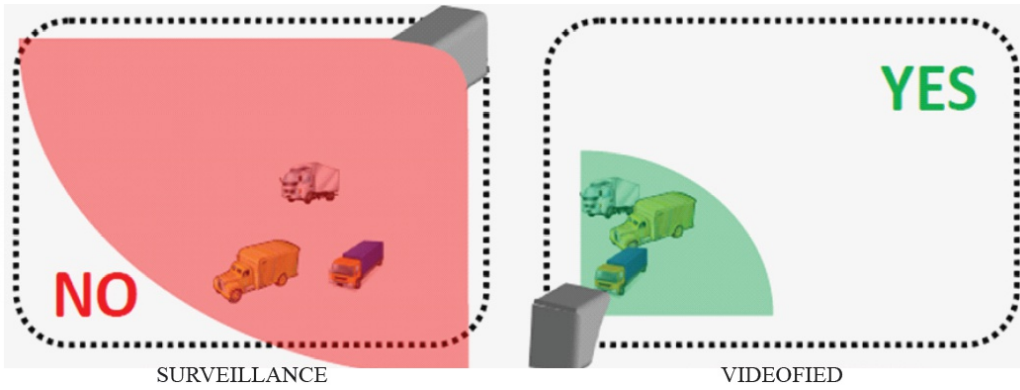
Smoke detector relay

Normally Open
Common

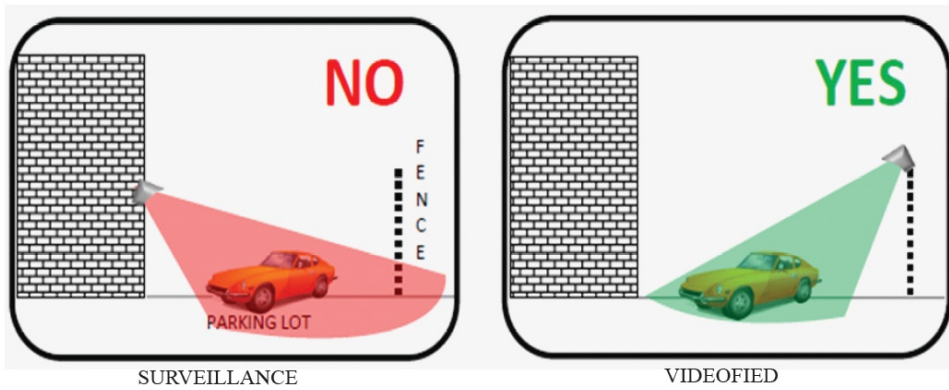


*** General advice on mounting outdoor detectors**

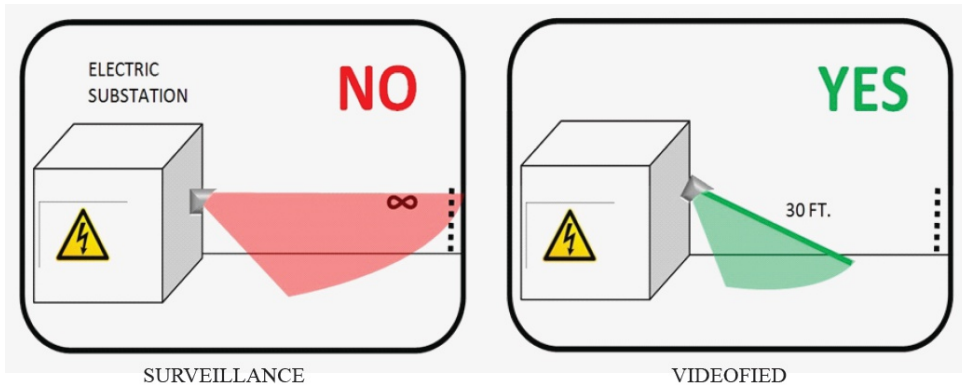
Protect **ASSETS** not **AREA**

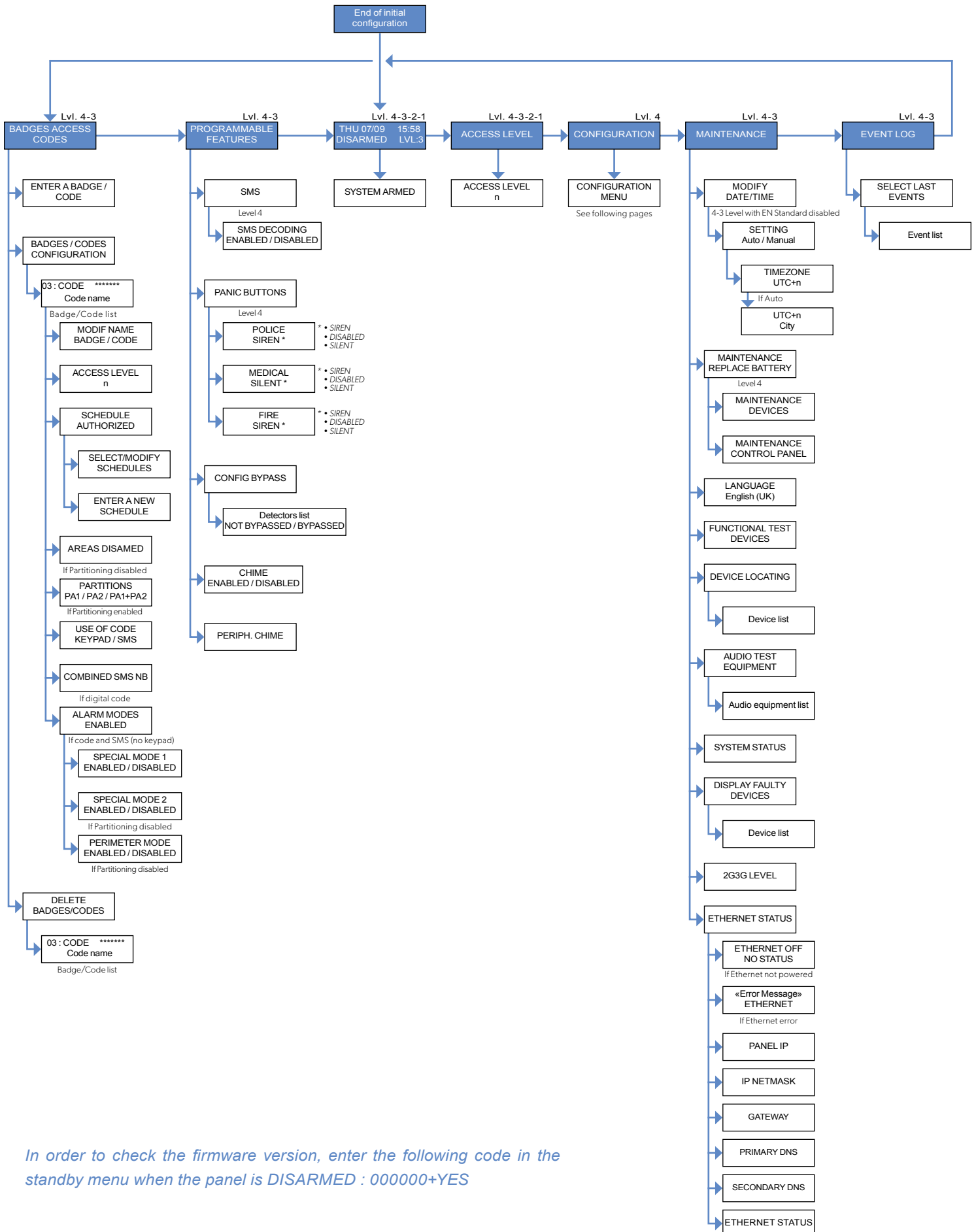


Look **Outside-in**, not **Inside-out**

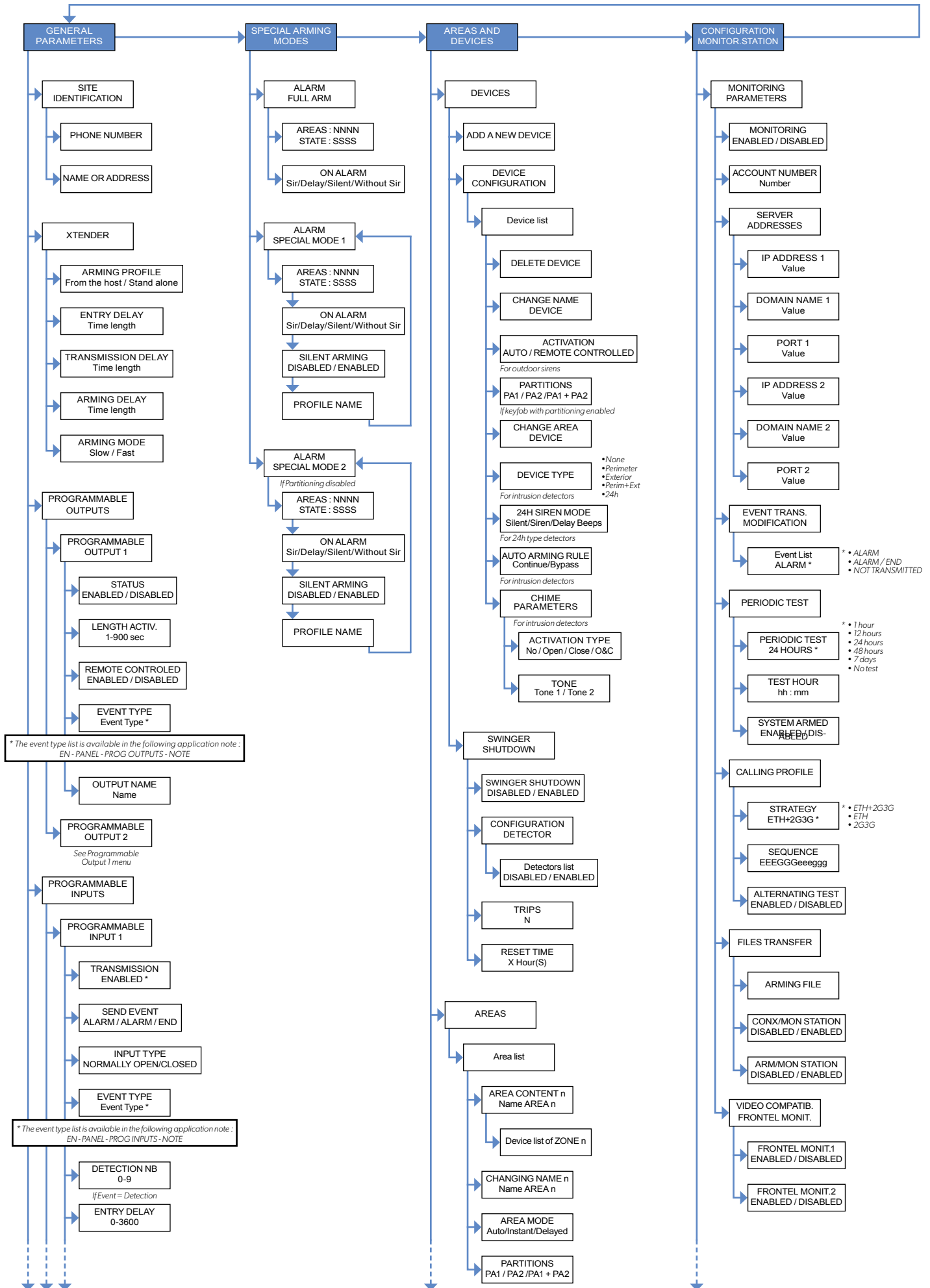


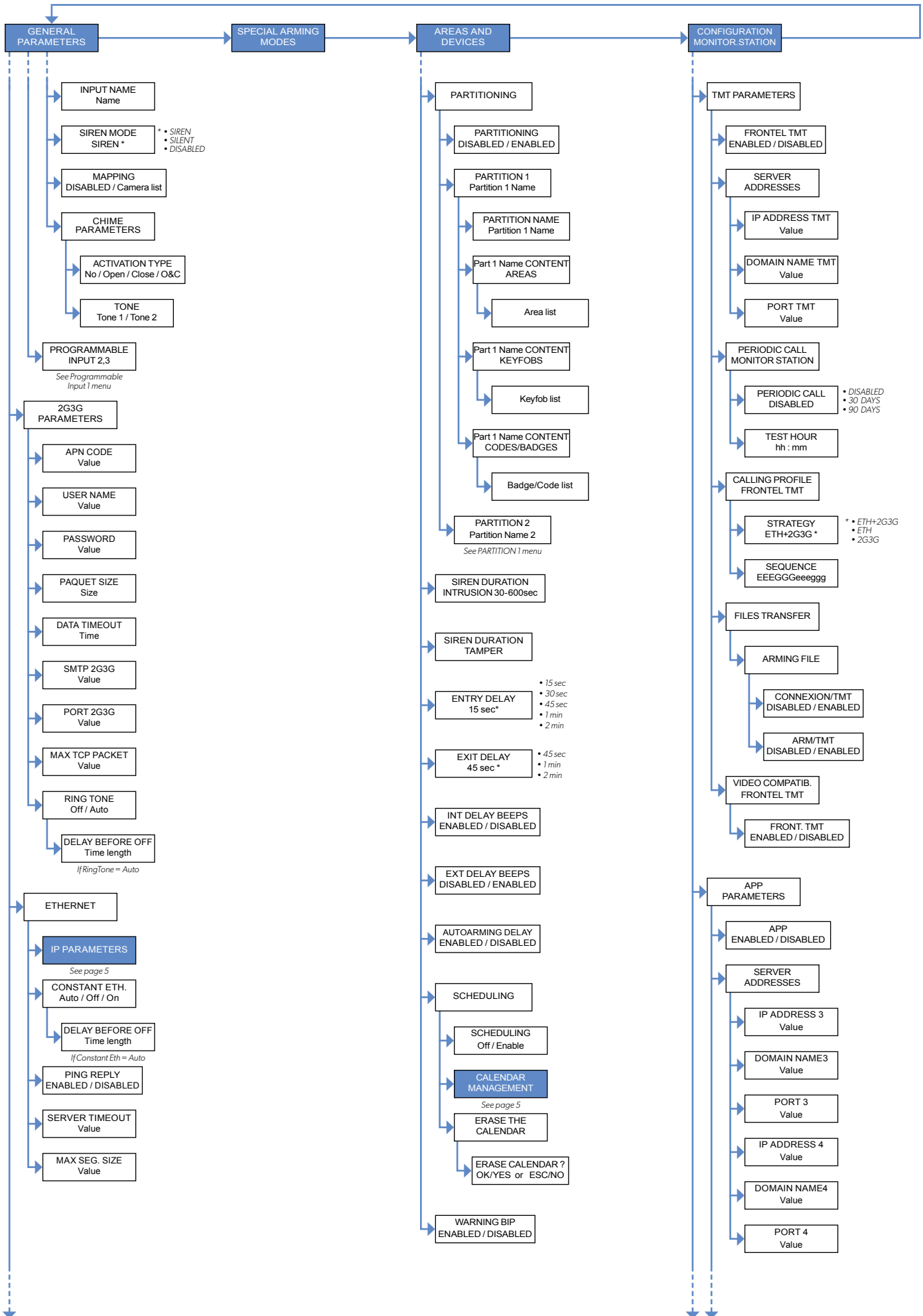
Terminate the view of the PIR

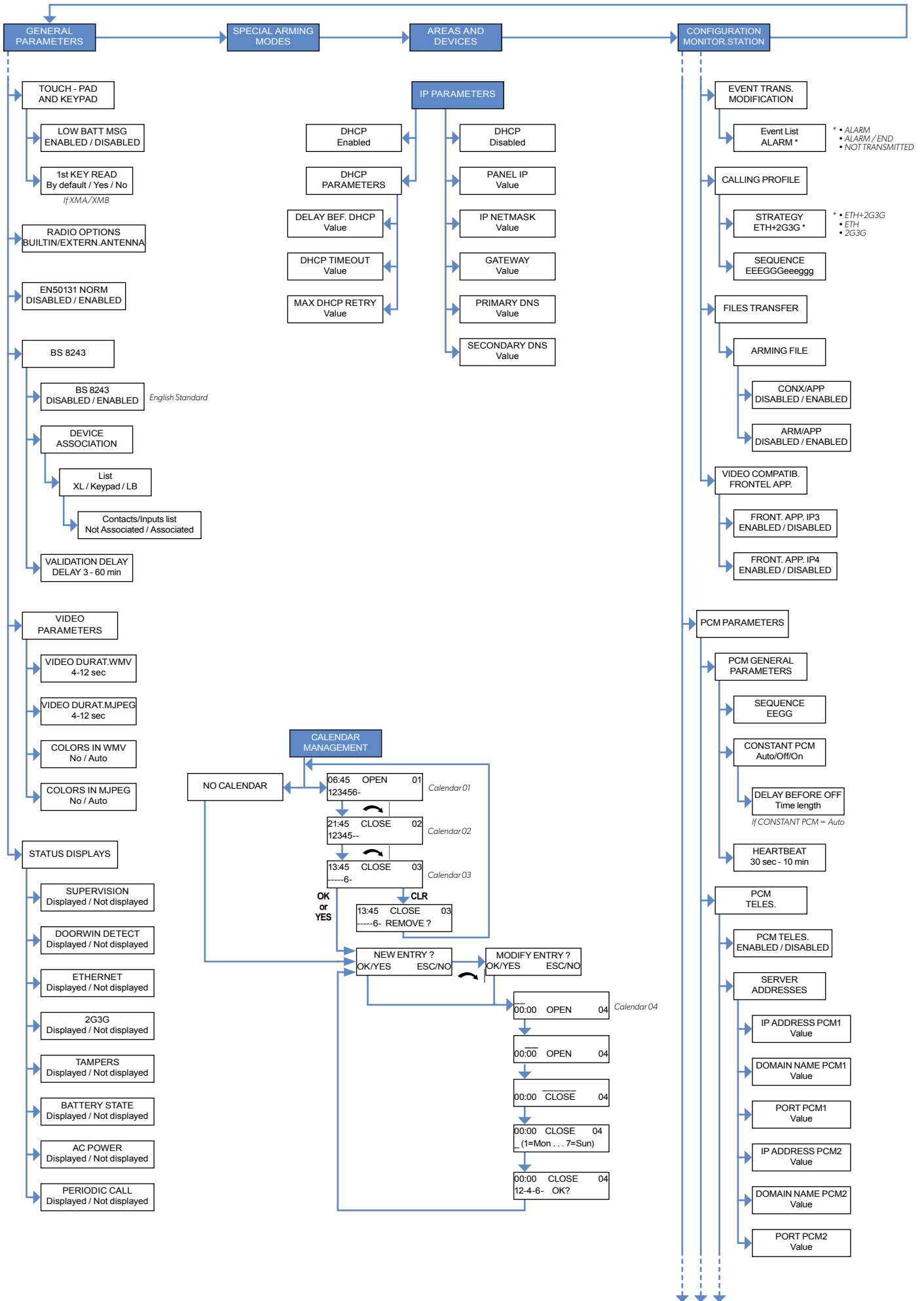


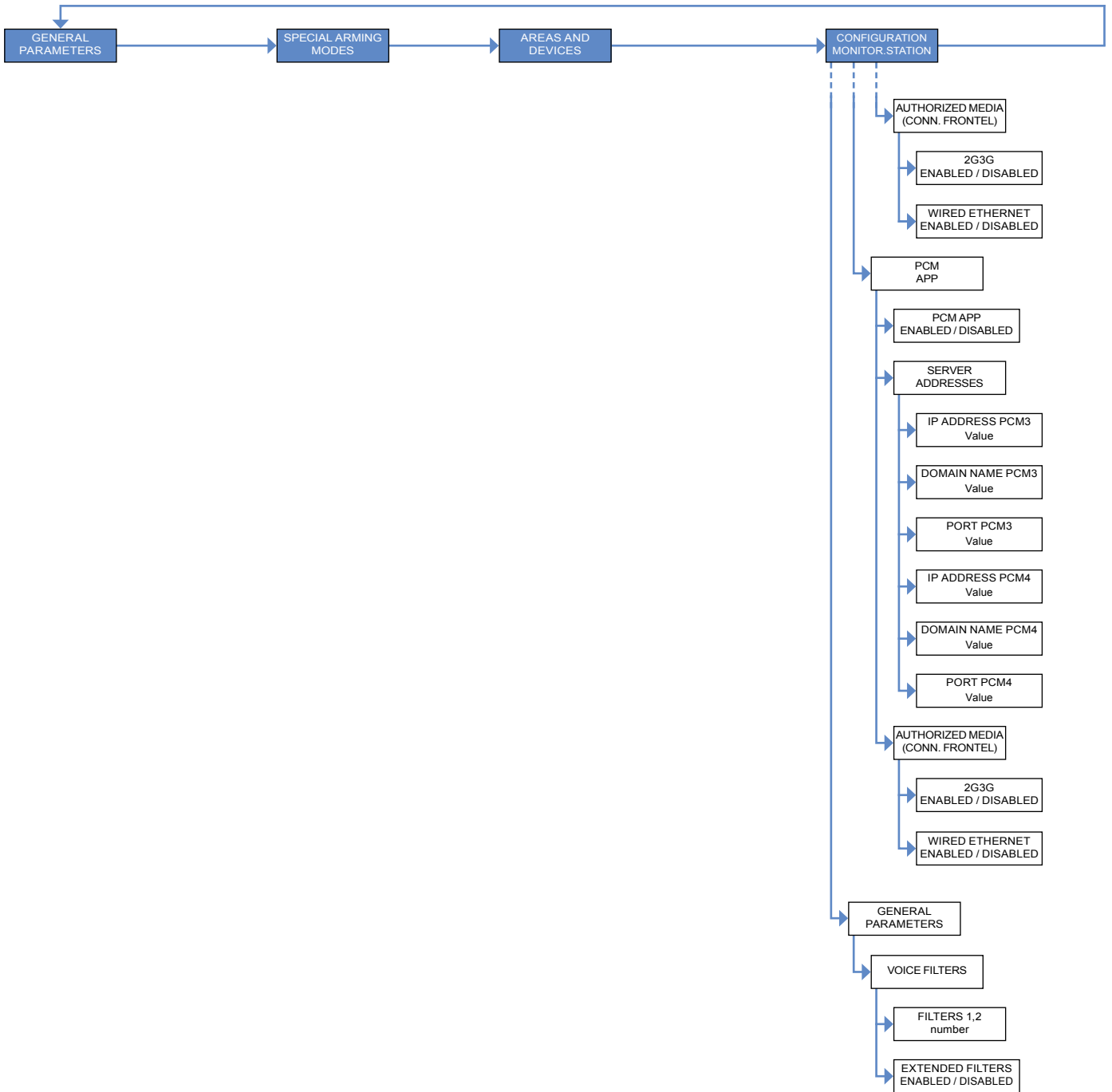


In order to check the firmware version, enter the following code in the standby menu when the panel is DISARMED : 000000+YES









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

