Description

The XLL control panel is a Videofied wireless alarm system operated by battery or mains power supply. This panel is intended mainly for residential and commercial markets. With the Motion Viewers™ and Videofied® range of products, the XLL panel provides video verification in case of intrusion.

The XLL panel is a standalone alarm system with an integrated GPRS / GSM communicator for connection to a central station.

Wireless Technology

The XLL GPRS, along with all Videofied devices, uses the patented S2View®, 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, both more difficult to install and 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.

The RSI VIDEO TECHNOLOGIES team wishes you a good installation.
Introduction.................................................................................................................................2
Summary...........................................................................................................................................3

1. XLL Panel Setup.................................................................................................................................4
1.1 XLL Panel Setup.........................................................................................................................................4
1.2 SIM Card Installation..........................................................................................................................4
1.3 XLL Assembly.....................................................................................................................................4
1.4 Powering and Initialization....................................................................................................................5
1.5 Pairing the Remote Keypad....................................................................................................................5

2. XLL Panel Programming...........................................................................................................................6

3. XLL Features Guide................................................................................................................................13
3.1 Get to Access level 4............................................................................................................................13
3.2 How to Arm/Disarm the System............................................................................................................13
3.3 Arming and Siren Mode Configuration...............................................................................................14
3.4 Manage badges and access codes........................................................................................................15
3.5 Delete the keypad or any other device..................................................................................................17
3.6 Read the events log..............................................................................................................................18
3.7 Opening the cover of an installed panel..............................................................................................18
3.8 Golden rules.......................................................................................................................................18

4. Transmitted Events List..........................................................................................................................19

5. 2G3G Error Codes...............................................................................................................................20

6. Technical Specifications and Security Notes........................................................................................21
1. XLL Panel Setup

1.1 XLL Panel Setup

Open the box and remove the cardboard mounting template sitting on top. Place the template on the wall with the arrow pointing upward. Mark the 5 screw points on the wall and drill pilot holes for wall anchors. Install wall anchors, then attach the base of the control panel to the wall.

XLL panel is provided with a reinforcement brace kit including 4 velcro straps. Insert the 4 straps in the back casing, then mount the casing on the wall. (The EN50131 standard requires the installation of this brace kit).

A screw must be used in the tamper protection hole for the panel wall tamper to function correctly.

Insert the Alkaline D type batteries as shown; ensuring the polarity matches the labeling on the inside of the battery cover.

1.2 SIM Card Installation

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

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

1.3 XLL Assembly

Connect the panel’s face to its base by carefully placing the hinges on it. 2 locking clips are provided to strengthen the hinges: position each locking clip before locking them completely. (The EN50131 standard requires the installation of these locking clips).
1.4 Powering and Initialization

- The panel is powered either with a mains power supply with 4 backup LR20 Alkaline batteries (Option 1 recommended) or with 4 LSH20 Lithium batteries (Option 2).
- Press and hold the PROGRAMMING BUTTON for 10 seconds, until the indicator LED blinks twice.
- The panel is now reset, a CMA, XMA or XMB has to be enrolled to configure the panel.

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

**Option 1**

- Batteries cable
- Batteries connector
- Mains Connector
- Programming button

To install the power supply inside the box, break the plastic battery separator.

**Option 2**

www.videofied.com
1.5 Pairing the Remote Keypad

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

  ![Keypad Display](image)

  - **Press on both CLR and ESC NO keys at the same time** and release. The indicator LED on the keypad will blink rapidly. Wait for the keypad to pair.
  - **If the keypad doesn’t pair up with the panel** and shows «XX», it certainly means that it is still paired to another system and needs to be reset. Take the batteries out, and press repeatedly on the keypad tamper switch. Then proceed to the above steps.
The system can also be programmed in: french, italian, german, dutch, spanish, swedish, portuguese, danish, czech and polish.

The language can be changed at any time once the panel is programmed in the MAINTENANCE menu.

The Radio Range test must be run during the device learning process in order to ensure proper pairing with the control panel. This test measures the strength of communication between the device and the control panel. The keypad will display a real time radio range value on a scale of 9.

To receive the most accurate results you must run the radio range test for at least 30 seconds.

**Result must be 8 out of 9 or better for reliable transmission.**

Using the Alphanumeric Keypad, enter the Installer Code of your choice.

The Installer Code will be used for all future maintenance and configuration.

**This code is important to keep track of.**

**There is no back door or Default codes to the system.**

Please refer to the restriction rule for codes (Chapter 3.4). Some codes are already used by default and therefore cannot be used.
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 a 4-8 digit account number provided by the Central Station.
Test Periodicity: 1 hour, 12 hours, 24 hours, 48 hours, 7 days or no tests.

We suggest a 24 hours periodic test call.

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

ALARM: event transmitted upon occurrence.

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

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

Please liaise with your Monitoring Station to ensure that the requested events to transmit are correctly set.
The **IP1 address**, **Domain name 1** and/or **Port 1** are provided by the monitoring station. Leave Port details at 888 unless otherwise instructed.

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

**WARNING:** You will use either an **IP address** or a **Domain name** but **not both**, leave the **Domain name** blank if an **IP address** has already been entered.

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

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

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

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

To switch between **UPPER** and lower case, use the **M/m key** from CMA keypad or hold a digit key (0-9) for XMA/XMB.
Once the 2G3G test completed, the keypad will display one of the following results:

- A level between 0/5 and 5/5.
- A GPRS Error code (please see Chapter 5: 2G3G errors codes and contact your technical support).

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

The 2G3G level test can last several minutes. Do not interrupt the test or remove the SIM card during the test.

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

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 3.3.

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

Other values are available: 2 minutes, 1 minutes, 45 seconds, 30 seconds, or 15 seconds.
Each device has a unique programming button or a specific manipulation. Please refer to the Installation Sheet for the device you would like to program.

Please check the radio level of each device on its final location. The result must be 8 out of 9 as a minimum (please refer to the Radio Range section, page 7 for further details).

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

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

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

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

If you wish to use an user code, please skip this step and once the system configuration done go to the BADGES/ACCESS CODES menu (please refer to chapter 3.4 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.
3.1 Get to Access level 4

To unlock and get access to the installer level 4, you need to successively enter TWO codes (in any order):

- INSTALLER CODE (entered during initial programming)
- USER CODE (Level 3): the user must authorize the installer to get access to the configuration of his panel.

3.2 How to Arm/Disarm the System

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

<table>
<thead>
<tr>
<th></th>
<th>Full arming with user code</th>
<th>Full arming with badge</th>
<th>Special Arming 1</th>
<th>Special Arming 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>With remote keypad</td>
<td>Enter your user code and press OK or YES</td>
<td>Present your badge on the keypad (XMB model only)</td>
<td>Press enter your user code and press OK or YES</td>
<td>Press</td>
</tr>
<tr>
<td>With remote badge reader BR250</td>
<td>N/A</td>
<td>Present your badge on the badge reader</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>With remote keyfob</td>
<td>N/A</td>
<td>N/A</td>
<td>Press</td>
<td>Press 2</td>
</tr>
</tbody>
</table>
3.3 Arming and Siren Mode Configuration

- Use 🔄 🔄 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

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.

<table>
<thead>
<tr>
<th>A</th>
<th>Armed</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>Disarmed</td>
</tr>
<tr>
<td>P</td>
<td>Perimeter (by default: all opening contacts*)</td>
</tr>
<tr>
<td>E</td>
<td>External (by default: all opening contacts with external access*)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Siren</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate triggering of all sirens</td>
<td></td>
</tr>
<tr>
<td>Delay Beeps</td>
<td>Entry/Exit delay beeps, then triggering of all sirens</td>
</tr>
<tr>
<td>Silent</td>
<td>No Sirens, No Beeps</td>
</tr>
<tr>
<td>Without Siren</td>
<td>Beeps on the keypad only</td>
</tr>
</tbody>
</table>

* You can set your devices as: External, Perimeter, or External + Perimeter. Please go to the menu:

**CONFIGURATION (LVL 4) > AREAS AND DEVICES > DEVICES > DEVICES CONFIGURATION > DEVICE TYPE**
3.4 Manage badges and access codes

Access Level

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Definition &amp; Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>LVL 1</td>
<td>Standby Level</td>
</tr>
<tr>
<td>LVL 2</td>
<td>Restricted USER level, where it is only possible to arm/disarm the system.</td>
</tr>
<tr>
<td>LVL 3</td>
<td>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.</td>
</tr>
<tr>
<td>LVL 4</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

How to return to the LVL1?

- After 1 min of no use of the keypad and no tests running, the display returns to the standby display and LVL1.
- When standby display, if the ESC NO key is held during 5s, the level is changed to LVL1.
Enter a new end user Badge/Code

BADGES
ACCESS CODES
OK or YES

ENTER A
BADGE/CODE
OK or YES

BADGE OR CODE
Enter a 4-6 digit user code and
OK or YES
or present a badge in front of the reader until
you hear the registration beep.

CONFIRM THE
CODE
OK or YES

CODE NAME :
OK or YES

ACCESS 2
ENTRY COMPLETE

Delete an end user Badge/Code

ENTER A
BADGE/CODE
Press twice on the
right arrow

DELETING
BADGES/CODES
OK or YES

Badges/codes list
Select badge/code
then
OK or YES

DELETING CODE
ACCESS 5
OK or YES

CODE
DELETED

Reserved Codes
Up to 19 codes (or badges) can be registered into the panel with the engineer code.
A code has 4 to 6 digits (0 to 9).
The table presents the reserved code possibilities that cannot be used.
Those codes are used for maintenance or as panic/duress codes.
A total of 186 codes are forbidden.

<table>
<thead>
<tr>
<th>Reserved Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
</tr>
<tr>
<td>From 9998 to 9999</td>
</tr>
<tr>
<td>From 99998 to 99999</td>
</tr>
<tr>
<td>From 314157 to 314159</td>
</tr>
<tr>
<td>All user codes +1</td>
</tr>
<tr>
<td>All user codes +2</td>
</tr>
<tr>
<td>All user codes -1</td>
</tr>
<tr>
<td>All user codes -2</td>
</tr>
</tbody>
</table>

When a code is created (1000 for example),
the 2 next codes and previous codes (0998, 0999, 1001 and 1002) will be automatically reserved.
The +1 code (1001) is used for disarming under duress.
The +2 code (1002) is used for panic.
The -1 and -2 codes (0998 et 0999) are reserved to prevent conflicts when creating a new user code.
3.5 Delete the keypad or any other device

You can now remove the batteries from the device.
3.6 Read the event log

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

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

3.7 Opening the cover of an installed panel

Unscrew the locking screw on the left-hand side of the panel, using a paper clip push through the opening hole to open the panel’s cover.

3.8 Golden Rules

1. Area 1 is always delayed. When you register a keypad or a badge reader into an area, that area will automatically be delayed.
2. Never position a panel next to a high voltage electrical cabinet.
3. Press CLR to erase a typing mistake.
4. Never register the same device twice (delete from the system first).
5. Registration of up to 25 devices (including the keypad).
6. Respect indoor infrared devices installation height (2m10 to 2m30).
7. Outdoor cameras have to be installed at 2m60 to 3 meters height. Those devices need to 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.
4. Transmitted Events List

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

The installer can modify the default sending settings for those events, although it will end the EN50131 standard compliance.

These are the default transmitted events:

- DEVICE (intrusions)
- ALERT (Panic Buttons)
- PANEL LOW BATT.
- TAMPER
- DEVICE LOW BATT.
- PERIODIC TEST
- DURESS CODE
- FIRE
- MEDICAL ASSIST.
- ETHERNET CABLE
- AC POWER LOSS (AC Power supply)

The following events are not sent by default:

- PANEL RESET
- PHONELINE FAULT
- RADIO JAMMING
- SUPERVISION
- 5 WRONG CODES
- ALARM CANCEL
- ARM/DISARM (On/Off)
- ZONE BYPASS (bypass function enabling/ disabiling)
- SWINGER SHUTDOWN

There are 3 different transmission states:

<table>
<thead>
<tr>
<th>Transmission State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALARM</td>
<td>event transmitted upon occurrence</td>
</tr>
<tr>
<td>ALARM/END</td>
<td>event is transmitted on occurrence and on event restoral</td>
</tr>
<tr>
<td>NOT TRANSMITTED</td>
<td>event is not transmitted, however it will appear on the keypad.</td>
</tr>
</tbody>
</table>

Example:

If the monitoring station system is set to receive arms and disarms, the ARM / DISARM parameter must be changed from NOT TRANSMITTED to ALARM / END.

How to modify the transmission state:

- At initial programming, right after the PERIODIC TEST CALL step:

  Press OK or YES to access EVENT TRANS. MODIFICATION menu.

- After initial programming, using a remote keypad:

  Use the arrows to access:

  CONFIGURATION (level 4) > CONFIGURATION MONITOR. STATION > MONITORING PARAMETERS > EVENT TRANS. MODIFICATION

  Then use the arrows to determine the event to modify. Press OK or YES to edit.
5. 2G3G Error Codes

**IMPORTANT:** The PIN of the SIM card has to be deactivated or 0000.

The following is a list of error codes that can appear after the 2G3G test.

### 2G3G LEVEL : ERROR XXX

In case of 2G3G (GPRS) errors during initial programming, we strongly suggest to continue with the installation and perform the 2G3G (GPRS) level test again once achieved.

This error checklist is provided for information purposes only. **This is not a comprehensive list**, but it is representative of most cases. Some events or codes are subject to change by SIM card operators.

However, the GPRS level test errors results in the majority of cases have the following causes:

- **SIM Card activation Delay:**
  Some operators require an additional delay up to 48 hours to activate automatic data transmission. Please check with your operator prior to installation.

- **APN CODE, USERNAME and PASSWORD:**
  The GPRS (2G3G) settings are supplied by the operator. Please make sure you have entered the code exactly as indicated by your local SIM card operator.

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

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

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

<table>
<thead>
<tr>
<th>Codes</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>03 ou 04</td>
<td>No network coverage or no SIM card inserted</td>
</tr>
<tr>
<td>003</td>
<td>SIM card not detected/not inserted</td>
</tr>
<tr>
<td>010</td>
<td>SIM not inserted</td>
</tr>
<tr>
<td>011</td>
<td>PIN code necessary -&gt; PIN code must be deactivated</td>
</tr>
<tr>
<td>012</td>
<td>PUK code necessary, SIM card blocked</td>
</tr>
<tr>
<td>013</td>
<td>Default SIM card</td>
</tr>
<tr>
<td>014</td>
<td>SIM card busy</td>
</tr>
<tr>
<td>015</td>
<td>Error on SIM</td>
</tr>
<tr>
<td>030, 043, 057, 102, 132, ...</td>
<td></td>
</tr>
</tbody>
</table>
  - 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.
6. Technical Specifications and Security Notes

### Operating Frequency
868/915/920 MHz

### Required Voltage
Nominal voltage = 6 V  
Low battery limit = 4.2 V

### Powering
Type B: 1 external power supply with battery backup 4x 1.5 Alkaline D cells (Option 1)  
or  
Type C: 8 x 1,5 V D Alkaline batteries (Option 2)

### Current consumption
Standby (1h average) = 420 μA ; Max = 1,3 A

### Operating temperature
-10° / +40° C (-14° /+104° F)

### Maximum relative humidity
75%, without condensing

### Dimensions (LxWxD)
225 mm x 180 mm x 55 mm (9 in. x 7 in. x 2-1/6 in)

### Weight
520 g (without batteries)

### Approvals
EN50131-1: 2006; + A1: 2009  
Grade 2 - Class II  
The panel must be used with a EN50131-3 certified keypad (CMA, XMA or XMB)
EN50131-3: 2009  
Grade 2 - ACE Type B
EN50131-4: 2009  
Grade 2 - Siren type W
Grade 2
EN50131-6: 2008  
Grade 2 - Type C
EN50130-5: 1998  
Class II

### Embedded
- Siren  
- 15 min maximum duration  
- Indoor use only  
- Can be self-powered  
- 105 dB (A) at 1 meter