Description

Since 2002, RSI VIDEO TECHNOLOGIES provides the only wireless video verification on the market, thanks to the Motion Viewer™ detectors and to the Videofied® product range.

After 2 years of development, RSI VIDEO TECHNOLOGIES is proud to present the new W alarm panel. The W alarm panel is wireless and mains powered with a backup rechargeable battery (provided). The W panel is the first Videofied® alarm panel that can be used as a connected device.

This panel is intended for residential and commercial markets.

Like all the Videofied® alarm panels, the W panel is compatible with every radio device manufactured by RSI VIDEO TECHNOLOGIES.

Technology

The W alarm panel uses the S2View® patented technology. That interactive and wireless technology ensures signal integrity. The bidirectional radio link maximizes the signal reliability.

AES encryption protects the communication between the panel and the devices. Transmission security is optimal.

The jamming detection feature identifies any intentional jamming from a third party.

The supervision feature consists of transmitting signals between every device of the system and the W alarm panel. Through the supervision, the detectors transmit every 8 minutes a presence signal.

The entire RSI VIDEO TECHNOLOGIES team wishes you a successful installation.
Introduction.........................................................................................................................2

Summary........................................................................................................................................3

1. W installation and setup........................................................................................................4  
   1.1 Panel overview..................................................................................................................4
   1.2 Panel mounting..................................................................................................................4
   1.3 Ethernet cable connexion..................................................................................................5
   1.4 SIM card installation.........................................................................................................5
   1.5 Powering and initialization...............................................................................................5
   1.6 Indicator lights..................................................................................................................6
   1.7 Pairing the keypad.............................................................................................................6

2. W panel programming............................................................................................................7  
   ETHERNET parameters configuration..................................................................................11

3. W panel features guide...........................................................................................................15  
   3.1 Get to access level 4........................................................................................................15
   3.2 How to arm/disarm the system.......................................................................................15
   3.3 Arming and siren mode configuration.............................................................................16
   3.4 Manage badges and access codes..................................................................................17
   3.5 Delete a device from the system...................................................................................19
   3.6 Read the event log.........................................................................................................20
   3.7 Golden rules..................................................................................................................20

4. Ethernet parameters...............................................................................................................21

5. Transmitter events list..........................................................................................................22

6. 2G3G error codes..................................................................................................................23

7. Security and certifications notes..........................................................................................24

8. Technical specifications...........................................................................................................26
1. W INSTALLATION AND SETUP

1.1 Panel overview

- SIM card installation
- Status LEDs
- Mini-USB connector for power supply
- Ethernet cable connection
- WIS100 Siren connector
- Battery connector
- COM button
- INIT button
- Locking screws

1.2 Panel mounting

Fix the back casing on the wall using the three mounting holes (4 mm diameter) as shown.

*Mounting the panel is not required for programming.*
1.3 Ethernet cable connection

*Only for models WIP 210/220/230, WIP 620/630 and WIP 720/730*

Once the panel is fixed on the wall connect a RJ45 cable between the site internet network and the panel Ethernet port. When the panel attempts a transmission via Ethernet, a red LED on the connector will flash. This will allow the installer to check whether the panel is connected to a valid network.

*Do not touch the RJ45 cable when the panel is powered.*

**IMPORTANT:**

*Only connect the panel on 10Base-T SELV networks.*

1.4 SIM Card Installation

Insert a Mini-SIM 2FF SIM card in the location shown in the image. Please refer to the markings for the insertion direction. Use a M2M (machine-to-machine) 2G/3G SIM card. If the panel is used with a smartphone application, the SIM card shall be able to receive SMS.

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

1.5 Alimentation et initialisation

**AC Power**

- Connect the backup battery.
- Install the power supply inside or outside the panel box depending on the needed cable length.
- Connect the power supply to the panel mini-USB connector
- Plug the power supply in an electrical outlet.
- Do not connect the 12V input (sealed by a label), specifically when the panel is powered.

**Initialization**

- **Leave the panel open.** The green status LED de statut verte is on. Press and hold the INIT button for 6-7 seconds until the status LED turns red for 1 second.
- The red LED blinks several times then turns off. That procedure resets the panel memory.
- The panel is now reset, a Videofied® keypad has to be enrolled to configure the panel.
1.6 Indicator lights

<table>
<thead>
<tr>
<th>Red LED on</th>
<th>Red LED blinking (1 sec)</th>
<th>Red LED blinking (3 sec)</th>
<th>Red LED off</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>Battery out of order or not detected.</td>
<td>Low voltage on the battery.</td>
<td>Normal operation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Green LED on (AC power detected)</th>
<th>Green LED off (AC power not detected)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>Low voltage on the battery</td>
</tr>
</tbody>
</table>

1.7 Pairing the remote keypad

- Press briefly the panel INIT button and release for the enrollment of a programming keypad.
- Insert 3 or 4 LS14500 Lithium batteries into the keypad.
- Do not mount the keypad. It will display one of the following screens:
  - `<--------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 does not pair up with the panel and shows “XX”, it certainly means that it is still paired to another system. The keypad needs to be reset. Remove the batteries and press repeatedly on the keypad tamper switch for 30 seconds to 1 minute. Then proceed to the above steps.
Use the keypad to program the panel

Keypad Display

**KEYPAD 1**
- **RECORDED**
  - **OK** or **YES**

**< - LANGUAGE : - >**
- **ENGLISH (UK)**
  - **OK** or **YES**
  - For language selection

**RADIO RANGE TEST?**
- **OK** or **YES**

**RF TEST**
- x/9
  - **Attendre**

- 9/9
  - **OK** or **YES**

**RADIO RANGE TEST?**
- **ESC**
  - **NO**

**INSTALLER CODE**
- 4 TO 6 DIGITS THEN OK/YES

**INSTALLER CODE:**
- **OK** or **YES**

**CONFIRM CODE**
- **OK** or **YES**

**Actions and comments**

The system can also be programmed in: french, italian, german, dutch, spanish, swedish, portuguese, danish, czech, turkish, 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 is important**, it 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.
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 installer 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.

Test Periodicity: 1 hour, 12 hours, 24 hours, 48 hours, 7 days or no tests.

**We suggest a 24 hours periodic test call.**
2. W PANEL PROGRAMMING

The CODE/STATE MODIF. menu is used 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 panel transmits in priority to IP1 (or DOMAIN NAME 1) / PORT 1 then to IP2 (or DOMAIN NAME 2) / PORT 2 as a backup.
2. W PANEL PROGRAMMING

How the alarms and videos are transmitted to the monitoring station:

- **2G3G**: SIM card transmission only
- **ETH**: Ethernet transmission only (not recommended***)
- **WLAN**: Wi-Fi** transmission only (not recommended***)
- **ETH+2G3G**: Ethernet* transmission with backup SIM card
- **2G3G+WLAN**: Wi-Fi** transmission with backup SIM card
- **ETH+WLAN**: Ethernet* transmission with backup Wi-Fi** (not recommended***)
- **ETH+2G3G+WLAN**: Ethernet* transmission with backup Wi-Fi** then backup SIM card

*Only for models WIP 210/220/230, WIP 620/630 and WIP 720/730

**Only available when the WWB100 module is installed.

***In case of internet loss or AC power loss, transmission failures can occur by using Wi-Fi and/or Ethernet without a 2G3G line backup.

### Strategy: ETH+2G3G

#### 2G3G PARAMETERS?

#### APN CODE

#### USER NAME

#### PASSWORD

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 6: 2G3G errors codes and contact your technical support).

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

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

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

Only for models WIP 210/220/230, WIP 620/630 and WIP 720/730

By setting the DHCP as ENABLED, a new IP address will be assigned dynamically to the panel every time it connects to the network.

Network parameters will not be asked.

If the router forces a static IP address for the panel, there will then be a need to define DHCP as DISABLED. You will then need to fill in the following network parameters fields:

- Panel IP
- IP Mask
- Primary DNS
- Gateway
- Secondary DNS

Warning: Verify that the IP address selected is available on the Network and accepted by the router.

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

- If the connection is successful: the local IP of the panel will be displayed (you can display other Ethernet parameters with the arrows).

- ETHERNET OFF NO STATUS: the Ethernet module is switched off. Please verify that the Ethernet cable is connected and try again.

- NETWORK/CABLE MISSING: the panel doesn’t detect Ethernet Cable or Network
2. W PANEL PROGRAMMING

For full compatibility with EN50131 norms, press **OK** or **YES**. Otherwise, press **ESC NO**.

Press **ESC NO** to default the area names.
Enter the name of Area 1 and confirm with **OK** or **YES**.
Repeat the procedure for areas 2, 3 and 4.
For further details, please refer to chapter 3.3.

Available delays are: 2 min, 1 min, 45 sec.

Available delays are: 15 seconds, 30 seconds, 45 seconds, 1 minute et 2 minutes.

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 RF test section on page 6 for further details.
2. W PANEL PROGRAMMING

Each device is recorded in an area.

Each area can be configured as delayed or immediate. Areas are used to set up special arming modes as well.

Please refer to the chapter 3.3 for further details about special arming modes.

By default (area set as Automatic), area 1 is delayed whereas areas 2, 3 and 4 are immediate. Recording a keypad or a badge reader in an area will automatically delay that area.

The name of the device shall contain every needed information to be properly processed in case of alarm.

During the functional device test, the device LED turns on when it detects an intrusion.

Press OK or YES to enter another device or ESC NO to move on to the next step.

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

Press OK or YES if you use one or more badges. ESC NO if you are not using any badges.

These badges will be used as a first user access (Level 3) and will be mandatory to access the engineer level (Level 4).

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 3.4 for further details).

Badges and codes are limited to 49 user accesses and 1 engineer code.
When the configuration is over, close the panel box as shown below and lock the panel. You can find screws to lock the panel inside the box (see chapter 1.1 on page 4). Then stick the provided tag to seal the panel.

**Box locking and sealing is mandatory to comply with NF&A2P and EN50131 standards.**

The keypad displays:

- **OPERATION COMPLETED?**
- **OK or YES**
- **SYSTEM CHECK IN PROGRESS**
- **INSTALLATION SUCCESSFUL!**

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 portal), to see full programming options.
3. W PANEL FEATURES GUIDE

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 (Level3): the user must authorize the installer to get access to the configuration of his panel.

3.2 How to Arm/Disarm the System

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

<table>
<thead>
<tr>
<th></th>
<th>Full arming with personal 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 enter your user code and press OK or YES</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</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**

- 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 / .
  - **SP1**: Partial Arming (1) is enabled by entering the user code and pressing on the keypad or on the keyfob.
  - **SP2**: Partial Arming (2) is enabled by pressing and entering the user code. On the keyfob, SP2 is enabled by pressing .

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.

<table>
<thead>
<tr>
<th>Areas: 1 2 3 4</th>
<th>Each time you press the corresponding number, the system will toggle the arming state for the respective area.</th>
</tr>
</thead>
<tbody>
<tr>
<td>State: A A A A</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

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

Reserved Codes

Up to 49 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.
3.5 Delete a device from the system

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 Golden rules

1. **Area 1** device are delayed by default (Area mode parameter set as Auto). When you register a keypad or a badge reader into an area set as Auto, that area will automatically be delayed.

2. **Never position** a panel next to a high voltage electrical cabinet. The interference will affect radio and 2G3G performance.

3. Press CLR to erase a typing mistake.

4. Never register the same device twice (delete from the system first).

5. The panel can register of **up to 25 devices** of all types, including the keypad and the keyfobs.

6. Follow the Motionviewer installation instructions. Consider the infrared field of detection when installing the Montionviewer cameras, in order to protect goods or an entry point instead of a zone.

7. Do not fix the keypad at the beginning of the installation as it will need to be portable during programming.

8. **Always clean** the lens of the cameras after the installation. Use a clean, dry cloth, taking care not to exert pressure on the lens.

9. Internal components are fragile, be careful opening or closing the panel.

10. LCD screen goes dark after 30 seconds of inactivity, press an arrow or numeric key to light it up.

11. Infrared detectors should never be installed in stairs or close to stairs (false alarm risks).

12. A colon display [:] means that the parameter can be changed. Press OK / YES to display the colon.
To configure Ethernet parameters, using the direction arrows, go to:

<table>
<thead>
<tr>
<th>Lvl. 4</th>
<th>OK or YES</th>
<th>GENERAL PARAMETERS</th>
<th>OK or YES</th>
<th>ETHERNET</th>
</tr>
</thead>
</table>

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 W panel can be configured to enable or disable the transmission of specific events like alarms or malfunctions.

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

**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.

---

**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/disabling)
- SWINGER SHUTDOWN

**There is 3 different transmission states:**

- **ALARM**: event transmitted upon occurrence
- **ALARM/END**: event is transmitted on occurrence and on event restoration
- **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.
6. 2G3G ERROR CODES

Security limitations on the SIM card must be disabled.
The PIN of the SIM card has to be disabled or 0000.

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

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

<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</td>
</tr>
<tr>
<td></td>
<td>-&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>No network coverage</td>
</tr>
<tr>
<td></td>
<td>Typographical error in the APN Code, username, password</td>
</tr>
<tr>
<td></td>
<td>SIM card not activated</td>
</tr>
</tbody>
</table>
7. SECURITY AND CERTIFICATION NOTES

Certifications

868MHz (WIP 210/220/230 and W 210)

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

NF&A2P - 2 boucliers – suivant le référentiel NF324-H58

<table>
<thead>
<tr>
<th>Marque commerciale</th>
<th>Référence Produits</th>
<th>N° de Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Videofied</td>
<td>Centrale WIP210</td>
<td></td>
</tr>
<tr>
<td>Videofied</td>
<td>Centrale WIP220</td>
<td></td>
</tr>
<tr>
<td>Videofied</td>
<td>Centrale WIP230</td>
<td></td>
</tr>
<tr>
<td>Videofied</td>
<td>Centrale W210</td>
<td></td>
</tr>
</tbody>
</table>

Standards:
- NF EN50131-1: 2007 - Grade 2 – Class II
- NF EN50131-3: 2009 - Grade 2
- NF EN50131-5-3: 2005 - Grade 2
- NF EN50131-6: 2008 Grade 2 – Type B
- NF C 48-212: 2004
- NF EN50130-5: 1998 Class II

Organisme certificateur:
- CNPP Cert.
  Route de La Chapelle Réanville CS22265
  F—27950 SAINT MARCEL
  Tel : +33(0)2.32.53.63.63
  Fax: +33(0)2.32.53.64.46
  Sites Internet : http://www.cnpp.com
  Email : certification@cnpp.com

- AFNOR Certification
  11, rue François de Pressensé
  93571 Saint Denis La Plaine Cedex
  Tel : +33(0)1.41.62.80.00
  Fax: +33(0)1.49.17.90.00
  Sites Internet : http://www.afnor.org
  et http://www.marque-nf.com
  Email : certification@afnor.org

915MHz (WIP 620 /630)

UL 1610
USA FCC (Part 15C, 22H, 24E and 27)
Canada IC (RSS-210 Issue 8, RSS-132, RSS-133 and RSS-139)

920MHz (WIP 720/730)

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

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

Security notes / (FR) Notes de sécurité / (DE) Hinweise zur Sicherheit

**English**

- Remove the battery before any maintenance!
- WARNING, there is a risk of explosion if a battery is replaced by an improper model!
- Observe polarity when setting up the battery!
- Do not throw the battery when it is used! Dispose of it properly according to Lithium Metal requirements

**Français**

- Retirez la batterie avant toute opération de maintenance!
- Attention ! Il y a un risque d’explosion si la batterie utilisée est remplacée par un mauvais modèle !
- Respectez la polarité lors de la mise en place de la batterie !
- Ne jetez pas la batterie usagée ! Ramenez-la à votre installateur ou à un point de collecte spécialisé.

**Deutsch**

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

---

**FCC Regulatory Information for USA and CANADA**

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

FCC Part 15.105 Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

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

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.
8. TECHNICAL SPECIFICATIONS

ELECTRICAL DATA

<table>
<thead>
<tr>
<th>Power supply</th>
<th>W210 / WIP 210 / WIP 220 / WIP 230</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5VDC/1A Mini-USB connector</td>
</tr>
<tr>
<td></td>
<td>AC/DC adapter (110/230VAC/50-60 Hz) available (WPS100)</td>
</tr>
<tr>
<td></td>
<td>WIP 620 / WIP 630 / WIP 720</td>
</tr>
<tr>
<td></td>
<td>12VDC/1A - Wire connection</td>
</tr>
</tbody>
</table>

Backup battery

<table>
<thead>
<tr>
<th>Battery technology</th>
<th>Rechargeable 3.7V Lithium-ion battery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Battery voltage (Fully charged)</td>
<td>4.1 V</td>
</tr>
<tr>
<td>Low battery level</td>
<td>3.95 V</td>
</tr>
<tr>
<td>Guaranteed autonomy when the low battery level is reached</td>
<td>36h</td>
</tr>
<tr>
<td>Average current consumption in standby mode</td>
<td>600 µA</td>
</tr>
<tr>
<td>Max consumption</td>
<td>1 A</td>
</tr>
</tbody>
</table>

RF S2View® technology

<table>
<thead>
<tr>
<th>Radio type</th>
<th>Bidirectional RF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating frequency</td>
<td>868MHz - WIP210/220/230 - W210 (Europe, South Africa, Asia)</td>
</tr>
<tr>
<td></td>
<td>915MHz - FHSS - WIP620/630 (USA, Canada, South America)</td>
</tr>
<tr>
<td></td>
<td>920MHz - FHSS - WIP720/730 (Australia, South America)</td>
</tr>
<tr>
<td>Transmission security</td>
<td>AES encryption algorithm</td>
</tr>
<tr>
<td>Radio jam detection</td>
<td>Yes</td>
</tr>
<tr>
<td>Supervision</td>
<td>Yes</td>
</tr>
<tr>
<td>Radio Antenna</td>
<td>Integrated</td>
</tr>
</tbody>
</table>

Tamper Detection

| Tamper               | Wall and cover tamper detection      |

BOX

<table>
<thead>
<tr>
<th>Physical and Environmental Data</th>
<th>Operating temperature -10°/+55°C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum relative humidity</td>
<td>75%, non-condensing</td>
</tr>
<tr>
<td>IP stack</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>Material</td>
<td>ABS—ULV0</td>
</tr>
</tbody>
</table>

Dimensions

| Panel                        | 143 mm x 200 mm x 44mm |

Installation / Mounting

<table>
<thead>
<tr>
<th>Control Panel / Base</th>
<th>Two screws secures control panel cover to base</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Three screws secure control panel base to the wall</td>
</tr>
</tbody>
</table>

ELECTRICAL DATA

<table>
<thead>
<tr>
<th>Power supply</th>
<th>W210 / WIP 210 / WIP 220 / WIP 230</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5VDC/1A Mini-USB connector</td>
</tr>
<tr>
<td></td>
<td>AC/DC adapter (110/230VAC/50-60 Hz) available (WPS100)</td>
</tr>
<tr>
<td></td>
<td>WIP 620 / WIP 630 / WIP 720</td>
</tr>
<tr>
<td></td>
<td>12VDC/1A - Wire connection</td>
</tr>
</tbody>
</table>

Backup battery

<table>
<thead>
<tr>
<th>Battery technology</th>
<th>Rechargeable 3.7V Lithium-ion battery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Battery voltage (Fully charged)</td>
<td>4.1 V</td>
</tr>
<tr>
<td>Low battery level</td>
<td>3.95 V</td>
</tr>
<tr>
<td>Guaranteed autonomy when the low battery level is reached</td>
<td>36h</td>
</tr>
<tr>
<td>Average current consumption in standby mode</td>
<td>600 µA</td>
</tr>
<tr>
<td>Max consumption</td>
<td>1 A</td>
</tr>
</tbody>
</table>

RF S2View® technology

<table>
<thead>
<tr>
<th>Radio type</th>
<th>Bidirectional RF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating frequency</td>
<td>868MHz - WIP210/220/230 - W210 (Europe, South Africa, Asia)</td>
</tr>
<tr>
<td></td>
<td>915MHz - FHSS - WIP620/630 (USA, Canada, South America)</td>
</tr>
<tr>
<td></td>
<td>920MHz - FHSS - WIP720/730 (Australia, South America)</td>
</tr>
<tr>
<td>Transmission security</td>
<td>AES encryption algorithm</td>
</tr>
<tr>
<td>Radio jam detection</td>
<td>Yes</td>
</tr>
<tr>
<td>Supervision</td>
<td>Yes</td>
</tr>
<tr>
<td>Radio Antenna</td>
<td>Integrated</td>
</tr>
</tbody>
</table>

Tamper Detection

| Tamper               | Wall and cover tamper detection      |

BOX

<table>
<thead>
<tr>
<th>Physical and Environmental Data</th>
<th>Operating temperature -10°/+55°C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum relative humidity</td>
<td>75%, non-condensing</td>
</tr>
<tr>
<td>IP stack</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>Material</td>
<td>ABS—ULV0</td>
</tr>
</tbody>
</table>

Dimensions

| Panel                        | 143 mm x 200 mm x 44mm |

Installation / Mounting

<table>
<thead>
<tr>
<th>Control Panel / Base</th>
<th>Two screws secures control panel cover to base</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Three screws secure control panel base to the wall</td>
</tr>
</tbody>
</table>

TRANSMISSION

Communicator

<table>
<thead>
<tr>
<th>Communicator type</th>
<th>2G &amp; LAN Ethernet (WIP210)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2G (W210)</td>
</tr>
<tr>
<td></td>
<td>LAN Ethernet (WIP220 / WIP 620 / WIP 720)</td>
</tr>
<tr>
<td></td>
<td>3G &amp; LAN Ethernet (WIP230 / WIP 630 / WIP 730)</td>
</tr>
<tr>
<td>Security protocol</td>
<td>Frontel</td>
</tr>
<tr>
<td>IP stack</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>Video transmission</td>
<td>By Frontel protocol to central monitoring station or App servers</td>
</tr>
</tbody>
</table>

Optional modules

<table>
<thead>
<tr>
<th>Wi-Fi</th>
<th>WW8100 (WLAN 802.11 b/g/n)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired Input/Outputs</td>
<td>WIO100 (out of NF&amp;A2P compliance)</td>
</tr>
<tr>
<td>Wired Siren</td>
<td>WIS100</td>
</tr>
</tbody>
</table>

Video

<table>
<thead>
<tr>
<th>Video Format</th>
<th>WMV or MPEG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Images per second</td>
<td>5</td>
</tr>
<tr>
<td>Image size</td>
<td>320x240 or 640x480 pixels</td>
</tr>
<tr>
<td>Video length</td>
<td>4 to 12 seconds</td>
</tr>
</tbody>
</table>

Miscellaneous

<table>
<thead>
<tr>
<th>Programming</th>
<th>Keypad</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max number of devices</td>
<td>24</td>
</tr>
<tr>
<td>Max number of codes/badges</td>
<td>50</td>
</tr>
<tr>
<td>Arming modes</td>
<td>4</td>
</tr>
<tr>
<td>Areas</td>
<td>4</td>
</tr>
<tr>
<td>Event log</td>
<td>4000 events stored on flash memory</td>
</tr>
</tbody>
</table>

EMEA SALES
23, avenue du Général Leclerc
92340 BOURG-LA-REINE
FRANCE
E-Mail : emeasales@rsvideotech.com

North American Headquarters
1375 Willow Lake Blvd, Suite 103
 Vadnais Heights, MN 55110
USA
E-Mail : usasales@rsvideotech.com

www.videofied.com