

# Wi-SOS 480

INSTRUCTION MANUAL V1.8



<b>1. INTRODUCTION.....</b>	<b>6</b>
1.1. About this document .....	6
1.2. Product overview .....	6
<b>2. QUICK START.....</b>	<b>6</b>
2.1. Equipment.....	6
2.2. Node installation.....	7
2.2.1. Initialising the Node .....	7
2.2.2. Sensor connection .....	9
2.2.3. Node mounting .....	9
2.3. Node configuration .....	10
2.4. Gateway installation .....	17
2.4.1. Gateway overview.....	17
2.4.2. Powering the Gateway .....	18
2.4.3. Mounting of the enclosure.....	20
2.4.4. SIM Card .....	23
2.4.5. Ethernet connection.....	24
2.5. Gateway configuration.....	24
2.5.1. Connecting to the Gateway.....	24
2.5.2. The Gateway's configuration interface .....	25
2.6. Data visualization and retrieval .....	36
2.7. Maintenance .....	42
2.7.1. General Maintenance.....	42
2.7.2. Periodical maintenance.....	42
2.7.3. Return material authorization.....	43
2.8. VW Node .....	44
2.8.1. Sensor connection .....	44
2.8.2. Barometric measurements.....	44
2.8.3. Battery lifespan .....	45
2.8.4. Configuration.....	45
2.8.5. Data storage .....	46
2.9. Digital Node .....	46
2.9.1. Sensor Connection .....	46
2.9.2. Battery lifespan .....	47
2.9.3. Configuration.....	48
2.9.4. Data storage .....	48
2.10. Volt Node .....	48
2.10.1. Sensor Connection .....	48
2.10.2. Battery lifespan .....	49
2.10.3. Configuration.....	51
2.10.4. Data storage .....	51
<b>3. WIRELESS RADIO .....</b>	<b>51</b>

3.1.	Maximum number of nodes connected in a network .....	51
3.2.	Radio configuration.....	52
3.3.	Results of signal coverage test.....	55
4.	CONTACT GEOSENSE.....	56
Annex 1: Details of mounting systems .....		57
	Mounting brackets .....	57
	Strong magnets .....	58
	Pole mounting.....	59
Annex 2: Android compatibility.....		62
Annex 3: Wi-SOS 480 water tightness .....		63
Annex 4: Recommended batteries .....		64
Annex 5: Communications security .....		65
	Long range radio communication from Nodes to the Gateway.....	65
	Security.....	65
	Encryption.....	65
	Gateway user access .....	65
	Remote access .....	66
	Local administration .....	66
Annex 6: Connecting an external modem to Wi-SOS 480.....		67
	Initial configuration of AirLink RV50 (via Ethernet cable).....	67
	Final Step: Connecting the LS-G6 Gateway to AirLink RV50.....	70
Annex 7: Connecting a Wi-Fi module to LS-G6 .....		71
	• Interconnection between Wireless Bridge and the WI-SOS 480 Gateway .....	71
Annex 8: Troubleshooting reference table .....		74
	Gateway .....	74
	Nodes .....	74
Annex 9: FAQ's.....		75
Annex 10: Modbus memory maps.....		77
	General Section .....	77

## FIGURES

Figure 1: View of the recommended positions to open the node. ....	7
Figure 2: Removal of the upper enclosure of the battery holder.....	8
Figure 3: Detail of power switch (SW A).....	9
Figure 4: Detail of the grounding screw. ....	10
Figure 5: a) Main screen of Android Configuration App and b) Node configuration screen, which has to be accessed for the configuration of the datalogger. ....	10
Figure 6: Network size configuration. ....	11
Figure 7: Sensor configuration options for the Vibrating Wire 5 ch node.....	11
Figure 8: Sensor configuration options of the Digital 2 ch node. ....	12
Figure 9: Sensor configuration options of the Volt 4ch node.....	13
Figure 10: Data readings of active sensors. ....	13
Figure 11: Radio configuration screen.....	14
Figure 12: Radio signal coverage performed at the end of the datalogger setup (using the Setup wizard). ....	16
Figure 13: Gateway, with all the parts indicated.....	17
Figure 14: Gateway opened. ....	18
Figure 15: Detail of the connections for the Power through PoE. ....	19
Figure 16: a) Section of shielded Ethernet cable; b) Detail of the connection for the Power through PoE using a shielded Ethernet cable.....	19
Figure 17: Wiring of the cable at the RJ45 connector (following T-568A/B specification) to be inserted in the PoE Injector. ....	19
Figure 18: DC terminal block. ....	20
Figure 19: Gateway mounted on a pole. ....	20
Figure 20: Gateway mounted on the wall. ....	21
Figure 21: Gateway mounted on a pole. ....	21
Figure 22: Gateway's antenna mounting. ....	22
Figure 23: Connection of the antenna cable to the connector. ....	22
Figure 24: Fixing of the antenna cable. ....	23
Figure 25: SIM card slot. Extraction button indicated. ....	23
Figure 26: PoE. Left port (Data & Power Out) is for the power cable and right port (Data In) is for data transmission. ....	24
Figure 27: Initial page of the gateway. This is the first page when entering the Web's Configuration Interface. ....	26
Figure 28: Summary of the datalogger status and the history of received / lost messages. ....	27
Figure 29: Gateway status page. ....	29
Figure 30: View of the tool to create a self-configured csv file of the network data. ....	30
Figure 31: View of the Internet configuration tab of the gateway. The present configuration is the one by default. ....	31
Figure 32: Options for manual configuration. ....	32
Figure 33: Settings for the configuration of the GPRS/3G connection.....	33

Figure 34: Remote Access tab, inside the gateway interface. ....	34
Figure 35: Radio configuration tab, inside the gateway interface. ....	35
Figure 36: Delete all tab, inside the gateway interface. ....	36
Figure 37: Reboot tab, inside the gateway interface. ....	36
Figure 38: In the “Last readings” tab, a gear icon appears on the right, for editing the formula of the sensor. ....	37
Figure 39: Menu to edit the formulae for transforming the raw data of the sensors into engineering units. ....	38
Figure 40: Circled in red, the icon to display the charts of each of the sensors. ....	39
Figure 41: Example of a chart of one datalogger. ....	39
Figure 42: View of the screen where the .csv files of raw data and data transformed into engineering units (of the complete network) can be downloaded. ....	39
Figure 43: View of the screen where the data of a specific datalogger can be downloaded. ....	40
Figure 44: View of the screen where the FTP can be configured. ....	41
Figure 45: View of last messages received by the gateway, displayed in API format. ....	41
Figure 46: Detail of a terminal block. ....	44
Figure 47: View of the inside of the digital datalogger connected to a RST inclinometer and b) Sisgeo inclinometer. ....	47
Figure 48: View of the Volt node internally where the four channels can be identified. ....	48
Figure 49: View of the wiring of the different types of analogue sensors, indicated in the Android Configuration App. ....	49
Figure 50: Summarized scheme of data transmission over time in a Wi-SOS 480 network. ....	<b>Error!</b>
<b>Bookmark not defined.</b>	
Figure 51: View of the geographical display (in the software of the gateway) indicating the results of the signal coverage tests. ....	55

## TABLES

Table 1: Connections of the terminal block. ....	44
Table 2: Indicative lifespan for VW Node 1 ch (using 1 C-size cell) and VW Node 5 ch. (using 4 C-size cells) ....	45
Table 3: Times of data storage (without overwriting) for VW Node 1 ch and VW Node 5 ch. ....	46
Table 4: Indicative lifespan for Digital Node. Estimations using 4 c-size cells ....	47
Table 5: Indicative lifespan for Digital Node. Estimations using 4 c-size cells ....	47
Table 6: Indicative storage capacity of the Digital Node. Estimations using 5 sensors. ....	48
Table 7: Indicative lifespan for Volt Node. Estimations using 4 c-size cells, considering SF9 ....	50
Table 8: Indicative storage capacity of the Volt Node. Estimations using 4 sensors. ....	51
Table 9: Slot times table. Columns are the number of nodes; rows are sampling rate. Slot times are in seconds. ....	52
Table 10: Summary of radio specifications by mode. ....	54

## 1. INTRODUCTION

### 1.1. About this document

This instruction manual explains the basic procedure for data acquisition with the Wi-SOS 480 family of nodes as follows:-

- VW-1-EI
- VW-1-FCC
- VW-5-EU
- DIG-2-EU
- VOLT-4-EU

### 1.2. Product overview

**Geosense Wi-SOS 480 Nodes** are low power, easy to use and field-friendly, and are used for data acquisition from a great range of sensors in the market. Moreover, radio models can be used for long range communications, up to 15 km in open-field scenarios, and 4 km in urban scenarios.

The nodes are battery powered, and easily configured through the Android Configuration G-LOG App. The nodes and the gateway are robust with enclosures rated to IP68 and IP67 respectively.

They can be used in a wide range of professional sectors, such as civil engineering, mining, environmental or industrial monitoring, among others.

## 2. QUICK START

### 2.1. Equipment

**Geosense Wi-SOS 480** system is shipped with the following:

Included:

- **RTC ½ AA-size bobbin cell battery:** Required to keep the time. If no RTC battery installed, the node does not keep time.
- Antenna (only for radio models)

Not included:

- Micro USB OTG to USB 2.0
- External mounting brackets (set of 2) for wall mounting (see Annex 1 for details)
- Plate for pole mounting (see Annex 1 for details)
- Strong magnets for mounting in metallic structures (see Annex 1 for details)
- C-size spiral cell batteries (see Annex 4 for details): 1 to 4 batteries can be connected.

- Gateway (included)

Included:

- Antenna
- Cable antenna
- PoE
- USB Local Administration Interface

Not included:

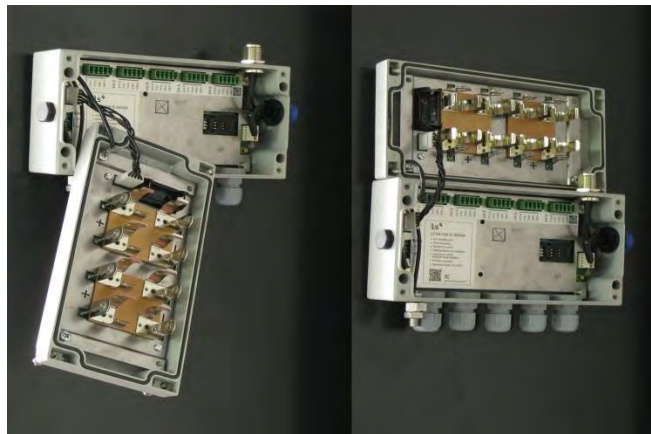
- Dataline surge protector
- Antenna surge protector

## 2.2. Node installation

### 2.2.1. Initialising the Node

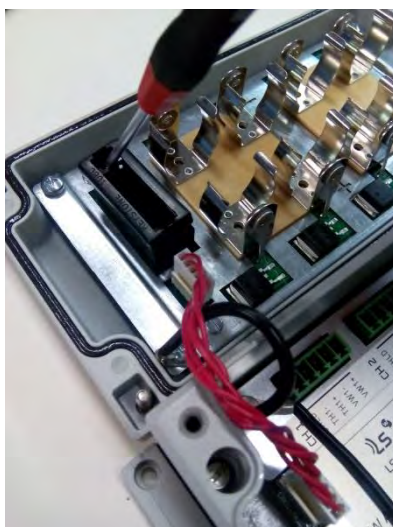
The node is shipped closed and without batteries installed. In order to initialise it, the following steps should be followed:

- Open the node (using a 2.5 mm Allen key) following the recommended positions (Figure 1) in order to avoid damaging the lateral gore valve. The batteries are inserted onto the cover, so be careful not to snap the cable between the cover and the main board.



*Figure 1: View of the recommended positions to open the node.*

- Insert the RTC battery (small battery included). First remove the upper enclosure of the battery holder (Figure 2). Polarity is indicated inside the holder.



*Figure 2: Removal of the upper enclosure of the battery holder.*

- c. Insert C-type batteries in the battery holders. 1 to 4 batteries can be connected. Polarity is indicated (see Annex 4 for further information on the batteries).

*Note that there is reverse battery protection, but it is not safe to keep batteries reversed in the datalogger for a long time.*

**WARNING: RISK OF EXPLOSION IF THE BATTERIES ARE SUBSTITUTED WITH AN INCORRECT MODEL. DISPOSE OF BATTERIES IN ACCORDANCE WITH LOCAL ENVIRONMENTAL REGULATIONS. THIS EQUIPMENT IS MEANT TO BE INSTALLED IN RESTRICTED ACCESS AREAS.**

- d. Check that power switch (SW A, Figure 3) is in the correct position. USB: the datalogger is powered by the USB cable connected to any other Android device / BATT (default): the node is powered by the batteries.

*Note that some Android devices are not capable of powering the node, especially when performing a reading. If reading fails, set the switch to BATT mode to power the node with batteries.*





*Figure 3: Detail of power switch (SW A).*

### 2.2.2. Sensor connection

Sensors are connected to the node at the node terminal blocks. Each terminal block corresponds to one channel of the node. The terminal blocks accept wires that are prepared by stripping a short length of insulation from the end.

Each node type has specific instructions for sensor wiring. The specifications for each model can be found in sections: 3.1. (vibrating wire nodes), 3.2. (digital nodes) and 3.3. (voltage nodes).

### 2.2.3. Node mounting

Nodes can be mounted (see Annex 1 for specific details):

- On the wall: mounting brackets can be supplied as additional accessories
- On a metallic structure: strong magnets can be supplied as additional accessories
- On a pole: plates for 35 and 50 mm pole diameters can be supplied as additional accessories for this mounting type
- Inside a manhole (with plastic or metallic cover): no special accessories are available for this mounting type. Even though the nodes are IP68 certified, we recommend installing them in holes with proper drainage so that they won't be permanently covered in water.

All **Geosense Wi-SOS 480** nodes are protected against lightning, and there is an easy to use grounding screw (Figure 4), next to the cable glands, which may be connected to guarantee protection.



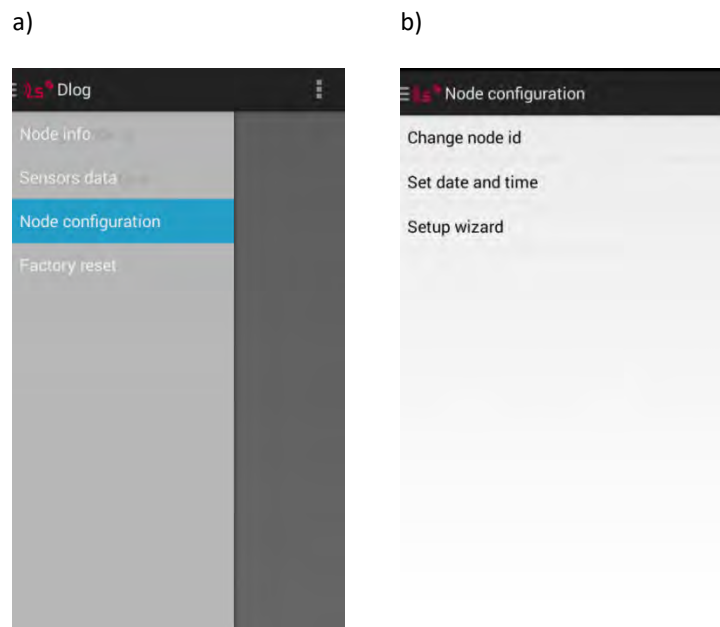
*Figure 4: Detail of the grounding screw.*

*Note that to protect the datalogger from surges (especially on installations with long cable runs) the datalogger must be properly grounded via connection to the grounding terminal.*

### 2.3. Node configuration

Different configuration parameters are required for each type of node (Vibrating Wire, Digital, Voltage). Complete configuration of the node is done through the Android Configuration App (see Annex 2 for Android compatibility). When a new version of the app is available, a message appears automatically when connecting the datalogger by USB.

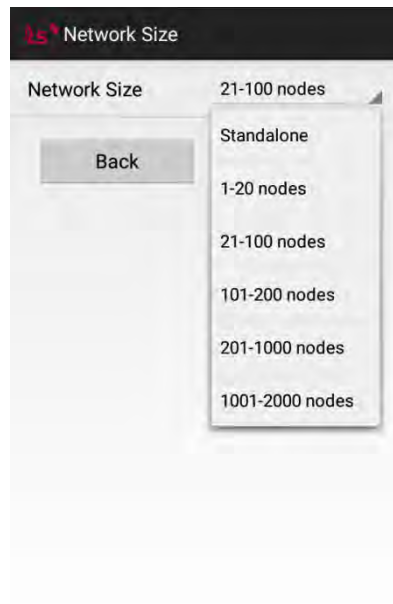
The configuration of the sensors and the radio is accessed by clicking the Setup wizard (in the tab menu “Node configuration”, Figure 5). Inside the Node configuration menu, there are also other parameters that can be changed by the user, such as the Node ID or the date and time (especially important when accessing the Node for the first time, or after installing the RTC battery).



*Figure 5: a) Main screen of Android Configuration App and b) Node configuration screen, which can be accessed for the configuration of the node.*

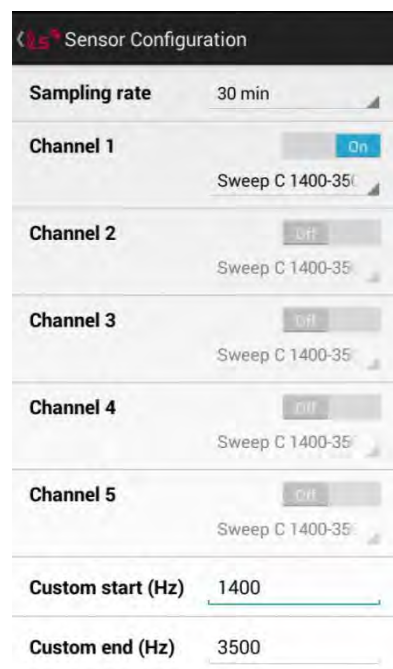
By selecting the Setup wizard, the step-by-step configuration of the sensors and the radio is completed:

- 1) **Network size.** The size of the network (Figure 6) defines the slot time for each of the nodes to send data to the gateway, in order to avoid data collision (see section 4.1. of this user guide).



*Figure 6: Network size configuration.*

- 2) **Sensor configuration.** Each type of datalogger has its own parameters for configuration:
- **VW Node** (Figure 7): activation of channels, sampling rate interval and VW sweep frequency for each sensor. For more information on the configuration, see Section 3.1.



*Figure 7: Sensor configuration options for VW Node-5ch.*

- **Digital Node** (Figure 8): sampling rate, communication protocol with sensors (see dropdown options) and bus addresses of the sensors (if connected through RS485 by digital bus). Be aware that all the readings are kept in accordance with the bus addresses introduced.

Therefore, the number of columns of data will equal the records indicated by the inserted addresses, and not necessarily be the same as the real number of sensors connected. If you lose track of the different addresses over time, we strongly recommend a factory reset. The last configuration is saved in the datalogger.

*Figure 8: Sensor configuration options of Digital Node-2 ch.*

- **Volt Node** (Figure 9): this node supports six different analogic sensor types: voltage, full Wheatstone bridge, thermistor, current loop, PT100, potentiometer. The interface for the sensor configuration in the Setup wizard requires the user to choose between the different sensor types in each channel (Figure 9a). For each specific sensor type, the details of the sensor wiring appear on the screen, and the configuration parameters (specific for each sensor type) must be selected by the user (Figure 9b). Each channel can be configured independently, with specific requirements for each sensor (sensor power, warm up times, etc.).

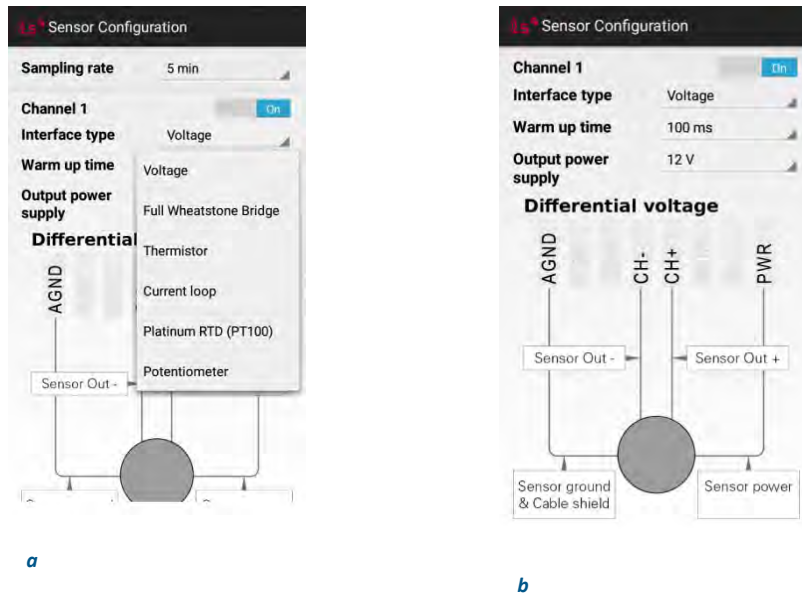


Figure 9: Sensor configuration options of Voltage Node-4ch

- 3) **Sensor data.** A reading of the active channels is displayed (Figure 10). In this stage, the user can see the readings of the sensors in this specific moment, to check if the sensors have been properly configured.

*Note that this action may take some time, depending on the sensor, and particularly so when there are strings of digital sensors connected to the RS485 port of digital node.*

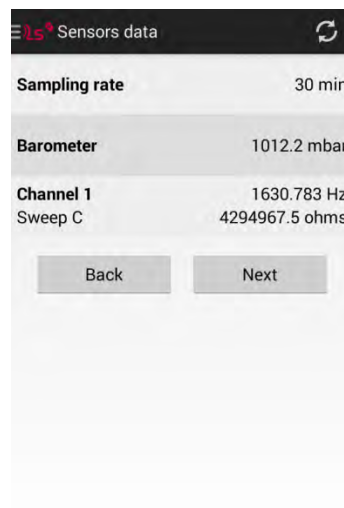
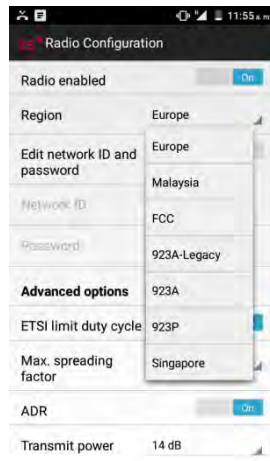


Figure 10: Data readings of active sensors.

- 4) **Radio configuration.** The details of the default network, specified in the Gateway Information sheet, must be used for the basic configuration of the radio (Figure 10).

The choice of the region is necessary to comply with the regulations of the country where the installation is done.

For advanced options, check Section 4 of this manual.



*Figure 11: Radio configuration screen.*

*Note that to simplify the node configuration tasks, especially in large installations, the network ID and password of the last node configured are saved into the Android app. The option of editing them must be activated by the user, otherwise the credentials introduced in the configuration of the node will be the ones that were introduced the last time the Android app was used.*

**5) Radio signal coverage test** - Once the gateway is configured, a signal coverage test can be performed (Figure 12).

This test will check for correct connectivity between the Node and the Gateway. Some test packets will be sent by the Node, and then the Android app will check on the gateway (using an Internet connection) for the reception of these packets. Hence, the test will check for:

- Correct gateway operation and communication
- Correct radio configuration on both Gateway and Node (including matching region and ID / password configurations)
- Quality of the signal received by the Gateway from the Node

For the results of this test to be immediately displayed in the Android device, the gateway needs to be installed with a working Internet connection, and the Android device also needs to be connected to the Internet.

In order to perform this test, the Dlog app needs to be supplied with the gateway's serial number and remote access password, specified on the Gateway Information Sheet.

The displayed results are listed for each Spreading Factor (SF). The SF represents a way of modulating data. The gateway is capable of receiving all frequencies with several SF's at the same time. The lower the SF number is, the shorter the message, thus more messages can be sent on the network. The SF is proportional to the distance between the Node and the Gateway: higher spreading factors are capable of transmitting data at higher distances, while lower spreading factors reach lower distances.

During the radio signal coverage test, the datalogger sends 5 or 10 packages of data at SF7 to SF12. The number of data packages that reach the Gateway can be viewed in the results in order to ensure correct communication. For more information see section 4 of this manual.

When doing the Radio signal coverage test, the position of the Android device is kept (if the user gave permission to the app to access to the GPS data), and a security token number identifies each test.

If the gateway and/or the Android device don't have Internet connectivity during the test, you will need to perform an "Offline test". In this mode, the results of the test cannot be displayed in the Android device. The security token number identifies each test and the resultd can be viewed in the software of the gateway. For further details see section 4.3.

*Note that performing the Radio signal coverage test takes approximately 2 minutes.*

a)

**Radio signal coverage**

Gateway ID

Server password

Offline test - Perform the coverage test, but don't fetch results from the gateway. The results can be checked later at the gateway interface.

Back Next

Offline test Skip

b)

**Radio signal coverage**

Date

Token

Node ID

Network ID

Latitude

Longitude

SF7	1 / 10
SF8	3 / 10
SF9	2 / 10
SF10	1 / 5
SF11	1 / 5

*Figure 12: Radio signal coverage performed at the end of the node setup (using the Setup wizard).*



## 2.4. Gateway installation

### 2.4.1. Gateway overview

Nodes transmit their readings to the gateway, and make them available for real-time access. Readings can be accessed over the Internet, via a private network, or stored on the gateway for local retrieval.

The **Wi-SOS 480 Gateway** (Figure 13) is made of a high-impact resistant polycarbonate, engineered to withstand harsh industrial and outdoor environments. It offers an excellent flammability rating, good UV and chemical resistance, and is rated IP67.

We advise that the Gateway should be setup and configured in an office environment, rather than going through the startup procedure in an outdoor or industrial environment.



*Figure 13: Wi-SOS 480 Gateway, with all the parts indicated.*

The gateway is composed of:

1. The enclosure
2. Cable gland for RJ45 PoE, or DC Power cable
3. N connector, for the sensor network radio antenna
4. Pressure stabilizer for protection against condensation
5. Sensor network radio antenna, with N connector
6. The mounting kit
7. A PoE injector, and its power supply cable

The Gateway enclosure can be opened (Figure 14) by putting a flat-head screwdriver in the small holes on either side of the door. You will need to open the Gateway to perform the initial installation and configuration procedure.



*Figure 14: LS-G6 Gateway opened.*

*Note that PoE power supply should be installed inside a box or indoors, since it is not waterproof.*

#### 2.4.2. Powering the Gateway

The Gateway can be powered by either PoE (Power over Ethernet), or via DC in. Only one power source is necessary. The nominal power consumption is about 3.2W (270 mA at 12V).

- Power through PoE
  - The PoE in the Gateway is IEEE 802.11af compliant. It is supplied with a compatible PoE power supply.
  - On the gateway side, the Ethernet cable (not included) must first be inserted into the case through the cable gland. Then, the cables must be unshielded and stripped, and connected into the terminal blocks in the correct order, as described on the Figure 15.

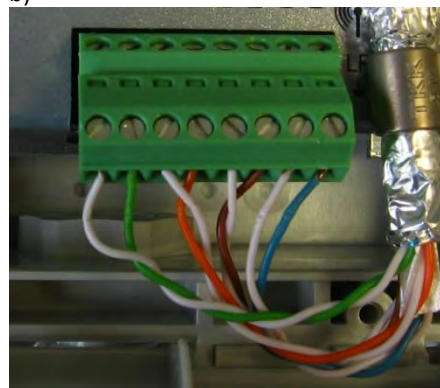


**Figure 15: Detail of the connections for the Power through PoE.**

a)

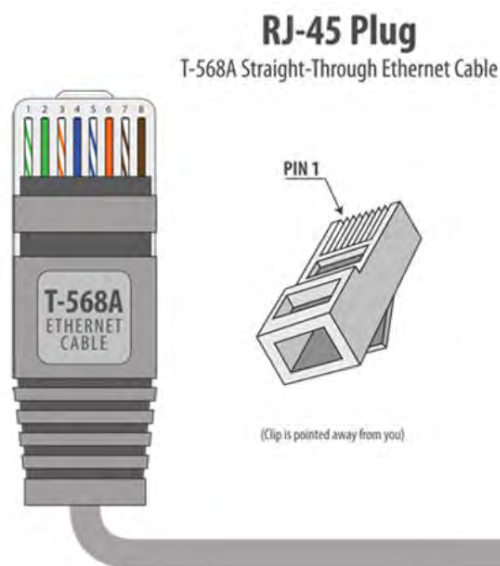
TX+ white/green
TX- green
RX+ white/orange
RX- orange
D+ white/brown
D- brown
C+ white/blue
C- blue

b)



**Figure 16: Details of the connection for the Power through PoE using a shielded Ethernet cable.**

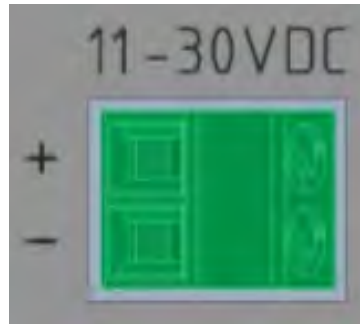
- The cable gland allows external cable diameter from 4 mm to 8 mm.
- On the other side of the PoE cable, the RJ45 connector must be inserted into the PoE injector. The PoE injector must be connected to 230VAC.
- The RJ45 cable must be wired in accordance with T-568A/B specification (Figure 16).



**Figure 16: Wiring of the cable at the RJ45 connector (following T-568A/B specification) to be inserted in the PoE Injector.**

- The Gateway can also be powered with a DC power supply, such as a solar panel. The input voltage range is 11 to 30 VDC.
- On the Gateway side, the cable must first be inserted through the cable gland. The DC in is the terminal block shown as in Figure 17.

*Note that if the Gateway is powered using a generator or another source that may induce surges or spikes, a voltage stabilizer may be installed in the power input of the Gateway.*



*Figure 17: DC terminal block.*

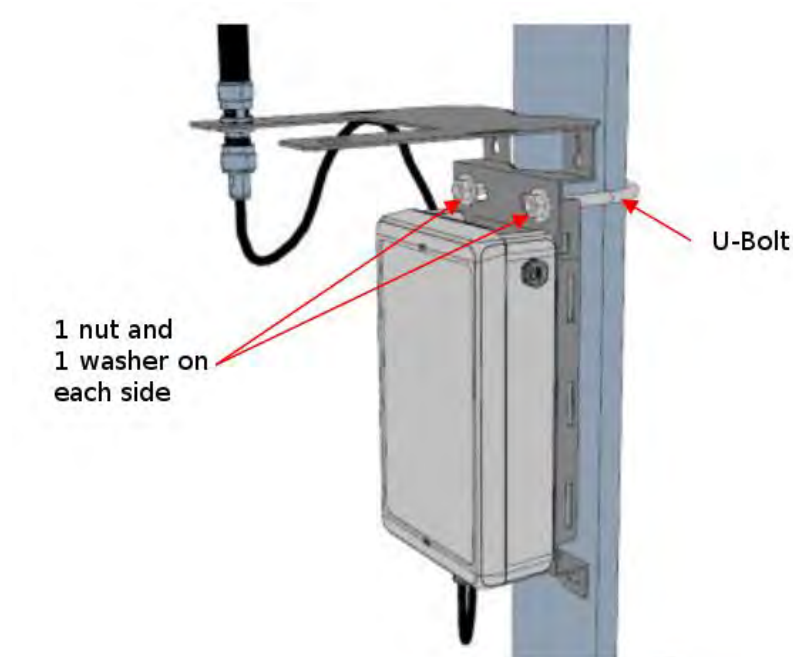
- The cable gland allows for an external cable diameter from 4 mm to 8 mm.

*Note that when powering out the Gateway, the shutting down process takes some time. Therefore, even if the power is disconnected, the gateway may still be active.*

### 2.4.3. Mounting of the enclosure

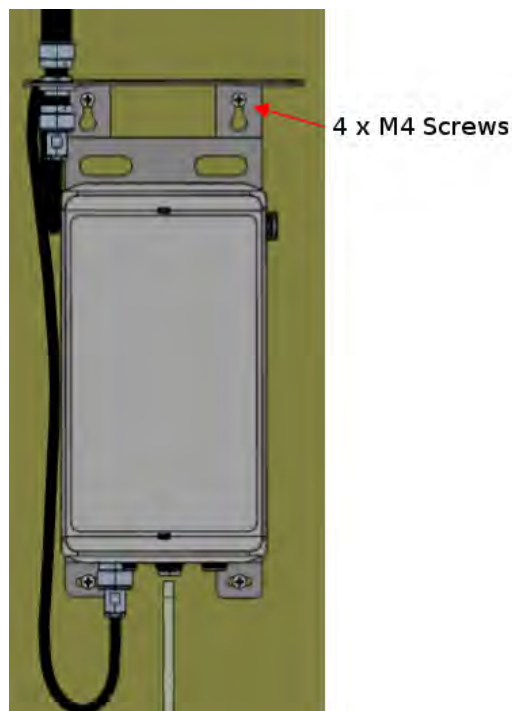
The Gateway enclosure comes with a mounting kit, which is designed for various configurations:

- Pole mounting by U-bolt (Figure 18)



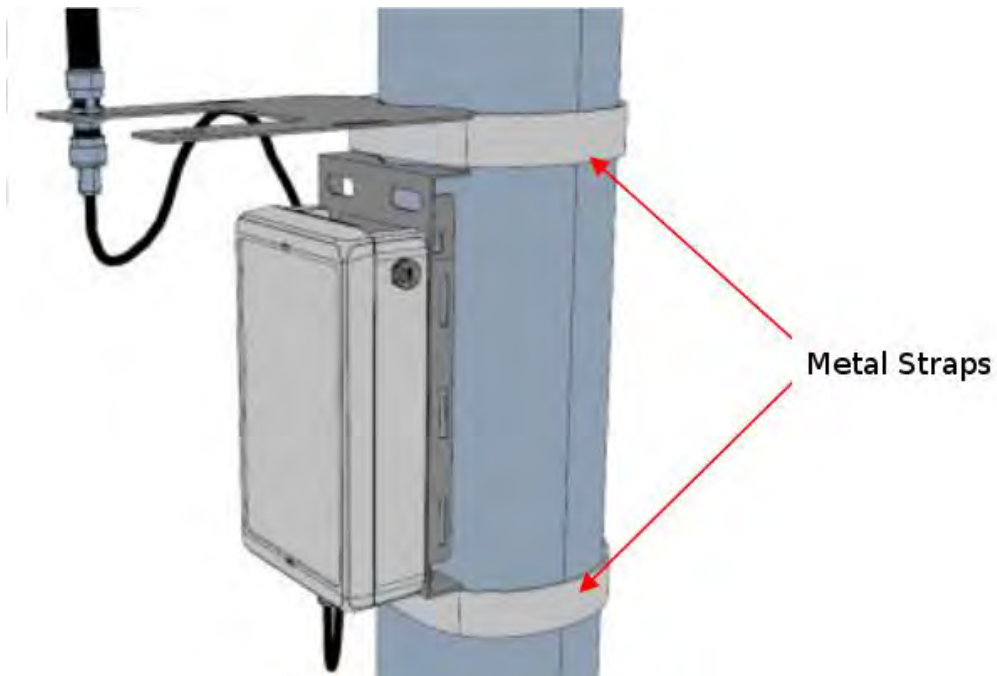
*Figure 18: Gateway mounted on a pole.*

- Wall mounting (Figure 19)



*Figure 19: Gateway mounted on the wall.*

- Metallic strapping mounting (tube, pipe, flue.) (Figure 20)



*Figure 20: Gateway mounted on a pole.*

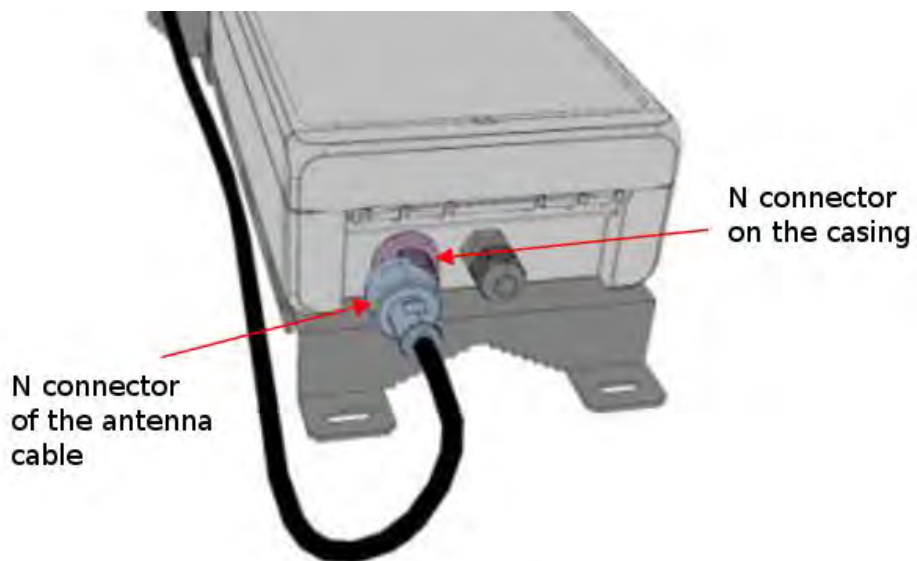
The metallic mounting kit must be grounded for safety reasons.

The antenna must also be mounted in its place on the mounting kit (Figure 21).



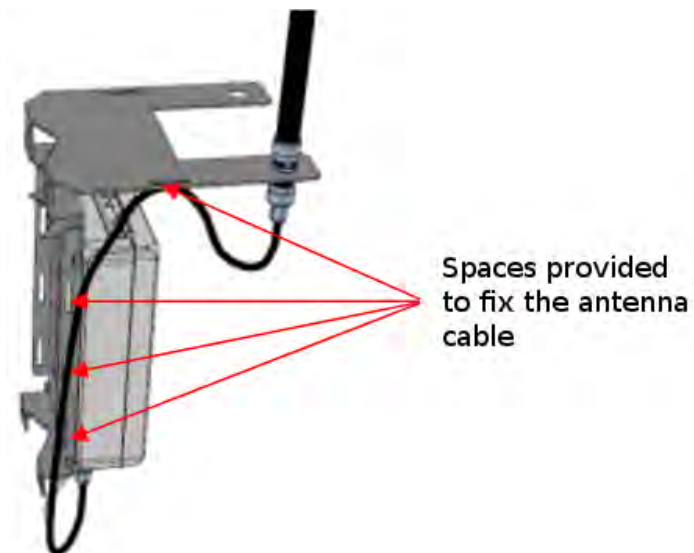
*Figure 21: Gateway's antenna mounting.*

The supplied antenna cable must be connected to the gateway enclosure, as shown on Figure 22:



*Figure 22: Connection of the antenna cable to the connector.*

Finally, the antenna cable must be strapped to the mounting kit to reduce accidental wear (Figure 23).



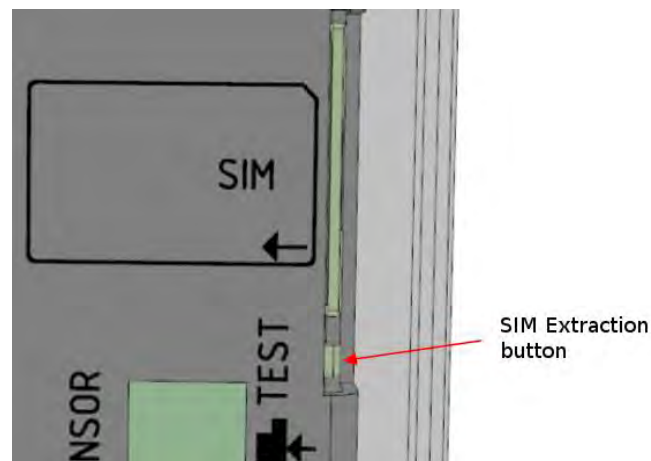
*Figure 23: Fixing of the antenna cable.*

#### 2.4.4. SIM Card

If the Gateway is meant to use a GPRS/3G connection, you will need to insert the SIM card in its place (Figure 24).

To insert a SIM card:

- Open the Gateway enclosure, using a flat-head screwdriver
- Push the SIM extraction button, using a small screwdriver, or the point of a pen
- Put the SIM in the tray, with the contacts facing out
- Put the tray back into the Gateway



*Figure 24: SIM card slot*

### 2.4.5. Ethernet connection

If the Gateway is meant to be connected to the Internet by Ethernet cable, this will be through the PoE injector (Figure 25).

*Note that Ethernet cable should be connected before plugging in the PoE injector to 230VAC. Once the gateway is initialized, Ethernet connection should be established to avoid problems with the default Internet access configuration (see section 2.5.2.2.).*



*Figure 25: PoE. Left port (Data & Power Out) is for the power cable and right port (Data In) is for data transmission.*

## 2.5. Gateway configuration

Configuration is done with a desktop or laptop computer. The Gateway provides a web interface for all configuration and data retrieval tasks. The interface is accessible through **any** of the Gateway's network connections, which will be explained in this section.

### 2.5.1. Connecting to the Gateway

#### 2.5.1.1. Local administration interface

To connect to the Gateway onsite, without depending on any external network, you may use the Local administration interface. This interface provides all features of the web administration, including the network configuration and access to the **Wi-SOS 480 WebCentre**.

To use the local administration interface, you must:

- Open the Gateway box, using a flat-head screwdriver
- Connect the supplied USB Ethernet adapter to the USB port on the front plate of the Gateway
- Connect an Ethernet cable between the Gateway's USB adapter and your laptop computer.
- Your computer must be configured to acquire an IP address automatically using DHCP
- Open the following website on your Internet Browser:
  - <http://169.254.0.1>
  - user: admin
  - password: VMjG6z
  - An SSL certification error will appear. This is normal, as this Gateway uses a self-signed certificate for SSL authentication. Add a security exception for this certificate so the connection is allowed. Check your browser's documentation for instructions on how to do this.



The Local administration interface should be used for:

- Initial configuration of a new Gateway
- Onsite data retrieval and Gateway configuration of a gateway without an internet connection
- In case the remote access password is forgotten. The local administration interface has a fixed password, which cannot be changed

#### 2.5.1.2. Remote Access connection

If the Gateway has a SIM card or it is connected to a router through Ethernet, the remote access to the Gateway is habilitated.

### 2.5.2. The Gateway's configuration interface

To access the Gateway's web configuration interface, you need a working network connection to the Gateway. There are 3 access methods to the interface:

- Using the Local administration interface
  - Explained earlier in this chapter, the local administration interface is meant to be used for initial configuration of the other interfaces, and onsite access to the gateway
  - The credentials for local access are fixed and cannot be changed
- Using the public network interface
  - If the Gateway has a working network interface (Ethernet or 3G) and its public IP is known, it's possible to access the web interface through it.
  - The password for this type of access is the remote web access password.
    - The default remote web access password is printed on your Gateway Information Sheet
    - The password can be changed in the web configuration interface
- Using the Wi-SOS 480 Remote Access Service
  - If the Gateway has a working Internet connection (through Ethernet or 3G), it's possible to use the Wi-SOS 480 Remote Access Service.
  - This service allows secure remote access to a gateway using an easy address, even if the network is inside a private network or is connected through a 3G connection.
  - The remote access address for any given gateway is <http://Wi-SOS480.wocs3.com/XXXX>, where XXXX corresponds to the Gateway's serial number.
  - The password for this type of access is the remote web access password.
    - The default remote web access password is printed on your Gateway Information Sheet
    - The password can be changed in the web configuration interface

#### 2.5.2.1. Networks

The first page shown when entering the Gateway's Web Configuration Interface shows the network ID and three different menus: networks, status and configuration. In case that the network ID has been changed for a specific Gateway (the same serial number), several networks will appear in this tab, under different IDs. A personalized name may be given to the network under the feature "Name". Finally, the number of Nodes, both active and inactive are shown, and displayed in green or red according their status (active / inactive).

When entering the network, several features of the Nodes are visible: status, model, serial number. Serial and Node ID coincide by default but ID may be changed (Figure 26). Through this page it is possible to:

- Download the compacted .dat / .csv files of the data collected by the network (raw data or engineering units (see section 2.6 for further information)).
- View the signal coverage test map, where test results are geographically plotted.
- See datalogger basic information: status, ID, serial number, model
- Access all the menus of the gateway configuration interface.
- Visualize data sent from the Nodes. Also, the messages lost and received by the Gateway are counted (under status tab). The green number indicates the messages received, the red number corresponds to the lost radio messages and the orange number to messages lost due to Gateway power interruption (Figure 27).
- Remotely change the sampling rate of the dataloggers\*

*\*This feature requires minimum Gateway software version 1.7. and minimum Node firmware version 2.15. Please contact Geosense for further information on firmware and software versions.*

**Network: 13170**

/ Networks / 13170

**Comments**

**Compacted readings CSV files** [compacted-readings-13170-current.dat](#) [More](#)

**Compacted engineering units CSV files** [compacted-eng-13170-current.dat](#) [More](#)

**Compacted custom CSV files**

[Signal coverage test map](#)

**Nodes**

☐ All 0 nodes selected of 26

Id	Name	Status	Model	Serial
1344		Disconnected	LS-G6-VW-5-EU	1344
1707		Disconnected	LS-G6-VOLT-4-EU	1707
1708		Disconnected	LS-G6-VOLT-4-EU	1708
1725		Disconnected	LS-G6-VOLT-4-EU	1725
1747	I PI Nova house test	OK	LS-G6-DIG-2-EU	1747

**Figure 26: Initial page of the gateway. This is the first page when entering the Web's Configuration Interface.**

Status	Ok
Last status change date	2016-01-13 01:55:13 AEDT
Monitoring status emails	✓ Yes
Messages received: today	368 1
Messages received: 1 day ago	107 5 2
Messages received: 2 days ago	74 1
Messages received: 3 days ago	0 0
Messages received: 4 days ago	0 0
Messages received: 5 days ago	0 0
Total number of messages since gateway installation	549 7 2

Note: all messages not received are stored in the node, and can be retrieved with the dlog app

*Figure 27: Summary of the datalogger status and the history of received / lost messages.*

#### Remote change of sampling rate

- The sampling rate can be remotely changed for one or several dataloggers.
- When the check box in the left of the corresponding line is selected and “Change sampling rate” applied, the new sampling rate option can be selected from a pop up menu.
- Once done and changes saved, a clock icon with the value of the new sampling rate next to it will appear on the ID column of the node.
- When it appears with an orange label, this means that the change has still not been applied.
- If the orange label disappears, this means that the change is effective.
- While the orange label is active, the changes can be cancelled.
- If the user tries to introduce a sampling rate not suitable according to the slot times required for the network, a message will appear where the user will have to accept that he/she understands the risk (Table 8).

By changing the sampling rate remotely, the user allows the Gateway to have the information about when is it going to receive data from the sensors. The advantage of letting the Gateway have this information is that the compacted files (including data from the entire network) can be closed and upload to the FTP as soon as the sampling of the entire network is completed.

#### 2.5.2.2. Status

In the status tab, the user can view the Gateway status or the Logs of the Gateway.

##### ➤ Gateway status

In the Gateway status menu, the following information is displayed (Figure 28).

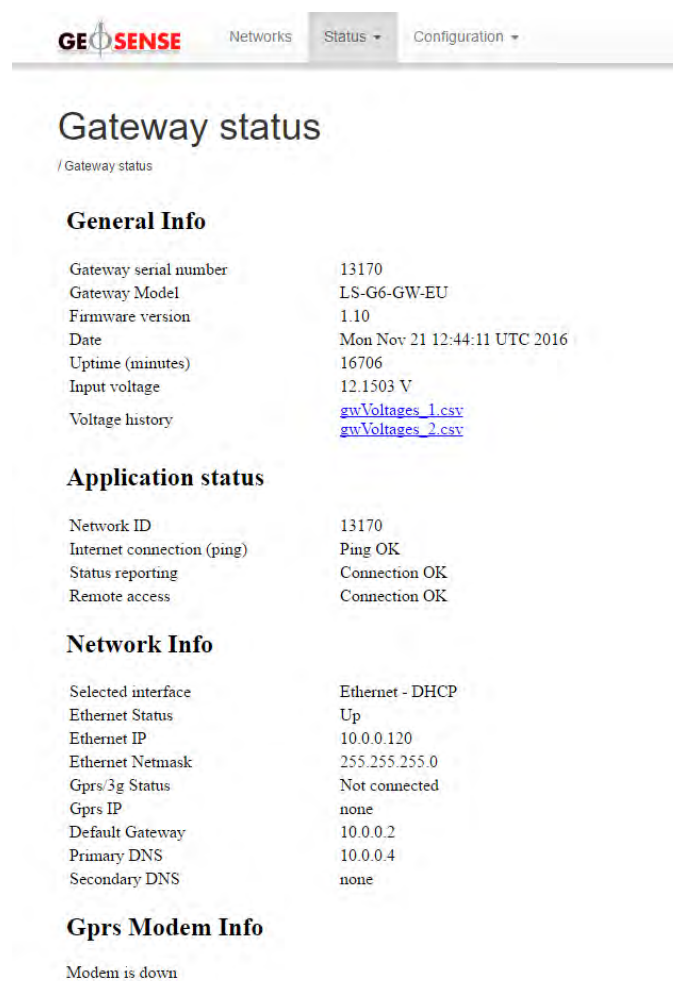
- General Information
  - Gateway serial number
    - Shows the hardware’s serial number. This value cannot be changed.
  - Gateway Model
    - Shows the hardware model.
  - Firmware version
    - Shows the current Firmware version. The Gateway’s firmware can be remotely updated by Geosense Technical Support, as long as the Gateway has an Internet connection, and remote access is working (see below)

- Date
  - Shows the current date, according to the Gateway's internal clock, always in UTC
- Uptime in minutes
  - Shows the time in minutes since the Gateway was connected or rebooted
- Input voltage
  - Shows the voltage that powers the Gateway. This reading has a precision of +/- 0.35V
- Voltage history
  - Link to a .csv file that includes the historical records of the voltage, every 15 minutes. Not separated by months.
- Application status
  - Network ID
    - Shows the current sensor radio network ID
  - Internet connection (ping)
    - Shows if the Gateway is able to connect to the Wi-SOS 480 server, in order to check for connectivity.
    - Check the "Internet configuration" section for more information on this check.
  - Status reporting
    - Shows if the Gateway is able to send status report.
    - These reports are sent via HTTP (port 80) to loadsensing.wocs3.com, and will provide information on the gateway's status to Geosense Technical Support
  - Remote access
    - Shows if the Gateway is able to open a remote access connection to the server.
    - This service uses a TCP connection to loadsensing.wocs3.com, on port 22
    - The remote access mechanism is used:
      - To provide the Wi-SOS 480 Remote Access Service, which allows remote access to the Web Configuration Interface
      - To provide remote access capability to Geosense Technical Support, which allows for remote support and remote updates of deployed Gateways
- Network information

Shows the parameters of the currently active network configuration

- Selected interface
  - Shows the connectivity to the Internet that has been selected by default or manually.
- Ethernet status, IP and Netmask
  - Shows the status of the Ethernet interface (up/down), and the current address if there is one
- GPRS/3G status and IP
  - Shows the status of the GPRS/3G interface (up/down), and the current address if there is one
- Default gateway and DNS servers
  -
- GPRS Modem Info
  - Status

- Indicates if the current status of the GPRS modem is correct.
- IMSI
  - Identification number of a certain user in a cellular network.
- Operator
  - Telecommunication operator used for the GPRS modem.
- Roaming
  - Indicates whether the itinerancies of data in roaming mode is activated or not.
- Mode
  - Indicates the technology (algorithm) used in telecommunications to define the channels and bandwidth to be used (CDMA or WCDMA).
- Signal
  - Indicates, in percentages, the signal coverage of the telecommunications operator.
- LAC
  - Location area code, a number that allows identification
- CI
  - Cell identity



*Figure 28: Gateway status page.*

➤ Logs

In the Logs page, the status actions are reported and the user can select by dates the logs to be displayed.

### 2.5.2.3. Configuration

The configuration tab shows the different configuration options.

#### ➤ General

The Gateway has an internal clock configured in UTC, however, the user can introduce the time zone in the Gateway software interface. By doing so the user will be able to retrieve and visualize the data in local time.

#### ➤ FTP client

In the configuration tab, the user can configure an FTP client, to push the data stored every 15 minutes in the Gateway automatically to the server (see 2.6 Data visualization and retrieval).

Note that 3 different protocols are available (FTP, FTPS and FTPS (ignoring self-signed certificates)). FTPS mode requires that the server has a security certificate, while FTPS ignores the presence of this certification.

The output of the FTP upload can be a new file every time that there is an upload, or alternatively a modification of the monthly generated file.

#### ➤ Compacted CSV

This feature allows the user to create a self-configured csv file, with the desired columns, customized header names, column order, etc. (Figure 29). The maximum number of columns is 520 (maximum supported by Excel). Once saved, a csv file called “compacted-custom-readings-XXXX-current.dat” (XXXX being the network ID) is created. Every time a new compacted csv file is created, the old one is saved with a variation of the suffix “current” by “yyyy-mm-changeX”. This file appears in the Networks main page, where the files to download are visible.

	Column	Node	Data source	Header name	
↑	1	1344	AtmPressure-1344-in-mbar	AtmPressure-1344-in-mbar	🗑️
↑	2	1725	reading-1725-Ch1	reading-1725-Ch1	🗑️
↑	3	1930	AtmPressure-1930-in-mbar	AtmPressure-1930-in-mbar	🗑️
↑	4	1930	thermResInOhms-1930-VW-Ch1	thermResInOhms-1930-VW-Ch1	🗑️

*Figure 29: View of the tool to create a self-configured csv file of the network data.*

### ➤ Modbus gateway

This feature will allow access to the data from the sensors via Modbus TCP protocol. The Modbus address maps can be viewed in the Annex 8.

### ➤ Internet

In the configuration tab, the user can also change the Internet connectivity details (Figure 30). By default, this is set in the automatic mode (Figure 30).

It is possible to select a custom NTP server (from a local network). A custom SMTP server can also be configured.

The screenshot shows the 'Internet' configuration page of the GEOSENSE gateway. At the top, there's a navigation bar with 'Networks', 'Status', and 'Configuration' tabs. The 'Configuration' tab is active. Below the navigation bar, the page title is 'Internet'. There's a sub-header '/ Internet'. The first section is 'Activate network Watchdog' with a checked checkbox. Below it, a warning message states: 'Disable the Network Watchdog if this gateway does not have an internet connection. The network watchdog is a mechanism to reboot the gateway in case of a network failure, modem freeze or other network error condition. It will reboot the gateway after 40 minutes of consecutive unsuccessful Internet connection attempts.' The next section is 'Network connection:' with two radio buttons: 'Automatic (Ethernet if connected, gprs/3g otherwise)' (selected) and 'Manual Configuration'. Below that is 'NTP server (to synchronize the gateway's clock):' with two radio buttons: 'Default (pool.ntp.org)' (selected) and 'Custom'. The next section is 'SMTP server:' with two radio buttons: 'Default (Internet service)' (selected) and 'Custom'. At the bottom, a message says 'Changes will not be applied until next device reboot.' and there is a 'Save configuration' button.

*Figure 30: View of the Internet configuration tab of the gateway. The present configuration is the one by default.*

- Network Watchdog
  - The Network Watchdog is the mechanism that checks whether the Internet connection is working properly.
  - This mechanism checks Internet connectivity every minute, by sending a ping request to loadsensing.wocs3.com
  - If the Gateway is unable to communicate with the server for 40 minutes, it will assume there is a problem with the connection, and reboot the Gateway
  - The Network Watchdog must be disabled if the Gateway does not have an Internet connection
    - If a Gateway with no Internet connection is left with the Network Watchdog enabled, it will start a reboot cycle every 40 minutes. This will lead to sensor data loss, as data entering during the reboot cycle will not be stored.
  - The Network Watchdog is enabled by default
- Network connection
  - Automatic (default)
    - In automatic mode, the network connection mode is automatically configured upon gateway startup

- If a connected Ethernet cable is detected, an Ethernet connection with DHCP will be used
  - An Ethernet cable is connected if there is some kind of network equipment (for example a router or a switch) on the other side of the cable. The PoE injector doesn't count.
- If no Ethernet cable connection is detected, the GPRS connection will be launched, with its configured parameters

Manual configuration (Figure 31).

**Network connection:**

☐ Automatic (Ethernet if connected, gprs/3g otherwise)  
☒ Manual Configuration

☒ Gprs/3G  
☐ Ethernet with DHCP  
☐ Ethernet with static IP

*Figure 31: Options for manual configuration.*

This setting will override auto-detection, and always launch a GPRS/3G connection

- Ethernet with DHCP
  - This setting will override auto-detection, and always launch an Ethernet connection, getting the configuration automatically through DHCP
- Ethernet with Static IP
  - This setting will override auto-detection, and always launch an Ethernet connection.
  - In this mode, you need to manually set all parameters of the network configuration:
    - IP Address
    - Netmask
    - Default gateway
    - DNS servers
- NTP server (to synchronize the gateway's clock)
  - The NTP server by default must be accessible through the Internet, so normally, if the Gateway is connected to the Internet, it is common to use an NTP server.
  - Even in situations where the Gateway is not connected to the Internet, it is still common have a custom NTP server, which may be in a local server.
- SMTP server
  - The default option is to use an SMTP server through the Internet. In the case of the Gateway not being connected to the Internet this option would not be valid.

A custom SMTP server can be defined if the Gateway is not connected to the Internet, however the monitoring e-mails are still required. A custom SMTP server can be placed in a local server.

## ➤ GPRS/3G



The GPRS/3G configuration tab (Figure 32) contains some configuration parameters specific to this type of connection.

GEOSENSE Networks Status Configuration

## GPRS / 3G

/ GPRS / 3G

☒ PIN Off (Sim card is unlocked)  
☐ PIN On (Sim card needs PIN code)

☒ APN Auto selection (will select based on the SIM card operator)  
☐ Manual APN Configuration

APN:   
Username:   
Password:

Changes will not be applied until next device reboot.

Save configuration

*Figure 32: Settings for the configuration of the GPRS/3G connection.*

This configuration will be applied whenever a GPRS/3G connection is used, regardless of whether it was the result of an automatic or manual configuration in the Internet tab.

- PIN setting
  - Off (default)
    - In this mode, the Gateway will not try to unlock the SIM card.
    - If the SIM card is protected by a PIN code, the GPRS/3G connection will fail.
  - On
    - This setting will allow you to enter the PIN code for use with a PIN-locked SIM card.
    - Be careful not to boot the Gateway with a PIN-protected SIM card with the wrong PIN set here. The Gateway will automatically try unlocking the SIM, and exhaust the three possible attempts.
    - There is no way to enter the PUK code in the Gateway. If your card gets PUK-locked, you will need to unlock it using a mobile terminal.
- APN settings
  - APN Auto selection (default)
    - Every mobile operator requires the setting of a specific configuration for connection to its network.
    - The Gateway features a database of the correct configurations for hundreds of operators around the world. This setting will try to configure the connection automatically based on the SIM card that is inserted.
    - This setting may fail if your operator is not in the database, or your configuration is non-standard.
  - Manual APN configuration
    - This setting will allow manual input of the mobile operator configuration values.
    - Use this setting if auto selection didn't work for you, or you need to input specific, non-standard configuration values.

## ➤ Remote access

This page will allow you to change the password used for remote access to the Web Configuration Interface (Figure 33).

The new or the initial provided password will be required to access the gateway either through the public network interface, or through the Geosense Webcentre Remote Access Service.

Be careful on setting weak passwords. This will make your gateway accessible from anywhere on the public network, or anywhere on the Internet if you have an Internet connection.

To change the password from the public interface or from the Remote Access Service, you will need to input the previous password. This is not required if you are connected through the local administration interface.

The default factory password is printed on the **Gateway Information Sheet**. Once you change the password, there is no way to recover it.

In case of a lost or forgotten remote access password, you will need to use the Local Administration Interface to change it to a known one (section 2.5.2).

The screenshot shows the 'Remote access' tab in the Geosense Gateway Web Configuration Interface. The top navigation bar includes 'Networks', 'Status', and 'Configuration'. The main heading is 'Remote access' with a breadcrumb '/ Remote access'. The text explains that this page changes the remote password for the gateway, which is used to access the website from:

- The gateway's Ethernet or GPRS/3G public IP
- The loadensing remote access service, as long as the gateway has an internet connection.
  - Set a **strong password** as this password is used to make your gateway accessible from the Internet
  - The remote access URL for this gateway is <https://loadensing-wocs3.com/13170/>

The factory default remote administration password can be found in the Gateway Information Sheet.

**Admin password**

This is the password for the "admin" user

Current password:

Note: The current password is not necessary if you are logging in through the local administration interface

New password:

Repeat new password:

**View only password**

This is the password for the "viewonly" user

The viewonly user can retrieve information from the gateway, but cannot change any configuration parameters. It is not enabled by default, and must be set a password by the administrator before it can be used.

User enabled: ☐

New password:

Repeat new password:

*Figure 33: Remote Access tab, inside the gateway interface.*

## View only password

This view is designed to provide access to users that are only allowed to see the data collected in the network, but are not allowed to change any of the configuration parameters. The "view only" user has to be defined by the administrator.

## ➤ Radio

This page allows you to configure the parameters of the Wireless Sensor Radio Network (Figure 34). There are three different Gateway models, according to the geographical areas in which they'll be placed. In addition, depending on the country's regulations, the radio configuration will be set specifically.

Note that for some countries, an advanced menu can be displayed. This refers to the possibility of choosing different channels through which data can be sent, in each spreading factor. This will be useful for projects with many Nodes (hundreds), sampling at a high rate. Some Nodes would be set at one group (plus one Gateway) and some other Nodes at a different frequency group (and also a second Gateway configured to this other group) and in this way, possible collision can be avoided.

*Note that if the user changes the default configuration of the advanced options, these should also be changed in the datalogger configuration (see sections 2.3. and 4).*

For the nodes to be able to connect to this Gateway and send data, both the Gateway and all participating Nodes need to be configured with the same parameters.

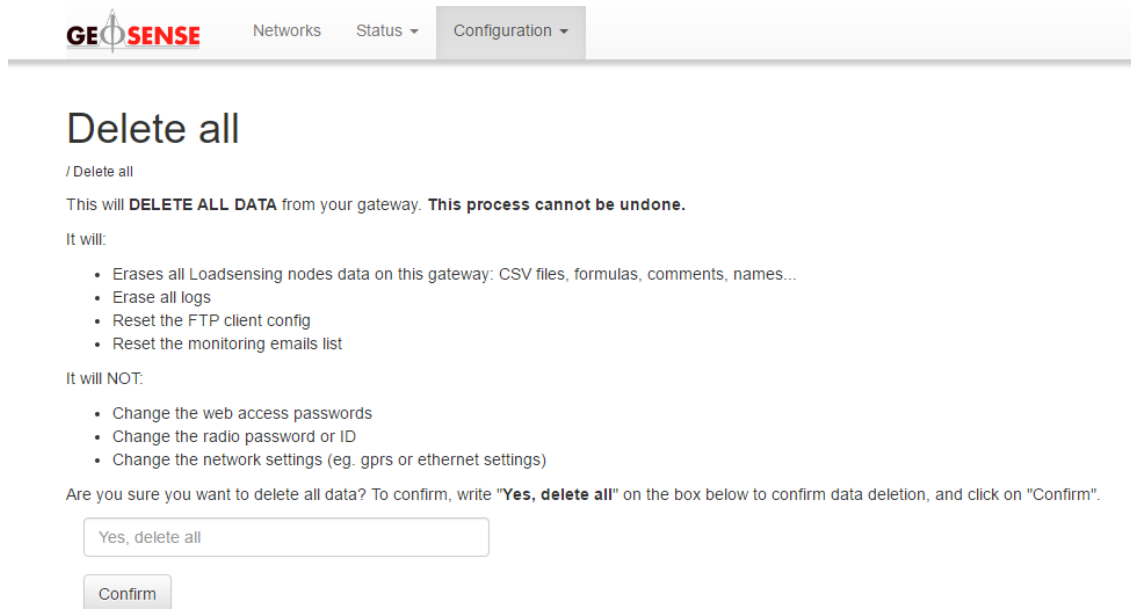
- Network ID
  - A numeric identifier of the wireless sensor network
  - Set by default to the serial number of the Gateway
  - Should only be changed if you're replacing a Gateway and don't want to reconfigure all Nodes in the network
- Network Password
  - This password is used to encrypt all data in transit on the Wireless Sensor Network.
  - The default factory password is printed on the Gateway Information Sheet.
  - Once you change the password, there is no way to recover it. You must change it to a new one in the Gateway as well as in all Nodes in the network.

The screenshot shows the 'Configuration' tab of the GEOSENSE gateway interface. The 'Radio' section is active, displaying configuration options for the wireless sensor network. It includes a breadcrumb trail '/ Radio', a warning about matching parameters with sensors, radio button selection for 'Europe' (selected) and 'Malaysia', a 'Change Country and frequency' button, and a section for 'Change Radio Network ID and password for this gateway:'. This section contains instructions, a 'Network ID' field with the value '13170', a 'Network Password' field, and a 'Change Network ID and password' button. A final warning states 'Changes will not be applied until next device reboot.'

**Figure 34: Radio configuration tab, inside the gateway interface.**

### ➤ Delete all

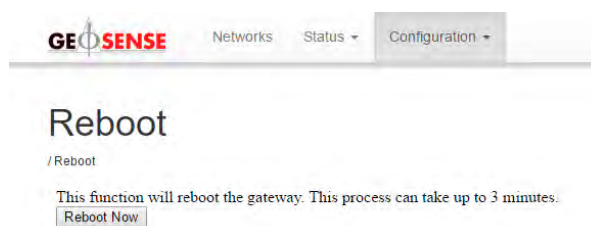
To delete all the data contained in the Gateway (but not all the configuration), the user has to access the tab “Delete all data” (Figure 35) and follow the instructions.



*Figure 35: Delete all tab, inside the gateway interface.*

### ➤ Reboot

After changing some of the configuration parameters of the Gateway, it needs to be rebooted to apply the changes (Figure 36).



*Figure 36: Reboot tab, inside the gateway interface.*

## 2.6. Data visualization and retrieval

For all models, data files (.csv) can be retrieved by USB cable from the datalogger using the OTG USB cable, through the Android application DLOG. The option for downloading data is in the “Sensors data” tab, using the arrow pointing down. The data files can also be sent via email.

For the radio model the data is sent to the Gateway and is retrieved from there. In the Gateway it is possible to display the data collected in the nodes, transformed into engineering units and with a graphical interface. The storage capacity of the Gateway is 8 GB.

For the transformation into engineering units, the user needs to introduce the required formula, depending on the sensor. In the Last readings tab, when selecting a node, a gear icon is placed to the far right of each channel's last reading (Figure 37). By clicking this icon, the menu to edit the formula corresponding to the sensor is displayed (Figure 38).

The formula should be selected from a drop-down menu of several Linear and Polynomial formulae available.






Last readings and Time series graphs			
Channel	Thermistor (Ohms) 	Frequency (Hz) 	
1	4294967.295	1529.097	
Pressure (mBar) 		Pressure (kPa)	
1011.1		101.11	
Received on 2015-09-01T09:47:30Z			

Figure 37: In the “Last readings” tab, a gear icon appears on the right, for editing the formula of the sensor.

## Engineering units

/ Networks / 13004 / Node 1140 / Engineering units

### Channel 1

☒ Use engineering units

Polynomial A with compensation

$$P = AR_i^2 + BR_i + C + K(T_i - T_0) - F(S_i - S_0) + D$$

P: Converted data in units

R<sub>i</sub>: Current Reading in digit during observation

T<sub>i</sub>: Temperature during the observation

S<sub>i</sub>: Current barometric pressure in kPa

Units: Magnitude that is measuring the sensor (ie: mBars, mm)

kPa

A: Polynomial gage factor (from calibration)

4.6290E-08

B: Polynomial gage factor (from calibration)

-1.5185E-01

C: Polynomial gage factor (from calibration)

9.6881E+02

K: Thermal factor in units/°C

0.015

T<sub>0</sub>: Temperature at the time of taking zero reading in °C

20

F: Conversion factor in units/kPa

1

S<sub>0</sub>: Barometric pressure at time of installation in kPa

101.1

D: Offset in units

0

Thermistor YSI44005 (°C)

$$T = \frac{1}{A + B(\ln R) + C(\ln R)^3} - 273.2$$

T: Temperature in °C

LnR: Natural log of thermistor resistance

A: 1.4051 x 10<sup>-3</sup>

B: 2.366 x 10<sup>-4</sup>

C: 1.019 x 10<sup>-7</sup>

Note: Coefficients calculated over the -50°C to +150°C span.

Figure 38: Menu to edit the formulae for transforming the raw data of the sensors into engineering units.

Gateway data visualization and retrieval is possible by accessing the Gateway (locally or through the server) and clicking the icon next to each header (Figure 39).

Data visualization in the charts is of only the last 400 readings of each sensor. In each chart, all the sensors connected to a datalogger are displayed. Some sensors may be deactivated from the chart by the user (Figure 40).

Under the Configuration tab, the time zone of the Gateway can be configured. It is important for correct display of the charts, as otherwise they will be shown in UTC.

Channel	Thermistor (Ohms) <a href="#">↗</a>	Frequency (Hz) <a href="#">↗</a>	Engineering units <a href="#">↗</a>	T (°C) <a href="#">↗</a>	
1	3165.588	2207.994	98.546 mm	23.7	<a href="#">⚙</a>

Figure 39: Circled in red, the icon to display the charts of each of the sensors.

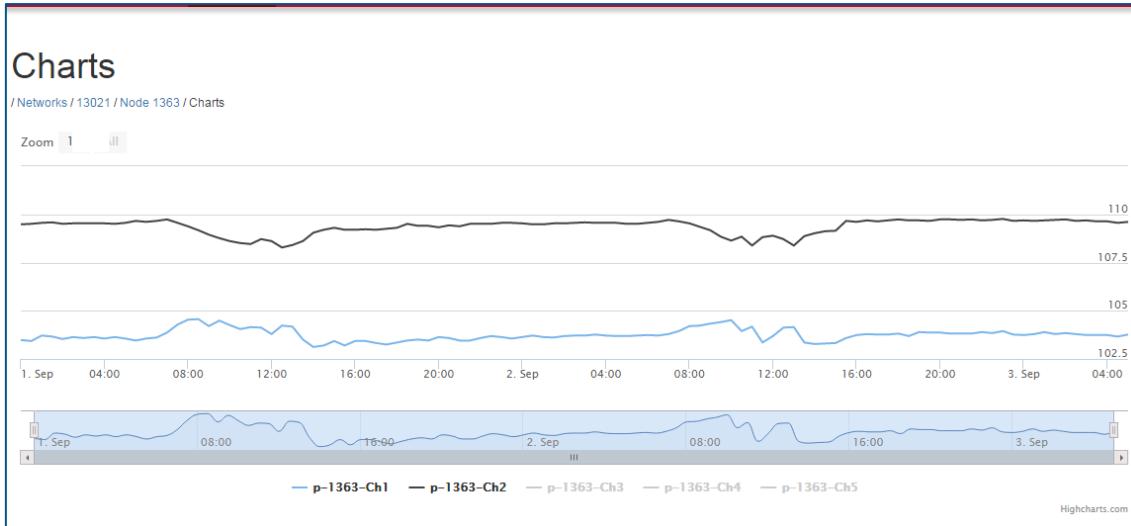


Figure 40: Example of a chart of one datalogger.

Retrieval of data can be done into two different ways:

- General network files: three .dat files are available to download (Figure 41):
  - compacted readings of raw data from the dataloggers
  - compacted readings in engineering units
  - compacted custom readings (created by the “Compacted CSV” option.)

A gateway with stable Internet connection through SIM card and a single (compacted) FTP upload usually consumes in the vicinity of 150 MB/month. The FTP upload happens every 15 minutes, and if the existing file in the FTP is consistent, only new data is uploaded and either appended to the existing file or a new file is created. In the case that the file is corrupted or removed, the whole file is uploaded again, to ensure that there is always a complete copy in the server.

Network: 13104 [✎](#)

/ Networks / 13104

Comments

Compacted readings CSV files [⬇ compacted-readings-13104-current.dat](#)  
+ More

Compacted engineering units CSV files [⬇ compacted-eng-13104-2015-12.dat](#)

Signal coverage test map

Nodes [🔍](#)

☐ All 0 nodes selected of 3

Id	Name	Status	Model	Serial
----	------	--------	-------	--------

Figure 41: View of the screen where the .csv files of raw data and data transformed into engineering units (of the complete network) can be downloaded.

Note that the file where the new data is saved is called xxxxx-current.dat. The current file is prepared to support up to 520 columns.

At the end of the month, the file is closed and named xxxxx-yyyy-mm.dat (yyyy:year; mm: month). Files of past months can be retrieved by clicking “+ More” below the current file. During the process of closing the file and changing the name, there is a delay of 1.5 hours.

- Specific files for each of the Nodes: two csv files are available to download (Figure 42):
  - health (containing battery in V, temperature in Celsius and uptime node in seconds)
  - data readings (raw data)

**Node 1852**

/ Networks / 13104 / Node 1852

Name	
Installation date	
Comments	
Model	LS-G6-VW-5-FCC
Firmware version	2.15
Serial number	1852
Health CSV files	<a href="#">1852-health-2015-12.csv</a>
Vibrating wire CSV files	<a href="#">1852-readings-2015-12.csv</a>

▼ Last readings and Time series graphs

Channel	Thermistor (Ohms)	Frequency (Hz)	Engineering units	T (°C)	
1	4294967.295	1571.536	-3.738 mm	-87.5	
2	4294967.295	1584.172	160.158 mm	-87.5	

Pressure	Pressure (kPa)	
988	98.8	

Received on 2015-12-17T20:53:32Z

► Status

► Metadata

► Last messages

Figure 42: View of the screen where the data of a specific datalogger can be downloaded.

In the configuration tab, also the FTP can be configured (Figure 43). The user can specify the FTP settings and the files that they want uploaded. When the FTP is first configured in the gateway, an upload test is performed.

The files can be uploaded to the FTP:

- Separately, per node type. Files are pushed every 15 minutes, in real time.
- Compacted in one file. Files are pushed every 15 minutes; however, this option is delayed one-hour respect to the real time. The reason for this delay is that the compacted file is generated every hour, and to avoid conflicts between reception of data and the file creation, the file is created with 1 hour delay. The new data can be uploaded in a separate file every new upload, or by appending the new data to the end of the existing file. The data consumption in both cases is similar.

The available protocols for the FTP are: FTP, FTPS (which requires a security certification) or FTPS (without security certification). The folder to which the data is uploaded can be directed by a relative path, or by the full path. Data can be accessed through http calls.



The way FTP upload works is like this:

1. Gateway checks which was the last data uploaded in the FTP file
2. It uploads the following data (in the same file).
3. If the Gateway doesn't find the file (because it was removed) it uploads it again from the beginning of the month.

The screenshot shows the 'Configuration' tab in the GEOSENSE interface. The 'FTP client' section is active, showing a status message: 'Data is pushed to the FTP every 15 minutes'. Below this, there are input fields for 'Hostname', 'Port number' (set to 21), 'Username', and 'Password'. There is a checkbox for 'Use anonymous FTP'. Below these are dropdown menus for 'Protocol' (set to FTP), 'FTP mode' (set to Passive), and 'Output' (set to Append to end of file). At the bottom, there is a table with columns 'Type of file', 'Enabled', and 'Full path (starting with /) or Relative path (starting with ./)'. The table lists several data types: Health, Vibrating wire data, Inclinator data, Volt data, SHM data, Weather data, and Compacted data, each with an 'Enabled' checkbox and a corresponding path input field.

Type of file	Enabled	Full path (starting with /) or Relative path (starting with ./)
Health	<input type="checkbox"/>	
Vibrating wire data	<input type="checkbox"/>	
Inclinator data	<input type="checkbox"/>	
Volt data	<input type="checkbox"/>	
SHM data	<input type="checkbox"/>	
Weather data	<input type="checkbox"/>	
Compacted data	<input type="checkbox"/>	

Figure 43: View of the screen where the FTP can be configured.

Alternatively, the last messages received by the Gateway are displayed in API format. This can be viewed under the tab “Last Messages” of the software interface (Figure 44).

The screenshot shows the 'Last messages' tab in the software interface. It displays a table with two columns: 'Type' and 'Message'. The 'Type' column shows 'coverageTestV1'. The 'Message' column shows a JSON object representing the message data.

Type	Message
coverageTestV1	<pre>{   "nodeModel": "LS-G6-VW-5-EU",   "commMetaData": {     "networkId": "13012",     "macAddress": "57673283",     "receivedTimestamp": "2015-09-01T09:35:20Z",     "frequencyHertz": 868.85,     "snr": 11,     "sequenceCounter": [       53     ]   },   "gatewayId": 13012,   "rssi": -51,   "type": "longRangeRadioMetaDataV1",   "sf": 12,   "macType": "ETSIv1" }</pre>

Figure 44: View of last messages received by the gateway, displayed in API format.

## 2.7. Maintenance

Proper maintenance of Wi-SOS 480 components is essential for obtaining accurate data. Equipment must be in good operating condition, which requires a program of regular inspection and maintenance. The person in charge of the logging system can carry out routine and simple maintenance. The more difficult maintenance such as Node calibration, performance testing, and component replacement, should be done by someone from the Geosense Technical Support Team.

A station log should be maintained for each monitoring site that includes serial numbers, dates of site inspections, and maintenance performed.

### 2.7.1. General Maintenance

- Check sensor leads and cables for cracking, deterioration, proper routing, and strain relief. Replace sensor cables if required.
- Check that the box junction and cable gland are dry and completely tightened.
- Check that the screws are correctly locked and the enclosure lid is in perfect condition.
- Check battery life periodically. Replace when less than 20% remaining.

### 2.7.2. Periodical maintenance

#### 1 Month

- a. Monitor data values collected by the units periodically. Abnormal or out of range sensor values may indicate problems with the unit.
- b. Monthly visual inspection of the station to observe any apparent problems.
- c. Do a visual inspection of the sensors and position of the Node & Gateway enclosures.

#### 6 Months

- a. Inspect the enclosure seal.

#### 12 Months

- a. Check battery life periodically. Replace when less than 20% remaining.

#### 2-3 years

- a. Battery replacement. The lifetime of the battery depends on the use of each Node, number of channels, sensors, etc.

### 2.7.3. Return material authorization

If goods are to be returned for either service/repair or warranty, the customer should contact Geosense for a Returns Authorisation Number, request a Returned Equipment Form QF034 and, where applicable, a Returned Goods Health and Safety Clearance Form QF038 prior to shipment. Numbers must be clearly marked on the outside of the shipment.

Complete the Returned Equipment Form QF034, including as much detail as possible, and enclose it with the returned goods.

All returned goods are also to be accompanied by a completed Returned Goods Health and Safety Clearance Form QF038 attached to the outside of the package (to be accessible without opening the package) and a copy of both forms should be faxed in advance to the factory.

#### **Chargeable Service or Repairs**

Inspection & estimate

It is the policy of Geosense that an estimate is provided to the customer prior to any repair being carried out. A set charge for inspecting the equipment and providing an estimate is also chargeable.

#### **Warranty Claim**

(See Limited Warranty Conditions)

This covers defects which arise as a result of a failure in design or manufacturing. It is a condition of the warranty that the Geosense Wi-SOS 480 system must be installed and used in accordance with the manufacturer's instructions and has not been subject to misuse. To make a warranty claim, contact Geosense and request a Returned Equipment Form QF034. Tick the warranty claim box and return the form with the goods as above. You will then be contacted and informed whether your warranty claim is valid.

#### **Packaging and Carriage**

All used goods shipped to the factory must be sealed inside a clean plastic bag and packed in a suitable carton. If the original packaging is not available, Geosense should be contacted for advice. Geosense will not be responsible for damage resulting from inadequate returns packaging or contamination under any circumstances.

#### **Transport & Storage**

All goods should be adequately packaged to prevent damage in transit or intermediate storage.

## 2.8. VW Node

### 2.8.1. Sensor connection

Most of the vibrating wire sensors can be interfaced to the VW node.

The Node is supplied with cable glands (one for each channel), for the adjustment to different cable diameters.

After each terminal block is connected, taking a sensor reading is recommended to ensure that the connections have been done correctly. This reading should be compared with the reading of the sensor on installation with a portable readout unit, before connecting to the WI-SOS 480 Node. Note that some configuration is required during the installation (see section 3 of this manual).

Cables must be connected in accordance to the following table:

Each terminal block has a group of 5 connectors.

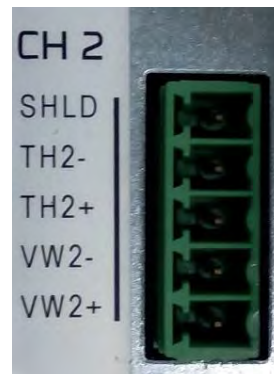
Each group has:

- 2 x Vibrating wire channel
- 2 x Thermistor channel
- 1 shield terminal

An example of the connections for one terminal block (Table 1 and Figure 45) is listed below.

*Table 1: Connections of the terminal block.*

Name	Function
SHLD	Used to connect the sensor shield if needed
TH2-	Thermistor input 2. No polarity.
TH2+	Thermistor input 2. No polarity.
VW2-	Differential voltage input 2.
VW2+	Differential voltage input 2.



*Figure 45: Detail of a terminal block.*

### 2.8.2. Barometric measurements

The Node includes a barometer (BOSCH BMP180 device). It is important to avoid placing the Node inside any type of enclosure as this could affect the correct readings of the barometer through the gore valve.

If the Vibrating Wire sensor requires barometric pressure compensation (such as piezometers installed in locations which can be affected by changes in barometric pressure), the current pressure readings

from the barometer are usually used directly. The transformed data (compensated by the barometric pressure) is displayed if the user selects the option “Polynomial A with compensation” in the Engineering Units drop-down menu (see section 2.6).

In the case that the desired measurement is the atmospheric pressure at the sea level (commonly used in meteorology), a correction of the barometric readings is needed.

The formula for the correction of the barometric readings to provide atmospheric pressure at the sea level is:

$$p_0 = \frac{p}{\left(1 - \frac{\text{altitude}}{44330}\right)^{5.255}}$$

$p_0$ = pressure at the sea level in mbar

$p$ = current pressure reading

altitude= altitude in m.a.s.l. (metres above sea level)

### 2.8.3. Battery lifespan

The following table gives the indicative battery lifespan per channel (Table 2). The user should take into account that consumption varies depending on the sensor used, the sampling rate and the environmental conditions.

*Table 2: Indicative lifespan for VW Node 1 ch (using 1 C-size cell) and VW Node 5 ch. (using 4 C-size cells)*

Number of sensors	Sampling rate (considering SF 7)			Sampling rate (considering SF 9)		
	30 minutes	5 minutes	30 secs	30 minutes	5 minutes	30 secs
1	>10 years	>10 years	1.2 years	>10 Years	>10 years	7 months
5	>10 years	7 years	3 months	>10 years.	5 years	2 months

NOTE: Extreme temperatures could cut down the capacity by 20 to 40%, check the specifications of your batteries. USB not used.

### 2.8.4. Configuration

The vibrating wire node requires configuring the sweep frequency before starting. There are several existing predefined sweep frequencies:

- Sweep Frequency A (450-1125 Hz),
- Sweep Frequency B (800-2000 Hz),
- Sweep Frequency C (1400-3500 Hz),
- Sweep Frequency D (2300-6000 Hz)
- Custom Sweep Frequency (min value: 300 Hz max value: 7000 Hz).

For the configuration of the radio communications of the Noder, see section 2.3 of this manual.

### 2.8.5. Data storage

The internal Node memory size is 4 MB. The 5-channel Node connected to 5 sensors stores up to 73.500 readings. The 1-channel Node stores up to 200.000 readings. Times of data storage for a 1 channel Nodes and a 5 channel Node are indicated in Table 3. Memory mode is a circular buffer. When memory is full, logging continues by overwriting earliest readings. Besides the data from the sensor, health data is collected hourly, which indicates the battery voltage, the internal temperature of the Node and the Node uptime.

*Table 3: Times of data storage (without overwriting) for VW Nodes; 1 ch and 5 ch.*

Number of sensors	Sampling rate		
	60 minutes	30 minutes	10 minutes
1	more than 10 years	more than 20 years	3.5 years
5	8 years	4 years	17 months

## 2.9. Digital Node

### 2.9.1. Sensor Connection

The digital Node supports 2 different sensor models by default (RS485 port):

- Geosense Digital Tilt Sensors
- RST Digital Tilt Sensors

Up to 30 sensors can be safely powered from the Node, however up to 60 sensors may be read and transmitted by the Node. If more sensors are to be supplied, an external 12 V battery should be connected. In this case, contact Geosense.

The wiring is indicated in the RS485 port of the Node. The Node needs to be placed at HALF to read the inclinometers. For the connection of SDI ports the wiring specification of the sensor must be checked.

a)



b)



*Figure 46: View of the inside of the digital Node*

Digital Nodes (Figure 46) can also support other digital sensors, with SDI interface connection. These types of sensors are not supported by default by the node, but drivers can be developed by Geosense engineers. The wiring for the sensors with SDI interfaces will depend on the model of the sensor; however, the label of each terminal is indicated.

### 2.9.2. Battery lifespan

The following table gives the indicative battery lifespan per channel (Table 4 and Table 5). The user should take into account that consumption varies depending on the sensor used, the sampling rate and the environmental conditions.

*Table 4: Indicative lifespan for a digital node. Estimations using 4 c-size cells*

Number of sensors	Sampling rate			
	6 hours	2 hours	30 minutes	5 minutes
10 (RS485)	>10 years	5.5 years	2.5 years	4 months
30 (RS485)	5,2 years	10 months	4 months	26 days

*Table 5: Indicative lifespan for LS-DIG datalogger. Estimations using 4 c-size cells*

### 2.9.3. Configuration

The configuration of the digital Node requires specifying the protocol of communication (from given options) and the bus addresses of the sensors connected in the RS485 port. This action is done through the Android Configuration App. The bus addresses of the digital sensors are specified by manufacturers. Up to 30 sensors can be connected in a bus chain. When connecting the sensors, we recommend using resistors. In some cases, this is clearly specified by manufacturer of the sensors.

For the configuration of the radio communications of the Node, see section 2.3 of this manual.

### 2.9.4. Data storage

Capacity for up to 90.000 readings from the sensors (each one with 2 axes and temperature, grouped by 5 sensors) (Table 6)

*Table 6: Indicative storage capacity of the digital Node. Estimations using 5 sensors.*

Number of sensors	Sampling rate		
	60 minutes	30 minutes	10 minutes
5	more than 10 years	5 years	20 months

## 2.10. Volt Node

### 2.10.1. Sensor Connection

The volt node supports 6 different sensor models that can be connected independently to four different channels (Figure 47):

- Voltage (+/- 10 V peak to peak)
- Full Wheatstone Bridge (39.06 mV)
- Thermistor (-40 to 85 °C for a standard 3K ohms)
- Current Loop (4-20 mA, 2 or 3 wires)
- Potentiometer (5 V)
- PT100 (-40 to 85°C)



*Figure 47: View of the LS-G6-ANALOG datalogger internally where the four channels can be identified.*



The wiring of the sensors is indicated in the Android configuration app, once the type of sensor to be connected to the channel is selected (Figure 48).

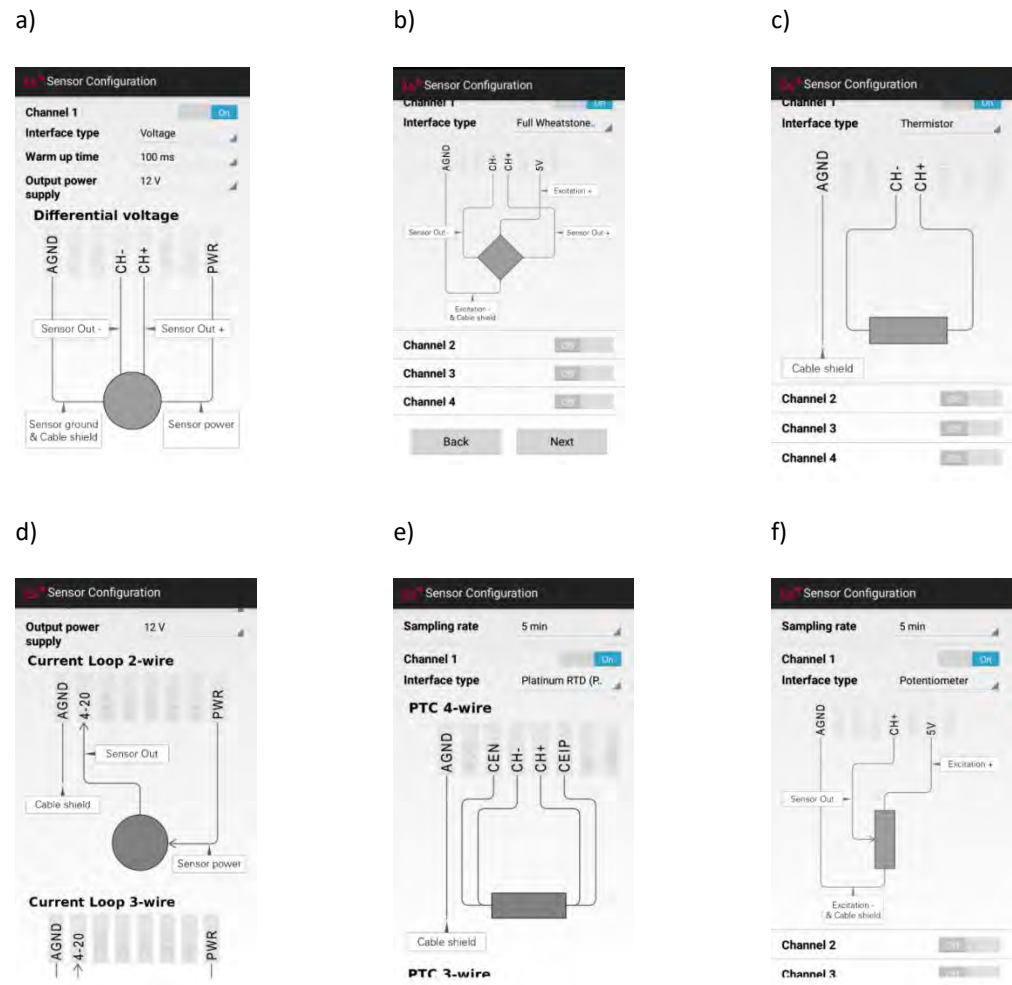


Figure 48: View of the wiring of the different types of analogue sensors, indicated in the Android Configuration App.

The Node can measure both voltage differential and single ended voltage sensors outputs. The standard wiring is for differential, and for single ended it is necessary to wire the negative input of the Node to the ground terminal

The wiring can be connected once the Setup Wizard in the Android Configuration App has been initialised, which is when the wiring schemes appear.

### 2.10.2. Battery lifespan

The following tables give the indicative battery lifespan for the volt Node, (Table 7 a, b and c) depending on the type of sensor, the warm up time and the sampling rate. The user should take into consideration that consumption will vary depending on the sensor used, the sampling rate and the environmental conditions.

Table 7: Indicative lifespan for the volt Node. Estimations using 4 c-size cells, considering SF9

a)

Channels & sampling	Sensor features			
	Current @12V@24mA	Current @12V@24mA	Current @24V@24mA	Current @24V@24mA
Warm up time	1 second	5 seconds	1 second	5 seconds
1 CH 5 min	6 months	3 months	4 months	2 months
1 CH 30 min	2.5 years	1 year	2 years	1 year
1 CH 1 hour	5.5 years	2.5 years	3.5 years	1.5 years
1 CH 6 hours	>10 years	>10 years	>10 years	9.5 years
4 CH 5 min	1.5 months	39 days	39 days	1 month
4 CH 30 min	9 months	7.5 months	7.5 months	6.5 months
4 CH 1 hour	1.5 years	1 year	15 months	1 year
4 CH 6 hours	8 years	6.5 years	6.5 years	5.5 years

b)

Channels & sampling	Sensor features			
	Voltage @12V@24mA	Voltage @12V@24mA	Voltage @24V@24mA	Voltage @24V@24mA
Warm up time	1 second	5 seconds	1 second	5 seconds
1 CH 5 min	5 months	2.5 months	1.5 years	2.5 months
1 CH 30 min	2.5 years	1 year	10 months	1.5 years
1 CH 1 hour	4.5 years	2.5 years	1.5 years	2.5 years
1 CH 6 hours	>10 years	>10 years	8.5 years	>10 years
4 CH 5 min	2 months	1 month	1.5 months	25 days
4 CH 30 min	1 year	6 months	10 months	5 months
4 CH 1 hour	2 years	1 year	1.5 years	10 months
4 CH 6 hours	>10 years	5 years	8.5 years	4.5 years

c)

Channels & sampling	Sensor features					
	FWB@5V@ 0.7 kΩ	FWB@5V @1.4 kΩ	Potentiometer@5V@1.5 kΩ	Potentiometer@ 5V@5 kΩ	Thermistor@5V @3 kΩ	PT100
1 CH 5 min	1.5 years	1.5 years	1.5 years	1.5 years	1.5 years	1 year
1 CH 30 min	8 years	8 years	>10 years	8.5 years	8.5 years	5.5 years
1 CH 1 hour	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years
1 CH 6 hours	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years

4 CH 5 min	5 months	6 months	6.5 months	7 months	7.5 months	4 months
4 CH 30 min	2.5 years	2.5 years	3 years	3.5 years	3.5 years	1.5 years
4 CH 1 hour	4.5 years	5.5 years	5.5 years	6 years	6.5 years	3.5 years
4 CH 6 hours	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years

### 2.10.3. Configuration

The configuration requires specifying the excitation power voltage and the warm-up time for the sensors that need power supply (voltage and current loop sensors). For the other sensors, 5V excitation supply is present in all channels connectors.

Excitation power voltage can be 12 V or 24 V, and warm-up times: 100, 300 and 500 milliseconds or 1, 2, 5 and 10 seconds.

See section 2.3 for the configuration of the radio communications of the Node.

### 2.10.4. Data storage

Capacity for up to 130.000 readings with 4 sensors connected (Table 8).

*Table 8: Indicative storage capacity of the volt node. Estimations using 4 sensors.*

Number of sensors	Sampling rate		
	60 minutes	30 minutes	10 minutes
4	more than 10 years	7 years	2.4 years

## 3. WIRELESS RADIO

### 3.1. Maximum number of nodes connected in a network

The number of Nodes that can be connected in a radio network is limited by the number of messages that can be transmitted over a period of time. All Nodes in the network take their readings at a synchronised time (e.g. if reading every 5 minutes, it's every hour, at minute 0,5,10,15 and so on). These messages are then written to internal Node memory, but are not transmitted immediately. The readings are transmitted to the Gateway at a random time inside a communication slot (**Error! Reference source not found.**).

The length of the communication slot depends on the number of Nodes in a network (Table 9), and is chosen automatically by the Android Configuration App when a Node gets configured. There are also combinations of network size and sampling rate which are not supported. This is to prevent all Nodes from sending at the same time and saturating the network.

*Table 9: Slot times table. Columns are the number of nodes; rows are sampling rate. Slot times are in seconds.*

	0-20	20-100	100-200	200-1000	1000-2000
10 secs	NO	NO	NO	NO	NO
30 secs	20	NO	NO	NO	NO
1 min	40	NO	NO	NO	NO
5 mins	60	240	NO	NO	NO
15 mins	60	600	600	NO	NO
30 mins	60	600	900	NO	NO
1h	60	600	900	2700	NO
6hrs	60	600	900	2700	3600
12hrs	60	600	900	2700	3600
24hrs	60	600	900	2700	3600

*Note that the digital Node doesn't necessarily comply with the slot times table (Table 9) because reading may take longer than VW or volt nodes.*

### 3.2. Radio configuration

Region and country: These values must match the location where the Nodes are deployed, in order to comply with the local regulations. There is a specific Gateway model for each region, and the Gateway must also be configured to the correct country / radio mode (Table10). To achieve communication, the Gateway and all the Nodes on a network need to be configured in the same way.

- 923A-legacy radio: This radio mode has some differences to the radios on other modes. In the rest of the countries, the Gateway is always listening to all Spreading Factors, and on different frequencies. The Node can choose which SF and frequency to transmit on. In this mode, this is not possible. The Gateway and all Nodes must be configured to a Specific Spreading Factor and channel, which must be the same for all devices on the network. The default values are Channel 1, Spreading Factor 9, so these will be the values used if the Advanced options were ignored on both the Gateway and the Nodes.
- Network ID and password:
  - These values are used to identify a radio network, and to protect (encrypt) the data in transit. A strong password will prevent a malicious attacker from both reading data from your sensors and from inserting bogus data posing as a sensor.
  - The radio network ID is set by default to the Gateway's serial number, but it can be changed. For example, if you are replacing a Gateway, you might want to set the new Gateway (with a new serial number) to the old Gateway's network ID, so that the Nodes don't have to be reconfigured.
  - The network password is set by default to a randomly generated value, which is printed on your Gateway Information sheet. The generated password is unique to each Gateway unit, so it can be used safely.
  - To achieve communication, the Gateway and all the Nodes on a network need to be configured with the same network ID and password.

- For security reasons, the network password cannot be read from a Node by the Glog Android app. For this reason, when entering the radio configuration dialog, the password displayed is the last one that was set using this Android device.
- Advanced options:
  - (Europe only) ETSI limit duty cycle: The European Telecommunications Standards Institute (ETSI) defines a time limit during which a radio device may transmit on a given frequency over a 1-hour period. In some rare cases (high sampling rates on high SF), the node may exhaust its radio time, and it will stop transmitting until the next hour. This option can be disabled for testing purposes, or for use in places where the norm doesn't apply (e.g. Inside a mine)
  - Maximum Spreading Factor: Defines the maximum spreading factor the Node is allowed to transmit to.
    - Lower spreading factors allow for faster data transmission, so more nodes can share the same radio space.
    - Higher spreading factors allow for more reliable data transmission, allowing for longer distances and better immunity to interference.
  - ADR (All modes except 923A-legacy): ADR (Adaptive Data Rate) is the mechanism which allows the node to automatically negotiate the lowest viable spreading factor with the gateway. When the ADR is off, the node will always use the highest SF (as set on the previous selector).
  - Transmit power: Allows adjusting of the transmit power, in dB. The maximum allowed transmit power is specific to each country.
- Channel (923A-legacy only): It's possible to choose between 4 different channels in Australia:
  - Channel 1: 921.9 MHz
  - Channel 2: 922.5 MHz
  - Channel 3: 923.7 MHz
  - Channel 4: 924.3 MHz
- Channel group (FCC only): In FCC mode, the radio will use frequency hopping on a group of 8 channels. You may want to use a different channel group to move away from interferences on specific channels. All devices on a network (the gateway and all nodes) must be set to the same configuration. There are 8 groups to choose from:
  - Group 0 (Channels 00-07) – 902.3 to 903.7 MHz
  - Group 1 (Channels 08-15) – 903.9 to 905.3 MHz
  - Group 2 (Channels 16-23) – 905.5 to 906.9 MHz
  - Group 3 (Channels 24-31) – 907.1 to 908.5 MHz
  - Group 4 (Channels 32-39) – 908.7 to 910.1 MHz
  - Group 5 (Channels 40-47) – 910.3 to 911.7 MHz
  - Group 6 (Channels 48-55) – 911.9 to 913.3 MHz
  - Group 7 (Channels 56-63) – 913.5 to 914.9 MHz

Table 10: Summary of radio specifications by mode.

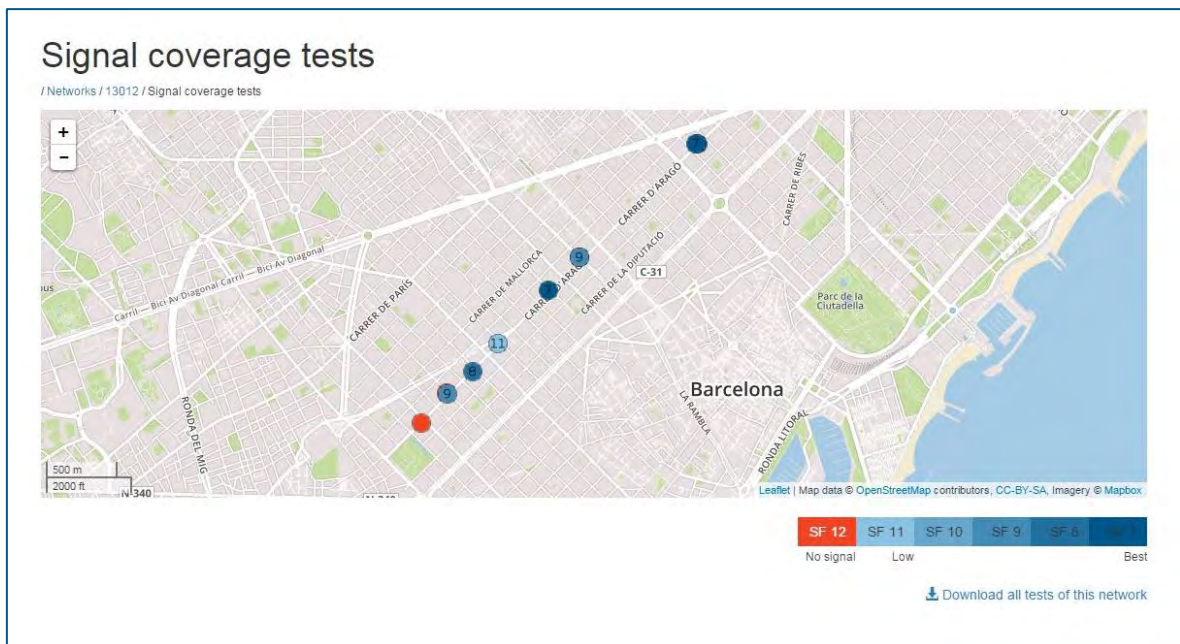
		EU	Malaysia	FCC	923P	923A	Australia 500 KHz	Singapore
Upload	# of channels used by the gateway	8	8	8 (one group of 8 available)	8	8	1 (4 available)	6
	Channel's frequencies (MHz)	868.1, 868.3, 868.5, 868.85, 869.05, 869.525	869.1, 869.3, 869.5, 869.7, 869.9	Group 0: 902.3, 902.5, 902.7, 902.9, 903.1, 903.3, 903.5, 903.7 Group 1: 903.9, 904.1, 904.3, 904.5, 904.7, 904.9, 905.1, 905.3 Group 2: 905.5, 905.7, 905.9, 906.1, 906.3, 906.5, 906.7, 906.9 Group 3: 907.1, 907.3, 907.5, 907.7, 907.9, 908.1, 908.3, 908.5 Group 4: 908.7, 908.9, 909.1, 909.3, 909.5, 909.7, 909.9, 910.1 Group 5: 910.3, 910.5, 910.7, 910.9, 911.1, 911.3, 911.5, 911.7 Group 6: 911.9, 912.1, 912.3, 912.5, 912.7, 912.9, 913.1, 913.3 Group 7: 913.5, 913.7, 913.9, 914.1, 914.3, 914.5, 914.7, 914.9	921.4, 921.6, 921.8, 922, 922.2, 922.4, 922.6, 922.8	917.2, 917.4, 917.6, 917.8, 918, 918.2, 918.4, 918.6	920.9, 921.2, 921.5, 922.8, 923.1, 923.4	
	Channel bandwidth (KHz)	125	125	125	125	125	500 (short range)	125
Download	# of channels used by the gateway	8	8	8 (one group)	8	8	1 (4 available)	6
	Channel's frequencies	868.1, 868.3, 868.5, 868.85, 869.05, 869.525	869.1, 869.3, 869.5, 869.7, 869.9		921.4, 921.6, 921.8, 922, 922.2, 922.4, 922.6, 922.8	923.3, 923.9, 924.5, 925.1, 925.7, 926.3, 926.9, 927.5	921.9, 922.5, 923.7, 924.3	920.9, 921.2, 921.5, 922.8, 923.1, 923.4
	Channel bandwidth (KHz)	125	125	500	125	500	500	125
	Upload/Download same channels?	Yes	Yes	Yes	Yes	No	No	Yes
	Power transmission (by default) (dB)	14	14	20	20	20	20	20
	# of available Spreading Factors	5	5	5	5	5	5	5
	# of used Spreading Factors per network	5	3	3	5	1		
	Configuration in datalogger	-	-	Channel group (Group 0 by default)	-	-	Channel and SF	-
	Configuration in gateway	-	-	Channel group (Group 0 by default)	-	-	Channel and SF	-

### 3.3. Results of signal coverage test

In section 2.3, the signal coverage tests are presented. There are several ways to get the results of the signal coverage tests:

- 1) Receiving the results of the signal coverage tests in the Android Configuration App (Figure 12).
- 2) They are also displayed geographically in the software of the Gateway (Figure 49). In this case, the Gateway must be connected to the Internet, to get the map. The position where the tests have been carried out is displayed with a specific symbol that related to the coverage at the specific point. The symbol selected (color legend) indicates the maximum SF from which >50% of the information packages sent by the node have reached the gateway. In red, the places where  $\leq 50\%$  of the packages of SF 12 are indicated. The Gateway is also indicated in the map.
- 3) Moreover, the results of the signal coverage tests can be downloaded from the Gateway in a .csv file (Figure 49, lower right corner). If the test is done “offline”, the results only appear in this .csv.

*Note that whether or not the Gateway has received the data from the tests, all the tests are saved in a .csv file inside the Android device (GLOG directory). Geographical data is also saved there (if GPS is activated in the Android).*



**Figure 49: View of the geographical display (in the software of the Gateway) indicating the results of the signal coverage tests.**

## 4. CONTACT GEOSENSE

Phone: +44 1359 270457 (08.30h - 18.00h GMT)

Technical support: [support@geosense.co.uk](mailto:support@geosense.co.uk)

Sales information: [sales@geosense.co.uk](mailto:sales@geosense.co.uk)

Geosense Ltd  
Nova House  
Rougham Industrial Estate  
Rougham  
Bury St Edmunds,  
Suffolk,  
England IP30 9ND


[www.geosense.co.uk](http://www.geosense.co.uk)



# Annex 1: Details of mounting systems

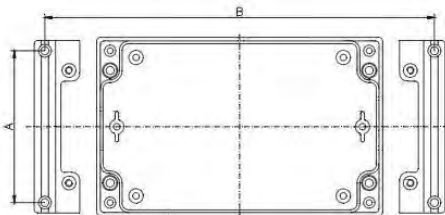
## Mounting brackets

### Metallic versions

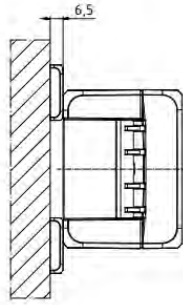
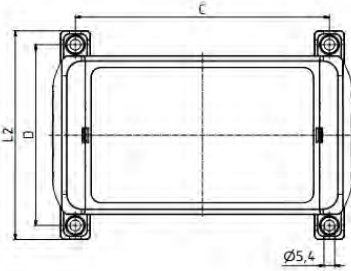
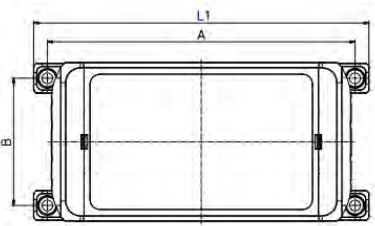


**External mounting brackets** (set = 2 pcs.)  
for mounting without opening the lid

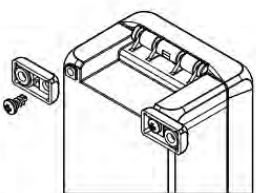
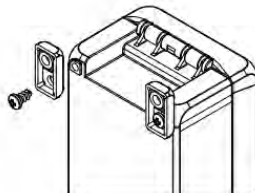
Order No.	A	B	for Type	Order No.	A	B	for Type
04.00 00 80	65	92	04.08 08 08	04.00 01 40	125	152	04.14 14 07
04.00 00 80	65	132	04.08 12 08	04.00 01 40	125	192	04.14 18 07
04.00 01 00	85	112	04.10 10 06	04.00 01 40	125	232	04.14 22 07
04.00 01 00	85	172	04.10 16 06	04.00 01 60	145	172	04.16 16 08
04.00 01 00	85	212	04.10 20 06	04.00 01 60	145	252	04.16 24 08
04.00 01 20	105	132	04.12 12 08	04.00 02 00	185	212	04.20 20 07
04.00 01 20	105	172	04.12 16 08	04.00 02 00	185	292	04.20 28 07



### Polycarbonate version



Anschraumbare / screw mounting dimensions							
Modell / model	A	B	L1	L2	D	L2	
BOCUBE B 100805	63	64	107	65	91	105	
BOCUBE B 100806	117	64	131	96	91	105	
BOCUBE B 100809	117	64	131	96	91	105	
BOCUBE B 100806	155	64	169	128	91	105	
BOCUBE B 100809	155	64	169	128	91	105	
BOCUBE B 111306	155	109	169	128	135	150	
BOCUBE B 111309	155	109	169	128	135	150	
BOCUBE B 211306	235	109	249	188	135	150	
BOCUBE B 211309	235	109	249	188	135	150	
BOCUBE B 261706	235	154	289	216	181	195	
BOCUBE B 261709	275	154	289	216	181	195	

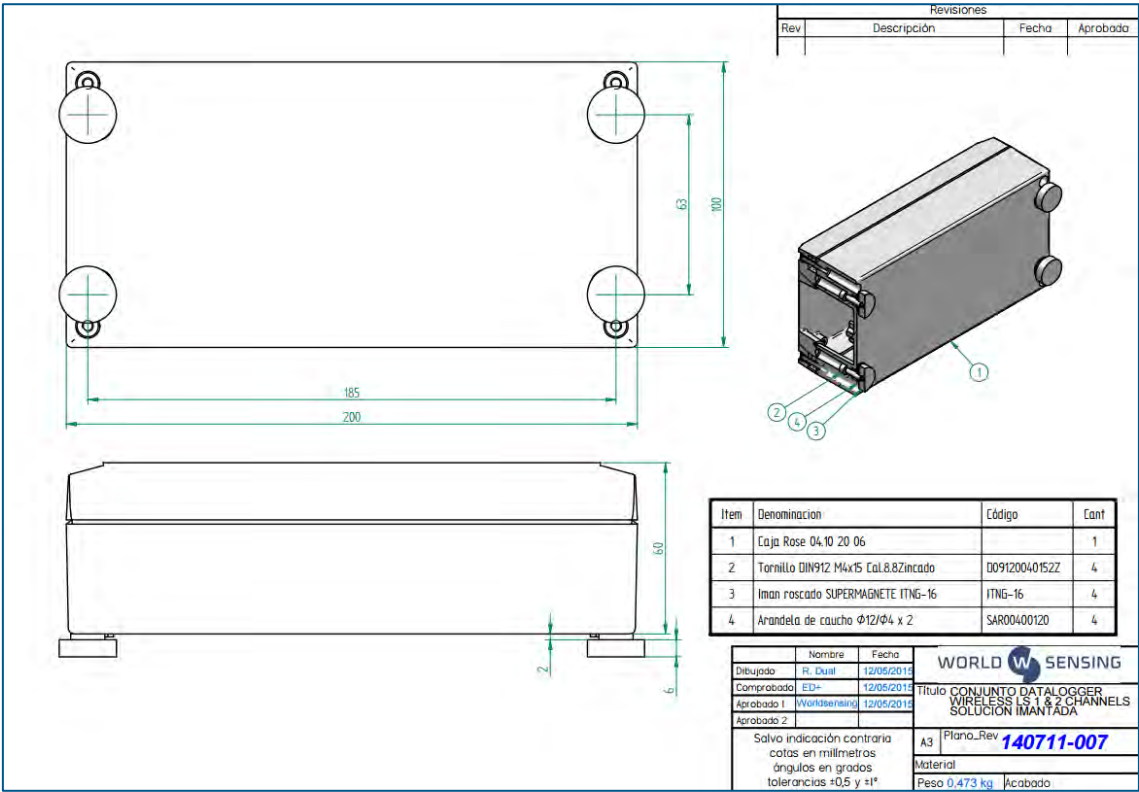


Artikel /  
Grate:  
Zeichnungs-Nr. / Drawing-No.  
2K 5390.04S.01

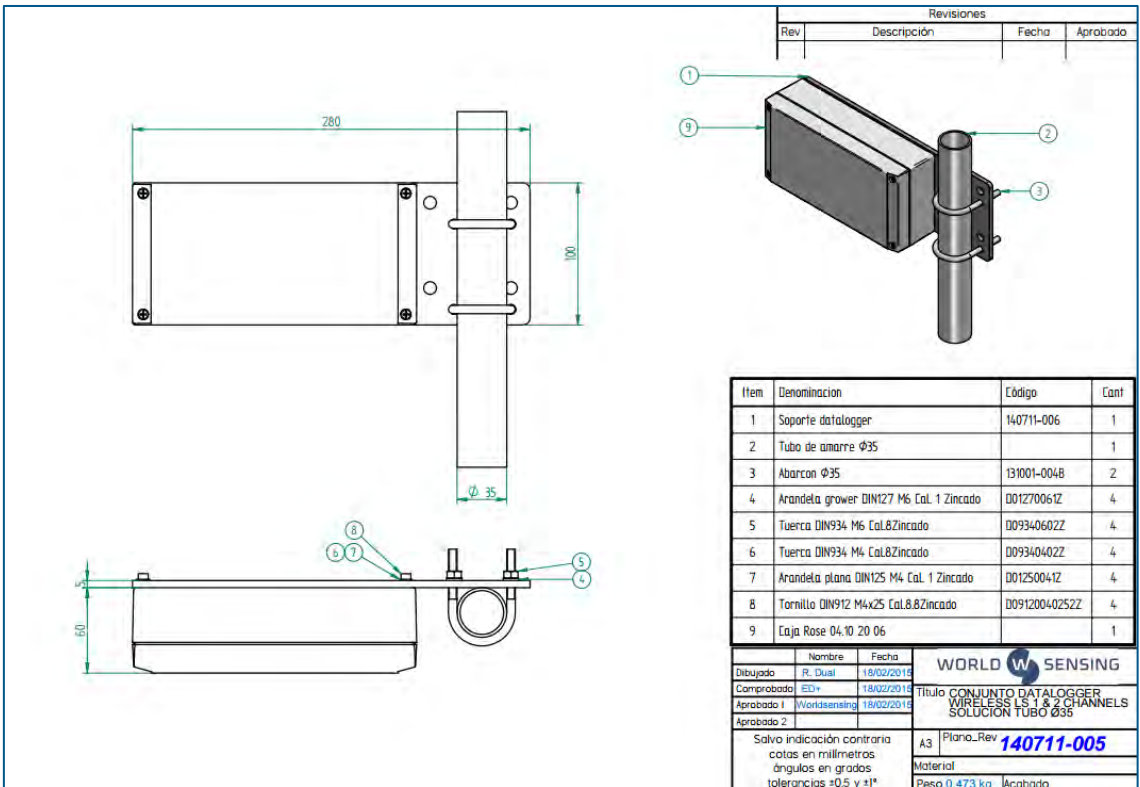
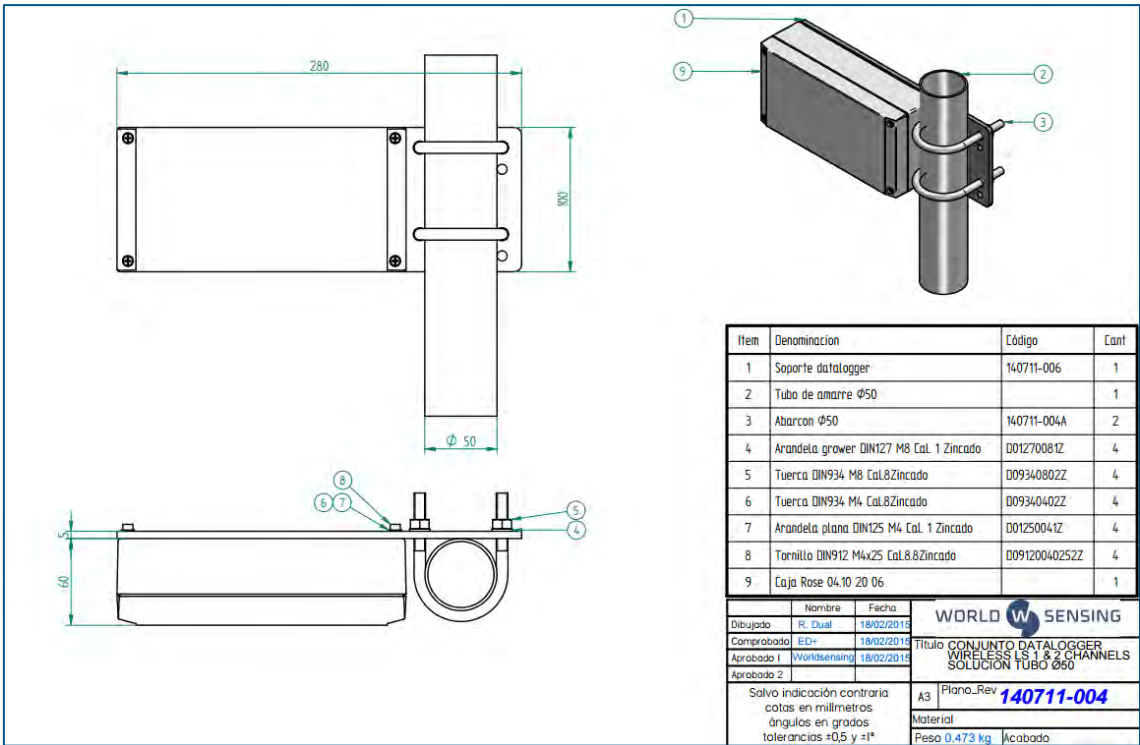
Artikel / Article:  
BOCUBE  
B WL  
Katalogz./Catalogue draw.

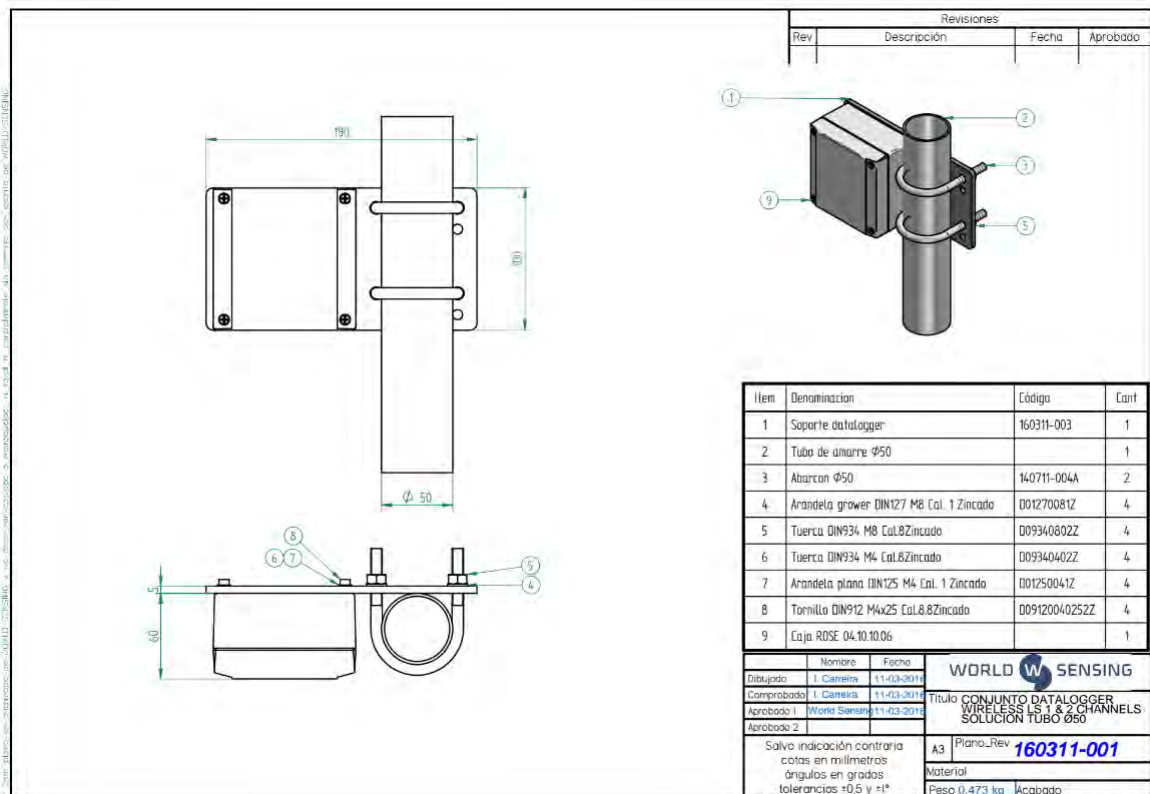
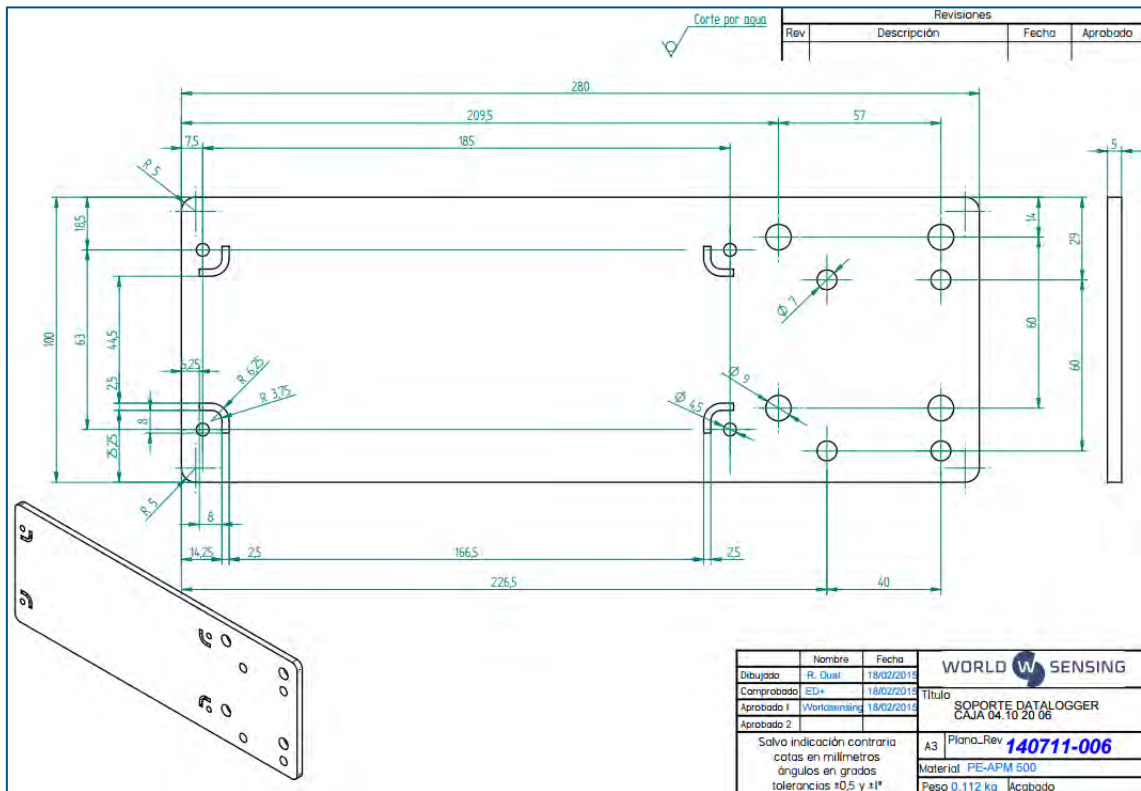
BOPLA  
B. R. 1.2012

Strong magnets

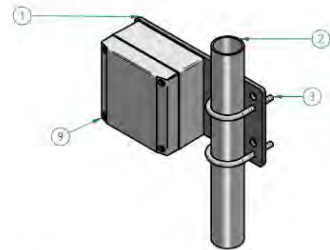
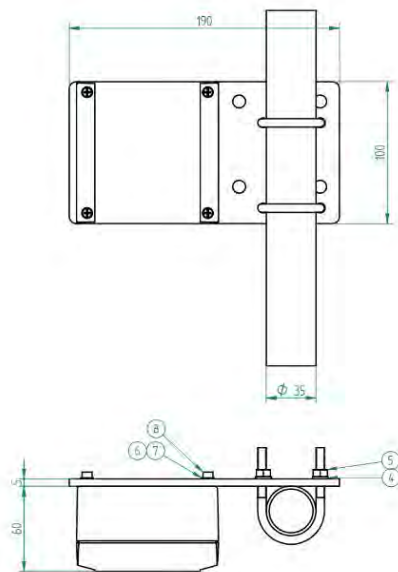


Pole mounting





3. Se debe adherir una etiqueta con el código de identificación de la pieza al soporte de montaje.



Item	Denominación	Código	Cant
1	Soporte datalogger	160311-003	1
2	Tubo de amarre Ø35		1
3	Aburton Ø35	131001-004B	2
4	Arandela grower DIN127 M6 Cal. 1 Zincado	D01270061Z	4
5	Tuerca DIN934 M6 Cal.8Zincado	D09340602Z	4
6	Tuerca DIN934 M4 Cal.8Zincado	D09340402Z	4
7	Arandela plana DIN125 M4 Cal. 1 Zincado	D01250041Z	4
8	Tornillo DIN912 M4x25 Cal.8Zincado	D09120040252Z	4
9	Caja ROSE 04.10.10.06		1

Dibujado	Nombre	Fecha	<b>WORLD SENSING</b> <b>TÍTULO CONJUNTO DATALOGGER</b> <b>WIRELESS LS 1 &amp; 2 CHANNELS</b> <b>SOLUCIÓN TUBO Ø35</b>
Dibujado	J. Camero	11-03-2016	
Comprobado	J. Camero	11-03-2016	
Aprobado 1	World Sensing	11-03-2016	
Aprobado 2			
Salvo indicación contraria cotas en milímetros ángulos en grados tolerancias ±0.5 y ±1°			A3 Plano_Rev <b>160311-002</b> Material Peso 0,473 kg Acabado

## Annex 2: Android compatibility

The Android Configuration app specifically developed to connect locally with the Wi-SOS 480, allowing configuration, data display and download. This document provides the basic information to know which Android devices are compatible with the nodes, and the USB cable that must be used for this local connection.

To download the Android Configuration App in your Android device, go the following link: <http://wsop.cat/industrial/dlog/Glog.apk> Information on how to use the application can be found in the LS-G6 user guide.

To be compatible with the Wi-SOS 480 nodes, an Android device must have the following specifications: **USB on the go (OTG) + Android at least 3.1**. From early 2013 most of the Android devices on the market fulfil these requirements. To check if your Android device includes the USB OTG feature, just search in the web “<model of the smartphone> specifications USB OTG” and ensure that the Android version is at least 3.1 (API version 12). Alternatively, you can download the following app, called USB OTG CHECKER: <http://www.pcnexus.net/2014/07/how-to-check-android-phone-tablet-for-usb-otg-support.html>.

Some Android devices may have the USB OTG feature locked. An example of unlocking process for Samsung SIII mini can be found in this tutorial: <https://www.youtube.com/watch?v=JevEyriLXZ0>.

The connection between the node and the Android device is done with “USB on the go” cable (OTG). This cable allows an Android device to act as “master”, meaning that other devices can be controlled from it. The Wi-SOS 480 nodes have a mini USB connection, while most Android devices have a micro USB connection. In order to connect the Android device to the node, a USB OTG cable from micro USB to mini USB is needed.





## Annex 3: Wi-SOS 480 water tightness

The Wi-SOS 480 family of Nodes from Geosense are rated IP67. The Nodes also pass the IP68 tests for extended immersion (1 meter for 3 days) if the installer uses extreme caution.

To ensure this condition, the user should be sure that:

- After sensor connection, the box is closed following a cross-shape order. By not following this order, the parallelism between base faces and cover may be missed, screwing may become more difficult and it can eventually generate a deformation of the screw threads or the helicoil inserts. Moreover, the toric joint (seal) would not seal properly, so the degree of protection against water intrusion (IP) would not be guaranteed.



- The box is screwed at 2 Nm, using a torque screwdriver
- The cable glands are closed using a 19 mm open spanner (holding the internal nut using a 22 mm open spanner).
- The antenna is mounted. If it is not, the antenna connector should be covered with a cap.
- The sealing ring is not manipulated, neither physically or chemically.

If any of these conditions are not given, or if one or several components (e.g. gore valve) are damaged, the IP67 and superior are not guaranteed.

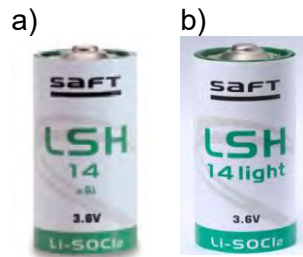
In the case that it is necessary that the Node is further sealed, due to being placed in an extreme environment or in a floodable manhole, additional sealants would be required to close the box (e.g. Sikaflex products).

*Note that box screws shouldn't be torqued more than 2.5 Nm, for all that the maximum torque that can be supported by the box screws is 3.5 Nm. If the torque is exceeded, the helicoil insert may be damaged. It is not recommended to use electric drills or electric screwdrivers.*

## Annex 4: Recommended batteries

Wi-SOS 480 Nodes can work with only one cell battery or more than one (up to four). The more batteries used, the longer the autonomy is.

The recommended batteries are LSH 14 models from Saft.



This equipment can work with just one cell of a battery specified in the following link.

([http://www.saftbatteries.com/force\\_download/LSH\\_14.pdf](http://www.saftbatteries.com/force_download/LSH_14.pdf)). More paralleled batteries increase the node autonomy

If another model of battery is used, it must meet the same specifications as the Saft batteries. Typical issues will be:

- Cell voltage: must be at least 2.7V to 5V
- Cell continuous current: Must be high current from 500 mA to 1 A

Cell voltage and continuous current change with temperature. Previous specs must be checked in the desired temperature range. Also, common batteries (alkaline) don't work in extreme temperatures.

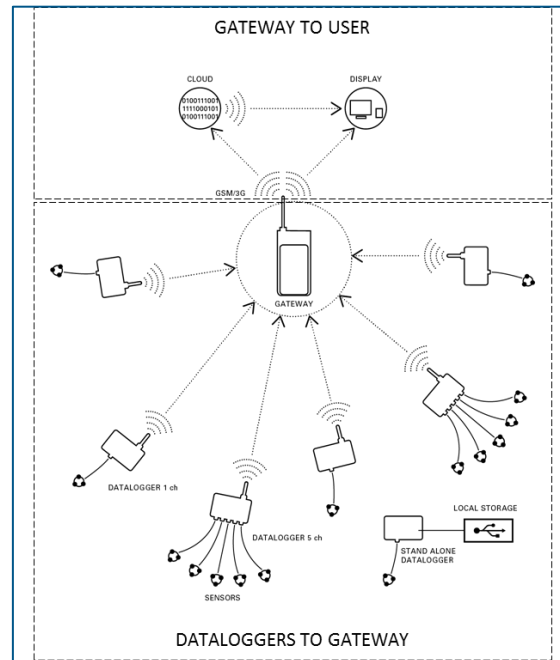
***WARNING: THERE IS RISK OF EXPLOSION IF THE BATTERIES ARE SUBSTITUTED FOR AN INCORRECT MODEL. DISPOSE OF BATTERIES IN ACCORDANCE WITH LOCAL REGULATIONS. THIS EQUIPMENT IS MEANT TO BE INSTALLED IN RESTRICTED ACCESS AREAS.***



## Annex 5: Communications security

### Long range radio communication from Nodes to the Gateway

This section explains the security of the radio communication from Nodes to the Gateway.



### Security

Each Geosense radio network uses its own identifier and password. The ID and password provide authentication and encryption to all radio communications within the network. This means that the ID and password are set on both the Gateway and the Nodes (via the USB Glog Android app). By default, the Gateway comes with a random password.

### Encryption

The radio network has a special need for secure communication, as many of its applications imply critical data of key infrastructures. This has been solved applying three encryption layers:

- Unique Network key ([EUI64](#)) at network level.
- Unique Application key ([EUI64](#)) at application level.
- Network specific key to encrypt all data using [AES](#)-128 (AES-EUI128).

### Gateway user access

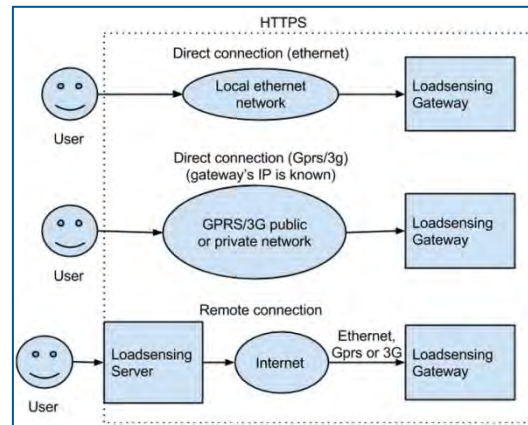
This section explains how communication between the user and the Gateway is secured.

## Remote access

This is the method used to access the Gateway over the internet or a local network. The Gateway has two interfaces integrated for remote access:

- Ethernet interface
- 3G/GPRS interface

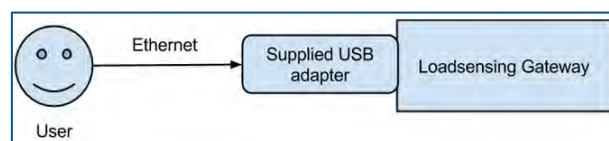
Both interfaces use HTTPS protocol for secure communication, and both interfaces use the remote access password. This password is unique and is randomly generated at production: it can be changed by the user using the gateway administration web. The different methods for remote access to the gateway are shown here:



## Local administration

The Gateway offers the possibility of direct local connection, using Gateway's internal USB port. When accessed by this method, the connection is also secured using https. However, this connection will ask for a password which is not unique (it is the same for all Gateways). This is done taking two important considerations into account:

- A direct data recovery method is needed if the remote access password is lost.
- The Gateway cannot be physically reached by anyone other than the customer.



- The radio communication from the Nodes to the Gateway is encrypted with AES.
- All remote communications that allow user's access to the Gateways are done with https protocols.

Both security methods conform to approved standards that are applied in all industries, from bank transactions through to most accessed internet services.

## Annex 6: Connecting an external modem to Wi-SOS 480

This example is using an AirLink® RV50 from Sierra, but another similar devices will work.

### Initial configuration of AirLink RV50 (via Ethernet cable)

1. Insert the SIM card following the device instructions. In our case, the Sierra AirLink RV50 has a cover with two Philips screws that gives access to the SIM Slots. The upper slot is the primary and is where SIM must be inserted. **Optional:** If you have a secondary SIM for fallback internet access, insert it on the lower slot.
2. Connect Cellular antenna.
3. Connect an Ethernet cable to your computer.
4. Connect power cable.
5. The device will give an IP address to your computer automatically. If not, or if you want to make sure that network settings are correct, follow the appendix on the last page.
6. Point your web browser to <http://192.168.13.31:9191> (AirLink RV50 factory IP)
7. Leave the administrator user name entered by default and enter the **default password: 12345** and click Login.
8. Optional: Change password. Go to Admin tab → Change Password → Enter Old password (12345) and then enter the new one.
9. Main status page will appear with basic status information. Check the **Network State field**. If it is in Network Ready state and the Active WAN IP Address is different from 0.0.0.0, then your Sierra AirLink has auto-configured from your provider and you can skip to next chapter. If not, follow next steps to configure it.

Parameter	Value
Phone Number	NA
Active WAN IP Address	0.0.0.0
Network State	SIM PIN incorrect 3 attempts left
Cell Info	CellInfo: RSSI: -125
Network Service Type	None
Signal Strength (RSSI)	-125
Channel	0
WAN/Cellular Bytes Sent	0
WAN/Cellular Bytes Rcvd	0
Persisted WAN/Cellular Bytes Sent	0
Persisted WAN/Cellular Bytes Rcvd	0
ALEOS Software Version	4.5.2
Customer Device Name	LT60940241011025
Network Operator Switching	Disabled : SIM card not ready at boot

10. Go to WAN/Cellular tab → SIM Slot 1 Configuration.

Enter your network provider APN in **User Entered APN** field.

If your SIM needs security PIN, set it via SIM PIN red button. A pop-up will appear:

Status **WAN/Cellular** LAN VPN Security Services GPS Events Reporting Serial Applications I/O Admin

Last updated time : 31/7/2016 17:16:12 Expand All Apply Refresh Cancel

**WAN/Cellular**

**SIM Slot 1 Configuration**

SIM Slot 2 Configuration

Reliable Static Route (RSR)

DMNR Configuration

[+] Network Credentials

APN in Use APN Not Found

AT User Entered APN

AT SIM PIN **SIM PIN**

[+] Advanced

AT LTE Authentication Mode NONE ▾

AT Network User ID

AT Network Password

[+] APN Backup

APN

LTE Authentication Mode NONE ▾

Network User ID

Network Password

Then Save & reboot the device (Upper left Reboot button).

**SIM PIN** Close

SIM Pin:

Enter SIM Pin:

Retype SIM Pin:

☐ Don't change  
☒ Enable  
☐ Disable

**Save Cancel**

Status: SIM PIN incorrect 3 attempts left

11. After rebooting device, access its configuration web again (<http://192.168.13.31:9191>) and then check Network State, if everything works as expected it would be "Network Ready", and an Active Wan IP Address should be present.

Status	WAN/Cellular	LAN	VPN	Security	Services	GPS	Events Reporting	Serial	Applications	I/O	Admin
Last updated time: 3/17/2016 17:33:06											
<div>Apply</div> <div>Refresh</div> <div>Cancel</div>											
Home	<div> <div>AT</div> <div>Phone Number</div> <div>NA</div> </div>										
WAN/Cellular	<div> <div>AT</div> <div>Active WAN IP Address</div> <div>10.40.246.141</div> </div>										
LAN	<div> <div>AT</div> <div>Network State</div> <div>Network Ready</div> </div>										
VPN	<div> <div>AT</div> <div>Cell Info</div> <div>CellInfo: TCH: 10688 RSSI: -102 LAC: 2114 CellID: 31868</div> </div>										
Security	<div> <div>AT</div> <div>Current Network Operator</div> <div>214-19</div> </div>										
Services	<div> <div>AT</div> <div>Radio Technology</div> <div>UMTS, Roaming</div> </div>										
	<div> <div>Network Service Type</div> <div>3G</div> </div>										
GPS	<div> <div>AT</div> <div>Signal Strength (RSSI)</div> <div>-102</div> </div>										
	<div> <div>AT</div> <div>Signal Quality (ECIO)</div> <div>-7.0</div> </div>										
Serial	<div> <div>Received Signal Code Power (RSCP)</div> <div>-109.0</div> </div>										
	<div> <div>AT</div> <div>Channel</div> <div>10688</div> </div>										
Applications	<div> <div>WAN/Cellular Bytes Sent</div> <div>3682</div> </div>										
	<div> <div>WAN/Cellular Bytes Rcvd</div> <div>6900</div> </div>										
About	<div> <div>Persisted WAN/Cellular Bytes Sent</div> <div>3352</div> </div>										
	<div> <div>Persisted WAN/Cellular Bytes Rcvd</div> <div>6760</div> </div>										
	<div> <div>ALEOS Software Version</div> <div>4.5.2</div> </div>										
	<div> <div>AT</div> <div>Customer Device Name</div> <div>LT60940241011025</div> </div>										
	<div> <div>Network Operator Switching</div> <div>OK</div> </div>										

Led indicators will help diagnosing problems. If the Gateway has internet connection, the first led (right-to-left) will be bright amber. The second led will be green if it has network signal too. The third led will indicate local network traffic.

If those first LEDS are blinking red, it means that the Gateway still doesn't have signal or internet, or this needs to be reconfigured.

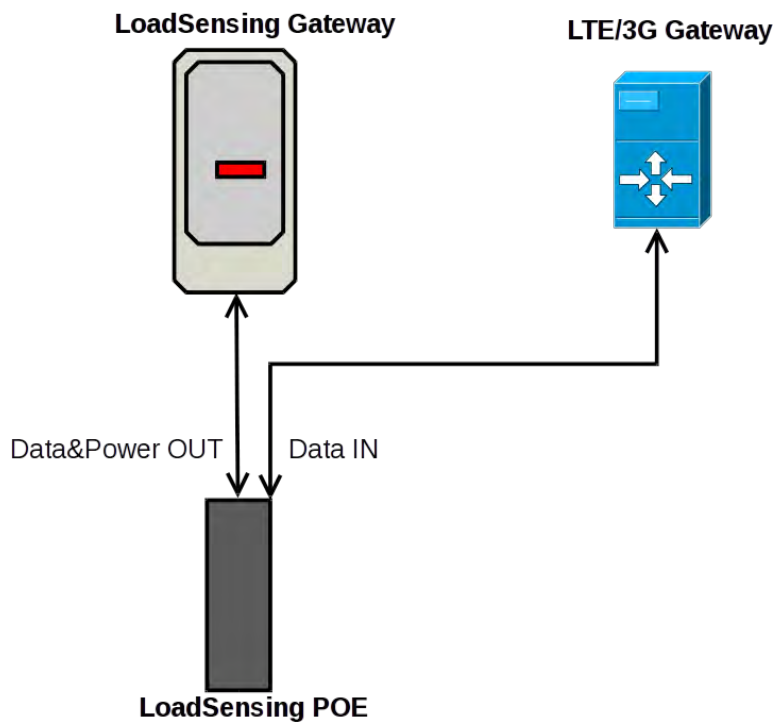


12. Finally, if the first two LEDs are fixed amber and green, check that your computer has internet access via AirLink RV50 (Open a web page, etc.). If not, repeat from step 9 and double check device settings.

If your computer now has internet access provided by LTE/3G, then we can jump to the final step.

### Final Step: Connecting the LS-G6 Gateway to AirLink RV50

To connect the LS-G6 Gateway to the Internet via your recently configured AirLink RV50, this process must be followed. Please double check connections before powering on POE adapter or devices may be damaged.



After connections are made and devices powered on, LS-G6 will reach the Internet through your AirLink RV50 and should be accessible via its Remote Access URL. Please check the LS-G6 Gateway Information Sheet for more information.

## Annex 7: Connecting a Wi-Fi module to LS-G6

This example is using a NanoStation loco M2 from Ubiquiti, however another Wireless bridge (commonly named “Access Point”) can be used if it supports Client mode (also known as Station Mode).

We will follow those steps:

- **First configuration of Wireless Bridge (via Ethernet cable).** We recommend doing this step within the Wireless Network range, but without installing the device on its final location. You'll need a computer and be able to temporarily change its IP address.
- **Wireless Bridge physical installation.** Now you can install the device (using its cable tie) to the final location, pointing to the source of Wireless Network.
- **Review LS-G6 Gateway (via Ethernet cable).** In this step you will assure that LS-G6 Gateway is expecting configuration via Ethernet and is able to connect directly to internet.

- **Interconnection between Wireless Bridge and the WI-SOS 480 Gateway**

1. Connect an Ethernet cable from the NanoStation to the POE port of the PoE Adapter. Please make doubly sure that you connect the POE port to the antenna and NOT to your computer as it could be damaged.
2. Connect another Ethernet cable from your computer to the LAN port of the PoE Adapter.
3. Your computer now needs a temporary IP address within the 192.168.1.x subnet. For example, assign 192.168.1.100 address and 255.255.255.0 netmask. Leave gateway and DNS blank. Depending on your Operating System the procedure might be different. If your computer is a laptop make sure you change the IP address for the LAN (cabled) adapter and not wireless one. Tip: Check Appendix on last page for more information
4. Direct your web browser to <http://192.168.1.20> (This is the NanoStation factory IP address)
5. Accept unsigned certificate warnings
6. Enter ubnt as both User Name and Password
7. The airOS configuration interface will appear. For security reasons, the first thing you should do is configure a new password to access the device. We recommend doing it now because the device will force you to change it later while configuring the Wireless Network
8. Go to System tab → System Accounts. Click on the key symbol to change the ubnt password. Note: For added security, we recommend changing both the username and password
9. The next step is to search for the Wireless Network and connect to it. Go to Wireless tab and make sure that Wireless Mode is set to Station. Then go to Select Button to do a Wireless Networks Survey:



### Basic Wireless Settings

Wireless Mode:

WDS (Transparent Bridge Mode): ☐ Enable

SSID:

Lock to AP:

Country Code:

IEEE 802.11 Mode:

Channel Width:

Frequency Scan List, MHz: ☐ Enable

Calculate EIRP Limit: ☒ Enable

Antenna:

Output Power:  dBm

Data Rate Module:

Max TX Rate, Mbps:  ☒ Auto

---

### Wireless Security

Security:

10.The Site Survey window will appear, listing all the Wireless Networks in your area. Then you choose your SSID (Network) and confirm it with the Select Button.

### Site Survey

Scanned Frequencies:  
 2.412GHz 2.414GHz 2.417GHz 2.419GHz 2.422GHz 2.424GHz 2.427GHz 2.429GHz 2.432GHz 2.434GHz 2.437GHz 2.439GHz 2.442GHz 2.444GHz  
 2.447GHz 2.449GHz 2.452GHz 2.454GHz 2.457GHz 2.459GHz 2.462GHz 2.464GHz 2.467GHz 2.469GHz 2.472GHz 2.474GHz

MAC Address	SSID	Device Name	Radio Mode	Encryption	Signal / Noise, dBm	Frequency, GHz / Channel
<input checked="" type="radio"/> 4C:5E:0C:71:5C:B8	Dharma	4C5E0C715CB8	802.11n	WPA2	-33 / -98	2.412 / 1
<input type="radio"/> 14:CC:20:50:E6:D4	Jazztel_08		802.11n	WPA	-64 / -98	2.412 / 1
<input type="radio"/> E8:39:DF:FC:6B:35	Jazztel_08		802.11n	WPA2	-70 / -98	2.412 / 1
<input type="radio"/> B2:46:FC:67:2A:00	MOVISTAR_2A00		802.11n	WPA2	-90 / -99	2.462 / 11

Selectable SSID's must be visible and have compatible channel bandwidth and security settings.

11.After selecting your preferred SSID (Network) the browser will return to the Wireless Settings tab.

There's one last and important thing to do: Set the Wireless Password or encryption Key! On the bottom of this page, Wireless Security will be auto-detected with selected network encryption setting. The password must be written on the textbox and saved with the Change button.

Tip: Tick "Show" to check if password is correct while you are writing.

### Wireless Security

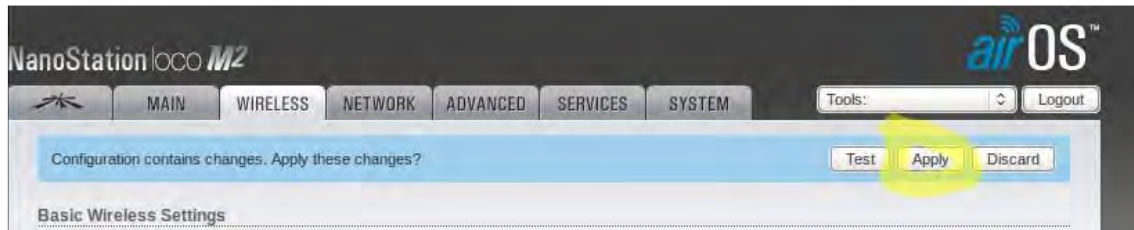
Security:

WPA Authentication:

WPA Preshared Key:  ☐ Show



12. As with every change that is made in Ubiquiti Devices, it must be Applied to take effect:



13. After several seconds, the device will reboot and connect to Wireless Network. The last step is to remove the Default IP Address and let the device ask for IP to the Wireless Network. Go to Network Tab and change Management IP Address to DHCP.

Tip: Leave DHCP Fallback Address as 192.168.1.20. In this way, if something goes wrong and the device cannot get an IP address from Wireless Network, after several minutes it will get that «rescue IP» so you can connect to it with your laptop to reconfigure it.

After changing to DHCP mode, remember to Apply settings!

Now your Wireless Bridge will be connected to your Wireless Network as if it were a Laptop, a Mobile or another device. Then it will <<convert>> this signal to Ethernet cable.

## Annex 8: Troubleshooting reference table

### Gateway

### Nodes

Fault	Possible cause	Remedy
Node not visible to gateway	Node isolated / not visible for anyone	Move location
Node not visible to Gateway. Cannot be accessed with Dlog unless switch is set to "USB".	Node battery is dead	Check battery
Node not visible to gateway	Radio configuration	Check radio configuration using DLOG. Check carefully that the radio configuration is the same on all devices.
Node not visible to Gateway	Antenna	Check connection & orientation
Node not visible to Gateway	Gateway	Check gateway is UP
Node not visible to gateway	Gateway antenna	Check connection & orientation

## Annex 9: FAQ's

- The Node appears as connected but the readings don't appear in the files.

When a Node is out of time (1970) it appears as connected but the readings don't appear in the files, nor in "Last readings". A warning message appears in the "log" tab. You should reconnect to the Node using the USB OTG cable and the DLOG app to set the date and time.

- I have done a few signal coverage tests but they don't appear on the map of the web interface.

Did you have GPS coverage? Were your android device and the Gateway connected to internet? Latitude and longitude collected by the mobile in the signal coverage test is sent to the Gateway through the internet so if your mobile or the Gateway didn't have connectivity (offline test), latitude and longitude will be only stored in the mobile, in a csv file called 'signal-coverage', and not in the Gateway.

- Is the Node protected over reverse polarity and over voltage?

Yes. The Node should not be damaged by a mis-wiring on the external cables, including input voltages of up to 20V

- Does the Node have ESD protection?

Yes. The Node should not be damaged by an Electrostatic discharge, in compliance with norm IEC 61000-4-2.

- Does the Node have surge protection?

As long as the Node has proper grounding, it should not be damaged by a short high voltage burst, such as a lightning strike at least 100m away.

Note that, while the Nodes have been engineered and built to comply with these specifications, the surge protection has not yet been through certification, so we don't have an external test report to certify compliance on this aspect.

- How should the Node be installed?

The Node should be installed with proper grounding connected to the screw outside the box in order to guarantee surge immunity, especially on installations with long cable runs.

- Is the Gateway protected over surges?

The Gateway does not ship with surge protection out of the box as the Nodes do.

However, if this kind of protection is desired, it's possible to achieve it by using external devices.

The Antenna link should be fitted with a CITEL P8AX.

The Ethernet link should be fitted with a CITEL Mj8-POE-B.

Both devices must be installed in accordance with their own specifications.

- What is the effect of strong winds (for example 80 km/h) on radio communications?

The impact of wind on radio waves is almost negligible.

- Is it possible to connect the Gateway to the Internet (through 3G) as well as to a private network through Ethernet?

No, this is not possible. The Gateway cannot have two active connectivity options at the same time. When it is using 3G, it will ignore the Ethernet and vice-versa. In the case that this would be a requirement, an external router may be used.

- Is it possible to connect a Gateway to a Virtual Private Network (VPN)?

There are different protocols used to tunnel the traffic and also different VPN types so it is not simple to introduce VPN functions into the WI-SOS 480 Gateway software. If it is necessary to connect a Gateway to a VPN, currently there are two options: use an external VPN router or contract a SIM card suitable for Private Networks from a telecommunications company.

- Is my data secure from unauthorized access?

The WI-SOS 480 G6 server is hosted inside the Gateway. The web page you see, where you download your CSVs from, is actually inside your own device, so your data never gets sent anywhere, unless you configure it otherwise (for example, using the ftp client feature).

Access to this information is protected by the Web Access password. We generate a random default password for each gateway (which is written in your Gateway Information Sheet), so no other customer has the same password.

If you want your web password to be changed from the default value, you can change it in the web interface.

When you access your information through <https://loadsensing.wocs3.com/<gwid>>, you are using the Geosense Remote Access Service. This service uses a server as a proxy to enable remote access to gateways with no public IP. The server however, is not a cloud storage service, does not store any of your information, and access still requires the web password.

- How do we deal with interferences?

As with any radio system, interference can cause difficulty in communication, leading to higher packet loss ratios. Most wireless systems (such as Wi-Fi) use the 2.4 GHz and 5 GHz bands. The sub-GHz bands are commonly less used by consumer devices, leading to less interference. The radio uses several systems to provide certain immunity to interference:

- Co-channel Gaussian minimum shift keying
- Automatic minimum spreading factor selection

## Annex 10: Modbus memory maps

### General Section

Address	Register name	Register content	Accepted Values
40001	Global Map Version	Version of the global memory map. A change in this version means that all the memory map changes.	0

### Common Section

Address	Register name	Register content	Values
40051	Common Map Version	Version of the common section memory map. A change in this version means that there are changes in the common section but not necessarily in the other sections.	0
40052	Node ID High	ID of the WI-SOS 480 Node. High and Low bytes in consecutive registers.	0 to 35535
40053	Node ID Low		
40054	Node Product Code	Product Code of the WI-SOS 480 Node	See product codes in LS - Command & Packets list V2.x document
40055	Health Received Timestamp High	Timestamp of the moment in which the last health message was received in the GW in seconds since the Unix epoch. GW time. High and Low bytes in consecutive registers.	0 to 4294967295
40056	Health Received Timestamp Low		
40057	Health Node Timestamp High	Timestamp of the last health message in seconds since the Unix epoch. Node time. High and Low bytes in consecutive registers.	0 to 4294967295
40058	Health Node Timestamp Low		

40059	Node Uptime High	Seconds from the last reboot of the node. High and Low bytes in consecutive registers.	0 to 4294967295
40060	Node Uptime Low		
40061	Node Battery Volts	Voltage of the battery in mV.	0 to 35535
40062	Node Temperature	Temperature in the node in °C	0 to 255
40063	Node Version Major	Node FW Version Major	0 to 255
40064	Node Version Minor	Node FW Version Minor	0 to 255

## Node Section

All the Nodes have a common part in the Node section:

Address	Register name	Register content	Values
40101	Node Section Map ID	ID of the Node Section memory map. This defines the contents of the Node section from the register 30103 onwards.	0 - VW 1 - VLT 2 - DIG-GSI-Sisgeo
40102	Node Map Version	Version of the node section memory map. A change in this version means that there are changes in the node section but not necessarily in the other sections.	0 to 35535

### LS-G6-VW

Address	Register name	Register content	Values
---------	---------------	------------------	--------

40101	Node Section Map ID	ID of the Node Section memory map. This defines the contents of the Node section from the register 30103 onwards.	0 - VW
40102	Node Map Version	Version of the node section memory map. A change in this version means that there are changes in the node section but not necessarily in the other sections.	0
40103	Data Received Timestamp High	Timestamp of the moment in which the last data message was received in the GW in seconds since the Unix epoch. GW time. High and Low bytes in consecutive registers.	0 to 4294967295
40104	Data Received Timestamp Low		
40105	Data Node Timestamp High	Timestamp of the last data message in seconds since the Unix epoch. Node time. High and Low bytes in consecutive registers.	0 to 4294967295
40106	Data Node Timestamp Low		
40107	Pressure	Pressure read by the node in hPa*10.	0 to 35535
40108	Channel 0 Presence	Shows if the channel 0 registers have valid data.	0: Channel not present 1: Channel present
40109	Channel 0 Frequency High	Frequency read on the VW in the Channel 0 in MHz High and Low bytes in consecutive registers. 0 if the Channel Presence is 0.	0 to 7000000
40110	Channel 0 Frequency Low		
40111	Channel 0 Thermistor High	Thermistor data read on the VW in the Channel 0 in mOhm. High and Low bytes in consecutive registers. 0 if the Channel Presence is 0.	0 to 4294967295
40112	Channel 0 Thermistor Low		
40113	Channel 1 Presence	Shows if the channel 1 registers have valid data.	0: Channel not present

			1: Channel present
40114	Channel 1 Frequency High	Frequency read on the VW in the Channel 1 in MHz High and Low bytes in consecutive registers. 0 if the Channel Presence is 0.	0 to 7000000
40115	Channel 1 Frequency Low		
40116	Channel 1 Thermistor High	Thermistor data read on the VW in the Channel 1 in mOhm. High and Low bytes in consecutive registers. 0 if the Channel Presence is 0.	0 to 4294967295
40117	Channel 1 Thermistor Low		
40118	Channel 2 Presence	Shows if the channel 2 registers have valid data.	0: Channel not present  1: Channel present
40119	Channel 2 Frequency High	Frequency read on the VW in the Channel 2 in MHz High and Low bytes in consecutive registers. 0 if the Channel Presence is 0.	0 to 7000000
40120	Channel 2 Frequency Low		
40121	Channel 2 Thermistor High	Thermistor data read on the VW in the Channel 2 in mOhm. High and Low bytes in consecutive registers. 0 if the Channel Presence is 0.	0 to 4294967295
40122	Channel 2 Thermistor Low		
40123	Channel 3 Presence	Shows if the channel 3 registers have valid data.	0: Channel not present  1: Channel present
40124	Channel 3 Frequency High		0 to 7000000



40125	Channel 3 Frequency Low	Frequency read on the VW in the Channel 3 in MHz High and Low bytes in consecutive registers. 0 if the Channel Presence is 0.	
40126	Channel 3 Thermistor High	Thermistor data read on the VW in the Channel 3 in mOhm. High and Low bytes in consecutive registers. 0 if the Channel Presence is 0.	0 to 4294967295
40127	Channel 3 Thermistor Low		

#### LS-G6-ANALOG

Address	Register name	Register content	Values
40101	Node Section Map ID	ID of the Node Section memory map. This defines the contents of the Node section from the register 30103 onwards.	1 - VLT
40102	Node Map Version	Version of the node section memory map. A change in this version means that there are changes in the node section but not necessarily in the other sections.	0
40103	Data Received Timestamp High	Timestamp of the moment in which the last data message was received in the GW in seconds since the Unix epoch. GW time. High and Low bytes in consecutive registers.	0 to 4294967295
40104	Data Received Timestamp Low		
40105	Data Node Timestamp High	Timestamp of the last data message in seconds since the Unix epoch. Node time. High and Low bytes in consecutive registers.	0 to 4294967295
40106	Data Node Timestamp Low		
40107	Channel 0 Presence	Shows if the channel 0 registers have valid data.	0: Channel not present  1: Channel present

40108	Channel 0 Input Type	Type of sensor connected to the channel 0.	See Input Type Codification Values table
40109	Channel 0 Data High	Data read on the node in the Channel 0. Units depend on the Input type. High and Low bytes in consecutive registers. 0 if the Channel Presence is 0.	0 to 4294967295
40110	Channel 0 Data Low		
40111	Channel 1 Presence	Shows if the channel 1 registers have valid data.	0: Channel not present  1: Channel present
40112	Channel 1 Input Type	Type of sensor connected to the channel 1.	See Input Type Codification Values table
40113	Channel 1 Data High	Data read on the node in the Channel 1. Units depend on the Input type. High and Low bytes in consecutive registers. 0 if the Channel Presence is 0.	0 to 4294967295
40114	Channel 1 Data Low		
40115	Channel 2 Presence	Shows if the channel 2 registers have valid data.	0: Channel not present  1: Channel present
40116	Channel 2 Input Type	Type of sensor connected to the channel 2.	See Input Type Codification Values table
40117	Channel 2 Data High	Data read on the node in the Channel 2. Units depend on the Input type. High and Low bytes in consecutive registers. 0 if the Channel Presence is 0.	0 to 4294967295
40118	Channel 2 Data Low		
40119	Channel 3 Presence	Shows if the channel 3 registers have valid data.	0: Channel not present

			1: Channel present
40120	Channel 3 Input Type	Type of sensor connected to the channel 3.	See Input Type Codification Values table
40121	Channel 3 Data High	Data read on the node in the Channel 3. Units depend on the Input type. High and Low bytes in consecutive registers. 0 if the Channel Presence is 0.	0 to 4294967295
40122	Channel 3 Data Low		

#### LS-G6-DIG (Geosense/RST-Sisgeo)

Address	Register name	Register content	Values
40101	Node Section Map ID	ID of the Node Section memory map. This defines the contents of the Node section from the register 30103 onwards.	2 - DIG-GSI-Sisgeo
40102	Node Map Version	Version of the node section memory map. A change in this version means that there are changes in the node section but not necessarily in the other sections.	0
40103	Data Received Timestamp High	Timestamp of the moment in which the last data message was received in the GW in seconds since the Unix epoch. GW time. High and Low bytes in consecutive registers.	0 to 4294967295
40104	Data Received Timestamp Low		
40105	Data Node Timestamp High	Timestamp of the last data message in seconds since the Unix epoch. Node time. High and Low bytes in consecutive registers.	0 to 4294967295
40106	Data Node Timestamp Low		
40107	Number of Channels	Number of channels present in the data.	0 to 50
40108	Reserved		0

40109		0
40110	First register of the channels data. See below for more information.	

A GSI node can have from 0 to 50 sensors connected. They are numbered from channel 0 to channel 49.

The following table has a description of the memory map for one channel. To calculate the address of the first register of a given channel, simply multiply the channel number (N) per 10 and add the base address 30110:

$$\text{Channel N address} = 30110 + (10 * N)$$

Address	Register name	Register content	Values
40110 + (10 * N)	ChN Number Axis	Number of axis of the channel. Sensors can have one or two axis. If this value is 0 means that no data was received of this channel.	0, 1, 2
40110 + (10 * N) + 1	ChN Temperature	Temperature read on the Channel N. Codified in two's complement. Value in tenths of °C.	+/-1000 [°C*10]  -32768 (0x8000): Invalid reading (sensor error)  -32767 (0x8001): No data received from this channel (communication error)
40110 + (10 * N) + 2	Ch N Axis 1 Reading High	Inclination read from the Axis 1 sensor of the channel. Codified in two's complement. Value in °/10000.	+/-250000 [°*10000]  -2147483648 (0x80000000): Invalid reading (sensor error)
40110 + (10 * N) + 3	Ch N Axis 1 Reading Low		-2147483647 (0x80000001): No data received from this channel (communication error)

40110 + (10 * N) + 4	Ch N Axis 2 Reading High	Inclination read from the Axis 1 sensor of the channel. Codified in two's complement. Value in °/ 10000.	+/-250000 [°*10000]
40110 + (10 * N) + 5	Ch N Axis 2 Reading Low		-2147483648 (0x80000000): Invalid reading (sensor error)  -2147483647 (0x80000001): No data received from this channel (communication error)
40110 + (10 * N) + 6	Reserved		0
40110 + (10 * N) + 7			0
40110 + (10 * N) + 8			0
40110 + (10 * N) + 9			0



Geosense Ltd

Nova House . Rougham Industrial Estate . Rougham . Bury St Edmunds . Suffolk . IP30 9ND . England .

Tel: +44 (0) 1359 270457 . Fax: +44 (0) 1359 272860 . email: [info@geosense.co.uk](mailto:info@geosense.co.uk) . [www.geosense.co.uk](http://www.geosense.co.uk)