PYRUS / SYRUS- 4T

Fire and Security Alarm transmitters series

with built in IOT technology.



Version 2.10 (25/10/2021)

a..

NUVATHINGS

product

INDEX

INTRODUCTION 3
WARRANTY 3
PRECAUTIONS 3
COMMUNICATIONS 3
MODELS 3
PYRUS TL/TLE 4
REGULATIONS 5
POWER SUPPLY CONSIDERATIONS 5
FCC INFORMATION 5
EN50136 ATS RATING 6
FEATURES 7
TECHNICAL FEATURES 8
INSTALLATION 9
INSTALLATION CONDITIONS 9
CIRCUIT CONTENTS 9
DEVICE ASSEMBLY 9
PCB WIRING DIAGRAM 11
BOX INTERNAL WIRING 13
INPUTS AND OUTPUTS CONNECTIONS 14
ANALOG SENSORS 14
DEVICE OUTPUTS 16
GENERAL WORKING MODES. 18
STATUS LEDS 18
CONTROL PANEL SERIAL INTERFACE 18
LORA WIRELESS COMMUNICATION 21
DOWNLOAD 22
NUVAEXPRESS 22
VIRTUAL COMPORT DOWNLOAD WITH ASSOCIATED PANEL 24
REPORTING FUNCTIONS 25
COMMUNICATIONS TO CENTRAL STATION SCHEMA 25
SIMS VPN 26
DEVICE REPORTS OPTIONS 26
SUBSCRIBER CODE 26
OPTIONS 26
DVR PICTURE BACKUP 26
NON-STANDARD CONTACT ID CODES 26
PROGRAMMING 27
CONFIGURATION OVER VIEW 27
INPUT CHANNELS CONFIGURATION 28
OUTPUTS CONFIGURATION 28

Introduction

Thank you for purchasing our CIRRUS-4T all purpose communicator and for trusting our company. This device fulfils all international IEC regulations for the functions it has been made for, manufactured under ISO9001 and ISO67 certification schemes to bring you and your customers the state of the art device that will fill up all your communication needs. This manual contains all the information necessary for CIRRUS setup.

Warranty

The device has a warranty of 24 months, from purchase date. The warranty covers material defects and its replacement, not covering related transport and travel expenses.
Warranty exclusions: defects or damages that result from abuse, misuse or from technical service other than service authorized centers. Improper use and normal wear and tear are excluded from the warranty.
Technical features of our devices are subject to change (due to the improvement) without any previous advice.
NuvaSafe is not responsible for defects and damages that result from misuse or improper installation of the devices.

Precautions

- Before powering the device:
  - Make sure that SIM card is placed **correctly, simcard format is MICRO-SIM**
  - Make sure not to invert **polarity**.
- Once the device is connected:
  - Don't remove SIM card once the device is powered.
  - Don't remove antennas during device operation.

Communications

The device is capable of communicate to cloud using the following channels.

1- WIFI.
2- GPRS / NB-IOT / LTE-CAT-M1
3- LORA / LORAWAN.
4 - ETHERNET (on demand)

The device also has the following communication channels.

1 – TTL / RS485 (pyrus model)
2 - RS232 by means of plugin board option.
2 – Bluetooth 5.0 (optional on demand)

Models

The device is offered with different options and assemblies, not all models are currently in stock, so some of them are to be produced depending on purchase quantity.

Communications/ Format	**BARE Circuit (to mount inside control panel external MMCX magnetic atennas provided)**	**Plastic Housing (to fix outside panel with external power provided from it, internal antennas and internal 7.4V 1.4Ah LiPo Batt)**
GPRS + LORA	☑EN50136 CIRRUS-GL	-
NB-IOT + LTE-CAT-M1 + GPRS + LORA	CIRRUS-TL	PYRUS-TL
GPRS + WIFI + LORA	☑EN50136 CIRRUS-GLW	PYRUS-GLW
NB-IOT + LTE-CAT-M1 + ETH + LORA	CIRRUS-TLE	PYRUS-TLE

PYRUS TL/TLE

Provided in small plastic housing, internal antennas compliant with DP4 and grade 3, 7.4V LIPO 1.2Ah internal battery, connections with grade 3 control panel must me made according to ATS rating.

EN50131-6 compliant power supply at grade 3.

Plastic Box.

IP65 / UL94-V0 plastic box with wall mounting flanges, electronic wall and box tamper.

Internal battery pack.

Internal CELL / LORA and WIFI antennas.



Regulations

The device is designed to fulfil all security and health requirements in accordance with following European Directives:

2004/108/EC	General electromagnetic compatibility Directive
2006/95/EC	Low voltage directive.
2014/53/EU	RED directive.
EN 60950-1	Information technology equipment - Electrical Safety
TBR21	PSTN Access (Only impedance clauses, as long as device cannot seize PSTN to make calls)
EN 50131-1 Grade 3	General Requirements of intrusion alarm systems.
EN 50131-6	Requirements for power supplies in security systems.
EN 301489-1	Electromagnetic Compatibility (EMC) standard for radio equipment and services.
EN 300 220-1	Short Range devices (SRD) operating in the frequency range from 25 to 1000 MHz.
EN 50136-2	Requirements for supervised premises transceivers
EN-54-21	Requirements for Fire alarm and failure transmitters.

This statement will not be valid in case of device modification without our consent.

The device is designed for residential, commercial and light industry use. The equipment has been designed to agree the Environment class II of the EN-50131 rules.

CIRRUS is compliant to Grade 2 and Grade 3 where single and dual path is applicable.

⚠ Power supply considerations.

- Power supply is intended for models EBF-CIRRUS series which have housing box and internal power supply + battery.
- Designed to fulfill the EN50131-6 at grade 2/3.
- Must be connected to mains 230V (-15+10%) VAC 50Hz, double insulation, Class II no ground terminal.
- The use of a readily accessible disconnect device shall be incorporated external of the equipment. Disconnect device must have a distance of at least 3mm between contacts.
- Battery check must be carried out every 2 years, battery low voltage detection is under 6.8V for Lipo model, battery switch disconnect activates under 6.0V.
- Emptied batteries must be disposed into a recycle point, **never throw batteries to the garbage**
- To comply with EN50131 (Grade 2) a 1.3Ah lead battery must be used and installed properly in the battery socket.
- Battery must be fixed inside the box, with the use of the provided flanges.

⚠ ¡¡CAUTION!!
RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS

FCC Information

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference.
(2) this device must accept any interference received, including interference that may cause undesired operation.
Changes or modifications made by the user and not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
- Reorient or relocate the antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Note: The CIRRUS Series wireless system is a two-way supervised wireless design. It is compliant with FCC rules as they pertain to 900 MHz Spread Spectrum devices.

EN50136 ATS rating

CIRRUS ATS rating is only valid when used with compliant grade1, grade 2 or grade 3 control panel.

Device is a Y alarm transmitter system, intended to be assembled inside control panel housing.

The method for sending the control panel's events to the Central station is :

- Store and Forward for Contact ID events (captured from phone line or RS485/RS232).

- Pass through for SIA events, (captured form phone Line or Serial or RS232 in case of GALAXY control panels)

Depending on configuration between CIRRUS and control panel, the following SPT/DPT ratings can be achieved.

DP4

CIRRUS-GLW can have a rating of DP4 where the primary is LAN (WIFI or ETH) and secondary is CELL, LORA is a third path in this case, consider LORA dutty cycle transmission must be limited in order to meet the RED / FCC regulations.

For FCC markets on air transmission time for LORA must be restricted to a maximum of 400mS, so Spread factor 9 is the maximum permitted to accomplish FCC rules.

Primary **D4, M4, T4, A4, S2, I3**

Secondary **D4, M4, T4, A4, S2, I3**

In order to achieve this rating, following configuration must be done:

- Configure the control panel to detect PSTN failure and to activate a PGM in this case within 180 seconds of line cut
- This PGM must be wired to a CIRRUS input and transmit an alarm or failure signal.
    - If your control panel cannot do this feature, use DP3 rating instead.
- Configure polling cadence time down to 1 minute; polling timeout at ARC would be in that case 180 seconds.

LORA transmission minimum transmission cadence is 3 minutes, in order to meet RED regulations.

DP3

CIRRUS-GL / CIRRUS-TL can have a rating of DP3 where the primary is GPRS and secondary is LORA, , consider LORA dutty cycle transmission must be limited in order to meet the RED / FCC regulations.

For FCC markets on air transmission time for LORA must be restricted to a maximun of 400mS, so Spread factor 9 is the maximum permitted to accomplish FCC rules.

Primary **D3, M3, T4, A4, S2, I3**.

Secondary **D3, M3, T4, A4, S2, I3**.

In order to achieve this rating, following configuration must be done:

- Configure the control panel to detect PSTN failure and to activate a PGM in this case within 180 seconds of line cut
- This PGM must be wired to a CIRRUS input and transmit an alarm or failure signal.
- Configure polling cadence time down to 3 minutes; polling timeout at ARC would be in that case 9 seconds.

SP4

CIRRUS-GL / CIRRUS-TL have to work as SP4 when secondary channel LORA is not linked with another device.

Primary **D3, M3, T4, A4, S2, I3**.

- Configure the control panel to detect PSTN failure and to activate a PGM in this case within 180 seconds of line cut
- This PGM must be wired to a CIRRUS input and transmit an alarm or failure signal.

Configure polling cadence time down to 3 minutes; polling timeout at ARC would be in that case 9 seconds.

MANDATORY INTERFACE WITH CONTROL PANEL

In order to meet DPT4 EN50136-2 rating, the following interfaces and configuration must be meet:

- Connect a PGM output of control panel signaling alarms and tampers to a input of CIRRUS circuit which is to be configured as NA-EOL, it will trigger alarm in case of main control panel alarm.
- Connect a PGM output fo control panel signaling control panel failures to an input of CIRRUS circuito which si to be configured as NA-EOL, int will trigger a failure alarm I such a case.
- Connect O2 of CIRRUS to an input of control panel, this way the channel's path failures of the alarm transmissions system, will be signaled to an input of control panel in order to trigger a mandatory indication on the keypad.
- Configure the control panel to transmit a periodic test at least at 4 hours cadence. The lack of this test at ARC would signal the PSTN interface failure.

Features

- Alarm transmitter CELL/WIFI/ETH/LORA communicator to cloud.
  - PSTN interface simulator for Control panels.
  - RS485 / RS232 interface, with different protocols supported, SIA and Fire Control panels.
  - EN50131 grade 2-3-4 and EN50136 SPT5 / DPT4.
  - EN-54-21.
  - LORA-MESH network between devices in ISM bands (868 / 915 / 433 MHz)
  - LORAWAN connectivity.
  - Low power WIFI / ETH connectivity.
- Secure cryptographic engine,
  - Dynamic Diffie-Hellman key interchange.
  - ECDSA message signature.
  - TLS 1.2 asymmetric communication on download communications.
- 3 input channels in PCB (Up to 6 doubled input channels)
  - Configurable as: NO, NC, EOL or doubled
  - Possibility of sensitivity adjustment (100mS and 1 Second resolution)
  - 24 hours/ Fire / gas / holdup / Entry-Exit options
  - 8 partitions.
  - up to 64 logical internal zones (IEE 802.15.4 radio sensors).
- Bluetooth 5.0 or Zigbee IEE 802.15.4 radio, option.
- Analogue sensors data-logger.
  - Temperature, Humidity, pressure probes, current transformers for electrical consumption measurements.
  - Measure of triphasic and monofasic MODBUS RTU mains counters and analyzers.
  - Integration with any MODBUS – RTU data source.
- 2 open collector output (200 mA maximum)
  - Connects to ground when activated.
  - Assigned to zones or reserved for home automation functions
  - Remote control from cloud.
  - Option for external MODBUS ouputs modules.(contact Nuvathings for these possibilities)
- DVR snapshot backup transmitter.
- Programming from cloud by means of web server interface.
- Universal Modem / Virtual Comport, simulator for many control panels, creating a virtual comport at GPRS, WIFI, ETH and even LORA-MESH channels
- 126976 internal event long, with date & time stamp.
  - Registers all signal pollings carried out from device.
  - Capability to register analogue sensors data.
  - Event and programming data retention: 40 years.
- Central station integration
  - Integration of Cloud with most important CRM for Central station automation software, by means of NUVA-CS application.
  - Captures signals of associated control panel, Contact ID / SIA-DC03 using PSTN simluator or SIA-DC-03 vía RS485/RS232
  - 8 subscriber codes.

Technical features

Environmental class EN50131 ..... class II
Environmental EN54-21 ..... class: 3K5 EN 60721-3-3
Operating temperature ..... from -10 to +50 C°
Working humidity ..... 0...95% no condensation
Main board power supply ..... 5...30VDC – 300mA fuse.

Circuit must be powered from a SELV circuit.

Average consumption @ 24V

PCB ..... 3 mA
CELL ..... 5 mA
WIFI 10mA
ETHERNET ..... 15 mA
LORA module ..... 3 mA
During CELL transmission 100mA

Zone EOL

Normal ..... 2K2 Ω
doubled ..... 4K7 Ω
Failure ..... 820 Ω

Outputs (Open collector)

O1 ..... Negative / 200mA
O2 ..... Negative / 200mA

GPRS / LORA Antenna

Gain 2.15dBi
Frequency bands ..... 850/900/1800/1900 Mhz

Dimensions

Length 120mm
Width ..... 75 mm
Depth ..... 45 mm.
Weight (aprox.) ..... 200 g.

LORA frecuencies

Europe 869.525MHz
Americas 919.5MHz

WIFI

Wi-Fi	Standards	FCC/CE/TELEC/SRRC
	Protocols	802.11 b/g/n/e/i
	Frequency Range	2.4 G ~ 2.5 G (2400M ~ 2483.5M)
	Tx Power	802.11 b: +20 dBm
		802.11 g: +17 dBm
		802.11 n: +14 dBm
	Rx Sensitivity	802.11 b: -91 dbm (11 Mbps)
		802.11 g: -75 dbm (54 Mbps)
		802.11 n: -72 dbm (MCS7)
	Antenna	PCB Trace, External, IPEX Connector, Ceramic Chip

Installation

Installation conditions

NuvaSafe certificate their products products under following conditions:

USB connection is not to be keep continuous, only for download and configuration operations.

Compliance with the rules is certified using shielded wire in all of device inputs / outputs (zones, outputs…).

⚠ The interconnections between devices must be made using self-extinguishing cables.

- Attention: This product is only suitable for mounting on concrete or other non-combustible surface.
- The wiring and installation of this device must be carried out according to corresponding national rules

Circuit contents

Content of the CIRRUS-GL package (certified series)

- Antenna GSM 1 UNIT
- LORA antenna , 1 unit
- Resistors 6 UNITS (3 x 2k2 + 3 x 4k7).
- Through hole Sticks 4 UNITS.
- I/O Wires with connectors.
- CIRRUS board 1 UNIT.

CONTENT OF THE PYRUS-TL PACKAGE

- PYRUS Housing.
- I/O Wires with connectors.
- Internal antennas.
- CIRRUS-V21 board 1 UNIT RS485 BASE.
- OPTIONAL 7V2 / 1.2AH LIPO BATTERY PACK.
- WALL FIXING SCREEWS.

Device assembly

Choose a place for module assembly which should be accessible for following resources: Power supply, ground connection and telephone line. When installed inside the control panel enclosure, use all fixing screws provided with device.

Device Placing

Before installing CIRRUS look for a place with the best signal strength, taking into consideration that insufficient level (less than 30%) may cause communication failures.

CIRRUS Y type

- Mark CIRRUS outlines inside control panel enclosure and make 5mm holes.
- Insert 4 sticks in corresponding holes for circuit fastening.
- Place the circuit in the correct position pressing it lightly.
- Insert the SIM card into the correct position.
- Make necessary connections.

PYRUS X type

- Place the plastic casing at convenient height and mark assembly holes on the wall.
- Before fixing the equipment, make the cables go through accesses of the box. The product also marked the accesses weaknesses.
- The equipment must be securely fastened to a vertical, solid and smooth surface which forms part of the building structure.

- Secure firm fixation to the case for all eternal cables (to avoid accidental disconnections which could cause short circuits).
- Insert the SIM card into the correct position.
- Make necessary connections and secure the battery.
- Fix the case firmly to the wall.
- tamper comes already mounted from factory.

Note: Set contains VPN SIMCARD, in case you don't have requested it, in that case use MICRO-SIM format.

Pre-requisites

For installations using IP (WIFI/ETH) or GPRS you must ensure you have the following:

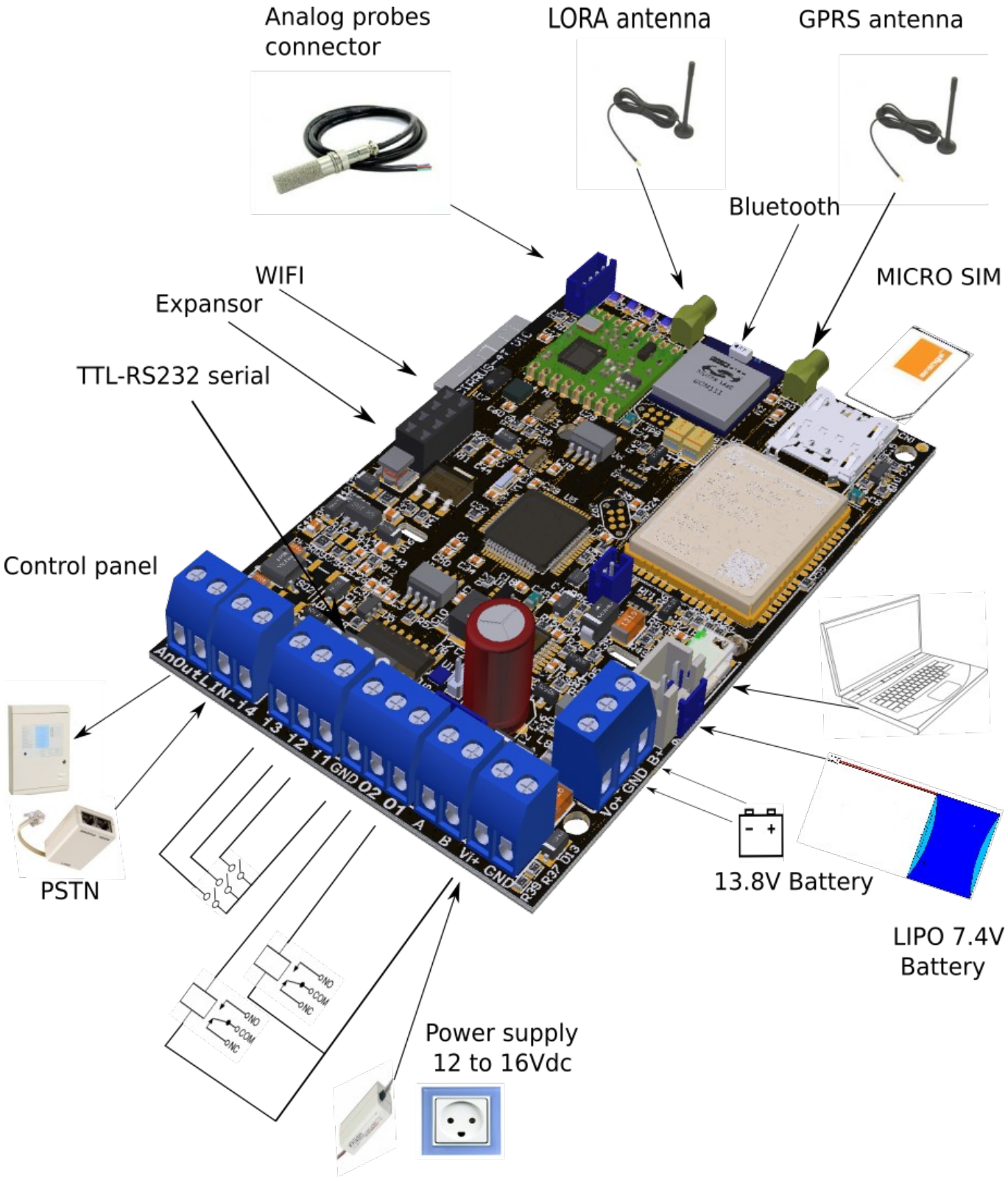
- Confirmation that the Monitoring Center is set up and ready for the account number or name to be used for this equipment.
- SSID and WIFI password configured in the device (using Nuvaexpress soft tool through USB).
- A SIM card enabled for CELL (recommend to unlock PIN code).
- The CELL Access Point Name (APN) of the SIM card provider. Some networks also require a User Name and Password which can also be obtained from the SIM card provider (GPRS only).

Circuit connections

Before powering the device make sure that everything is connected correctly, and make sure that there isn't any short circuit in order to avoid possible failures.

Connection	Description
LIN-i4	For PSTN line connection.
ANOUT	PSTN simulation output.
+B	Battery positive terminal, different options are suitable, from 7.2 LiPo pack till 13.8 Lead acid.
+Vi	Power supply input, 9…35 VDC 300 mA. May be powered directly from external panel.
GND	Power supply and battery negative terminals.
+Vo	Power supply output, can power external devices meeting EN50131-6 at grade 3 50mA max!
USB	For local communication with PC using micro USB cable..
A,B	RS485 terminals. Or bus keypad.
I1,i2,i3	EOL input zone (resistor 2K2), detects when the loop opens or closes in relation to ground, may be connected to any output Push-Pull or Open Drain, even resistive / analog data can be measured.
O1..O2	Open drain outputs, when active may reach up to 200 mA, and can be activated in case of alarm in the inputs channels, programmable events or scheduled calendar.

PCB WIRING DIAGRAM

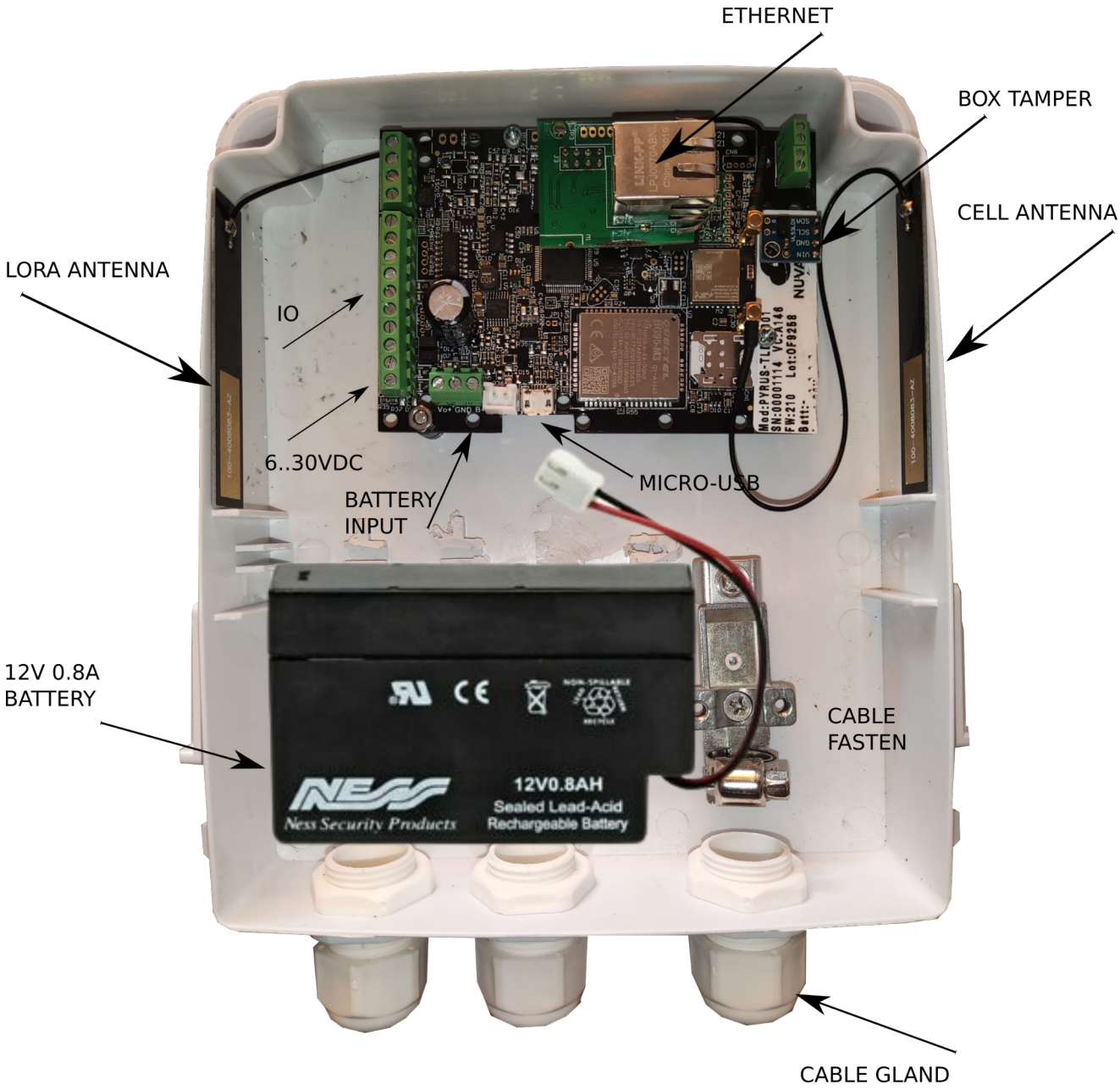


Note:

PYRUS models have battery backup function, also terminal Vo provides up to 50mA backup current for peripherals at grade 3.

- **CELL antenna** should be connected to the GSM module connector of CIRRUS.
- **LORA antenna**, must be connected to the LORA module connector of CIRRUS.
- **Land line input (PSTN)**, to be connected both of the cables to terminals LIN of CIRRUS board (**IMPORTANT: don't connect PSTN cables to terminal LOUT**).
- **Power supply unit input** , positive on Vi+ and negative on GND terminals.
- **Battery Input B+:GND:** Connect to a Lead 13.8V battery
- **Associated control panel:** , connect output **LOUT** of the circuit to phone line input (**LINE IN**) of the control panel., or RS485 and ETHERNET.
- **Telephones**, must not be connected to **LOUT.**
- **I1/2/3** must be connected to an output of control panel which must activate in case of TAMPER or in case of PSTN line failure. Connection must be EOL, so in case of cutting wires, main control panel will trigger alarm.
- **O1/2**, must be connected to inputs of control panel, and they should configured to activate in case of tamper, or in case communication failure.

BOX INTERNAL WIRING



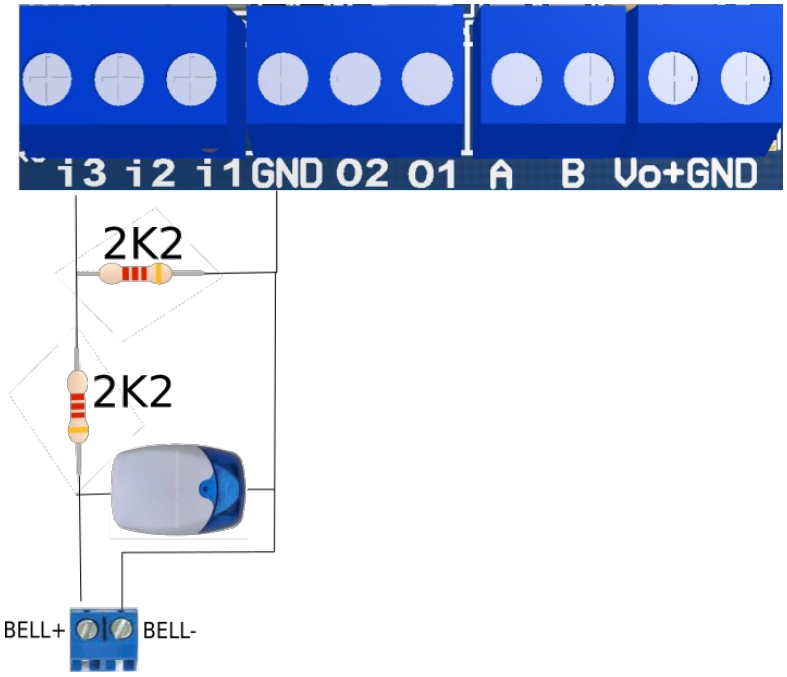
Inputs and outputs connections

Input Channels.

CIRRUS has 3 input channels, totally configurable (NO/NC/EOL) which may activate both board output and report communicator to Cloud. They can also be configured to sense analogue values and 4-20mA sensors.

Connecting the zone input to a 12V/24V driven output

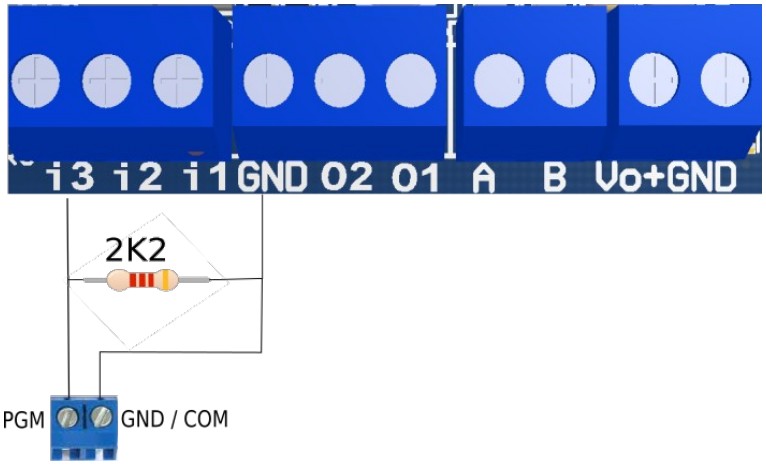
In order to provoke the alarm of the input zone when activating a 12V driven output use following wiring diagram. The zone should be programmed as EOL.



Note: The presence or lack of siren won't affect the trigger of the zone.

Connecting the zone input to a 0V driven output

In order to provoke the alarm of the zone input when activating a 0V driven output, use the following wiring diagram. Zone should be programmed as NO-EOL, this configuration should be used for mandatory wiring with control panel



Analog sensors

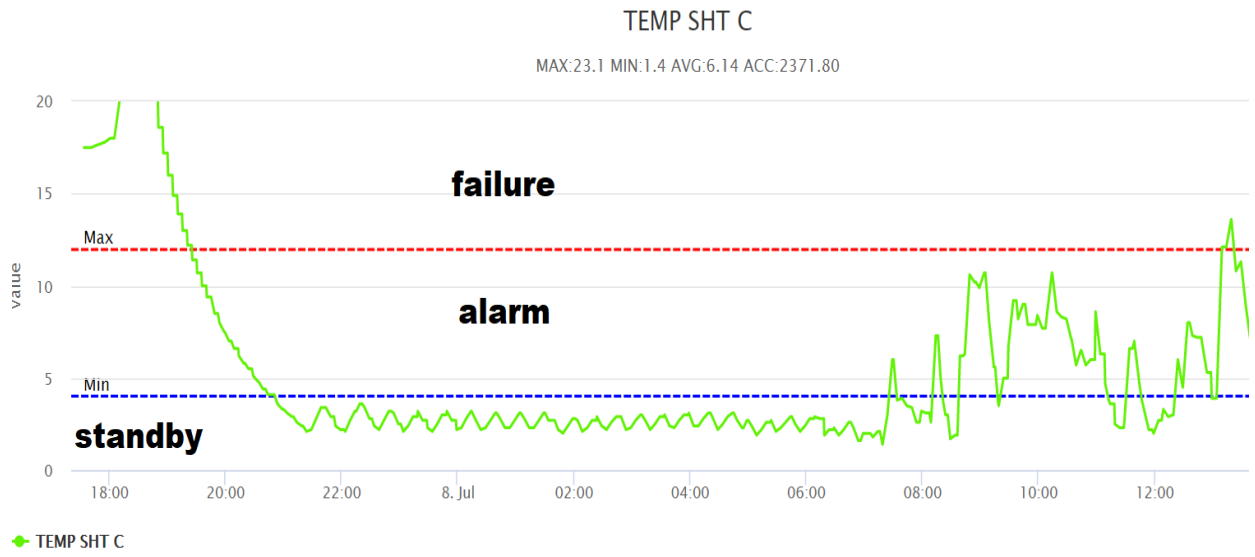
One of the most advanced functions of CIRRUS series is the chance to measure, register and send to cloud analogue sensor's data, which can be directly wired to the input zones i1,i2,i3) or as probes that can be connected to analogue expansions. Trigger levels n1 and n2 can be defined for each channel so when analogue data crosses those limits, asynchronous measure and alarms can be triggered, sent to cloud, and the cloud can then alert the user with help of email or push notification.

input channels 1i-i2-i3 can also register as analogue data, pulse count and pulse duration in 24h timelapse, pull down of 150ohm 1% offer the chance to measure 4-20mA sensors.

Analogue channels can work in 3 modes, depending on the levels n1, n2 and analogue data usual value.

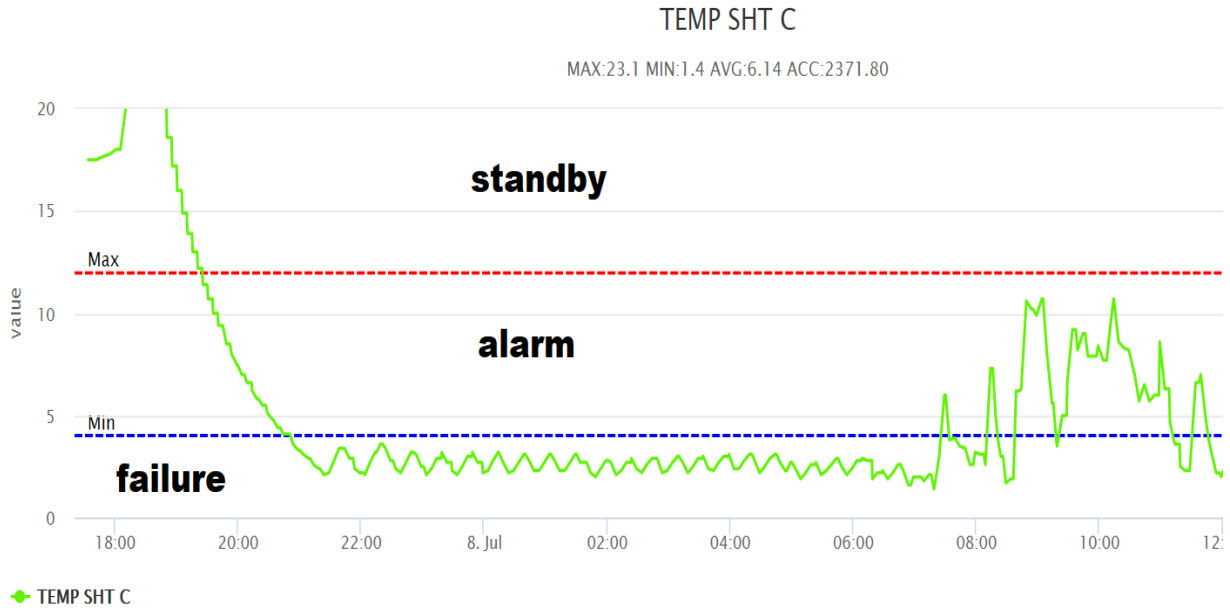
Analogue channel, normally low

This working mode enables to control an analogue value which is normally bellow limits n1, and n2, when value crosses up the trigger level n1, an alarm is issued and so activation of outputs is possible, but in case the analogue data crosses n2, then tamper alarm or failure events can be generated.



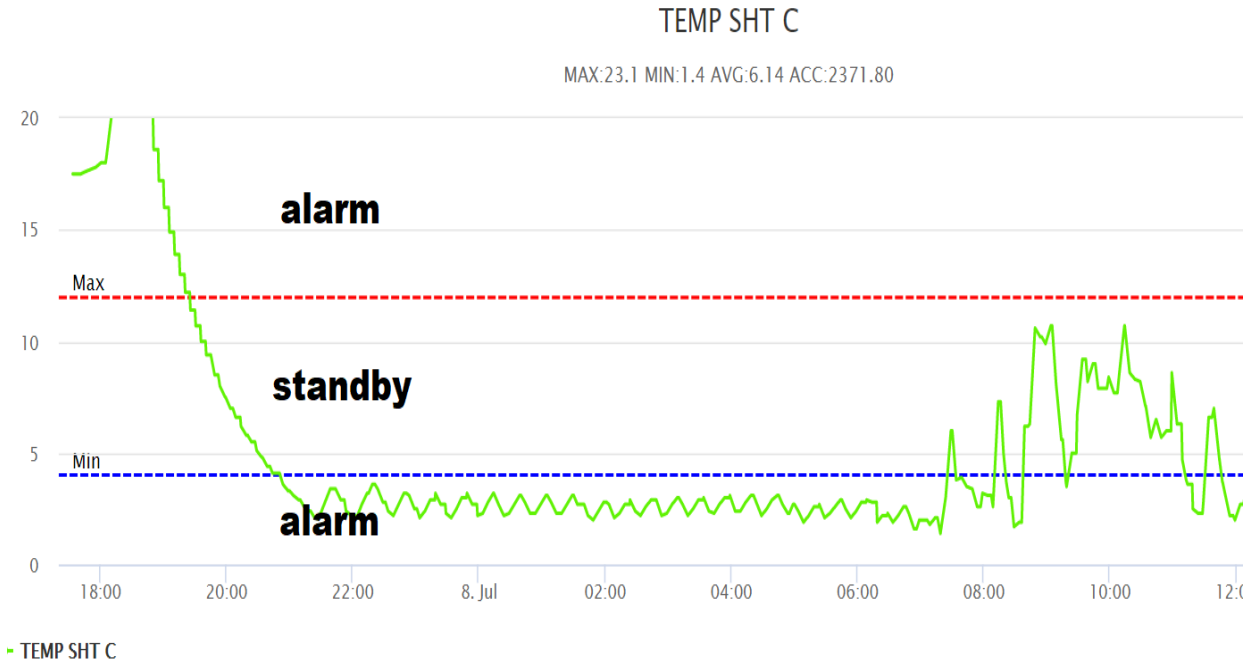
Analogue channel normally high

This working mode enables to control an analogue value which is normally over limits n1, and n2, when value crosses down the trigger level n1, an alarm is issued and so activation of outputs is possible, but in case the analogue data crosses n2, then tamper alarm or failure events can be generated.



Analogue channel normally medium.

This working mode enables to control an analogue value which is normally within limits n1 and n2, when value crosses up the trigger level n2 or down n1, an alarm is issued and so activation of outputs is possible, in this case there is no tamper / failure level.



Note that combining the same sensor in two channels , one defined as normally low and another defined as normally high, a normally medium with tamper is obtained.

Device outputs

CIRRUS has 2 open collector output, max voltage it is 35VDC, with maximum continuous current of 200mA. Options as activation time and working modes are completely programmable.

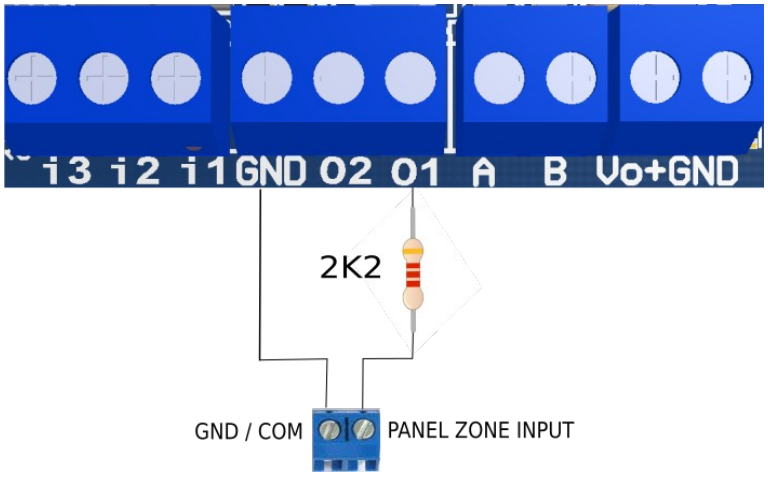
By means of MODBUS relay expansion module, up to eigth 5A/275Vac relays can be added to the device

CIRRUS output may be activated directly in case of alarm of its zone input, programmable events or Remote Cloud control.

Timing value	Device output's behavior
1-65534	The output will get activated when alarm is detected in the associated zone, at the end of the activation time, the zone and alarm will be restored, however if zone continues detecting, it will be automatically bypassed and won't be restored till the zone stops detecting.
0	The output will be activated while associated channel is detecting, and would be restored (deactivated) when detection is ended. The output follows zone input state.
65535	The output will be activated for infinite period and would be restored by means of device disarming , remote control or when associated event restores.

If you wish the output to be activated when PSTN/GSM/WIGFI failure are detected, and to be restored when mentioned failure is repaired, you should program a value of 65535 output activation time, and the corresponding options.

Connecting O1/02 to control panel input



Outputs must be configured as Normally activated (connecting to ground) in order to produce a failure in the output if an error occurs in the software or in the case the wiring is cut. The control panel that will be connected to the output must have its input configured as NC-EOL.

NOTE : EOL resistor of some control panels might be different than 2K2

General working modes.

Status LEDS

CIRRUS LEDs indicate following states:

LED	OFF	Flashing	ON	Blinking
D1	GSM not available	Single flash GSM online, double flash=GPRS online	GSM call active	GPRS activity
D2	PSTN failure	PSTN OK	Seized line.	Ring PSTN
D3	Power off	Disarmed Power Ok	Armed Power Ok	Low power supply
D4	No LORA comm.	LORA Tx/RX	Lora TX	-

Flashing frequency of D1 LED indicates signal strength:

- Flash every 8 sec: RF signal from 1 to 39%
- Flash every 4 sec: RF signal from 40 to 79%
- Flash every 2 sec: RF signal from 80 to 100%

Note: After powering the circuit, wait for GSM network connection before making any test, while LORA or WIFI almost start on time.

Control panel Serial interface.

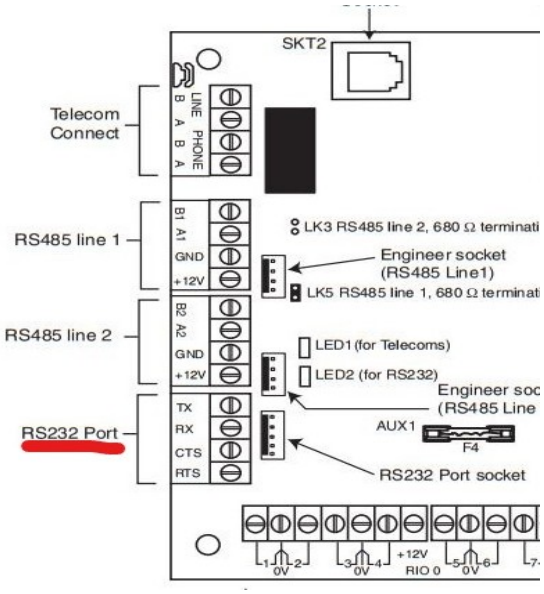
The transmitter is capable of carrying out Virtual COM bi-directional with the control panel:

GALAXY DIMENSION

The Dimension, G2,G3,Classic, have an RS232 channel

By means of **CB-232**, cable which can be connected to CIRRUS and then to the Galaxy control panel, as shown in the picture-.

It is necessary to properly configure the Galaxy panel to activate Serial Reporring on RS322 channel..



Configuration for Galaxy control panel.

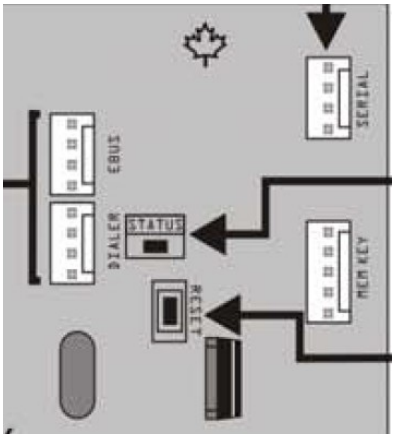
Enter engineer mode , and go to **Menu 56**

- Menu 6 – Int RS232 1
- Select direct mode
- Select SIA Format
    - Enter SIA (Option 2)
    - Select SIA level 3
- Make sure triggers 10 y 18 are active
- Activate triggers for all wanted events.
- Introduce subscriber code <_____>
- Select : **Comms Setup**
    - Enter Baud Rate - 57600
    - Enter Data Bits - 8
    - Enter Stop bits - 1
    - Select parity – No Parity

CIRRUS-4T config.

From web interface select control panel model in Device EDIT , configuration will be carried out automatically.

PARADOX MG,SP y EVO.



The Magellan/ Spectra and EVO control panels have a SERIAL connector where events are delivered in real time to the transmitter and also enables bi-directional connection by means of VCOM simulation.

In order to carry out this connection CB-PTTL cable is need, connect both ends to SERIAL channel of CIRRUS and Paradox control panel, as shown in the picture.

Cirrus configuration.

From web interface select control panel model in Device EDIT , configuration will be carried out automatically on Cirrus.

DSC PC1616, PC1832 and PC1864

These control panels can be connected and controlled by means of keypad bus interface, the connections are:

- Yellow keypad wire to the B terminal.
- Green keypad wire to A terminal, and also connect A terminal with 10K resistor to i2 terminal and from i2 terminal connect a 1K resistor to GND.

ADEMCO VISTA

These control panels can be connected and controlled by means of keypad bus interface, the connections are:

- Yellow → Terminal B
- Green → Terminal A

It is also necessary to install a 1K resistor between the Green terminal of control panel till 12V aux .

In order to achieve the integration and be able to arm / disarm the system it is need to configure the CIRRUS as the eight keypad of the system, in order to do this, enter Vista installer's programming and press:

*196 10

DETNOV

Detnov Fire control panels are to be connected by means of RS485 where alarm protocol has been established between the control panel and the transmitter, this procotol is based on Contact ID, and Fire / Failure signals are transmitter seamlessly, acknowledge of receipt and transmission path failure are also signaled by means of this protocol.

By Means of ETHERNET , MODBUS-TCP integration is done, the connection can be through crossover cable or through, this permits to monitor the complete internal status of control panel, thus being able to show it on nuvasafe cloud. Also bidirectional communication is offered through this means.

SIA-DC03

Any control panel , including intrusion and Fire control panels can be connected by means of Ethernet to the device , thus enabling routing of LAN signals to CELL and LORA intefaces. As example GALAXY FLEX can be connected by this method.

SIA-DC09

Any control panel , including intrusion and Fire control panels, capable of signaling using this protocol in both Contact ID or SIA, can be connected by means of Ethernet to the device, thus enabling routing of LAN signals to CELL and LORA intefaces. As example GALAXY FLEX can be connected by this method.

On preparation , Texeccom.

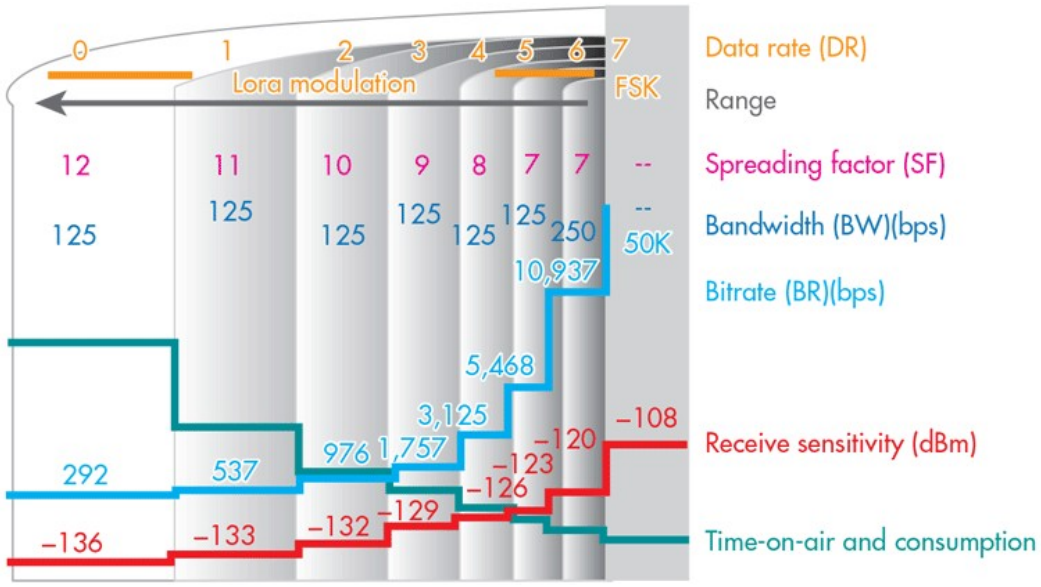
☑ ***EN50136***

Despite of using these serial interfaces for download of control panel, PSTN and IO connections are mandatory to meet EN50136 regulations

LORA wireless communication

LORA is a radio communication chipset capable of covering long distances at very low power (from 14 to 20dBm) in unlicensed ISM bands (915MHz Americas and 868MHz Europe). Lora is capable of reaching the category of a secondary Alarm transmission path as stated in EN50136 DP4 classification.

In the LORA communication speed (Spread Factor), antenna type/location and transmitted power directly determines the link range, the slower the communication speed the longer range we can experience.



CIRRUS devices are applying hopping from SF7 till SF10 and Bandwidth of 125KHz, yielding to an effective communication speed from 5k6bps to 976 bps, indoor city ranges can be up to 1Km between devices.

CIRRUS Devices provided with LORA transceiver will automatically form a mesh network between them, so in case of loosing TCP-IP connectivity, the devices will broadcast their event and polling signals over RF till they reach a device with an operative TCP-IP link, this device will be in charge of relieving these messages to cloud, and ack will be transferred from cloud to the originating node through the relieving node.

The main goal of LORA communication is to offer a reliable unlicensed RF backup communication channel in case of router or GPRS network failures (which is a very common situation) thus offering a state of the art link security against failures and communication Tampering.

LORA communication is a two way fully functional backup network, that offers not only event and polling signal communications, as long as download function with device and associated control panel (see next section).

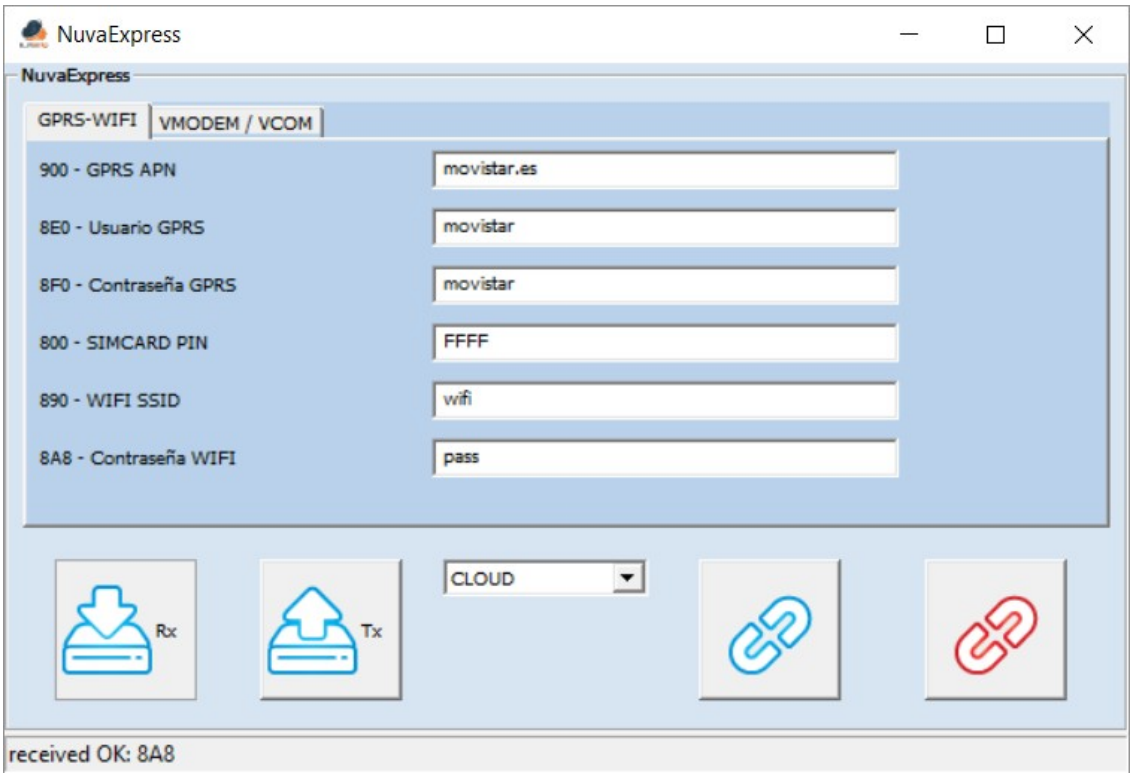
For areas with already operative LORAWAN networks, the device is capable of operating in these networks, please check NuvaSafe's engineering dept in order to activate LORAWAN in the devices, but LORAWAN protocol could not meet the requirements of EN50136-2 rules.

Download

Download is the communication between CIRRUS and Cloud for programming / monitoring functions, this function is fully provided in Nuva-Cloud, so there is no need for installable software to run that function.

Nevertheless, there is an available application "nuvaexpress", which enables Cloud (using WIFI, GPRS or LORA) and USB setup of the device.

NuvaExpress

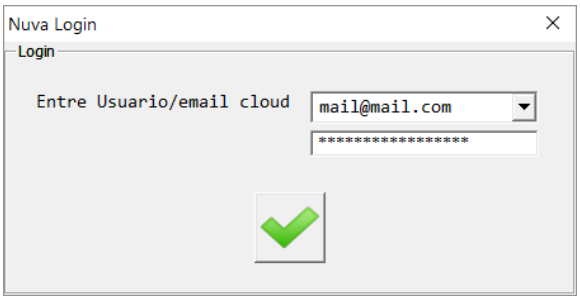


USB connection

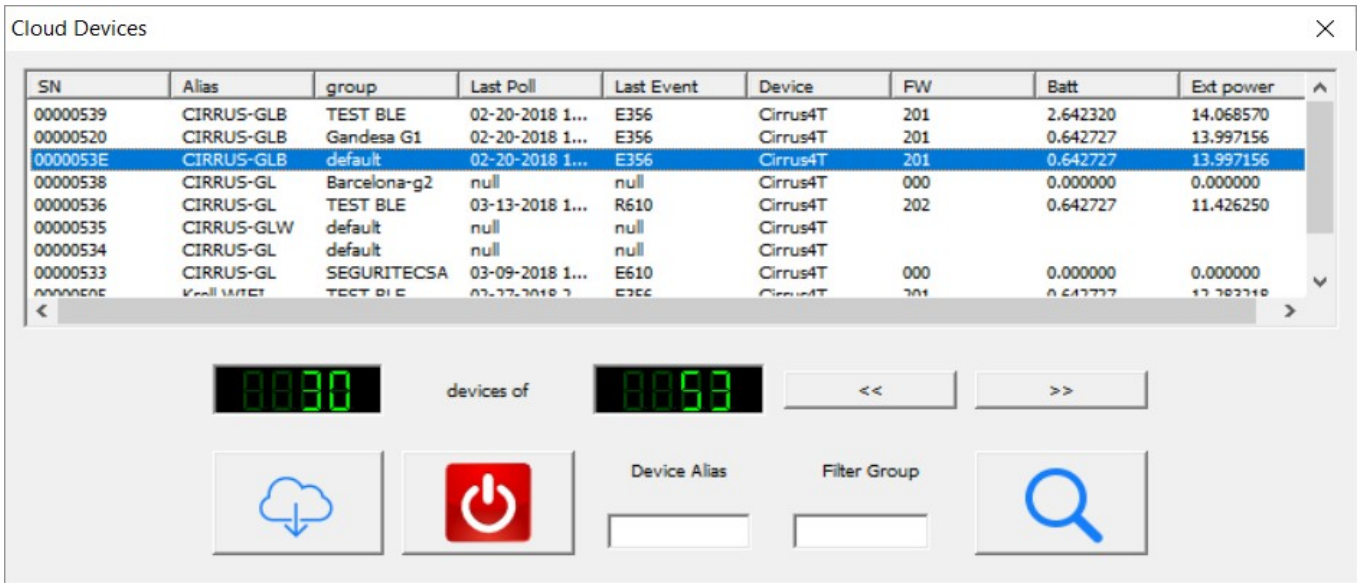
Before start , you need to install the USB drivers of the CIRRUS-4T, so once the application is installed, go to / *Program Files* / NuvaExpress / drivers /, and then execute the corresponding file as administrator dpinst_amd64 for 64 bits or dpinst_x86 in case of a 32 bits computer. Once installed execute the application as **administator.**

CLOUD connection.

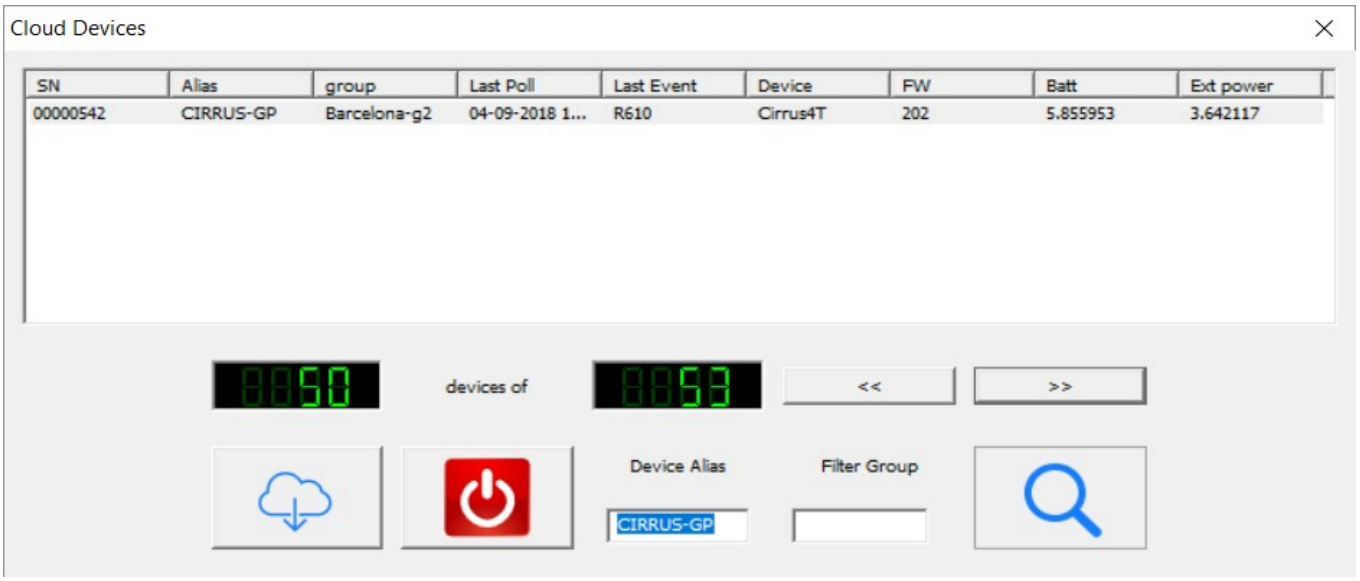
Once started the Nuvaexpress, you must select the option for CLOUD connection, in that case a window will appear asking for our credentials in the cloud (ask your distributor in order to get those credentials).



Once logged, a window with existing devices assigned to our company / group will appear after pressing the blue (connect) button.



We can navigate using the cursors, or we can put a text on "Device Alias" field and then the magnifier button, so this way we can make a search for a device



Select a device from the list and then press the "download from cloud" button, providing the device is powered and online, it is possible to carry out the Virtual Modem y Virtual Comport con el panel.

In order to know if a device is online, from he list above, check the "Last Poll" data, it must be recent in order to consider a device online.

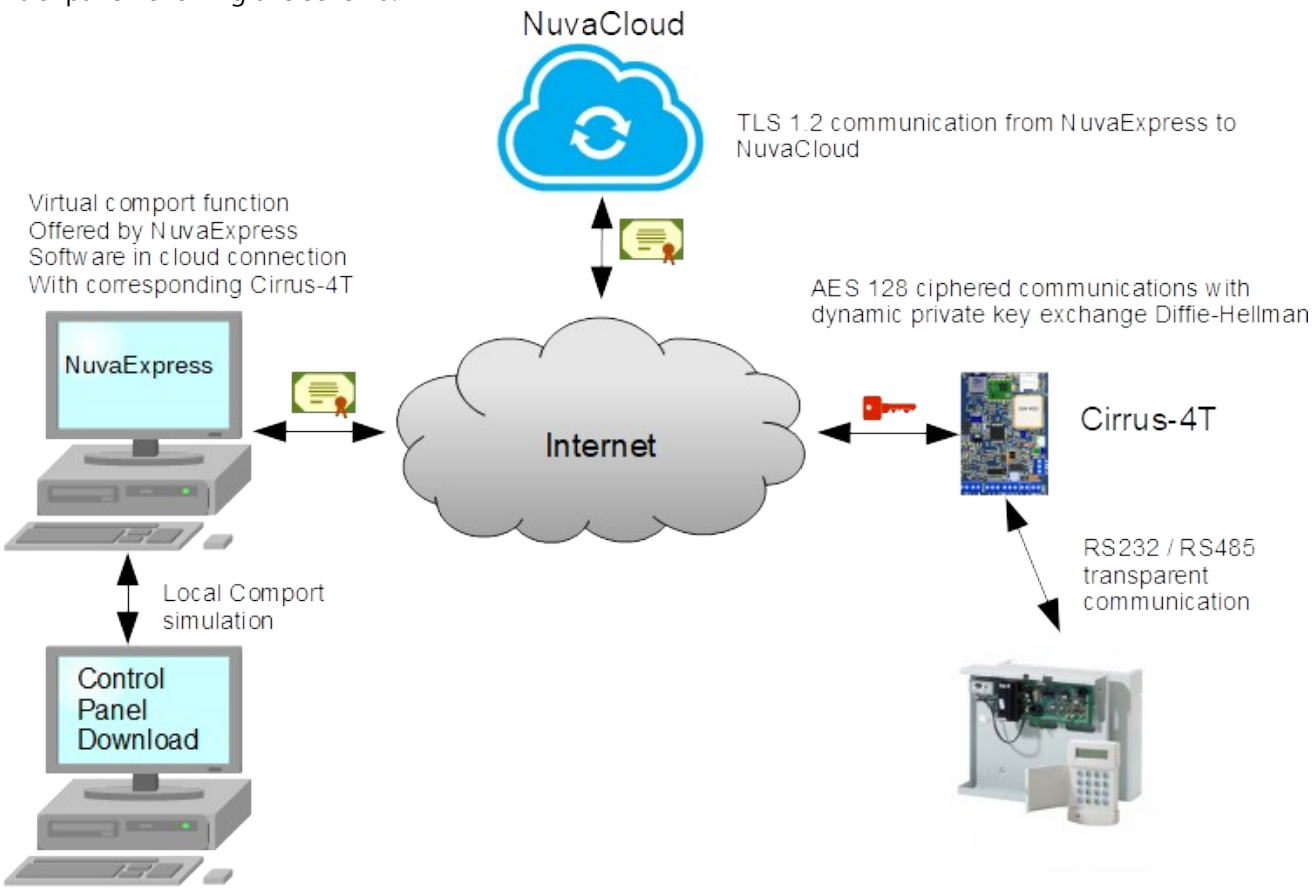
Once downloaded the device, the application will try to connect with the device , if the device it is detected on USB , it will use USB otherwise will try to connect through the cloud.

Once connected on main page you can read or write basic configuration of the device by using the RX/TX buttons.

Once finished configuration, press disconnect button (red lace button)

Virtual COMPORT download with associated panel

Using the corresponding cable for each control panel a bidirecctional serial connection can be made with the control panel following this schema.



Tested control panels for Virtual Comport serial are:

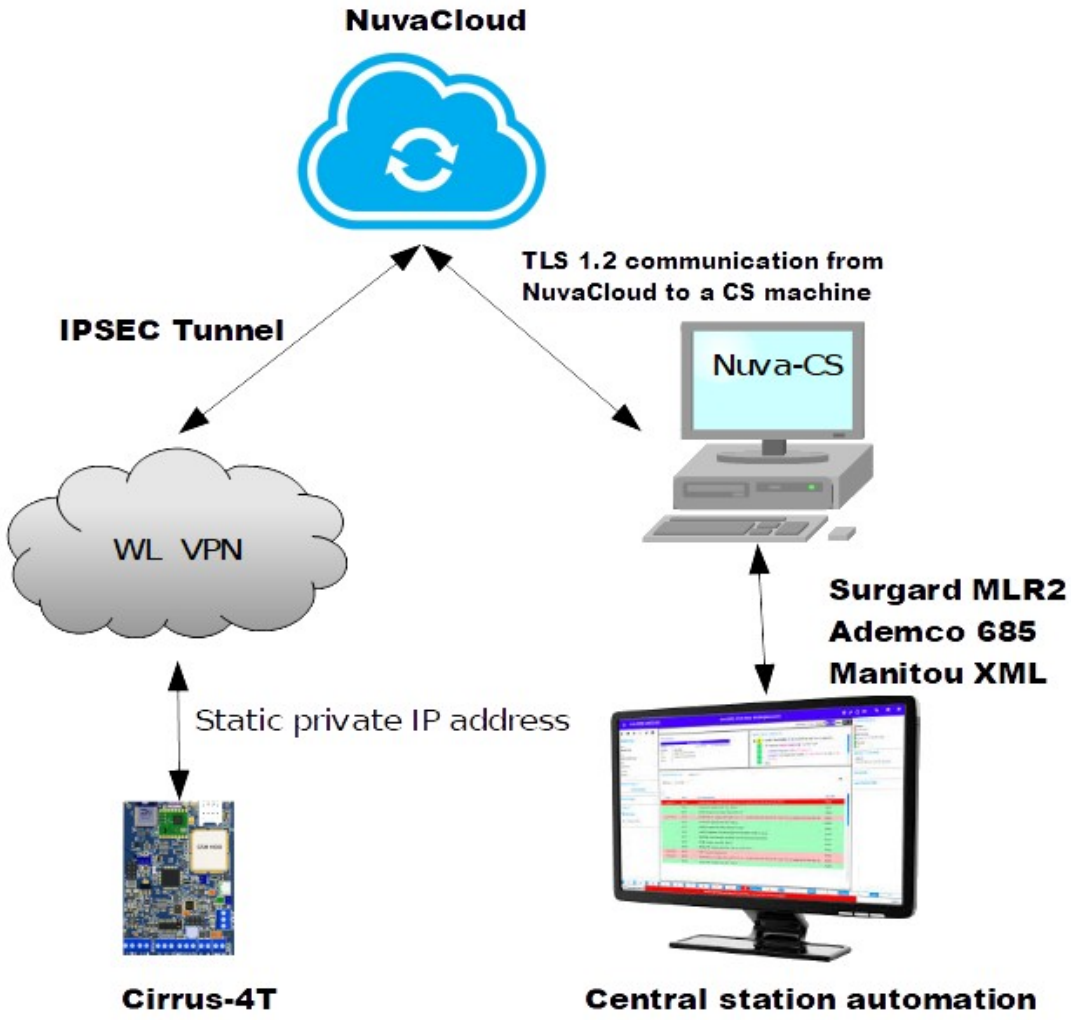
CONTROL PANELS
DSC P1616/32/64 using CB-DTTL
Paradox MG / SP / DGP / EVO using CB-PTTL.
Honeywell Galaxy series RS232, using CB-232
Risco LIGHTSYS, PROSYS , AGILITY, using CB-232
Notifier ID3000
DETNOV Fire Control panels

Reporting functions

Normal working mode of the device is to send all their events and status to a Cloud Server which later, by means of internal logic, will allow resend these Reports to Central station or call centers.

From factory all events are activated to be reported.

Communications to Central Station schema



The devices Cirrus-TL or Cirrus-TLW/E with cellular connectivity are delivered from factory with embedded VPN SIMCARD, which can be from a national carrier or a multi-carrier, but all of them are to use the same VPN.

The VPN connectivity offers the following advantages over public network communications.

- The SIMCARDS have a private fixed IP, so the device can always be accessed from cloud, which can only be accessed using secure protocols such , HTTPS and TLS 1.2.

- There are not over consumptions due to unwanted internet traffic.

- The communications are private and encrypted and only accessible from server, being compliant with UL1610 and EN50136 standards.

- UPD (DTLS) can be used without need of SSL (note that opening an SSL socket in GPRS can take up to 8 seconds), this fact combined non wished traffic loads, dramatically reduces the amount of data needed to communicate with server and so reducing the cost of the SIMCARDS.

SIMS VPN.

NuvaSafe will bill to the security companies by volume of data, multi-operator, number of SIMCARDS and the cloud service, with scaled quantities. If your company already have a VPN tunnel is created, there is the possibility of opening a secondary tunnel to the Nuva-cloud so that all communications are secure, in this case won't be billed for SIM service, but yes by means of cloud of service.

Nuva-CS Software

Once data from the Communicator arrives to the cloud, it can be redirected to the Central station serving you, so will need to install on an internal machine of the receiving station a small application called Nuva-CS that receives events from the main cloud over a TLS 1.2 connection and that once received forwards them to the software using Ademco 685, SURGARD MLR2 either Manitou XML protocols.

The operators of the CRA will benefit from access to computers through the web / Apps or by specific integrations with different management softwares.

Device reports options

Report to Central station is done in Cloud receiving software.

Subscriber code

This is the identification code of CIRRUS, which permits Central Station to identify to what client does the device belong to. P, the device will capture Subscriber code from main panel communication, so there is not need to setup this option.

Options

Channels test report

This is a periodic report to check correct state of communication paths between CIRRUS and Central Station.

☑ *EN50136* : To comply with the regulations the phone test must be activated., default to 60 minutes.

Cadence time of periodic test.

Programming in minutes, from 1 to 65635, from cloud server, default to 60 minutes.

Polling function

Polling is the periodic communication established between the device and the cloud, using the available TCP-IP connections.

DVR Picture backup.

This device offers a unique function by means of it is capable ot sending pictures to cloud , coming from Digital video Recorders, this way when IP connection of premises is jammed so DVR cannot send videos, there is still chance for the device to send small snapshots using CELL or LORA backup channels.

NON-STANDARD CONTACT ID CODES

The device uses the following Contact ID codes to signal technical events.

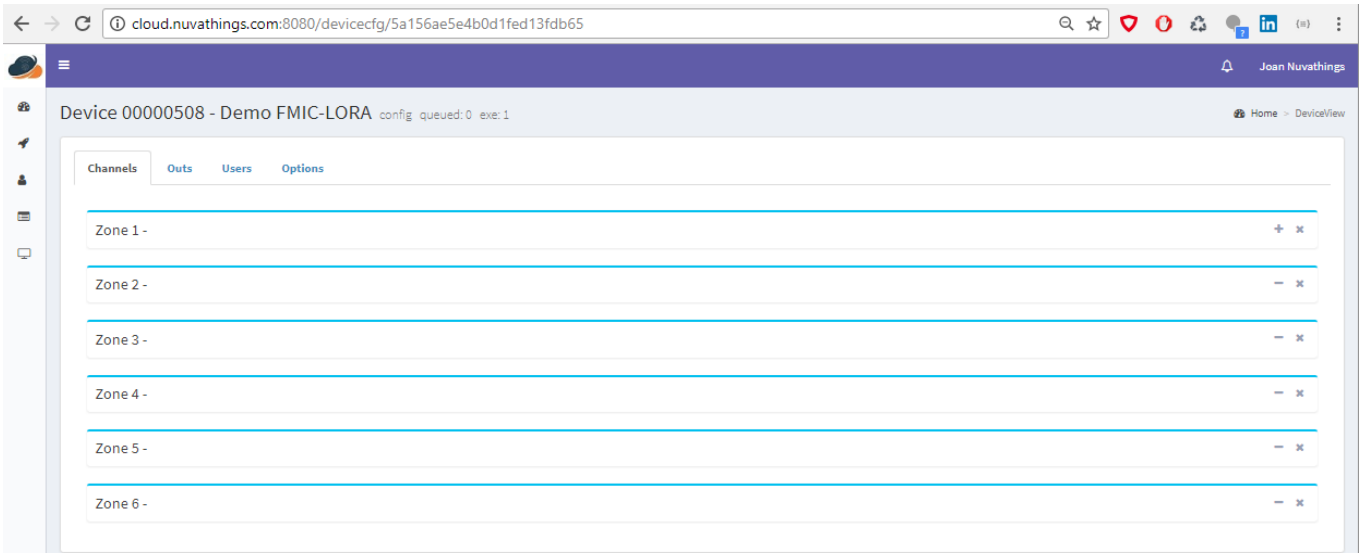
CODE	Description	CODE	Description
E351	PSTN failure	E352	CELL failure
E35D	LORA failure	E35E	ETHERNET failure
E35F	WIFI failure	E60B	Analog measure
E356	Polling failure	E610	Polling signal

Programming

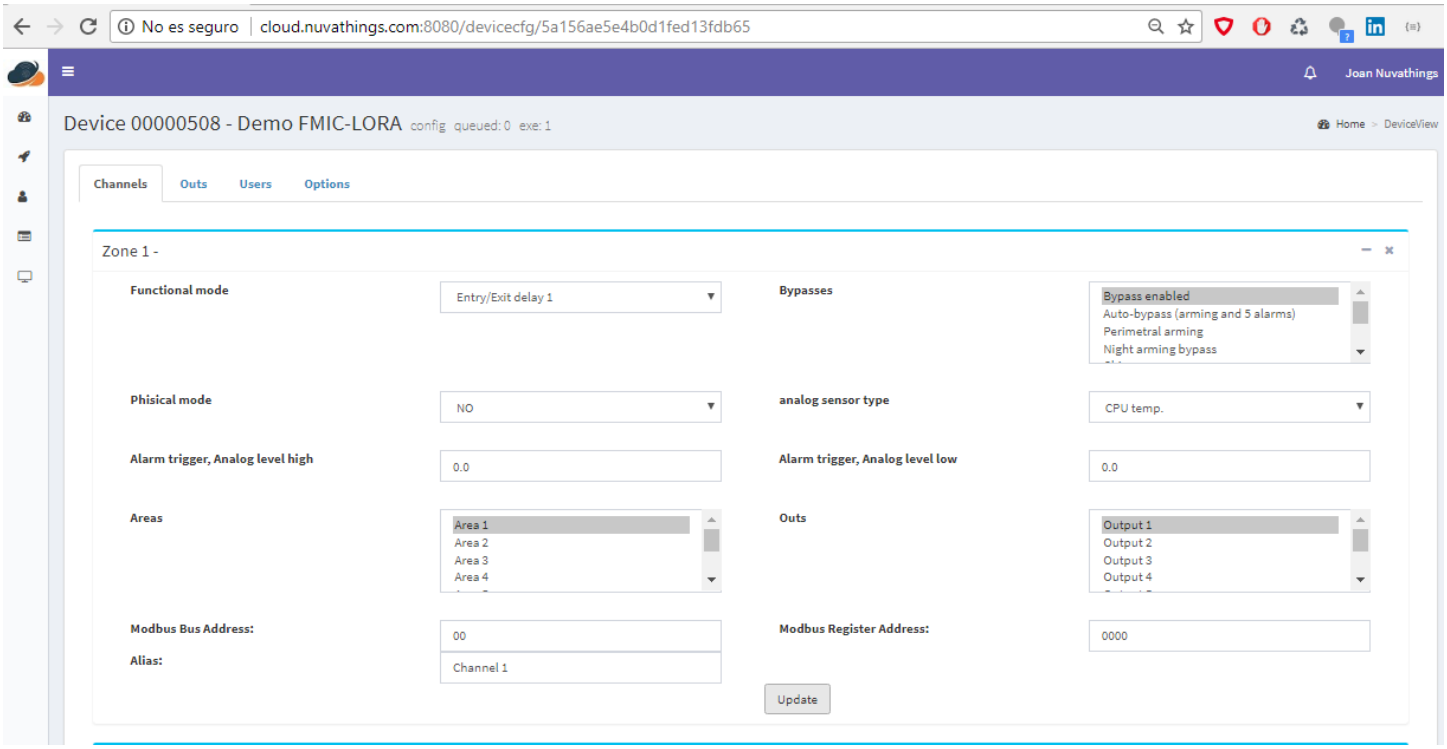
The only way to program device is from NUVA-Cloud., acces it at cloud.nuvasafe.com

Configuration over view

Configuration is accessed from device's folder by clicking "config" button.



From this view it is possible to configure input channels working mode, outputs, user's codes and system options. The configuration is build up of tabs, and inside the tabs every input item has it owm form block, so it is posible to update device's configuration one by one, all changes made are sent to the device and stored in DDBB, so forget about unmatched configuration databases in different computers.

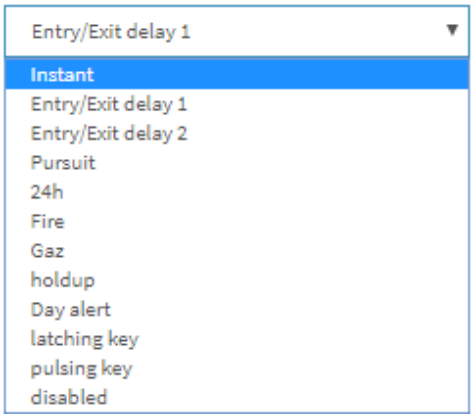


The upper line has a "queued" and "exe" counters and gives you feedback about how many changes have been sent to device and how many of them have been already executed.

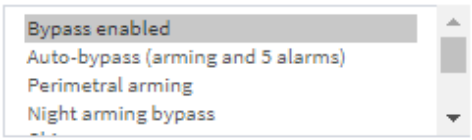
Input channels configuration

The different options are the following:

Functional mode



Only a single option is to be assigned to device's channel.

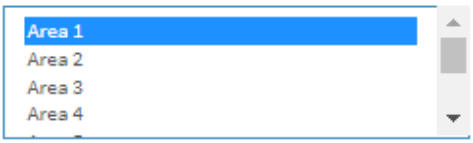


Bypasses

In this case multiple options can be assigned to the channel, to do this, just click options while holding down key "CTRL"

Areas and outputs

Also multiple options are possible to be select for each channel.





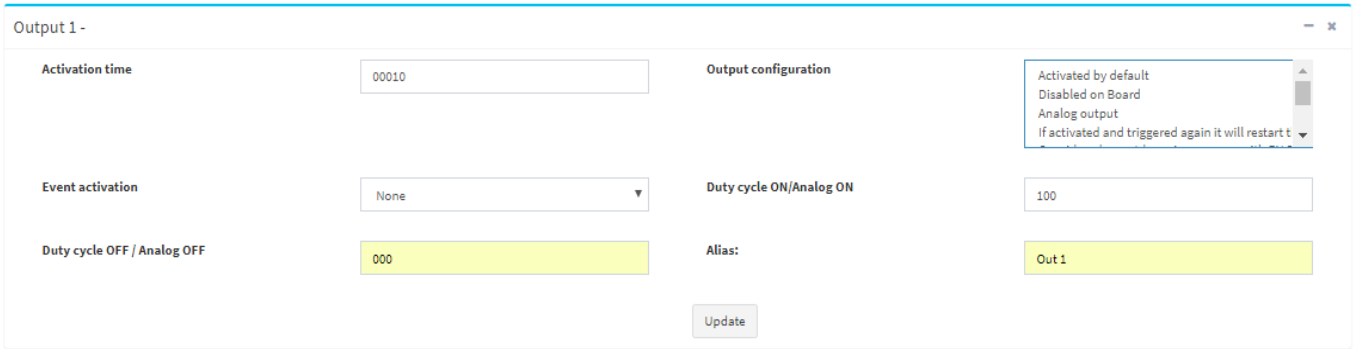
Alias

Alias permits to assign a name to the input channel, this name is to be displayed in cloud and APP's later.

Outputs configuration

Consider the following mapping between outputs and board available outputs.

- Output 1, 2 – Board Open drain ouputs O1, O2
- Output 3 – Line switch relay
- Output 4 – Can be connected to 0-10 analogue output.
- Output 5..8 – Matching with Relay 1.. 4 of relay expansión module.



Activation time.It is a counter between 1 to 65534 (seconds) or forever with value 65535.

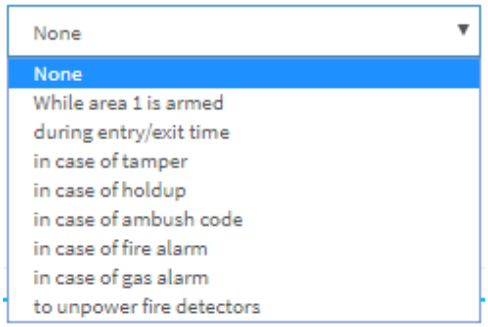
Activation time.

There are multiple options to be pick.

- Activated by default: means the channel will be active state while in standby, for NO outputs this means to be shorted to GND.
- Disabled on Board: this option disables the output physically in the circuit board, only to be used then the terminal has another function than being an output.
- Analogue output: the output (Output 4) is to be connected to the 0-10V analogue output, not to be used in alarm transmitters where AnOut works as PBX simulation.
- If activated and triggered again, with restart counter.
- Outdoor advice device (EN50131)
- Triggers even when disarmed.
- Beacon activation: it is activated when a moving beacon is detected within the controlled area.
- Remote control, Enables the output to be controlled from web or APP

Event activation

These options permit the output to be activated in the following events:



Dutty cycle ON

For the analogue output, this is the % value from 0-10V to be applied when output is activated, otherwise it is the OFF period for a total period of (Dutty ON + Dutty OFF)

Dutty cycle OFF

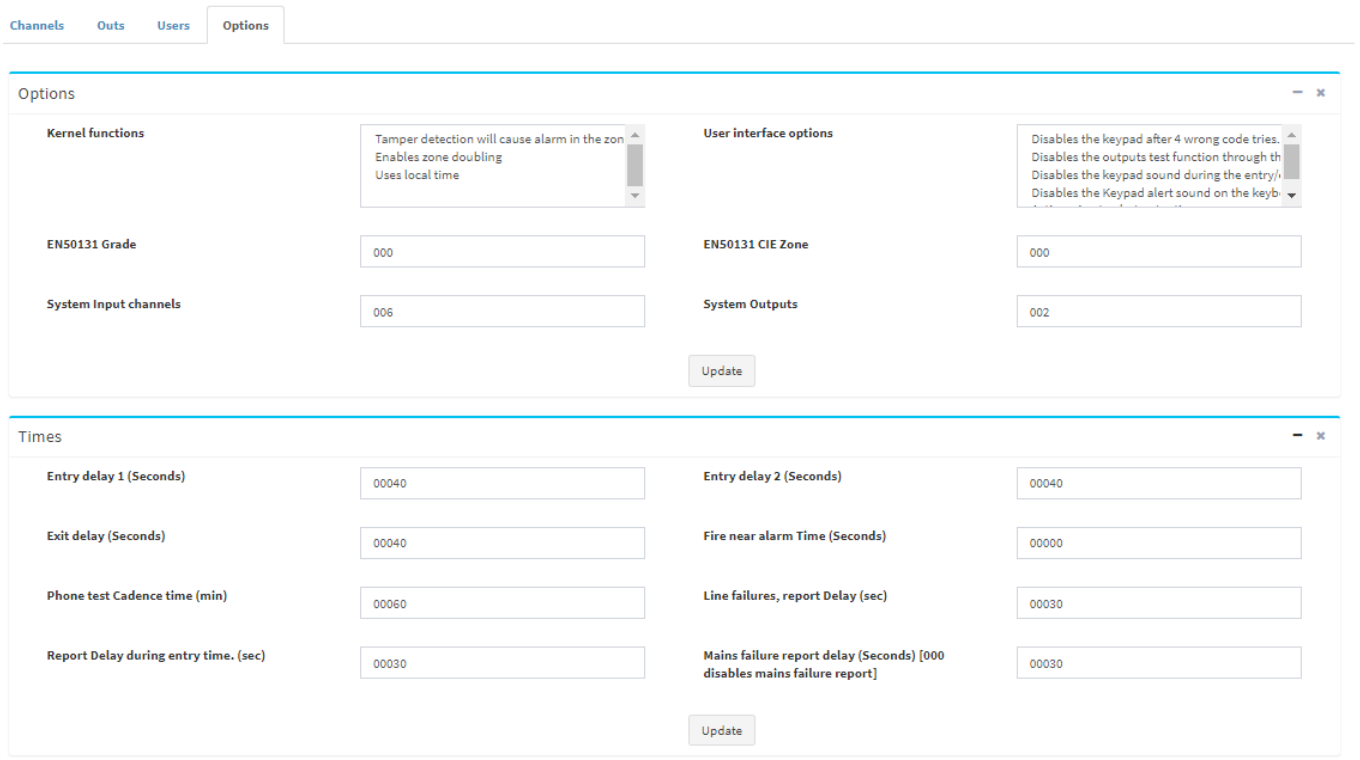
For the analogue output, this is the % value from 0-10V to be applied when output is in Standby, otherwise it is the OFF period for a total period of (Dutty ON + Dutty OF F)

consider that if Dutty ON = 2, and Dutty OFF = 5, the output will repeat till its timer elapses to activate during 2 seconds and deactivate during 5 seconds.

Alias

The name for the output, to be displayed in WEB and APP.

Options and Timers



Options:

Multiple options can be activated providing they are not exclusive functions.

- Tamper detection causes alarm, a open condition in the zone's loop will trigger tamper alarm, otherwise , failure will be issued..
- Activates zone doubling, enabling to connect up to 6 sensors to the 3 zone inputs.
- User local time, default will use UTC.

User interface options (in preparation)

- Disables keypad after 4 wrong code attempts
- Disables output test function.
- Disables keypad sounds during entry time.
- Disables keypad alert
- User ringer to alert entry time.

EN50131 grade

Defines the EN50131 grade as : 0,1,2,3 or 4.

EN50131 CIE zone

Defines the channel number to use when sending panel tamper event.

System input zones

Defines the used zones of the device, so this way it will limit the display in web and APP..

System outputs

Defines the used outputs of the device, so this way it will limit the display in web and APP..

Timers

All timers work with maximum time of 65535, seconds of minutes depending on the case.

Entry time 1.

Maximum time for entry time for entry / exit zones 1, defined in seconds in order to meet En50131 regulations , maximum time is to be 30 seconds.

Entry time 2.

Maximum time for entry time for entry / exit zones 2, defined in seconds in order to meet En50131 regulations , maximum time is to be 30 seconds.

Exit time

Maximum time for exit time after arming system for entry / exit zones 1 and 2, defined in seconds in order to meet En50131 regulations , maximum time is to be 40 seconds.

Fire pre-alarm time

Defined time in seconds between fire zone/gas zone detection and its alarm, during this time it is possible to cancel the alarm.

Periodic test.

Time lapse in minutes for sending periodic test to central station / cloud, event is E602 in contact ID, check value in order to get the STP/DPT rating.

Communication lines failure delay

Delay in seconds applied when system has to send a failure indication about a communication channel, (such ETH, GPRS and WIFI), depending on SPT/DPT and EN50131 grade, has to be setup accordingly , for compliance in grade 2, cannot be longuer than 180 seconds, for grade 3 cannot exceed 60 seconds.
If the failure restores before the delay elapses, then the failure won't be reported.

Entry time report delay.

This delay is applied when an alarm triggers during or at the end of entry time, for grade 2 and 3 this delay can't exceed 30 seconds, during this time only indoor sirens can be triggered and if before the delay concludes the system gets disarmed, then the alarm report will be cancelled.

Mains failure delay

Delay applied to the mains failure event, if power restores before the delay concludes, then the report won't be sent