GSM 3G 4G LTE
Cellular IoT Gateway

KING PIGEON

S475 S475E

User Manual

Ver 1.6.4

Date Issued: 2020-09-21

King Pigeon Hi-Tech. Co., Ltd.

www.IOT-Solution.com

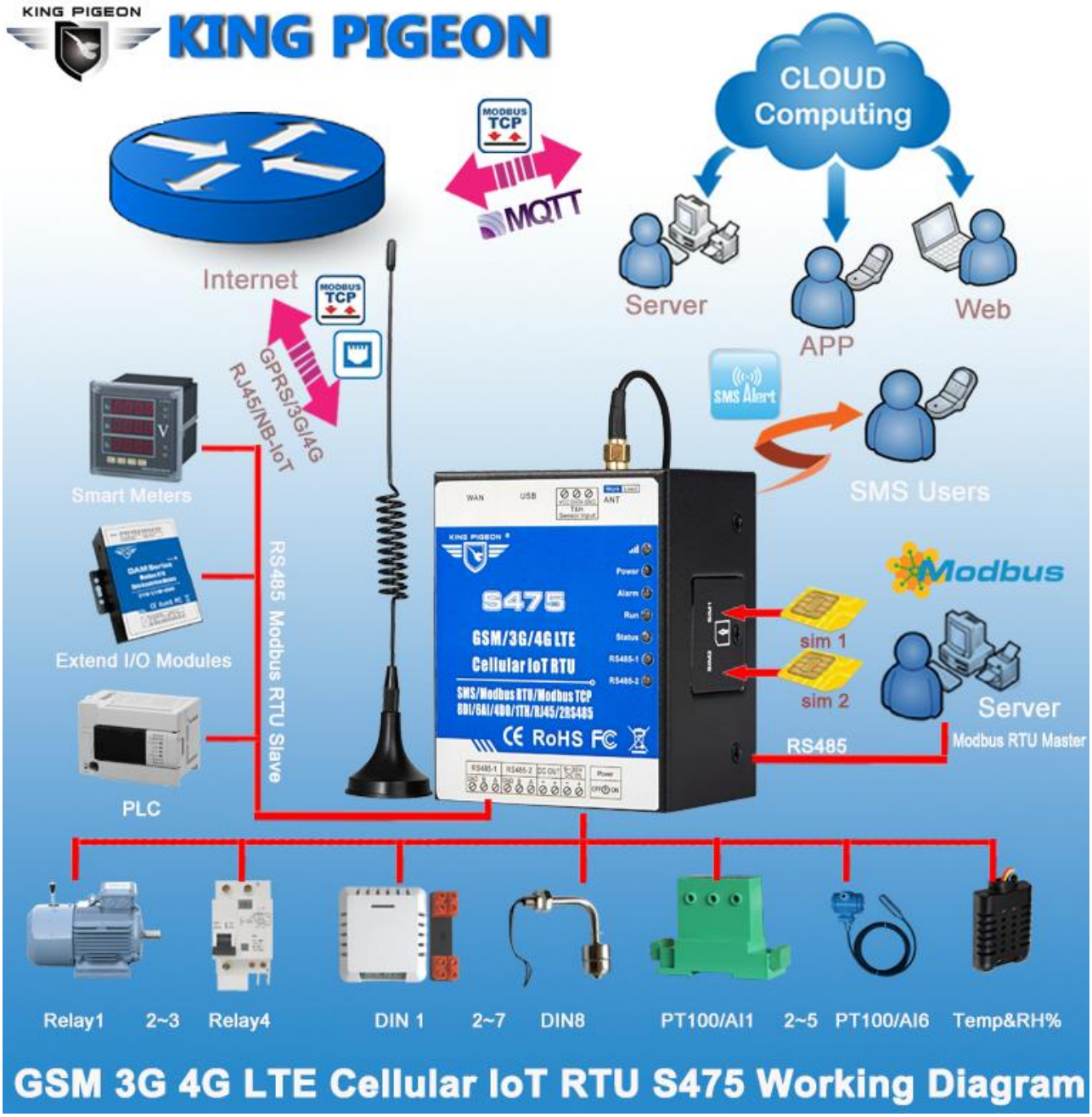
Table of contents

【UPGRADE HISTORY】

DATE	CONFIGURATOR VERSION	FIRMWARE VERSION	HARDWARE VERSION	DESCRIPTION
2018.10.25	*V1.0*	*V25*	*V 1.3*	*First edition*
2019.03.18	*V1.0*	*V25*	*V 1.3*	*Modified the start address of the 32-bit map register in Appendix C*
2019.04.09	*V1.1*	*V26*	*V1.3*	*Network port and cellular add MQTT connection to cloud platform*
2019.04.20	*V1.2*	*V27*	*V1.3*	*Adding S475 E Series Products*
2019.08.15	*V1.3*	*V28*	*V1.3*	*Adding the function of Ethernet as Modbus TCP master*
2019.9.23	*V1.3*	*V28*	*V1.3*	*1.Modified Cellular network Settings default parameter* *2.Adding MQTT protocol instruction*
2020.3.13	*V1.4.2*	*V31*	*V1.4.1*	*1.Add DIN1-3 pulse counter features*
2020.04.09	*V1.4.2*	*V31*	*V1.4.1*	*Revised MQTT data release format*
2020.7.29	*V1.5*	*V31*	*V1.4.1*	*Remove supports SDK*
2020.09.18	*V1.6.3*	*V31*	*V1.4.1*	*1.Modify wiring diagram* *2.Modify MQTT settings and reissue instructions*
2020.9.21	*V1.6.4*			*Modify SMS command error*

Model List

Model	GSM/3G/4G	Ethernet	DIN	AIN/PT100	Relay	T&H	SD Card	Mapping Registers				
								Boolean	16-Bit	32-Bit	64-Bit	RS485 Port
S475	√	√	8	6	4	1	8G	64	128	64	64	2
S475E	×	√	8	6	4	1	8G	64	128	64	64	2
Notice	1. Default version is GSM/GPRS module inside. 2. Pls check the slave devices' register quantity and data type,then choose the right model of S475/S475E according to the mapping registers in the model list. 3.For 3G WCDMA, 4G LTE version, please tell our sales where would you like to use them. 4.The S475E series has no communication module, so it can't call and SMS to alarm.											



1. Brief introduction

The Cellular IoT Gateway S475/S475E is an industrial class, high reliability, high stability, and programmable Remote Terminal Unit (RTU). It embedded 32-Bit High Performance Microprocessor MCU, inbuilt industrial Cellular module. It provides 8 digital inputs, 6 analog (ultra high 24 bit resolution) or PT100 Resistance Temperature Detector (RTD) inputs, 4 relay outputs, 1 ambient sensor input for monitoring onsitetemperature and humidity, 1 Ethernet RJ45 port for connect internet WAN or LAN, and 2 RS485 serial port,supports 320 IO tags via Modbus RTU protocol. It can monitoring and operates the I/O ports by SMS, APP, Web Server, internet, timers and programmed inter-lock events automatically.

The Cellular IoT Modbus Gateway S475/S475E inbuilt TCP/IP protocol stack make it suitable for internet of things (IoT)
applications, it can be operated easily by the provided cloud, app, and web server, or integrated to your IoT applications via Ethernet or the TCP/UDP protocol, or integrated to SCADA systems by standard Modbus TCP

protocol, too. This is very useful if you need remote control onsite devices with low cost solution.

The Cellular IoT Modbus Gateway S475/S475E supports 2 RS485 ports,which can be used as Modbus RTU Master and Slave at the same time and supports transparent data transmission . The Cellular IoT Modbus RTU can be used as Modbus RTU Master to reading smart meters, I/O modules, PLC, and converts to SMS alert once triggered the threshold value, or transmit data to remote server over GPRS/3G/4Gnetwork.

Typically applications:

The Cellular IoT Modbus Gateway S475/S475E is designed for working in the harsh industrial application environment, widely used in a variety of industrial automation:
BTS Monitoring, Security Alarm System applications, Supervision and monitoring alarm systems, Automatic monitoring system, Vending Machines security protection, Pumping Stations, Tanks, Oil or Water levels, Buildings and Real Estate, Weather Stations, River Monitoring and Flood Control, Oil and gas pipelines, Corrosion protection, Temperatures, water leakage applications, Wellheads, boat, vehicle, Energy saving, street lights control system, Valve controls, Transformer stations, Unmanned machine rooms, Control room application, Automation System, M2M, etc.

2.Safety Directions

Safe Startup

Do not use the unit when using GSM/3G/4G equipment is prohibited or might bring disturbance or danger.

Interference

All wireless equipment might interfere network signals of the unit and influence its performance.

3. Standard Packing List

Gateway X1; AC/DC Adaptor X1; GSM/3G/4G Antenna X1;User Manual X1(QR code download link); PC Configurator X1(QR code download link) .

Note: The package does not include any SIM card.

Optional: 35mm Standard DIN rail fixed Bracket

4. Features and Specification

4. 1 Mainly Features

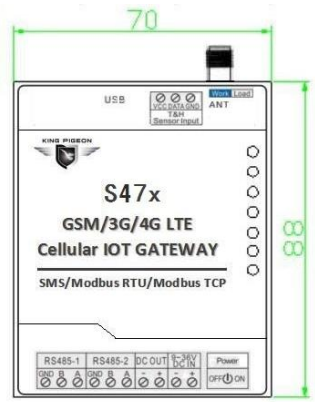
- GSM/GPRS/3G/4G network communication, can be operated from anywhere, no distance limitation;
- Quad band 850/900/1800/1900Mhz GSM GPRS Module inside,3G/4GModules are optional;
- Modular design, can easily upgrade the cellular module if network upgrade;
- Embedded ARM® Cortex™-M4 32 Bit RISC Core, 168 MHz inside, RTOS system, reliable performance with in-built watchdog;
- Wide range power supply 9~36VDC with over voltage and phase-reversal protection;
- 8 digital inputs, compatible dry and wet contact, DIN0 can be used as high speed pulse counter max 1MHz,DIN1-3 can be used as low speed pulse counter max 1KHz.DIN1 can arm and disarm ;
- 6 analog inputs, 24bit resolution, compatibles 0/4~20mA, 0~5V, can change to PT100 Resistance Temperature Detectors;
- 4 relay output (5A/30VDC, 5A/250VAC), compatibles pulse outputs;
- 1 temperature & humidity sensor input for monitoring onsite environment, the sensor model is AM2301, Measures temperature from -40-80°C,0.5°C accuracy, Relative Humidity from 0-99RH%, accuracy is 3%;
- Inbuilt inter-lock logic programmer and powerful timer program function;
- Resend the data while communication failure and alert to users by SMS;
- Embedded TCP/IP protocol stack, support TCP/UDP, Modbus TCP, Modbus RTU over TCP , KingPigeon IoT RTU protocol and transparent transmission function, support self-defined handshake protocol active connecting server and automatically reconnect the server function after connection failure;
- Built-in TCP listening port, can be used as a TCP server, supports up to 5 terminal accesses;
- With dual SIM interface: SIM card 1 active, SIM 2 standby mode, improve communication quality;
- Supports RJ45 Ethernet port for connect internet;
- 2 RS485 port, supports Modbus RTU Master and Slave, can be used to extend I/O ports or meters;
- Supports SMS Alert when I/O triggered or recovery, and external power lost or recovery;
- Provides 1 channel 9~36VDC power source output for external device, saving wiring cost;
- Up to 10 SMS Alert and dial numbers, can program to receive specified alarm message,10 authorized numbers can switch on/off device with a free charge call at the specified time;
- Inbuilt 8G SD card to save up to 100000 historical data and events;
- Inbuilt large capacity automatically rechargeable backup battery;
- Using metal shell, protection class IP30. Metal shell and system security isolation, especially suitable for industrial applications in the field;
- L70 * W87 * H52mm, compatible wall installation and DIN35mm industrial rail installation.

4. 2 Specifications

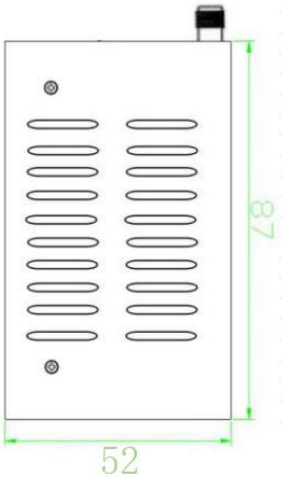
Item	Reference Scope
DC Power supply	Standard adapter: DC 12V/2A Range 9-36VDC
Power consumption	Standby:12V/130mA; Working Max.: 12V/500mA
GSM Frequency	850/900/1800/1900Mhz
3G/4G	Optional: WCDMA/TDD-LTE/FDD-LTE
TCP/IP stack	TCP,UDP
SIM interface	Dual SIM Card,supporting 3V and 1.8V SIM Card
External antenna	SMA Antenna interface, 50 Ohm, Gain: 3dB
Serial Interfaces	1 USB Port
Protocols	SMS, GPRS UDP,TCP,MQTT, Modbus RTU, Modbus TCP and more equipment protocols can be added according to requirements.
Ethernet	1 RJ45 Ethernet port for connect internet.
RS485	2 RS485, Support Transparent transmission and Modbus RTU Slave, Modbus RTU Master.
Digital Inputs	8 Digital input, NC/NO type,wet /dry contact .DIN0 can be used as high speed pulse counter max 1MHz,DIN1-3 can be used as low speed pulse counter max 1KHz.DIN1 can arm and disarm.
Analog Inputs	6 Analog Inputs. 24 bit resolution, 0-5V or 0-20mA or 4-20mA;
Temp.&Hum Inputs	Temperature range: -40°C to +80°C, Humidity Range: 0~100%RH;
Relay Outputs	4, Rated: 5A/30VDC,5A/250VAC
Power Outputs	1 Port, for external device;
Extend I/O tags	Max.320
Memory Capacity	Internal 8G SD card inside, can save the data for 100000events.
Backup Battery	3.7V 900mAH
Temperature range	-20°C ~ +70 °C
Humidity range	Relative humidity 95% (condensation free)
Exterior dimension	70mm*87mm*52mm
Net Weight	350g

5. Physical Layout and Installation Diagram

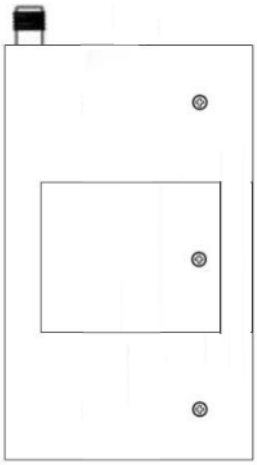
5.1 Control Unit size



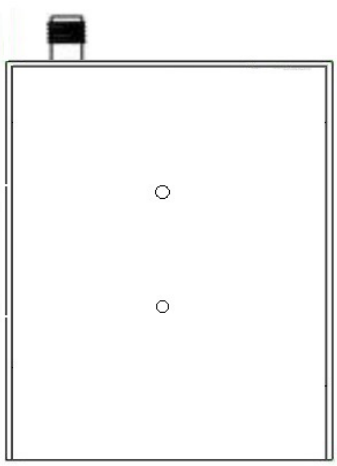
(Front view)



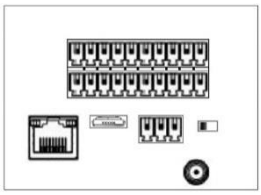
(Left side view)



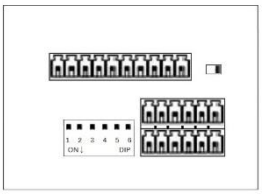
(Right side view)



(Back view)

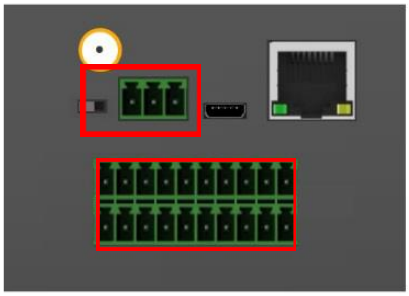


(Vertical view)

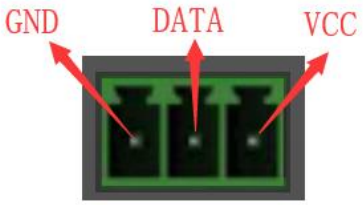


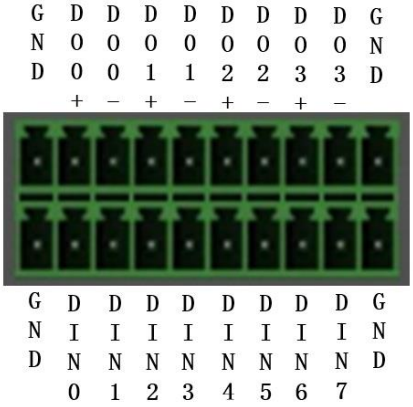
(Bottom view)

5.2 Interface definition

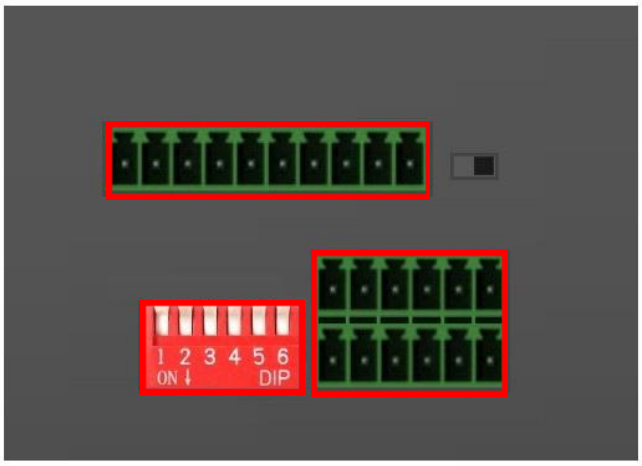


S/N	Function	Description
1	GND	Negative electrode
2	DATA	Temp/humi data
3	VCC	Temp/humi Power

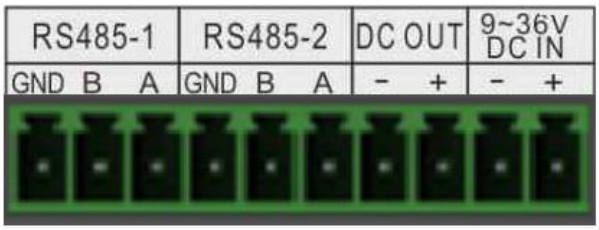


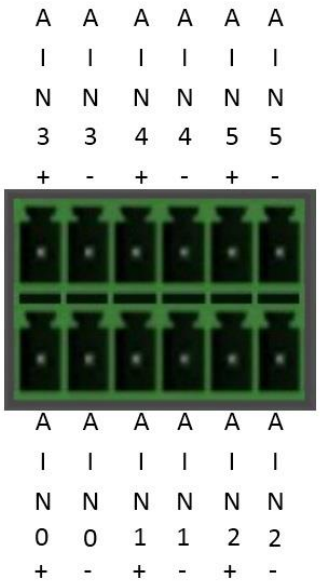


S/N	Function	Description
4	GND	GND
5	DO0+	1st relay output +
6	DO0-	1st relay output -
7	DO1+	2nd relay output +
8	DO1-	2nd relay output -
9	DO2+	3rd relay output +
10	DO2-	3rd relay output -
11	DO3+	4th relay output +
12	DO3-	4th relay output -
13	GND	GND
14	GND	GND
15	DIN0	1st digital input
16	DIN1	2nd digital input
17	DIN2	3rd digital input
18	DIN3	4th digital input
19	DIN4	5th digital input
20	DIN5	6th digital input
21	DIN6	7th digital input
22	DIN7	8th digital input
23	GND	GND

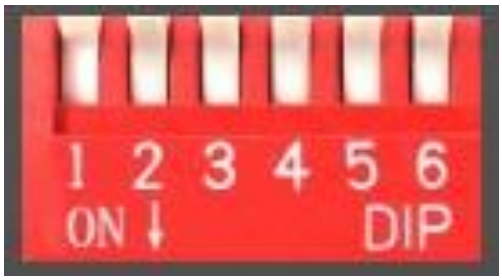


S/N	Function	Description
24	GND	GND
25	485_1 B	485_1 B data-
26	485_1 A	485_1 A data+
27	GND	GND for input
28	485_2 B	485_2 B data-
29	485_2 A	485_2 A data+
30	DC_OUT -	Power output negative electrode
31	DC_OUT +	Power output port, positive electrode
32	DC_IN -	Power input negative electrode.
33	DC_IN +	Power input positive electrode.





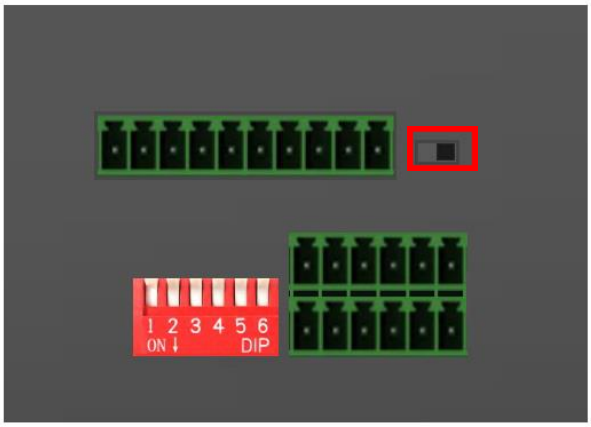
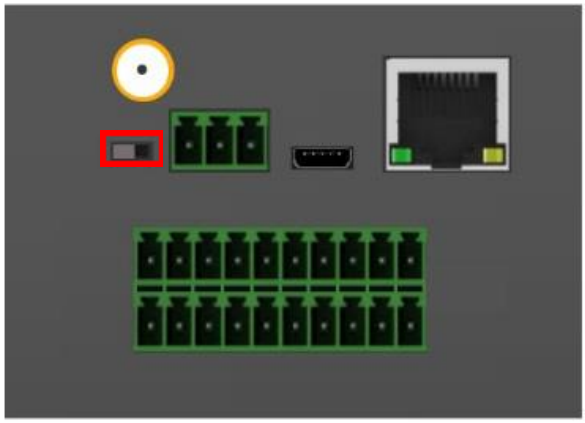
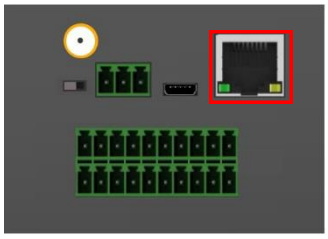
S/N	Function	Description
34	AIN3+	4th analog input +
35	AIN3-	4th analog input -
36	AIN4+	5th analog input +
37	AIN4-	5th analog input -
38	AIN5+	6th analog input +
39	AIN5-	6th analog input -
40	AIN0+	1st analog input +
41	AIN0-	1st analog input -
42	AIN1+	2nd analog input +
43	AIN1-	2nd analog input -
44	AIN2+	3rd analog input +
45	AIN2-	3rd analog input -



S/N	Description
1	1st analog input switch
2	2nd analog input switch
3	3rd analog input switch
4	4th analog input switch
5	5th analog input switch
6	6th analog input switch
Note: Switch to ON (down side), stands for "4-20mA" type; Switch to OFF (up side), stands for "0-5V" type.	

5.3 LED Indicator Definition

LED Indicator Definition	
	Cellular network indicator. When 2G register network, off 2 seconds, on 0.2s and so on; When 3G 4G register network, on 2s, off 0.2s... When light off,stands for communication is abnormal.
Power	RTU status indicator, LED ON when switched RTU on..
Alarm	Alarm Indicator, alarm will ON and flick. Normally is OFF;
Run	RTU running status indicator, ON or OFF stands for RTU halted, flicks slowly stands for RTU is running.
Status	Arm/Disarmed Indicator, Arm is ON, disarmed is OFF.
RS485-1	When transmitting data by RS485, the LED will flick, otherwise, it is off.
RS485-2	When transmitting data by RS485, the LED will flick, otherwise, it is off.

Switch & Button Definition	
	
Power Switch	For switch ON/OFF the RTU
	
Upgrade Firmware Switch	For upgrade firmware purpose only. Only when upgrade new firmware version will use it, otherwise keep it at Work Side all the time.
SIM Card Slot	
	
Dual SIM Card Slot	For SIM Card Installation, supports 3V/1.8V Nano SIM Card. Note:Turn off the device when insert or remove the SIM card.
Ethernet Connector Definition(only for S47X)	
	
Ethernet	Rate indicator(green): Light ON stands for 100Mbps;OFF stands for 10Mbps.

	Link indicator(yellow):Light ON stands for connected;OFF stands for disconnect; Flick stands for transmitting data.
ATN Port Connector Definition	
ATN	GSM/3G/4G Antenna connector, 50Ohm, SMA male.
USB Port Connector Definition	
USB	USB port, for configuration and upgrading firmware and exporting historical data;

6. Settings&Operation

The Cellular IoT Gateway is user-friendly design, The user can setup it or export historic data by the PC Configuration through USB cable, and upgrade firmware by USB port. The Cellular IoT Gateway also can be configured some basically parameters by SMS Commands, please refer to **SMS Command List**.

Tips!

1) Please insert the SIM Card firstly, and install the GSM/3G/4G Antenna, please power on to check the LEDs status according to above mentioned LED Definitions, keep switch on it during the programming.

2) Download the software from this link: http://rtu-m2m.com/Download/Software/CP210x_Windows7_8_10_Drivers.zip.

Below is the steps to setup the parameters by PC Configuration, please follow it step by step.

6.1 Start to Configure

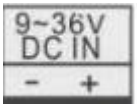
Step1: Install the Configuration software

The Configuration software link: http://rtu-m2m.com/Download/Software/CP210x_Windows7_8_10_Drivers.zip, then installs it on the computer.

Step2: Connection

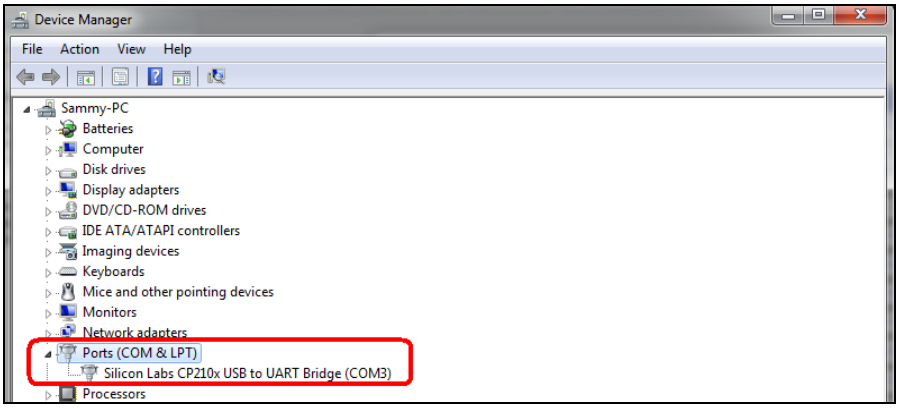
Please insert the SIM Card, and install the GSM/3G/4G Antenna.

Step3: Connect the Gateway to the PC by USB cable. And connect the external DC Power to DC Power Ports, Power on, and switch on the device, see below:



Step4: Install USB Driver

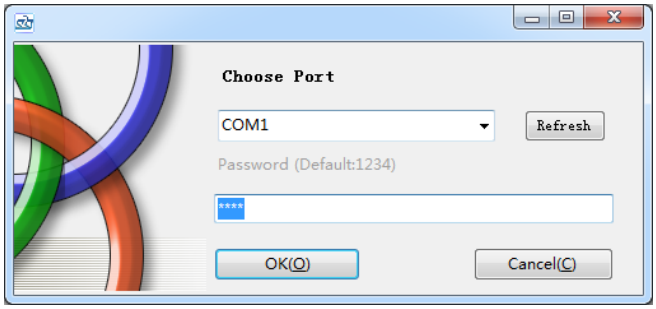
Install the USB Driver to the computer from the CD firstly. When successful, it can be found out at the device manager of the XP or Windows 7 or Win8/Win10, please see the below photo. Also, the driver for different OS can be downloaded from Silicon Laboratories, Inc. http://www.silabs.com , the model is CP210x.



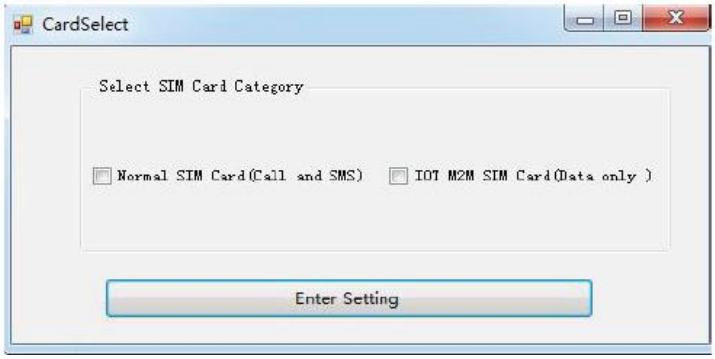
Step5: **Run the Configuration software** (Compatible with Windows XP/7/8/10)

Tips: *In some computer, it required download net framework 4.0 while installation, then please click "Yes" to go to Microsoft website to download this service pack.*

Please click S47X configuration software to run it. Enter the password, default is 1234. Then you can enter the configuration page as below:



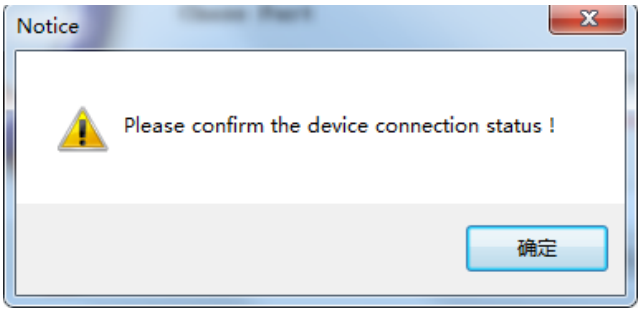
Select Sim card type and click"Enter Setting",after successful login, the software interface is shown in the following figure:



Select the card type of S475 device, the SIM card that supports SMS and phone calls, please select "Normal SIM card", and the SIM card with only data function, please select "IoT M2M SIM card", select "IoT M2M SIM card" and configure The software will disable all functions related to SMS and phone calls.
If the device is S475E, please select "IoT M2M SIM Card".

Notice:

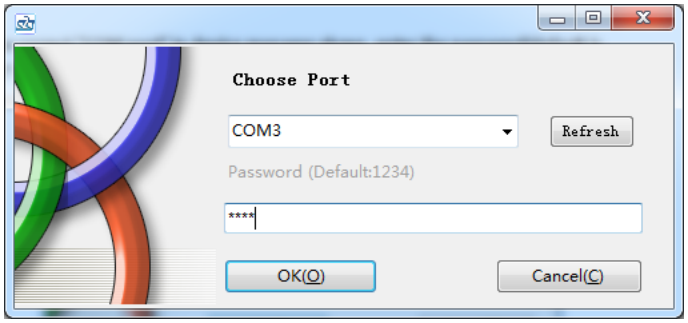
If display the below windows, then means the RTU connect to the PC failure. The reasons are below:



1) *USB Driver installation failure;*
2) *USB Cable connection is disconnected;*
3) *The Upgrade Firmware Switch at Load side, not at Work side.*
4) *Power Switch switched off or DC Power Connection is disconnected.*

Step6: **Choose the correct "COM port" in device manager above, enter the password(default is 1234),click the "OK" to connect and start to program**

Details please check the picture as below:



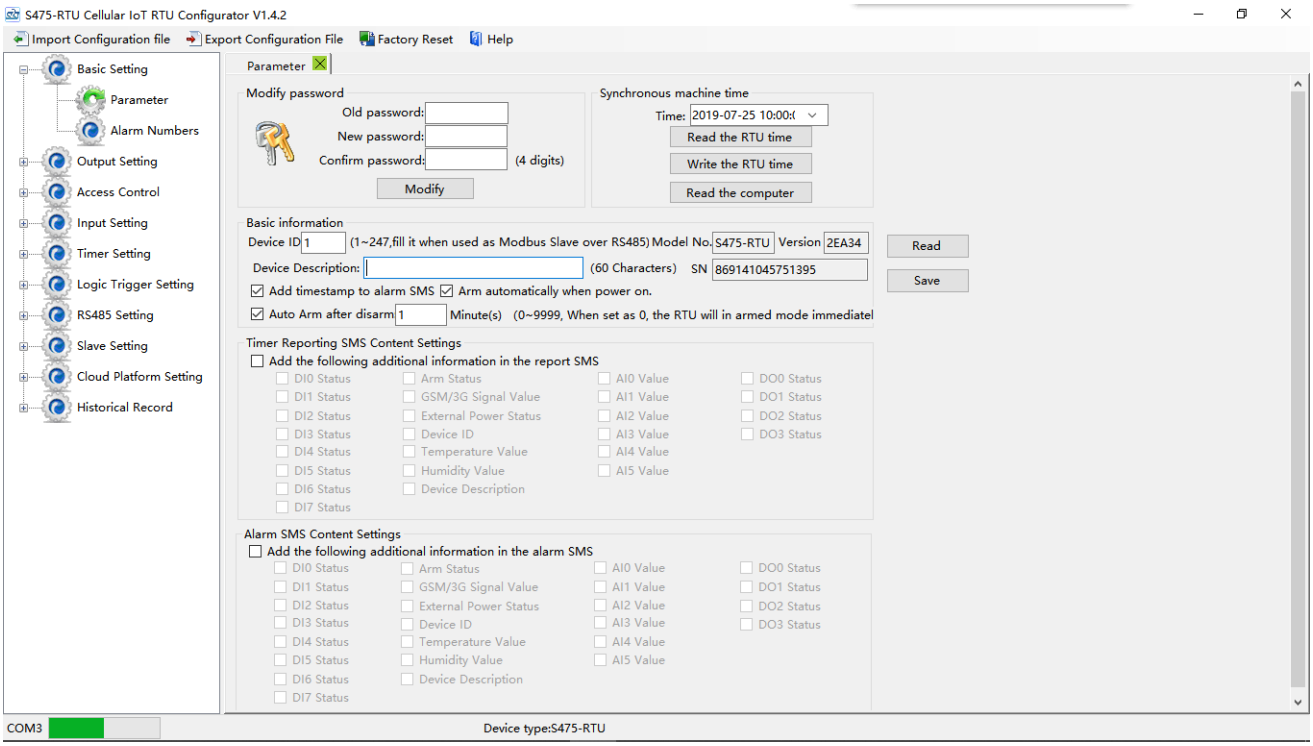
Tips: *If not connect successfully, will not enter into next step. Pls check if USB connect well, or COM port and password correct or not.*

6.2 Setting Self-checking

Phenomenon	Possible Reason
Can't enter software	*1. USB Driver installation failure;* *2. COM Port not correct or USB driver installation failure;*
After switching panel on, only Power light on, panel can't work	*1. The Upgrade Firmware Switch at Load side, not at Work side.* *Solution: Switch the power switch to OFF---->Upgrade switch to Work side----> Power switch to ON;* *2. SD card fall out from the slot.* *Solution: Shake panel to listen if there is voice or not;* *3. In upgrade mode, use upgrade tool erased the firmware.*
Can't enter into working mode	*1. The Upgrade Firmware Switch at Load side, not at Work side.* *Solution: Switch the power switch to OFF---->Upgrade switch to Work side----> Power switch to ON;*
Can't find COM Port	*1. Have not installed driver;* *2. PC system problem cause driver installation failure, can't support Apple OS system.*

	3.Check USB line, and try other common driver software such as "Drive The Life".
In working mode, the device not response the Modbus command	*Have not set the device ID.* *Solution: In setting mode, set device ID---->Switch the device to Run mode.*
After switching panel on, not running according to parameter setting	*After parameter setting, forget to click "Save" button in the menu.* *Solution: Back to Set mode---->Click "Save" Button after setting one page in the menu.*

6.3 Configuration software interface and running



Load Profile: Click it to load additional Profile to the PC Configurator;

Export Profile: Click it to save the present configuration parameters as a profile for next RTU configuration or backup the parameter settings.

Tips: *The Load Profile and Export Profile is very useful while you need to program bulks of RTU with similar parameters. After programmed the first unit then you can export profile to save it, for the second RTU then you can load profile directly to save you time.*

Default: Click it to recovery the parameters to factory defaults.

Notice:

1. After setting or revising parameter, need to click the "Save" button of this page for saving parameters in device

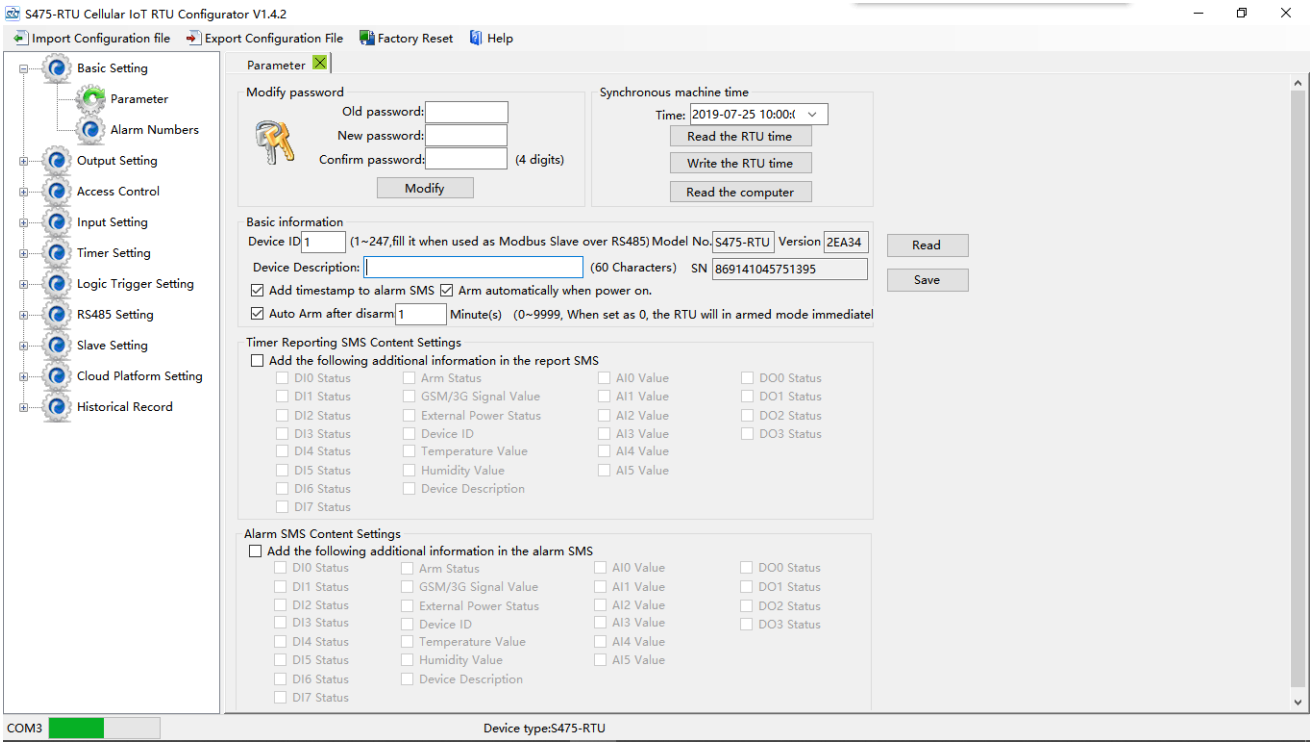
2. Before export profile, need to read Slaves configuration details first, to avoid Slaves information missing.

3.Easy way to revise parameter: Open parameter setting page---->Click "Read" button to get device current value ---->Revise and click "Save" button in the menu.

4. Reboot the device, switch the Power Switch to OFF, then switch it to ON, the device will enter into normal running mode after that.

Basic Settings

Reminder: *Please click the "Read" for previous parameter before starting to set.*



Modify Password: This is for modifying the RTU's Password, default is 1234.

Synchronous machine time: This is to setup the RTU's time for daily report or other timers. After click Write the RTU Time, the RTU will be synchronous the same time as the PC. If connect to King Pigeon Cloud Server, no need this step.

Device ID: Non-necessary. This is mainly for monitoring center to identify the RTU;
If communicate via Modbus protocol, device ID only can be 1~247.

Device Description: This is the description of the RTU, e.g.: installation address, usage instructions and so on.

Add Timestamp to alarm SMS: Tick it stands for while alarm occurrence, the Alarm SMS will include the RTU'S current time information.

Arm automatically when power on: Tick it stands for once the RTU powered up, the RTU will enter into Arm Mode automatically.

Auto arm after disarmed: Fill the timeout to enter into Armed Mode automatically after disarmed operation. This is useful for security protection applications.

Tips:

Arm: *Under this mode, any alarm occurrence will send SMS and dial the authorized numbers immediately, and execute the programmed I/O outputs.*

Disarmed*: Under this mode, alarm occurrence will not send SMS & dial the authorized numbers.*

Timer Reporting SMS Content Settings: Tick the related items to add its value/status to the Timer report SMS contents.

Alarm SMS Content Settings: Ticks the related items to add its value/status to the Alarm SMS Contents.

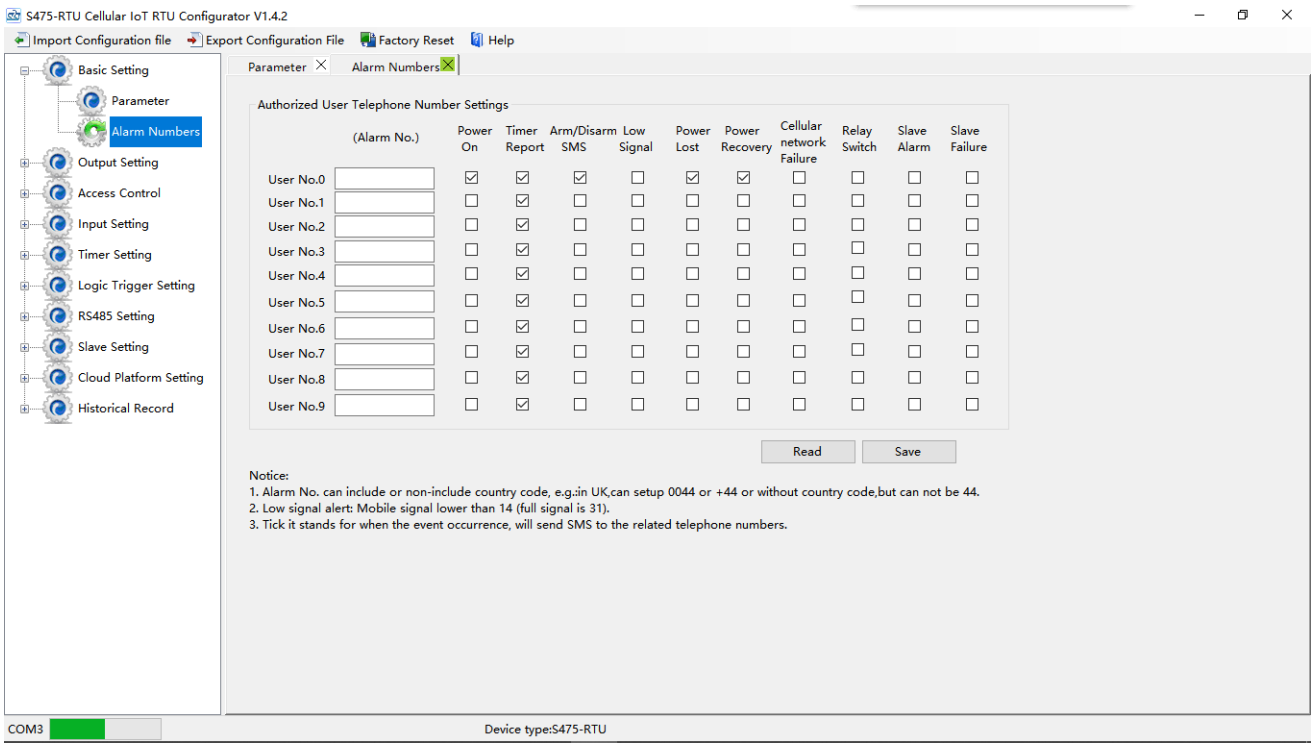
SN:S475 is IMEI number,S475E is null.

Number Settings

This is to setup the Authorized User Telephone Numbers to receive the Alarm SMS or dial. Tick it stands for while the related event alarm occurrence will send SMS to this number.

Reminder:

Please remember that click "Save" button to save it after parameter be written, below pages are the same.



Power On: Tick it stands for while the RTU powered up, will automatically send SMS to this number, include device model, version, description, IMEI, status, signal value etc....

Timer Report: Tick it stands for Timer report SMS will send to this number.

Arm/Disarm SMS: Tick it stands for Arm or Disarm the RTU, will send SMS to this number.

Low Signal: Tick it stands for while GSM/3G/4G Network signal strength lower than 14 will send SMS to this number.

Power Lost: Tick it stands for while external DC Power loss will send SMS to this number.

Power Recovery: Tick it stands for while external DC Power recovery, will send SMS to this number.

Cellular network Failure: Tick it stands for while GPRS connection re-try 3 times and still failure will send SMS to this number.

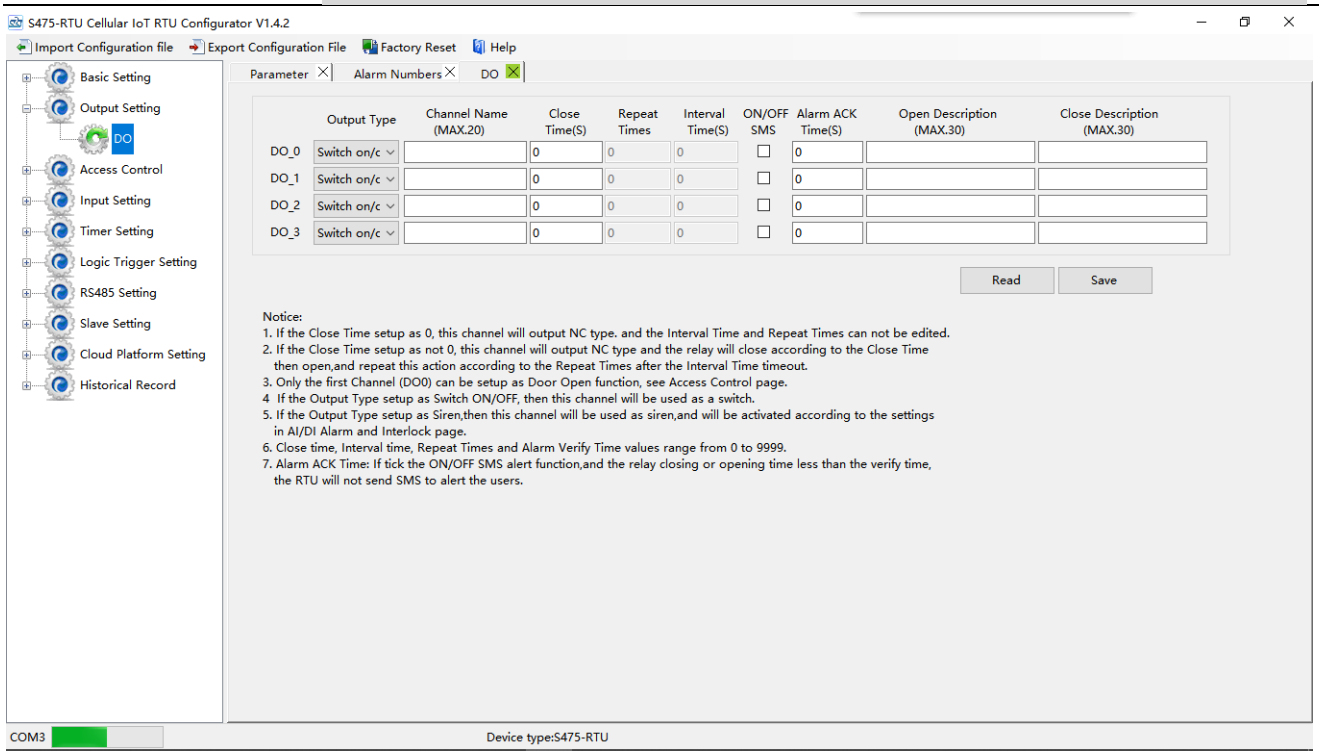
Relay Switch: Tick it stands for while relay is activated,will send SMS to this number.

Slave Alarm: Tick it stands for the salve tag triggered will send SMS to this number.

Slave Failure: Tick it stands for when slave communication failure alarm verify time arrive, will send SMS to this number.

Relay Output (DOUT) Settings

This page is to setup the output parameters and definite the output usages, the outputs will be used in the Interlock Page for programmable logic events.



Output Type: Support 3 output types. The user can choose the output type for the relay outputs, includes Open Door, Switch ON/OFF, Siren. The relay 2 and 3 only used for Switch ON/OFF; Relay 0 can option as Open Door and Switch ON/OFF; Relay 1 can option as Siren and Switch ON/OFF.

1) **Open Door:** Only the first Channel(DO0) can be setup as Open Door, use it for electric lock. If setup as Open Door, then the authorized number calls in RTU, can open the electric Lock directly or output a pulse signal and disarmed the RTU directly. See **Access Control** page about the authorized number.

Notice:

If relay 0 used for Open Door, then can't be action as normal Switch ON/OFF.

Application:

When RTU installed in generator room, many workers out and in, not convenience and safe for everyone taking keys. This function can authorize the person to remotely control the door and disarm the device within appointed time, avoid fault anti-thief alert. After worker maintenance the generator room, can touch the inside Arm/Disarm switch button to arm device, DIN2 can do this.

---

2) **Switch ON/OFF:** For switch on/off device,can be used as a normal timed event, linkage event, and SMS control.
3) **Siren:** This is for output pulse signal for siren sounds, If setup as Siren, then while the RTU alarm and ticked the Siren function in AIN or DIN trigger pages, then this channel will execute the setting parameters.

Channel Name: Setup the Output Channel name, e.g.: Pump or Motor and so on, in order to identify it in SMS Contents.

Open Description: Stands for when the Relay Open, send what SMS to the authorized numbers;

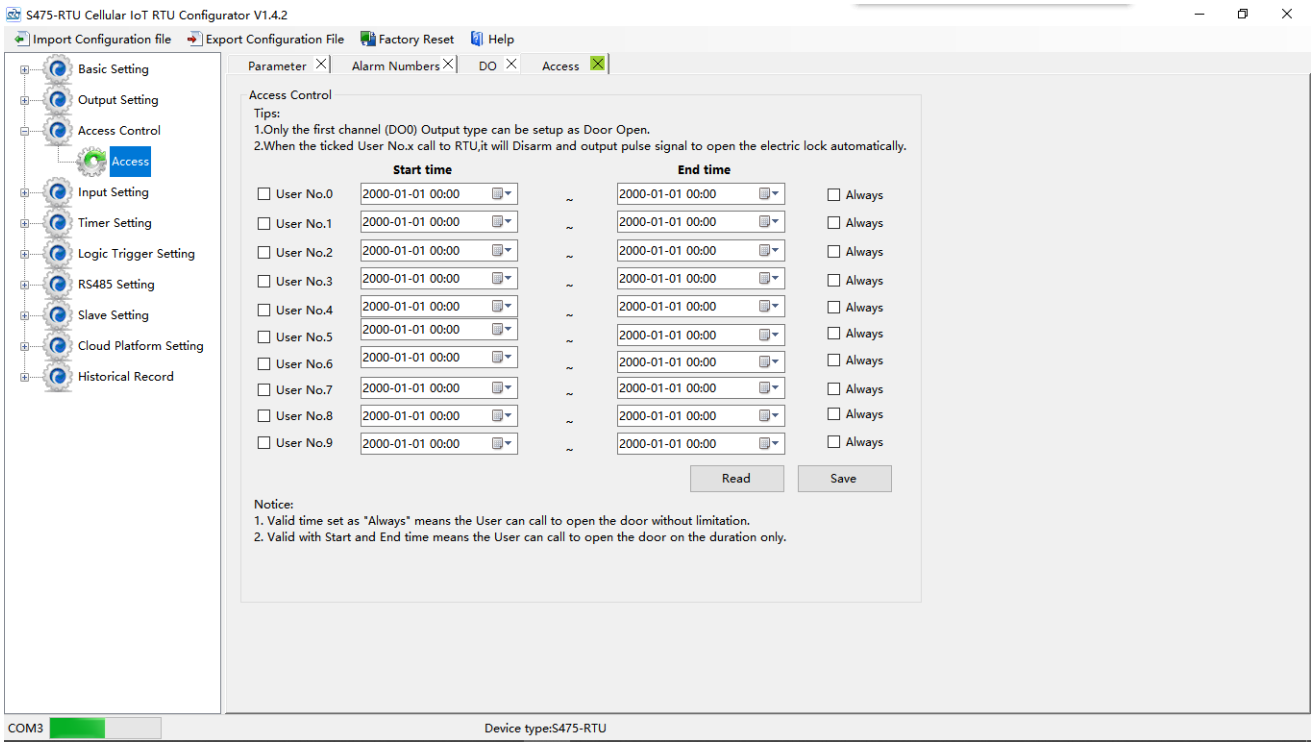
Close Description: Stands for when the Relay Close, send what SMS to the authorized numbers.

Close Time: Stands for the relay close and last time, default 0 second, means always close.

Repeat Times: Stands for how many times does this relay should to repeat.
Interval Time: Stands for interval how many seconds then the relay repeat the action again. Match with "Repeat Times" can work as pulse output, unit: second.
ON/OFF SMS: Tick it stands for while the Recovery action, will also send SMS to the authorized numbers;

Access Control Settings

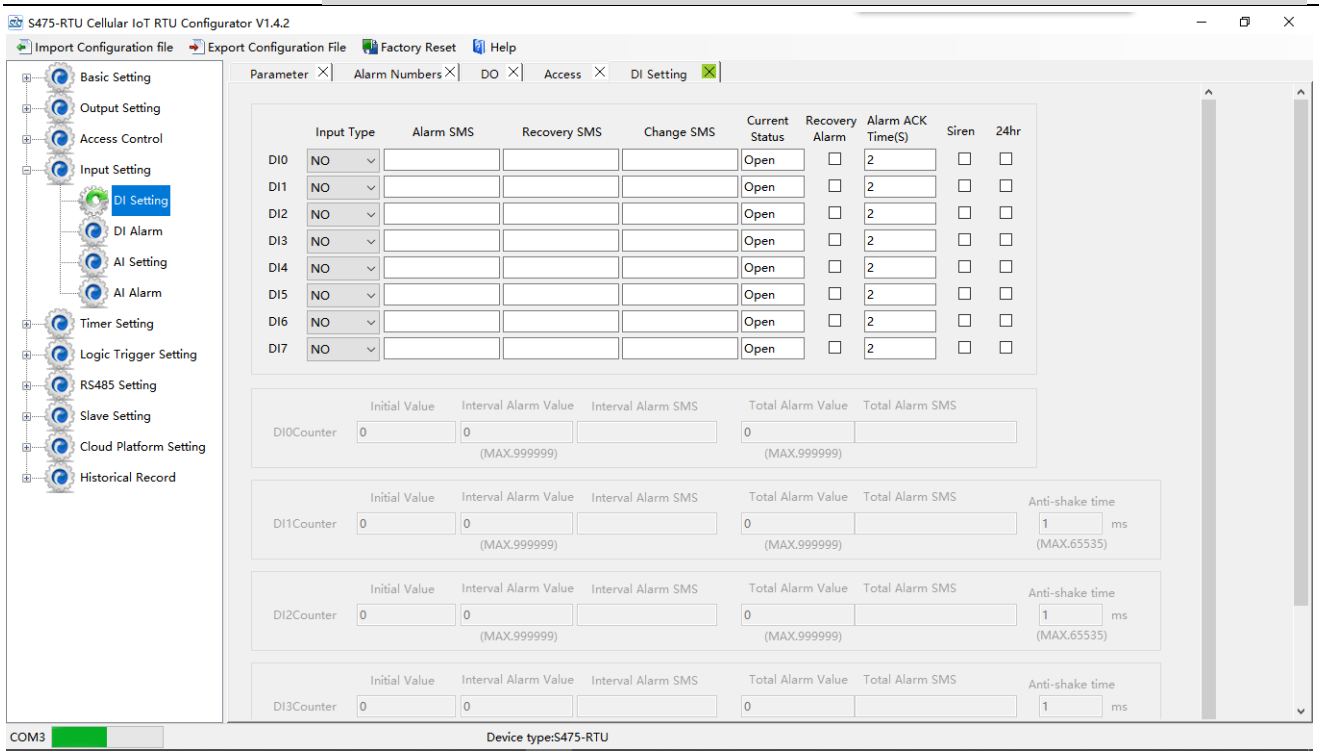
This page is for setting which authorized number at what time can dial to the RTU and let the first channel (DO0) output a pulse output.
Only when the output type of the first channel (DO0) setup as **Open Door** can dial to control it.
It is very useful for serviceman dial to open the electric lock door and disarmed at specified time of the Room. Also this function can be used as authorized number dial in the RTU to output a pulse output or always close then call again to open the relay at specified time. In this condition, please setup the output type of DO0 as **Open Door**, and setup other parameters correctly, and remember to setup the **Auto Arm after Disarmed** time as 0 to keep the RTU in Armed Mode if required.
Tick the box ahead the User No. stands for enable the first Authorized number can dial in to let the first channel (DO0) output a pulse output.



Start Time: Stands for from what time this authorized number can dial in to control it.
End Time: Stands for till what time this authorized number cannot dial in to control it.
Always: Stands for this authorized number can dial in to control it all the time.

DIN Trigger Settings

This page is for setting the digital input alarm conditions and usages.



Input Type: The user can choose the input type for related channel. Includes: Counter, Arm/Disarm, NC, NO, Change and Disabled.

1) **Disabled:** Not use this channel.
2) **NC:** For connecting Normal close type detector, open will alarm.
3) **NO**: For connecting normal open type detector, close will alarm.
4) **Change**: For connecting normal open or normal close type detector, once the status changed, will be treated as alarm.
5) **Counter**: DIN0 can be used as high speed pulse counter max 1MHz,DIN1-3 can be used as low speed pulse counter max 1KHz.DIN1 can arm and disarm. Need to tick up the Pulse Counter box to setup initial value and interval alarm value and total alarm value. E.g.: contact a PIR sensor to count how many people pass through the ATM machine and so on.
6) **Arm/Disarm:** Only the Second Channel (DIN1) can be used as Arm/Disarm Switch. For connecting a pulse output type switch to Arm or Disarmed the RTU.

Alarm SMS: Under Arm or 24h status, once triggered will send this SMS content to authorized numbers.
Recovery SMS: Under Arm or 24h status, if tick the "Recovery Alarm", when triggered digital input recovery normal will send this SMS content to authorize number.
Change SMS: Under Arm or 24hr status, only when digital input choose "Change" type, once action will send this SMS to authorize number.
Current Status: Stands for input's current status.
Alarm ACK Time: Stands for when the digital input Close or Open lasted time more than this value, will be treated as a true alarm, if less than this value, then will not alarm.
Siren: Tick it stands for while this digital input triggering, the DO that output type was setup as **Siren** will execute its output parameters.
24Hr: Tick it stands for no matter the RTU is in Arm or Disarmed mode, this digital input triggered will alarm.
Initial Value: When DIN0-DIN3 as counter, the value begin to count.
Step Alarm Value: DIN0 -DIN3 as counter, under Arm or 24hr status, when counter value arrive

"Step Alarm Value" will send SMS to authorize number.

Total Alarm Value: When counter value arrive "Total Alarm Value", will automatically refresh it to "Initial Value". Under Arm or 24hr status, will call and SMS to authorize number.

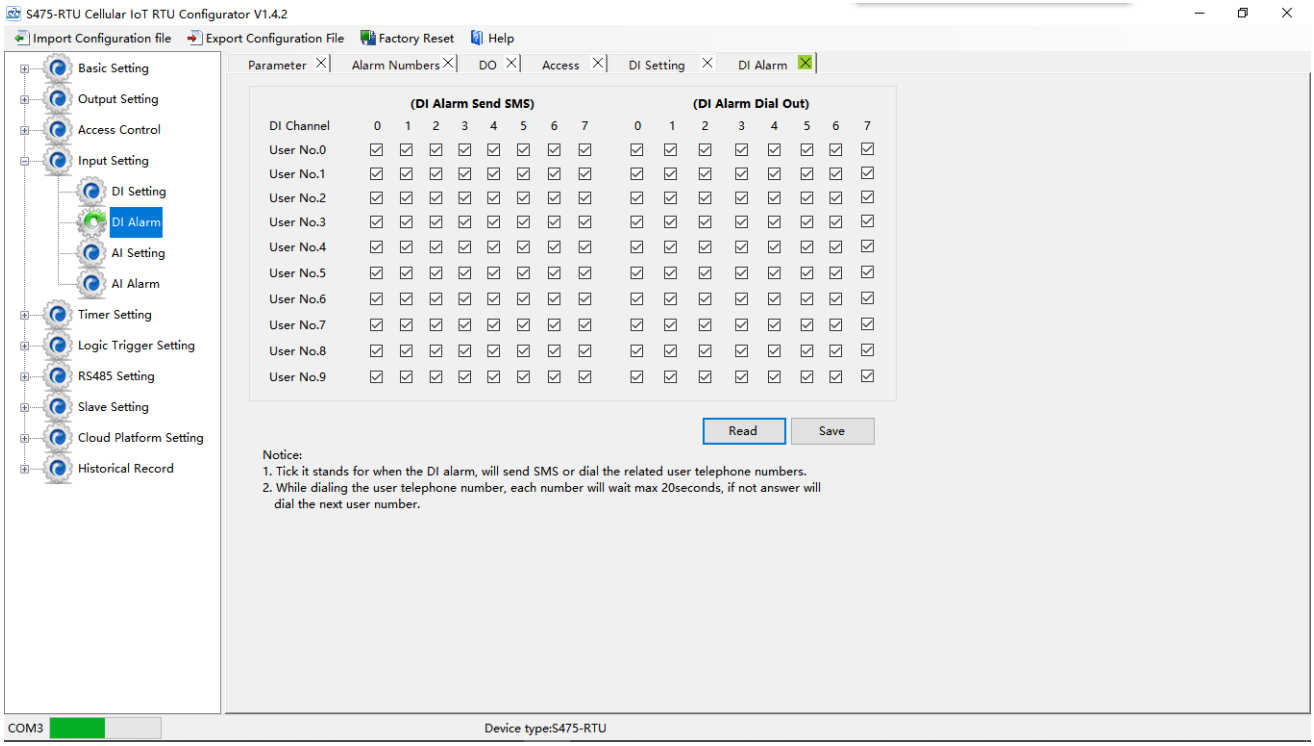
Step Alarm SMS: When step alarm, will send this SMS to authorize number.

Total Alarm SMS: When arrive total max value, will send this SMS to authorize number.

Anti-shake time: Unit is ms, default is 1, which means the maximum pulse sampling frequency is 1KHz.Pulse sampling frequency = 1000 / anti-shake time, such as 1ms corresponds to 1000Hz, 10ms corresponds to 100Hz, 100ms corresponds to 10Hz, 1000ms corresponds to 1Hz

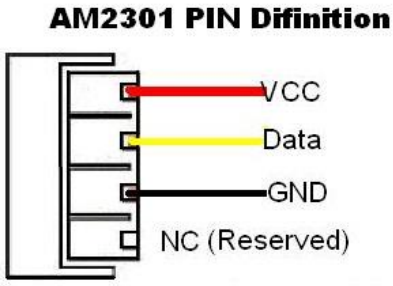
DIN/AIN Alarm Settings

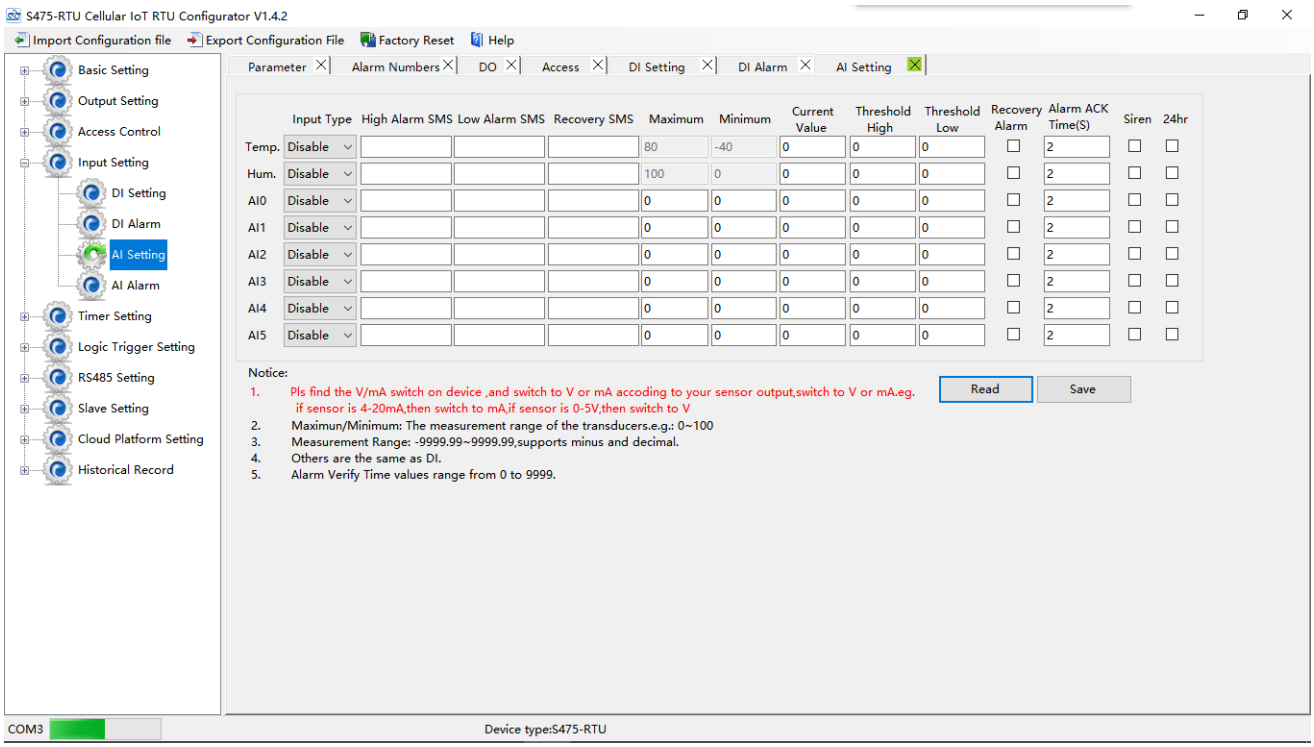
This page is for setup while DIN/AIN alarm, send SMS & Dial to which authorized numbers. Tick it stands for enable to send SMS or dial the related authorized number, see below page is for DIN settings, the AIN Alarm Settings is the same:



AIN Trigger Settings

This page is to setup the analog input alarm conditions and analog input parameter. AIN can be used for monitoring temperature, current, voltage, power factor, water level, pressure, environment, wind speed... And also one channel temperature and humidity transducer can be connected as below:





Input Type: The user can choose the input type for related channel. Includes: Disable, 0~5V, 0~20mA, 4~20mA.

1) **Disabled:** Not use this channel.
2) **0~5V:** For connecting transducers that output voltage 0~5V. Please remember to switch the related channel DIP switch to V side, see **DIP Switch Definitions**.
3) **0~20mA:** For connecting transducers that output current 0~20mA, Please remember to switch the related channel DIP switch to A side, see **DIP Switch Definitions**.
4) **4~20mA**: For connecting For connecting transducers that output current 0~20mA, Please remember to switch the related channel DIP switch to A side, see **DIP Switch Definitions**.
5) **Temperature and Humidity:** Enable/Disable support. Only accept AMS230x series sensor, the temperature maximum is 80, minimum is -40, and Humidity maximum is 100, minimum is 0, cannot change them.

High Alarm SMS: Under Arm or 24h status, once current value higher than threshold high value will send this SMS content to authorized numbers.

Low Alarm SMS: Under Arm or 24h status, once current value lower than threshold low value will send this SMS content to authorized numbers.

Recovery SMS: Under Arm or 24h status, if tick the "Recovery Alarm", when current value recovery normal will send this SMS content to authorize number.

Maximum: The transducer's maximum measure range. E.g.:100 Celsius degree. Usually it can be found out at the transducer's specification.

Minimum: The transducer's minimum measure range. E.g : -50 Celsius degree. Usually it can be found out at the transducer's specification.

Current Value: Stands for input's current value of the transducers.

Threshold High: The high value(reached) need to alarm; Example: set 40Celsius degree to alert.

Threshold Low: The low value(reached) need to alarm; Example: set -10Celsius degree to alert.

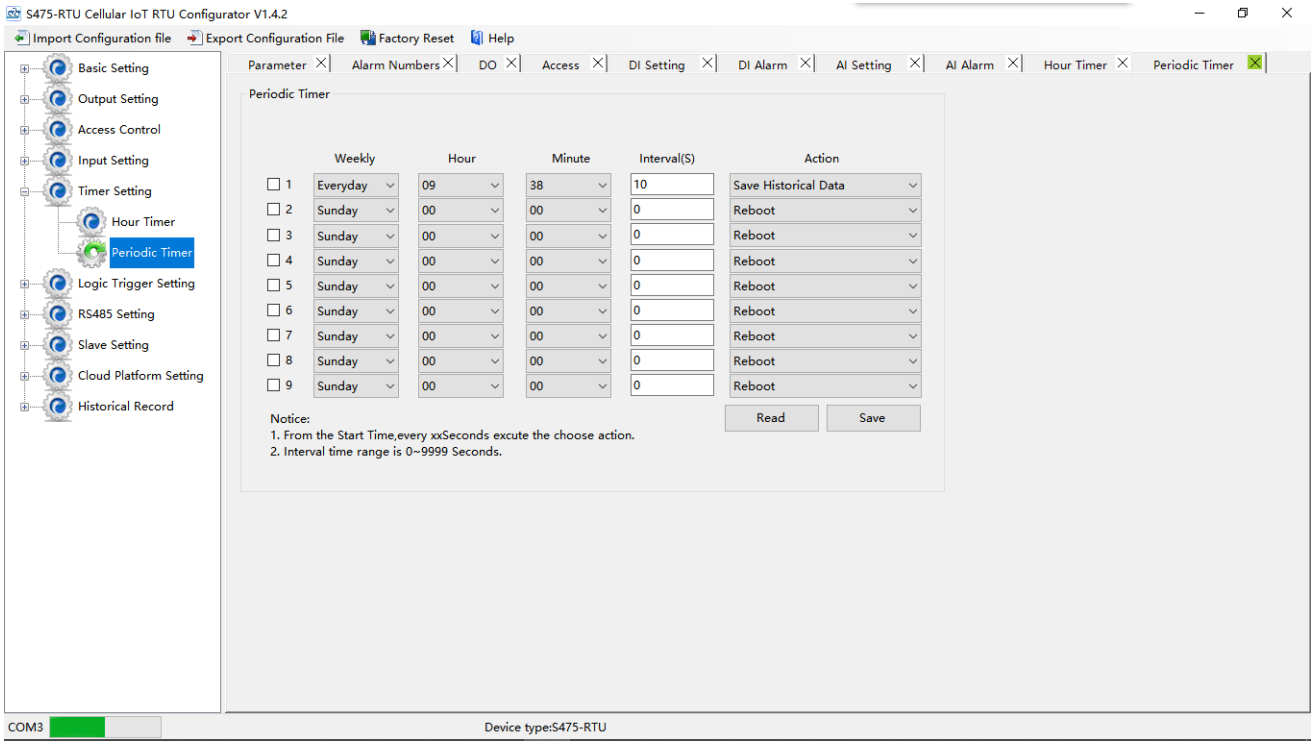
Recovery Alarm: Tick it stands for when the analog input recovery, will send SMS to the authorized numbers.

Siren: Tick it stands for while this input triggering, the DO that output type was setup as **Siren** will execute the its output parameters.

24Hr: Tick it stands for no matter the RTU is in Arm or Disarmed mode, this input triggered will alarm.

Timer Settings

This page is for setup hour timer and periodically timer, it is useful for scheduling when to execute what action automatically or it with repeat this action according to the interval time. Tick it stands for enable this timer event:



Weekly+Hour+Minute: Stands for what day and at what time does the RTU should start to execute the action and interval how many seconds then repeat to execute the action.

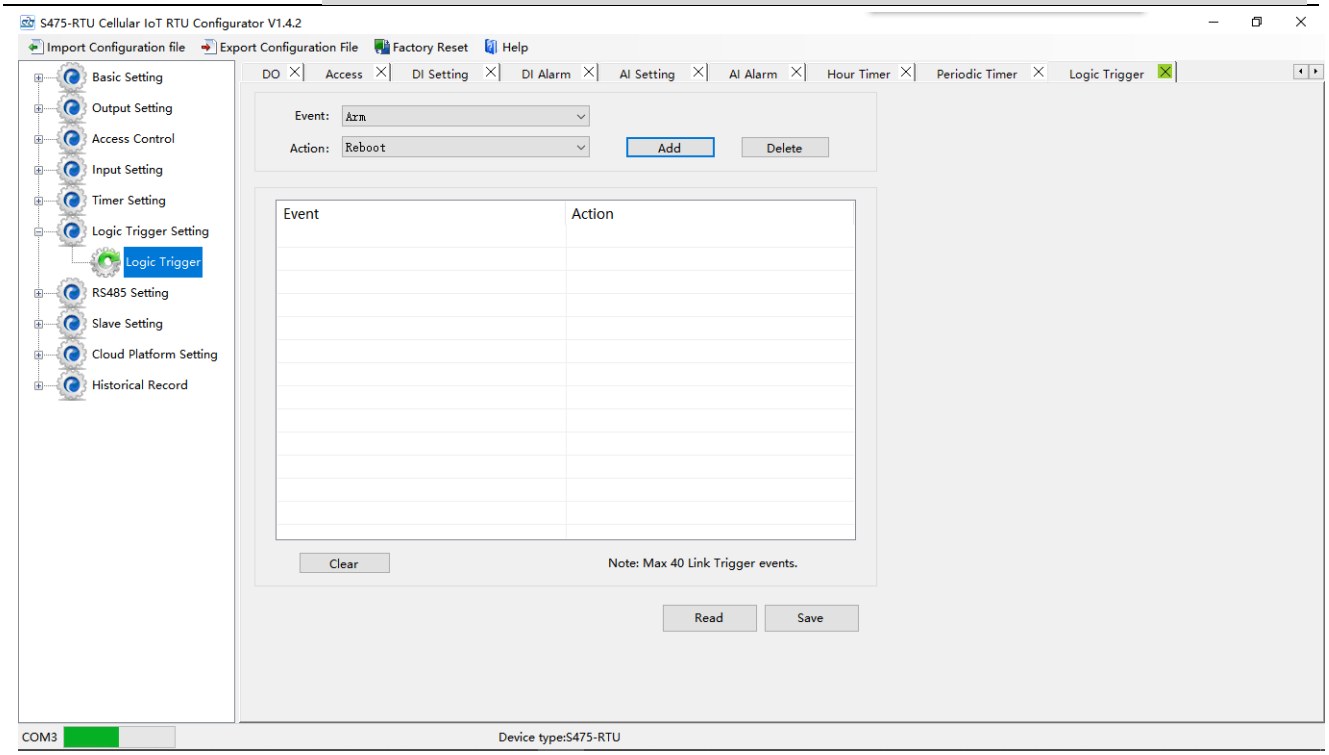
Interval: Stands for interval how many seconds does the RTU should repeat to execute the action. If setup it as 0, then this event will not be repeated.

Action: Stands for what action does the RTU should to execute at the specified time.

Question: *Have set the timer SMS report, but finally not get the SMS.*
Solution: *Have no ticked the "Timer Reporting SMS Content" in first Basic Parameter Settings page.*

Interlock Settings

This page is for setup if what happen, then what action does the RTU should execute, it is a programmable logic events. Total can program up to 40 logic events for automatically control purposes.

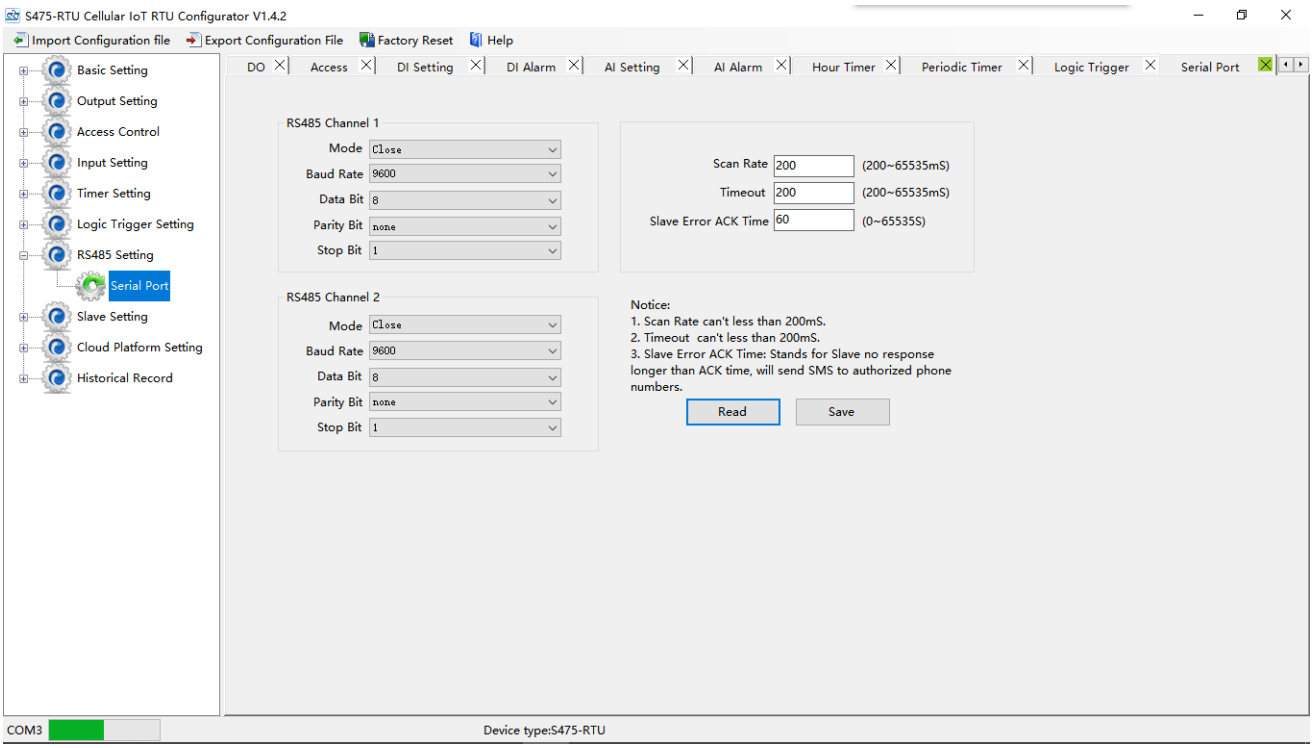


Event: Stands for if this occurrence.

Action: Stands for then what action does the RTU should execute.

RS485 Serial Port Settings

This page is for setup the serial port parameters. Over the RS485, the S475 RTU can be used as Modbus RTU Slave, Modbus RTU Master and transparent transmission.



Modbus RTU Master: Stands for the RS485 used for Modbus RTU Master.

Modbus RTU Slave: Stands for the RS485 used for Modbus RTU Slave, and the "Scan rate", "Time out" and "Slave failure verify time " of Master function will be disable.

Transparent Transmission: The RS485 will transparently transmit serial data without any protocol. It can convert serial port data into IP data or convert it into serial port data through IP data, and then transmit data through wired or wireless network to realize transparent data transmission.

Baud Rate: 1200/2400/4800/9600/19200/38400/57600/115200 optional.

Data Bit: 8 bit.

Parity Bit: None, Even and Odd optional.

Stop Bit: 1 or 2 stop bit optional.

Scan Rate: When RS485 used as Master, the interval time between two polling command.

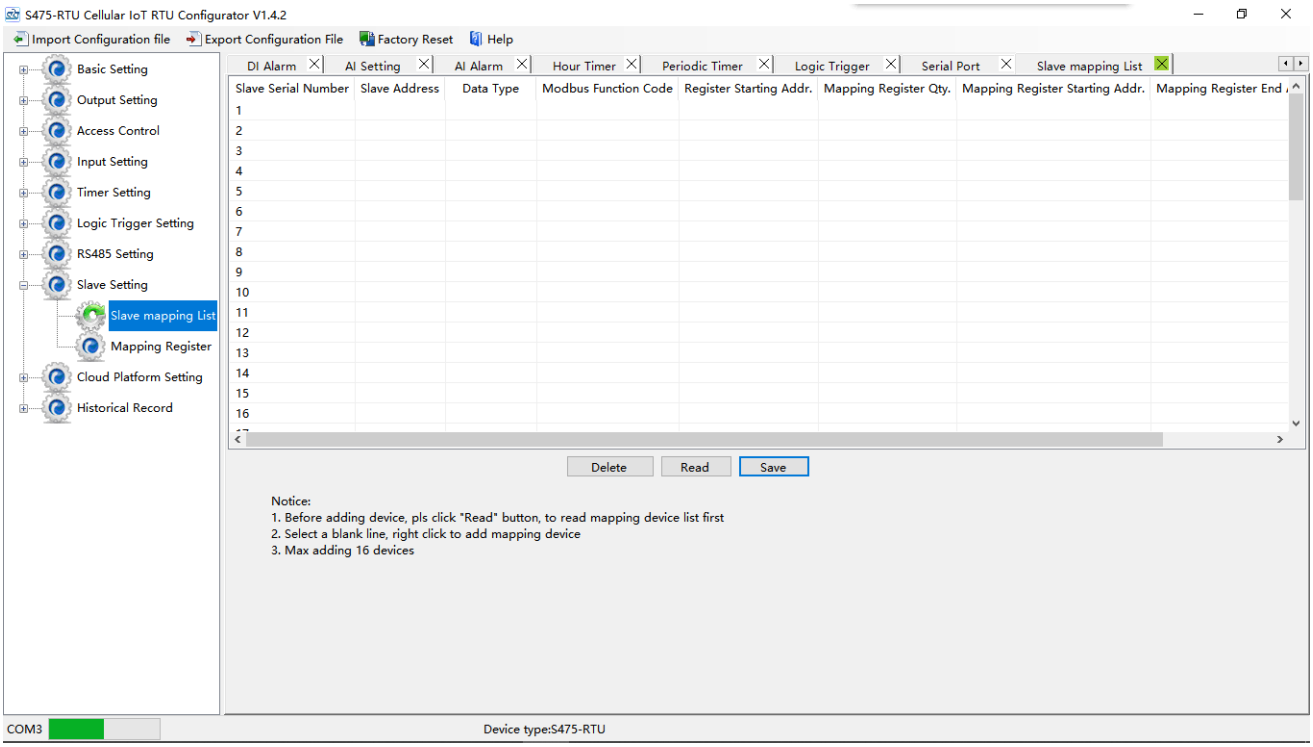
Time out: When RS485 used as Master, after sending command to slave, the longest time waiting for slave data back. If longer than this setting value, will ensure slave no response.

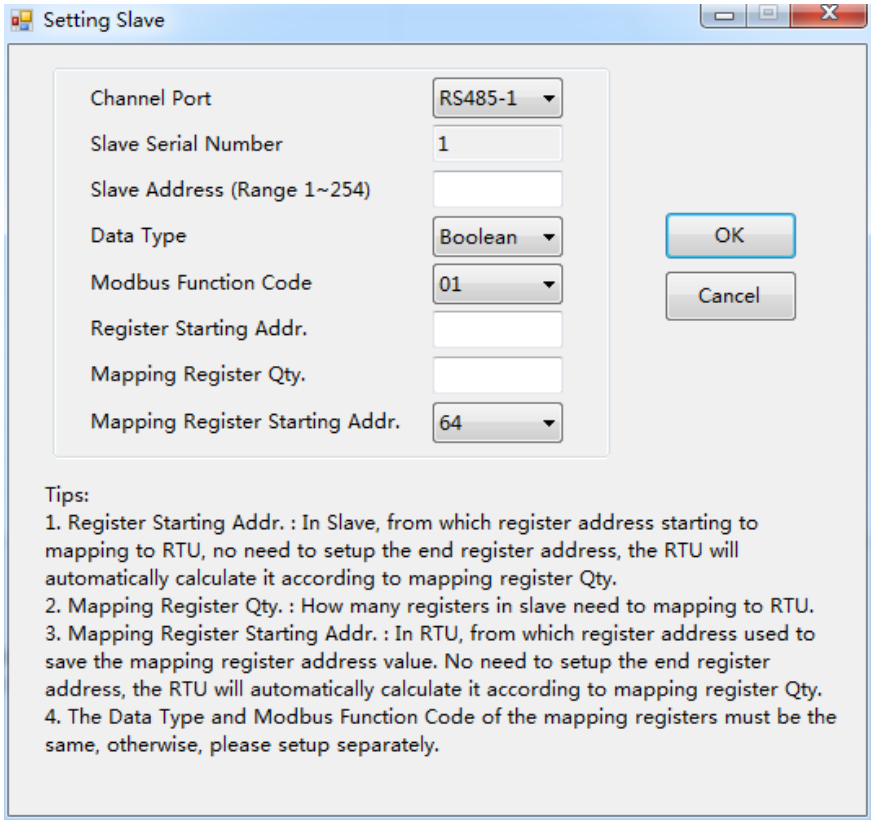
Slave Error ACK time: When RS485 used as Master, if no response time between Master and Slave longer than this value, will send SMS to authorize number.

Slave Settings

This page is for adding, revising and deleting the slaves. When used as Modbus RTU master, slave data mapping can be added to local register. When editing a slave, just select a row and right click to complete the delete, add, modify parameters, etc.

Note: When adding a slave, first read the list of slaves that have been mapped to prevent the new slave covering the added slave device.





Channel Port: The communication way of the slave connected to the RTU.

Slave Serial Number: The number of slave.

Slave Address: Stands for the Modbus RTU Slave ID.

Data Type: Stand for "Boolean", "16 Bit", "32 Bit", "64 Bit".

Modbus Function Code: Stand for Modbus RTU protocol function code, command for slave reading and writing.

Register Starting Address: The starting register address for slave data reading and writing.

Mapping Register Quantity: How many data quantity need to read, used for mapping to device register address.

Mapping Address Starting Address: Stand for mapping the slave starting register data to local device start mapping address.

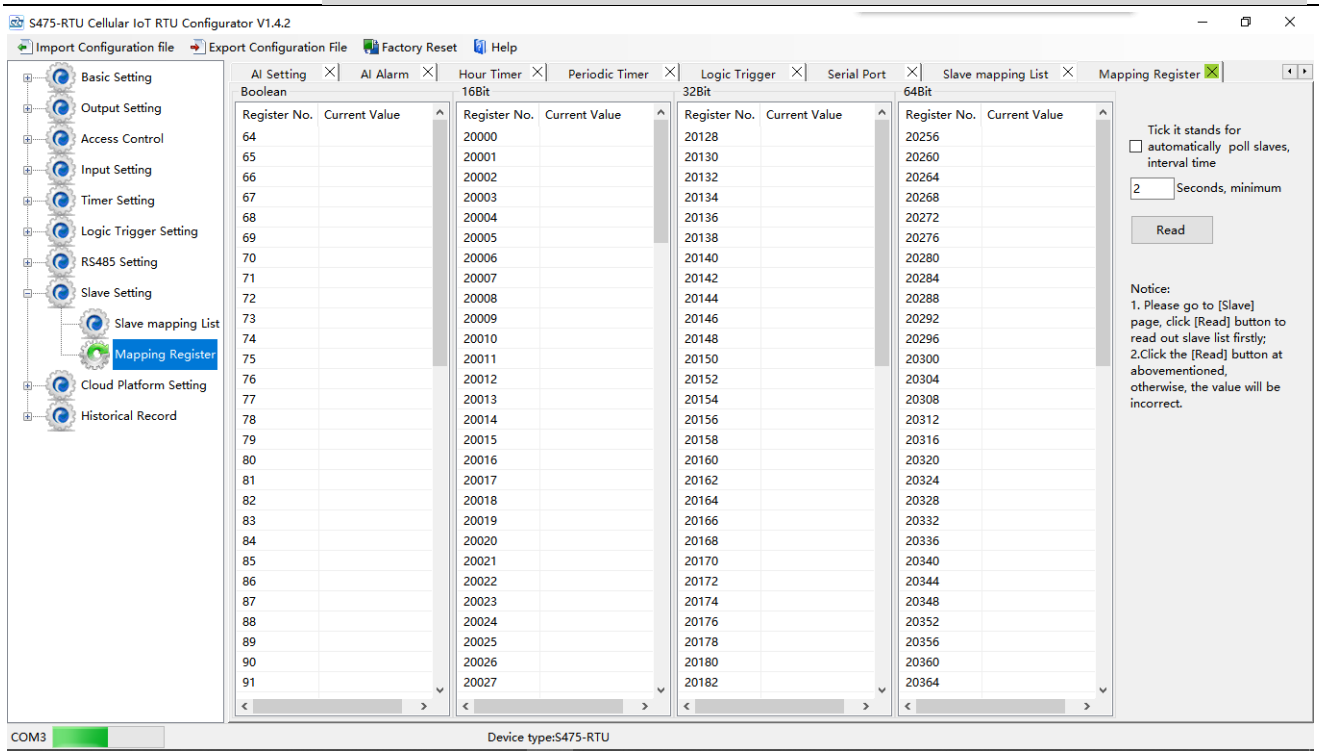
Mapping Address End Address: Calculate the end mapping address according to start address and reading Data quantity.

Register Settings

Click "Register" page to real time check slave current value.

Reminder:

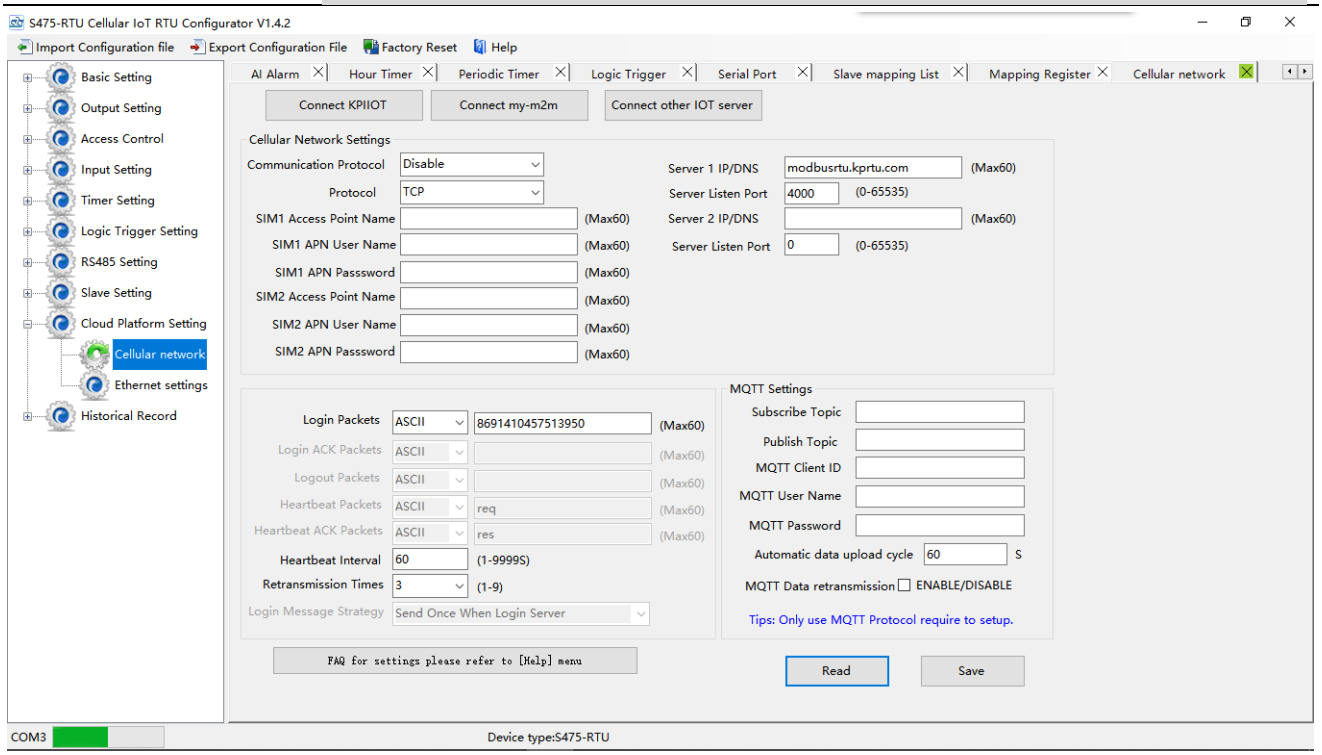
Before reading data, pls read slave list from "Slave Mapping List" first, then can check slave current value in "Register" page:



Cellular network Settings

This page is to configure the function parameters of the device to connect the Internet. The rich automatic handshake login message, self defined heartbeat message and logout mechanism, enable the device to be quickly compatible with a variety of third-party upper computer system. This device can communicate 2-way with the monitoring software or cloud platform in the Internet through GPRS/3G/4G wireless cellular network.

1) Modbus RTU Protocol: Modbus RTU over TCP, communication with upper computer system. For example, connect to www.my-m2m.com cloud server. Domain: modbus.dtuip.com, Port: 6651.
2) Modbus TCP Protocol: Communication with upper computer system via modbus TCP. For example, connect to www.my-m2m.com cloud server. Domain: modbus.dtuip.com, Port: 6655.
3) King Pigeon IoT RTU protocol: Communication with upper computer system via King Pigeon IoT protocol on TCP. The advantage is that when the device is abnormal, the data can be sent to the host computer immediately, instead of waiting for the host computer to ask for a response. For example, connect to www.rtu-m2m.com cloud platform.



Cellular Data: "Disable", "Modbus RTU protocol", "IoT RTU protocol" or "Modbus TCP protocol" optional.

Protocol: TCP or UDP optional.

Access Point Name: APN, GSM operator provide.

APN User Name: User Name, GSM operator provide.

APN Password: Network password, GSM operator provide.

Sever 1/2 IP/Domain: Server IP address or DNS.

Server Port: Stands for the server's port.

Server Strategy: Only support "Prefer server 1" function, no "Both connection" now. When server 1 disconnect, will connect to server 2 automatically.

Login Packets: Server register handshake protocol package. When transparent transmission or Modbus protocol, this item used for device ID, provided by cloud. Contact King Pigeon sales if need to connect to King Pigeon www.my-m2m.com cloud server.

Login ACK Packets: Once set, device need response within 10 seconds after device send login message, otherwise it will continue sending login message according to "Reconnection Times" ,still not response will offline once time, then try to reconnect, according to "Server Offline 3 Times, Device Reconnection Time".

Logout Packets: Once server send to device, device will be offline.

Heartbeat Packets: Heartbeat content to avoid network offline.

Heartbeat ACK Packets: Once set, device need response within 6 seconds after device send heartbeat message, otherwise it will continue send login message according to "Reconnection Times" ,still not response will offline once time, then try to reconnect, according to "Server Offline 3 Times, Device Reconnection Time".

Heartbeat Interval: Network keep online heartbeat interval time.

Retransmission Times: After setting heartbeat and login message, if server no response, the times which server will send data.

Login Message Strategy: "Send Once When Login Server", "Plus It In Front Of Every Packet", "Both Of Them" optional. "Plus It In Front Of Every Packet" when data transmission.

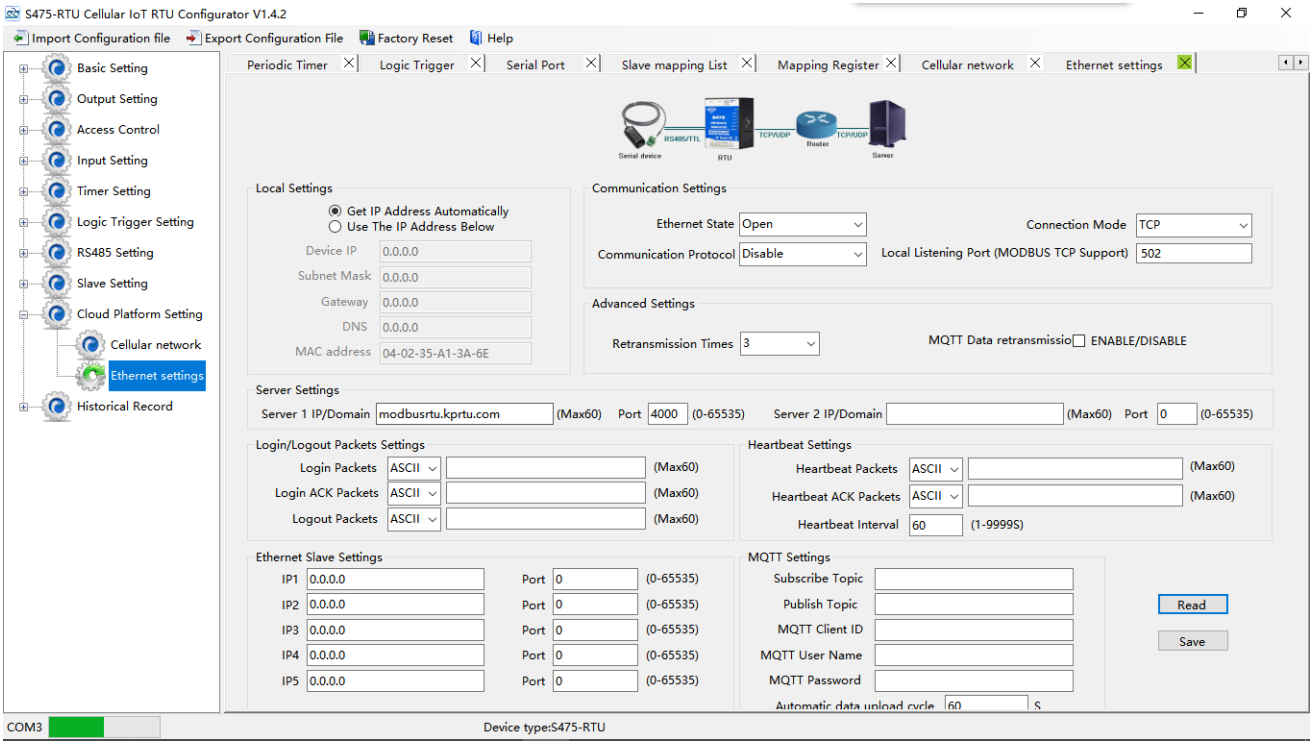
MQTT Setting

Subscribe Topic： S375/S175/S375 subscribe to receive topics

Publish Topic： S375/S175/S375 released themes

MQTT Client ID: The device ID that needs to be subscribed after connecting to the cloud platform through the MQTT protocol.After subscribed, the device will send message to the users. this item used for device ID, provided by cloud.Contact King Pigeon sales if need to connect www.my-m2m.com cloud server.
MQTT User Name: User accounts using the MQTT protocol.
MQTT Password: User password using the MQTT protocol.

Ethernet Settings



Get IP address Automatically: Tick it stands for: the device automatically obtains the IP address in the LAN. Only when the router in the LAN allows the dynamic allocation of IP addresses can be used.
Use The IP Address Below: Tick it stands for the user setup a fixed IP address for the module.

01) Communication Settings
Ethernet State: Open or Close optional.
Communication Protocol: "Disable", "Modbus RTU protocol", "IoT RTU protocol" or "Modbus TCP protocol" optional.
Connection Mode:TCP or UDP optional.
Local Listening Port:it can be used to set a port number to listen to the visitor's data, the default is 502.

02) Advanced Settings
Retransmission Times: After setting heartbeat and login message, if server no response, the times of server resend data.
Server Response Timeout, Device Re-connect Interval Time: Connecting server fail for 3 times, then the interval time of next time reconnecting.

03) Server Settings
Server IP/DNS: Server IP address or DNS.
Port: Stands for the server's port.

Reminder:

Server 1 is primary server, server 2 is backup server; connecting server 1 first; if it is not successfully in 50 seconds, will connect to server 2 automatically; can't "both connect" at a time.

04) Login/Logout Packets Settings

Login Packets: Server register handshake protocol packet. When transparent transmission or Modbus protocol, this item used for identification device ID, provided by cloud. Contact King Pigeon sales if need to connect www.my-m2m.com cloud platform.

Login ACK Packets: Once set, device need response within 10 seconds after device send login message, otherwise it will continue sending login message according to "Reconnection Times" ,still not response will offline once time, then try to reconnect, according to "Server Offline 3 Times, Device Reconnection Time".

Logout Packets: Once server send to device, device will be offline.

05) Heartbeat Settings

Heartbeat Packets: Heartbeat content to avoid network offline.

Heartbeat ACK Packets: Once set, device need response within 6 seconds after device send heartbeat message, otherwise it will continue sending login message according to "Reconnection Times" ,still not response will offline once time, then try to reconnect, according to "Server Offline 3 Times, Device Reconnection Time".

Heartbeat Interval: Network keep online heartbeat interval time.

06) Ethernet Slave Settings

IP: The IP address of Modbus slave.

Port: The port of Modbus slave.

07) MQTT Settings

Subscribe Topic： S375/S175/S375 subscribe to receive topics

Publish Topic： S375/S175/S375 released themes

MQTT Client ID: The device ID that needs to be subscribed after connecting to the cloud platform through the MQTT protocol.After subscribed, the device will send message to the users. this item used for device ID, provided by cloud.Contact King Pigeon sales if need to connect www.my-m2m.com cloud server.

MQTT User Name: User accounts using the MQTT protocol.

MQTT Password: User password using the MQTT protocol.

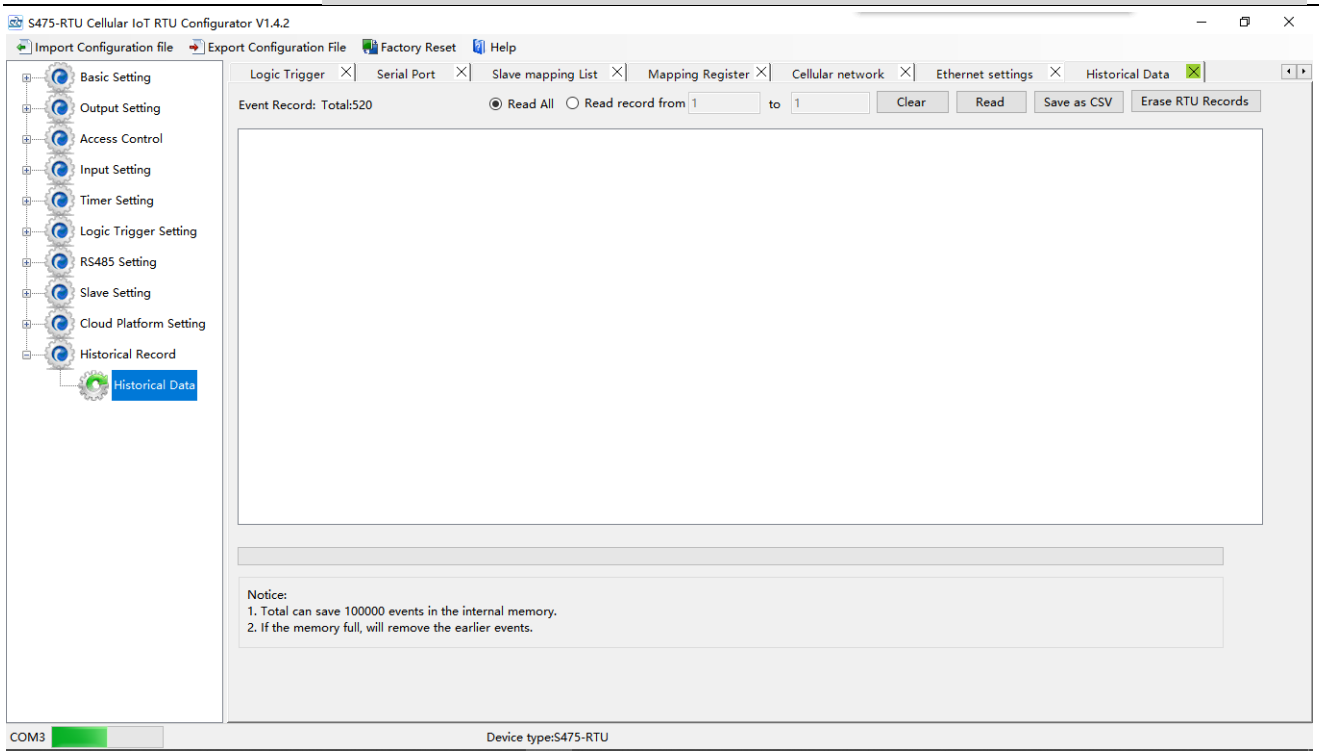
Automatic data upload cycle: Default is 60s

MQTT data retransmission: When the network is disconnected, the data will be stored, and the data will be reissued to the server after coming to the network

Historical Record

The device inbuilt 8G SD card, store alarm and historical records. For saving historical records, need to set the saving historical records interval time in "Periodically Timer" page.

For historical record, once full, will automatically remove the earlier records for new records. And can save as CS format for other purpose usage.



Event Recode: Display device current historical records qty, "Read All" or "Read Record from xx to xx" optional.

Clear: Clear the screen.

Read: Read historical records.

Save as CSV: Historical records export as CSV file.

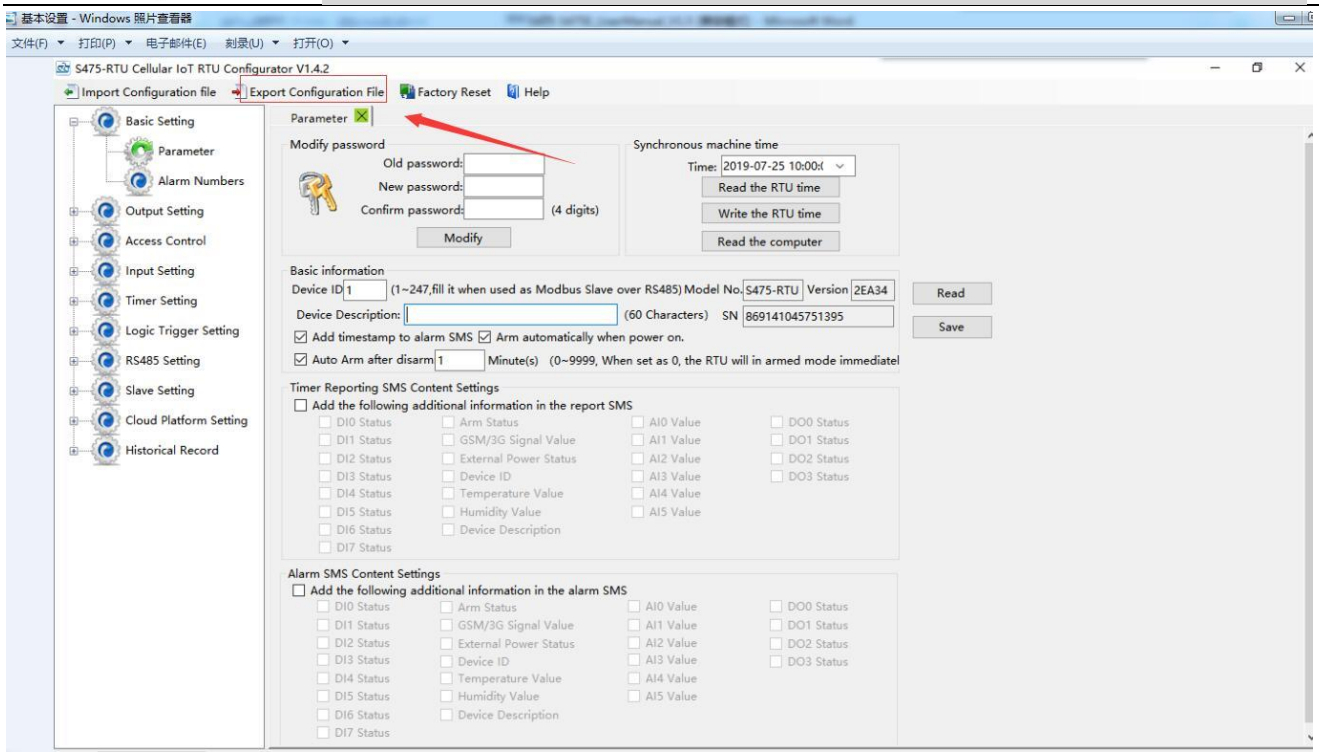
Erase RTU Records: Click this button will erase all device historical records, be careful.

7.Configuration and Reset

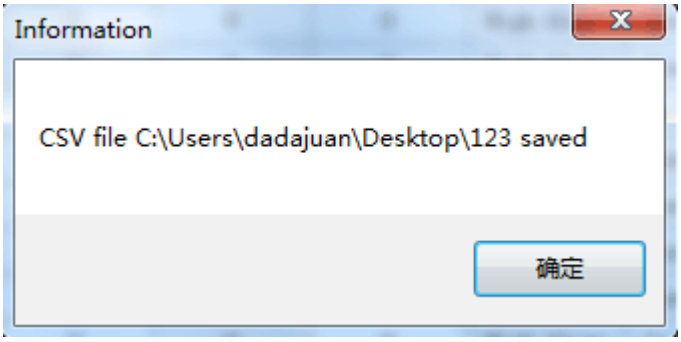
The Load Profile and Export Profile is very useful while you need to program bulks of RTU with similar parameters. The “Default” function can reset the device to factory default status.

7.1 Export Profile

Click “Export Profile” button----> *chose the path and input the name to save.*

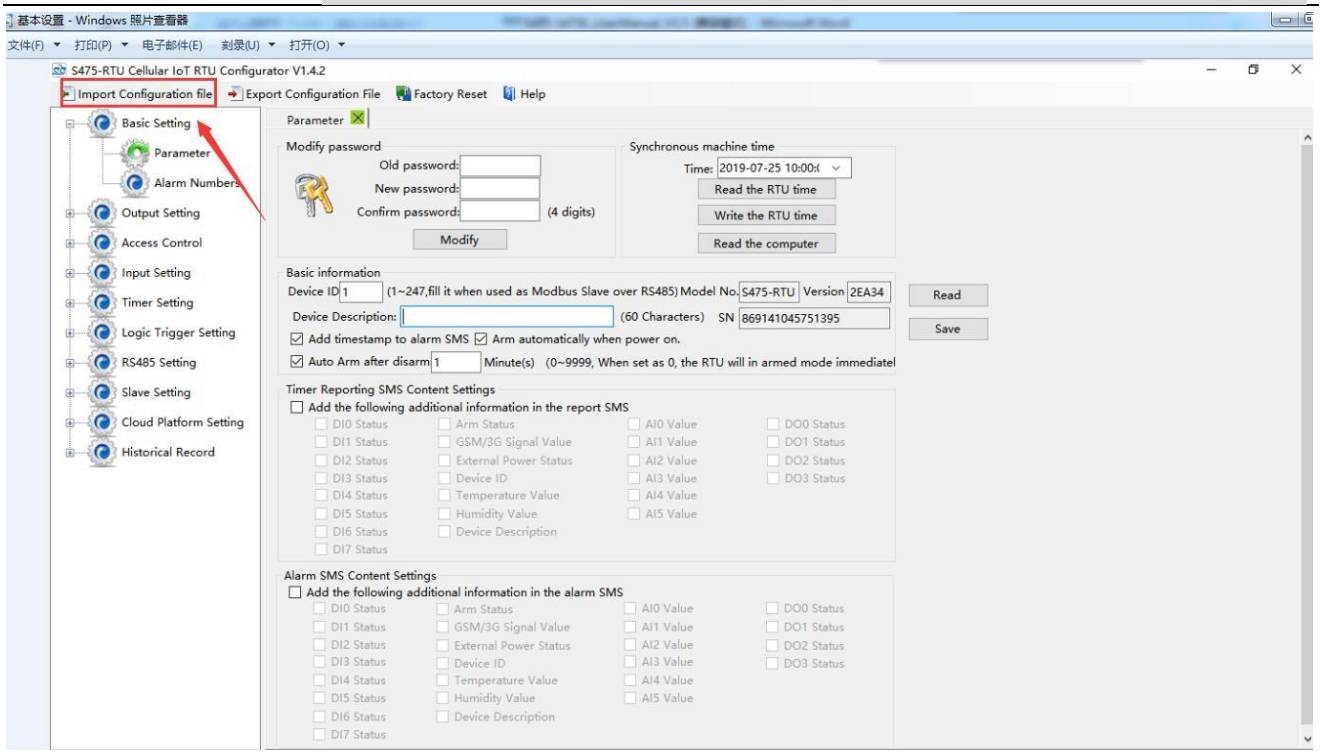


Then it will display as below after a moment:

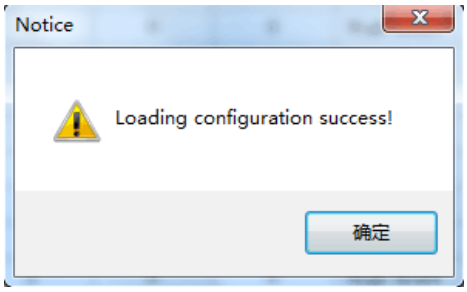


7.2 Load Profile

Click “Load Profile” button----> *chose the file which need to load.*



Then it will display as below after a moment:



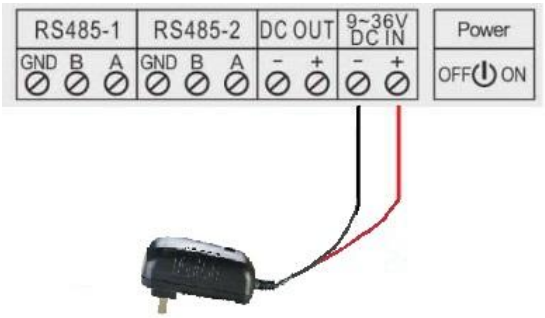
7.3 Reset

When device is on, connect the PC configuration software, click the “Default” button on software to reset.
It will restore all parameters of the device to the factory default initial value.Please contact King Pigeon sales if forget password,website www.iot-solution.com.

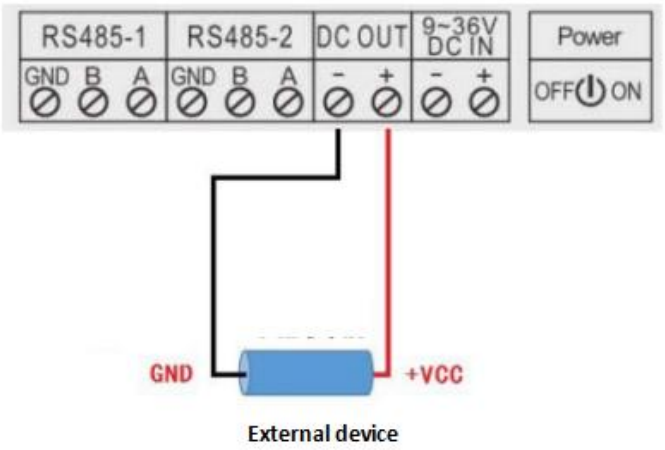
8. Connection and Application

8.1 Wire Connection

8.1.1 Power wire connection:

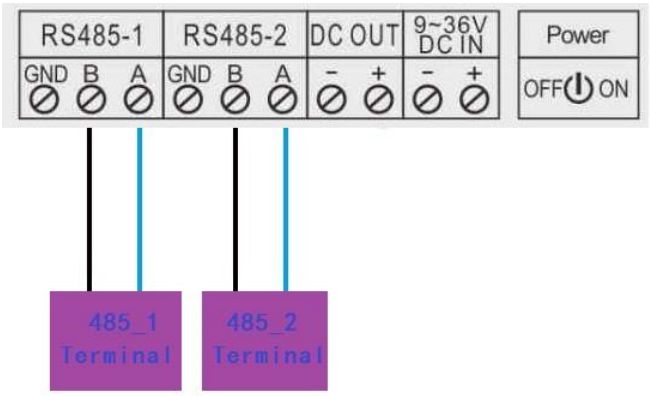


8.1.2 DC output



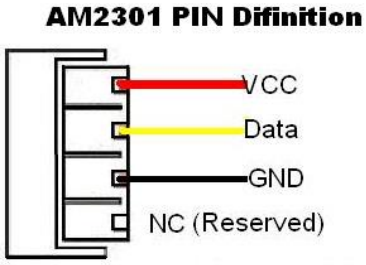
8.1.3 RS485

S47X supports two RS485 ports for communication, connection as below:

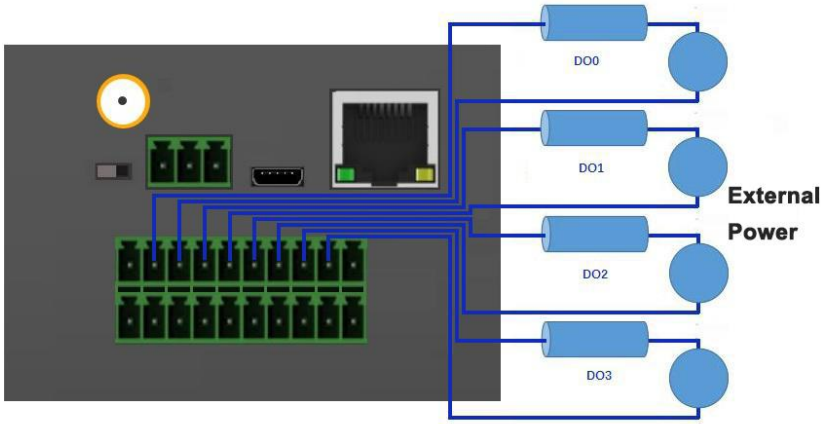


8.1.4 Temperature/Humidity input

S47X supports one channel temperature and humidity input for sensor AM230X as below:

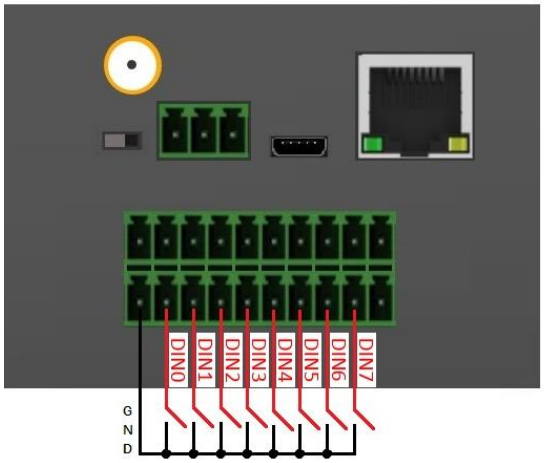


DO

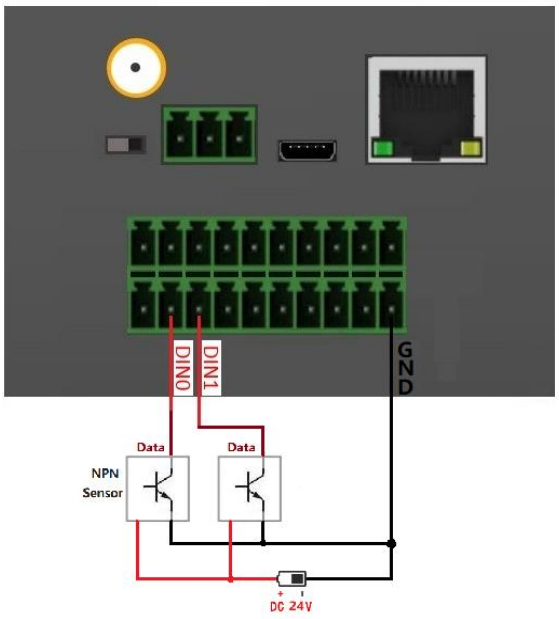


DIN

Dry contact:

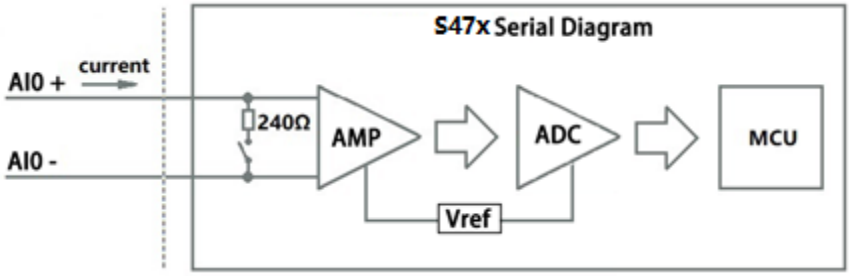


Wet contact:

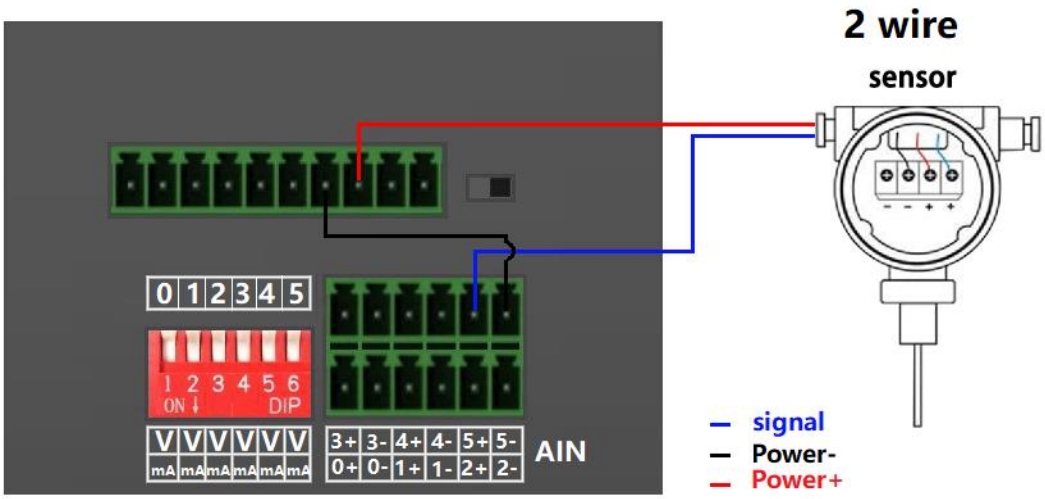


AIN

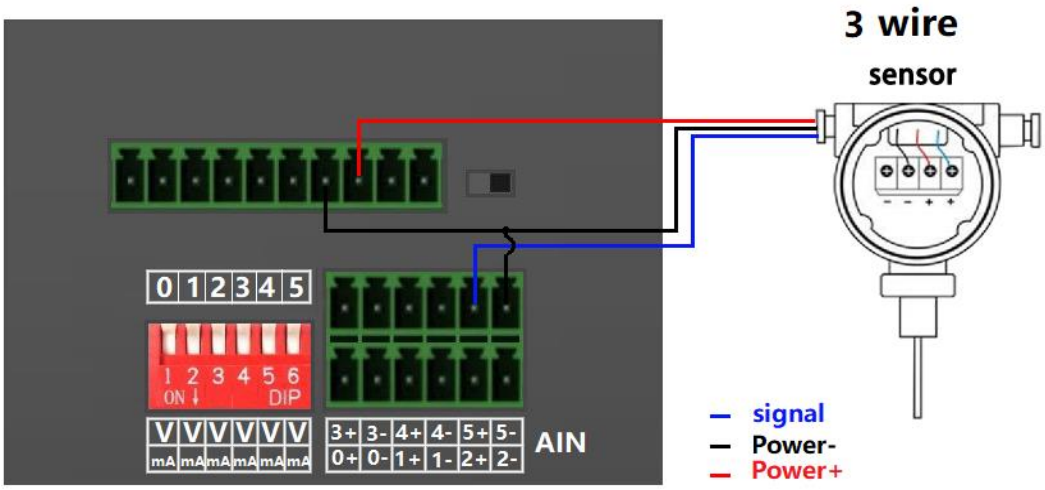
Internal interface principle:



2 Wire wiring

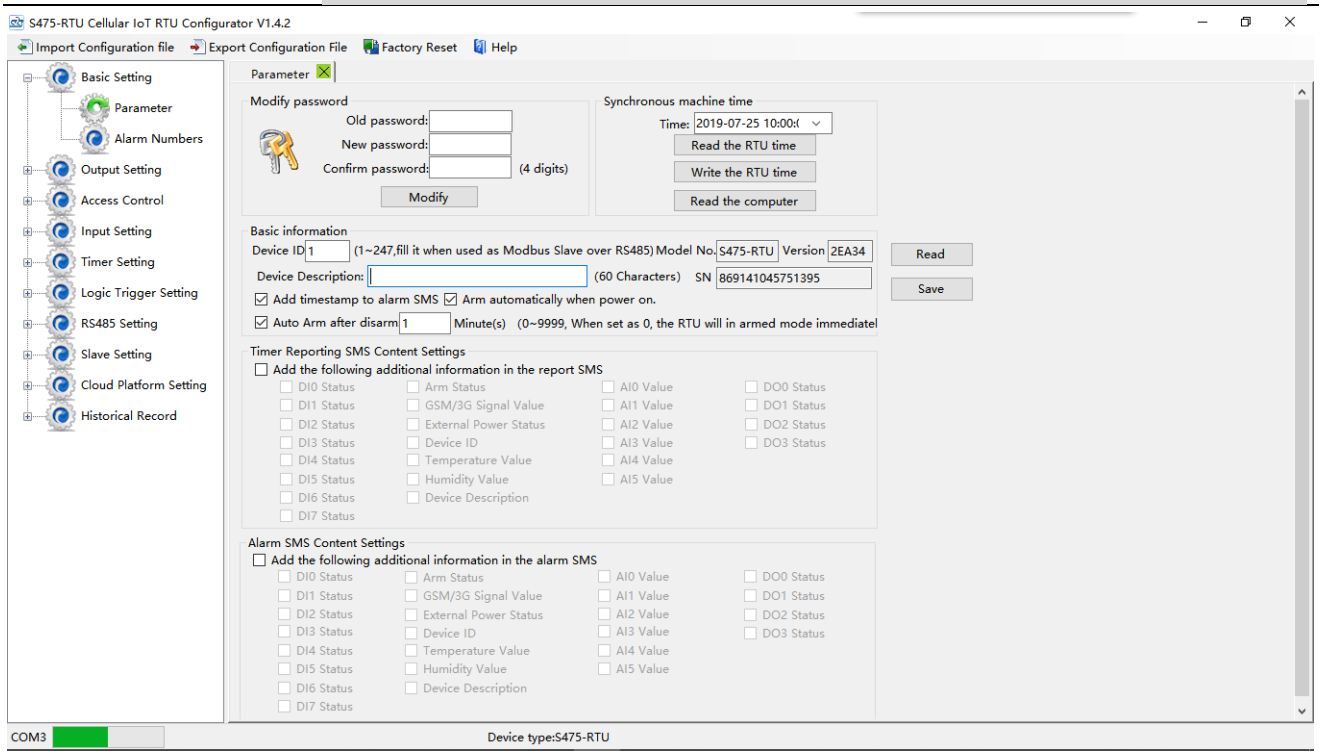


3 Wiring

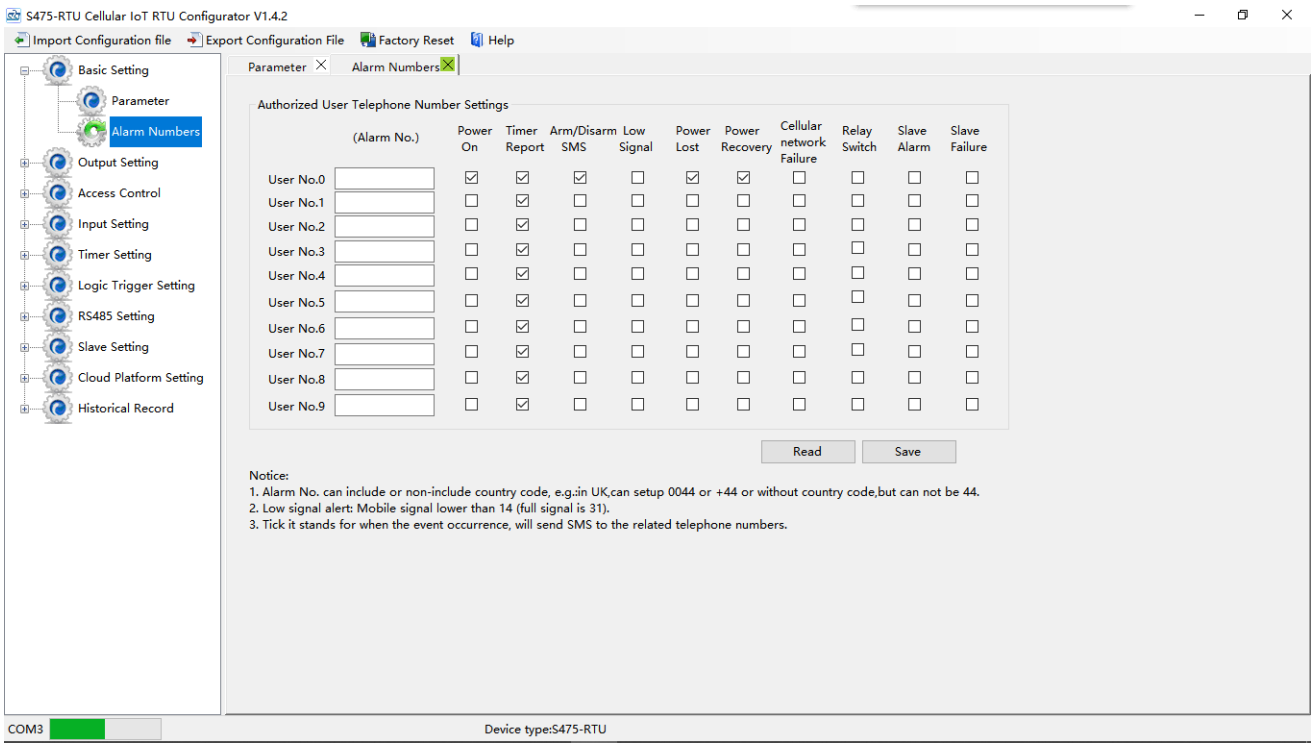


8.2 Quickly Verify Device Communication Function

Connect power supply to the device then switch on the device, run the configuration software, and log in. In “Basic Settings” page, click [Read the RTU Time] > [Write the RTU Time] to write the correct time to the device.Choose [Arm automatically when power on]. Then click the [Save]. As below:



In “Numbers”page,enter the phone number used to receive the alarm,choose the options according to request,such as power on,power lost....then click [Save],as below:



Then switch off the device,insert sim card,switch on the device.after the device register network successfully,the phone number can receive SMS sent by the device.If you cut off the device power, the phone number will receive power failure SMS sent by the device....That shows the device work normally.

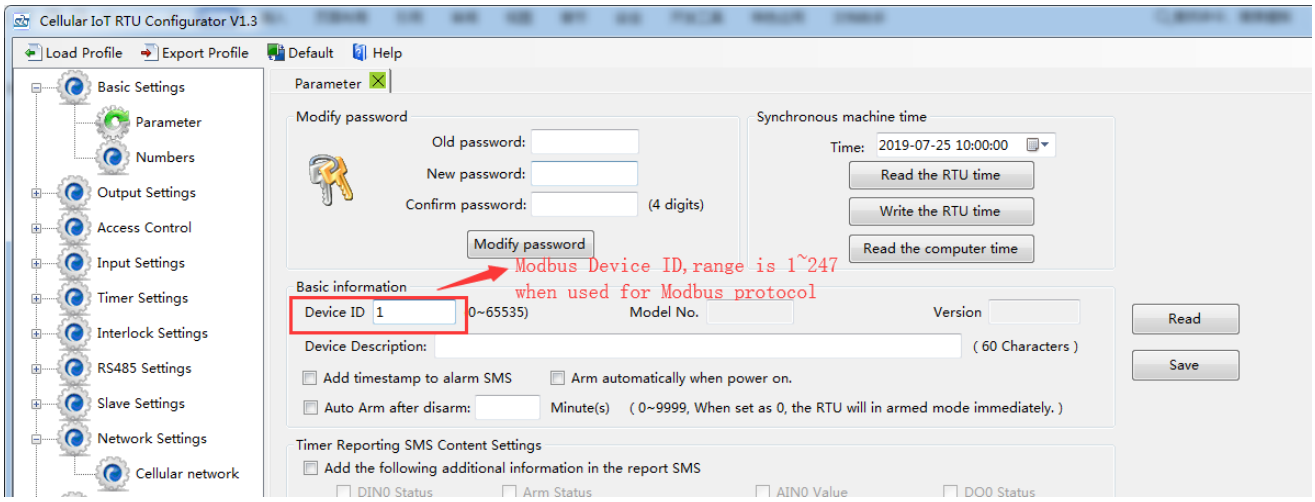
8.3 Modbus RTU Slave Application

Device support Modbus RTU slave function, can be connected to HMI, SCADA, DCS, MES system. It can be used for fieldbus data acquisition, remote SMS alarm, remote dial alarm and GPRS/3G/4G to cloud...

For example, when device as Modbus RTU slave, connect to HMI as below:

(1) Connect device to HMI via RS485 port, set HMI RS485 port parameter;

(2) In "Basic Parameter Settings" page, set "Device ID", range is 1~247 in Modbus protocol as below:



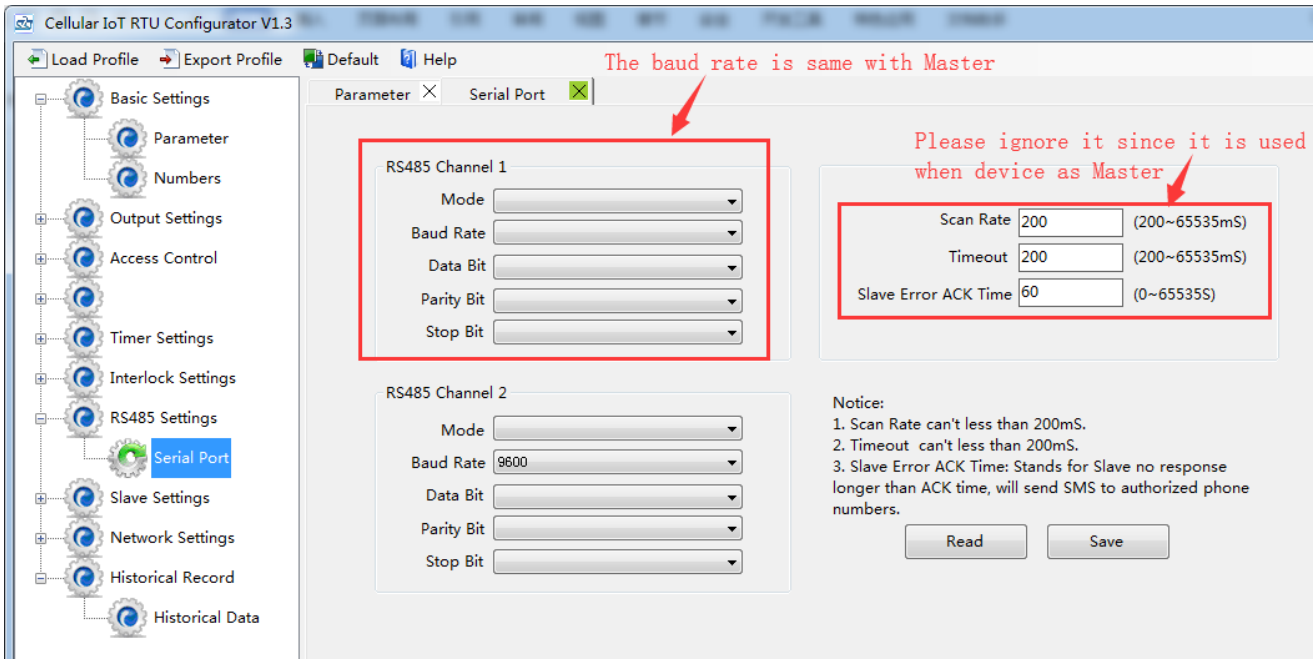
(3) In "Serial Port" setting page, set device parameter as below:

A) RS485 used as "Modbus RTU Slave";

B) Baud Rate, Data Bit, Parity Bit, Stop Bit setting should be corresponding with HMI, otherwise communication will be failure. If multiple Masters, all Masters parameter should corresponding with device;

C) No need set: "Scan Rate", "Time Out", "Slave Fault Verify Time";

D) Click "Save" button.



(4) In HMI configuration software, set the Modbus RTU Register address of device. Refer to **[“S47X reigister”]**;

(5) Switch the device on, enter into working mode, device running according parameter setting.

8.3.1 Read device digital output DO value

The DO register address of the relay included in the device belongs to the retaining coil and the address is 0-3. See Appendix B for details.

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	01H	Read the hold coil, function code 01
Register Starting Address	2	00 00H	Range: 0000H-0003H
Read Register Qty	2	00 04H	Range: 0001H-0004H
16 CRC Verify	2	3D C9H	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H device, consistent with download data
Function Code	1	01H	Read the hold coil
Return Bytes Qty	1	01H	Return data length
Returning Data	1	02H	Data returned
16 CRC Verify	2	D0 49H	CRC0 CRC1 low byte in front, high behind

Example: Read 2 DO states, device address 1,then,

Server Send: 01 01 00 00 00 04 3D C9

01= Device address; 01= Read Relay DO function code;00 00= Register starting address; 00 04= Continuous reading of 2 DO data; 3D C9= CRC verify.

Device Answer: 01 01 01 02 DO 49

01= Device address; 01= Read relay function code; 01=Return data bytes Qty; 02=The returned data is converted into binary: 0000 0010, 4 bits high 0000 is useless, and 4 bits low 0010 corresponds to DO3, DO2, DO1 and DO0 respectively(values are as follows) ; DO 49=CRC Verify.

DO3	DO2	DO1	DO0
0	0	1	0
Disconnect	Disconnect	Closure	Disconnect

If you want to read the state of a DO or several DO states, you only need to modify the "DO register start address" and "the number of read registers", then recalculate the CRC, and the returned data is parsed according to the above description.

8.3.2 Control device digital output DO status

1) Control 1 channel device DO output

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	05H	Write single holding coil type, function code 05
DO Register Address	2	00 00H	Range: 0000H-0003H
Active	2	FF 00H	This value: FF 00H or 00 00H, FF 00H= Close relay, 00 00H= Open relay
16CRC Verify	2	8C 3AH	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, according to the data Master send
Function Code	1	05H	Write single holding coil type
DO Register Address	2	00 00H	Range: 0000H-0003H
Active	2	FF 00H	This value: FF 00H or 00 00H, FF 00H= Already actived close relay, 00 00H= Already actived open relay
16CRC Verify	2	8C 3AH	CRC0 CRC1 low byte in front, high behind

Example: Control relay DO0 close, then:

Server send:01 05 00 00 FF 00 8C 3A

01=Device address;05= Control single relay command;00 00=Relay DO0 address;FF 00=DO0 close;8C 3A=CRC verify.

Device answer: 01 05 00 00 FF 00 8C 3A

01=Device address;05=Control single relay command;00 00=Relay DO0 address;FF 00= Active DO0 close;8C 3A=CRC verify.

If single control other relay outputs, only need to change "DO Register Address" and "Active", calculate CRC verify again.

2) Multiple control DO outputs

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247,according to setting address
Function Code	1	0FH	Write multi holding coil,function code 15
DO Starting	2	00 00H	Range: 0000-0003, stands for DO0-DO3

<table>
<tr><td>Register Address</td><td></td><td></td><td></td></tr>
<tr><td>Control Relay Qty</td><td>2</td><td>00 04H</td><td>Qty: 0-4</td></tr>
<tr><td>Write Byte Qty</td><td>1</td><td>01H</td><td>Write 1 byte, since device only 4DO, use 4 binary can do it</td></tr>
<tr><td>Writing Data</td><td>1</td><td>0FH</td><td>0FH stands for 4 DO status, high 4 byte invalid, low 4 byte F converter to binary as below
<table>
<tr><td>DO3(bit3)</td><td>DO2 （bit2）</td><td>DO1 （bit1）</td><td>DO1 （bit0）</td></tr>
<tr><td>1</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>Active close</td><td>Active close</td><td>Active close</td><td>Active close</td></tr>
</table>
1= Active close，0= Active open</td></tr>
<tr><td>16CRC Verify</td><td>2</td><td>7E 92H</td><td>CRC0 CRC1 low byte in front, high behind</td></tr>
</table>

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, according to the data Master send
Function Code	1	0FH	Write multi holding coil type
DO Register Address	1	00 00H	Range: 0000-0003,stands for DO0-DO3
Active	1	00 04H	Range:0001H-0004H, stands for already actived relays
16CRC Verify	2	54 08H	CRC0 CRC1 low byte in front, high behind

Example: Close device 4 DO at same time, then:

Server send: 01 0F 00 00 00 04 01 0F 7E 92

01= Device address; 0F= Control multi relay; 00 00= Relay DO0 starting address; 00 04= Control 4 relays; 01= Send data qty; 0F= Data sent converter to binary 0000 1111 high 4 byte invalid, low 4 byte 1111 sort to match DO3 DO2 DO1 DO0, 1 stands for close relay, 7E 92 CRC verify.

DO3	DO2	DO1	DO0
0	0	1	0
close	close	close	close

Device answer: 01 0F 00 00 00 04 54 08

01= Device address; 0F= Control multi relay; 00 00= Relay DO0 starting address; 00 04= Actived 4 relays; 54 08 CRC verify.

If need to control multi relays at same time, only need to change "Relay Starting Address", "Control Relay Qty", "Write Data" and calculate "CRC Verify" again.

8.3.3 Read Device DIN Status

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	02H	02 read input coil DIN status
DIN Register Address	2	00 00H	Range: 0000H-0007H, stands for DIN0-DIN7
Read DIN Register Qty	2	00 08H	Range: 0001H-0008H,Read qty of DIN status
16CRC Verify	2	79 CCH	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	02H	read input coil DIN status
Return Bytes Qty	1	01H	Return data length
Returning Data	1	0FH	Return DIN data, stands for DIN7-DIN0 status
16CRC Verify	2	E1 C8H	CRC0 CRC1 low byte in front, high behind

Example: Inquiry device 8 DIN data at same time, then:

Server send: 01 02 00 00 00 08 79 CC

01= Device address; 02= Inquiry DIN status; 00 00= DIN Starting address; 00 08= Serial reading 8 DIN status; 79 CC = CRC verify.

Device answer: 01 02 01 0F E1 8C

01= Device address; 02= Inquiry DIN status; 01= Returning data bytes qty; 0F DIN status, every byte stands for one DIN status, 0F converter to binary 0000 1111 from high to low byte, stands for DIN7-DIN0 status,
0= Open, 1= Close.

DIN7	DIN6	DIN5	DIN4	DIN3	DIN2	DIN1	DIN0
0	0	0	0	1	1	1	1
Open	Open	Open	Open	Close	Close	Close	Close

E1 8C: 16 byte CRC verify.

If need to inquiry multi DIN status, only need to change "DIN Starting Address", "Reading DIN Register Qty", calculate CRC verify again.

8.3.4 Read device AIN DIN pulse count value, tempe&humi value, external power voltage value

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	04H	04 read input register
Register Starting Address	2	00 00H	One address can read 2 bytes. AIN address range: 0000-000BH, One AIN data take two address, temperature address: 0018H, humidity address: 0019H, DIN1 count value address: 001A, 001B External power voltage address: 000E。
Read Register Qty	2	00 1CH	Read qty of input register, read AIN0 to DIN0 count value address, total 28 register, 0000H to 0001BH.
16CRC Verify	2	F1 C3H	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	04H	04 read input register
Data Bytes Range	1	04H	Return data length
Returning Data	38	00 00 00 E7 00 00 00 DD 00 00 00 DD 00 00 00 DC 00 00 00 DE 00 00 00 DF 00 00 00 00 04 C6 01 9A 00 00 00 01 00 01 00 01 00 01 00 01 00 01 00 01 0B 36 1B E4 00 00 00 0B	Return Temperature&Humidity value
16CRC Verify	2	A9 3CH	CRC0 CRC1 low byte in front, high behind

Example: Inquiry device 6AIN temperature, humidity, external power voltageand DIN0 count value at same time, then:

Server send: 01 04 00 00 00 1C F1 C3

01H= Device address; 04= Read input register value; 00 00= Starting address(For the detailed address, please refer to “(c.) Input Register Type in Appendix B Local Register); 00 1C= Serial reading 28 input register value;
F1 C3: CRC verify.

Device answer: 01 04 38 00 00 00 E7 00 00 00 DD 00 00 00 DD 00 00 00 DC 00 00 00 DE 00 00 00 DF 00 00 00 00 04 C6 01 9A 00 00 00 01 00 01 00 01 00 01 00 01 00 01 0B 36 1B E4 00 00 00 0B A9 3C

01= Device address; 04= Input register value;

38: Return data bity,00 00 00 E7 00 00 00 DD 00 00 00 DD 00 00 00 DC 00 00 00 DE 00 00 00 DF 00 00 00 00 04 C6 01 9A 00 00 00 01 00 01 00 01 00 01 00 01 00 01 0B 36 1B E4 00 00 00 0B, detail as follows:

AIN	AIN0	AIN1	AIN2	AIN3	AIN4	AIN5
Receiving Data	00 00 00 E7	00 00 00 DD	00 00 00 DD	00 00 00 DC	00 00 00 DE	00 00 00 DF
Decimal Value	194	207	0	0	0	0
Real Value	1.94	2.07	0	0	0	0

Other Value	External Power Voltage	Temperature	Humidity	DIN0 Count Value
Receiving Data	04 C6	0B 36	1B E4	00 00 00 0B
Decimal Value	1222	2870	7140	11
Real Value	12.22V	28.7℃	71.4%RH	11 times

A93C:CRC verify.

8.4 Modbus RTU Master Application

When RS485 as Modbus RTU Master, can extend I/O tags, support slaves for connecting Remote I/O data acquisition module, Smart meter, Power monitoring module, Smart transducer...; Can mapping register value from Slave to Master, these registers' can be setup high or low threshold value, and NC/NO type, moreover, can enable to send SMS to users once alarm occurrence by the registers if required. Also can remote control Slaves by writing coil.

Mapping Register Table and function code:

Reminder:

1.Use this function code when connect to Modbus RTU/Modbus TCP upper computer via GPRS/3G/4G (Device as Modbus RTU Slave). Stands for when Cloud communication with S47X, the S47X is Modbus RTU Slave of Cloud Server.

2. When device connect to Modbus RTU/Modbus TCP upper computer via GPRS/3G/4G (Device as Modbus RTU Slave). The I/O of S47X itself refer to "Modbus RTU Slave Application" above.

For example, when device as Modbus RTU master,as below:

Step1: Connect the slave to device RS485 port.

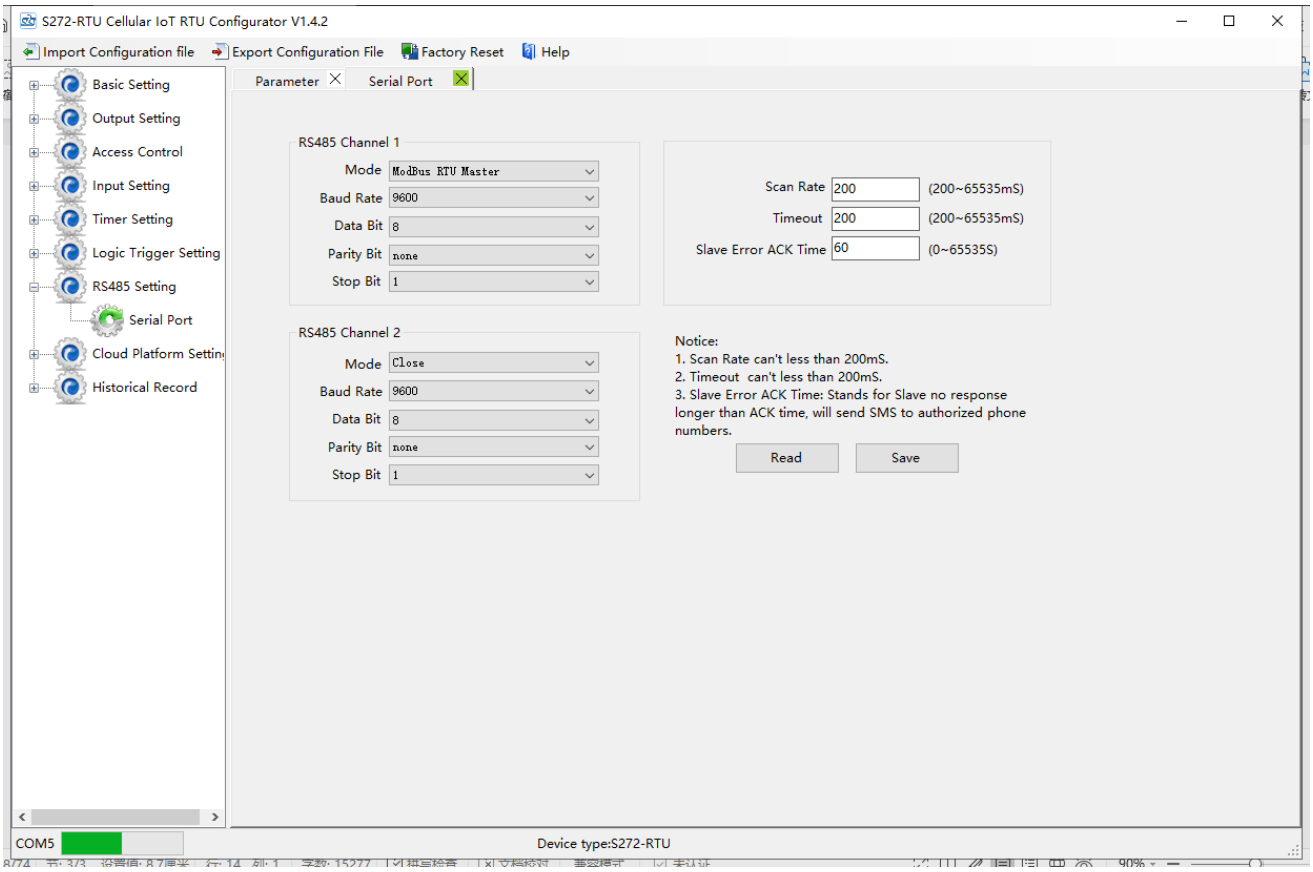
Step2: Find the salve port communication parameter and register address from user manual.

Step3: Write device RS485 parameter according to slave port communication parameter, pls ensure both parameter are same, others communication failure, refer to "port setting" part.

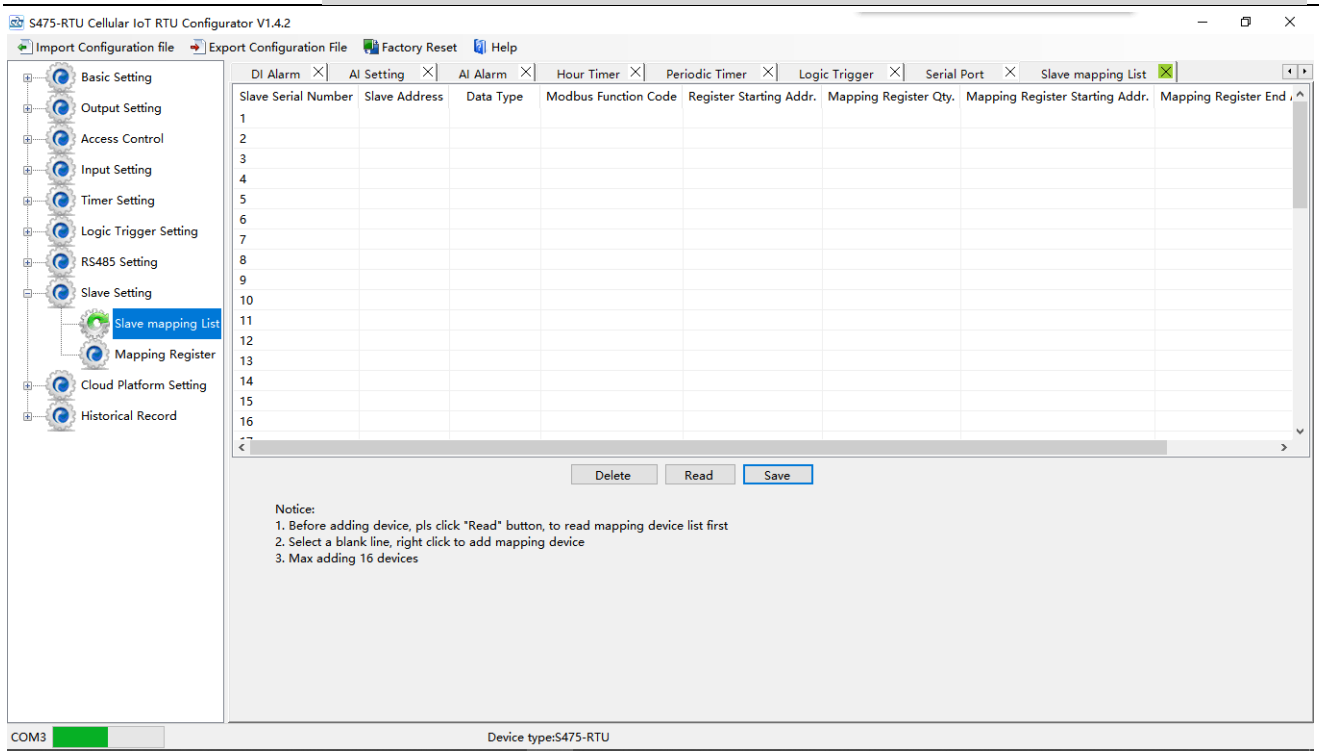
Step4: Set RS485 port as Modbus RTU Master, then set polling and time out parameter, refer to "port setting" part.

Serial Port Setting:

In “Serial Port” setting page, choose RS485 port as “Modbus RTU Master”. Baud Rate, Data Bit, Parity Bit and Stop Bit parameter need to be same as connected device; Scan Rate, Time Out and Slave Failure Verify Time can be set as default:



Step5: Back to Slave Mapping page as below, right click the line to add.

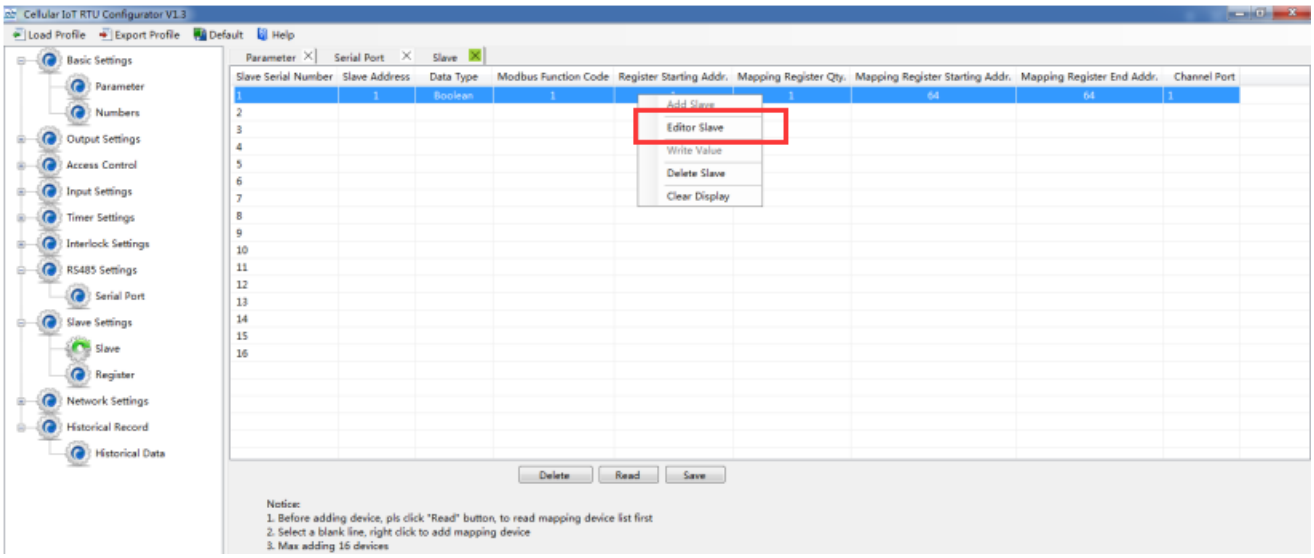


Click Add Slave as below:

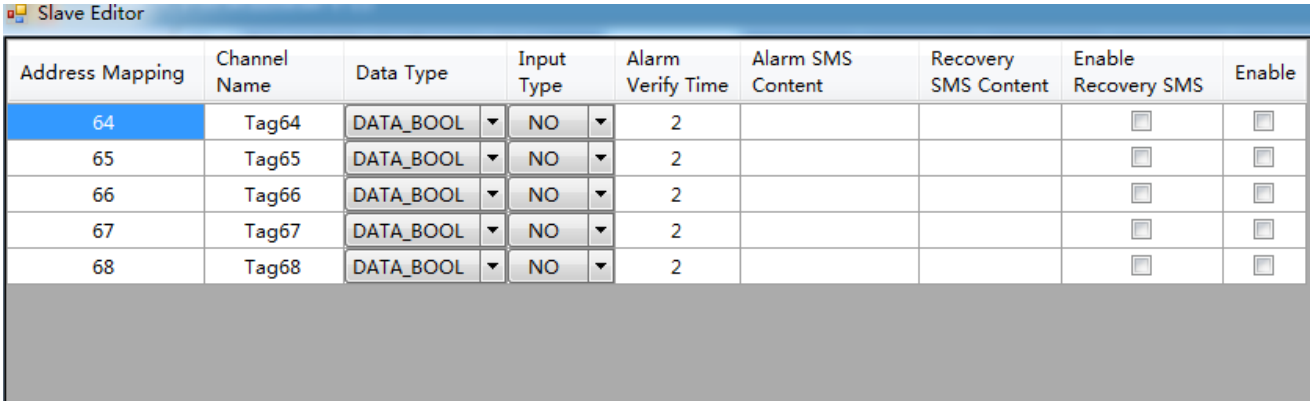
If one slave have multi register, then need to add seperately according to register type; For exmaple, Mxxx

remote I/O module, with digital and analog inputs, need to add the digital(Boolean) first, then add the analog(16 Bit).

Step6: Right click the line to edit the slave.



Click the "Editor Slave" to set channel name, alarm SMS content, recovery SMS content and relay active etc. as below:



Step7: Restart the device, enter into working mode, device running according parameter setting, include alarm SMS and call. If set the network communication function, then can remote transmit data to cloud server via GPRS/3G/4G.

Reminder:

After adding slaves, device switched off/on to restart is necessary.

8.4.1 Read Boolean Mapping Address Data

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	01H	Read holding coil type, function code 01
Boolean Register	2	00 40H	Range: 0040H-007FH, address refer to **["Slave**

Starting Address			**Mapping Register Address"]** at manual bottom
Read Register Qty	2	00 0AH	Range: 0001H-0040H, total 64 address for Boolean mapping
16 CRC Verify	2	BD D9H	CRC0 CRC1 low byte in front, high byte in behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, according to the data Master send
Function Code	1	01H	Read holding coil
Return Byte Length	1	02H	Return Data Length
Returning Data	2	73 01H	
16CRC Verify	2	5D 0CH	CRC0 CRC1 low byte in front, high behind

Example: Start from address 64, read 10 Boolean mapping data value, then:

Server send: 01 01 00 40 00 0A BD D9

01= Device address; 01= Read holding coil; 00 40=Read Boolean data start from address 64; 00 0A = Serial to read 10 Boolean status;

BD D9= CRC verify.

Device answer: 01 01 02 73 01 5D 0C

01= Device address; 01= Read holding coil; 02= Return Byte Length; 73 01= Return 10 Boolean status. High byte stands for low address data, low address stands for high address. According to Modbus protocol, fix 73 01H real value to be 01 73H, converter to Binary as below:

Register mapping address	Invalid	Invalid	Invalid	Invalid	Invalid	Invalid	73	72
Value	0	0	0	0	0	0	0	1
Register mapping address	71	70	69	68	67	66	65	64
Value	0	1	1	1	0	0	1	1

The address value higher than 10 digits will be seen as invalid.

5D OC =CRC verify.

8.4.2 Modify Boolean Mapping Address Data

If control slave's relay status which connected to RS485, need to add slave in salve list of configurator. Write command 15 for mapping, when mapping address value modified, will write to RS485 matched slave address.

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	05H	Write single holding coil, function code 05H
Boolean Mapping Register Address	2	00 40H	Range: 00 40H-00 7FH, address refer to **["Slave Mapping Register Address"]** at manual bottom

Write value	2	FF 00H	This value: FF 00H or 00 00H, FF 00H stands for write 1; 00 00H stands for write 0
16 CRC Verify	2	8D EEH	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, according to the data Master send
Function Code	1	05H	Write single holding coil
Boolean Mapping Register Address	2	00 40H	Range: 0040H-007FH
Write value	2	FF 00H	This value: FF 00H or 00 00H. FF 00H stands for write 1,00 00H stands for write 0.
16 CRC Verify	2	8D EEH	CRC0 CRC1 low byte in front, high behind

Example: Modify Boolean mapping address 64 status, modify to 1, then:
Server send: 01 05 00 40 FF 00 8D EE
01= Device address; 05= Write Boolean value; 00 40=The mapping address which need to revise;
FF 00 = Write 1; 8D EE = 16 Bit CRC verify.
Device answer: 01 05 00 40 FF 00 8D EE
01= Device address; 05= Write Boolean value; 00 40= The mapping address which need to write;
FF 00= Write 1; 8D EE = 16 Bit CRC verify.
If need multi modify, pls check function 15 of Modbus protocol.

8.4.3 Read Data Type Mapping Address Data

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	03H	Read holding register, function code 03
Mapping Register Starting Address	2	4E 20H	One address can read 2 bytes. Mapping data type address range, refer to **["Slave Mapping Register Address"]** at manual bottom.
Read Mapping Register Qty	2	00 0AH	Read input register qty.
16 CRC Verify	2	3D 2FH	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description

Device Address	1	01H	01H Device, according to the data Master send
Function Code	1	03H	Read holding coil
Range Data Bytes	1	14H	One address can read 2 bytes
Returning Data	20	00 14 00 1E 00 28 00 32 00 4B 00 41 00 0A 00 25 00 14 00 2AH	Returning Data
16 CRC Verify	2	FB 34H	CRC0 CRC1 low byte in front, high behind

Example: Mapping address start from 20000, read 10 address data, then:

Server send: 01 03 4E 20 00 0A D3 2F

01= Device address; 03= Read holding register; 4E 20=Mapping register starting address, current is Decimal data 20000; 00 0A = Read 10 register value;

D3 2F = 16 Bit CRC verify.

Device answer: 01 03 14 00 14 00 1E 00 28 00 32 00 4B 00 41 00 0A 00 25 00 14 00 2A FB 34

01= Device address; 03= Read holding register; 14= Returning 20 byte; 00 14 00 1E 00 28 00 32 00 4B 00 41 00 0A 00 25 00 14 00 2A = Returning data.

Register Mapping Address	20000	20001	20002	20003	20004	20005	20006	20007	20008	20009
Value	00 14	00 1E	00 28	00 32	00 4B	00 41	00 0A	00 25	00 14	00 2A

FB 34 = 16 Bit CRC verify.

8.4.4 Modify Data Type Mapping Address Data

If need to revise slave data which RS485 connected, need to add slave in salve list of configurator. Write command 16 for mapping, when mapping address value modified, will write to RS485 matched slave address. If address 20000 mapping slave data type is Signed Int, sort AB.

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	06H	Write single holding register, function code 06
Mapping Register Address	2	4E 20H	Address range: 4E 20H-50 1CH. Mapping data type address range, refer to **["Slave Mapping Register Address"]** at manual bottom.
Write Data	2	00 64H	Data writing value is Decimal data 100
16 CRC Verify	2	9E C3H	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, according to the data Master send

Function Code	1	06H	Write single holding register
Mapping Register Address	2	4E 20H	Address range: 4E20H-501CH, mapping data type address range.
Write Data	2	00 64H	Write 100 successfully
16 CRC Verify	2	9E C3H	CRC0 CRC1 low byte in front, high behind

Example: If address 20000 mapping slave data type is Signed Int, sort AB, modify mapping address 20000 register to 100, then:

Server send: 01 06 4E 20 00 64 9E C3

01= Device address; 06= Modify single holding register value; 4E 20=Modify address 20000 register value; 00 64 = Write Decimal value 100;

9E C3 = 16 Bit CRC verify.

Device answer: 01 06 4E 20 00 64 9E C3

01= Device address; 06= Modify single holding register value; 4E 20= R Modify address 20000 register value; 00 64= Modify to Decimal value 100.

9E C3 = 16 Bit CRC verify.

If need to modify multi data type mapping address, pls check function code 16 in Modbus protocol.

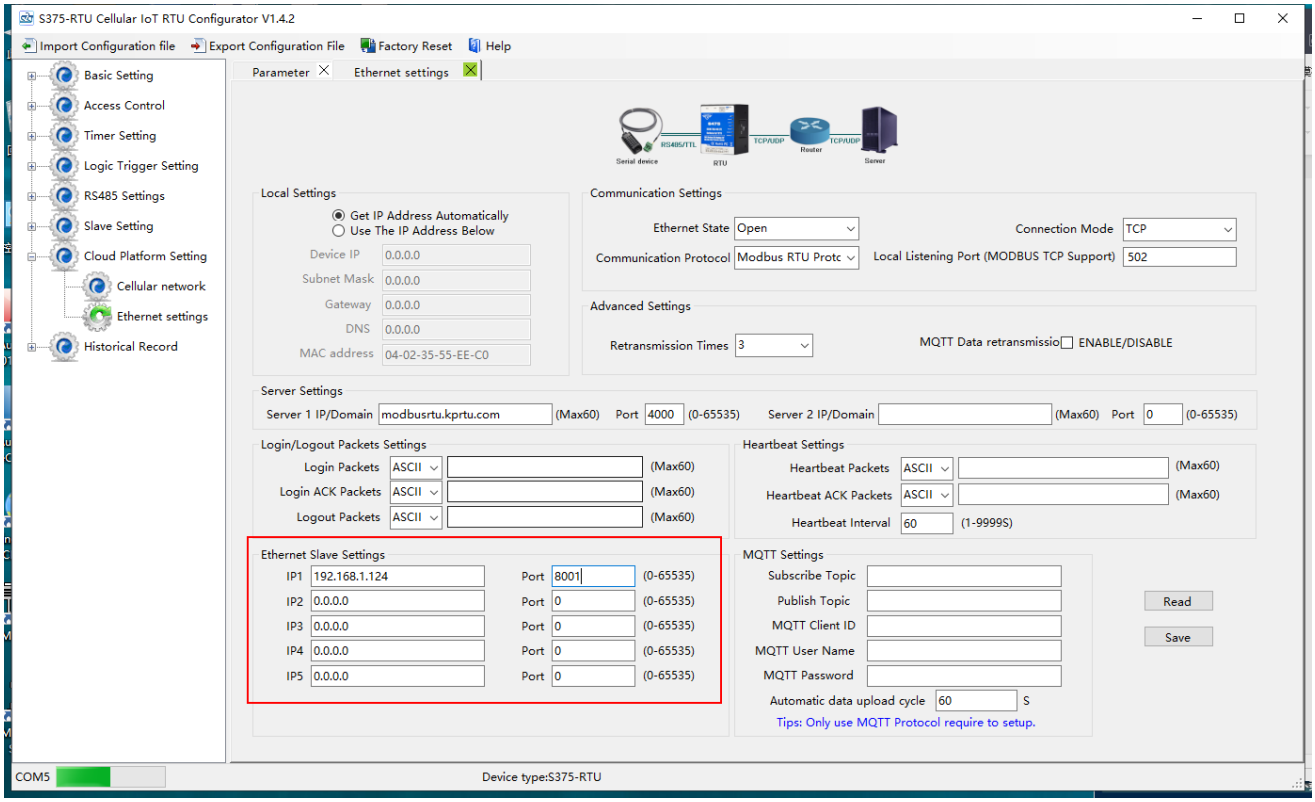
8.5 Modbus TCP Master Application

When Ethernet as Modbus TCP master,can extend I/O tags, support slaves for connecting Remote I/O data acquisition module, Smart meter, Power monitoring module, Smart transducer... Can mapping register value from Slave to Master, these registers' can be setup high or low threshold value, and NC/NO type, moreover, can enable to send SMS to users once alarm occurrence by the registers if required. Also can remote control Slaves by writing coil.

For example, when device as Modbus TCP master,as below:

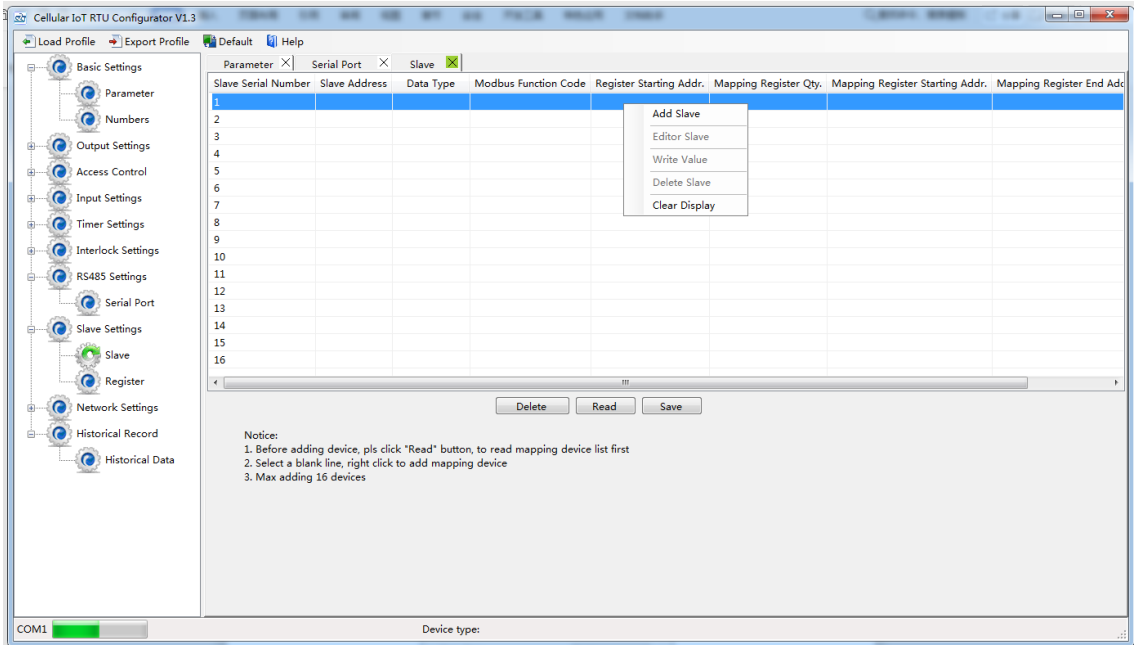
1)Ethernet Setting:

In "Ethernet Settings" page, choose correct slave IP and port,click "save" to add,support up to 5 Ethernet slave.

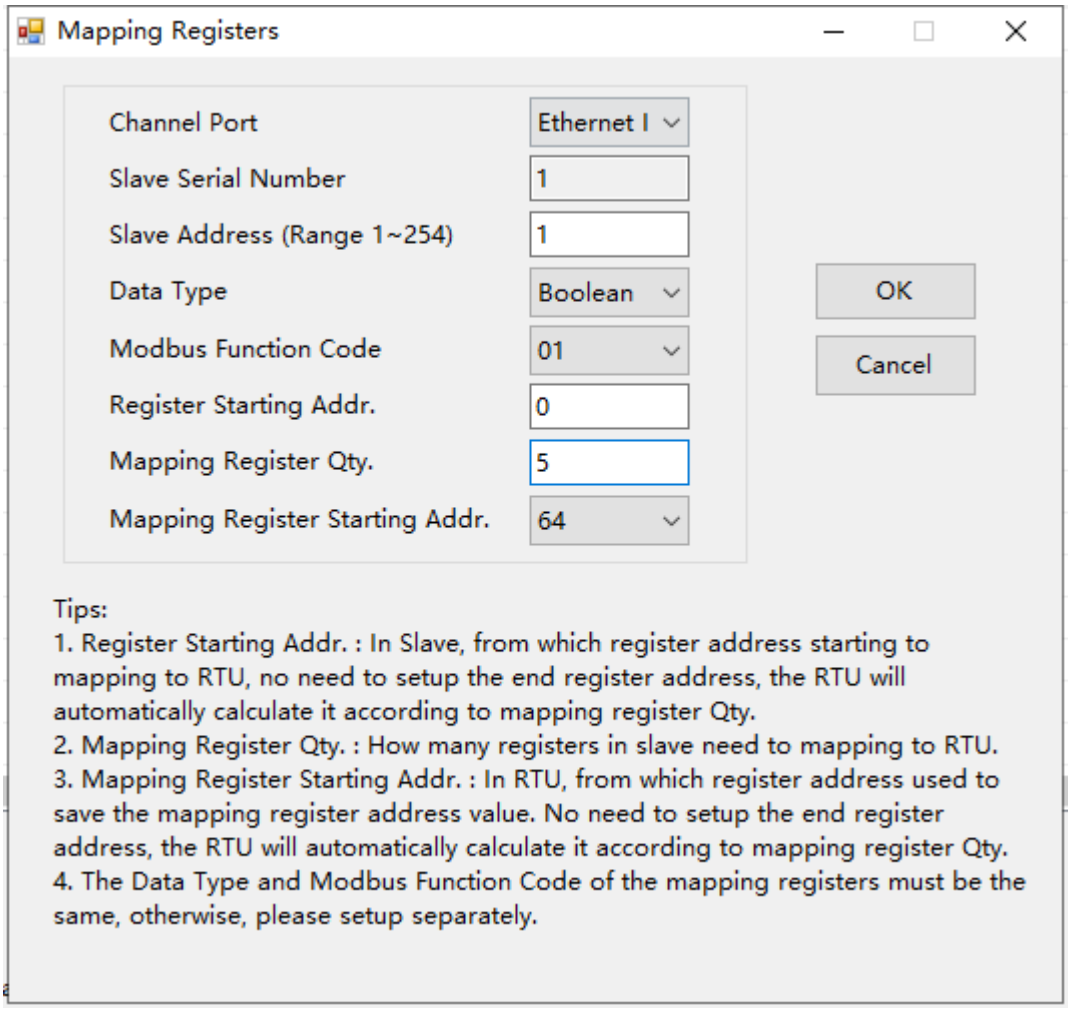


2)Slave Setting:

In “Slave”page,right click the line to add,as below:

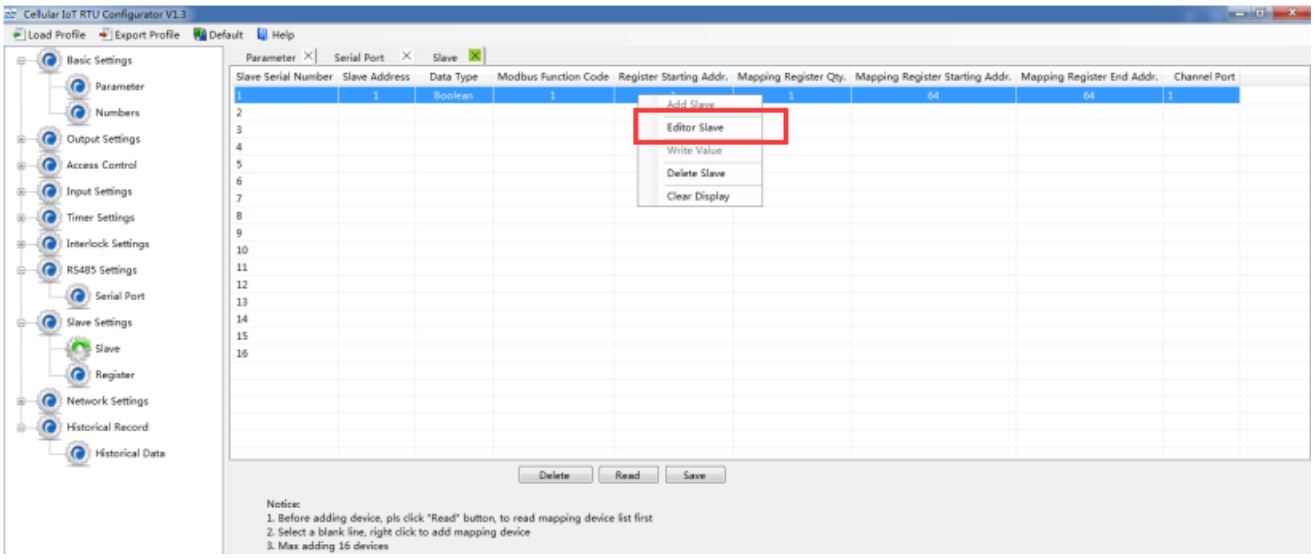


Click Add Slave as below:



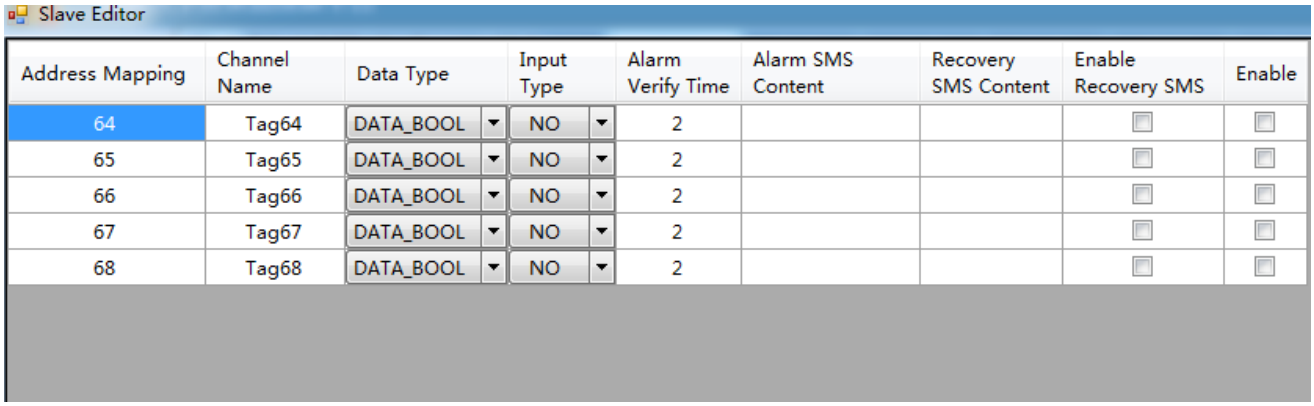
If one slave have multi register, then need to add seperately according to register type; For exmaple, Mxxx remote I/O module, with digital and analog inputs, need to add the digital(Boolean) first, then add the analog(16 Bit).

Right click the line to edit the slave.



Click the "Editor Slave" to set channel name, alarm SMS content, recovery SMS content and relay active etc. as

below:



Reminder:

After adding slaves, device switched off/on to restart is necessary.

8.5.1 Read Boolean Mapping Address Data

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Transaction ID	2	00 00H	Identification of Modbus requests/responses transactions
Protocol Identifier	2	00 00H	00 00: Modbus protocol
Data Length	2	00 06H	The length of subsequent data
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	01H	Read holding coil type, function code 01
Boolean Register Starting Address	2	00 40H	Range: 0040H-007FH, address refer to ["**Slave Mapping Register Address**"] at manual bottom
Read Register Qty	2	00 0AH	Range： 0001H-0004H

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Transaction ID	2	00 00H	Identification of Modbus requests/responses transactions
Protocol Identifier	2	00 00H	00 00: Modbus protocol
Data Length	2	00 05H	The length of subsequent data
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	01H	Read holding coil type, function code 01
Return Data Length	1	02H	Range: 0000H-0003H
Returning Data	2	73 01H	

Example: Start from address 64,read 10 Boolean mapping data value, then:

Server send: 00 00 00 00 00 06 01 01 00 40 00 0A

00 00= Transaction ID; 00 00 = Protocol Identifier,00 00 stands for Modbus protocol; 00 06 = The length of

subsequent data; 01= Device address;01 = Read holding coil; 00 00 = Read Boolean data start from address 64; 00 0A = Serial to read 10 Boolean status;

Device answer: 00 00 00 00 00 05 01 01 02 73 01

00 00= Transaction ID; 00 00 = Protocol Identifier,00 00 stands for Modbus protocol; 00 05 = The length of subsequent data; 01= Device address; 01 = The function code of reading Boolean; 02= Return Data Length; 73 01= Return 10 Boolean status. High byte stands for low address data, low address stands for high address. According to Modbus protocol, fix 73 01H real value to be 01 73H, converter to Binary as below:

Register mapping address	Invalid	Invalid	Invalid	Invalid	Invalid	Invalid	73	72
Value	0	0	0	0	0	0	0	1
Register mapping address	71	70	69	68	67	66	65	64
Value	0	1	1	1	0	0	1	1

The address value higher than 10 digits will be seen as invalid.

8.5.2 Modify Boolean Mapping Address Data

If control slave's relay status which connected to Ethernet, need to add slave in salve list of configurator. Write command 15 for mapping, when mapping address value modified, will write to Ethernet matched slave address.

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Transaction ID	2	00 00H	Identification of Modbus requests/responses transactions
Protocol Identifier	2	00 00H	00 00: Modbus protocol
Data Length	2	00 06H	The length of subsequent data
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	05H	Write single holding coil, function code 05H
Boolean Mapping Register Address	2	00 40H	Range: 00 40H-00 7FH, address refer to ["**S47X Mapping Register Address**"] at manual bottom
Write value	2	FF 00H	This value: FF 00H or 00 00H, FF 00H stands for write 1; 00 00H stands for write 0

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Transaction ID	2	00 00H	Identification of Modbus requests/responses transactions
Protocol Identifier	2	00 00H	00 00: Modbus protocol
Data Length	2	00 06H	The length of subsequent data

Device Address	1	01H	01H Device, according to the data Master send
Function Code	1	05H	Write single holding coil
Boolean Mapping Register Address	2	00 40H	Range: 00 40H-00 7FH, address refer to ["**S47X Mapping Register Address**"] at manual bottom
Write value	2	FF 00H	This value: FF 00H or 00 00H. FF 00H stands for write 1,00 00H stands for write 0.

Example: Modify Boolean mapping address 64 status, modify to 1, then:
Server send: 00 00 00 00 00 06 01 05 00 40 FF 00
00 00= Transaction ID; 00 00 = Protocol Identifier,00 00 stands for Modbus protocol; 00 06 = The length of subsequent data; 01= Device address; 05= Write holding coil; 00 40=The mapping address which need to revise; FF 00 = Write 1;
Device answer: 00 02 00 00 00 06 01 05 00 40 FF 00
00 00= Transaction ID; 00 00 = Protocol Identifier,00 00 stands for Modbus protocol; 00 06 = The length of subsequent data;01= Device address; 05= Write holding coil; 00 40= The mapping address which need to write; FF 00= Write 1;
If need multiple modify, pls check function 15 of Modbus protocol.

8.5.3 Read Data Type Mapping Address Data

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Transaction ID	2	00 00H	Identification of Modbus requests/responses transactions
Protocol Identifier	2	00 00H	00 00: Modbus protocol
Data Length	2	00 06H	The length of subsequent data
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	03H	Read holding register, function code 03
Mapping Register Starting Address	2	4E 20H	One address can read 2 bytes. Mapping data type address range, refer to **["Slave Mapping Register Address"]** at manual bottom.
Read Mapping Register Qty	2	00 0AH	Read input register qty.

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Transaction ID	2	00 00H	Identification of Modbus requests/responses transactions
Protocol Identifier	2	00 00H	00 00: Modbus protocol
Data Length	2	00 17H	The length of subsequent data
Device Address	1	01H	01H Device, according to the data Master send

Function Code	1	03H	Read holding register
Range Data Bytes	1	14H	One address can read 2 bytes
Returning Data	20	00 14 00 1E 00 28 00 32 00 4B 00 41 00 0A 00 25 00 14 00 2AH	Returning Data

Example: Mapping address start from 20000, read 10 address data, then:

Server send: 00 00 00 00 00 06 01 03 4E 20 00 0A

00 00= Transaction ID; 00 00 = Protocol Identifier,00 00 stands for Modbus protocol; 00 06 = The length of subsequent data; 01= Device address; 03= Read holding register ; 4E 20=Mapping register starting address, current is Decimal data 20000; 00 0A = Read 10 register value;

Device answer: 00 00 00 00 00 17 01 03 14 00 14 00 1E 00 28 00 32 00 4B 00 41 00 0A 00 25 00 14 00 2A

00 00= Transaction ID; 00 00 = Protocol Identifier,00 00 stands for Modbus protocol; 00 17 = The length of subsequent data;01= Device address; 03= Read holding register; 14= Returning 20 byte; 00 14 00 1E 00 28 00 32 00 4B 00 41 00 0A 00 25 00 14 00 2A = Returning data.

Register Mapping Address	20000	20001	20002	20003	20004	20005	20006	20007	20008	20009
Value	00 14	00 1E	00 28	00 32	00 4B	00 41	00 0A	00 25	00 14	00 2A

8.5.4 Modify Data Type Mapping Address Data

If need to revise slave data which Ethernet connected, need to add slave in salve list of configurator. Write command 16 for mapping, when mapping address value modified, will write to Ethernet matched slave address.

If address 20000 mapping slave data type is Signed Int, sort AB.

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Transaction ID	2	00 00H	Identification of Modbus requests/responses transactions
Protocol Identifier	2	00 00H	00 00: Modbus protocol
Data Length	2	00 06H	The length of subsequent data
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	06H	Write single holding register, function code 06
Mapping Register Address	2	4E 20H	Address range: 4E 20H-50 1CH. Mapping data type address range, refer to **["Slave Mapping Register Address"]** at manual bottom.
Write Data	2	00 64H	Data writing value is Decimal data 100

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description

Transaction ID	2	00 00H	Identification of Modbus requests/responses transactions
Protocol Identifier	2	00 00H	00 00: Modbus protocol
Data Length	2	00 06H	The length of subsequent data
Device Address	1	01H	01H Device, according to the data Master send
Function Code	1	06H	Write single holding register
Mapping Register Address	2	4E 20H	Address range: 4E20H-501CH, mapping data type address range.
Write Data	2	00 64H	Write 100 successfully

Example: If address 20000 mapping slave data type is Signed Int, sort AB, modify mapping address 20000 register to 100, then:

Server send: 00 00 00 00 00 06 01 06 4E 20 00 64

00 00= Transaction ID; 00 00 = Protocol Identifier,00 00 stands for Modbus protocol; 00 06 = The length of subsequent data; 01= Device address; 06= Modify single holding register value; 4E 20=Modify address 20000 register value; 00 64 = Write Decimal value 100;

Device answer: 00 00 00 00 00 06 01 06 4E 20 00 64

00 00= Transaction ID; 00 00 = Protocol Identifier,00 00 stands for Modbus protocol; 00 06 = The length of subsequent data; 01= Device address; 06= Modify single holding register value; 4E 20= R Modify address 20000 register value; 00 64= Modify to Decimal value 100.

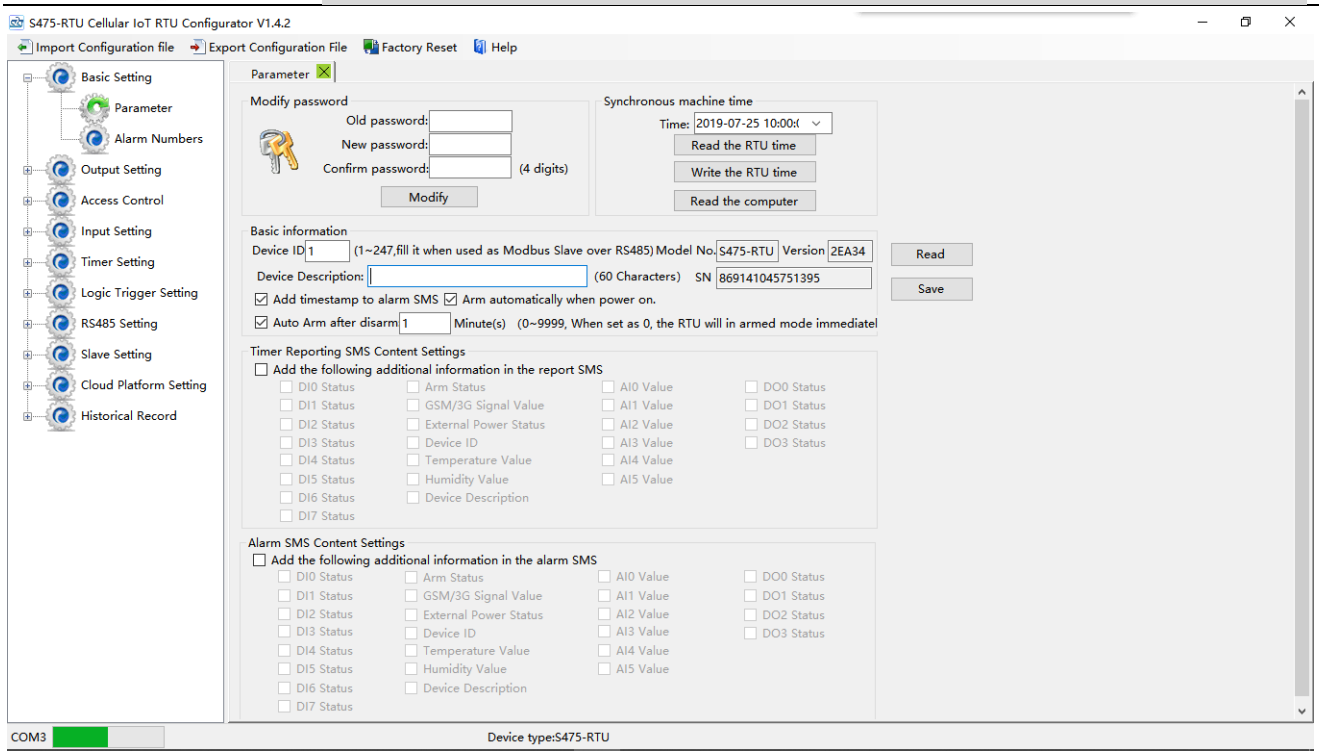
If need to modify multiple data type mapping address, pls check function code 16 in Modbus protocol.

8.6 Transparent Transmission DTU Application

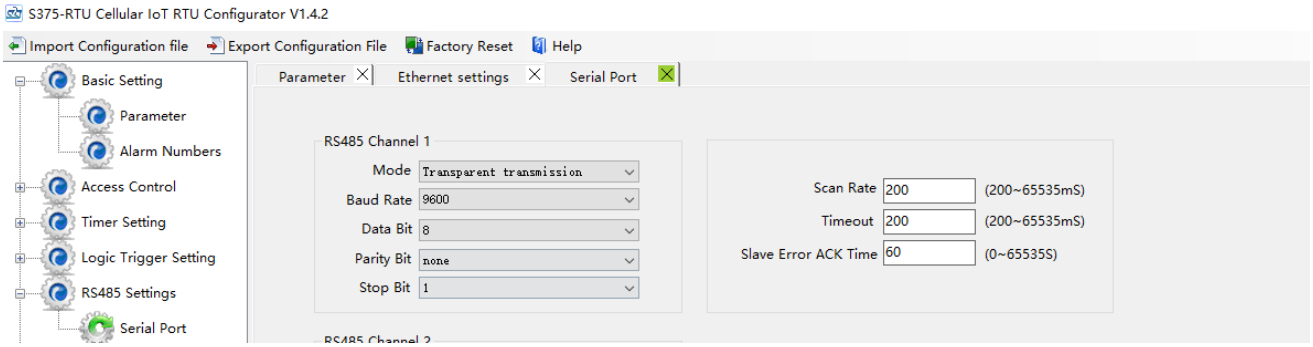
Device can support data transparent transmission: DTU function. Could server transmit data to device via GPRS/3G/4G, device will transfer the data to RS485 port directly without deal with. Once device receive data from RS485, also transmit to cloud server directly via GPRS/3G/4G. When device RS485 port no need mapping slave, or connect to others which is not standard Modbus RTU protocol, then can choose transparent transmission as below:

(1) Items connect to device via RS485, set RS485 port parameter;

(2) Basic setting page to set device ID;



(3) In "Serial Port" setting page, device parameter as below:



A) Choose RS485 as "Transparent Transmission";

B) Baud Rate, Data Bit, Parity Bit, Stop Bit setting should be corresponding with items, otherwise communication will be failure. If multiple items, all items parameter should corresponding with device;

C) No need set: "Scan Rate", "Time Out", "Slave Fault Verify Time";

D) Click "Save" button.

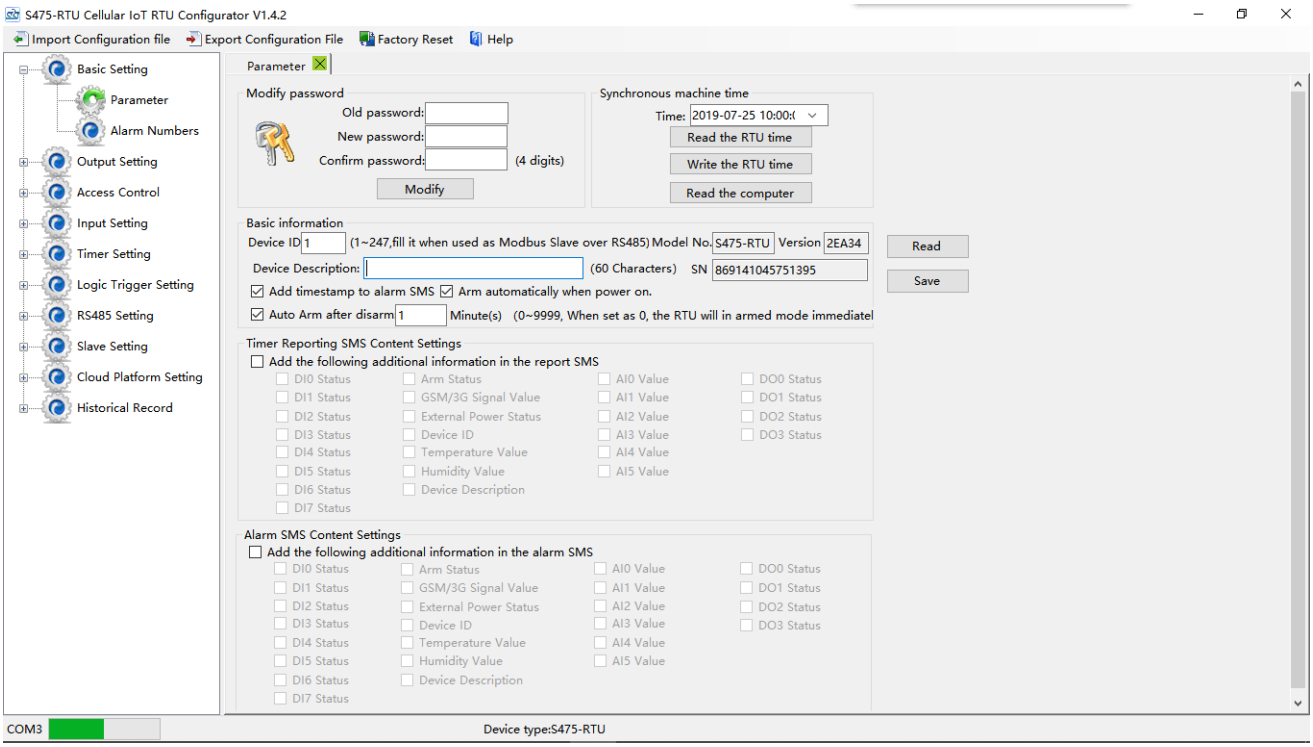
Reminder:

The device ID which connect to RS485 can't be same with S475's device ID.

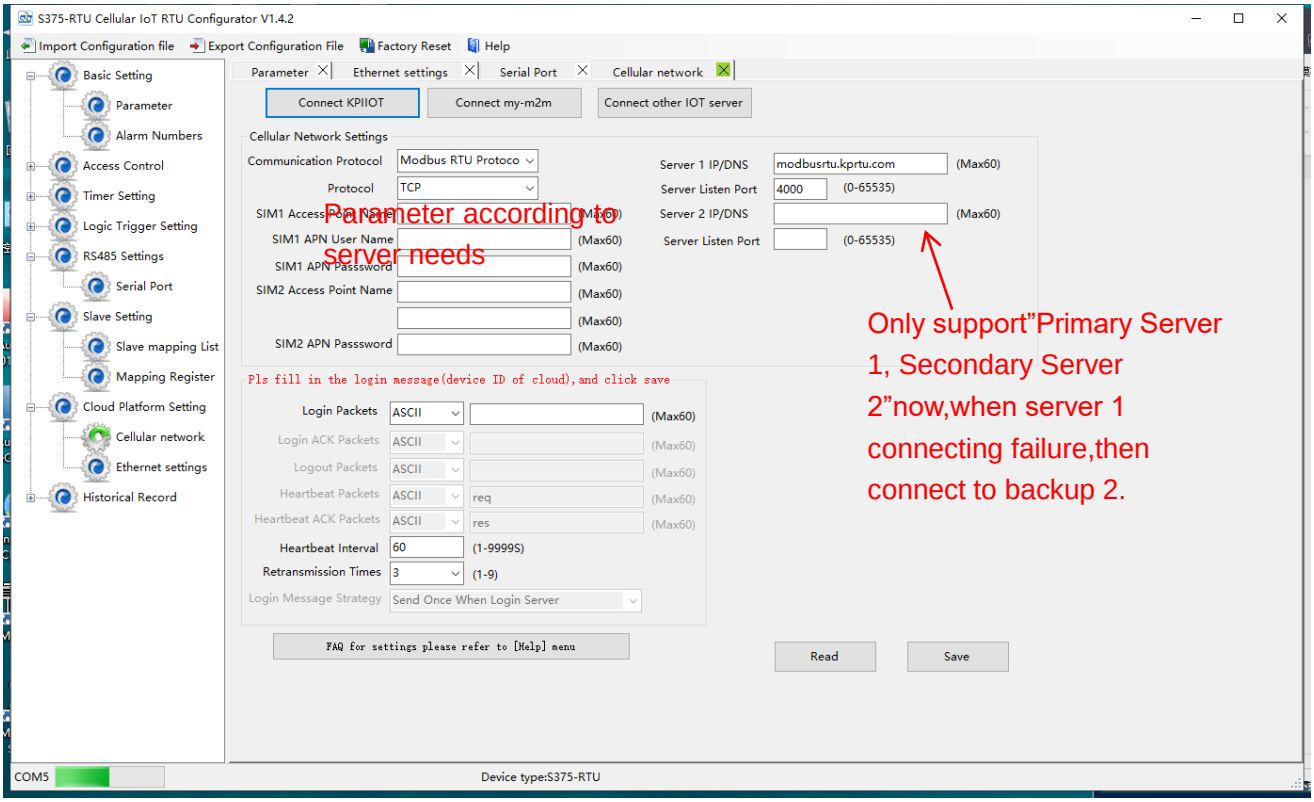
8.7 Device connect to cloud Application

Device can connect to cloud and SCADA via GPRS/3G/4G network or Ethernet, also can connect to clients own server and King Pigeon www.My-M2M.com cloud server. King Pigeon my-m2m.com cloud as sample below: King Pigeon my m2m cloud support Modbus TCP, cloud configuration, wechat alarm function, welcomed editable function.

(1) In "Basic Parameter" setting page, set device ID, range 1~247 in Modbus RTU protocol as below:



(2) In "Cellular network" setting page, set parameter as below:
When Communication Data as "Modbus RTU Protocol", then server IP/DNS should be: modbus.dtuip.com, port is 6651, pls contact King Pigeon Sales for "Login Message Writing";



(3) Click "Save Settings" in the menu, then switch device off.
(4) Switch the device on, enter into working mode, then Slave and Master I/O can connect to network.
(5) Need enter MQTT parameter when choose MQTT protocol.（For details, refer to 12.MQTT Flag and Cloud

Platform on page 69）

9. Device SMS Command

1. The default Password is 1234.
2. The unit cannot support PIN Code Protected SIM Card.
3. You can program the GSM unit with SMS commands using your phone.
4. Remember that commands must be CAPITAL LETTERS. It is PWD not pwd, CAP not Cap etc. Don't add spaces or any other character.
5. In some GSM operators they use different SMS parameter; the units can't return the SMS confirmation in some gsm operators, but it can performance the functions correctly. Also, you can try to add the country code

> For example:
> E.g.: the country code is 0086, or +86.
> The user cell phone number is 13600000000 and has been assigned as a SMS Alert number, the simcard number in the panel is 13512345678.
> When you setup the number as the authorized number, please setup as 008613600000000 or +86136000000000. Not 13600000000.

before the number, see the below settings:

6. If the password is correct but the command is incorrect, the device will return: SMS Format Error, Please check Caps Lock in Command! So please check the Command, or add the country code before the telephone number or check the input is in ENGLISH INPUT METHOD and CAPS LOCK. If password incorrect then will not any response SMS.
7. Once the Unit received the SMS Command, will return SMS to confirmation, if no SMS return, please check your command or resend again.
8. The SMS commands that you will certainly use in the GSM units are the following:

SMS Commands For Program and Operation the S47X**

SMS Command List:

The SMS commands will be used for remote control the RTU are below:

1) Commands error return SMS

Event	Return SMS Content
Any incorrect Command	SMS Format Error, Please check Caps Lock in Command!

2) External DC Status

Event	Return SMS Content
External DC goes off	External DC Power Goes OFF
External DC Power Goes ON	External DC Power Goes ON

3) Modify Password, 4 digits, default is 1234

SMS Command	Return SMS Content
Old Password＋P＋New Password	This is the New Password, please remember it carefully.

4) Reboot

SMS Command	Return SMS Content
Password+Reboot	

5) ***Arm/Disarm SMS Command***

SMS Command		Return SMS Content
Arm	password+AA	Armed
Disarm	password+BB	Disarmed

6) ***Set RTU time,*** format is 1234D2018-01-01T15:00:00W01,the W01 stands for Monday.

SMS Command	Return SMS Content
password+Dxxxx-xx-xxTxx: xx: xxWxx	xxxx(Y)XX(M)XX(D)xx(H)X(M)xx(W)

7) ***Inquiry Current Status SMS Command***

SMS Command	Return SMS Content
password+EE	Armed/Disarmed Model:S475 Version:2CV25 IMEI:8645xxxxxxxxxx GSM Signal Value:25 External DC Power Goes OFF/ON

8) ***Setup 10 User number***(Alarm Number&Access Control Number), max 21digits. (Return 0~4 or 5~9 separately while setting.)

SMS Command		Return SMS Content
Setup	password＋A＋series number+T+tel number **Notice:** Series number = 0~9	Tel1: --- Tel2: --- Tel3: 13570810254 Tel4: --- Tel5: ---
Inquiry	password+A	Return all numbers
Delete	password+A+series number	Return 0~4 or 5~9 numbers.

9) Setup Daily Report time

SMS Command		Return SMS Content
Setup	password+DR+series number+T+time **Notice:** Series number =0~9, e.g.: 1234DR1T12:30	Daily SMS Report at: xx:xx
Inquiry	password+DR	
Delete	password+DRDEL	

10) Inquiry DIN Status

SMS Command		Return SMS Content
Inquiry Status	password+DINE	DIN1:Open/Close DIN2: Open/Close -----

11) Set Digital Output

SMS Command		Return SMS Content
Set DO Name	password+DO+channel number+T	DOx:xxxx
Inquiry DO Name	password+DO+ channel number<nnnn>	
Delete DO Name	password+DO+ channel number+DEL	
Switch ON(Close)	password+DOC+ channel number<nnnn> , can close multi channel, till next event trigger or SMS command.	DOx: ON DOy:ON
Switch OFF(Open)	password+DOO+ channel number<nnnn>	DOx: OFF

		DOy:OFF
Inquiry DO Current Status	password+DOE+ channel number<nnnn>	DOx: ON/OFF DOy:ON/OFF
Inquiry all DO Current Status	password+DOE	DO1: ON/OFF DO2:ON/OFF ---
Time Switch ON (Close)	password+DOLC+ channel number<nnnn> , can close multi channel, till time setting in configurator software finished.	
Set Pulse Output time	password+DOT+xxx (3 digital, unit is seconds)	Pulse Output Time:xxxS
Inquiry pulse output time	password+DOT	Pulse Output Time:xxxS
Pulse Ouput	password+DOP+channel number<nnnn>	No SMS Return

12) Setup AIN

SMS Command		Return SMS Content
Set Threshold	password+AINR+channel number+Lxxx+Hxxx	AINx: Low:xxx,High:xxx.
Inquiry Threshold	password+AINR+ channel number<nnnnnnnn>	AINx: Low:xxx, High:xxx. AINy: Low:xxx, High:xxx.
Delete Threshold	password+AINR+ channel number+DEL	
Set AIN measurement range	password+AINM+ channel number+Lxxx+Hxxx	AINx: Min:xxx,Max:xxx
Inquiry measurement range	password+AINM+ channel number<nnnnnnnn>	AINx: Min:xxx, Max:xxx. AINy: Min:xxx, Max:xxx.
Delete measurement range	password+AINM+channel number+DEL	
Inquiry AIN Current Value	password+AINE+channel number<nnnnnnnn>	AINx：xxxx ,+【Normal/Higher/Lower】
Inquiry All AIN Current Value	password+AINE	AIN0：xxxx ,+【Normal/Higher/Lower】 AIN1：xxxx ,+【Normal/Higher/Lower】 ----

13) Set Server Parameter(Can not setup DNS by SMS)

SMS Command		Return SMS Content
Set Server IP	password+IP+ IP address+P+Com port	Server: Port:
Inquiry	password+IP	Server: Port:
Delete	password+IPDEL	Server: Port:0

14) Set GPRS APN/USER NAME/PASSWORD

SMS Command		Return SMS Content
Set	password+AP+apn+#+username+#+user password	APN: User Name: Password:
Inquiry	password+AP	
Delete	password+APDEL	

15) GPRS Online

SMS Command	Return SMS Content
password+GPRSonline	GPRS always online

16) Delete Historical Data

SMS Command	Return SMS Content
password+HISDEL	Delete all historical records

17) Clear/Inquiry Pulse Counter Value

SMS Command		Return SMS Content
Clear Pulse Counter Value	password+DIN0CLR	Clear Successfully
Inquiry Pulse Counter Value	password+PR	Counter Current Value: XX

10. S47X Register Address

Tips: *All address in S47X Register Table displayed as Decimal data.*

Read &Write Holding Coil (Function Code 01, Function Code 05, Function Code 15.)			
Register Address (Decimal)	**Definition**	**Data Type**	**Description**
0	DO0	Bool	1:Relay close 2:Relay open
1	DO1	Bool	
2	DO2	Bool	
3	DO3	Bool	

Read input Coil (Function Code 02:Read coil.)			
Register Address (Decimal)	**Definition**	**Data Type**	**Description**
0	DIN0	Bool	when dry contact, NC=1, NO=0; When wet contract, 0~0.5V=1, 3~24V=0
1	DIN1	Bool	
2	DIN2	Bool	
3	DIN3	Bool	
4	DIN4	Bool	
5	DIN5	Bool	
6	DIN6	Bool	
7	DIN7	Bool	

Read input Register (Function Code 04:Read input register.)			
Register Address (Decimal)	**Definition**	**Data Type**	**Description**
0-1	AIN0	32 Bit int	Y=X/100
2-3	AIN1	32 Bit int	Y=X/100
4-5	AIN2	32 Bit int	Y=X/100
6-7	AIN3	32 Bit int	Y=X/100
8-9	AIN4	32 Bit int	Y=X/100
10-11	AIN5	32 Bit int	Y=X/100

12-13	(reserved, not work)	---	---
14	Power voltage	16 Bit int	Y=X/100
15-23	(reserved, not work)	---	---
24	Temperature	16 Bit int	Y=X/100
25	Humidity	16 Bit int	Y=X/100
26-27	DIN0 count value	32 Bit iunint	This value Enable when DIN0 as counter mode
28-29	DIN1 count value	32 Bit unint	This value Enable when DIN1 as counter mode
30-31	DIN2 count value	32 Bit unint	This value Enable when DIN2 as counter mode
32-33	DIN3 count value	32 Bit unint	This value Enable when DIN3 as counter mode

Tips: *In description, the parameter definition as below:*

Y= Real value; X=The value stored in register;

"Y=X/100" means "Real value= Current value stored in register/100"

Read &Write Holding Coil (Function Code 03 Function Code 06, Function Code 16.)			
Register Address (Decimal)	**Definition**	**Data Type**	**Description**
90（**bit0**）	DI0 clear	Bool	Write 1 to clear the DI Count value
90（**bit0**）	DI1 clear	Bool	
90（**bit0**）	DI2 clear	Bool	
90（**bit0**）	DI3 clear	Bool	

11. Slave Mapping Register Address

Boolean Slave Register Assignment Table

Holding Coil (Function Code 01, Function Code 05, Function Code 15.)			
Boolean Register Address (Decimal)	**Definition**	**Flag (MQTT)**	**Description**
64	Boolean 64	REG64	Boolean type, slave mapping address, can mapping slave input coil and holding coil status.
65	Boolean 65	REG65	Same as above
……	64 data similar as above	……	Same as above
127	Boolean 127	REG127	Same as above

16 Bit Slave Register Assignment Table

Read and Write Holding Register (Function Code 03,Function Code 06, Function Code 16)				
16 Bit Register	**Definition**	**Flag**	**Data Type**	**Description**

Address (Decimal)		(MQTT)		
20000	16 Bit data 20000	REG20000	Sort AB, its data type according to slave mapping data type	According to configurator set mapping rules, this address will sort slave mapping data to AB, stock in this address, for cloud easy reading together, can mapping slave inputting and holding register.
20001	16 Bit data 20001	REG20001	Same as above	Same as above
20002	16 Bit data 20002	REG20002	Same as above	Same as above
…….	128 data similar as above	…….	Same as above	Same as above
20127	16 Bit data 20127	REG20127	Same as above	Same as above

32 Bit Slave Register Assignment Table

Holding Register				
32 Bit Register Address (Decimal)	**Definition**	**Flag (MQTT)**	**Data Type**	**Description**
20128	32 Bit data 20128	REG20128	Sort ABCD, its data type according to slave mapping data type	According to configurator set mapping rules, this address will sort slave mapping data to ABCD, stock in this address, for cloud easy reading together, can mapping slave inputting and holding register.
20130	32 Bit data 20130	REG20130	Same as above	Same as above
20132	32 Bit data 20132	REG20132	Same as above	Same as above
…….	64 data similar as above	…….	Same as above	Same as above
20254	32 Bit data 20254	REG20254	Same as above	Same as above

64 Bit Slave Register Assignment Table

Holding Register				
64 Bit Register Address (Decimal)	**Definition**	**Flag (MQTT)**	**Data Type**	**Description**
20256	64 Bit data 20256	REG20256	Sort ABCDEFGH, its data type according	According to configurator set mapping rules, this address will sort slave

			to slave mapping data type	mapping data to ABCDEFGH, stock in this address, for cloud easy reading together, can mapping slave inputting and holding register.
20260	64 Bit data 20260	REG20260	Same as above	Same as above
20264	64 Bit data 20264	REG20264	Same as above	Same as above
…….	60 data similar as above	…….	Same as above	Same as above
20508	64 Bit data 20508	REG20508	Same as above	Same as above

12. MQTT Flag and Cloud Platform

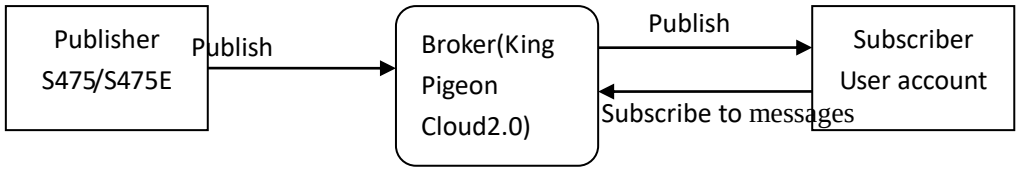
Introduction to mqtt

MQTT is a client-server based message publish/subscribe transfer protocol. The MQTT protocol is lightweight,simple, open, and easy to implement. These characteristics make it applicable to a wide range. In many cases,including restricted environments, such as: machine-to-machine (M2M) communication and Internet ofThings (IoT). It has been widely used in communication sensors via satellite links, occasionally dialed medicaldevices, smart homes, and some miniaturized devices. The MQTT protocol runs on TCP/IP or other network protocols and provides orderly, lossless, bidirectional connections.

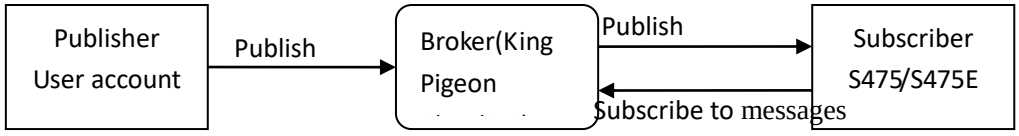
Implementation principle of mqtt

There are three kinds of identities in the MQTT protocol: publisher (Publish), broker (Broker) (server), and subscriber (Subscribe). Among them, the publisher and subscriber of the message are both clients, the message broker is the server, and the message publisher can also be a subscriber. Take S475/S475E connected to King Pigeon cloud 2.0 platform as an example:

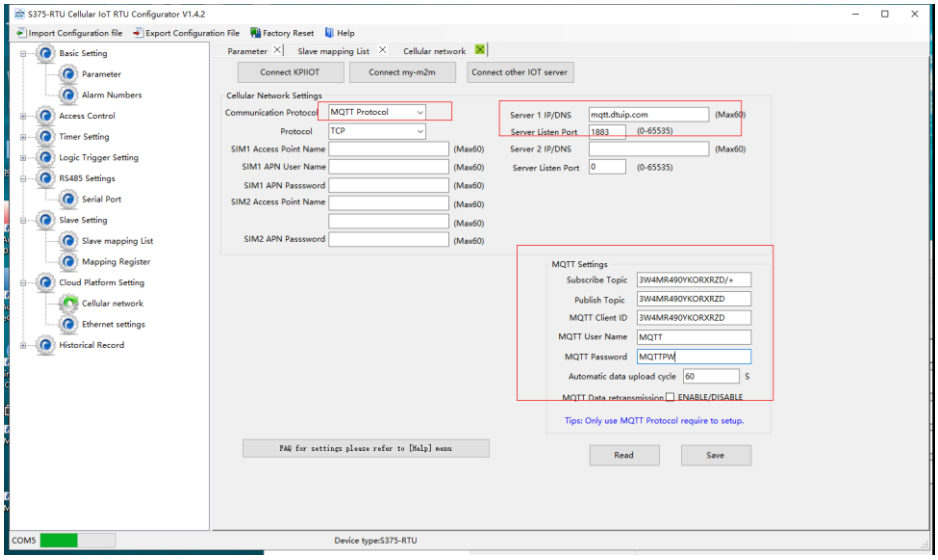
When the equipment releases IIO point data:



When the customer controls the equipment:



Client configuration



1) Communication protocol: MQTT protocol
2) Server IP domain name: King Pigeon Cloud 2.0 default:mqtt.dtuip.com
3) Port: Broker Server Port number（King Pigeon Cloud 2.0 default:1883）.
4) Subscription topic: Client subscribe topic (King Pigeon cloud 2.0 default: serial number/ +)
5) Publish topic: Device publish data topic (King Pigeon cloud 2.0 default: serial number/ +).
6) Mqtt client ID: the unique identification, which can be serial number, device ID, or IMEI code (KingPigeon Cloud 2.0 default is serial number)
7) Mqtt user name: Device's account on the broker server (King Pigeon Cloud 2.0 default is MQTT)
8) Mqtt password:Password of device's account on the broker server(King Pigeon Cloud 2.0 default is MQTTPW)

After the configuration is completed, the client will initiate a connection to the server:

Connect: the client sends a connect message request to the server;

Connack: the server responds to a connack confirmation message, indicating that the connection is successful;

After the client establishes a connection, it is a long connection, and the client can publish or subscribe messages on the server;

Take devices and customers' mobile phones as clients

After the device publishes the topic on the proxy server, customers can view the data through subscription.That is, the device is the publisher, and the customer's mobile phone is the subscriber.

Similarly, users can control the device by publishing topics through the mqtt server.That is, the user is the publisher and the device is the subscriber.

Payload data format in equipment release message

Publish Topic: MQTT client ID (filled in configuration software)

```
{
        "sensorDatas":
        [
            {
                "flag":"DI1",              Read write identification
                "switcher":1               Data type and value
            },
            {
                "flag":"AI1",
                "value":10.00
            },
            {
                "flag":"REG64",
                "switcher":0
            },
            {
                "flag":"REG20000",
                "value":1.00
            }
        ],
        "time":"1591841863",
        //Time stamp (When power on,first time connection no time stamp,later connectionshave time stamp)

        "state":"alarm",
       //Alarm and recovery identification (only for alarm or recovery data, but nottimly report)

        "retransmit":"enable"
       //Historical data identification (only for re-transmission of historical data, but not for real-time data)
    }
```

Note:

Read / write identifier: the character is "flag", followed by "read / write ID representing IO data point"

Data type and value: it can be divided into:

1. Switch data: the character is "switcher", followed by "0" or "1" (0 for open, 1 for closed)
2. Numerical data: the character is "value", followed by "specific value"

Time identification: the character is "time", followed by "specific reporting time stamp"

Alarm and recovery identification: the character is "state", followed by "alarm" or "recovery" (alarm represents alarm data and recovery represents recovery data)

Historical data identifier: character "retransmit", followed by "enable"

The data collected during the network disconnection will be temporarily stored in the device, and will be redistributed when the network is restored. The "retransmit" field is used to identify the historical data.(it is necessary to check enable mqtt data supplementary transmission function in the configuration software)

Payload data format in device subscription message

(The topic of the King Pigeon 2.0 platform downstream publish message is called "device serial number/sensor ID", so the device subscribe topic needs to add the wildcard "/+" in order toreceive the data sent by the platform to achieve control)Subscribe topic: device serial number /+(corresponding to the data filled in the subscribe topic item on the configuration software)

```
{
    "sensorDatas":
    [
        {
            "sensorsId": 211267,    //Platform sensor ID
            "switcher":1,           //Data type and value
            "flag":"DO1"            //Read write identification
        }
    ],
    "down":"down"                   Platform downlink message identification
}
```

Note:

Platform sensor ID: character is "sensorid", followed by ID number (ID is automatically generated by platform)

Data type and value: it can be divided into:

1. Switch data: the character is "switcher", followed by "0" or "1" (0 for open, 1 for closed)
2. Numerical data: the character is "value", followed by "specific value"

Read / write identifier: the character is "flag", followed by "read / write ID representing IO data point"

Platform downlink message identification: the character is "down", followed by "down", which means that this is the platform downlink data.

Device I/O data point read and write flag

Data name	Read write flag	Data type	Description
DO	DOx	Switcher	0 is open, 1 is closed
DI	DIx	Switcher	0 is open, 1 is closed
AI	AIx	Value	True value = original value
Temperature	TEMP	Value	True value = original value
Humidity	HUMI	Value	True value = original value
External power voltage	EXTPWR	Value	True value = original value
DI0 pulse count value	COUNT	Value	True value = original value
DI1 pulse count value	COUNT1	Value	True value = original value
DI2 pulse count value	COUNT2	Value	True value = original value
DI3 pulse count value	COUNT3	Value	True value = original value

Note:

"DOX" means: DO0, DO1, DO2, DO3;

"Dix" means: DI0, DI1, DI 2, DI3, DI4, DI5, DI6, DI7;

"AIX" means: AI0, AI1, AI2, AI3, AI4, AI5.

Expand IO data point read and write flag

Data name	Read write flag	Data type	Description
Boolean data	REG64~REG127	Switcher	According to the slave register data definition
16 bit data type	REG20000~REG20127	Value	According to the slave register data definition
32 bit data type	REG20128~REG20254	Value	According to the slave register data definition
64 bit data type	REG20256~REG20508	Value	According to the slave register data definition

Note:

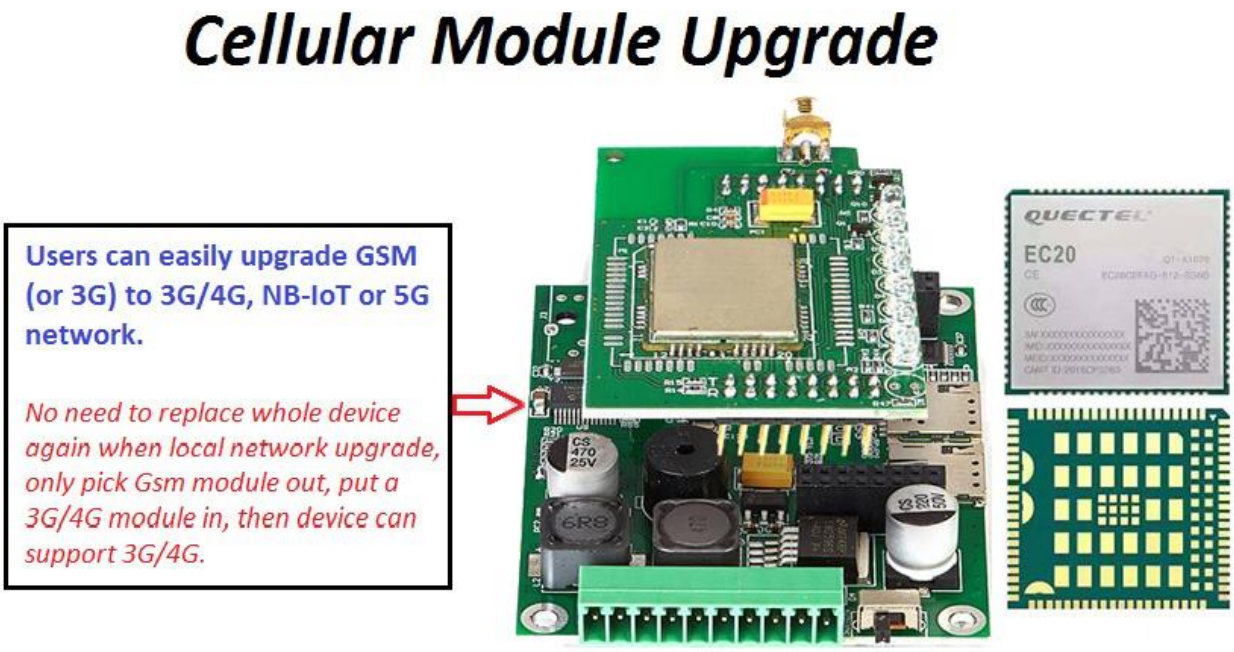
Expand IO read and write ID to "REGx" (x is the mapping register address, please check the detailed addressAppendix C Modbus**Expand IO data point**mappingregister address

13. Upgrade Firmware

The device supports upgrade firmware via USB port directly. If you required upgrade, please contact us to discuss and modify the firmware according to you requirements, we can provide the upgraded firmware to you to upgrade them.

14. Cellular Module Upgrade

The device adopt modular structure design, when user local Gsm operator upgrade network, no need to replace the whole hardware, only need to replace inbuilt communication module, easily upgrade Gsm to 3G, or 3G to 4G network.



15. Warranty

1) This system is warranted to be free of defects in material and workmanship for one year.
2) This warranty does not extend to any defect, malfunction or failure caused by abuse or misuse by the Operating Instructions. In no event shall the manufacturer be liable for any alarm system altered by purchasers

The End!
Any questions please help to contact us feel free.
Http://www.IOT-Solution.com