

v1.0

# **HZS1006000-F1 Signal Source Instructions**

v1.0

Catalog

HZS1006000-F1 Signal Source Instructions .....	1
1. Product Description .....	3
1.1 Product Overview .....	3
1.2 Product Appearance .....	3
1.3 Product Parameters .....	4
1.4 Hardware Interface .....	5
1.5 Host computer instructions .....	7
2. Signal Update Guide .....	11
2.1 Signal name .....	11
2.2 Signal naming conventions .....	11
2.3 Storage method .....	12
3. API Usage Guide .....	14
3.1 HZS1006000-F1 AT Command Instructions .....	14
3.2 Basic AT commands .....	14
3.3 Detailed usage process example .....	16
3.4 Cascade device selection process .....	19
3.5 Instructions for using the cascade software .....	22
4. Signal Source Firmware Update Guide .....	24
4.1 Firmware name .....	24
4.2 Update Method .....	24

# 1. Product Description

## 1.1 Product Overview

HZS1006000-F1 is a high-performance software-defined radio (SDR) signal generator. Its digital baseband source can generate drone jamming signals with various digital modulation schemes, which are then converted into radio frequency signals through an SDR platform.

The digital source supports an output frequency range of 100 MHz to 6000 MHz, with bandwidth adaptively configurable based on the selected jamming waveform, reaching a maximum of 200 MHz while maintaining precise frequency characteristics.

The module allows selection of corresponding digitally modulated jamming waveforms for different types of drones to achieve optimal countermeasure effects. It supports effective jamming against common protocols including ELRS, Crossfire, Flysky, Ocusync, Lightbridge, and Syncleas.

This product features a compact form factor, flexible interfaces, and simple integration.

## 1.2 Product Appearance

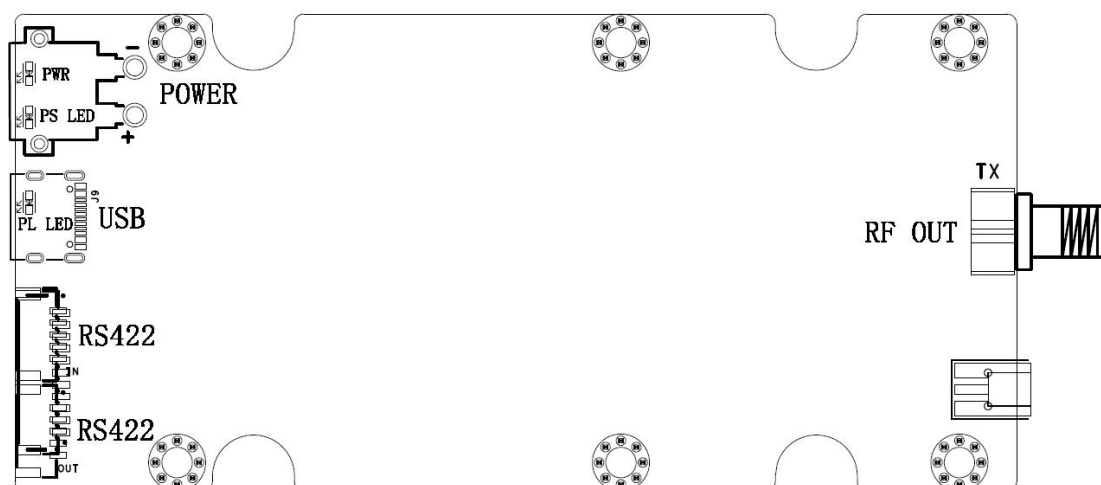




Figure 1-1 Product appearance pictures

## 1.3 Product Parameters

The product parameters are shown in the following table

Table 1-1 Product parameters

Name	Parameters	Notes
Operating voltage	DC: 28-32V	DC_IN
Working current	0.27A Max	
Frequency coverage	100M-6000MHz	
Maximum real-time bandwidth	200MHz	
Output dynamic range	>25dbm	Gain level up to 35 levels
Maximum output power	>5dbm(CW mode, typical value)	There will be differences in different frequency tests
Output frequency accuracy	<0.1MHz	
RF output interface	SMA	RF OUT
Module size	105mm * 50mm	
Communication control interface	RS422	

---

module weight	120 g
---------------	-------

operating temperature	0 - 50
-----------------------	--------

---

## 1.4 Hardware Interface

### 1.4.1 Communication interface

The module is configured via RS422 and uses a GH series 5P connector. The interface definition is as shown below:

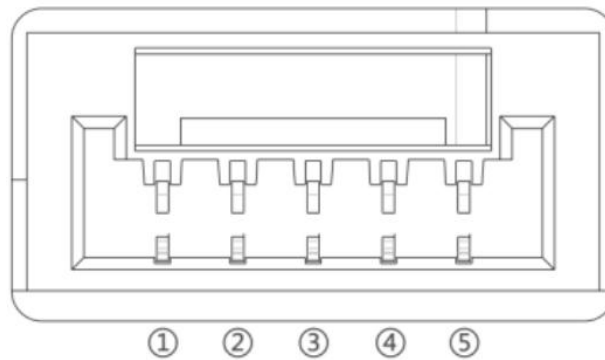


Figure 1-2 GH series 5P connector interface diagram

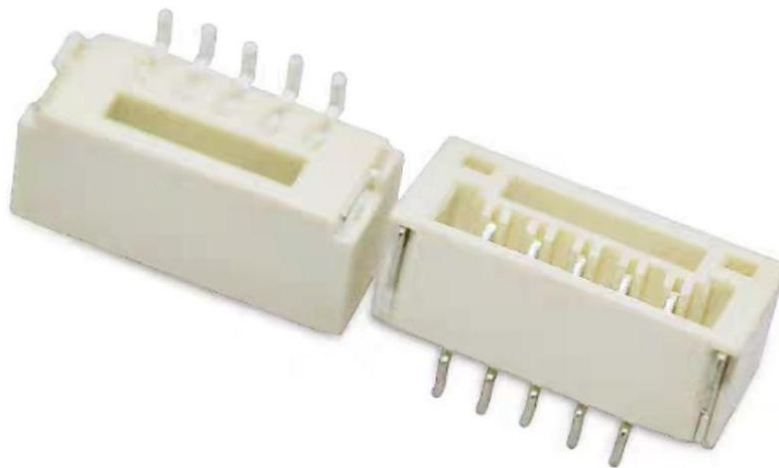


Figure 1-3 Appearance of the GH series 5P connector

The definition of each interface is shown in the following table:

Table 1-2 GH series 5P connector pin definition

Pin Number	Name	Input/Output	Description
1	Y	Output	Driver Non-Inverting Output
2	Z	Output	Driver Inverting Output
3	GND	/	Ground
4	B	Input	Driver Inverting Input
5	A	Input	Driver Non-Inverting Input

### 1.4.2 Power supply interface

The module is equipped with an XT30 model aircraft male connector to ensure stable and reliable power supply. The interface definition is as shown below. The signal source module uses 28V power supply.

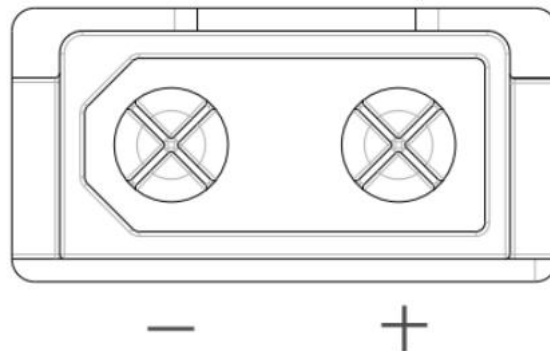


Figure 1-4 Signal generator XT30 power supply diagram

Connect the XT30 female connector to the 28V power interface to power it.



Figure 1-5 Signal generator XT30 power supply cable

### 1.4.3 RF Output port

The module output port is SMA female, as shown below



Figure 1-6 Signal generator RF output port

## 1.5 Host computer instructions

1.5.1 Before operation, you need to prepare a USB to RS422 cable and connect it to the computer as shown in the figure:



Figure 1-7 RS422 connection cable

1.5.2 Connect the signal source module to the computer with a USB to RS422 cable.

The connection method is shown in the figure



Figure 1-8 RS422 connection method

Install the CH340 driver on the computer, connect the 28V power supply to the signal source module, and double-click to open the control software.

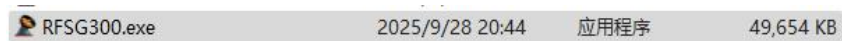


Figure 1-9 Signal source control software

When you open it, you will see the interface shown below

Figure 1-10 Signal source control software

1.5.3 Port: When the USB to 422 cable is inserted, the port will automatically display and wait for the signal source to start. After the startup is successful, click to open port. The following page will be displayed.

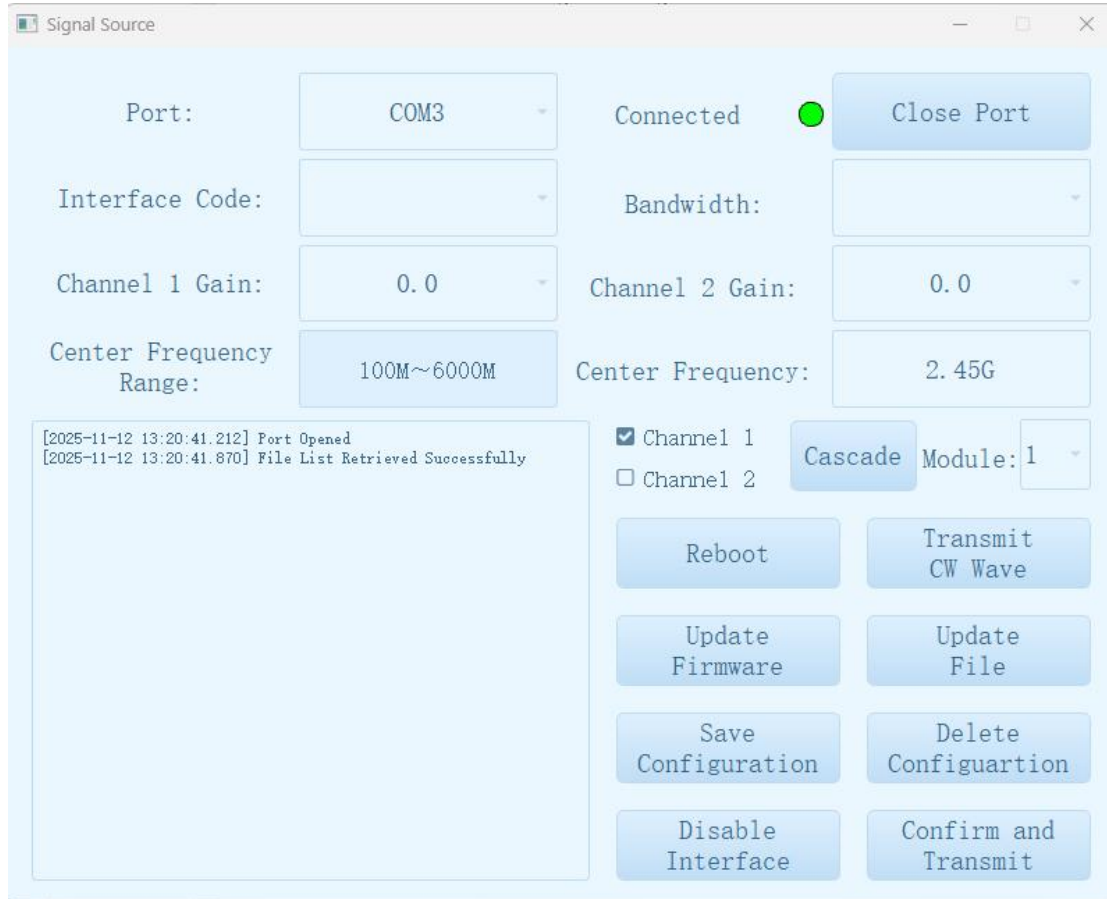


Figure 1-11 Select Open port

1.5.4 At this time, first select the interference code, then select the bandwidth and set the center frequency. For example, if the current bandwidth is 150M and the center frequency is 2.45G, the actual frequency of the interference code is 2375MHz - 2525MHz, 2.45G is the center frequency, and the bandwidth is 75M on each side.



Figure 1-12 Selecting the interference code

1.5.5 Click Confirm and Transmit to send the interference.

1.5.6 If you want to save the current configuration, just click **Save Configuration**, and the current configuration will be automatically executed the next time you start.

1.5.7 If you do not need to save the configuration and only want to test the function, please **Delete Configuration** and restart the test. RFSG can output various types of interference signals. Currently, the available interference code types are:

1. ELRS
2. GNSS
3. ofdm
4. lfm
5. TBS\_ELRS\_A
6. ELRS\_2450A
7. TBS

## 2. Signal Update Guide

HZS1006000-F1 is a high-performance software-defined radio signal generator. Users can update signals via USB and transmit customized signals.

### 2.1 Signal name

The signal name is name\_0m.sc16, as shown below, where the format name\_0m.sc16 is defined as a custom signal.

名称	大小	类型	已修改
885ELRS868915_0m.cs16	983.0 kB	未知	2025年8月26日 16:05
885TBS868915_0m.cs16	983.0 kB	未知	2025年8月26日 15:59
ELRS2450A_0m.cs16	2.5 MB	未知	2025年8月26日 16:32
ELRS_0m.cs16	491.5 kB	未知	2025年8月20日 19:29
GNSS_0m.cs16	491.5 kB	未知	2025年8月20日 19:46
lfm_signal_5m.cs16	245.8 kB	未知	2025年8月21日 16:55
lfm_signal_10m.cs16	245.8 kB	未知	2025年8月21日 17:51
lfm_signal_40m.cs16	245.8 kB	未知	2025年8月21日 17:50
ofdm_signal_5m.cs16	102.4 kB	未知	2025年8月19日 17:45
ofdm_signal_10m.cs16	102.4 kB	未知	2025年7月29日 14:44
ofdm_signal_40m.cs16	102.4 kB	未知	2025年8月20日 15:46
rfsg300	8.8 MB	未知	2025年10月13日 14:39
TBS_0m.cs16	491.5 kB	未知	2025年8月20日 21:33
TBSELRSA_0m.cs16	983.0 kB	未知	2025年8月26日 16:10

Figure 2-1 IQ file

### 2.2 Signal naming conventions

**name\_0m.c16** , The signal is a signal ending in .cs16, a binary file, the data type is int16, and the arrangement is I1 Q1 I2 Q2... If the user needs to add a custom signal, , You need to replace **name** with your own signal name, which can be a combination of letters and numbers. .sc16 is the file extension, indicating that the file type is a 16-bit complex signal (IQ). \_0m is a fixed identifier used by the system to identify the signal version.

## 2.3 Storage method

2.3.1 Use a USB data cable to connect the computer to the HZS1006000-F1 signal source device, as shown in the figure below. After the connection is successful, a removable disk (U disk) with a capacity of approximately 32 MB will automatically pop up on the computer.



Figure 2-2 Connecting the signal source to the signal source

2.3.2 The following device description is displayed on the computer: Connection is successful.



Figure 2-3 Signal source USB disk

2.3.3 Copy the prepared custom signal file ( test\_0m.sc16) to the USB drive.

2.3.4 After copying the file, be sure to safely unmount the USB drive using the operating system's eject function to ensure the data is written intact.



Figure 2-4 Update File Button

2.3.5 Reopen the HZS1006000-F1 control software and click the **Update File button** on the main interface. The device will automatically read the newly uploaded signal file and complete the update.

2.3.6 After the update is complete, restart the signal source device. The signal source software will automatically recognize and read the signal file. You can then select a custom file from the drop-down list and start transmitting. To automatically execute the current configuration at power-up, click Save Configuration. This will automatically execute the next time you power on the device.

## 3. API Usage Guide

### 3.1 HZS1006000-F1 AT Command Instructions

HZS1006000-F1 High-Performance Software-Defined Radio Signal Generator

The HZS1006000-F1 is a high-performance software-defined radio (SDR) signal generator that supports control via serial AT commands. This device features a dual-PHY chip architecture, enabling simultaneous or independent control of two RF channels.

The RFSG can transmit jamming signals of up to 200 MHz bandwidth using the RS422 communication protocol interface. Users can operate the device with the provided software or develop their own custom applications. The HZS1006000-F1 can be controlled via AT commands to output various types of jamming signals, including the following:

1. ELRS
2. GNSS
3. OFDM
4. LFM
5. TBS\_ELRS\_A
6. ELRS\_2450A
7. TBS

### 3.2 Basic AT commands

Table 3-1 Basic AT commands

Command	Function	Response
AT	Test device connection status	OK
AT+HELP	Display all supported AT commands	List all available commands
AT+GMR	Query firmware information	Firmware version information
AT+RST	Restart device	System_will_reboot_now
AT+FREQ=Frequency value	Set transmit center frequency	AT+FREQ_OK
AT+BW	Set bandwidth	AT+BW_OK
AT+GAIN1	Set channel 1 gain	AT+GAIN1_OK
AT+GAIN2	Set channel 2 gain	AT+GAIN2_OK
AT+STATUS	Query current device status	List device status
AT+CW	Continuous wave mode	AT+CW_OK
AT+SAVEIQFILE	Save signal file	AT+SAVEIQFILE_OK
AT+STOPLOAD	Stop transmitting	AT+STOPLOAD_OK
AT+FILE	View signal file list	List all signal names
AT+LOADIQFILE	Load signal file	The signal is emitted
AT+SAVECFG	Save current configuration	AT+SAVECFG_OK
AT+RFSG_UPDATEFRM	Update firmware	The firmware will reboot after a successful update.
AT+DELCFG	Delete configuration file	AT+DELCFG_OK
AT+RFSGPHY1	Select channel 1	PHY1_Selected
AT+RFSGPHY2	Select channel 2	PHY2_Selected
AT+RFSGPHY1_2	Enable both channels	PHY1_2_Selected
AT+RFSGID	Select the corresponding	RFSG_ID_OK

### 3.3 Detailed usage process example

#### 3.3.1 Scenario 1: Sending OFDM interference signal

Goal: Send a 30MHz bandwidth OFDM interference signal in the 2.4GHz band

AT

AT+RFSGPHY1

AT+STOPLOAD

AT+BW=30

AT+FREQ=2400000000

AT+GAIN1=35

AT+LOADIQFILE=ofdm\_signal\_10m.cs16

#### 3.3.2 Scenario 2: Sending LFM sweep signal

Goal: Transmit a 160MHz bandwidth LFM signal in the 2400MHz band

AT

AT+STOPLOAD

AT+BW=160

AT+FREQ=2400000000

AT+GAIN1=15

AT+GAIN2=15

AT+LOADIQFILE=lfm\_signal\_40m.cs16

AT+STATUS

#### 3.3.3 Scenario 3: Interference with the TBS remote control link

Target: Jam TBS Crossfire remote control at 868MHz

AT

AT+STOPLOAD

AT+RFSGPHY1

v1.0

AT+BW=0

AT+FREQ=885000000

AT+GAIN1=15

AT+LOADIQFILE=TBS\_0m.cs16

### **3.3.4 Scenario 4: Interference with the ELRS remote control link**

Target: Jam the ExpressLRS remote control at 915MHz

AT

AT+STOPLOAD

AT+RFSGPHY1

AT+BW=0

AT+FREQ=915000000

AT+GAIN1=10

AT+LOADIQFILE=ELRS\_0m.cs16

### **3.3.5 Scenario 5: Transmitting GNSS interference signals**

Target: Interfere with GPS/Beidou navigation systems

AT

AT+STOPLOAD

AT+RFSGPHY1

AT+BW=0

AT+FREQ=1585000000

AT+GAIN1=15

AT+LOADIQFILE=GNSS\_0m.cs16

### **3.3.6 Scenario 6: Sending ELRS2450A Signal**

Target: Send ELRS2450A signal

AT

AT+STOPLOAD

AT+BW=0

v1.0

AT+FREQ=900000000

AT+GAIN1=15

AT+LOADIQFILE=ELRS2450A\_0m.cs16

### **3.3.7 Scenario 7: Continuous Wave Mode**

Goal: Send a single carrier signal

AT

AT+STOPLOAD

AT+FREQ=2400000000

AT+CW

### **3.3.8 Scenario 8: Simultaneous interference with the TBS remote**

#### **control link**

AT

AT+STOPLOAD

AT+BW=0

AT+FREQ=885000000

AT+GAIN1=15

AT+LOADIQFILE=885TBS868915\_0m.cs16

AT+STATUS

### **3.3.9 Scenario 9: Send ELRS\_868\_915**

AT+STOPLOAD

AT+BW=0

AT+FREQ=885000000

AT+GAIN1=15

AT+LOADIQFILE=885ELRS868915\_0m.cs16

### **3.3.10 Scenario 10: Sending TBS+ELRS\_A**

AT+STOPLOAD

v1.0

AT+BW=0

AT+GAIN1=15

AT+FREQ=885000000

AT+LOADIQFILE=TBSELRSA\_0m.cs16

### **3.3.11 Configuration saving and restoration process**

Save the current configuration:

Set all parameters and save the configuration

AT+SAVECFG

Deleting a Configuration:

Clear saved configuration

AT+DELCFG

### **3.3.12 PHY Selection Process**

Use only PHY1:

AT+RFSGPHY1

Use only PHY2:

AT+RFSGPHY2

Use dual PHY mode:

AT+RFSGPHY1\_2

## **3.4 Cascade device selection process**

When operating devices, each device has a unique device number, which is used to control the corresponding number of devices in the cascade, and is unique for each device number .

### **How to confirm the device number:**

Step 1: Connect the USB to the USB interface of the signal source .



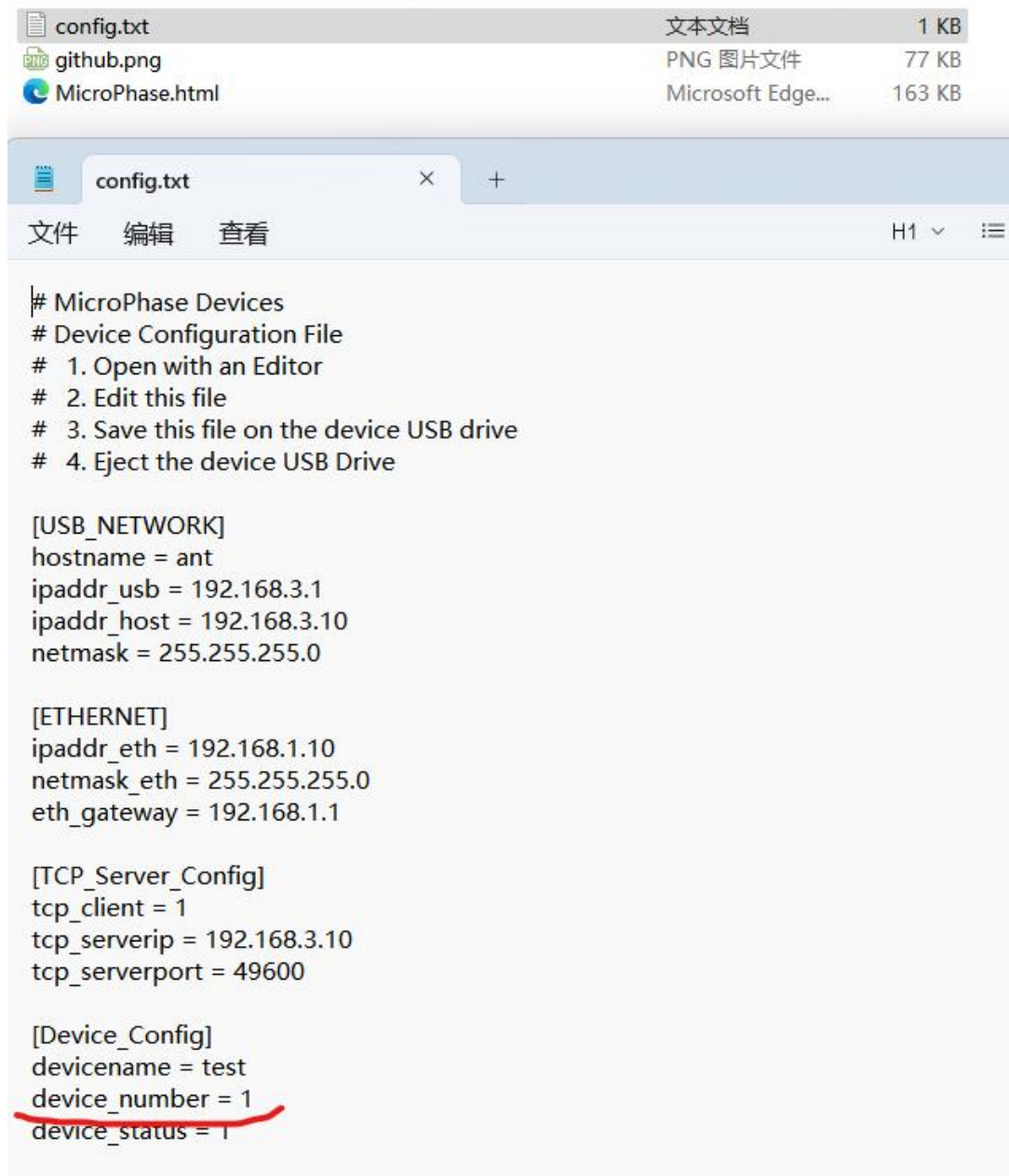
Figure 3-1 Connecting a USB to a signal source

Step 2: See the following instructions on your computer indicating successful connection .



Figure 3-2 Signal source U disk

Step 3: Open the USB key, select the config.txt file and open it :



```
# MicroPhase Devices
# Device Configuration File
# 1. Open with an Editor
# 2. Edit this file
# 3. Save this file on the device USB drive
# 4. Eject the device USB Drive

[USB_NETWORK]
hostname = ant
ipaddr_usb = 192.168.3.1
ipaddr_host = 192.168.3.10
netmask = 255.255.255.0

[ETHERNET]
ipaddr_eth = 192.168.1.10
netmask_eth = 255.255.255.0
eth_gateway = 192.168.1.1

[TCP_Server_Config]
tcp_client = 1
tcp_serverip = 192.168.3.10
tcp_serverport = 49600

[Device_Config]
devicename = test
device_number = 1
device_status = 1
```

Figure 3.3 source configuration file

Step 4: device\_number is the number of the device, if you need to change the number of the device:

Step 4.1: Please change the number and eject the USB key.

Step 4.2: When the U disk is ejected, the device status light changes from slow flashing to fast flashing and then to slow flashing, indicating successful configuration.

Wait for successful configuration of the device.

Step 4.3: Restart the device to make the change.

Step 5: Use AT+RFSGID to select the corresponding number to control the corresponding device .

Step 6: Select the device and send AT+RFSGID= device number.

Step 7: Execute the other AT commands.

### 3.5 Instructions for using the cascade software

3.5.1 When using the signal source software, the cascade function is not available by default. When the cascade function is required, connect the devices properly according to the instructions. First, select the corresponding module number, and then click the cascade button to connect to the device.

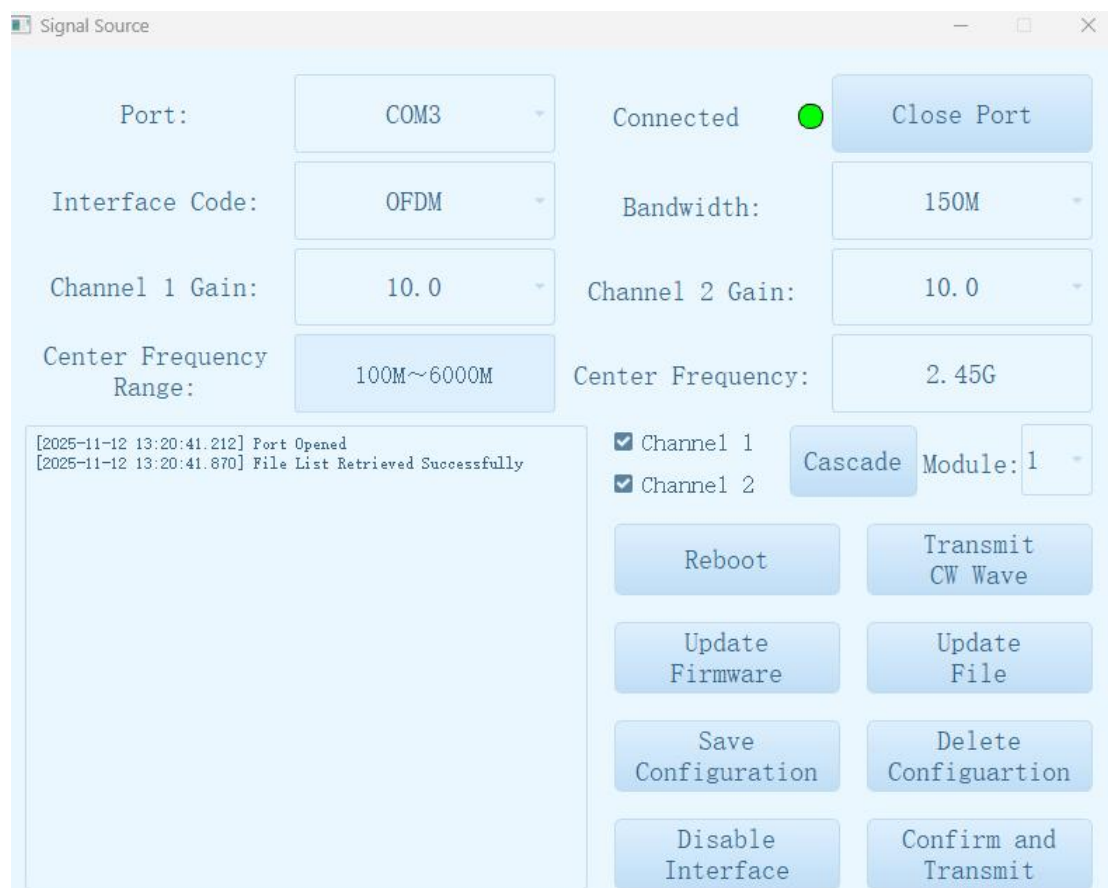


Figure 3.4 Opening the signal source software

3.5.2 Signal Source Connection Method: Connect the first signal source to the computer, and then connect the subsequent signal sources in series. Currently, up to 10 devices can be supported. The connection method is as shown in the figure.

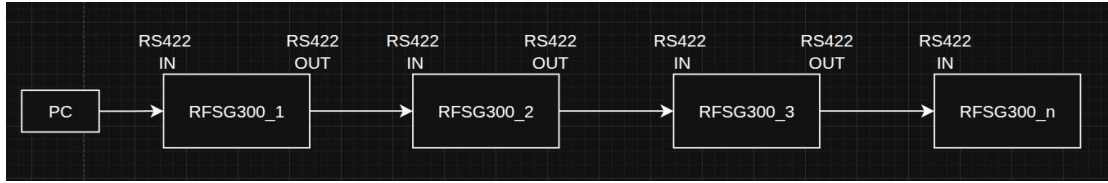


Figure 3.5 Signal source connection method

3.5.3 Then, open the signal source software, select the serial number of the signal source to be cascaded, and click the cascade button. At this point, other signals can be sent to operate it.

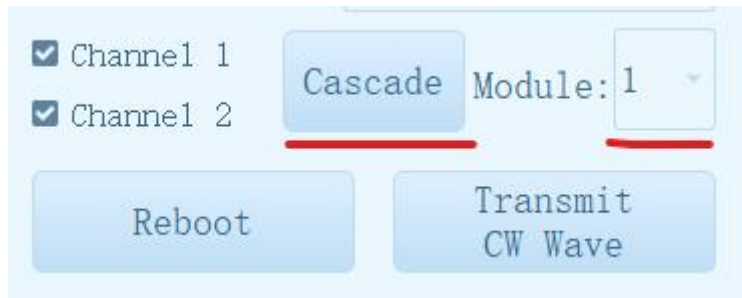


Figure 3.6.A cascade of buttons

## 4. Signal Source Firmware Update Guide

HZS1006000-F1 uses USB for firmware updates.

### 4.1 Firmware name

The firmware name is firmware.frm. This firmware is provided by us, as shown below. If you need to obtain the latest firmware, please contact us.

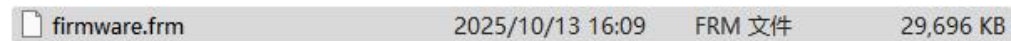


Figure 4-1 Signal source firmware

### 4.2 Update Method

#### 4.2.1 USB cable to connect computer and signal source device



Figure 4-2 Connecting USB to the signal source

4.2.2 The following device description is displayed on the computer: Connection is successful.



Figure 4-3 Signal source USB flash drive

### 4.2.3 Copy the firmware to the USB drive

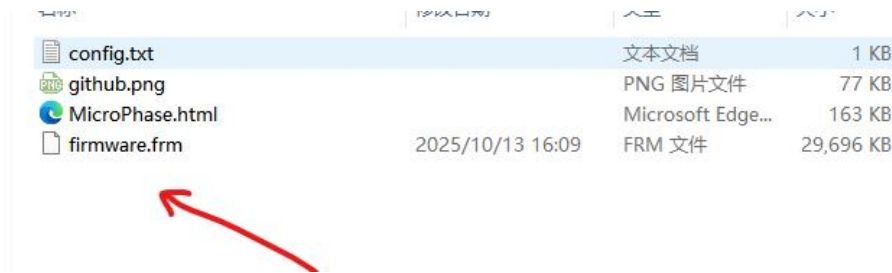


Figure 4-4 Put the firmware into the USB drive

4.2.4 After the file copy is complete, be sure to safely unmount the USB drive using the operating system's eject function to ensure that the data is fully written.

4.2.5 When U disk is ejected, the device status light changes from slow flashing to fast flashing

4.2.6 Wait 3 minutes, the indicator light changes from fast flashing to slow flashing, and the update can be completed by restarting the device.