

***CD30***

**Installation and Operation Manual for Unmanned Aerial Vehicle Detection, Positioning, and Countermeasures System**

Catalogs

[1.Overview 4](#_Toc175065406)

[2.Precautions 5](#_Toc175065407)

[3.Installation instructions 6](#_Toc175065408)

[3.1 Installation of fixed main equipment 6](#_Toc175065409)

[3.2Installation of fixed lightning rod 6](#_Toc175065410)

[3.3 Fixed Network Cable Installation 7](#_Toc175065411)

[3.4 Installation of mobile main equipment 8](#_Toc175065412)

[3.5 Mobile Network Cable Installation 8](#_Toc175065413)

[3.6 Installation of the operating computer 8](#_Toc175065414)

[4.Software Functions and Operating Instructions 9](#_Toc175065415)

[5. Software features and operating instructions 9](#_Toc175065416)

[5.1 Main interface of unmanned aerial vehicle defense system 10](#_Toc175065417)

[5.2 Automatic detection interface 11](#_Toc175065418)

[5.3 System Settings sub-screen 15](#_Toc175065419)

[5.3.1 Antenna Settings 15](#_Toc175065420)

[5.3.2 Detection frequency band settings 16](#_Toc175065421)

[5.3.3 Eliminating Detection Alarm Frequency Band Settings 17](#_Toc175065422)

[5.3.4 Network Settings 18](#_Toc175065423)

[5.3.5 Software and database updates 19](#_Toc175065424)

[5.4 Jamming interface 20](#_Toc175065425)

[5.5 Signal recording sub interface 20](#_Toc175065426)

[5.6 Equipment connection 21](#_Toc175065427)

[5.7 Platform Shutdown 21](#_Toc175065428)

[5.8 Advanced Features 21](#_Toc175065429)

[5.8.1 Lateral function of any signal 21](#_Toc175065430)

[5.8.2 Frequency hopping signal self-learning function 22](#_Toc175065431)

[6. Common problem handling 23](#_Toc175065432)

[7. Data analysis methods for advanced users 25](#_Toc175065433)

[7.1 Autonomous learning function 25](#_Toc175065434)

[7.2Analysis of detection results 25](#_Toc175065435)

# 1.Overview

As more and more drones fly into the sky, the safety hazards they pose when approaching important areas have become increasingly serious. Since 2016, there have been multiple incidents in China where civilian drones have intruded into the routes or airports of manned civil aircraft. Multiple drone intrusion incidents have emerged in important political venues both domestically and internationally; Prisons and border guards often engage in illegal and criminal activities using drones. On February 14, 2019, the "Management Regulations for Trial Operation of Specific Types of Unmanned Aerial Vehicles (Provisional)" was issued. According to the requirements of the regulations, personnel in the fields of trial operation approval, including flight markings, airworthiness, air traffic control, etc., were broken down from the boundaries of the management field, reducing repetitive evaluations by various operational management stakeholders, and improving the efficiency of evaluation and approval. Drone management requires early detection of drone equipment and methods. Although drone manufacturers have set airport no fly zones and restricted fly zones for drone products to ensure airspace security, drone intrusion incidents still occur frequently. Controlling drones through laws and regulations, as well as setting up no fly zones, cannot completely solve the safety hazards caused by drone black flights. In order to effectively enforce regulations, it is necessary to have means to obtain evidence of drones and leave evidence for punishment. At the same time, hostile and terrorist elements will not comply with this regulation. Therefore, Shenzhen WaveFeng Technology Co., Ltd. has independently developed a drone detection and jamming system based on smart radio with complete intellectual property rights, combined with the use of hardware environment, We have independently developed a platform software for unmanned aerial vehicle detection and jamming based on smart radio.

# 2.Precautions

(1) This product belongs to high-end precision equipment, please handle it carefully and do not fall!

(2) This product belongs to hierarchical manufacturing, please do not invert it!

(3) This product contains an internal signal receiver. Try to arrange it on the top floor of an unobstructed building or in an uninhabited and unobstructed open area!

(4) This product contains a signal receiver inside and should be placed on an unobstructed rooftop as much as possible! Try to avoid the radio transmitting equipment such as the mobile communication base station, absolutely can’t be installed with the same pole and column with the mobile communication base station, the same height, should be as far as possible away from the above equipment, and the height is lower than the above equipment.

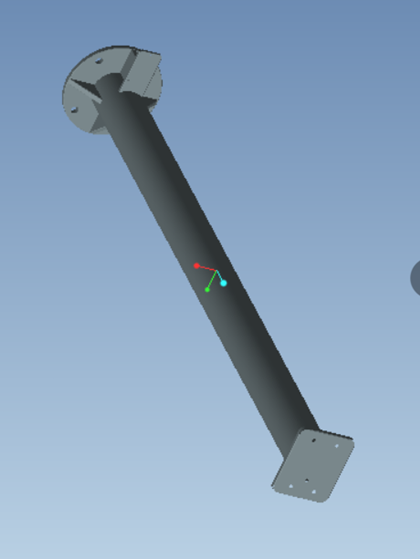
(5) This product belongs to special equipment and requires professional installation. Please do not install it yourself!

# 3.Installation instructions

## 3.1 Installation of fixed main equipment

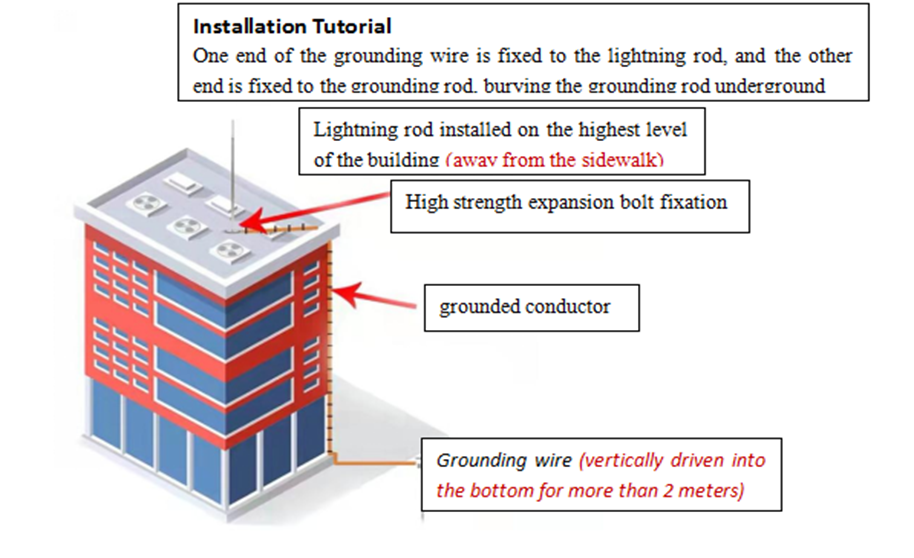
A. The fixed bracket needs to be fixed in the selected position by punching holes with explosive screws;

B. Align the arrow on the host chassis with the due north direction;

C. Install the host on the fixed bracket using four M5 screws;

## 3.2Installation of fixed lightning rod

Fixed installation. Due to the long-term outdoor exposure of the equipment, lightning rods should be installed to prevent lightning strikes. The lightning rods (not too thick to block the detection line of sight) should be higher than the height of the equipment, and the equipment is within the protection range of the lightning rods. Please refer to the following diagram for installation.



## 3.3 Fixed Network Cable Installation

A. Need to connect the network cable to the switch;

B. Connect the device and operating terminal to the same switch;(If the distance between the detection host and the operating computer does not exceed 30 meters, the network cable can also be directly connected to the detection host and the operating computer);

C. Host plugged into the power cord (pay attention to the use of 85V ~ 265V three-phase power line, in addition to the fire line, zero line should have a ground, good connection to the earth);

D. Set the address of the operating terminal and outdoor host of the device on the same network segment based on the website of the switch;

E. The network needs to be tested and connected. You need to input ping+address（Default 192.168.2.6） on the terminal(Default 192.168.2.100) to pass the test;

F. After connecting, start the computer and detect the host one by one;

G. Note that the transmission range of the network cable is roughly 30 meters to 50 meters, beyond which you will need to add a switch relay to enhance the network signal.

## 3.4 Installation of mobile main equipment

A. Select an open and unobstructed location;

B. Erect the bracket and open it;

C. Adjust the appropriate position to keep the platform of the bracket in a horizontal state;

D. Align the direction with due north according to the arrow on the host chassis;

E. Install the outdoor host of the equipment on the bracket;

F. Connect the power cord;

G. Connect the network cable.

## 3.5 Mobile Network Cable Installation

A. Connect the outdoor host of the device directly with a network cable.

B. After connecting the network cable, turn on the computer and detect the host one by one.

## 3.6 Installation of the operating computer

(Factory-installed system and software)

# 4.Software Functions and Operating Instructions

|  |  |
| --- | --- |
| ***Operating environment*** | ***Linux Ubuntu20.04 LTS；***  ***GNURADIO for Linux 12.04*** |

# 5. Software features and operating instructions

***The software has the following main functions:***

⑴. Drone detection

⑵. UAV Flight Control and Image Signal Recognition

⑶. Drone model identification

⑷. UAV positioning

⑸. Location of drone controller

⑹. Drone signal feature recording

⑺. Electronic map automatic positioning and display

⑻. Drone countermeasures

⑼. Drone trajectory tracking

⑽. Unattended

⑾. List of drones and remote-control detection results

⑿. Whitelist

## 5.1 Main interface of unmanned aerial vehicle defense system

Figure 1 shows the main interface of the C30 unmanned aerial vehicle detection and countermeasures system. It includes six functions: automatic detection, anti-emission, signal recording, device connection status display, system settings, and system shutdown.

Before using the system, it is necessary to ensure that the device and operating host are in a connected state, and the connected state icon is.

Figure 1 Operating System Main Interface

The six functions are as follows:



(1) Automatic detection function

(2) Anti launch function

(3) Signal recording function

(4) System settings function

(5) Device connection status

(6) Platform shutdown

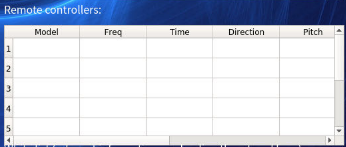
Click the platform on/off button, and the system will prompt whether the computer and detection device can be connected to the network? Users can check if the network is connected properly according to the prompts.

## 5.2 Automatic detection interface

Figure 2. Detection interface

The following will explain the functions in sequence according to the numerical order of the interface：

1. **Start：**Detect drones；
2. **Stop：**Stop detection；
3. **Setting：**Antenna, detection frequency band, network, etc. can be set;
4. **Longitude and latitude setting:** the location point offline map is obtained through the longitude and latitude of the location point**;**
5. **Unattended:** After activation, intelligently detect the drone and automatically counter it. The counter frequency band is selected according to the counter frequency band on the counter interface;
6. **Detection location:** Selection of detection city;
7. **Offline Maps：**If the system has installed the offline map data, you can choose the offline map without a network;
8. **Automatic elimination of environmental frequency hopping signal alarm:** If the autonomous recognition of the frequency hopping signal is opened in the Settings, this function can be opened in the case of many false positives in the complex electromagnetic environment, and the system will automatically learn the environment, automatically eliminate the false positives; After the elimination, if the alarm is still wrong, you can select the frequency of the false alarm in the detection result column on the right, and click select to eliminate the alarm of this frequency jump signal；
9. **Flying hand positioning results display list [Note: Flying positioning equipment should be configured]:** Support browsing history records, export results, and clear data; place the mouse on the table head and click will display "Put this UAV in the white list", "Remove this UAV from the white list", "jamming this UAV", "Draw this UAV history track" and "Turn off this UAV track display". Before selecting "Put this drone in the white list", you can directly enter the name of the use unit in the table. After entering the white list, the name of the unit will be displayed；
10. **Decoding result map display [Note: flying hand positioning equipment]:** suitable for the display of UAV positioning information obtained through decoding; When unattended is selected, countermeasures will be applied based on the decoding results, but not vice versa；
11. **Map display of pure spectrum detection results:** suitable for displaying information of all conventional drones outside the decoding protocol; If selected, when unattended, countermeasures will be performed based on the results of spectrum detection, and vice versa. If both Decode and Spectrum Detection Results Display are selected, the results of whoever detects the results first will be used for countermeasures；
12. **Suburban environment 2.4G level setting:** setting options for better detection of 2.4G in suburban areas;
13. **Detection method:** Frequency band group scanning or fixed frequency band tracking scanning can be selected;
14. **Detection distance [the function of spectrum detection]:** The detection distance, distance calibration, or unexpected distance can be set. Distance calibration is set to adapt to the use environment. The UAV is suspended at a height of 100 meters at 500 meters. After detecting the results of the UAV, the stop detection system will automatically conduct the distance calibration. After calibration, the detection distance is relatively accurate, with an error of about 200 meters.
15. **Roof mode：**In complex electromagnetic environments, such as on the roofs of many buildings, activating this function can increase the detection distance.
16. **Artificial level:** If you have certain radio knowledge, you can identify targets in complex electromagnetic environments based on level setting parameters
17. **Jamming:** Enter the reverse control interface.
18. **Browsing history：**Select start and end dates to browse history.
19. **Export detection results:** Export detection results in the form of a table.
20. **Playback of drone history trajectory:** This function can depict the flight trajectory of a drone by selecting the number on the left side of the detection result list with the mouse.
21. **Clear detection result database:** Clear the detection results.
22. **Spectrum Drone Detection Results List:** Display spectrum detection results in a table, circle above the table to choose whether to pop up the spectrum detection results or not. Mouse over the left header of the detection result column and click on it, it will show “Countermeasure this drone”, “Whitelist this drone”, “Plot trajectory” and “Cancel alarm”. “Eliminate Alarms”. The “Whitelist” is a spectrum detection whitelist, using different frequencies to distinguish between black and white lists, whitelist users need to lock their drones to a fixed frequency, and when the system detects this frequency in the future, it will be considered as a whitelist, and will not be countered when unattended; the “Eliminate Alarms”, can eliminate the jumping alarms; the “Eliminate Alarms”, can eliminate the jumping alarms. Alarm” can eliminate the false alarms of frequency-hopping UAVs, and the FPV or frequency-hopping UAV that eliminates the alarms will automatically restore the alarms after the detection host is restarted, in order to adapt to different usage environments. Refer to the description of 8 above, for the mapping alarm, choose carefully. Remote control detection results；
23. **white list：**When using the whitelist function, set the friendly drone to a fixed operating frequency. After detecting the drone, click on the target serial number in the detection result to list the drone as a whitelist without being suppressed. In the whitelist column, click on the line number to cancel the whitelist;
24. **Surrounding electromagnetic environment map:** can understand the surrounding electromagnetic environment.
25. **Detection signal waterfall diagram:** Can analyze signal characteristics.



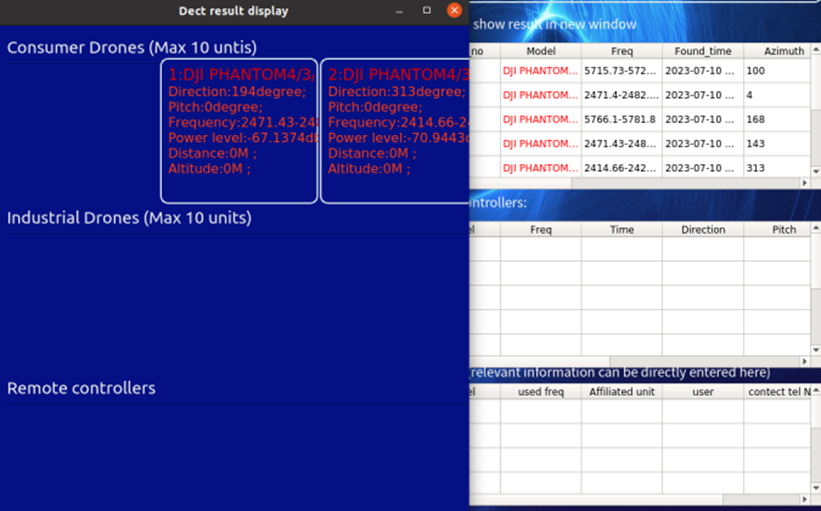
Figure 3: List of detection results

Figure 4. Schematic diagram of the operating system platform detection results

## 5.3 System Settings sub-screen

This interface includes five settings: antenna settings, detection frequency band settings, eliminate detection alarm frequency band settings, network settings, and software and database updates.

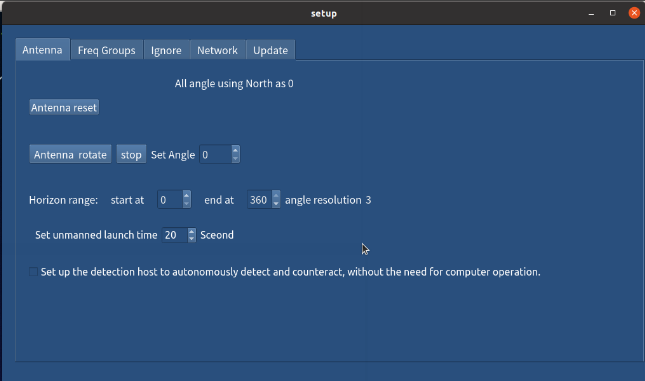


Figure 5. System settings interface

5.3.1 Antenna Settings

* Based on the detected geographical situation, if there are mountains or tall buildings on the back, the protection angle range can be set arbitrarily, which can effectively eliminate false azimuth caused by signal reflection.
* Set the unmanned launch time according to actual usage, with a range of 20S-3 minutes.
* According to actual usage, set the device to automatically start detection and jamming after power on, without the need to connect to the operating computer.

5.3.2 Detection frequency band settings

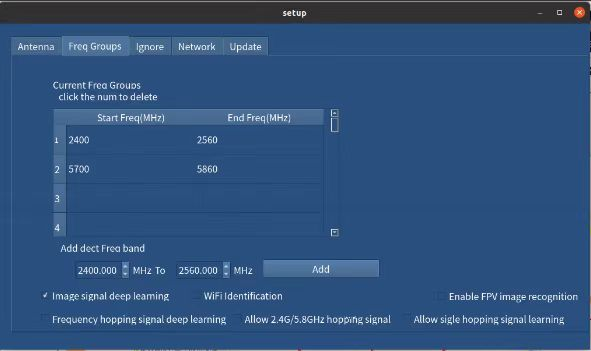


Figure 7. Detection band setting

1. Click on the line number to delete the detection frequency band: Click on the line number to delete the set detection frequency band;
2. Add detection frequency band: The input frequency band can be added with a detection frequency band (160MHz is one band);
3. Enable autonomous learning of image transmission signals: autonomously learn the image transmission signals of unknown drones and display the detection results during detection;
4. Identify WIFI unmanned aircraft, however, if there are too many WIFI signals around may cause some false alarms, the customer can decide whether to open the WIFI unmanned aircraft identification according to the actual situation of the electromagnetic environment, whether to open the choice of the system will be able to be stored, the next time the power is turned on in accordance with the last choice of whether to carry out the WIFI identification, the WIFI identification can be identified all the unmanned aircraft controlled by WIFI technology, including 5.2G WIFI address code, without prior resolution of the address code. WIFI identification can recognize all unmanned aircraft controlled by WIFI technology, including 5.2GWIFI unmanned aircraft, without the need to parse the WIFI address code in advance;
5. Enable FPV image recognition: Identify FPV image transmission drones;
6. Turn on the independent learning of FHF signal: After turning on the independent learning of FHF signal, please make sure that there is no unmanned aircraft flying over the sky, the system will automatically learn the electromagnetic environment (without affecting the detection of the UAV's mapping signals), and when the learning is finished, the system will prompt that the learning of the electromagnetic environment is finished, and the UAV can be detected by FHF and display the results of the detection normally, if there is still a false alarm, you can refer to the manual 5.2.22 to eliminate the false alarm. Eliminate false alarms; the choice of turning on the FH autonomous learning will not be stored by the system, so the system defaults not to turn on the autonomous learning of FH signals every time after turning on the detecting mainframe, and if it needs to be turned on, the customer should take the initiative to choose it.
7. Allow autonomous learning in the 2.4G/5.8G frequency band: autonomously learn signal recognition in the 2.4G/5.8G frequency band and display detection results during detection;
8. Allow single frequency autonomous learning: recognize signals in the single frequency band set for autonomous learning and display detection results during detection;

5.3.3 Eliminating Detection Alarm Frequency Band Settings

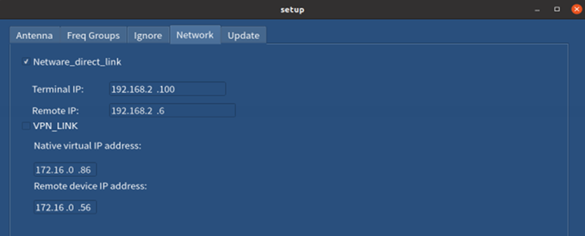
When the system self-learning function is activated, some false alarms may occur. In the system settings, it can be set to eliminate alarm bands, such as mobile communication bands, radio and TV bands, etc. Users can set this according to the frequency band allocation of each country. This setup eliminates the detection of frequency bands set up, and then the system will automatically store them, and this function is very useful for effectively eliminating all kinds of false alarms.



Figure 8. De-detection alarm band setting

5.3.4 Network Settings

The network settings include four address settings: the IP address of the local Gigabit network, the IP address of the intelligent radio platform, and the VPN mode, please consult the company's professional and technical personnel. After modifying the IP address, the operating computer should also be reset to the new IP address.

Figure 9. Network Settings

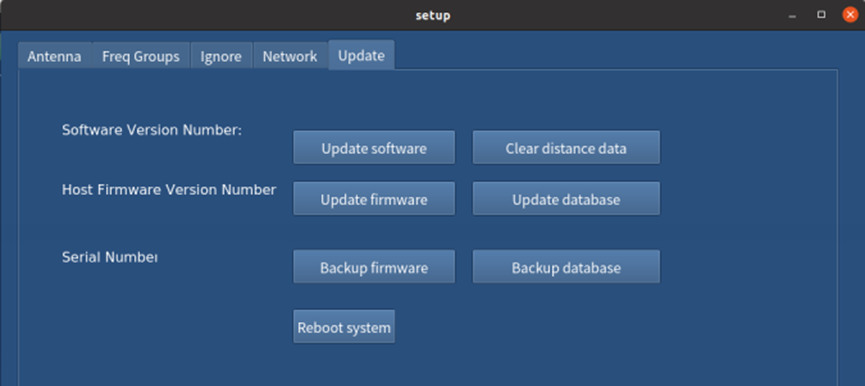
5.3.5 Software and database updates

Figure 10. Software and Database Update

1. Update the local software: the product supports one-year free software upgrade, lifetime paid software upgrade, update path: the manufacturer's new software to the computer desktop computer-personal C30-release-update-console;
2. Restore initial data: If the setup error leads to work abnormality, select this item to restore the initial settings, such as VPN setup work error;
3. Update remote device software: this function is to upgrade the host software of the detection device, update path: before clicking this button to put the manufacturer's new software to the computer desktop computer-personal-C30-release-update-platform;
4. Update model database: This function is to upgrade the database of the detection equipment, update path: before clicking this button to the manufacturer's new software to the desktop computer - personal - C30-release-update-platform;
5. Remote device restart: this function can be remote restart device.
6. Backup Remote Device Software: This function can back up the remote device software in order to update the remote device software.
7. Backup Model Database: This function can back up the remote database in order to update the database.

## 5.4 Jamming interface



1Figure 11. Schematic diagram of the jamming interface

1. Detected frequency: This function displays the frequency of detected drones, providing accurate information for countermeasures;
2. Reflection channel: This function can select the frequency band to counter the drone based on the detected frequency; For example, if a 2.4G DJI Elf 4 is detected, you can only select the 2.4GHz reflection channel for drone countermeasures;
3. Reaction method: The reaction method mainly involves displacement. Drive away refers to cutting off the image transmission signal between the drone and the remote control and allowing the drone to return. This mode is generally selected by default;
4. Reverse azimuth angle: You can set the reverse azimuth angle by yourself, and after setting it, press the confirmed setting angle;
5. Press this button to start emission；
6. Press this button to end the launch；

## 5.5 Signal recording sub interface

When recording signals, we can choose to record the image transmission or frequency hopping signal. When recording the image transmission signal, double-click on the drone image transmission frequency in the spectrum graph, adjust the gain and reference level, and the recording will be stored to identify the model;



A.Start recording

Press the button to start recording the drone feature signal. If the system discovers drone feature data, the recording result will be automatically saved and displayed in the "drone model column".



B.End recording

Press the button to end the drone feature signal recording.

## 5.6 Equipment connection

The device connection display function will automatically connect when the device is connected to the operating terminal. When using the operating system, it is necessary to ensure that this icon shows that the device is connected.

## 5.7 Platform Shutdown

If you want to shut down the operating system, clicking on the platform shutdown will disconnect the system from the device, and the device connection display icon will be displayed as, indicating that the link to the device has been disconnected.

## 5.8 Advanced Features

5.8.1 Lateral function of any signal

This system has the lateral function of any signal. In the detection interface, double-click the frequency to be lateral in the spectrum diagram to reveal the direction and approximate distance of this frequency. For special signals, this function can be used for lateral measurement.

After stopping detection, the lateral function of this signal will automatically cancel.

5.8.2 Frequency hopping signal self-learning function

For the autonomous learning of frequency hopping signal, in the process of detection, the system automatically eliminates the false alarm at the end, after the environment is stabilized [i.e. after detecting for a period of time], you can press the right button to eliminate the alarm of the frequency hopping signal of this flying unmanned aircraft in the column of the detection result, and at this time the alarms of other non-unmanned aircrafts' frequency hopping signals will be eliminated, and the alarms will be real if there is an emergence of the illegal frequency hopping unmanned aircrafts.

The alarm canceling function of this FH signal will be canceled by itself after the power failure and restart of the detecting host.

# 6. Common problem handling

1. *What problems should be paid attention to in the deployment of anti-UAV equipment?*

A: The deployment of UAV detection and defense equipment should be deployed in an open place as far as possible. Within the visual range of defense, there should be no building shelter.

1. *What are the factors related to the distance detected?*

A: detection distance and electromagnetic environment, have no shelter and equipment receiving performance, like listen to sound, the more noisy sound can be more far, so the electromagnetic environment (in detection frequency has a lot of radio signal), detection distance, the closer, such as in the unmanned aircraft use 2.4GHz band, because there are a lot of WIFI signal, will affect the detection distance, in this case, unmanned aircraft flight distance will become closer, such as the original flight 2 km, perhaps can only fly 500 meters, so also don't have to worry about detection distance is not far enough.

1. *Why does blocking a building or other obstacles affect detection and countermeasures?*

A: Since the use frequency of UAV is usually in the high frequency band above 2.4GHz, the penetration performance and diffraction performance of this radio frequency band are relatively weak, and the signal cannot penetrate the occlusion to reach the detection device, so the occlusion will affect the detection and counter distance.

1. *How do drone radios work?*

A: The drone needs to transmit the video from the drone to the remote control and GPS, and the remote control transmits the signal to the drone through the frequency jump signal, so as to control the drone. There are also WIFI-controlled drones.

1. *What is the displacement and crash landing of anti-drones?*

A: Generally, if the remote-control signal is lost (disturbed), the UAV is designed to return to the takeoff site; if the remote-control signal and GPS navigation signal are disturbed at the same time, the unmanned aircraft cannot make a judgment and can only land in place, commonly known as crash landing.

1. *What is the approximate detection distance in different environments?*

A: The roof of urban environment is surrounded by low buildings: for DJI UAV is about 600 m-1000 m; urban environment, open area, less surrounding buildings cover, detection distance is about 1.5 km-3 km; suburban environment, island or large farmland, no residential about 5-8 km.

1. *How far is the counter distance about?*

A: The distance of our device can usually reach 1 km, etc. The drone takes off 1 km from the detection equipment and flies 100 meters directly above it. The counter-dry ratio is usually used to measure the counter distance of the device, that is, the distance of the jamming signal from the drone: the distance of the remote control from the drone. Under the above conditions, the counter-dry-pass ratio is 10:1.

1. *Can your device be used for multiple networking?*

A: Yes, you can deploy a detection device every few kilometers according to the geographical range you need to cover, and then connect to the control center using a dedicated network or virtual private network.

# 7. Data analysis methods for advanced users

## 7.1 Autonomous learning function

Due to the fact that this system is a very professional spectrum detection device, rather than a signal decoding device, it can not only detect commonly used drone models in the database, but also independently learn new unknown drone models or use similar feature image transmission or frequency hopping signals. It is recommended that users choose whether to turn on or off the autonomous recognition function of image transmission and frequency hopping signals based on the level of alert, The system has enabled the autonomous learning function of image transmission signals by default.

## 7.2Analysis of detection results

*In the detection result column or exported detection result data, advanced users can carefully analyze the detection results, as follows:*

1. In the detection results, if the same model or suspected model that has been continuously alerted within 1-2 minutes and has changes in direction and distance, it can be basically determined that it is a drone signal and its flight trajectory can be plotted;
2. If the detection direction and distance do not change significantly, it may be unmanned aerial vehicles hovering or fixed image reconnaissance equipment installed.
3. The frequency of drone usage can be observed simultaneously. The frequency of drone signal usage may vary depending on the electromagnetic environment. The system displays the number of drones based on the frequency. When the drone jumps from one frequency to another, the system detects that the drone frequency will be retained for a certain period of time, and then automatically erases the detection result after jumping to another frequency.