



# 79GHz Anti-smashing Radar

## User's Manual



# Foreword

## General

This manual introduces the functions and operations of the 79GHz anti-smashing radar (hereinafter referred to as the "Radar").






## Models

DHI-ITSJC-2302-DC12

DHI-ITSJC-2202-DC12

## Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

| Signal Words   | Meaning   |
|--|---|
|  <b>DANGER</b>   | Indicates a high potential hazard which, if not avoided, will result in death or serious injury.  |
|  <b>WARNING</b> | Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.                              |
|  <b>CAUTION</b> | Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result. |
|  <b>TIPS</b>    | Provides methods to help you solve a problem or save you time.  |
|  <b>NOTE</b>    | Provides additional information as the emphasis and supplement to the text.   |

## Revision History

| Version | Revision Content | Release Time |
|---------|------------------|--------------|
| V1.0.0  | First release.   | March 2020   |

## About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our

official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.

- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

# Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the Radar, hazard prevention, and prevention of property damage. Read these contents carefully before using the Radar, comply with them when using, and keep the manual well for future reference.

## Operation Requirements

- Make sure that the barrier will not jitter obviously, and when installing guardrail at one side of the lane, secure the guardrail to prevent it from moving back-and-forth or jittering.
- After installing the Radar, please insulate the exposed cable cores.
- Install the Radar 60 cm (23.6") away from the ground (70 cm (27.6") is recommended when large trucks are frequently seen).
- Do not impact the Radar. Prevent the Radar from falling down.
- Do not place metal objects in the range of 0.5 m (1.6 ft) right in front of the Radar. Guardrails and speed bumps that might contain metal elements should be installed as far away from the Radar as possible.
- Do not disassemble the Radar.
- Clean the surface of the Radar with a soft dry cloth or a clean soft cloth dipped in neutral detergent, and then dry the surface.

### **WARNING**

- Use accessories suggested by the manufacturer, and install and maintain the Radar by professionals.
- When using a laser beam device, avoid exposing the device surface to laser beam radiation.
- Do not provide two or more than two kinds of power supply modes; otherwise, the Radar might be damaged.

## Power Requirements



- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure that the same model is used.
- Use the recommended power cables in the region and use them under the rated specification.
- Use the power adapter provided with the Radar; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Note that the power supply requirement is subject to the device label.

- Connect device (type-I structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. Keep a convenient angle when using it.

## Application Environment Requirements

- Do not aim the Radar at strong light (such as lamplight, sunlight) for focusing.
- Transport, use and store the Radar under the allowed humidity and temperature conditions.
- Prevent any liquid from flowing into the Radar.
- Install the Radar in a well-ventilated place, and do not block the ventilation of the Radar.
- Do not press, vibrate or soak the Radar during transportation, storage and installation.
- Pack the Radar with packaging materials provided by its manufacturer or materials with the same quality before transporting it.
- It is recommended to use the Radar with a lightning-proof device for better lightning-proof effect.
- Ground the Radar to improve its reliability.

# Table of Contents

|   |            |
|---|------------|
| <b>Foreword</b> .....                                 | <b>I</b>   |
| <b>Important Safeguards and Warnings</b> .....        | <b>III</b> |
| <b>1 Product Introduction</b> .....                   | <b>1</b>   |
| 1.1 Overview .....                                    | 1          |
| 1.2 Features .....                                    | 1          |
| <b>2 Appearance and Structure</b> .....               | <b>2</b>   |
| 2.1 Appearance .....                                  | 2          |
| 2.2 Dimensions .....                                  | 2          |
| <b>3 Installation</b> .....                           | <b>3</b>   |
| 3.1 Tools .....                                       | 3          |
| 3.2 Installation Method .....                         | 3          |
| 3.2.1 Radar for Triggering Snapshot .....             | 3          |
| 3.2.2 Radar for Anti-smashing .....                   | 5          |
| 3.3 Wiring .....                                      | 7          |
| 3.3.1 Cable Description .....                         | 7          |
| 3.3.2 Cable Connection .....                          | 8          |
| <b>4 Configuration on Mobile App</b> .....            | <b>9</b>   |
| 4.1 Connecting Your Phone to Radar Wi-Fi.....         | 9          |
| 4.2 Connecting App to Radar .....                     | 9          |
| 4.2.1 Setting Radar Parameters .....                  | 10         |
| 4.2.2 Upgrading Firmware .....                        | 12         |
| 4.2.3 Modifying Wi-Fi Information.....                | 12         |
| 4.2.4 Viewing Real-time Data .....                    | 13         |
| <b>5 Commissioning</b> .....                          | <b>15</b>  |
| 5.1 Radar for Anti-smashing .....                     | 15         |
| 5.2 Radar for Triggering Snapshot.....                | 15         |
| <b>6 FAQ</b> .....                                    | <b>16</b>  |
| <b>Appendix 1 Cybersecurity Recommendations</b> ..... | <b>17</b>  |

# 1 Product Introduction

## 1.1 Overview

The 79GHz anti-smashing radar adopts leading technologies of high-precision microwave measurement and high-speed digital signal processing, endowing it with high accuracy, free of commissioning, and high stability. The radar is ideal for working with boom barrier to monitor and control vehicles that enter and leave, and prevent the barrier arm from hitting people or vehicles when it falls. It can also work with the camera to read and recognize license plate, providing reliable evidence for parking management.

The Radar sends the information of detection target to the host computer or central platform through RS-485 communication or Wi-Fi, so the real-time information can be displayed on the computer or the platform. It can also send the information to the relay to trigger the camera for taking snapshots, and helps control barrier opening and closing.

## 1.2 Features

- 79GHz monolithic microwave integrated circuit (MMIC) technology allows higher resolution and more stable detection.
- Uses the latest algorithm to filter interference, suitable for advertising barriers, fence arm barriers, straight arm barriers, and folding arm barriers.
- Uses MIMO (multiple-input multiple-output) technology to recognize movement directions of targets, ideal for scenes with both vehicles and people entering and leaving.
- Adjustable detection distance and width, and no need of reading scene data, applicable to complicated scenes.
- Supports upgrading through RS-485 and mobile app (with Wi-Fi connection), and allows online commissioning and firmware upgrade, providing ease of operation.
- Convenient installation and maintenance: Compared with coils, you can easily installed the Radar by tightening the screws, with no need of road construction.
- Capable of identifying vehicles and people, preventing the barrier arm from hitting the vehicles and people.
- Long service life of 5–10 years.
- Two LED indicators are designed to better know the working status of the Radar: Red for power, and green for activity.
  - ◇ Solid red: Power is supplied.
  - ◇ Solid green: Target is detected. When the target leaves, the green indicator turns off.
- Automatically goes to the last working status before it is powered off.
- Adaptable to harsh environments, and its detection performance will not be influenced by electromagnetic interference, light, dust, rain, and snow.

## 2 Appearance and Structure

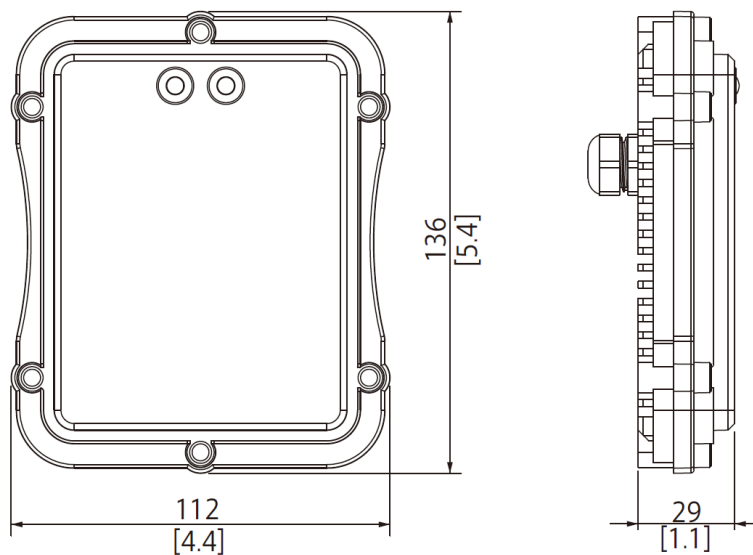
### 2.1 Appearance

Figure 2-1 Appearance



### 2.2 Dimensions

Figure 2-2 Dimensions (mm [inch])





## 3 Installation

### 3.1 Tools

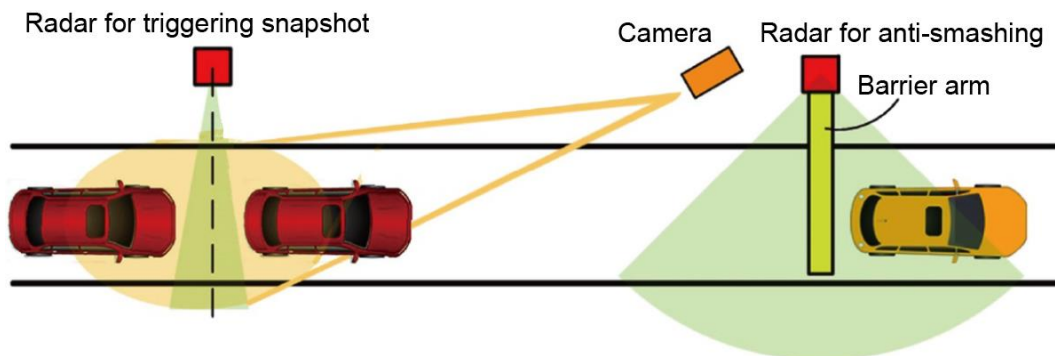
Hole opener, Phillips screwdriver, straight screwdriver, wire stripper, RS-485 cable, and PC.

Extra tools needed when installing radar for triggering snapshot: Impact driver, M10 drill, and wrench.

### 3.2 Installation Method

The Radar, either used for triggering snapshots or anti-smashing, needs to be installed vertical to the lane direction. Install the anti-smashing radar on the casing of the boom barrier, and when the Radar is used for triggering snapshots, install it on a pole, with the lower side of the Radar 0.6 m (2.0 ft) away from the ground.

Figure 3-1 Installation example



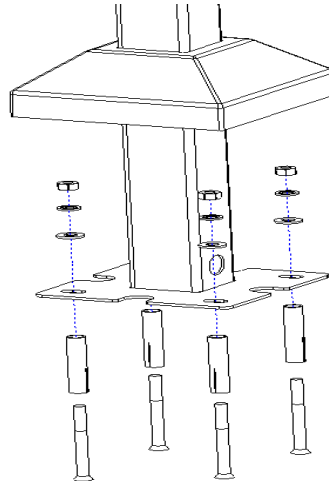
- When installing the Radar on the casing of the barrier, the casing must be stable (jittering angle no more than 5°) to ensure the detection accuracy of the Radar.
- When installing guardrail at one side of the lane, secure the guardrail to prevent it from moving back-and-forth or jittering.

#### 3.2.1 Radar for Triggering Snapshot

Step 1 Install the mounting pole.

- 1) Install the mounting pole on the same side with the license plate recognition camera.
- 2) Mark four holes on the ground according to holes of the mounting pole, and then use M10 drill to drill four 50 mm (2.0") holes in the ground based on the marks.
- 3) Use four M6 expansion screws to fix the mounting pole to the ground. Put the cover in place.

Figure 3-2 Install the mounting pole

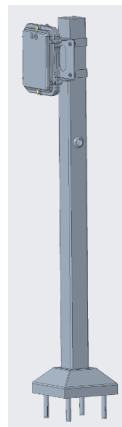
**Step 2** Install the Radar.

- 1) Install the Radar 60 cm (23.6") away from the ground (70 cm (27.6") is recommended when large trucks are frequently seen).
- 2) Fix the rear plate of the Radar to the mounting pole by using 4 flange screws.
- 3) Fix the Radar to the rear plate by using two M4 screws. See Figure 3-3 and Figure 3-4.

Figure 3-3 Install the Radar



Figure 3-4 Installation completed

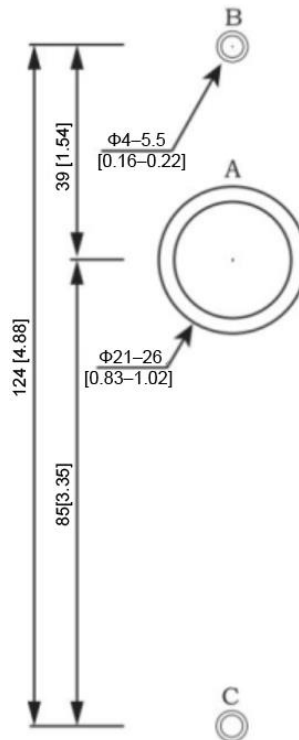


## 3.2.2 Radar for Anti-smashing

### Step 1 Drill holes.

- 1) Drill a  $\Phi 23$  mm (0.9") circular hole (hole A) on the casing of the advertising barrier and at a height of 68 cm (26.8") from the ground (78 cm (30.7") is recommended when large trucks are frequently seen).
- 2) Drill two  $\Phi 5$  mm (0.2") circular holes (holes B and C). The distance between holes A and B is 39 mm (1.5"), and the distance between holes A and C is 85 mm (3.3").

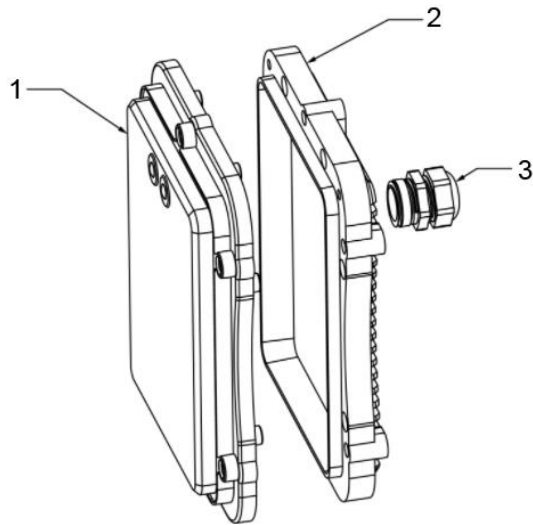
Figure 3-5 Hole size (mm)



### Step 2 Fix the Radar.

- 1) Install waterproof joints between the Radar and the casing of the barrier. See Figure 3-6.
- 2) Fix the Radar to the casing through holes B and C by using screws.
- 3) Connect radar cables to the barrier through hole A. See Figure 3-7.  
For the installation result, see Figure 3-8.

Figure 3-6 Waterproof joint installation



1: Front cover; 2: Rear cover; 3: Waterproof joint

Figure 3-7 Fix the Radar

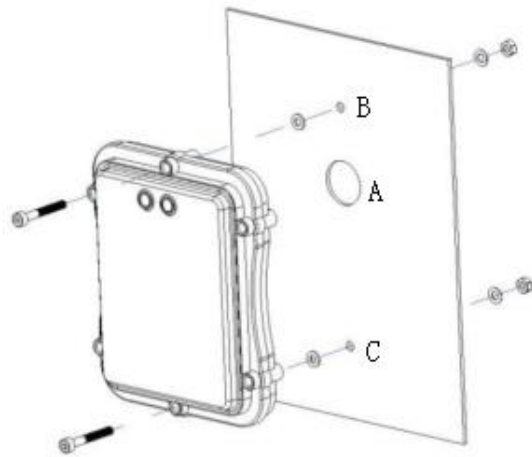
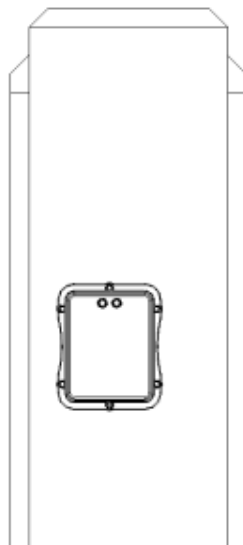


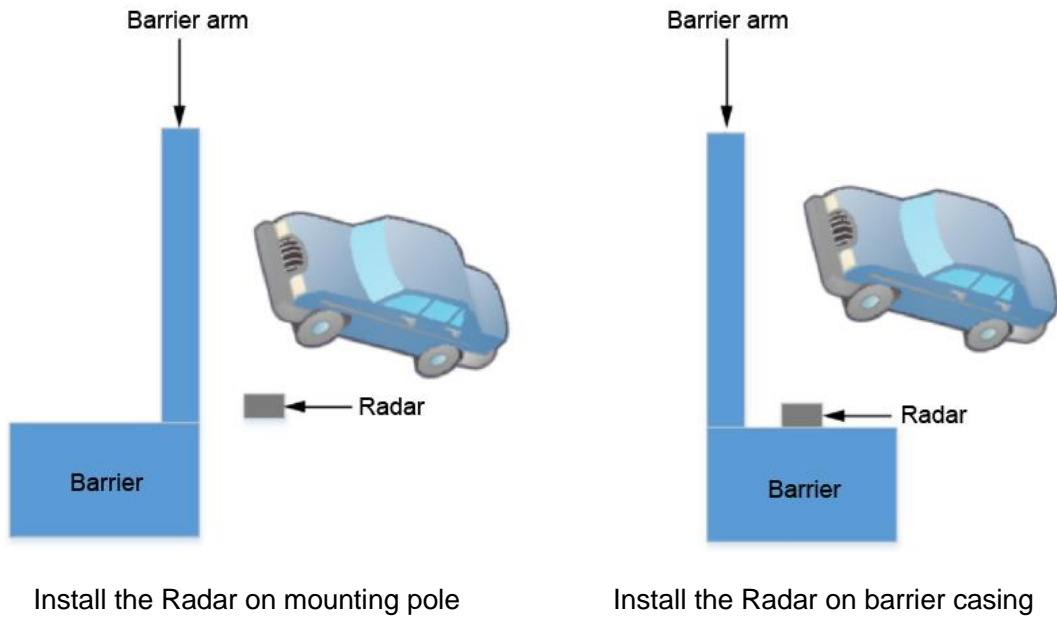
Figure 3-8 Installation completed





The Radar can be installed either on the barrier casing or the mounting pole. See Figure 3-9. For both of the installation methods, the Radar needs to be installed within 50 cm (19.7") of the barrier arm. **Right Width** and **Left Width** should be more than 0.5 m (1.6 ft) to avoid interference from the barrier arm and ensure radar detection accuracy. You can set the widths on the mobile app STJ79 (see "4.2.1 Setting Radar Parameters").

Figure 3-9 Radar installation methods



## 3.3 Wiring

### 3.3.1 Cable Description

Figure 3-10 Cable

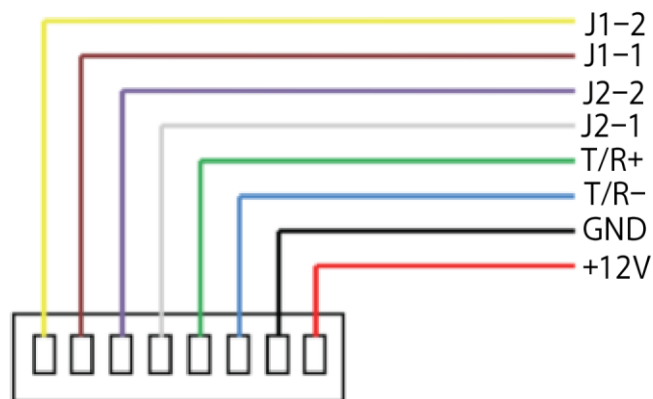


Table 3-1 Cable description

| Cable                       | Description  |
|-----------------------------|--|
| J1-1 (brown), J1-2 (yellow) | Relay output.  |
| J2-1 (white), J2-2 (purple) | Program loading control, barrier closing signal input. |
| T/R- (blue), T/R+ (green)   | RS-485 communication.                                  |
| GND (black), +12V (red)     | 12V power output.                                      |

### 3.3.2 Cable Connection

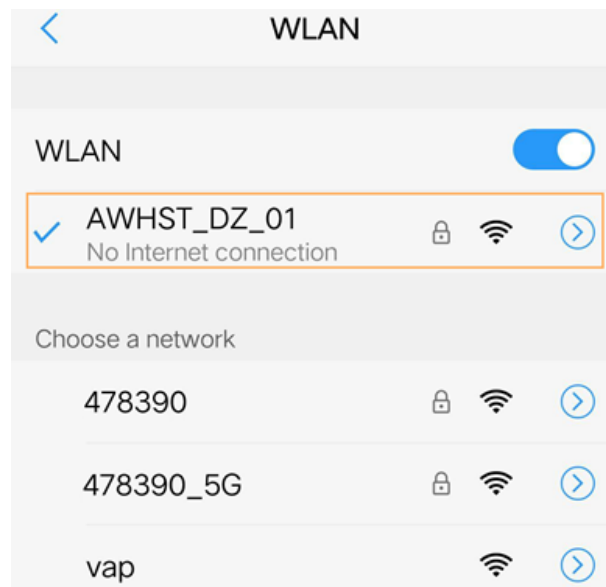
- Connect the Radar to power: Connect +12V (red) and GND (black) to positive and negative terminals of power source respectively. A solid red indicator on the Radar indicates that the power supply is normal.
- Connect the Radar to camera:
  - ◇ Alarm: Connect J1-1 (brown) and J1-2 (yellow) to alarm output ports of camera.
  - ◇ RS-485 communication: Connect T/R- (blue) and T/R+ (green) to RS-485 ports of the camera, and then connect the RS-485 cable to computer serial port.
- Connect to barrier: Connect J1-1 (white) and J1-2 (purple) to the I/O and COM ports of the barrier.
- Upgrade radar firmware: Connect J2-1 (white) and J2-2 (purple) to the push button. When connecting the radar to barrier, you can also connect J2-1 (white) and J2-2 (purple) to closing signal input port of the barrier.

## 4 Configuration on Mobile App

### 4.1 Connecting Your Phone to Radar Wi-Fi

After connecting the Radar to power, enable WLAN of your phone from **Settings > WLAN**, select **AWHST\_DZ\_01** and enter the Wi-Fi password (123456789 by default).

Figure 4-1 Wi-Fi connection



### 4.2 Connecting App to Radar

Step 1 Scan the QR code provided in the accessory to download and install the STJ79 app, and an icon is generated on the desktop of your phone.

Step 2 Open the app, and then tap **WiFi Connection**. The app is successfully connected to the Radar. Now you can start setting radar parameters.




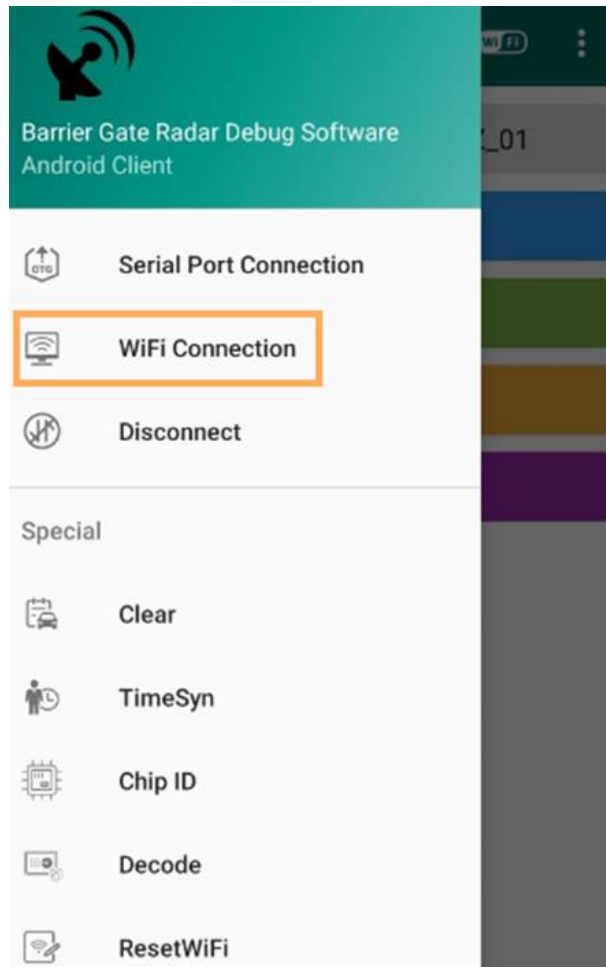
Tap  at the upper-right corner, and then tap **Instructions** to view help.

Figure 4-2 Wi-Fi connection



### 4.2.1 Setting Radar Parameters

In the **Parameter** section, tap **Basic Parameter Setting** and **Advanced Parameter Setting** to set the parameters.

Figure 4-3 Set basic parameters

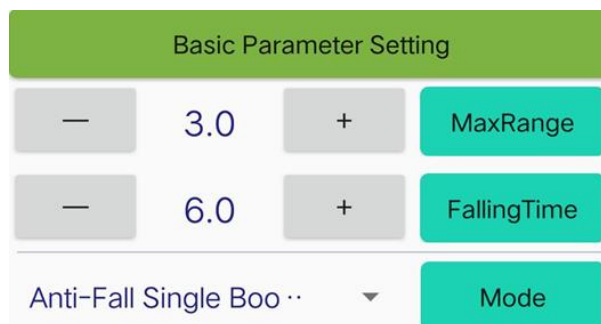




Figure 4-4 Set advanced parameters



Table 4-1 Set basic and advanced parameters

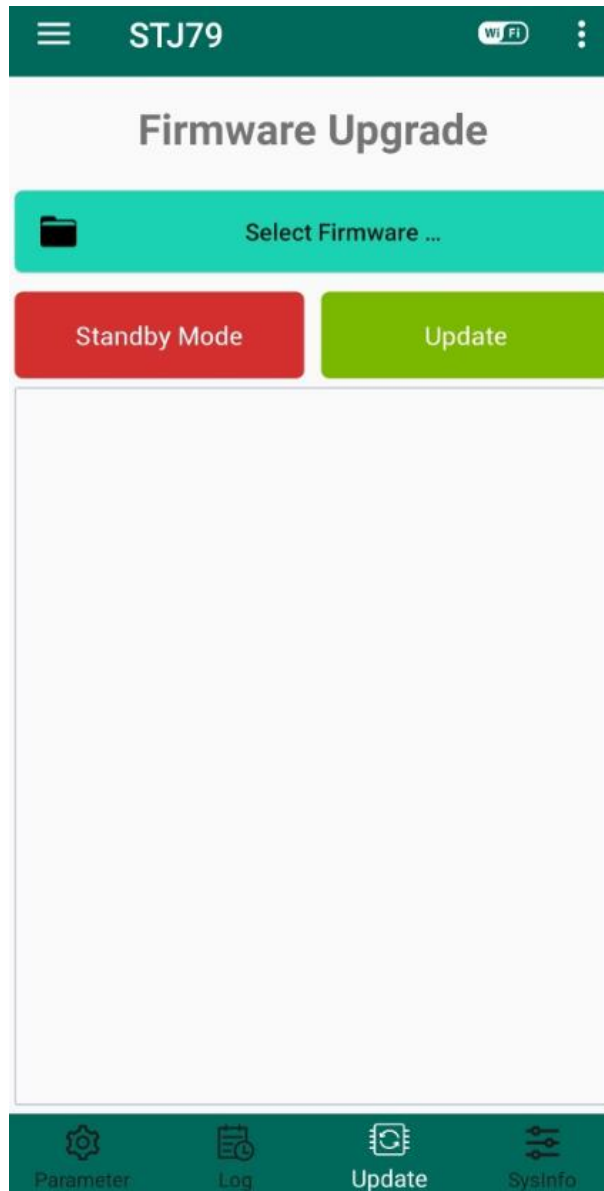
| Type               | Name         | Description   |
|--------------------|--------------|---|
| Basic Parameter    | Max Range    | The maximum detection range of the Radar, generally the length of the barrier arm or lane width. Value range: 0.3–6.0 (3.0 by default).   |
|                    | Falling Time | Set this parameter only when the Radar is used for anti-smashing.<br>Set falling time according to the time that the barrier arm takes to rise and then fall. The value is 6 s by default, and it does not affect the opening/closing speed of the barrier. |
|                    | Mode         | Select mode according to the actual installation position of the Radar.   |
| Advanced Parameter | Left Width   | Detection width at the left or right side of the radar normal line. Value range: 0–1.0 (1.0 by default).  |
|                    | Right Width  | How to tell the left or right side: The left or right side of the Radar when you face the Radar and the indicator lights are at the upper side.   |
|                    | Min Range    | The range filtered by the Radar. Value range: 0.3–6.0 (0.3 by default). Suitable for setting the minimum range when there is interference near the Radar.   |
|                    | Sensitivity  | Reserved parameter. Keep the default value (0.3).   |
|                    | DPV          | DPV means distinguishing people and vehicles. <ul style="list-style-type: none"> <li>● <b>Yes:</b> The Radar will detect only vehicles.</li> <li>● <b>No:</b> The Radar will detect both people and vehicles.</li> </ul>                                    |
|                    | Direction    | Set this parameter only when the Radar is used for triggering snapshots.<br>Select direction according to the approaching direction of vehicles. The Radar can only detect vehicles approaching from the selected direction.                                |

## 4.2.2 Upgrading Firmware

In the **Update** section, tap **Select Firmware** to select firmware of interest, and then tap **Update**. The firmware upgrade starts.

**Standby Mode** is recommended when the above upgrade method failed or the Radar crashed.

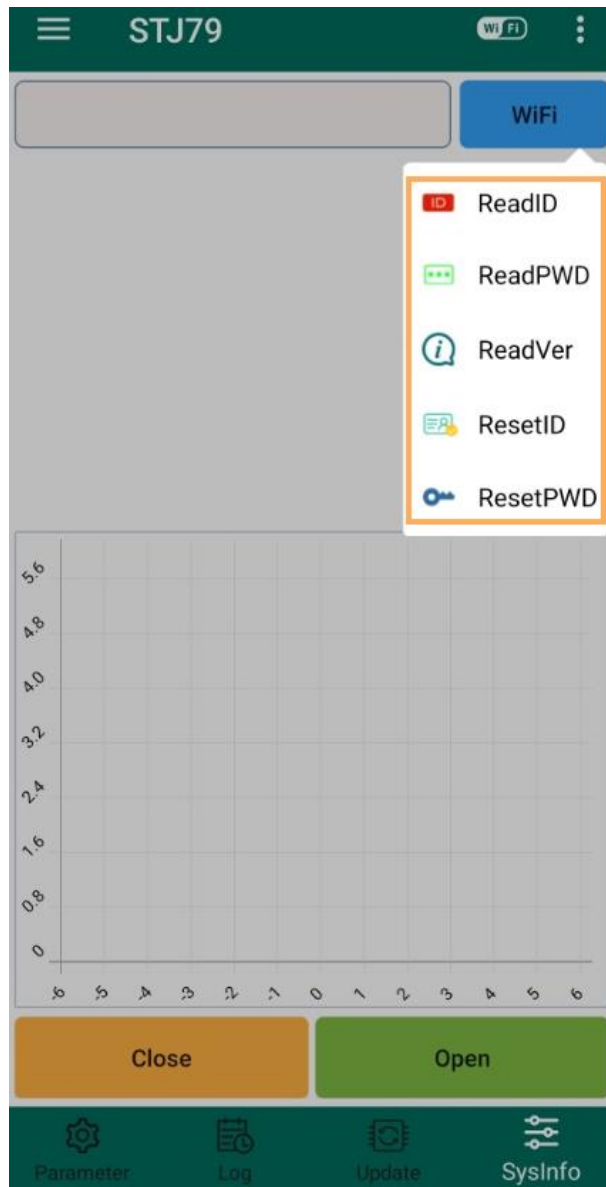
Figure 4-5 Firmware upgrade



## 4.2.3 Modifying Wi-Fi Information

In the **SysInfo** section, tap **WiFi**, and then tap the corresponding item to view or modify the Wi-Fi account or password.

Figure 4-6 View and modify Wi-Fi information



## 4.2.4 Viewing Real-time Data

In the **SysInfo** section, tap **Open**, and then you can view the real-time detection data. If a target is detected, a green dot will show at the target's position. See Figure 4-7. If the green indicator keeps on (meaning target is detected) after the Radar is installed, you can check whether there is interference in the detection range according to the actual conditions near the Radar. If yes, adjust the **Min Range** (see Table 4-1) to filter out the interference and ensure detection accuracy.

Figure 4-7 View real-time data



## 5 Commissioning

### 5.1 Radar for Anti-smashing

After installing and configuring the Radar, you can check the following items to see whether the Radar can properly work.

- The Radar can identify people and vehicles.
  - ◇ After opening the barrier and making a person enter the radar detection range, the green indicator does not turn on, and after the person leaves, the barrier arm does not fall. This means the radar successfully identified the person.
  - ◇ After opening the barrier and driving a vehicle to the radar detection range, the green indicator turns on, and after the vehicle leaves, the barrier arm falls. This means the radar successfully identified the vehicle.
- The barrier arm does not hit vehicles.
  - ◇ Open the barrier, and drive a vehicle at speed lower than 10 km/h to pass the barrier. When it passes the barrier, the green indicator keeps on, and the barrier arm does not jitter or hit the vehicle.
  - ◇ Open the barrier, and drive a vehicle to the radar detection range. Stop the vehicle in the detection range for 1 minute, the green indicator keeps on, and the barrier arm does not jitter or hit the vehicle.
- The barrier arm does not hit people.
  - ◇ When the barrier arm is falling after a vehicle leaves, a person passes the barrier, the green indicator turns on, and the barrier arm rises and does not hit the person.
  - ◇ A person moves back and forth along the direction of the barrier arm, the green indicator keeps on, and the barrier arm does not hit the person.

### 5.2 Radar for Triggering Snapshot

After installing and configuring the Radar, you can check the following items to see whether the Radar can properly work.

- When a person enters the radar detection range, the green indicator does not turn on, the camera does not capture pictures, and the barrier does not open.
- When a vehicle enters the radar detection range, the green indicator turns on, the camera captures pictures of the vehicle, and the barrier opens.
- When vehicles pass the radar detection range at speed lower than 10 km/h, the green indicator keeps on, and the camera will not take multiple snapshots for a vehicle detected.
- When vehicles pass the radar detection range at different speeds (0 km/h to 30 km/h), the capture position error of the camera is smaller than 1 m (3.3 ft).

## 6 FAQ

### **1. Can I control the opening of the barrier by setting the Falling Time on the mobile app?**

No. The **Falling Time** on the mobile app does not influence the opening and closing of the barrier.

### **2. Why the green indicator keeps on and the barrier does not close after the vehicle leaves?**

- Check whether there is metal object within the radar detection range. If yes, move the object away. For objects that cannot be moved, reduce the radar detection distance and width until them get out of the detection range of the Radar.
- The Radar has a program logic error. Power off the Radar and restart it, and then check again after vehicle passes.

### **3. The Radar cannot connect to the mobile app STJ79?**

Make sure that your smart phone is connected to the radar Wi-Fi. The default Wi-Fi name and password are AWHST\_DZ\_01 and 123456789 respectively.

# Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

## **Mandatory actions to be taken for basic equipment network security:**

### **1. Use Strong Passwords**

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

### **2. Update Firmware and Client Software in Time**

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

## **"Nice to have" recommendations to improve your equipment network security:**

### **1. Physical Protection**

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

### **2. Change Passwords Regularly**

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

### **3. Set and Update Passwords Reset Information Timely**

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

### **4. Enable Account Lock**

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

## 5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

## 6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

## 7. Enable Whitelist

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

## 8. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

## 9. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

## 10. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

## 11. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

## 12. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

## 13. Network Log

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

## 14. Construct a Safe Network Environment

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.



- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.

ENABLING A SAFER SOCIETY AND SMARTER LIVING