# Multilane Radar Detector

## User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.          V1.0.0

# Foreword

## General

This manual introduces the functions and operations of the multilane radar detector (hereinafter referred to as the "Radar").

## Model

DHI-ITARD-024MA-H

## Safety Instructions

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

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

## Revision History

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

The Radar is a high-technology product that requires professional operations. Read the user's manual carefully before using the Radar, or contact professionals or technical support if you have any doubts. Specifically:

● Use high-quality DC power supply to avoid crosstalk from other devices.

● During storage and use, avoid damage caused by impact or fall. Take appropriate lightning protection measures when using outdoors.

● The interfaces provided by the radar are not hot-swap interfaces. When connecting, please power off before operation to avoid accidental burnout.

● The RS–485 and RS–232 interfaces of the Radar are not hot-swap interfaces. Power off the Radar before connecting these interfaces to avoid accidental burnout.

# Table of Contents

# 1 Product Introduction

## 1.1 Overview

The Radar can be installed above the lane to detect vehicles 15 m–45 m (49.2 ft–147.6 ft) away and cover vehicles of 1–4 lanes. It will send capture signals to the camera when the vehicle approaches the specific position, and also detect the vehicle speed and the lane that the vehicle is driving on.

## 1.2 Features

- One single radar covers up to 32 vehicles of 1–4 lanes.
- Precisely detects speed and position of vehicles when they are 18 m–35 m (59.1 ft–114.8 ft) away.
- Flexible to install: Either installed right above the lane or at the side of a lane.
- Special functions such as illegal lane change, wrong-way driving detection.
- The detection performance is not impaired by adjacent lane or vehicles in front of or behind the vehicle of interest.
- All-weather working, and detection performance is immune to glaring sunlight, dense fog or other adverse weather and lighting conditions.
- High capture rate: About 99% when traffic is smooth, and 96% and 92% respectively when traffic is saturated and congested.
- Accurate positioning: The position accuracy of triggering capture signal is as high as ±0.5 m (1.6 ft).

## 1.3 Appearance

Figure 1-1 Product appearance
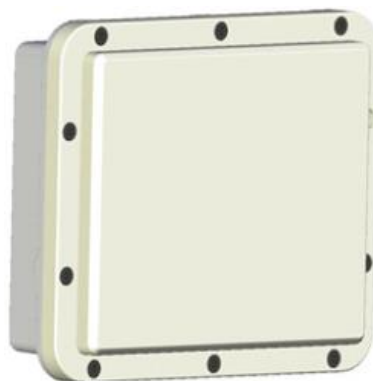
# 2 Cable Connection

When using RS–232 transmission, the cable length cannot be more than 15 m (49.2 ft).

Use RS–485 to communicate over medium and long distance. Make sure that the shielded twisted pair cable is used, and the shield layer of the cable is grounded. When the transmission distance is more than 300 m (984.3 ft), terminal resistance (generally 120 Ω) is required.

Figure 2-1 Cable



Table 2-1 Cable description

| Pin Color | Description |
| --- | --- |
| Blue | RS–232T, RS–485- |
| Green | RS–232R, RS–485+ |
| Yellow | GND |
| Red | DC 12V+ power input |
| Black | DC GND |

# 3 Installation

## 3.1 Installation Modes

Based on the vehicle movement direction, three installation modes are available: Approaching (detects head of vehicles), receding (detects tail of vehicles), and both directions (detects either head or tail, depending on the vehicle movement direction).
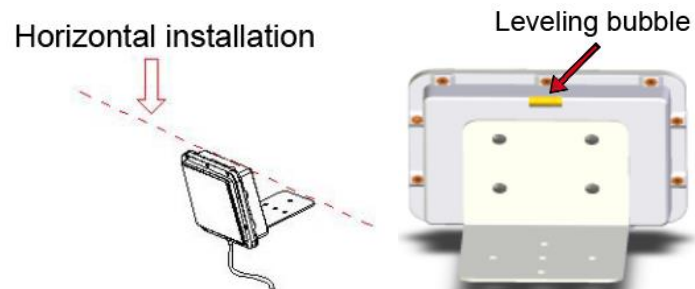
The Radar can either be installed right above the lane, or at the side of a lane.

## 3.2 Notes to Installation

When installing the Radar, make sure that:

● Keep the Radar as horizontal as possible. Check whether the leveling bubble on the rear panel of the Radar is in the middle. If not, fine-tune the installation angle of the Radar.

Figure 3-1 Keep the Radar horizontal



● The radar beams can cover the entire area to be detected.

When the installation height is confirmed and the Radar is kept at horizontal position, the Radar coverage depends on the elevation angle and the azimuth angle.

## 3.2.1 Adjusting Elevation Angle of Radar

The elevation angle of the Radar refers to the angle between the normal line of the front cover and the horizontal line.

Figure 3-2 Adjust elevation angle of Radar
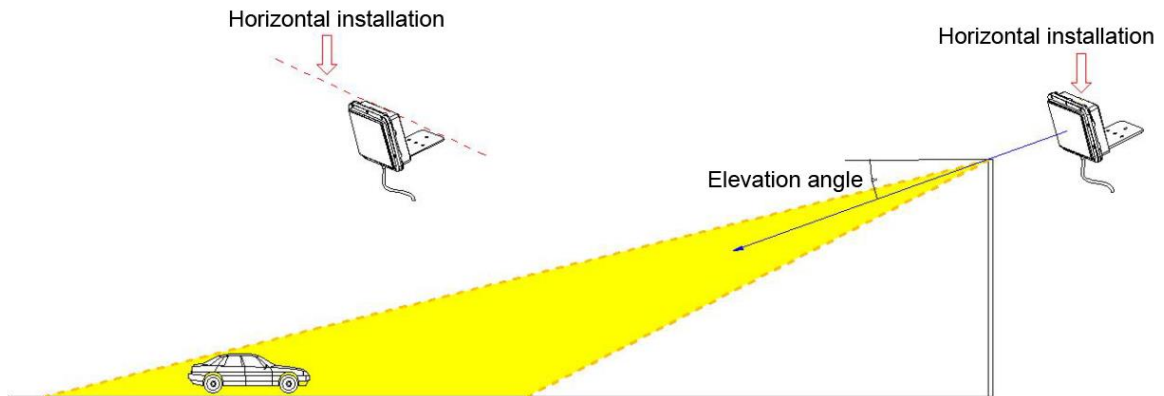


How to adjust the elevation angle of the Radar:

● Measure the elevation angle by using a protractor, and then adjust the angle (if necessary) according to Table 3-1, Table 3-2, and Table 3-3.

Table 3-1 Typical elevation angle in approaching mode (m (ft))

| Capture Distance | Installation Height | | | |
| --- | --- | --- | --- | --- |
| | 5 (16.4) | 6 (19.7) | 7 (23.0) | 8 (26.3) |
| 19 (62.3) | 12° | 14° | 16° | 19° |
| 21 (68.9) | 12° | 14° | 16° | 17° |
| 23 (75.5) | 12° | 13° | 15° | 16° |
| 25 (82.0) | 11° | 13° | 15° | 15° |
| 27 (88.6) | 11° | 13° | 14° | 15° |
| 29 (95.1) | 11° | 13° | 14° | 15° |

Table 3-2 Typical elevation angle in receding mode (m (ft))

| Capture Distance | Installation Height | | | |
| --- | --- | --- | --- | --- |
| | 5 (16.4) | 6 (19.7) | 7 (23.0) | 8 (26.3) |
| 25 (82.0) | 16° | 18° | 20° | 22° |
| 26 (85.3) | 15° | 17° | 19° | 21° |
| 28 (91.9) | 14° | 16° | 18° | 20° |
| 30 (98.4) | 14° | 15° | 17° | 19° |
| 32 (105.0) | 13° | 15° | 16° | 17° |

Table 3-3 Typical elevation angle in both-direction mode (m (ft))

| Capture Distance | Installation Height | | | |
| --- | --- | --- | --- | --- |
| | 5 (16.4) | 6 (19.7) | 7 (23.0) | 8 (26.3) |
| 25 (82.0) | 13° | 15° | 170° | 19° |
| 27 (88.6) | 12° | 14° | 16° | 18° |
| 29 (95.1) | 11° | 13° | 15° | 17° |

● Adjust the elevation angle by using a laser pointer.

Put the bottom of the laser pointer on the middle of the front cover, and then adjust the elevation angle of the Radar, until the laser spot is located at the distance shown in Table 3-4, Table 3-5, and Table 3-6.

Table 3-4 Radar beam transmitting distance in approaching mode (m (ft))

| Capture Distance | Installation Height | | | |
| --- | --- | --- | --- | --- |
| | 5 (16.4) | 6 (19.7) | 7 (23.0) | 8 (26.3) |
| 19 (62.3) | 23 (75.5) | 24 (78.7) | 24 (78.7) | 24 (78.7) |
| 21 (68.9) | 23 (75.5) | 24 (78.7) | 24 (78.7) | 26 (85.3) |
| 23 (75.5) | 23 (75.5) | 26 (85.3) | 26 (85.3) | 28 (91.9) |
| 25 (82.0) | 26 (85.3) | 26 (85.3) | 26 (85.3) | 30 (98.4) |
| 27 (88.6) | 26 (85.3) | 26 (85.3) | 26 (85.3) | 30 (98.4) |
| 29 (95.1) | 26 (85.3) | 26 (85.3) | 26 (85.3) | 30 (98.4) |

Table 3-5 Radar beam transmitting distance in receding mode (m (ft))

| Capture Distance | Installation Height | | | |
| --- | --- | --- | --- | --- |
| | 5 (16.4) | 6 (19.7) | 7 (23.0) | 8 (26.3) |
| 25 (82.0) | 18 (59.1) | 19 (62.3) | 19 (62.3) | 20 (65.6) |
| 26 (85.3) | 19 (62.3) | 20 (65.6) | 20 (65.6) | 21 (68.9) |
| 28 (91.9) | 20 (65.6) | 21 (68.9) | 22 (72.2) | 22 (72.2) |
| 30 (98.4) | 20 (65.6) | 22 (72.2) | 23 (75.5) | 23 (75.5) |
| 32 (105.0) | 22 (72.2) | 22 (72.2) | 24 (78.7) | 26 (85.3) |

Table 3-6 Radar beam transmitting distance in both-direction mode (m (ft))

| Capture Distance | Installation Height | | | |
| --- | --- | --- | --- | --- |
| | 5 (16.4) | 6 (19.7) | 7 (23.0) | 8 (26.3) |
| 25 (82.0) | 21.5 (70.5) | 22.5 (73.8) | 23 (75.5) | 23 (75.5) |
| 27 (88.6) | 23.5 (77.1) | 24 (78.7) | 24.5 (80.4) | 24.5 (80.4) |
| 29 (95.1) | 25 (82.0) | 26 (85.3) | 26 (85.3) | 26 (85.3) |

## 3.2.2 Adjusting Azimuth Angle of Radar

The azimuth angle of radar refers to the angle between the normal line of the front cover and the direction of moving vehicles. The broken yellow lines represent the boundaries of the radar beam, while the blue line represents the central line of the radar beam.

When the Radar is installed right above the lane, make sure that the radar beam is as parallel as possible to the vehicle movement direction. See Figure 3-3.

For roadside installation, make sure that the center of the radar beam is aimed at the middle area of the detected lane. See Figure 3-4. Use a laser pointer to help you aim the radar beam at the middle area of the detected lane.

Figure 3-3 Top view of radar beam when Radar is installed above the lane
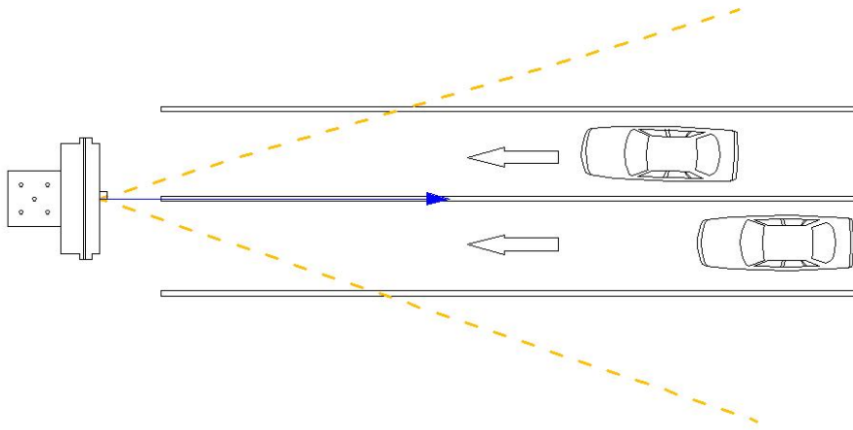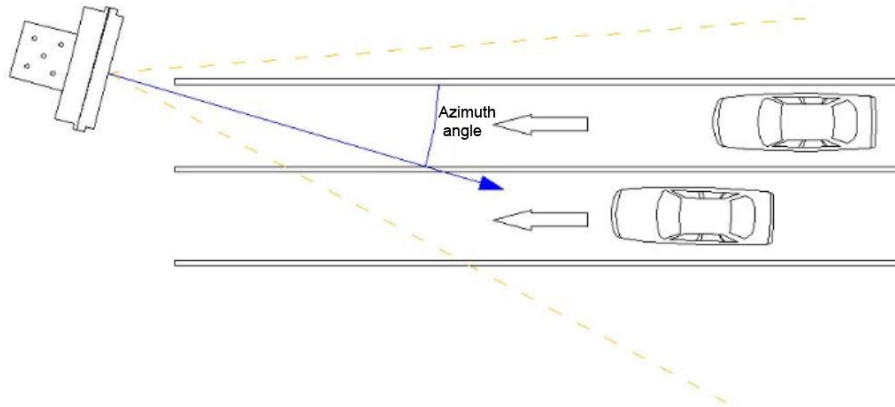


Figure 3-4 Top view of radar beam with roadside installation

# 4 FAQ

| Question | Solutions |
|---|---|
| The Radar does not work after being powered on | 1) Check power connection and voltage<br>2) Check whether the positive and negative electrodes of power module are correctly connected<br>3) Check communication cable connection<br>4) Check the data receive interface, or the software can work properly<br>5) Check the serial port settings of the program |
| Messy code | 1) Check communication cable connection<br>2) Check baud rate settings<br>3) Check EMC/EMI |
| The Radar does not capture targets | 1) Check the elevation angle and the azimuth angle of the Radar. Make sure that the area to be detected is fully covered by the radar beam<br>2) Compare the animation and the real trajectory of the vehicles<br>3) Check whether the capture distance is reasonable<br>4) Check whether the threshold is set too high |
| Vehicles are not captured | 1) Check whether there are strong EMI source around the Radar<br>2) Check the elevation angle and the azimuth angle of the Radar. Make sure that the area to be detected is fully covered by the radar beam<br>3) Check whether the threshold is set too high |
| Missed capture | 1) Check the elevation angle and the azimuth angle of the Radar. Make sure that the area to be detected is fully covered by the radar beam<br>2) Compare the animation and the real trajectory of the vehicles<br>3) Check whether the capture distance is reasonable<br>4) Check whether the threshold is set too low |

# 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

**Federal Communications Commission (FCC) Interference Statement**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1.  This device may not cause harmful interference.

2.  This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

**RF exposure warning**
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.