

Narrow Wave Tablet Radar

Quick Start Guide



V1.0.0

Foreword

General

This manual introduces the functions and operations of the narrow wave tablet radar (hereinafter referred to as the "Radar"). Read carefully before using the Device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 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, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	September 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This chapter introduces 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.



- Pay attention to personnel safety when installing the Radar at intersections or certain road sections.
- Non-professionals are forbidden to disassemble and install the Radar.
- Before powering on the Radar, check all the power connections to prevent short circuit.
- Properly ground the Radar.
- Securely install the Radar to reduce the impact of vibration on the Radar.
- The cables must meet the requirements of shielding, insulation, and moisture resistance.

Power Source Requirements



- Use high-quality DC power supply that meets the voltage requirements to avoid crosstalk from other devices.
- Strictly comply with the local electric safety standards.
- Make sure that the power supply is correct before operating the Radar.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, please refer to device labels.
- Install easy-to-use device for power off before installing cables, which is for emergent power off when necessary.
- Prevent the line cord from being trampled or pressed, especially the plug, power socket and the junction.
- Application Environment Requirements
- Make sure that there are no obstructions in the front of the Radar.
- Do not hot swap the serial port.
- Do not impact the Radar. Prevent the Radar from falling down.
- 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.
- Do not block the ventilation near 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.

Maintenance Requirements



WARNING

- Use accessories suggested by the manufacturer, and install and maintain the Radar by professionals.
- Do not provide two or more power supply modes; otherwise, the Radar might be damaged.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Product Introduction.....	1
2 Device Structure.....	2
2.1 Dimensions.....	2
2.2 Structure.....	2
3 Client Operation.....	4
3.1 Connecting Radar.....	4
3.2 Installing Client.....	4
3.3 Configuring Client.....	6
3.3.1 Device Connection.....	6
3.3.2 Speed Measurement Status.....	6
3.3.3 Parameter Settings.....	7
4 Updating Device.....	9
4.1 Updating Program.....	9
4.2 Updating WEB.....	9
Appendix 1 Cybersecurity Recommendations.....	10

1 Product Introduction

The narrow wave tablet radar is a narrow beam radar with planar antenna system. It is specifically designed to detect moving vehicles to meet modern traffic management challenges.

The product uses modern microwave radar technology and high-speed digital signal processing technology for precise positioning and accurate speed measurement. The Radar can be applied to a wide range of complex road environments such as tunnel entrance and highway interchanges, providing real-time traffic information and forensic evidence for traffic speed violations.

2 Device Structure

2.1 Dimensions

Figure 2-1 Front view (mm (inch))

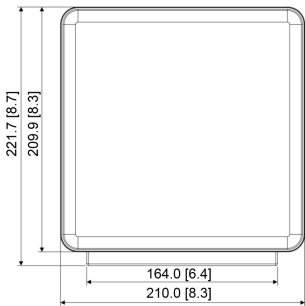
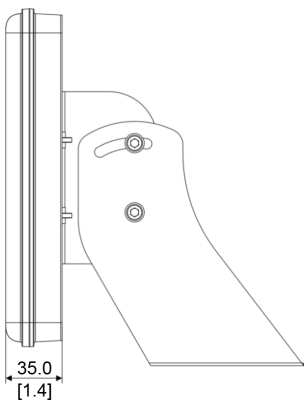


Figure 2-2 Side view (mm (inch))



2.2 Structure

The device structure relates to the Radar and the bracket.

Figure 2-3 Radar structure

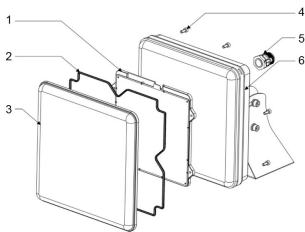


Table 2-1 Radar structure

No.	Description
1	Antenna
2	Sealing washer
3	Front cover

No.	Description
4	Set screw
5	PG connector
6	Rear cover

Figure 2-4 Bracket structure

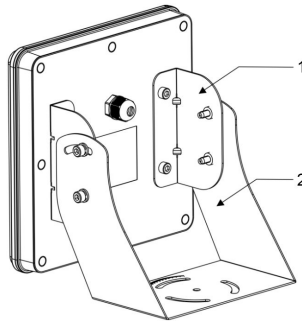


Table 2-2 Bracket structure

No.	Description
1	Bracket 1
2	Bracket 2

Figure 2-5 Radar wiring

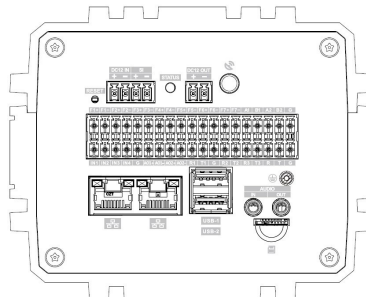


Table 2-3 Radar interface

Interface		Function
R1, T1, G	3-channel radar port	Supports connecting 3 radars at the same time.
R2, T2, G		
R3, T3, G		

3 Client Operation

3.1 Connecting Radar

You need to connect radar before login client, and the connection can be done through Wi-Fi hotspot or port.

- Wi-Fi connection
- Normally you need a DC 12V power supply to power on the radar, and then use a computer with Wi-Fi function to search nearby hotspot. Connect the Wi-Fi named **WIFI+SN (serial number)** in searched outcomes, and then login client on PC to configure the radar. For the Wi-Fi password, please contact technical support.
- Ethernet connection
- Connect the radar and PC through Ethernet, and then login client on PC to configure the radar.
- Connection details see Table 3-1 .

Table 3-1 Port connection

Radar		Connection	PC	
Color of the cable	Signal	Connection	DB9 Female	Signal
Yellow	RXD		2	TXD
Green	TXD		3	RXD
Brown	GND		5	GND

3.2 Installing Client

Procedure

Step 1 Open the compressed file of client installation program.



You can get the installation program from technical personnel.

Step 2 Double click **setup.exe**, and then install the client following instructions.

Step 3 After finishing installation, double-click  on desktop to open the radar client.

Figure 3-1 Radar client

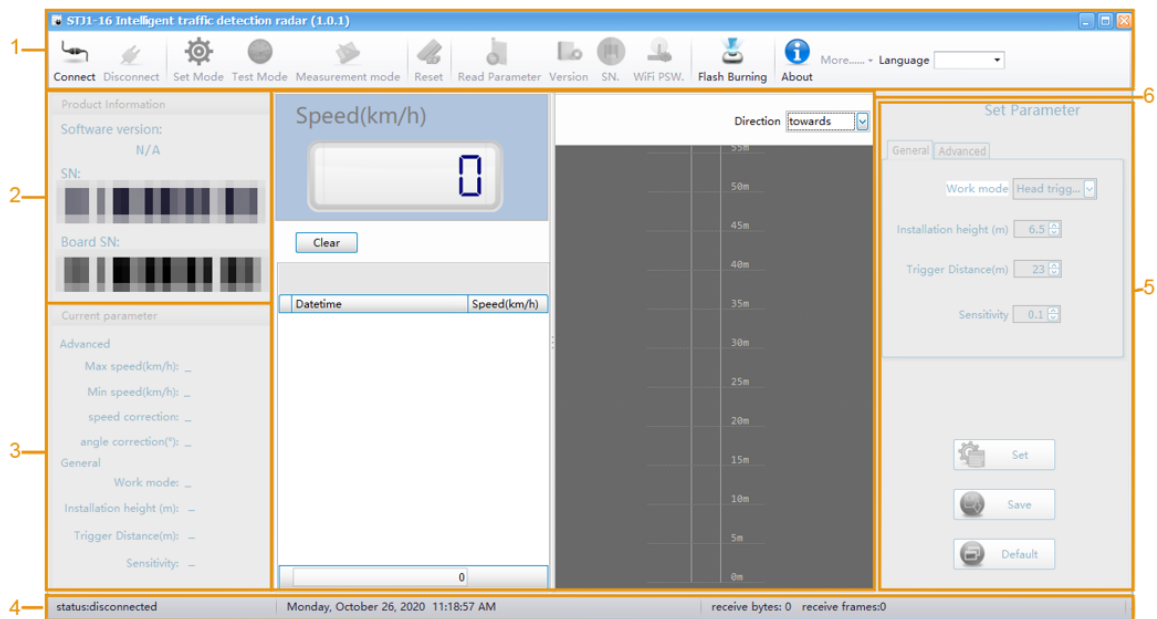


Table 3-2 Introduction of the client

No.	Name	Description
1	Function Menu	Select functions to do corresponding operations. • Connect/Disconnect: Connect or disconnect the radar. For details see "3.3.1 Device Connection". • Set Mode: Configure related parameters of the radar speed measurement. For details see "3.3.3 Parameter Settings". • Test Mode: The normal working status of the radar, measuring vehicle speed. For details see "3.3.2 Speed Measurement Status". • Measurement mode: Click this and then the radar turns to measurement mode, which is used to do indoor stimulation and calibration. • Reset: Click this and the radar restarts. • Read Parameter: Click this to read and check current configured parameters. • Version: Click this to refresh software version. • SN: Click this to refresh the radar serial number. • WiFi PSW: Click this to reset Wi-Fi password. • Flash burning: Update program. For details see "4.1 Updating Program". • About: Click this to check the client version. • Language: Language switch between Chinese and English, and it will take effect after restart.
2	Product Information	Display the software version, SN and board SN.

No.	Name	Description
3	Current Parameter	Display current configured speed measurement parameters of the radar, including advanced and general settings.
4	System Specifications	Display the connection status, system time, received bytes and frame of the radar.
5	Parameter Settings	Configure general and advanced parameters of radar speed measurement. For details see "3.3.3 Parameter Settings".
6	Speed Measurement Status	Display the speed and position of the vehicles. For details see "3.3.2 Speed Measurement Status".

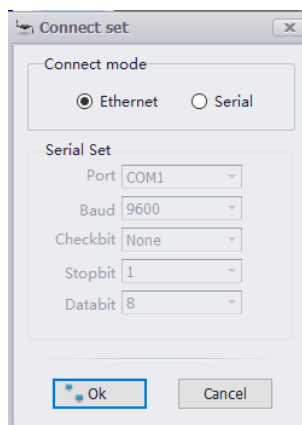
3.3 Configuring Client

3.3.1 Device Connection

Click **Connect** in function menu, select **Ethernet** or **Serial** according to actual connection method, and then click **OK** to connect the radar.

- Ethernet: When connecting the radar through Wi-Fi hotspot, select this.
- Serial: When connecting the radar through serial, select this and corresponding **P**ort, **B**aud, **C**heckbit, **S**topbit and **D**atabit.

Figure 3-2 Device connection

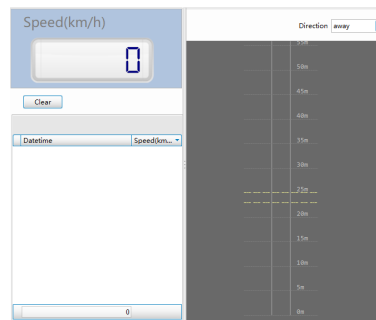


3.3.2 Speed Measurement Status

After successfully connected, the device will be on test status by default, namely, capture mode when the radar works properly. Under this mode, when a vehicle passes the trigger spot, its position and speed will be displayed and reported.

- Click **Clear** to delete current speed measurement data.
- Select **Towards** or **Away** in the dropdown list of **Direction**, you can select different driving direction.
- Click **Datetime** or **Speed**, you can sort the data as ascending or descending according to time or speed.

Figure 3-3 Test status



3.3.3 Parameter Settings

Normally you do not need to change the speed measurement parameters, if you do, you can configure the general or advanced parameters in settings.

Click **Set Mode** > **Set Parameter**, and then click **General** or **Advanced** on parameter settings interface. To configure related parameters, click **Set**.

Figure 3-4 Parameter settings

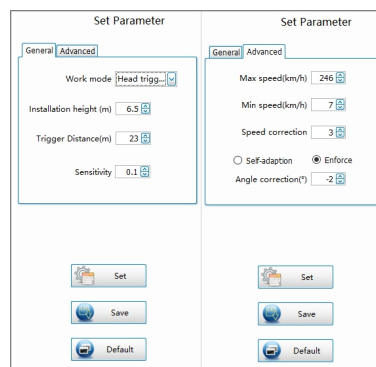


Table 3-3 Parameter description

Parameter		Description
General	Work mode	Select the mode of triggering the radar. You can choose Head trigger, Tail trigger, Continue or Both trigger.
	Installation height	Enter the actual installation height of the radar.
	Trigger distance	Set up the distance that triggers the radar.
	Sensitivity	Set up the capture sensitivity of the Radar. The larger the value, the more sensitive the Radar.

Parameter		Description
Advanced	Max speed	Set up the maximum and minimum of the radar measured speed, used for over speed and slow speed respectively.
	Min speed	
	Speed correction	Do not modify this parameter if you are not professionals.
	Angle correction	

- Click **Save** to save current configured parameters, they will take effect after restart the radar.
- Click **Default** to restore the device parameters to original configuration.

4 Updating Device

4.1 Updating Program

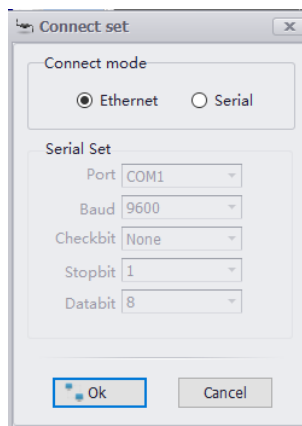
Background Information

Update the device program through Wi-Fi.

Procedure

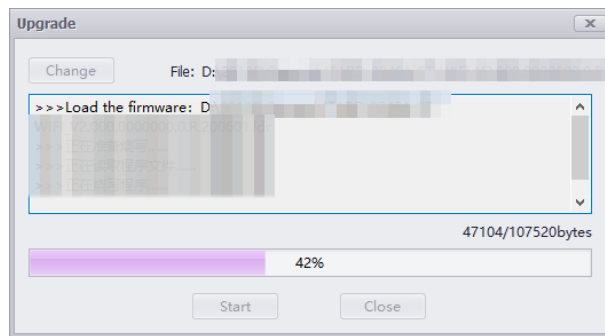
- Step 1 Open the client, disconnect the radar and then click **Flash Burning** on function menu bar.
- Step 2 Select **Ethernet** and then click **OK**.

Figure 4-1 Connection



- Step 3 Click **Change**, select update file and then click **Start**.

Figure 4-2 Program Update



4.2 Updating WEB

Background Information

Supports updating the radar on WEB interface.

Procedure

- Step 1 Log in to Web interface, select **Settings** > **System Management** > **Radar Update**.
- Step 2 Click **Import**, select the update file according to the path and then open it. Update the file to radar.ldr.
- Step 3 Click **Update** and then system starts to update the radar.

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 device 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 device (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 device 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 device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (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 device 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. MAC Address Binding

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

8. Assign Accounts and Privileges Reasonably

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

9. 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.

10. 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.

11. Secure Auditing

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

12. Network Log

Due to the limited storage capacity of the device, 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.

13. Construct a Safe Network Environment

In order to better ensure the safety of device 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.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.