

EAS RF Antenna User's Manual













Foreword

General

This manual introduces the installation, functions and operations of the EAS Radio-Frequency Antenna (hereinafter referred to as "the Device"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

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

Signal Words	Descriptions
 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, lower performance, or unpredictable result.
 ESD PROTECTION	Indicates electrostatic sensitive equipment.
 WARNING ELECTRIC SHOCK	Indicates high voltage danger.
 LASER RADIATION	Indicates strong laser radiation.
 FAN WARNING	Indicates dangerous moving parts, please stay away from moving fan blades.
 WARNING MECHANICAL INJURY	Indicates that equipment parts will cause mechanical wounding to people.
 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 date
V1.0.0	First release.	June 2021

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 section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Operating Requirements

- Transport, use and store the Device under the allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Install the Device in a well-ventilated place, and do not block its vents.
- Do not press hard, vibrate violently, or soak the device.
- Use factory package or same-quality material for packaging when transporting the device.
- It is recommended to use this device with a surge protection device (SPD) to improve the lightning protection effect.
- It is recommended to ground the earthing hole of the device to improve device reliability.
- It is recommended to install the device 2 meters away from the escalator to improve device reliability.

Power Requirements:

- Only use the wire assembly (power cable) recommended in this area and use it within its rated specifications.
- Only use the standard power adapter of the device, otherwise the user will be responsible for personnel injury or device damage.
- Use a power supply that meets the requirements of SELV (Safety Extra Low Voltage) and supply power in accordance with the rated voltage of (IEC60065) or (IEC60950-1 compliant with Limited Power Source). The specific power supply requirements are subject to the device label.
- Connect the I-type structure to the power socket with protective earthing.
- Use an independent power cable from the power supply box for power supply.
- When connecting power, the left cable should be neutral wire and right live wire.
- Be strictly grounded and powered independently.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Product Introduction.....	1
1.1 Introduction	1
1.2 Features	1
1.3 Advantages	1
2 Appearance	2
3 Installation and Configuration	4
3.1 Cautions	4
3.2 Packing List.....	4
3.3 Installation and Configuration	5
3.4 Descriptions of TX Board Ports and Hardware Manual Configuration	6
3.5 TX Antennas Sync.....	9
Appendix 1 Cybersecurity Recommendations	11

1 Product Introduction

1.1 Introduction

Dahua RF anti-theft antenna is an anti-theft device that can effectively identify the RF tags and labels. The product can effectively reduce goods theft as well as operating cost of merchants, and improve the shopping experience of customers. It has advantages of minimalist and elegant appearance, unmatched performance and colorful functions, which is regarded as a significant part of the EAS system.

1.2 Features

- Detection of EAS tags & labels: Effectively detect and identify the RF tags and labels within coverage.
- Sound and light alarm: When the RF tags or labels are detected, the alarm tone and the alarm indicator will be triggered. Multiple alarm tones and alarm volume levels are selectable.
- Power-on self-test function: Effectively identify with extremely low false alarm rate and avoid more than 95% of external interference sources.
- Detection distance of tags: Taking small pencil as a test block, the distance is more than 1.6m (the distance between TX and RX antennas) under the laboratory circumstance.
Detection distance of labels: Taking DHI-ISC-ETR1-5050 as a test block, the distance is more than 1.4m (the distance between TX and RX antennas) under the laboratory circumstance.
- CCTV Linkage: Standard CCTV Linkage, which sends the alarm signal to the monitoring camera synchronously. And camera will record the alarm videos automatically for future reference.

1.3 Advantages

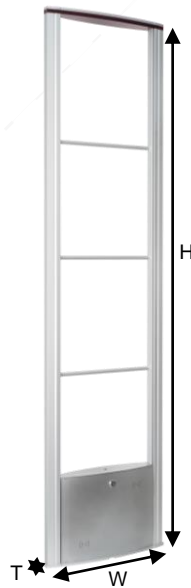
- Stable hardware performance: The high-performance TX antennas work perfectly with RX antennas, which has features as stable operation, no temperature drift, and no performance degradation in long-term use.
- Strong anti-interference ability: Equipped with sensitivity adjustment function, it can effectively reduce the interference of environmental noise on the Device.
- Powerful signal processing capability: Unique receiving signal filtering algorithm ensures accurate identification of tag signals with extremely low false alarm rate.
- Wide applicability: Compatible with most RF tags and labels.
- Energy saving and environmental protection: Extremely low operating power consumption, energy saving and environmental-friendly with no pollution.

2 Appearance

Figure 2-1 Appearance



Figure 2-2 Product Dimensions



1670 mm x 420 mm x 80 mm (H*W*T)
(66.75" x 16.54 x 3.46")






3 Installation and Configuration

3.1 Cautions

- Only be used for indoors.
- Do not cover the Device and keep it ventilated.
- Do not expose the Device to sunlight, water and moisture.
- Only be installed by professionals enforcing safety requirements.
- Be strictly grounded and powered independently.
- Operating temperature: $-5\text{ }^{\circ}\text{C}$ to $50\text{ }^{\circ}\text{C}$ (23°F to 122°F)

3.2 Packing List

Table 3-1 Packing List

Packing List	Image	Packing Box
TX Antenna		
RX antenna		
2-Cord Power Cord (RX)		
24 VDC Power Supply (TX)		

3.3 Installation and Configuration

Table 3-2 Tool requirements

Name	Image	Name	Image
Cross and slotted screwdrivers		M10x100 expansion screw x 4	
Marker x 1		Open-end wrenches	
Cutting Machine x 1		Hammer x 1	
Fine sand		Scuff-plate	
Impact driver x 1			

Installation Procedures

- ◇ Site survey: The Device must be installed at least 2 meters away from large electrical appliances, escalators, metal panels and more.
- ◇ Device check:
 1. After connecting the Device, power on to check whether there is any problems.
 2. Determine the installation location according to the site. (The space is recommended to be 1.2m-1.8m.)
- ◇ After determining the installation location, use a marker to draw lines, punch holes, and cut grooves. Then clean up the site.



- ◇ Install and fix the Device: Put fine sand in the cutting groove to protect the cables and fill the gaps. Next install the scuff-plate on the floor. Then fix the Device.



- ◇ The Device installation is complete.



3.4 Descriptions of TX Board Ports and Hardware Manual Configuration

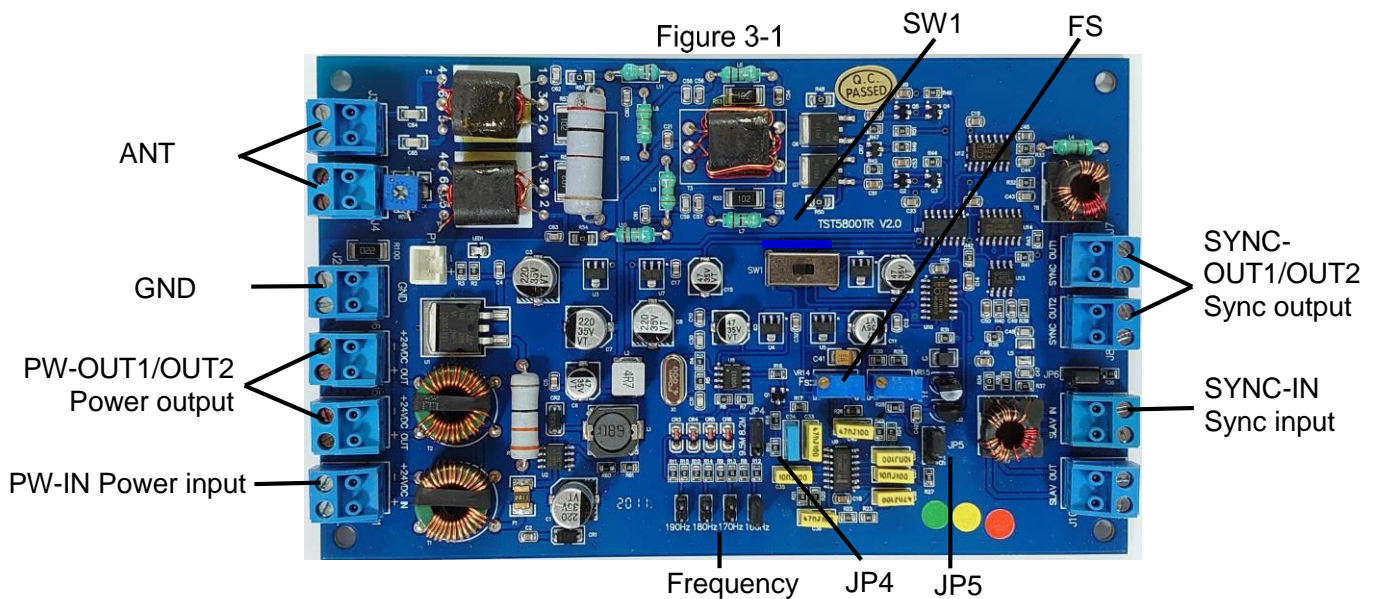


Table 3-3 Function setting

Function	Terminal	Settings		Factory settings
Sweep frequency width	JP4	8.2M	9.5M	8.2M
	JP5			
TX antennas sync mode	SW1	TX primary antenna mode	TX replica antenna mode	TX primary antenna mode

Frequency can be set as 160, 170, 180 and 190Hz. Set the frequency by a jumper cap: for example, if the jumper cap is put in the 160Hz port, the frequency is 160Hz. The factory setting is 160Hz.

Table 3-4 Potentiometer function

VR14(Δ)	Sweep frequency width
VR15(FS)	Center frequency

Remarks:

1. Please keep the potentiometers VR14 and VR15 in the factory state.
2. The factory setting of the center frequency is 8.2M (JP3, JP4 are set down).
3. The factory setting of the sweep frequency width is 950K.

Table 3-5 Specifications

Dimensions	165*102 mm
Net weight	0.15 kg

Figure 3-2

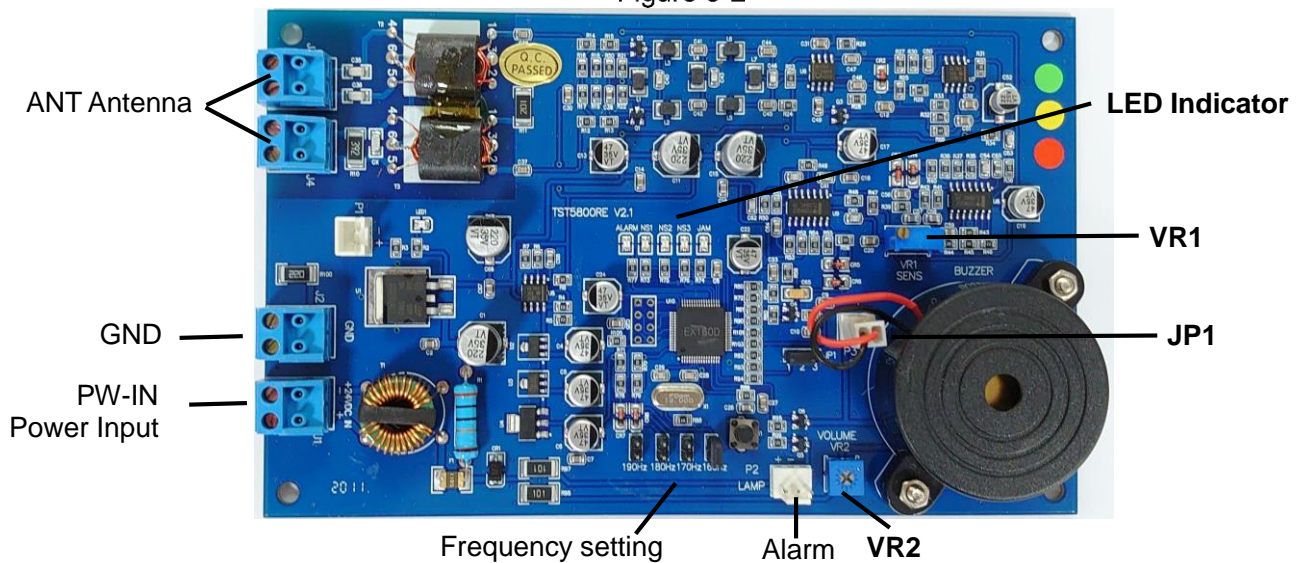





Table 3-6 LED Indicator

Port	Function	Descriptions		
NS1	Signal strength	High	Middle	Low
NS2				
NS3				
ALARM	Alarm prompt	Alarm indicator on (red indicator)		
JAM	Noise prompt	Keeps off. The antenna cannot be used when the indicator is on.		

Frequency can be set as 160, 170, 180 and 190Hz. Set the frequency by a jumper cap: for example, if the jumper cap is put in the 160Hz port, the frequency is 160Hz. The factory settings is 160Hz.

Table 3-7 Function setting

Function	Connection port	Settings		Factory settings
Alarm tone type	JP1	Intermittent tone	lasting tone + Intermittent tone	Intermittent tone

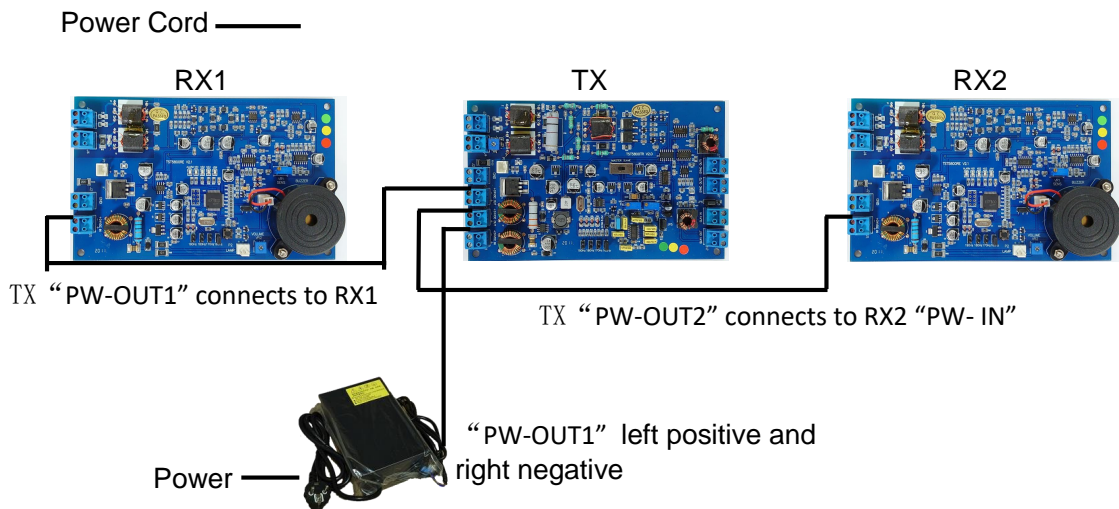
Table 3-8 Potentiometer function

VR1(SENS)	Receiving sensitivity (clockwise to increase, counterclockwise to decrease)
VR2(VOLUME)	Alarm volume (clockwise to increase, counterclockwise to decrease)

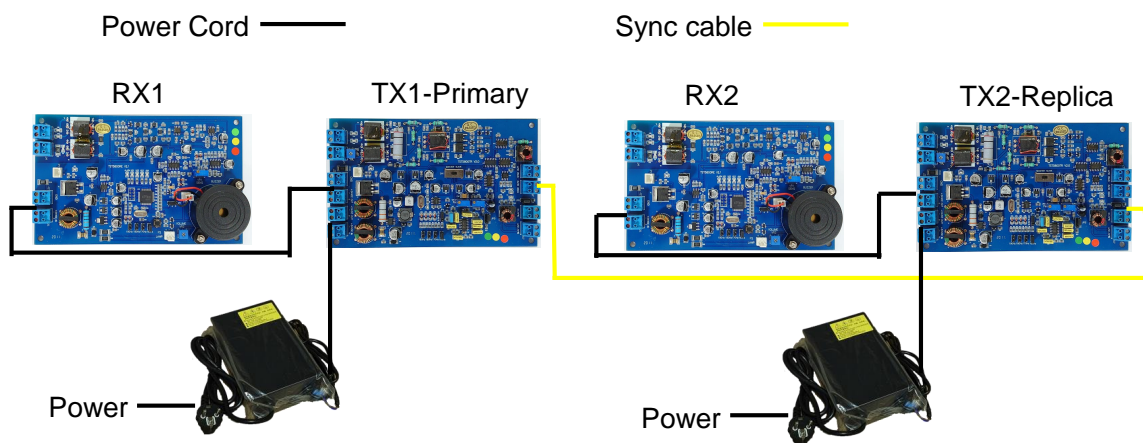
Table 3-9 Specifications

Dimensions	165*102 mm
Net weight	0.11 kg
Detection distance of big square	200cm
Detection distance of small square	170cm
Detection Distance of Labels	140cm

Schematic Diagram of 1TX&2RX:



Schematic Diagram of sync use of multiple antennas:

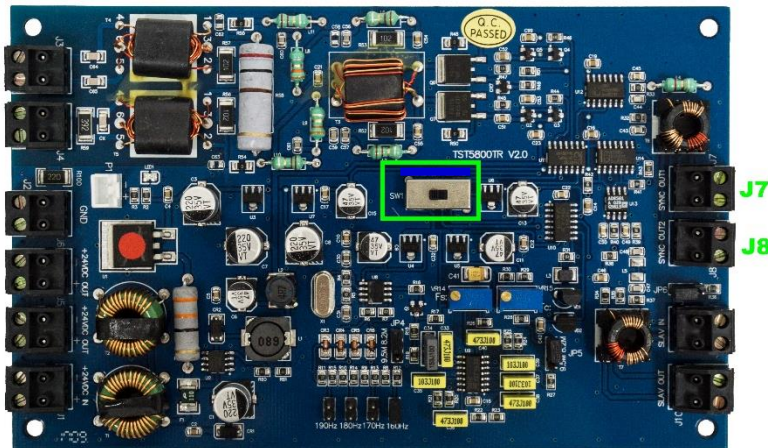


3.5 TX Antennas Sync

When it needs to be installed multiple TX antennas in the same installation channel, each TX antenna needs to set to be synchronous, or the antennas cannot work normally because of the interactive interference. The sync way is as follows:

①TX primary antenna: Turn the toggle switch SW1 to the left position, the J7 and J8 terminals on the TX primary antenna are the synchronous signal output terminals. One TX primary antenna can output two synchronous signals at the same time to connect two TX replica antennas. **When in sync use, if the TX primary antenna fails, the entire synchronous system will be completely paralyzed, and all TX replica antennas will fail.**

Figure 3-3



②TX replica antenna: Turn the toggle switch SW1 to the right position, the J9 terminal is the synchronous signal input terminal, which connects to the output signal of the TX primary antenna. Meanwhile, J7, J8 terminals of the TX replica antenna can be used as the synchronous signal output terminal to connect to another 2 replica TX antennas.

Figure 3-4

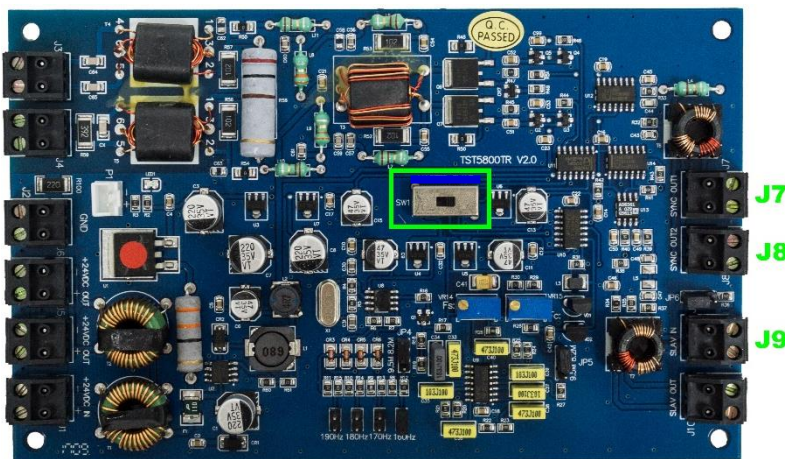
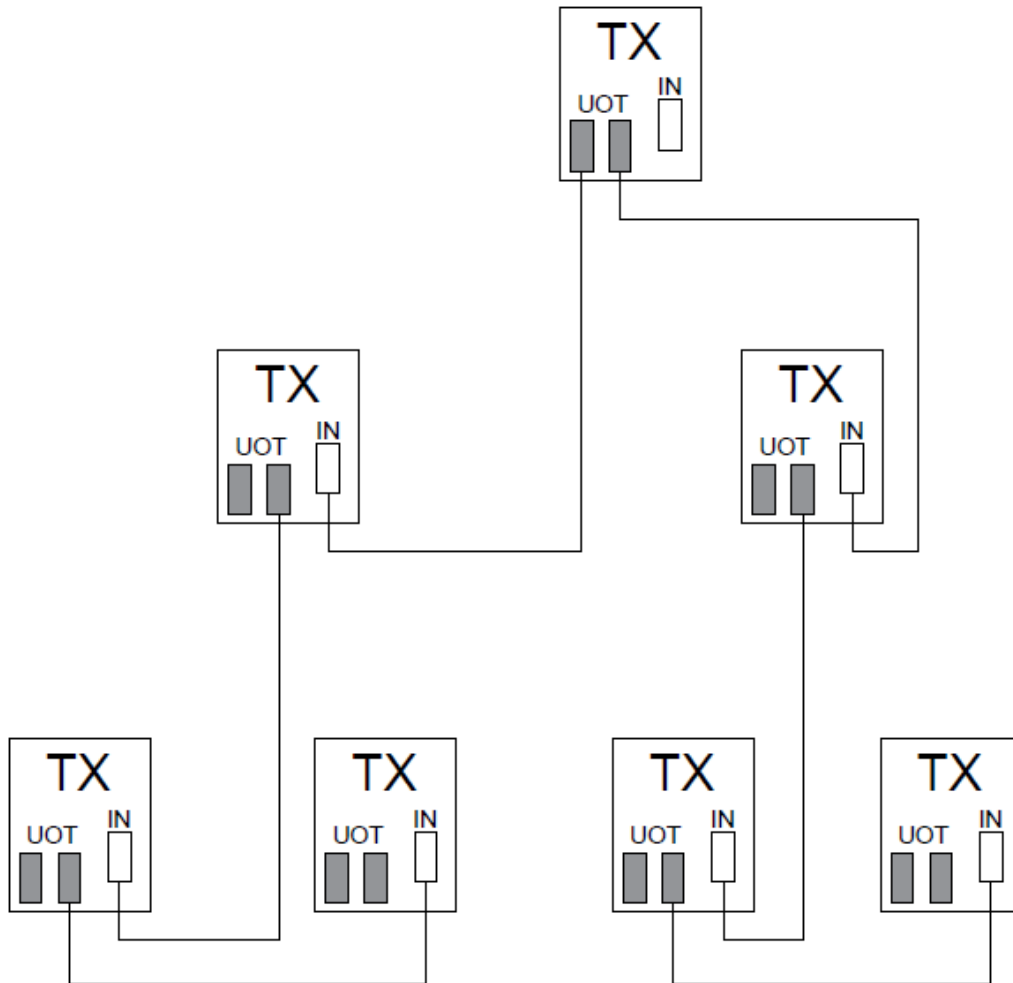


Figure 3-5 Schematic diagram of TX antennas sync



⚠ CAUTIONS

- When multiple antennas are in sync use, all antennas must be installed in the same direction, the side with the mainboard facing the same direction. That is to say, antennas cannot be installed with mainboard facing mainboard.
- TX primary antennas sync mode supports up to 7 antennas for synchronous connection (as shown in the figure above). If there are more than 7 antennas for synchronous connection, a synchronizer must be used. A synchronizer can output to 8 TX replica antennas at the same time, and each TX replica antenna can also output two groups of synchronous signals, which means it supports up to 24 TX antennas for synchronization.
- When in sync use by synchronizer, if the synchronizer fails, the entire synchronous system will be completely paralyzed, and all TX replica antennas will fail.

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 from Dahua 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.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883