

HDCVI Two-way Talk Modem

User's Manual



V1.0.0

Foreword

General

This manual introduces the functions and operations of the HDCVI two-way talk modem (hereinafter referred to as the "Device"). 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.	June 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 section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, comply with the guidelines when using it.

Transportation Requirements



- Transport the device under allowed humidity and temperature conditions.
- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during transportation.
- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.

Storage Requirements



- Store the device under allowed humidity and temperature conditions.
- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during storage.

Installation Requirements



- Strictly comply with the local electrical safety code and standards, and check whether the power supply is correct before operating the device.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Make sure that the power adapter meets the device operating voltage requirement before powering up the device (The material and length of the power cable might influence the device voltage).



- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during installation.
- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- We assume no liability or responsibility for all the fires or electrical shock caused by improper handling or installation.
- Ground the device to protective ground before you power it on.
- Use qualified video transmission cable to improve video quality, and use RG59 coaxial cable or higher standard.

Operating Requirements



- Use the device under allowed humidity and temperature conditions.
- Protect the line cord and wires from being walked on or squeezed particularly at plugs, power sockets, and the point where they exit from the device.
- Prevent liquid from flowing into the device to avoid damage to its internal components.
- Do not block the ventilation opening near the device to avoid heat accumulation.

Maintenance Requirements



Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Overview.....	1
1.1 Introduction.....	1
1.2 Features.....	1
2 Ports.....	2
3 Device Connection.....	4
Appendix 1 Security Recommendation.....	5

1 Overview

1.1 Introduction

HDCVI Two-way Talk Modem can modulate the audio signal output by DVR, and then transmit it to HDCVI camera via the coaxial cable for demodulation, achieving HDCVI camera two-way talk.

1.2 Features

- Supports 12 VDC $\pm$ 30% wide voltage input.
- Supports low power consumption.
- Supports hot plugging.
- Supports 1-channel or 4-channel HDCVI camera.



Different devices support different channels, please refer to the actual device.

2 Ports



The figure is for reference only. Structures might differ from different devices, refer to the actual product.

Figure 2-1 Ports (1)

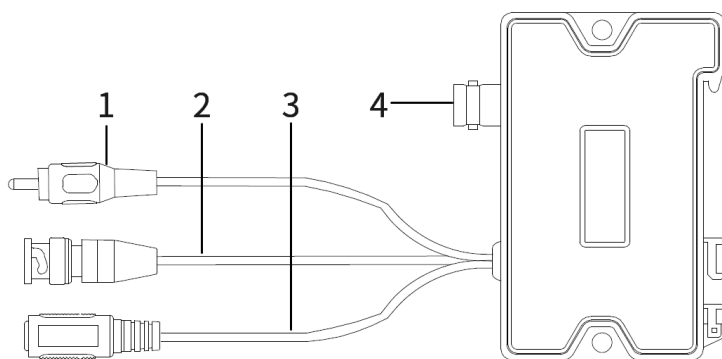


Table 2-1 Port description (1)

No.	Description
1	Connects the audio output port of DVR.  Suggest the input audio cable not exceeding 5 m.
2	Connects the Device to DVR.
3	12 VDC power input.
4	Connects the Device to HDCVI Camera.

Figure 2-2 Ports (2)

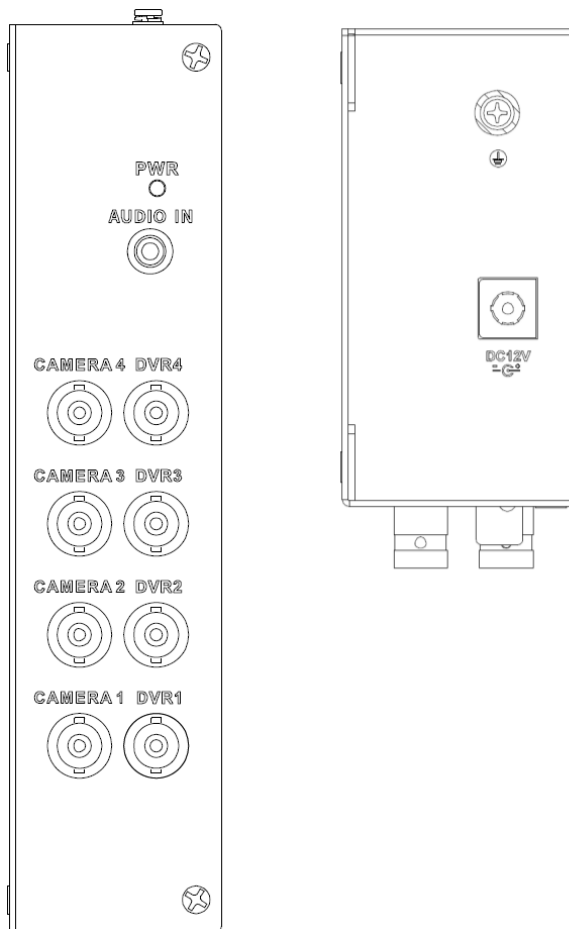


Table 2-2 Port description (2)

Port	Description
PWR	Power indicator light. - Indicator on: The Device is powered on. - Indicator off: The Device is powered off.
AUDIO IN	Connects the audio output port of DVR.  Suggest the input audio cable not exceeding 5 m.
CAMERA 1–CAMERA 4	Connects the Device to HDCVI Camera.
DVR 1–DVR 4	Connects the Device to DVR.
DC 12V	12 VDC power input.
	Grounding terminal.

3 Device Connection

1. Connect the Device to HDCVI Camera through coaxial cable.
2. Connect the Device to DVR through coaxial cable and audio cable.
3. Connect the Device to power adapter to power up the Device.



It is not recommended to use twisted-pair cables for coaxial video connections.

Figure 3-1 Device connection (1)

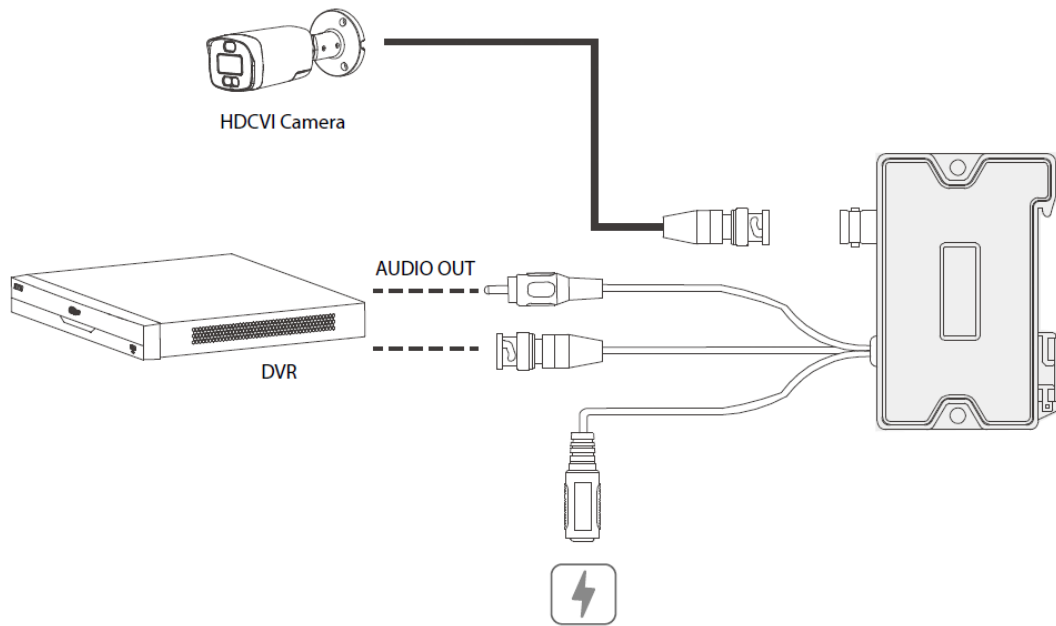
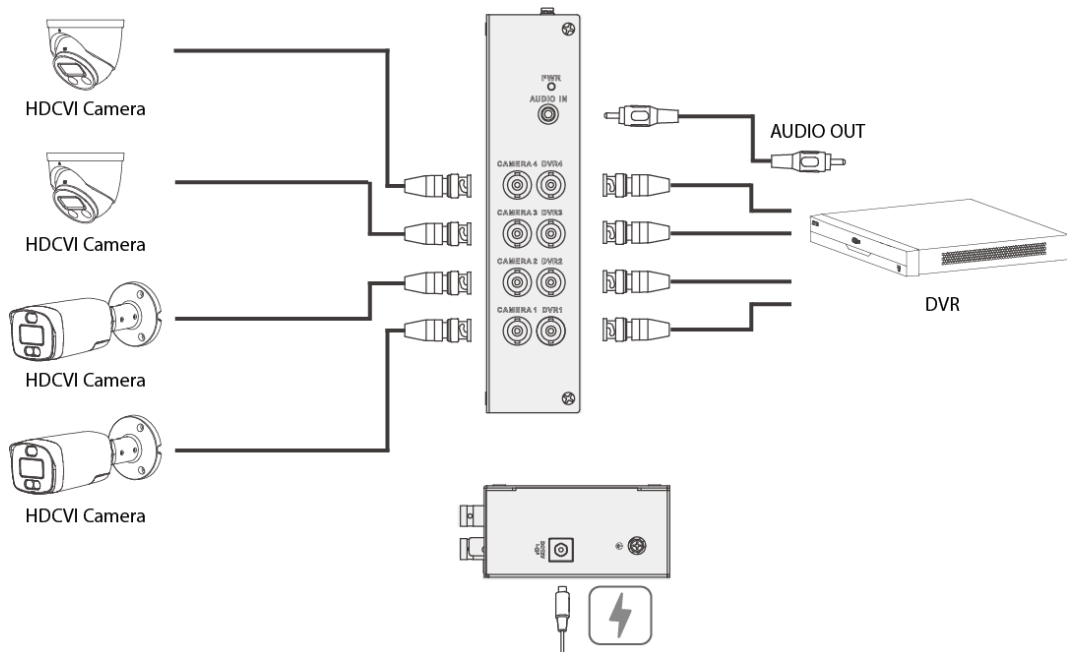


Figure 3-2 Device connection (2)



Appendix 1 Security Recommendation

1. Account Management

a. Use Strong 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.

b. Change Password Regularly

It is suggested to change passwords regularly to reduce the risk of being guessed or cracked.

c. Assign Accounts and Permissions Reasonably

According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

d. Enable Account Lock

The account lock feature is enabled by default, and it is recommended 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.

e. Set and Update Passwords Reset Information Timely

The platform supports password reset function. To reduce the risk of being attacked, please set up related information for password reset in time. 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.

f. Enable Account Binding IP/MAC

It is recommended to enable the account binding IP/MAC mechanism to further improve access security.

2. Service Configuration

a. Enable HTTPS

It is suggested to enable HTTPS, so that you visit web service through a secure communication channel.

b. Disable Unnecessary Services and Choose Secure Modes

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

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

- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.

3. Network Configuration

a. Enable Firewall Allowlist

It is suggested to enable allowlist 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 allowlist.

b. Network Isolation

The network should be isolated by partitioning the video monitoring network and the office network on the switch and router to different VLANs. This prevents attackers from using the office network to launch Pivoting attacks on the video monitoring network.

4. **Security Auditing**

a. **Check Online Users**

It is recommended to check online users irregularly to identify whether there are illegal users logging in.

b. **View the Platform Log**

By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

5. **Physical Protection**

It is suggested to perform physical protection to the device that has installed the platform. 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.

6. **Perimeter Security**

It is suggested to deploy perimeter security products and take necessary measures such as authorized access, access control, and intrusion prevention to protect the software platform security.