

Analog 4-Wire Video Intercom

Quick Start Guide








Foreword

General

This document mainly introduces structure, installation, wiring and menu operations of the analog 4-wire video intercom.

Safety Instructions

The following categorized signal words with defined meaning 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, 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.	August 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 following description is the correct application method of the device. Please read the manual carefully before use, in order to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

Operating Requirements

- Do not expose the device to direct sunlight or heat source.
- Do not install the device in a humid or dusty area.
- Install the device horizontally at stable places to prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids.
- Install the device at well-ventilated places and do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device by yourself.
- The device should be used with screened network cables.

Power Requirements

- Use recommended power cables in the region under their rated specification.
- 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.
- Appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.

Device Update

Do not cut off power supply during device update. Power supply can be cut off only after the device has completed update and has restarted.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Structure	1
1.1 Introduction	1
1.2 Features	1
1.3 Front Panel	1
1.4 Rear Panel	3
2 Installation	4
2.1 Indoor Monitor	4
2.2 Door Station	4
3 Wiring	6
3.1 Preparations	6
3.1.1 Port Connection Rules	6
3.1.2 Cord Specification	7
3.2 Wiring One Door Station and One Indoor Monitor	7
3.3 Wiring Three Door Stations and One Indoor Monitor	8
3.4 Wiring Two Door Stations and Three Indoor Monitors	9
4 Menu Operations	10
Appendix 1 Cybersecurity Recommendations	11

1 Structure

1.1 Introduction

The analog 4-wire video intercom consists of a door station and an indoor monitor. It is applicable to buildings, such as residential buildings, for people to do voice and video calls. The door station is installed outdoors and indoor monitor is installed indoors.

1.2 Features

Indoor Monitor

- Real-time video/voice communication
- Can be connected to three door stations
- Can be connected to cameras (CVBS)
- Plug-and-play

Door Station

- Real-time voice communication
- Self-adaptive IR illumination
- Built-in camera (720 × 576@50I)

1.3 Front Panel

Figure 1-1 Front panel

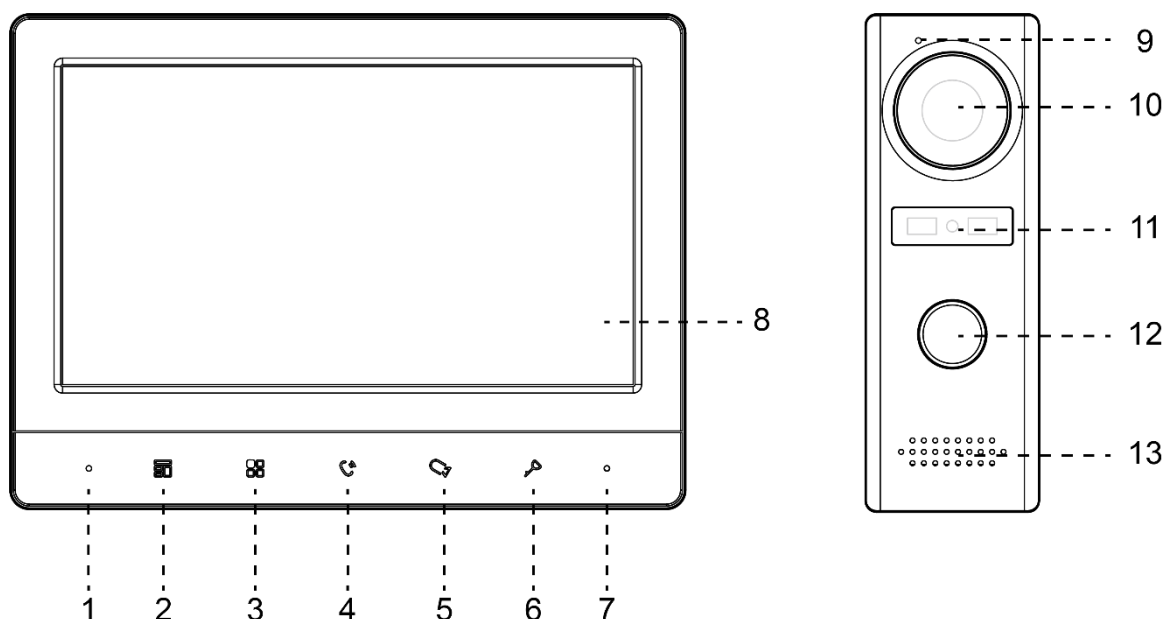







Table 1-1 Front panel

No.	Icon	Description
1	–	Microphone.
2		Press to hang up the incoming call.
3		Bring up the menu.
4		When someone is calling from the door station: <ul style="list-style-type: none"> ● Press once to do voice communication with the person. ● Press twice quickly to hang up.
5		<ul style="list-style-type: none"> ● When someone is calling from the door station, press to do voice communication with the person. ● When no one is calling, press once, twice, three times and four times to view live video of: door station 1, door station 2, analog camera 1 and analog camera 2 respectively.
6		When someone is calling, press to open the door where the door station is installed.
7	–	Power indicator.
8	–	LCD screen.
9	–	Microphone.
10	–	Built-in camera.
11	–	Power indicator.
12	–	Call button. <ul style="list-style-type: none"> ● Press once to call indoor monitor. ● Press and hold for 10 seconds to change the bell type of the door station. The power indicator will flash. ● Press and hold for 15 seconds to turn up the bell volume of the door station. The power indicator will flash. When the volume reaches maximum, this step will set it to minimum. Repeat this step to set appropriate volume. ● Press and hold for 20 seconds to change to DWDR (digital wide dynamic range)/normal mode of the door station. The power indicator will flash.
13	–	Speaker.

1.4 Rear Panel

Figure 1-2 Rear panel

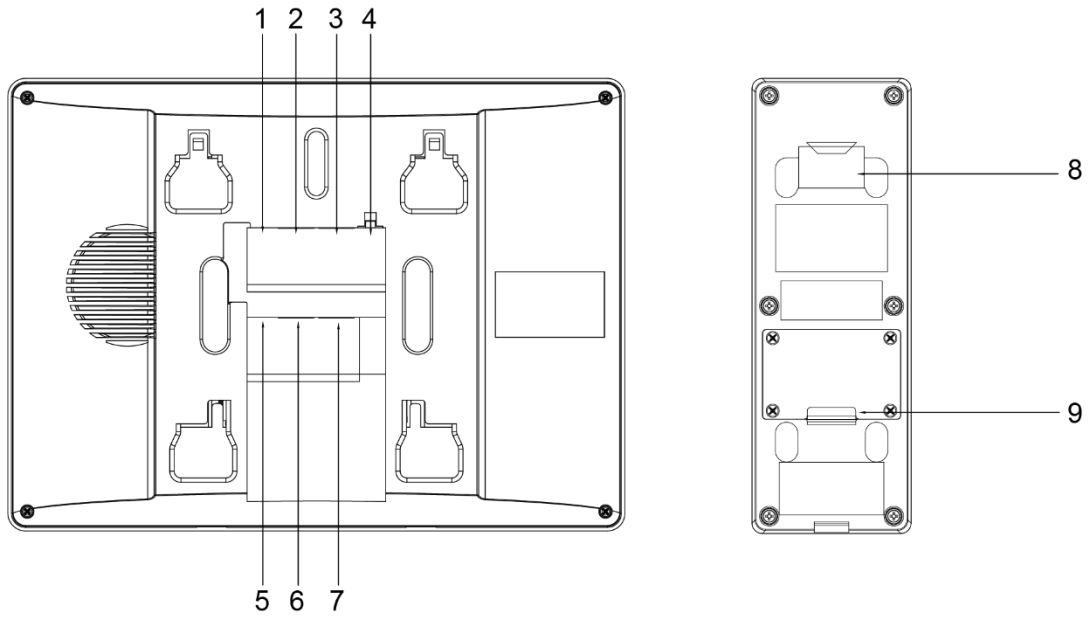


Table 1-2 Rear panel

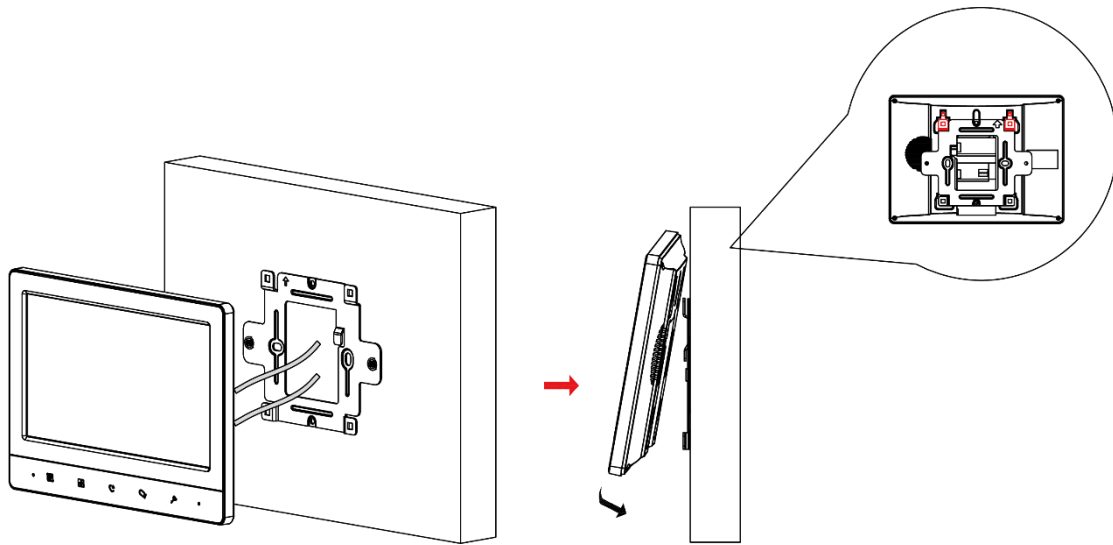
No.	Description	No.	Description
1	Analog camera port 1.	6	VTH cascading port 1.
2	VTO port 1.	7	VTH cascading port 2.
3	VTO port 2.	8	VTO hanging slot.
4	Power input.	9	Wires.
5	Analog camera port 2.	—	—

2 Installation

2.1 Indoor Monitor

Fix the bracket on the wall by screws, hang the indoor monitor on the bracket, and then apply silicone sealant to the gap between the device and the wall.

Figure 2-1 Indoor monitor installation



2.2 Door Station

Install the door station bracket on the wall, and then hang the door station on the bracket; or install the door station cover on the wall, and then hang the door station on the cover. Finally, apply silicone sealant to the gap between the device and the wall.

Figure 2-2 Door station installation

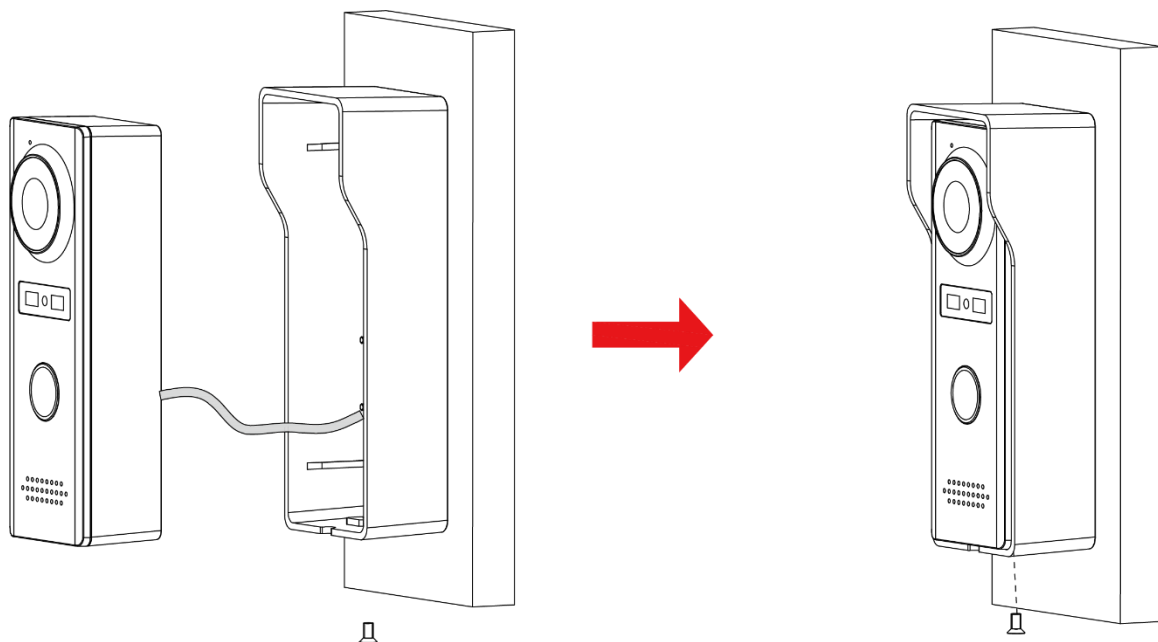
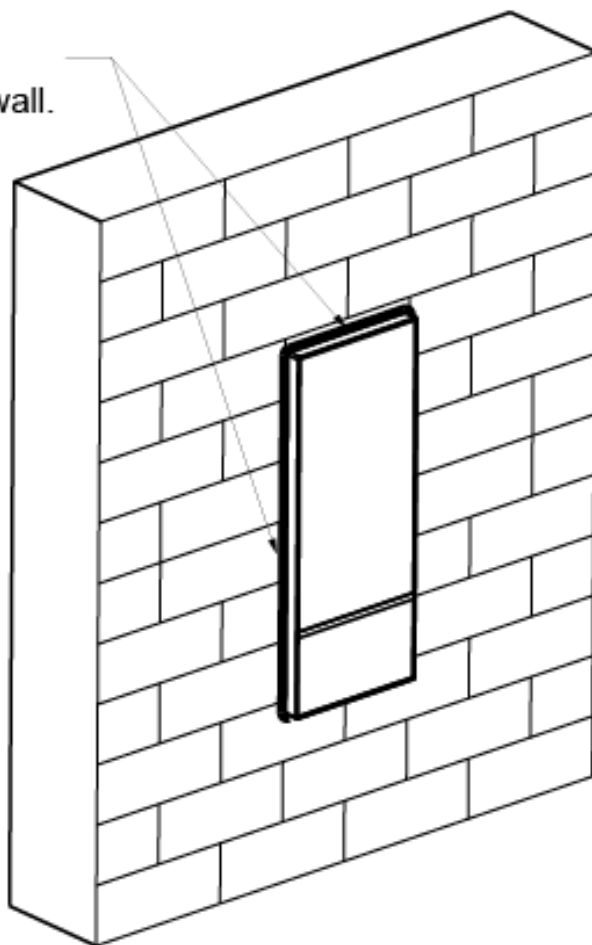


Figure 2-3 Apply silicone sealant to the gap between the device and the wall

Apply silicone sealant to gaps between the device and the wall.



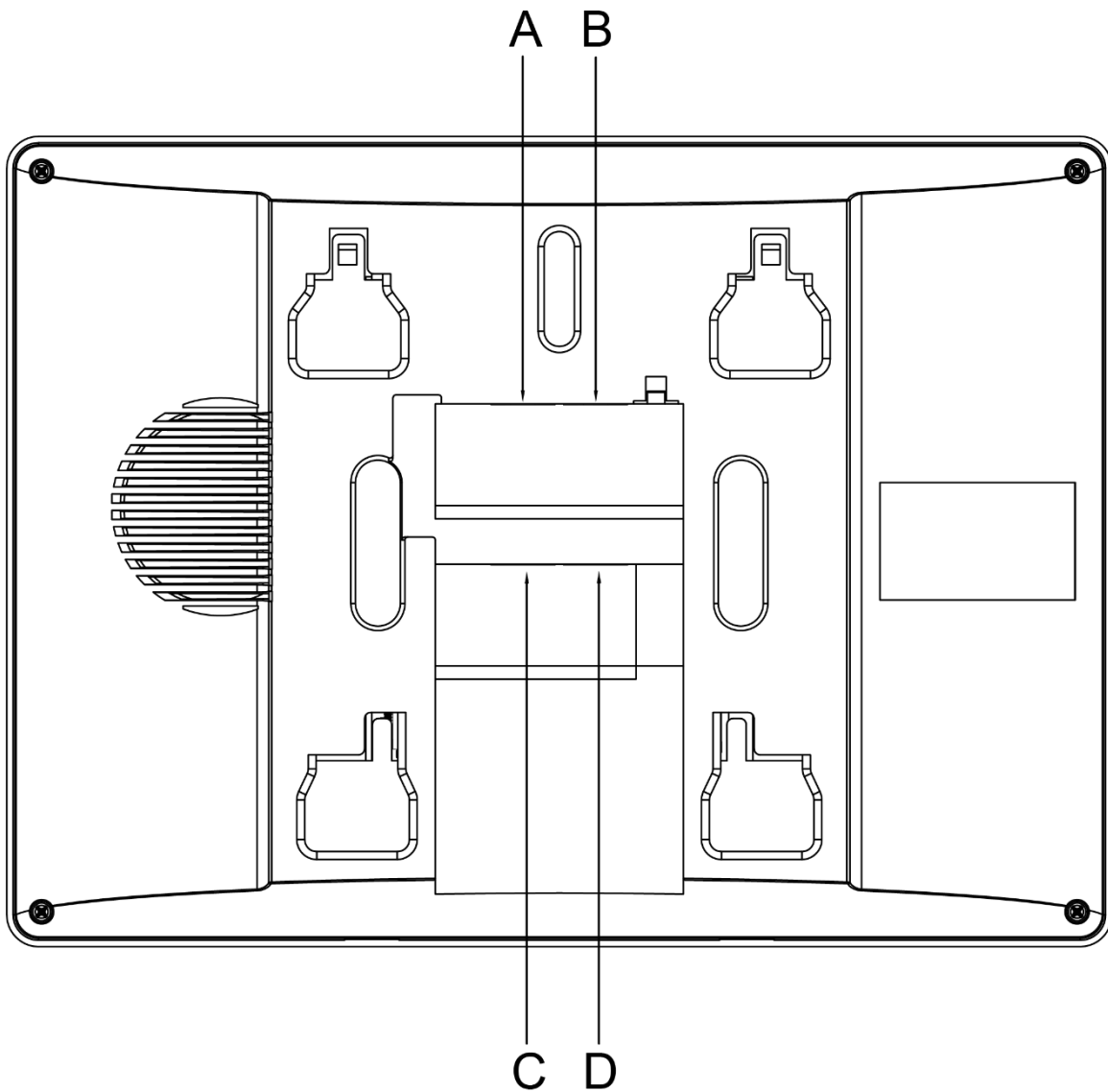
3 Wiring

At most 2 door stations and 3 indoor monitors can be wired in one communication system.

3.1 Preparations

3.1.1 Port Connection Rules

Figure 3-1 Port connection rules



- Port A of an indoor monitor can be connected to Port C of another indoor monitor to do data communication.
- Port B of an indoor monitor can be connected to Port D of another indoor monitor to do data communication.
- Port A of an indoor monitor cannot be connected to Port B or D of another indoor monitor to do data communication.

- Port C of an indoor monitor cannot be connected to Port B or D of another indoor monitor to do data communication.

3.1.2 Cord Specification

Depending on the distance between the door station and indoor monitor, you need to select RVV4 cords of different specifications.

Table 3-1 Cord specification

Transmission Distance (TD)	RVV4 Cord Specification
TD ≤ 10 m	RVV4 × 0.3 mm ²
10 m < TD ≤ 30 m	RVV4 × 0.5 mm ²
30 m < TD ≤ 50 m	RVV4 × 0.75 mm ²



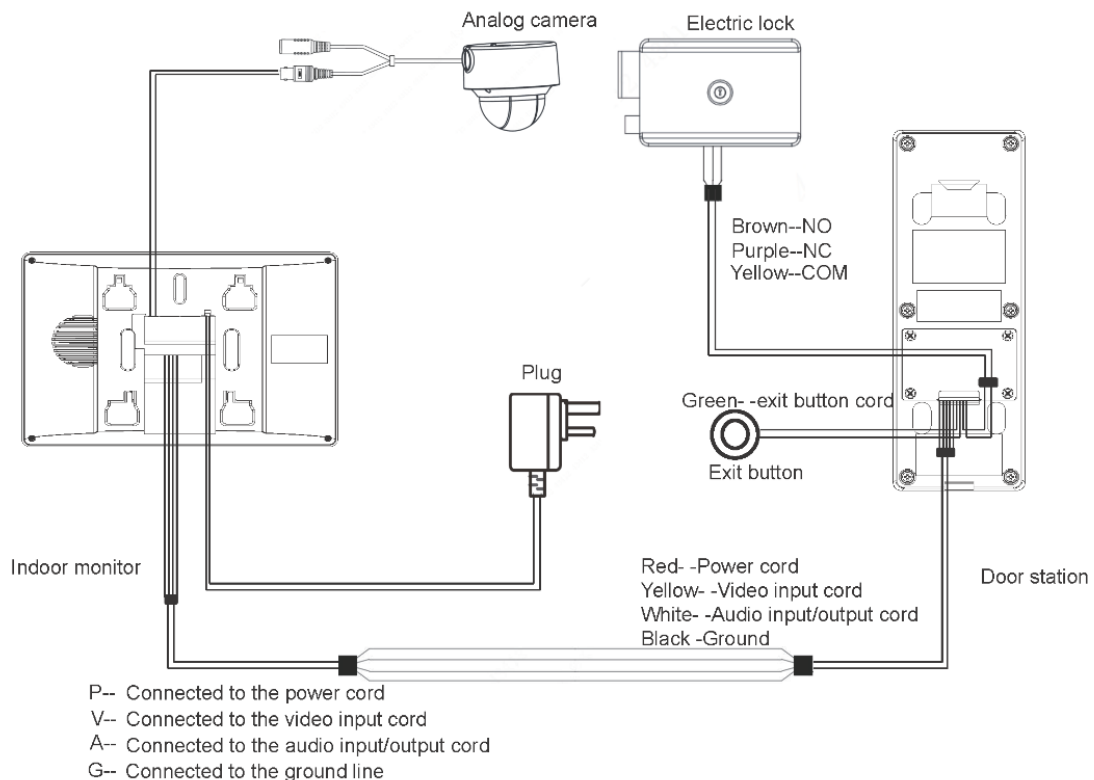
If the distance between the door station and indoor monitor is more than 50 m, please use coaxial cables.



- Do not pull the cords violently.
- During wiring, wrap the cord joints with insulated rubber tape to prevent short circuit.

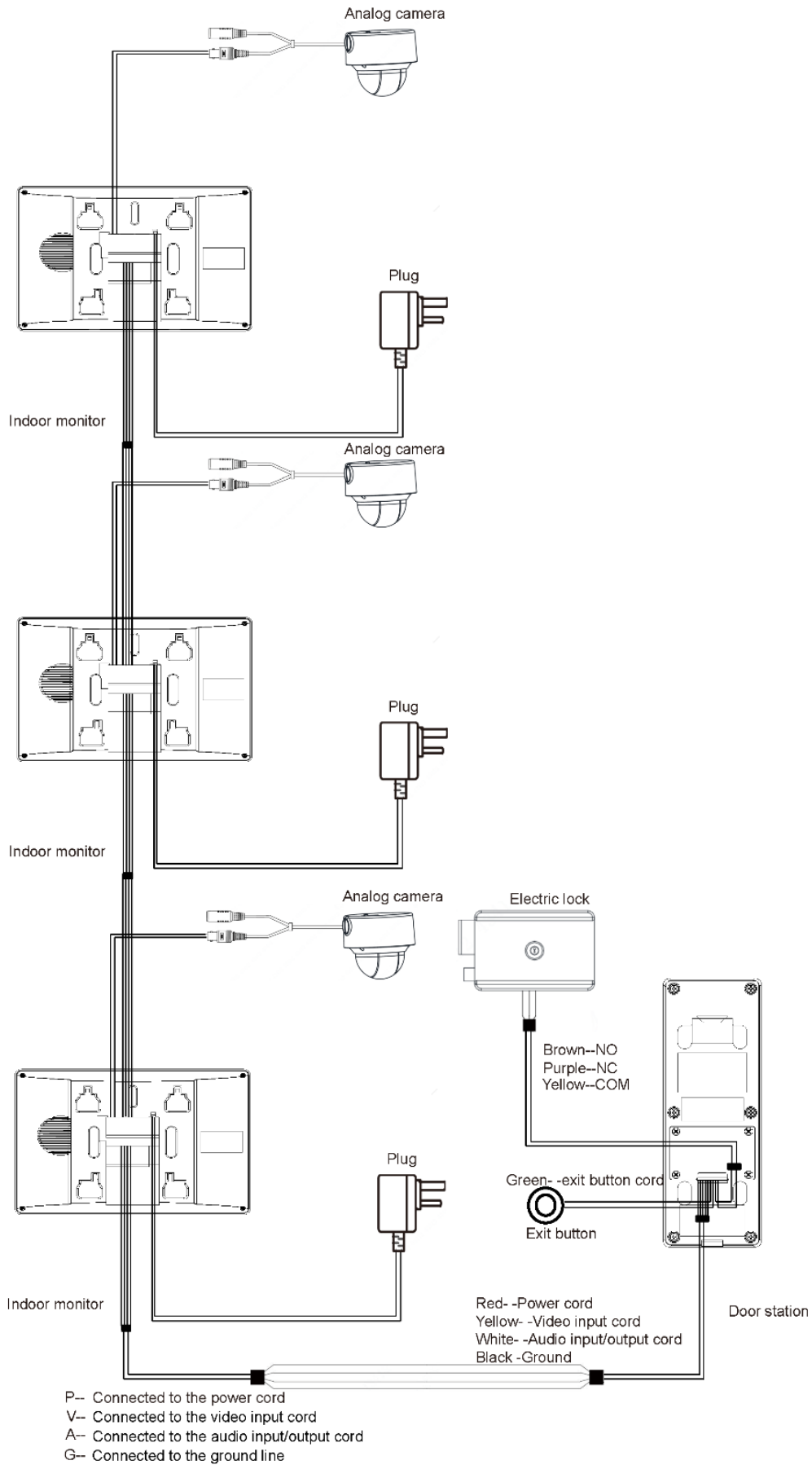
3.2 Wiring One Door Station and One Indoor Monitor

Figure 3-2 Wiring (1)



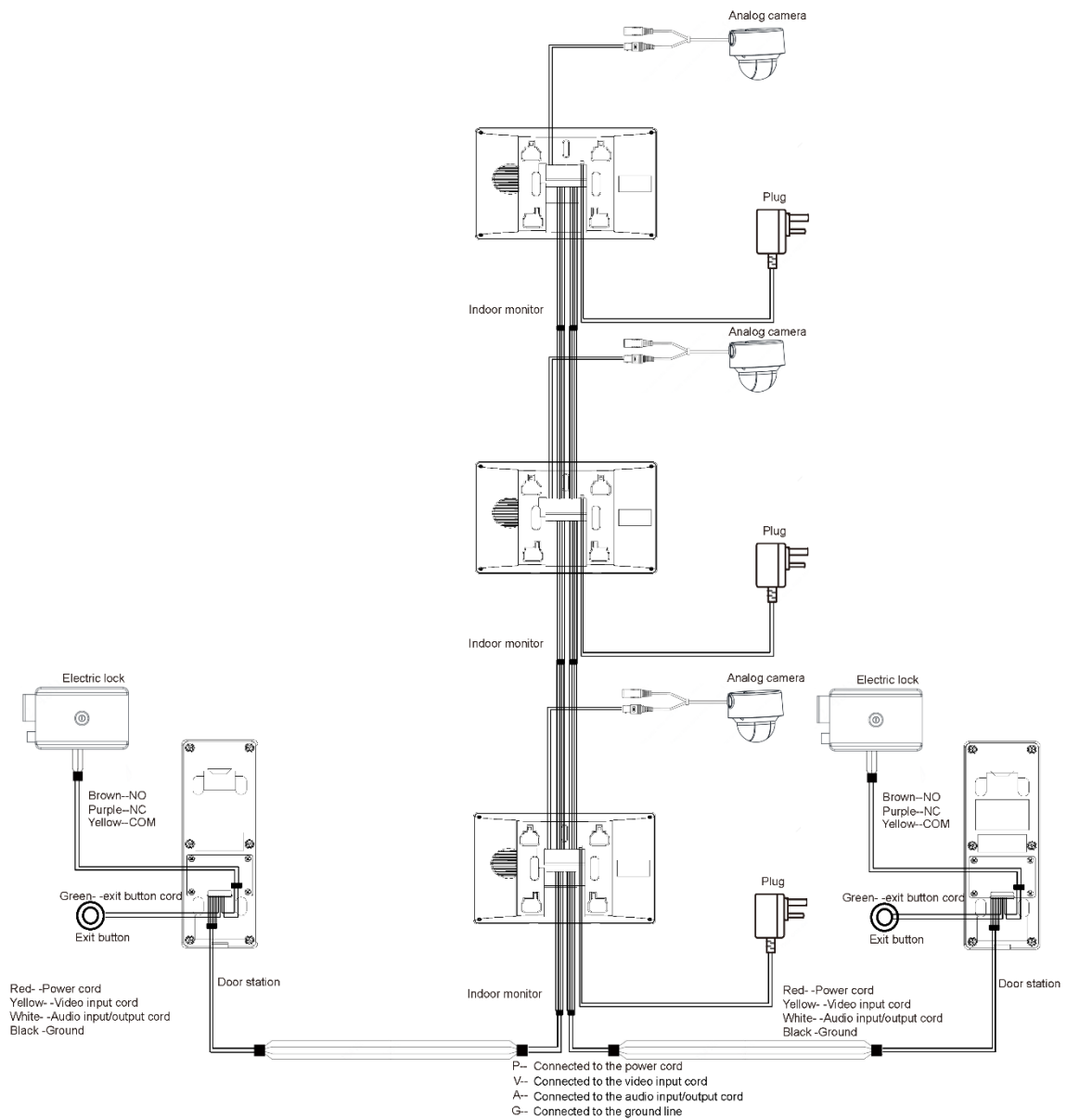
3.3 Wiring Three Door Stations and One Indoor Monitor

Figure 3-3 Wiring (2)



3.4 Wiring Two Door Stations and Three Indoor Monitors

Figure 3-4 Wiring (3)







The recommended analog cameras (CVBS) are HAC 1230 series.

4 Menu Operations

Figure 4-1 Menu



Table 4-1 Menu operations

Icon	Function
	<ul style="list-style-type: none"> Wake up the screen. Turn down Vol (volume), Bright (brightness), Contrast and BellVol (bell volume), change Bell and turn off DND (do not disturb).
	Turn up Vol (volume), Bright (brightness), Contrast and BellVol (bell volume), change Bell and turn off DND (do not disturb).
	Select an item to adjust or change.
	Exit the menu and lock the screen.

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.