

2-Wire Door Station

User Manual



V1.0.6

Foreword

General

This manual introduces the structure, functions and networking of the EACH door station (hereinafter referred to as "the VTO"). 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.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.6	Revised network diagram.	December 2025
V1.0.5	Added induction loop.	June 2025
V1.0.4	Updated the important safeguard and warnings.	March 2025
V1.0.3	Revised the network diagram.	February 2025
V1.0.2	- Revised the network diagram. - Revised DIP configuration.	December 2024
V1.0.1	Revised network diagram.	September 2024
V1.0.0	First release.	July 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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 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 Safeguard 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.

Installation Requirements



- Do not connect the power adapter to the device while the adapter is powered on.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Please follow the electrical requirements to power the device.
 - ◇ Following are the requirements for selecting a power adapter.
 - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
 - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
 - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
 - ◇ We recommend using the power adapter provided with the device.
 - ◇ When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Install the device on a stable surface to prevent it from falling.
- Install the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

Operation Requirements



Battery Pack Precautions

Preventive measures (including but not limited to):

- Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
- Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.

- Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
- Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.



- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Transport, use and store the device under allowed humidity and temperature conditions.
- If the device is powered off for longer than a month, it should be placed in its original package and sealed. Make sure to keep it away from moisture, and store it under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.

Table of Contents

Foreword.....	I
Important Safeguard and Warnings.....	III
1 Product Overview.....	1
1.1 Introduction.....	1
1.2 Function.....	1
2 Network Diagram.....	2
3 Installation.....	6
4 Structure.....	7
4.1 Front Panel.....	7
4.2 Rear Panel.....	8
5 Wiring.....	9
5.1 Wiring for 4103F Model and 4103F-1 Model.....	9
5.2 Wiring for 4103F-I1 Model.....	11
6 Basic DIP Configuration.....	12
6.1 DIP Switch Introduction.....	12
6.2 Configuring VTO ID.....	13
7 Updating the Device.....	16
Appendix 1 Security Recommendation.....	17

1 Product Overview

1.1 Introduction

The 2-wire hybrid VTO uses the metal front panel and supports modular cascading. Using two wires for communication, the VTO supports video intercom with 2-wire hybrid VTH, and supports local lock and external RS-485 lock; it also supports call alarm and message notification on DMSS app.

1.2 Function

2-Wire Communication

Supports 2-wire communication.

Video/Voice Call

Make video or voice call to VTHs.

Monitoring

Videos can be monitored by VTH or DMSS app users.

Auto IR Illumination

Supports auto IR illumination at night.

Unlock

There are 5 unlock methods: IC card, ID card, password, fingerprint and remote unlock.



Unlock methods of IC card, ID card, fingerprint and password are available when the device is connected to the corresponding modules.

Induction Loop

Devices with  support the induction loop function.

2 Network Diagram



When multiple indoor monitors are connected in the cascade mode to the port on the branch terminal, to reduce signal reflection, the 14th DIP switch of the farthest indoor monitor from the port needs to be turned on.

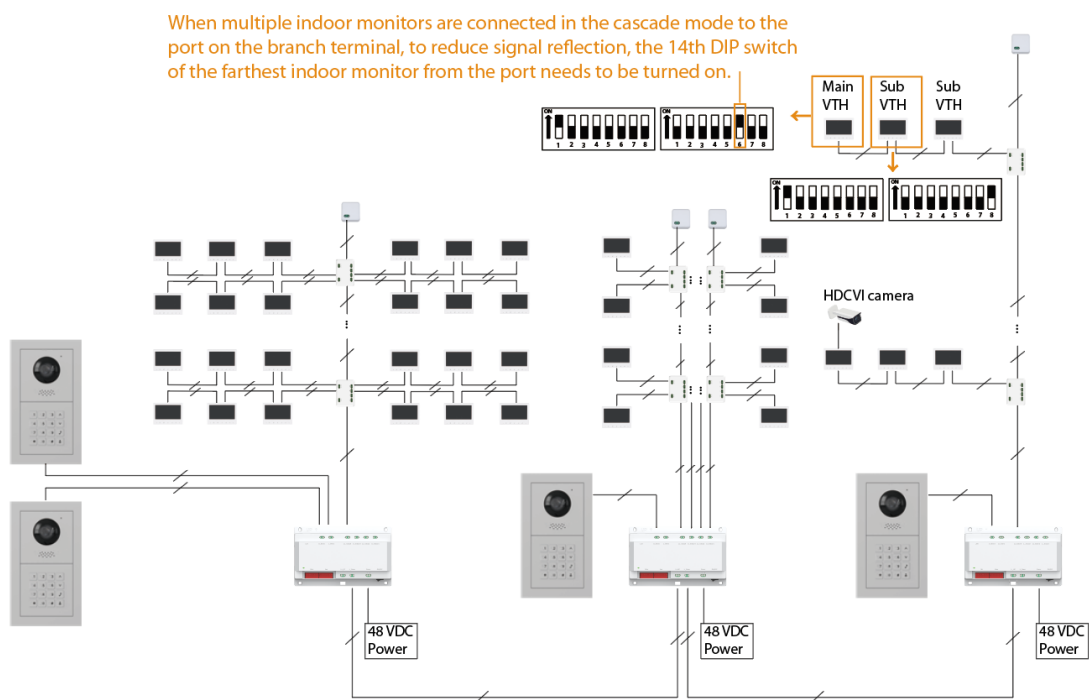
Refer to the following image to configure the DIP switch of the device in the cascade. The DIP switch of ID should be configured according to the actual situation.



- The power supply of HDCVI camera cannot be grounded.
- The product appearance is for reference only.

Network Diagram

Figure 2-1 Network diagram

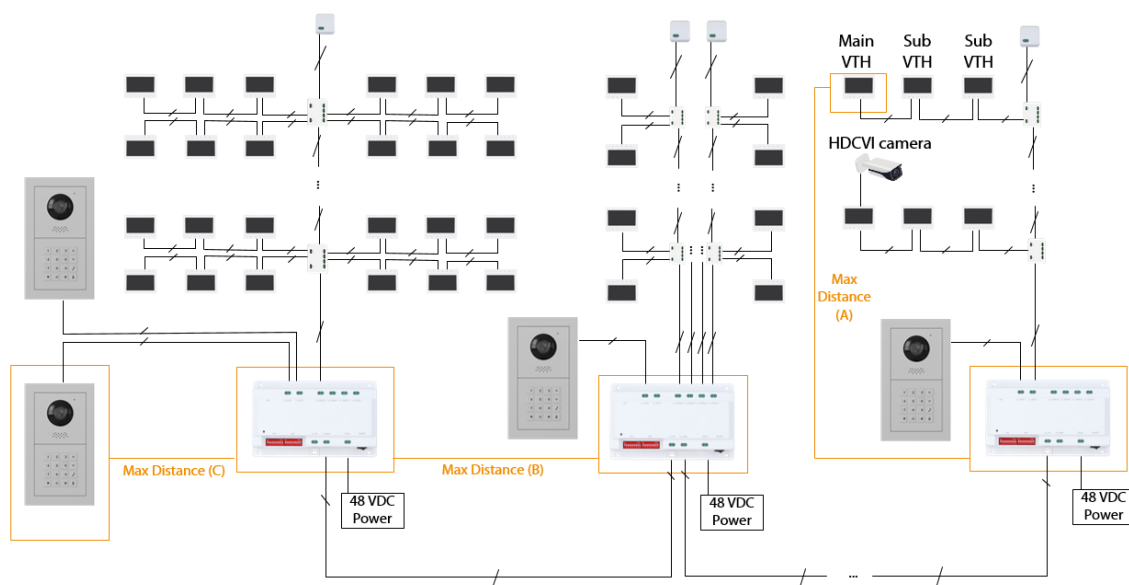


Wiring Distance between the Controller, VTH and the VTO



- Max distance (A) refers to the distance between the 2-wire controller and the VTH. $A \leq 100$ m.
- Max distance (B) refers to the distance between the cascading 2-wire controllers. $B \leq 100$ m.
- Max distance (C) refers to the distance between the 2-wire controller and the VTO. $C \leq 100$ m.
- The number of cascading controllers must be less than or equal to 10.
- For systems with multiple VTHs in a cascade, the number of devices must be less than or equal to 10 in each branch.

Figure 2-2 Max distance



Network capacity for VTH

The capacity for the VTH indicates the maximum number of VTHs that can be connected to one indoor monitor port on the 2-wire controller.

Each controller can connect up to 22 VTHs with Wi-Fi function or up to 100 VTHs without Wi-Fi function.



- The 2-wire VTHs with the Wi-Fi function can work at the same time. The number of 2-wire VTHs without the Wi-Fi function that work at the same time is 5% of the maximum capacity according to different cable specifications and distances.
- The capacity values are based on the default settings for voice and screen brightness, and standard cables that are mentioned in the following table.
- In the network, if you want to replace the VTH with Wi-Fi function to the VTH without Wi-Fi function, the conversion ratio is 1:8.

For example, if you want to reduce 1 VTH with Wi-Fi function in the network, you can connect to 8 VTHs without Wi-Fi function.

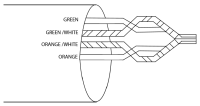


The maximum number of VTHs with Wi-Fi function cannot exceed 22.

The maximum number of VTHs without Wi-Fi function cannot exceed 100.

Table 2-1 Network capacity for VTH (240 W power supply as an example)

Cable Type	Cable Specification	AWG	Device Type	A=0–25 m	A=26–50 m	A=51–75 m	A=76–100 m
Regular cable	RVV 2 × 1.5 mm ² (Recommend)	AWG 15	With Wi-Fi	22	22	22	17
			Without Wi-Fi	100	100	100	100
	RVV 2 × 1 mm ²	AWG 17	With Wi-Fi	22	22	18	13

Cable Type	Cable Specification	AWG	Device Type	A=0–25 m	A=26–50 m	A=51–75 m	A=76–100 m
	RVV 2 × 0.5 mm ²	AWG 20	Without Wi-Fi	100	100	100	100
			With Wi-Fi	22	17	11	8
			Without Wi-Fi	100	100	91	68
	Cat5e Double Pair	AWG 24	With Wi-Fi	22	14	9	7
Network cable  Connect the cables according to the cable color.			Without Wi-Fi	100	100	75	56
	Cat5e Single Pair	AWG 24	With Wi-Fi	14	7	4	3
			Without Wi-Fi	100	56	37	28

Network capacity for 2-wire controller

The capacity for the 2-wire controller indicates the maximum number of controllers that can be connected to one corresponding port on the controller.



The capacity values are based on standard cables that are mentioned in the following table.

Table 2-2 Network capacity for the controller

Cable Type	Cable Specification	AWG	B=0–100 m
Regular cable	RVV 2 × 1.5 mm ²	AWG 15	8
	RVV 2 × 1 mm ²	AWG 17	10
	RVV 2 × 0.5 mm ² (Recommend)	AWG 20	10
Network cable	Double-pair network cable	AWG 24	10
	Single-pair network cable	AWG 24	10

Network capacity for VTO

The capacity for the VTO indicates the maximum number of VTOs that can be connected to one 2-wire controller.

Up to 2 VTOs can be connected to one 2-wire controller.



The capacity values are based on standard cables that are mentioned in the following table.

Table 2-3 Network capacity for the VTO

Cable Type	Cable Specification	AWG	C=0–25 m	C=26–50 m	C=51–75 m	C=76–100 m
Regular cable	RVV 2 × 1.5 mm ² (Recommend)	AWG 15	2	2	2	2
	RVV 2 × 1 mm ²	AWG 17	2	2	2	2
	RVV 2 × 0.5 mm ²	AWG 20	2	2	2	2
Network cable	Double-pair network cable	AWG 24	2	2	2	2
	Single-pair network cable	AWG 24	2	2	1	1

3 Installation

- Do not expose the VTO to condensation, high temperature, direct sunlight, stain, dust, and chemically corrosive substances.
- Installation should be done by professional teams. Do not dismantle or repair the VTO by yourself in case of device failure. Contact after-sales service if you need any help.
- Prepare cross screwdrivers and gloves yourself.
- The recommended installation height of the VTO should be no more than 2 m from the ground.

4 Structure

4.1 Front Panel

Figure 4-1 Front panel

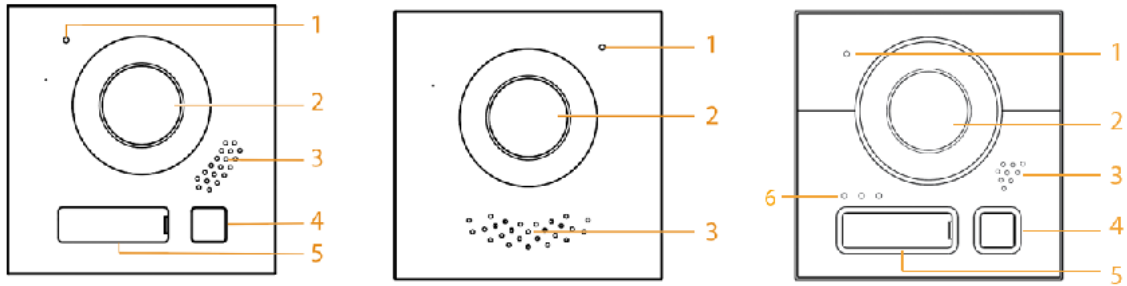


Table 4-1 Front panel description

No.	Name	Description
1	Microphone	Audio input.
2	Camera	Capture images or record videos for the VTO.
3	Speaker	Audio output.
4	Call button	Call button.
5	Nameplate	Displays the custom information.
6	Indicators	Displays status on calling, talking and unlock.



Devices with  on the upper-right corner support the induction loop function.

4.2 Rear Panel

Figure 4-2 Rear panel

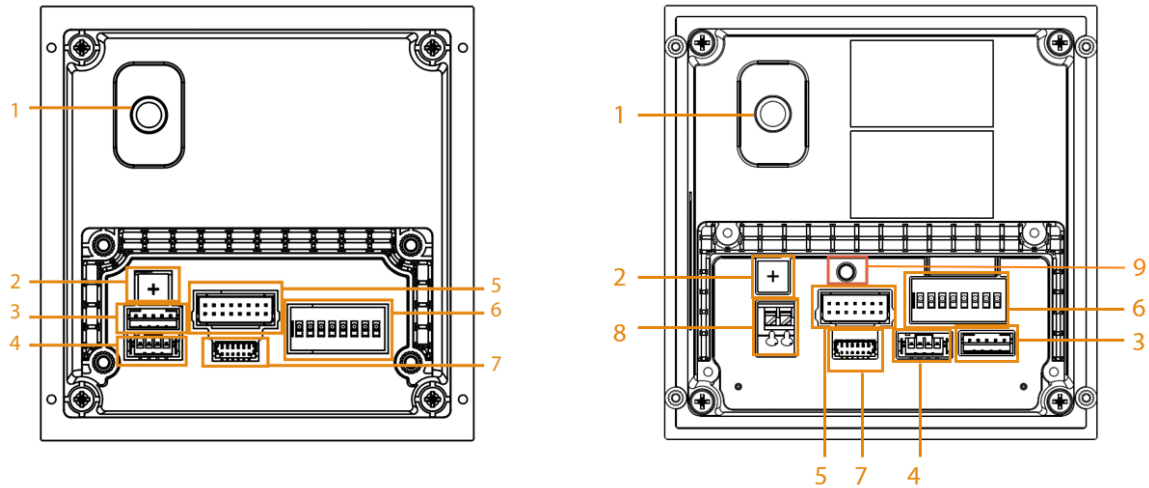


Table 4-2 Rear panel description

No.	Description
1	Tamper button.
2	Volume adjusting button. Use the screwdriver to adjust the volume of the talk. Rotate the button clockwise to turn down the volume.
3	Debug port.
4	Connect to other modules.
5	Functional port.
6	DIP switch.
7	Debug port.
8	2-wire port.
9	Reset button. Press the button for 8 seconds to reset the Device.

5 Wiring

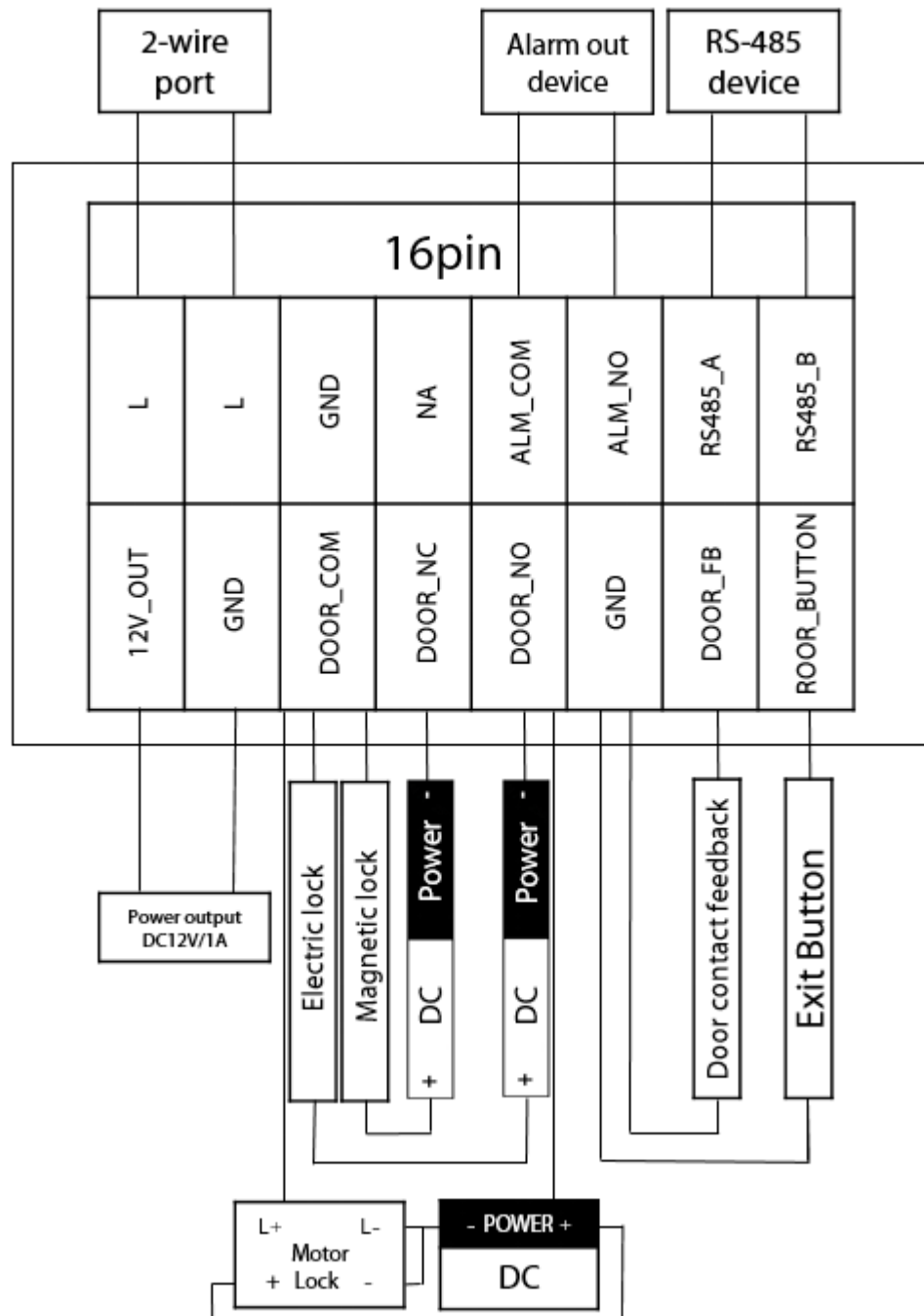
5.1 Wiring for 4103F Model and 4103F-1 Model

The wiring for 4103F model and 4103F-1 model is as follows.



The alarm input port is connected as dry contact.

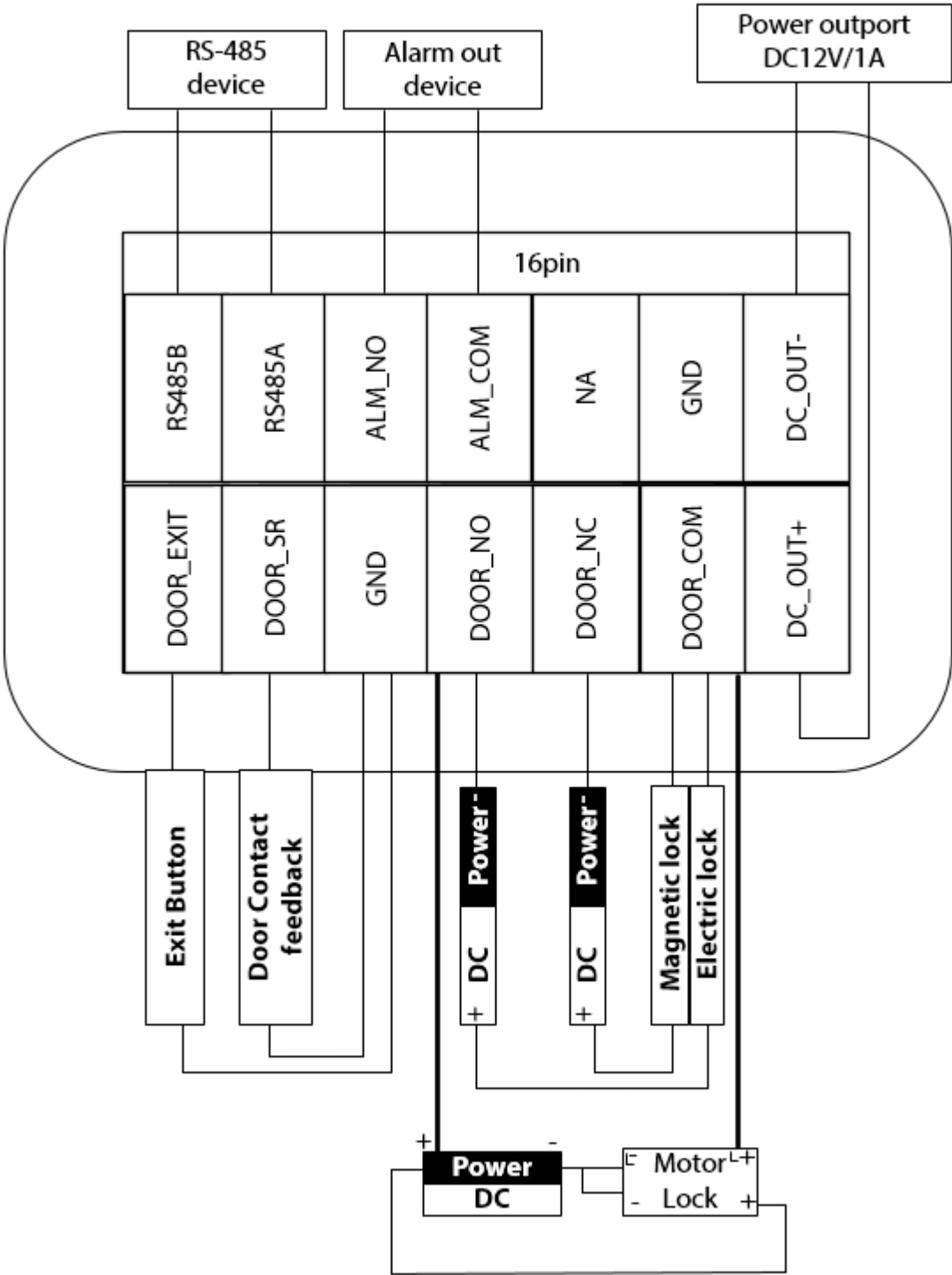
Figure 5-1 Wiring



5.2 Wiring for 4103F-I1 Model

The wiring for 4103F-I1 model is as follows.

Figure 5-2 Wiring



6 Basic DIP Configuration

Configure the DIP switches to achieve the function you would like to program, which includes:

- Configure the address of the VTO.
- Configure the connection mode.

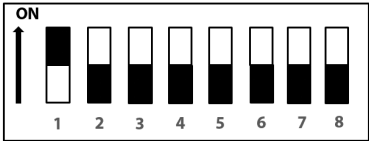
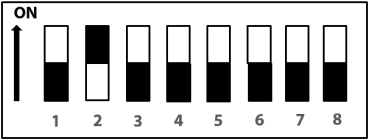
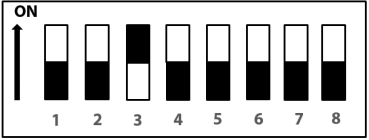
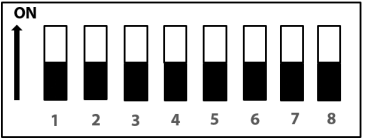
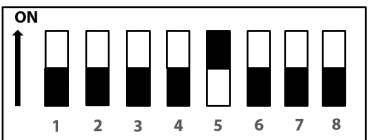


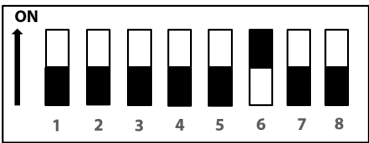
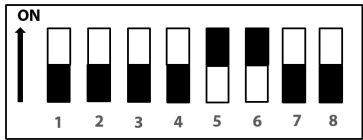
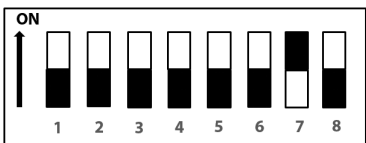
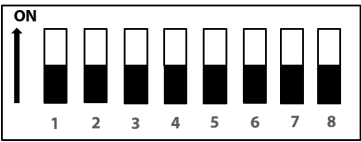
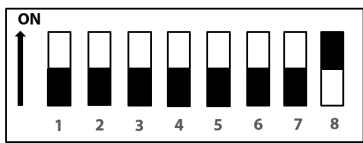
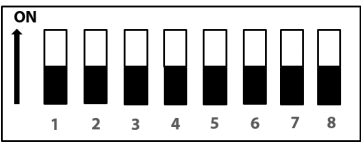
Move the actuator completely to the top or bottom position. If the actuator is in the middle position, it is considered to be in the top position.

6.1 DIP Switch Introduction

On the Dip-switch, set the code corresponding to the function you want to program as shown in the table below.

Table 6-1 DIP Switch mapping relations and function

DIP Switch No.		Corresponding Function	Description
DIP 1		VTO Address 1	Address DIP configuration. Supports programing a maximum of 14 VTO addresses.
DIP 2		VTO Address 2	
DIP 3		VTO Address 4	
DIP 4		VTO Address 8	
DIP 5		Lock-release activation time: 2 Sec	Lock-release activation time
		Lock-release activation time: 4 Sec	

DIP Switch No.		Corresponding Function	Description
DIP 6		lock-release activation time: 6 Sec	
		Lock-release activation time: 8 Sec	
DIP 7		ON: NTSC  Mainly used in the U.S., Canada and Japan.	Television signal coding system 
		OFF: PAL  Mainly used in Germany, Britain, China and Spain.	In a networking system, this parameter must be configured to the same status for all the VTOs.
DIP 8		ON: LED lighting of nameplate panel turned on.	LED lighting of nameplate panel 
		OFF: LED lighting of nameplate panel turned off.	If it cannot be configured, update the module program to the latest.

6.2 Configuring VTO ID

This section introduces how to configure the ID of a VTO through the coding rules of DIP switches.

Procedure

Step 1 Find the mapping relation between the DIP switch number and the ID number you plan to configure from the table.

It follows a calculation rule that combining only the numbers listed in the **ID No.** only to form a new ID number.

Step 2 Manually move the actuator(s) corresponding to the DIP switch(s) to the status **ON**, so that the ID of the VTO can be configured.

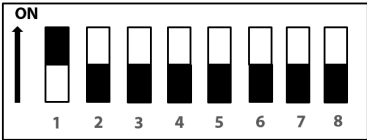
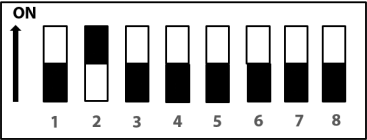
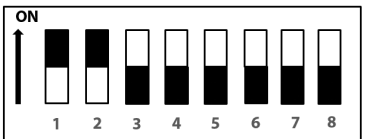
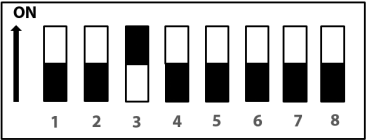
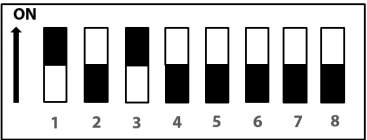
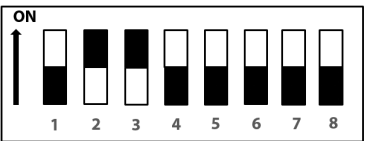
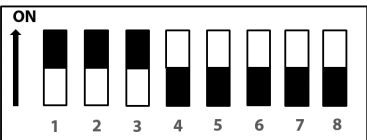
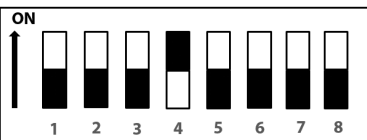
For example, if you want to set your VTO ID as 4, you need to first find the mapping relation (DIP 3 equals to the ID number of 4) in the table, and then manually move the actuator of the DIP 3 to the status **ON**. If you want to set your VTO ID as 3, you need to do the calculation (1+2=3; which equals to the value of DIP1 and DIP 2 combined together in

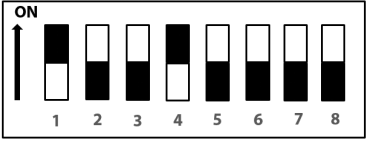
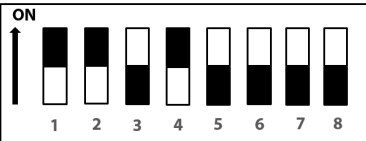
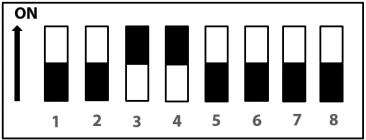
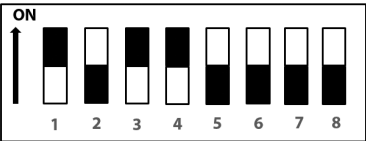
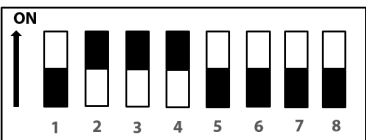
the mapping relation), and manually move both the actuator of DIP 1 and DIP 2 to the status **ON**.



Here is the list of commonly used VTO ID (1-14) and their corresponding DIP switch number combinations.

Table 6-2 Common VTO ID (1-14) and DIP switch numbers

VTO ID	DIP Switch Combination	Coding Rule
1		DIP 1
2		DIP 2
3		DIP 2+ DIP 1
4		DIP 3
5		DIP 3 + DIP 1
6		DIP 2 + DIP 3
7		DIP 3 + DIP 2 + DIP 1
8		DIP 4

VTO ID	DIP Switch Combination	Coding Rule
9		DIP 4 + DIP 1
10		DIP 4 + DIP 2
11		DIP 4 + DIP 2+ DIP 1
12		DIP 4 + DIP 3
13		DIP 4 + DIP 3+ DIP 1
14		DIP 4 + DIP 3+ DIP 2

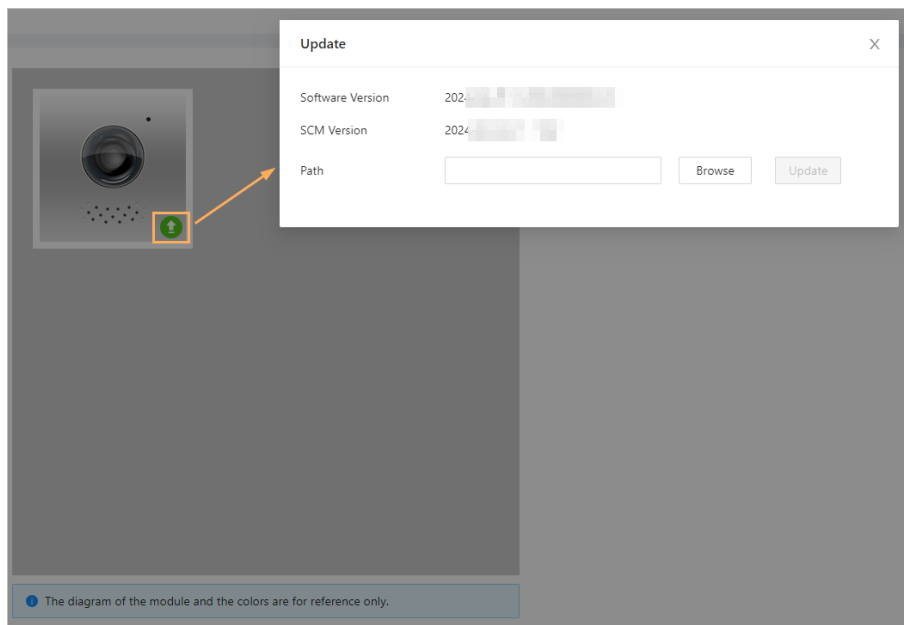
7 Updating the Device

The Device can be updated on the webpage of the 2-wire controller after it is connected to the 2-wire controller.

Procedure

- Step 1 Log in to the webpage of the 2-wire controller.
- Step 2 Click **Config** next to the corresponding VTO.
- Step 3 Select **Module**.
- View the VTO and all the cascading modules.
 - Click  to view the current version information.
 - Click **Browse** to select the update file, and then click **Update**.

Figure 7-1 Module



Appendix 1 Security Recommendation

Account Management

1. Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

- SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up complex passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.

4. Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.

2. **MAC address binding**

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).