Two-door Slave Access Controller

User’s Manual

V1.0.1

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

● Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.

● These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system’s credentials. You will need to either update the camera’s firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

● Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
● You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:
Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:
In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:
If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:
● UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
● If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:
Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:
Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:
If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

General

This document elaborates on structure, installation, interface and wiring of two-door slave access controller.

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.

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others' such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

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 regions. For detailed information, see the paper User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's 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, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (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 occurred when using the device.
- If there is any uncertainty or controversy, please refer to our 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 Requirement

- Please don’t place and install the device in an area exposed to direct sunlight or near heat generating device.
- Please don’t install the device in a humid, dusty or fuliginous area.
- Please keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Please don’t drip or splash liquids onto the device; don’t put on the device anything filled with liquids, in order to prevent liquids from flowing into the device.
- Please install the device at well-ventilated places; don’t block its ventilation opening.
- Use the device only within rated input and output range.
- Please don’t dismantle the device arbitrarily.
- Please transport, use and store the device within allowed humidity and temperature range.

Power Requirement

- Please make sure to use batteries according to requirements; otherwise, it may result in fire, explosion or burning risks of batteries!
- To replace batteries, only the same type of batteries can be used!
- The product shall use electric cables (power cables) recommended by this area, which shall be used within its rated specification!
- Please use standard power adapter matched with the device. Otherwise, the user shall undertake resulting personnel injury or device damage.
- Please 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.
- Products with category I structure shall be connected to grid power output socket, which is equipped with protective grounding.
- Appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.

Table of Contents

1 Overview

As a slave controller of access master controller, two-door slave access controller is matched with access master controller and is widely used in banks, prisons and safe places.

Its rich functions are as follows:

- Adopt sliding rail type and lock type installation, convenient installation and maintenance.
- Integrate alarm and fire alarm.
- Support 4 sets of card readers.
- Support 9 groups of signal input (exit button *2, door sensor *2 and intrusion alarm *5).
- Support 5 groups of control output (electric lock *2 and alarm output *3).
- With RS485 port, it may extend to connect lift control module, alarm or household control module.
- Support CAN bus and connect master controller.
- FLASH storage capacity is 16M (which may extend to 32M), max supports 20,000 card holders and 30,000 offline records.
- Support illegal intrusion alarm, exit overtime alarm, duress card alarm and duress code setup. Also support black-white list and patrol card setup.
- Data storage during outage, built-in RTC (support DST), online upgrading.


Caution

If this product needs to connect external power supply, please use 12V 0.5A adapter and ensure that working temperature shall not exceed -5℃～+55℃.

2 Packing List

Before installation, please check according to Table 2-1.

No.	Name	Quantity
1	Access controller	1
2	Installation positioning drawing	1
3	Accessory kit (screw, expansion pipe and wiring terminal)	1
4	Quick start guide	1
5	Certificate of qualification	1

Table 2-1

3 Installation Guide

3.1 System Structure

System structure of two-door slave access controller, door lock and reader is shown in Figure 3-1.

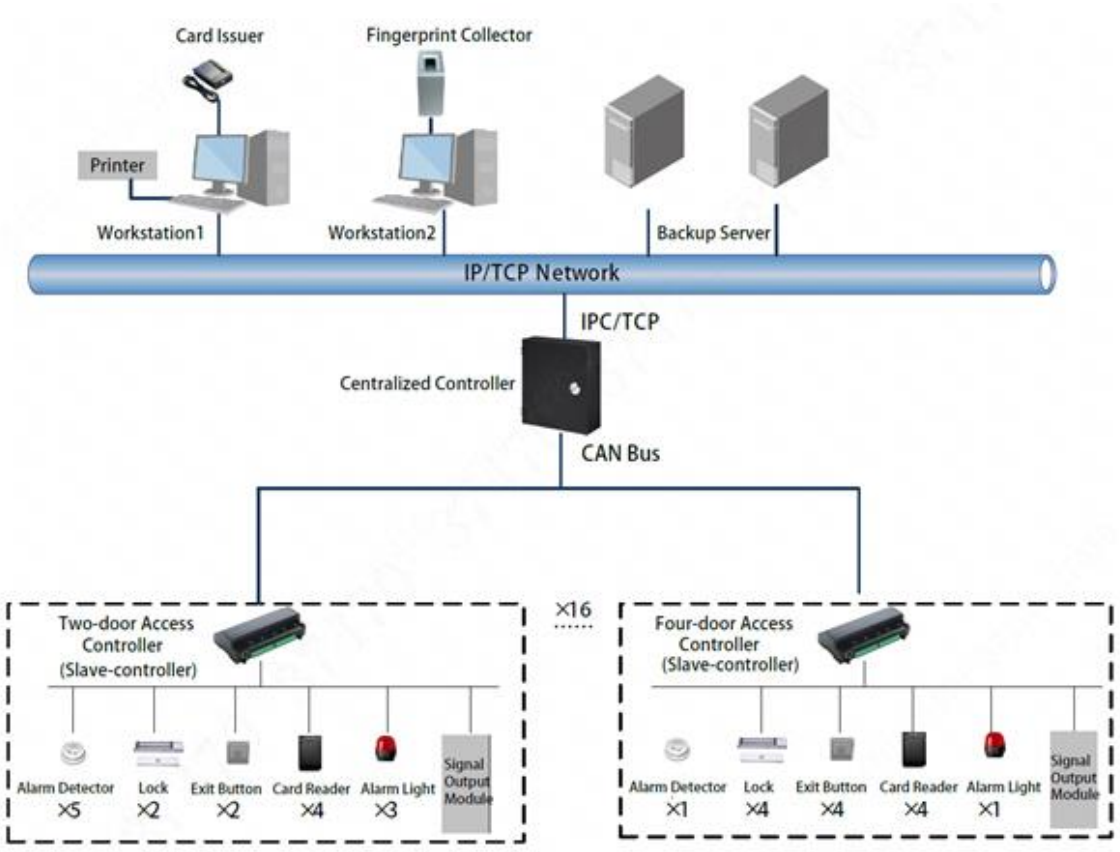


Figure 3-1

3.2 External Dimension

Its appearance and dimension is shown in Figure 3-2 and Figure 3-3. The unit is mm.

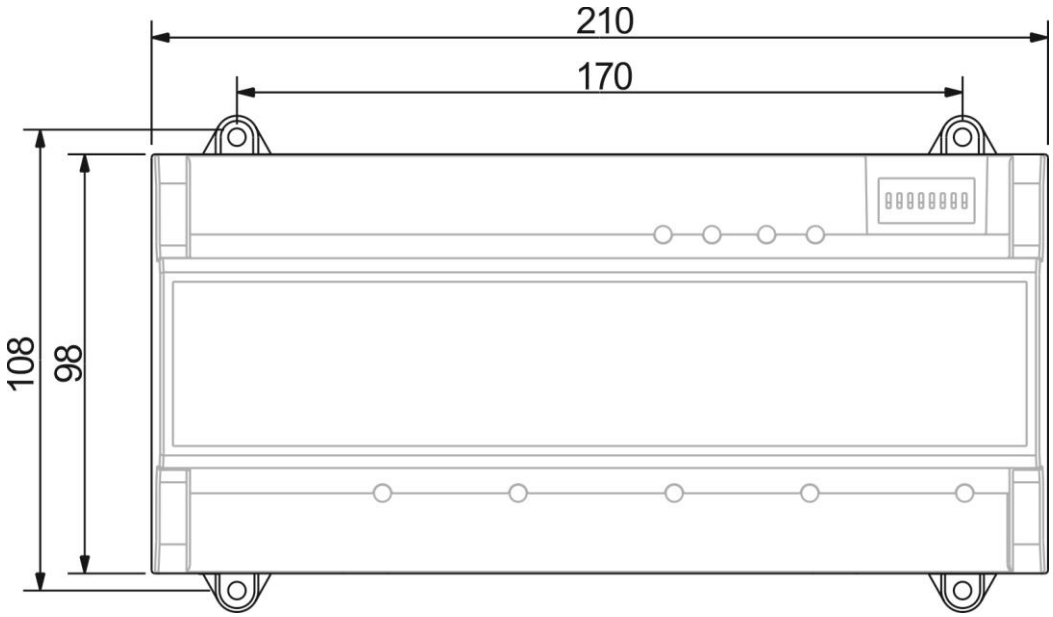


Figure 3-2

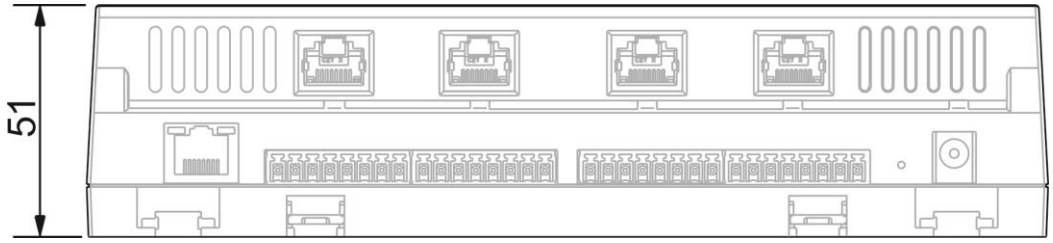


Figure 3-3

3.3 Device Installation

There are two installation modes.

- Mode 1: fix the whole device onto the wall with screws.
- Mode 2: install U-shaped guide rail, and hang the whole device onto the wall (U-shaped guide rail is a self-bought fitting).

Mode 1

Installation diagram is shown in Figure 3-4.

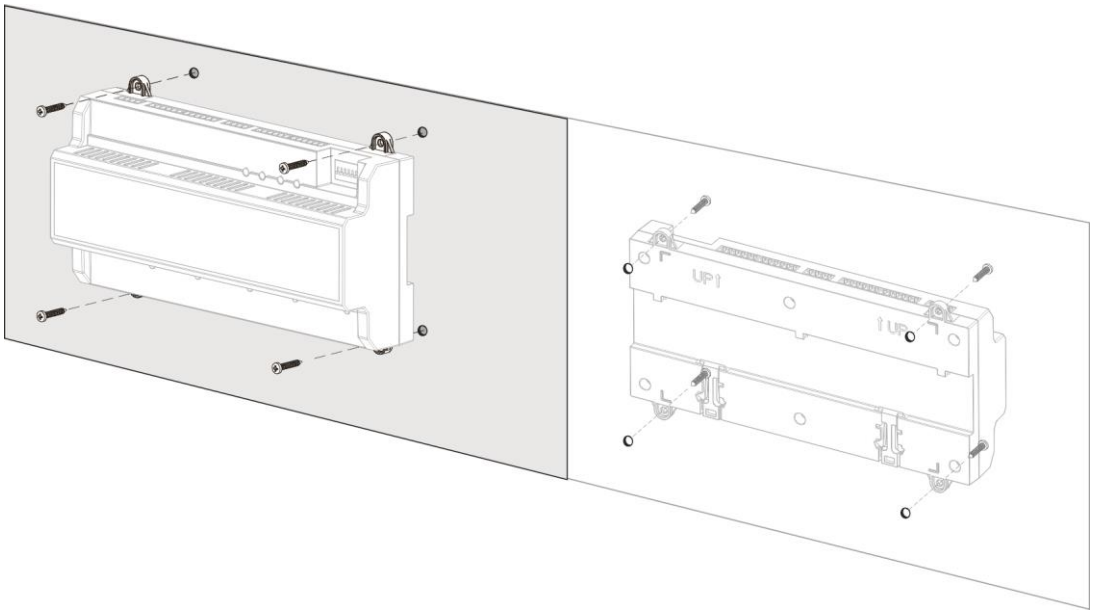


Figure 3-4

Mode 2

Installation diagram is shown in Figure 3-5.

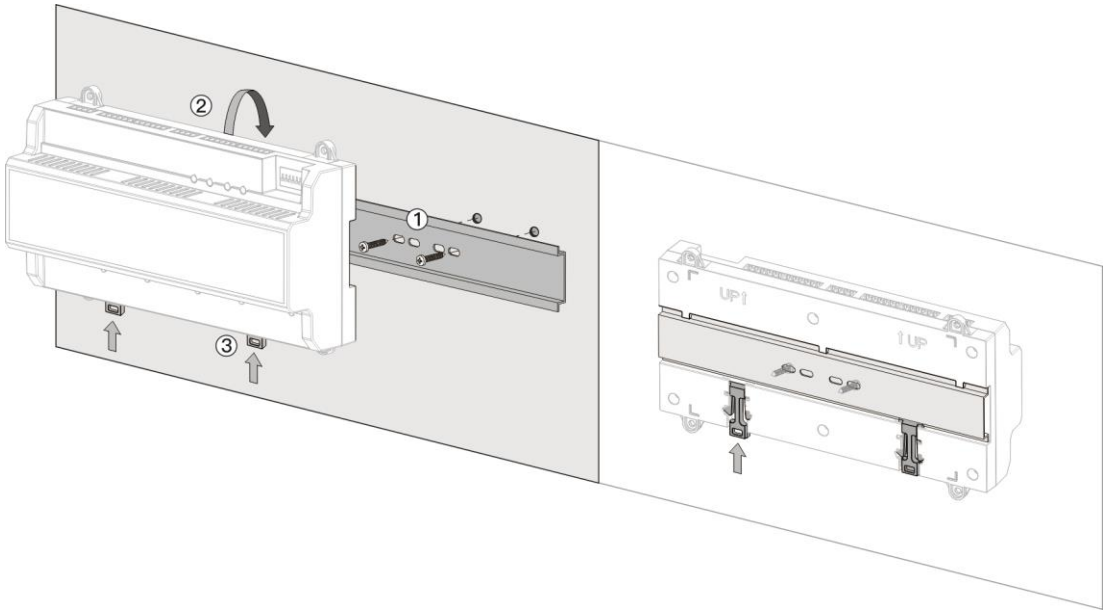


Figure 3-5

Step 1 Fix the U-shaped guide rail onto the wall with screws.

Step 2 Buckle the upper rear part of the device into upper groove of U-shaped guide rail.

Step 3 Push the snap joint at the bottom of the device upwards. The installation is completed when you hear the fitting sound.

3.4 Disassembly

If the device is installed with mode 2, please disassemble it according to Figure 3-6.

Align a screwdriver with the snap joint, press it down and the snap joint will pop up, so the

whole device can be disassembled smoothly.

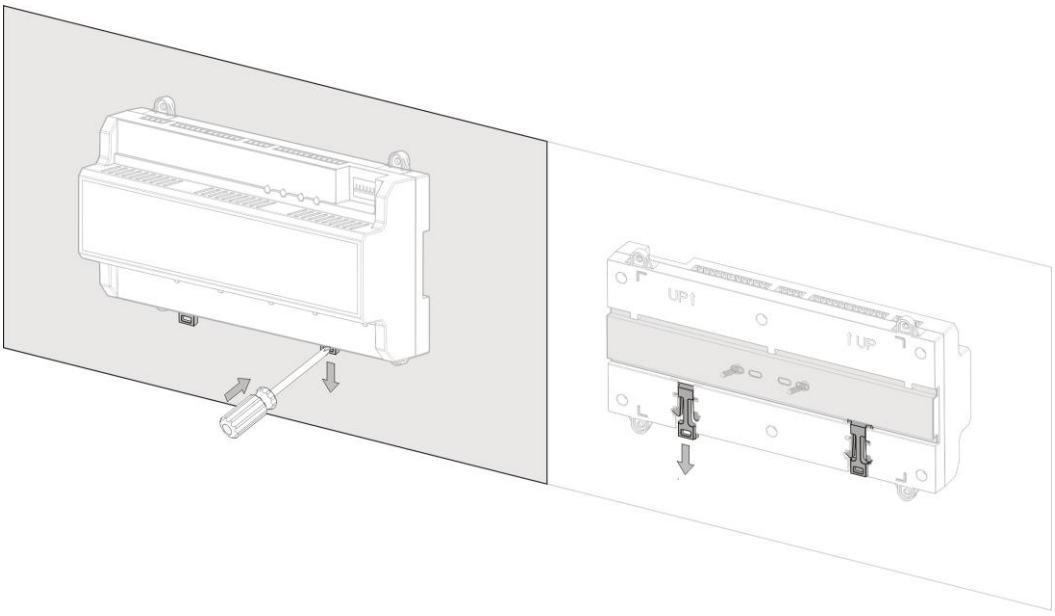


Figure 3-6

3.5 Wiring Description

Device wiring diagram is shown in Figure 3-7.

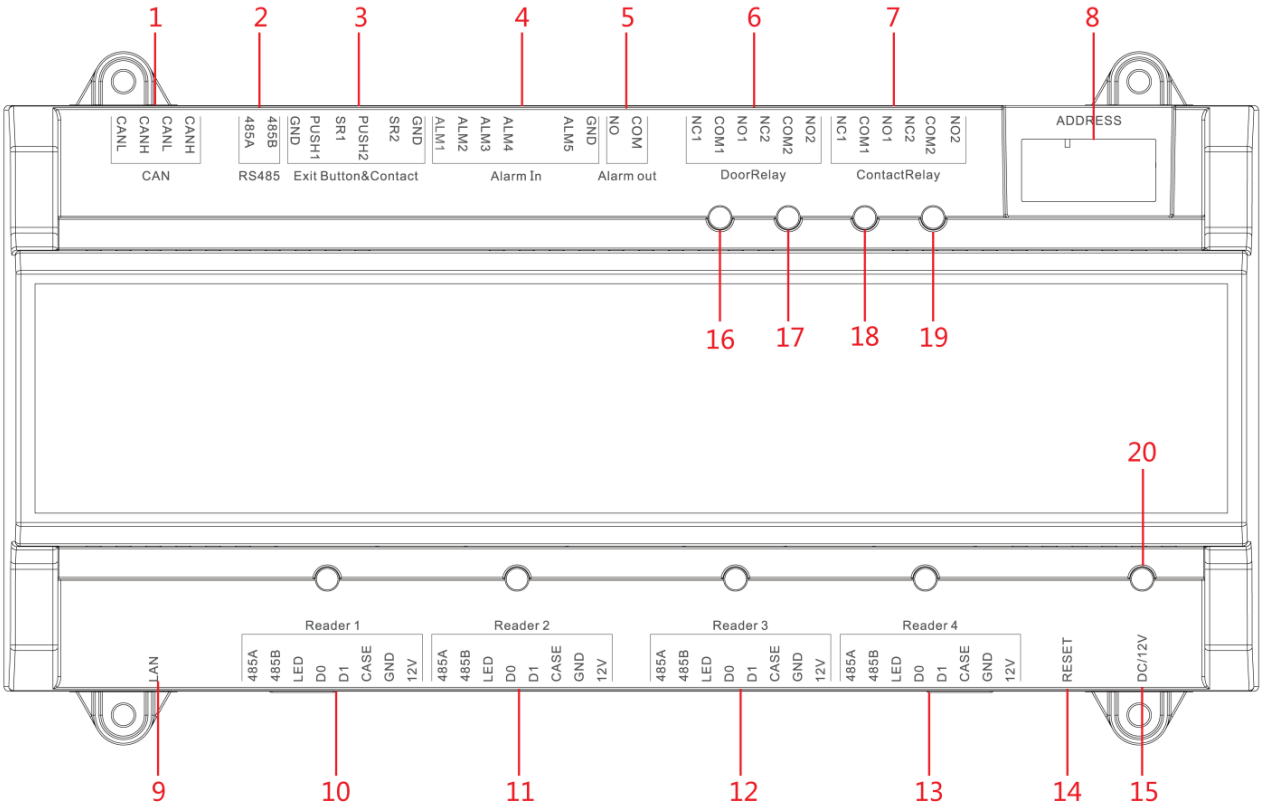


Figure 3-7

Interfaces are described in Table 3-1.

No.	Interface Description	No.	Interface Description
1	CAN bus	9	Not available at present
2	External extension module	10	Entry reader of door 1
3	Door sensor and exit button	11	Exit reader of door 1
4	External alarm input	12	Entry reader of door 2
5	External alarm output	13	Exit reader of door 2
6	Lock control output	14	Reboot
7	Internal alarm output	15	DC 12V power interface
8	Address code/transmission rate		

Table 3-1

Indicator lights are described in Table 3-2.

No.	Description
16	Lock status indicator
17	
18	Alarm status indicator
19	
20	Power indicator

Table 3-2

3.5.1 Wiring Description of CAN Bus

Wiring terminals of CAN bus are described in Table 3-3.

Interface	Wiring Terminal	Description
CAN bus	CANL	CAN bus input
	CANH	
	CANL	CAN bus output
	CANH	

Table 3-3

3.5.2 Wiring Description of Exit Button/Door Sensor

Corresponding wiring terminals of exit button and door sensor are shown in Figure 3-8. Please refer to Table 3-4 for descriptions of wiring terminals.

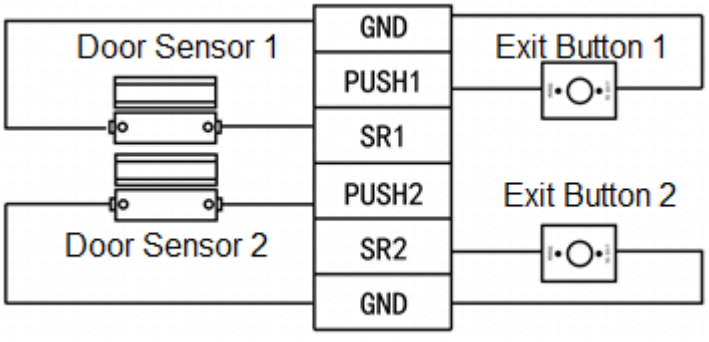


Figure 3-8

Interface	Wiring Terminal	Description
Exit button+ door	GND	Shared by exit button of door 1 and door

Interface	Wiring Terminal	Description
sensor		sensor input of door 1
	PUSH1	Exit button of door 1
	SR1	Door sensor input of door 1
	PUSH2	Exit button of door 2
	SR2	Door sensor input of door 2
	GND	Shared by exit button of door 2 and door sensor input of door 2

Table 3-4

3.5.3 Wiring Description of External Alarm Input

External alarm input connection is shown in Figure 3-9. Please refer to Table 3-4 for descriptions of wiring terminals.

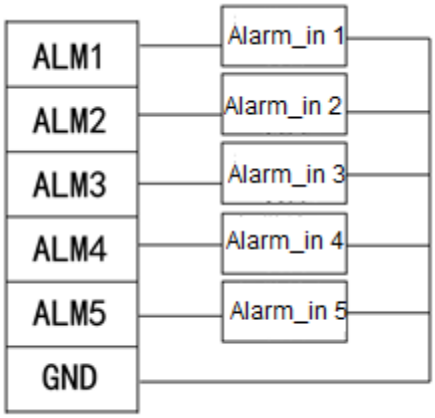


Figure 3-9

Interface	Wiring Terminal		Description
External alarm input	ALM1	Alarm input interface 1	External alarm input interfaces are able to connect smoke detector and IR detector etc..
	ALM2	Alarm input interface 2	
	ALM3	Alarm input interface 3	
	ALM4	Alarm input interface 4	
	ALM5	Alarm input interface 5 (reserved)	
	GND	Shared by alarm input interface 1, 2, 3, 4 and 5	

Table 3-5

3.5.4 Wiring Description of External Alarm Output

There are two connection modes of external alarm output, depending on alarm device. For example, IPC can use Mode 1, whereas audible and visual siren can use Mode 2, as shown in Figure 3-10 and Figure 3-11. Please refer to Table 3-6 for descriptions about wiring terminals.

Figure 3-10

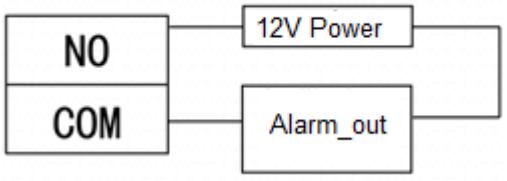


Figure 3-11

Interface	Wiring Terminal	Description
External alarm output	NO	External alarm output interfaces are able to connect audible and visual sirens.
	COM	

Table 3-6

3.5.5 Wiring Description of Lock

Support 2 groups of lock control outputs; serial numbers after the terminals represent corresponding doors. Please choose a proper connection mode according to lock type, as shown in Figure 3-12, Figure 3-13 and Figure 3-14. Please refer to Table 3-7 for descriptions of wiring terminals.

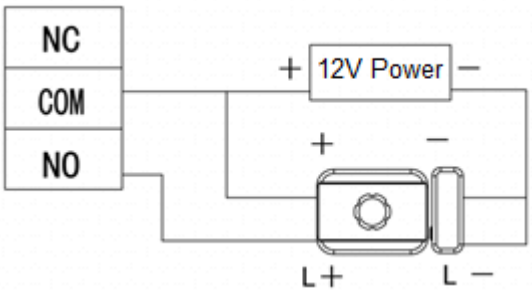


Figure 3-12

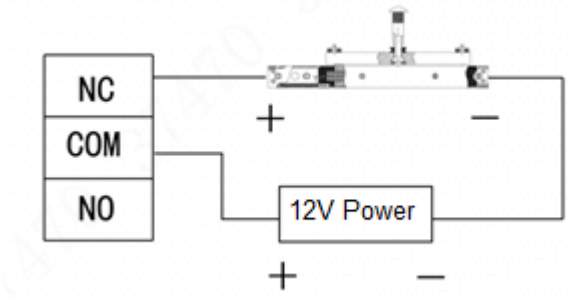


Figure 3-13

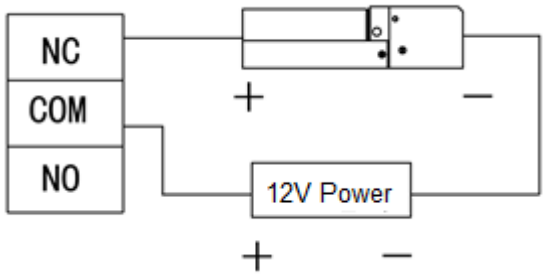


Figure 3-14

Interface	Wiring Terminal	Description
Lock control output	NC1	Lock control of door 1
	COM1	
	NO1	
	NC2	Lock control of door 2
	COM2	
	NO2	

Table 3-7

3.5.6 Wiring Description of Internal Alarm Output

Corresponding wiring terminals of internal alarm control output are shown in Table 3-8.

Interface	Wiring Terminal	Description
Internal alarm control output	NC1	Intrusion, overtime and vandal-proof alarm output of door 1. Output time lasts for 15s.
	COM1	
	NO1	
	NC2	Intrusion, overtime and vandal-proof alarm output of door 2. Output time lasts for 15s.
	COM2	
	NO42	

Table 3-8

3.5.7 Wiring Description of Reader

Note

1 door only supports to connect one type of reader—485 or Wiegand.

Please refer to Table 3-9 for descriptions of wiring terminals corresponding to readers. Take Door 1 for example, and other readers are the same as door 1. Please refer to Table 3-10 for descriptions of video cable specification and length.

Interface	Wiring Terminal	Cable Color	Description
Entry Reader of Door 1	485+	Purple	485 reader
	485-	Yellow	
	LED	Brown	Wiegand reader
	D0	Green	
	D1	White	
	CASE	Blue	
	GND	Black	Reader power supply

Interface	Wiring Terminal	Cable Color	Description
	12V	Red	

Table 3-9

Reader Type	Connection Mode	Length
485 Reader	CAT5e network cable, 485 connection	100m
Wiegand Reader	CAT5e network cable, Wiegand connection	30m

Table 3-10

3.6 DIP Switch

Set device number and speed with DIP switch. DIP switch is shown in Figure 3-15. Please refer to

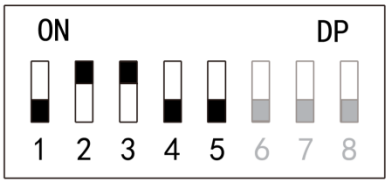
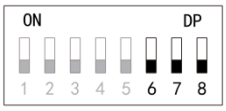
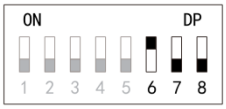
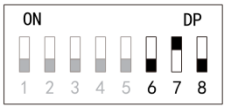
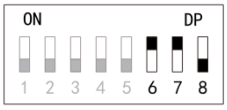
Function	No.	Description
Device Number	1～5	Set device number with binary system. The left is the lowest order. For example:  Binary representation 00110 corresponds to 6 in decimal system.
Speed	6～8	Set the speed. ● All of them are at the bottom transmission speed is 50kb/s.  , ● Only digit 6 is at ON position transmission speed is 80kb/s.  , ● Only digit 7 is at ON position transmission speed is 100kb/s.  , ● Digits 6 and 7 are at ON position transmission speed is 125kb/s.  ,

Table 3-11 for details.

-  the switch is at ON position, meaning 1.
-  the switch is at the bottom, meaning 0.

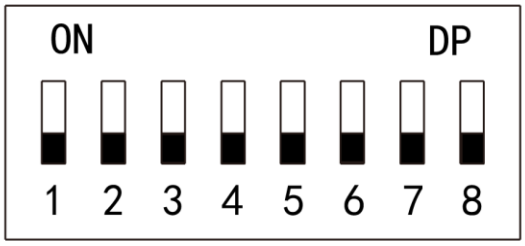


Figure 3-15

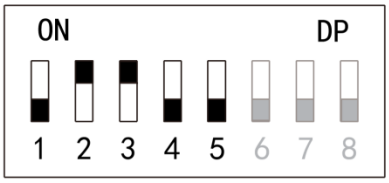
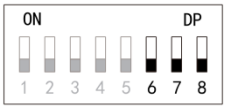
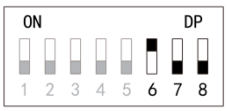
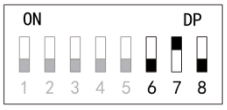
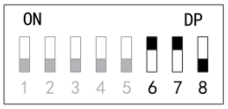
Function	No.	Description
Device Number	1～5	Set device number with binary system. The left is the lowest order. For example:  Binary representation 00110 corresponds to 6 in decimal system.
Speed	6～8	Set the speed. ● All of them are at the bottom transmission speed is 50kb/s.  , ● Only digit 6 is at ON position transmission speed is 80kb/s.  , ● Only digit 7 is at ON position transmission speed is 100kb/s.  , ● Digits 6 and 7 are at ON position transmission speed is 125kb/s.  ,

Table 3-11

3.7 Reboot

Insert a needle into RESET hole, and long press the reboot controller.

4 Technical Parameters

Parameter	Specification
Processor	32-bit ARM processor
Storage Capacity	16M
Max User	20,000
Max Record	30,000
Communication Port of Reader	Wiegand,RS485
Communication Port	CAN
Quantity of Connected Reader	4 groups
Working Power	Rated power 10V～15V DC, rated current 0.75A
Real-time Monitoring	Support
Fire Alarm Linkage	Support
Vandal-proof Alarm	Support
Illegal Intrusion Alarm	Support
Unlock Overtime Alarm	Support
Duress Card Setup	Support
DST and Time Sync	Support
Online Upgrading	Support