USER MANUAL

Elevator Control Panel & Elevator Floor Expansion Board

Applicable Models: EC16 & DEX16

Version: 1.2

Date: September 2023

English

Trademark

ZKTeco is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without the express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/ documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or

amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on http://www.zkteco.eu.

If there is any issue related to the product, please contact us.

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of **EC16 Elevator Control Panel & DEX16 Elevator Floor Expansion Board**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Features and parameters with ★ are not available in all devices.

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface names e.g., **OK**, **Confirm**, **Cancel**.
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.
For Device	
Convention	**Description**
< >	Button or key names for devices. For example, press <OK>.
[ ]	Window names, menu items, data table, and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forwarding slashes. For example, [File/Create/Folder].

Symbols

Convention	Description
	This represents a note that needs to pay more attention to.
	The general information which helps in performing the operations faster.
	The information which is significant.
	Care taken to avoid danger or mistakes.
	The statement or event that warns of something or that serves as a cautionary example.

Table of Contents

1 SAFETY INSTRUCTIONS 7

1.1 IMPORTANT SECURITY INSTRUCTIONS 7

1.2 INSTALLATION CAUTIONS 8

2 OVERVIEW 9

2.1 SYSTEM INTRODUCTION 9

2.2 PACKAGE C ENCLOSURE INTRODUCTION 9

2.3 SYSTEM EQUIPMENT COMPOSITION 10

2.4 TECHNICAL PARAMETERS 11

2.5 ELECTRICAL SPECIFICATIONS 12

2.6 LED INDICATORS DESCRIPTION 13

3 TERMINAL INSTRUCTIONS 14

4 WIRING DESCRIPTION 16

4.1 ELEVATOR CONTROLLER NETWORKING CABLING 16

4.2 CONNECTION POWER SUPPLY 17

4.3 ETHERNET CONNECTION TO THE COMPUTER 18

4.4 ELEVATOR CONTROL AND ELEVATOR BUTTON WIRING 19

4.5 MO, EMG, FIRE, TAMPER INTERFACE DESCRIPTION 20

4.6 WIRING OF EXPANSION BOARD 22

4.7 INSTALLATION OF ELEVATOR MANAGEMENT SYSTEM 23

4.8 ELEVATOR CONTROLLER SYSTEM POWER SUPPLY STRUCTURE 24

5 ELEVATOR CONTROL OPERATING INSTRUCTIONS 25

5.1 CONNECT TO ZKBIO CVSECURITY SOFTWARE 25

5.1.1 LOGIN SOFTWARE 25

5.1.2 ADD DEVICE ON THE SOFTWARE 26

5.1.3 SYNCHRONIZE ALL DATA TO DEVICES 27

5.1.4 ADD EXPANSION BOARD ON THE SOFTWARE 28

5.1.5 ADD READER ON THE SOFTWARE 29

5.1.6 SET ELEVATOR CONTROL RULES ON SOFTWARE 31

5.2 USER VERIFICATION ON THE QR-600 SERIES READERS 36

5.3 CONNECT TO ZKBIOSECURITY MOBILE APP 36

5.3.1 MOBILE APP CONFIGURATION 36

5.3.2 LOGIN 38
5.3.3 ENABLE THE DYNAMIC QR CODE ON THE SOFTWARE 40
5.3.4 VERIFICATION QR CODE 41
6 COMMUNICATION CONNECTION 42
6.1 ACCESS CONTROL NETWORKING WIRES AND WIRING 42
6.2 TCP/IP COMMUNICATION 43
6.3 MODIFY THE IP ADDRESS 44
7 OTHERS 47
7.1 USB DISK UPGRADE 47
7.2 RESTORE FACTORY SETTINGS 47
APPENDIX 1 ELEVATOR CONTROL AND ELEVATOR BUTTON WIRING 48
METHOD 1 COMMON ANODE BUTTON CONNECTION 48
METHOD 2 COMMON CATHODE BUTTON CONNECTION 51
APPENDIX 2 BUZZER, INDICATOR LIGHT PROMPT INSTRUCTIONS 54
APPENDIX 3 PRIVACY POLICY 55
APPENDIX 4 ECO-FRIENDLY OPERATION 57

1 Safety Instructions

1.1 Important Security Instructions

1. Before operating the equipment, please read and strictly follow all security and operation instructions. Please keep the instructions in good condition for future reference.
2. Please use the accessories recommended by the manufacturer or delivered together with the product. Any other related product is not recommended to be used as the alarm or monitoring system (cameras, infrared detectors, smoke detectors, etc.). The alarm or monitoring system should comply with the local applicable fire-prevention and security standards.
3. Do not place this equipment on any unstable table, tripod mount, supterminal or base to prevent the equipment from falling and damages, and more undesirably causing severe personal injuries. Therefore, it is important to install the equipment as instructed by the manufacturer.
4. All peripheral devices must be grounded.
5. No external connection wires can be exposed. All connections and idle wire ends must be wrapped with insulating tapes to prevent accidental contact with exposed wires from damaging the equipment.
6. Do not attempt to carry out unauthorized repair of the equipment. Disassembly or detachment is likely to cause electric shock or other physical problems. All repair should be done by qualified repair personnel.
7. In any of the following cases, disconnect the power supply from the equipment first and notify qualified repair personnel for repair:
   - ✧ The power cord or connector is damaged;
   - ✧ Liquid leaks into or any objects fall into the equipment;
   - ✧ The equipment has got wet or exposed to bad weather (rain, snow, etc.);
   - ✧ If the equipment cannot work normally even though it is operated as instructed;
   - ✧ The equipment falls down or its performance changes obviously.
8. If it is necessary to replace a component, the repair personnel must use only the substitutes specified by the manufacturer.
9. After the equipment is repaired, the repair personnel needs to conduct security inspection to ensure the equipment works normally.
10. Operate the equipment with only the type of power supply indicated on the label. Contact the operator for any uncertainty about the type of power supply.

Violation of any of the following cautions may result in personal injury or equipment malfunctions. We assume no responsibility for any damage caused by mishandling that is beyond normal usage defined in this product manual.

- Before installation, switch off the external circuit (that supplies power to the system).
- Before connecting the equipment to power supply, ensure the output voltage is within the specified range.
- Never connect the product to the power before completion of installation.

1.2 Installation Cautions

1. To protect the wiring from rats, all wires should be placed in pipes. It is recommended to use PVC conduits or galvanized tubes. Although the control panel has a good anti-static, anti-lightning, and anti-leakage design, it is important to ensure that the case of the control panel and the AC ground wire are connected perfectly and the AC ground wire is grounded.
2. It is recommended not to plug and unplug connection terminals frequently when the system is energized. Be sure to unplug the connection terminals before starting any relevant welding job.
3. Do not detach or replace any control panel chip without permission because unprofessional operation may cause damage to the control panel.
4. It is recommended not to connect any other auxiliary devices without permission. All non-routine operations must be confirmed with our engineers in advance.
5. A control panel should not share one power socket with any other large-current devices.
6. It is preferable to install card readers and buttons at a height of **55 inches to 59 inches (1.4m to 1.5m)** above the ground, subject to proper adjustment according to customers' usual practice.
7. It is advised to install the product in a place convenient for future maintenance, like **a weak electric well**.
8. The exposed part of any connection terminal is strongly recommended **not be longer than 0.16 inches (4mm)**. Professional clamping tools may be used to avoid short-circuit or communication failure resulting from accidental contact with excessive exposed wires.
9. To save access control event records, exterminal data periodically from control panels.
10. Prepared countermeasures against unexpected power failure, like **selecting power supply with UPS**.
11. If the RS485 reader is connected externally and shares the power supply with the device (The control panel does not supterminal RS485 readers with fingerprint verification function), the connection between the EXT RS485 terminal and the reader is recommended **not to be longer than 328 ft (100m)**. Otherwise, it is recommended to use a separate power supply for the reader.
12. The length of the connection between computer and elevator controller: RS485 communication is **less than 3937 ft (1200m)**. In order to make the communication more stable, it is recommended to control **within 2624 ft (800m)**. It is recommended to use the power supply delivered with the system as the control panel power supply.
13. It is recommended to use the power supply delivered with the system as the control panel power supply.
14. In a place with strong magnetic interference, galvanized steel pipes or shielded cables are recommended, and proper grounding is required.

2 Overview

2.1 System Introduction

The elevator control system is a digital management system that controls access to elevators for personnels. This elevator control system introduced by ZKTeco mainly consists of the EC16 master elevator controller, DEX16 floor expansion board, QR600 series reader and D147 card issuer and other auxiliary equipment. Each elevator controller can be connected to up to seven floor expansion boards, which can control up to 128 floors. After entering the elevator, users must swipe the card, QR code or password inside the elevator to pass the authentication before they are authorized to press the designated floor button and finally reach the corresponding floor.

2.2 Package C Enclosure Introduction

EC16 elevator master controller is a bare board, which can be installed and fixed to Package C enclosure, and the DEX16 expansion board supports stacking and fixing on the master control board.

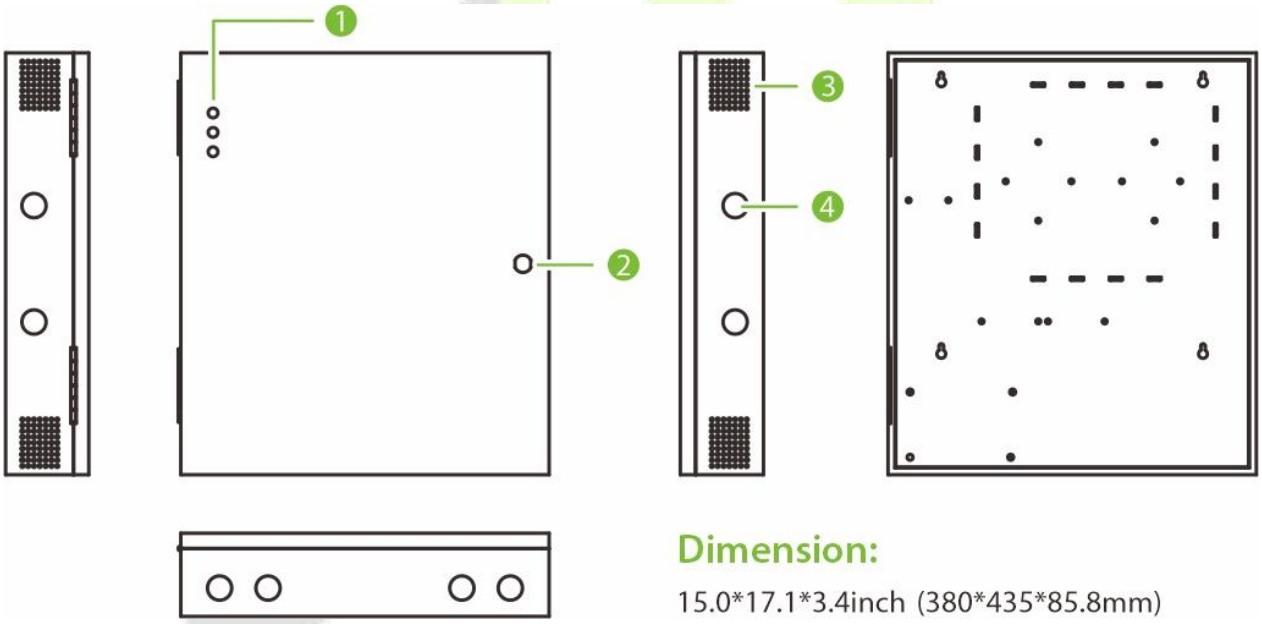


Figure 1-1 Package C Enclosure Appearance

No.	Description
1	Status Indicator (Includes PWR, COMM, RUN)
2	Keyhole
3	Wire Hole
4	Heat Dissipation Holes

2.3 System Equipment Composition

The elevator controller system is composed of the following equipments:

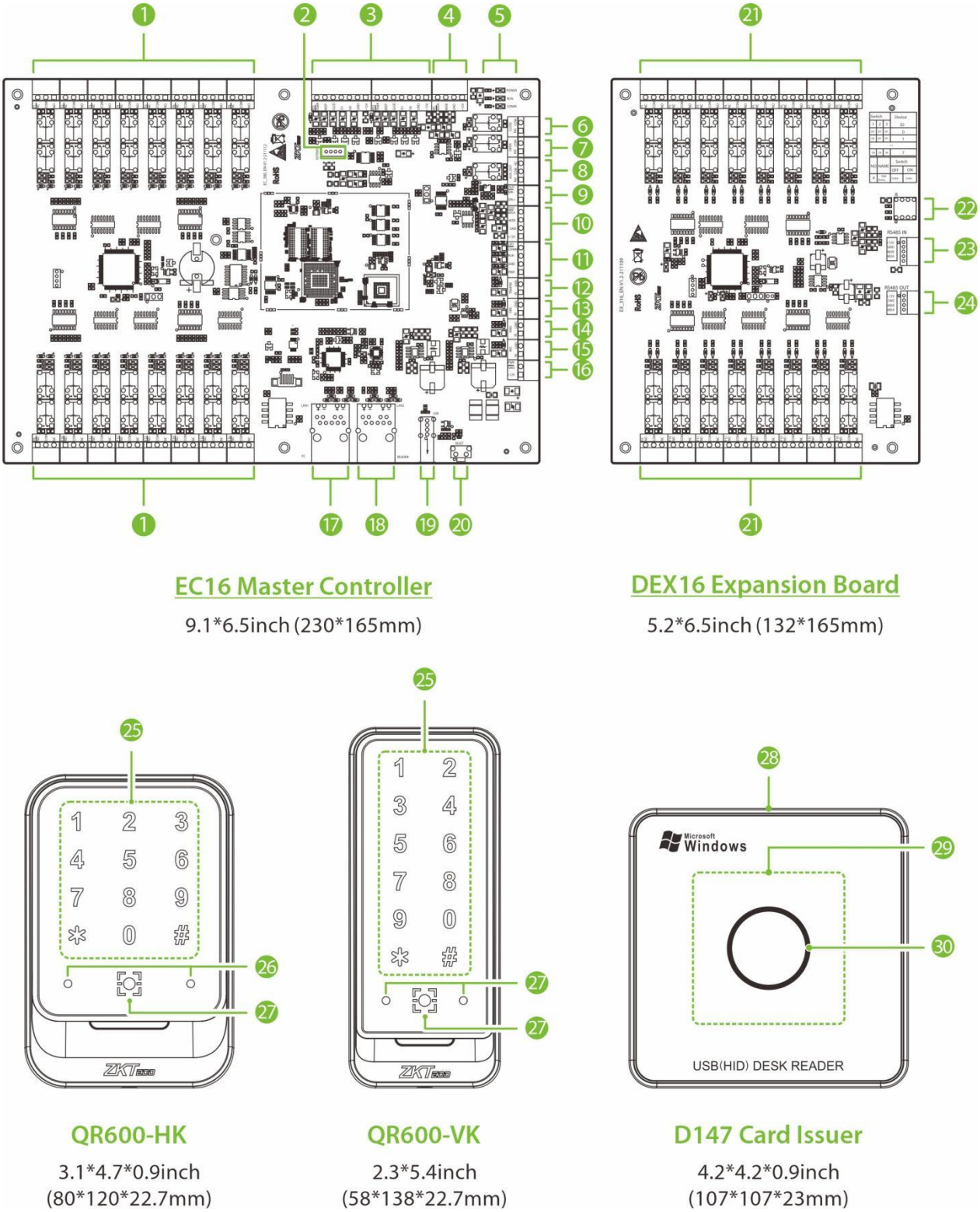


Figure 1-2 System Equipment Appearance

No.	Description	No.	Description
1	Floor Button Control Port	16	Power Input
2	Extend Port	17	Ethernet Interface (LAN1)
3	Wiegand	18	TCP/IP Reader Interface (LAN2)*
4	RS-485	19	U disk interface
5	LED Indicator	20	Reset Button
6	Elevator Door Closing Button*	21	Floor Button Control Port
7	Elevator Door Opening Button*	22	DIP Switch
8	Alarm Output	23	RS-485 Input
9	Speaker*	24	RS-485 Output
10	Voice*	25	Touch Keypad & RFID Card Reading Area
11	LED Indicator Port	26	Flash
12	Tamper Switch Port	27	QR Code Collector
13	FIRE	28	USB Jack
14	Emergency Button	29	RFID Card Reading Area
15	Manual Button	30	LED Indicator
Note: * Hardware reservation function is currently not supported.			

2.4 Technical Parameters

EC16 Elevator Controller			
Controllable Floors	16 floors	**Power Supply**	Adopt Package C enclosure matching adapter
User Capacity	30,000	**PC Communication**	TCP/IP
Card Capacity	100,000	**Reader Communication**	Wiegand, RS-485
Fingerprint Capacity	30,000	**Number of connectable expansion boards**	Up to 7 DEX16s can be connected at the same time
Record Capacity	200,000	**Number of expandable floors**	Up to 128 floors
DEX16 Expansion Board			
Controllable Floors	16 floors	**Communication With EC16**	Wiegand, RS-485
Power Supply	12V DC, powered by EC16		

2.5 Electrical Specifications

EC16 Elevator Controller		
Power	**Main Power Supply**	12VDC ± 20%, maximum current 600mA (without reader and expansion board)
	Wiegand Reader	12VDC ± 20%, maximum output current 350mA
	RS-485 Reader	12VDC ± 20%, maximum output current 750mA
Output	**Auxiliary Relay Output**	Contact load: 1A / 24VDC **Note:** When connecting to the elevator button, the maximum allowable voltage is 24V.
Input	**FIRE**	Maximum allowable input voltage 15V
	Emergency	
	Manual	
	TAMPER	
	Wiegand Reader TAMPER	
DEX16 Expansion Board		
Power	**Main Power Supply**	12VDC ± 20%, maximum current 350mA
Output	**Auxiliary Relay Output**	Contact load: 1A / 24VDC **Note:** When connecting to the elevator button, the maximum allowable voltage is 24V.

2.6 LED Indicators Description

LED indicators on the EC16

When the EC16 elevator controller is powered on, the LED indicators under normal circumstances will show the following.

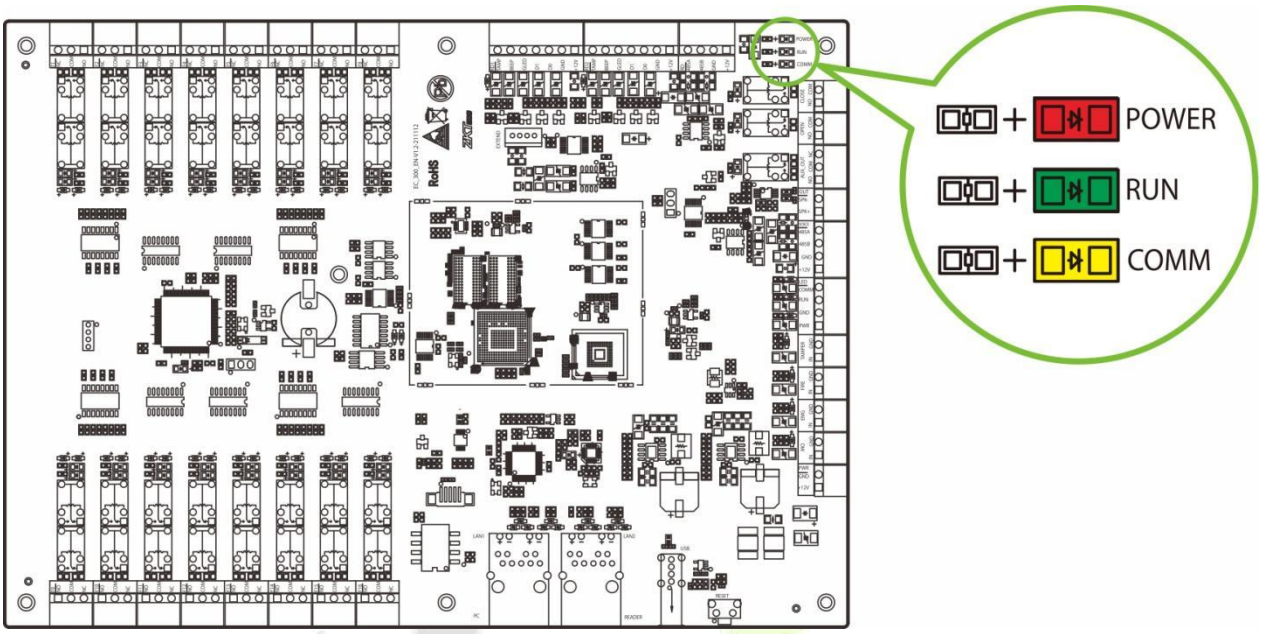


Figure 1-3 LED indicator diagram of the elevator controller

- **POWER indicator (Red):**

  Solid Red LED indicates normal energization.

- **RUN indicator (Green):**

  Slowly flashing Green LED indicates normal working status of the system.

- **COMM indicator (Yellow):**

  Slowly flashing Yellow LED indicates data communication is in progress.

LED indicators on the Package C Enclosure

- **PWR indicator (Red):**

  Solid Red LED indicates normal energization.

- **COMM indicator (Yellow):**

  Slowly flashing Yellow LED indicates data communication is in progress.

- **RUN indicator (Green):**

  Slowly flashing Green LED indicates normal working status of the system.

3 Terminal Instructions

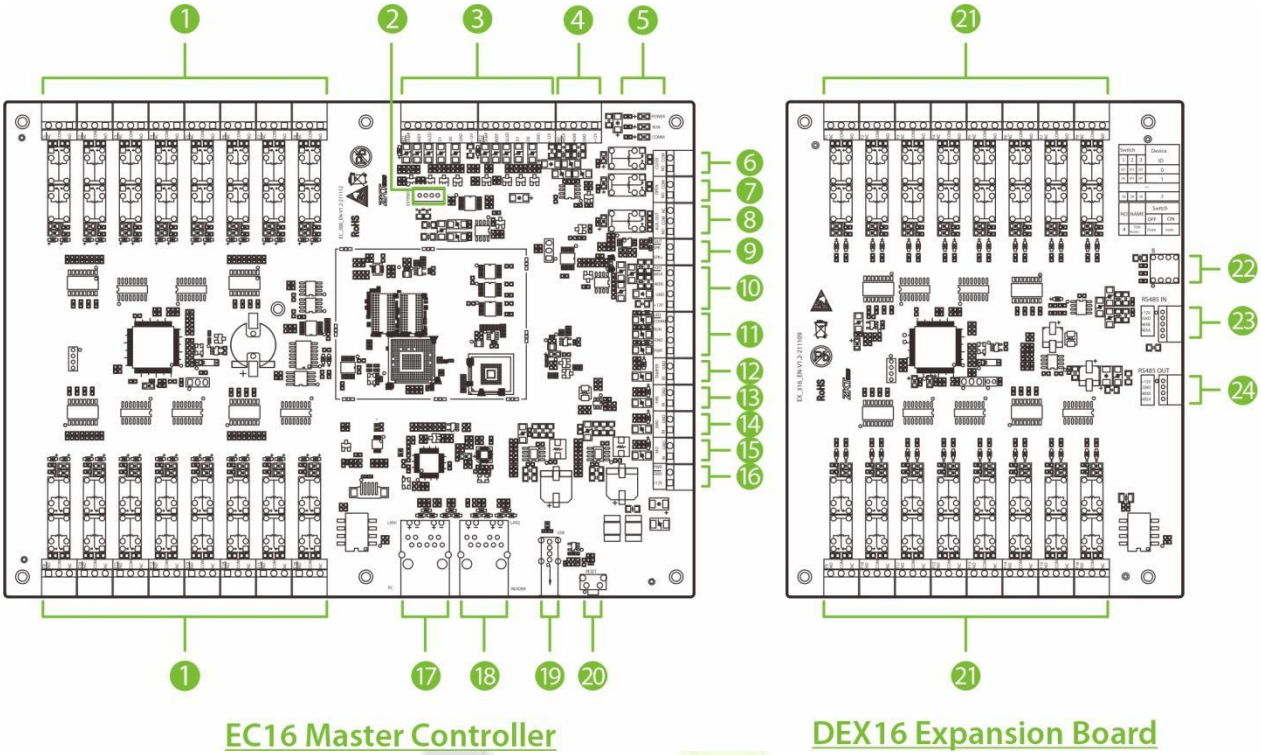


Figure 3-1 Terminal diagram of the elevator controller and the expansion board

The terminals are described as follows:

No.	Terminal	Number	Description
1	Floor Button Control Port	16	Used to connect elevator buttons for floor selection control.
2	Extend Port	1	Expansion output for connecting DEX16 expansion board to expand floors.
3	Wiegand	2	Wiegand reader communication terminal. Used to connect Wiegand readers, etc. And supports line interruption alarm message alerts.
4	RS-485	1	RS-485 reader communication terminal, used to connect RS-485 reader. Connect up to two readers.
5	LED Indicator	1	Equipment operating status indicators, respectively, are power light (POWER), operating status indicator (RUN) and communication indicator (COMM).
6	Elevator Door Closing Button	1	Hardware reservation function is currently not supported.
7	Elevator Door Opening Button	1	Hardware reservation function is currently not supported.
8	Alarm Output	1	Used to connect with the alarm.
9	Speaker	1	Hardware reservation function is currently not supported.
10	Voice	1	Hardware reservation function is currently not supported.

No.	Terminal	Number	Description
11	LED Indicator Port	1	Used to indicate the operating status of the system. Connect to the enclosure.
12	Tamper Switch	1	Used to connect to the tamper switch of the enclosure.
13	FIRE	1	It is used to connect the fire switch, after starting the fire button, all the buttons of the elevator cannot be lit normally.
14	Emergency Button	1	In an emergency, when the emergency interface receives a short-circuit signal, the elevator control will not control the elevator buttons (the buttons are in the released state), and the equipment can only be restored to the control state if it is powered off and restarted or set by software.
15	Manual Button	1	When the manual interface receives a short-circuit signal, the elevator control will not control the elevator buttons, and the elevator will resume the control state after release.
16	Power Input	1	12V power supply terminal, used to connect the Package C enclosure matching adapter to power the elevator controller.
17	Ethernet Interface (LAN1)	1	Used for equipment networking and remote control.
18	TCP/IP Reader Interface (LAN2)	1	Used to connect TCP/IP multimodal intelligent collection terminal. Hardware reservation function is currently not supported.
19	U Disk Interface	1	Mainly used for upgrading the elevator controller.
20	Reset Button	1	Long press 1 to 5 seconds for U disk upgrade, 5 to 10 seconds to restart the controller, 10 seconds or more to restore factory settings.
21	Floor Button Control Port	16	Used for connecting elevator extension floor buttons for floor selection control.
22	DIP Switch	1	Set the RS-485 address of the expansion board according to the current connection order of the expansion board and follow the operation prompt next to it.
23	RS-485 Input	1	Used to connect the signal output terminal of the EC16 controller (i.e. Extend Port) or the signal output terminal of the upper level DEX16.
24	RS-485 Output	1	Used for output when connecting to DEX16 expansion floor.

Recommended use of wires:

Interface	Wire specifications	Maximum transmission distance (theoretical value)
Power Supply	18AWG*2PIN	1.5m
Wiegand	Adopt 6-core communication shielded wire (RVVP 6*0.5mm) (6PIN, 8PIN, 10PIN for different readers) to reduce interference in the transmission process	100m
Floor Control	24AWG*2PIN	50m
Input	24AWG*2PIN	100m
RS-485	Adopt 4-core communication cable (RVVP 4*0.5mm)	Share power with control panel: 100m. Use independent power supply (connect with RS-485 signal interface only): 1000m.

4 Wiring Description

4.1 Elevator Controller Networking Cabling

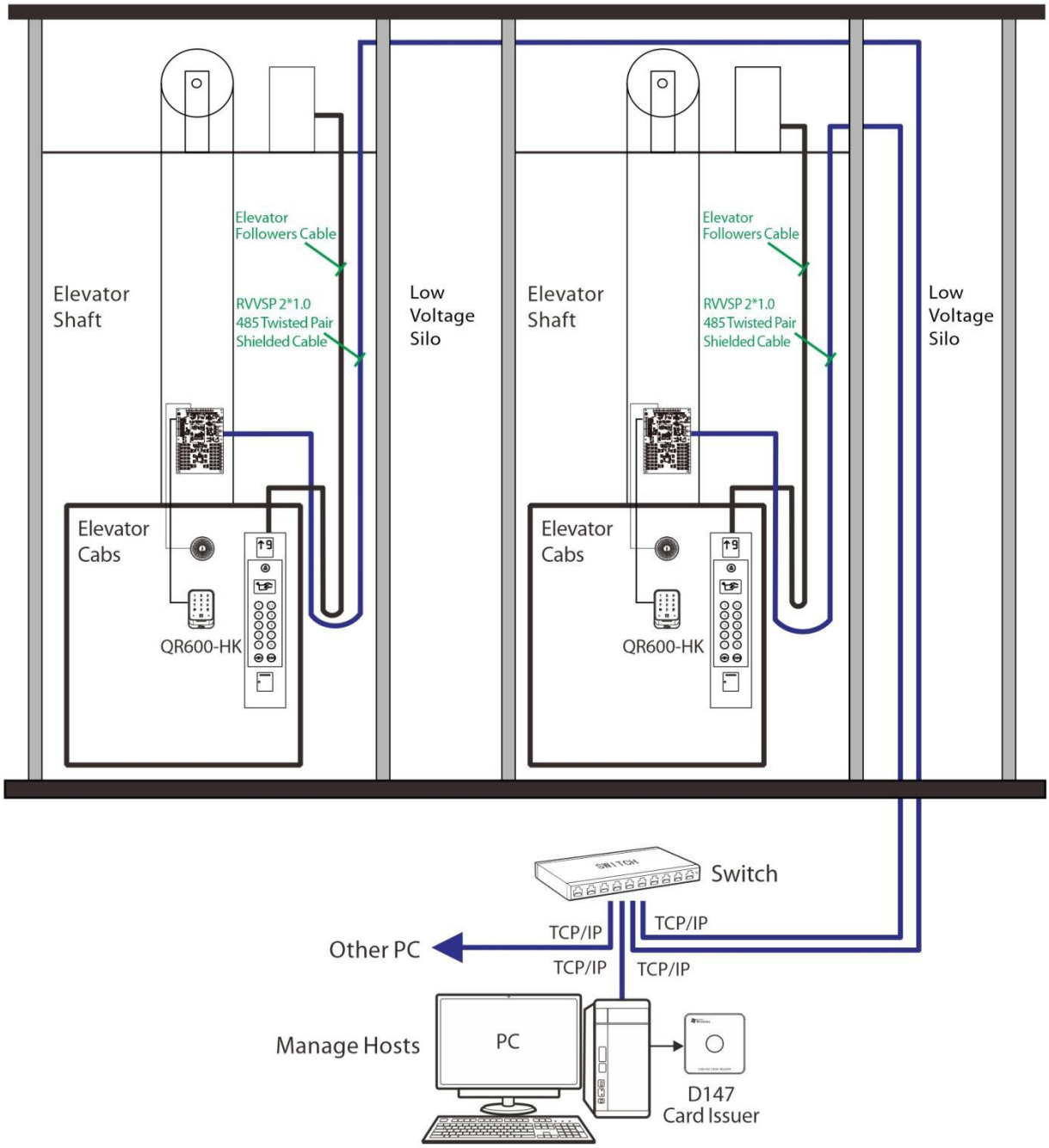


Figure 4-1 Diagram of elevator controller networking cabling

Note: Make sure the power is turned off before wiring. Wiring in the energized state may cause serious damage to the equipment.

4.2 Connection Power Supply

This device uses the adapter matched with the Package C enclosure to supply power to the elevator controller, providing a 12V power supply which takes into account the power consumption of the elevator controller itself, the power consumption of up to seven DEX16 expansion boards and the output power consumption of the RS-485 reader. The wiring is shown in the following diagram.

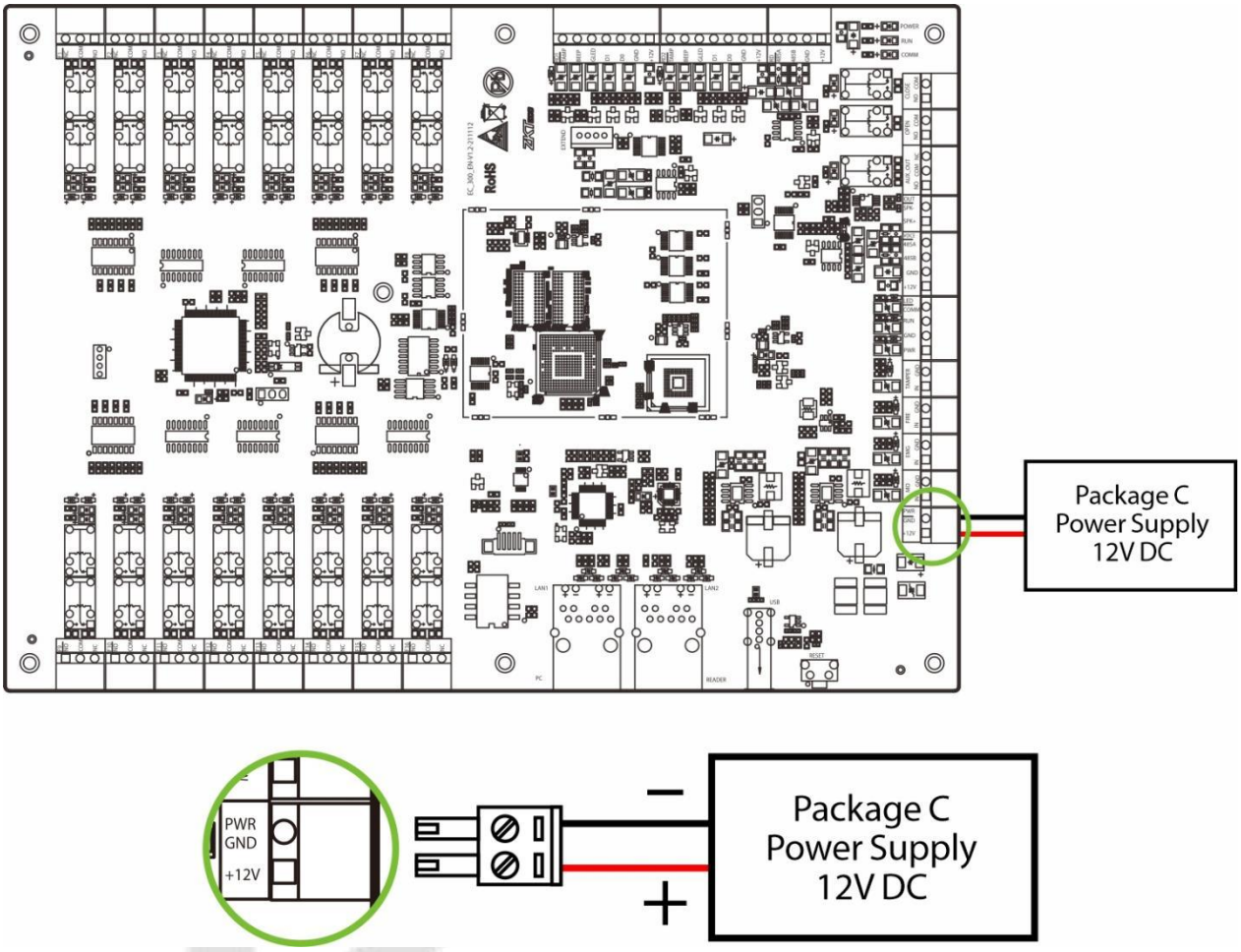


Figure 4-2 Power wiring diagram

4.3 Ethernet Connection to the Computer

Connect the elevator controller and the computer software via Ethernet cable. The wiring is shown in the following diagram.

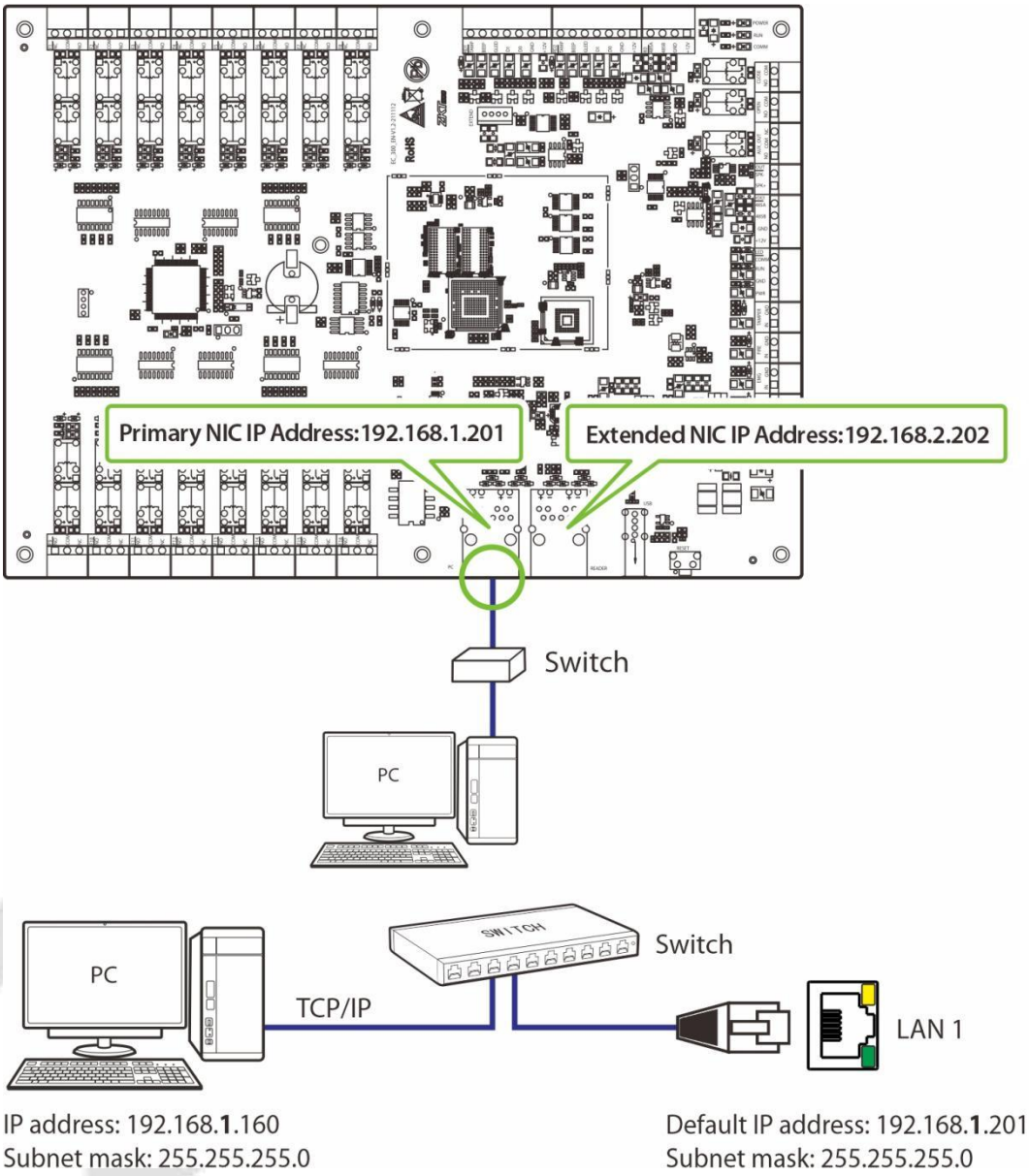
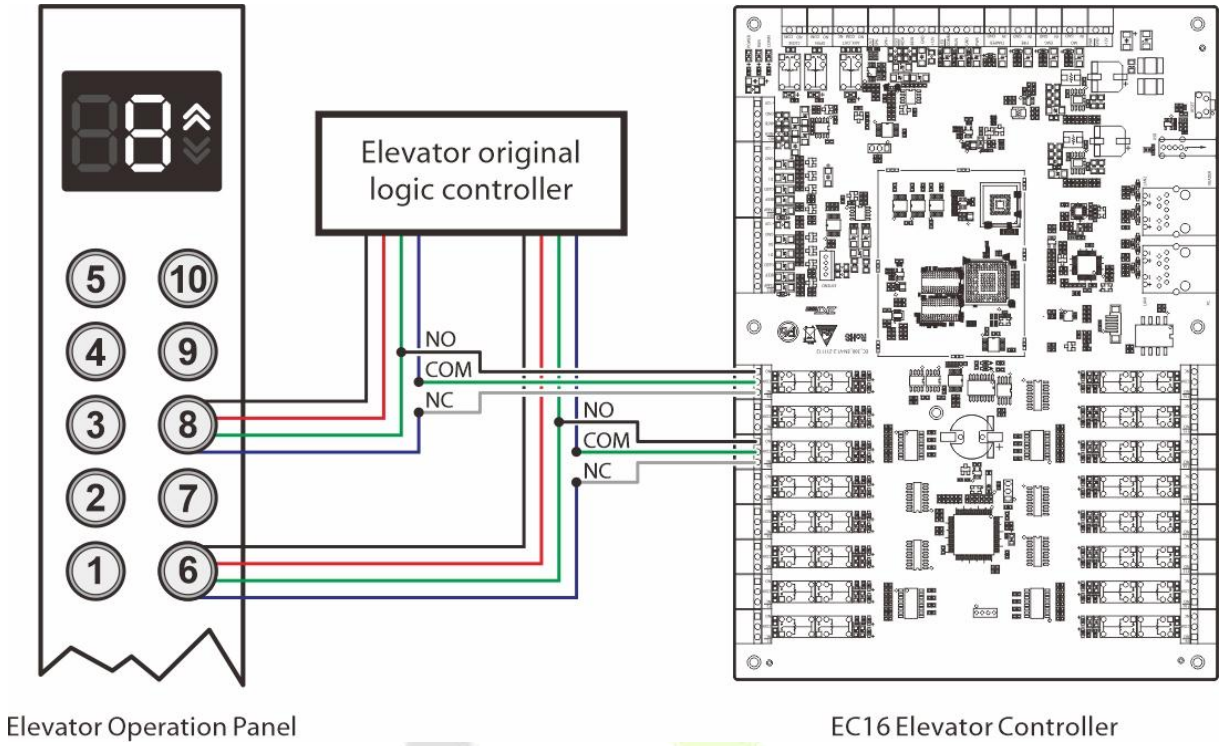


Figure 4-3 Ethernet wiring diagram

Note:

1. *IP addresses can cross network segments, but they must belong to the same subnet, and the gateway and IP address must be in the same network segment.*
2. *Dual Ethernet interfaces: the default IP address **192.168.1.201** for the primary NIC and **192.168.2.202** for the expansion NIC.*
3. *The IP address of the primary NIC can be set by yourself, and the network segment of the expansion NIC must be **192.168.2.(1 to 253**).*

4.4 Elevator Control and Elevator Button Wiring



- Elevator Button Wiring Description

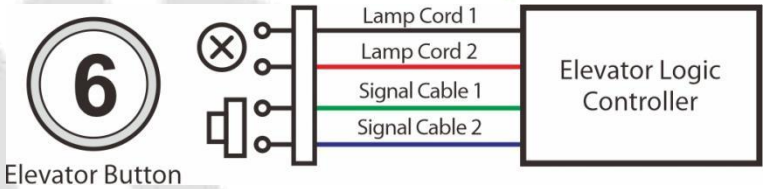


Figure 4-4 Elevator button wiring schematic

Instruction:

*Connect **Signal Cable 1** to the **NO** terminal on the corresponding floor of the elevator logic controller. After Signal Cable 2 is disconnected, **COM** and **NC** terminals are connected to the **COM** and **NC** terminals of the corresponding floor respectively.*

- Wiring for swipe to select floor and direct floor selection

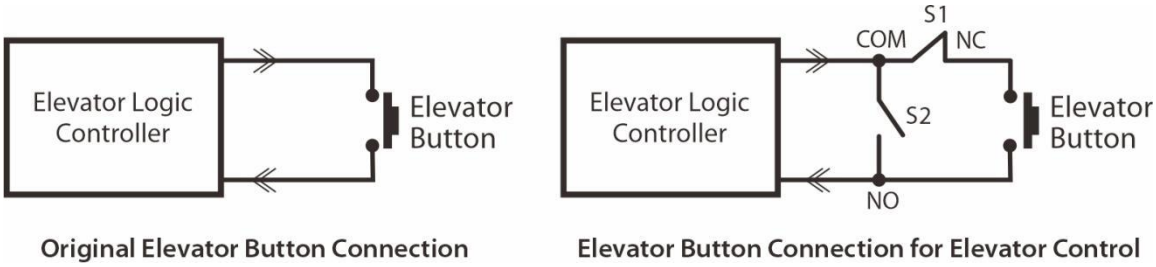


Figure 4-5 Swipe card to select the floor and direct selection of floor wiring diagram

Instruction:

S1 and S2 switches are two relays (S1 relay is normally closed and S2 relay is normally open) of the elevator control board respectively. S1 is disconnected after power on, and S1 is closed after swiping the layer selection card, then the elevator button can be lit by pressing; S2 is closed after swiping the direct access card, then the elevator button will be lit automatically.

Note: *Refer to Appendix 1 Elevator Control and Elevator Button Wiring for detailed wiring.*

4.5 MO, EMG, FIRE, TAMPER Interface Description

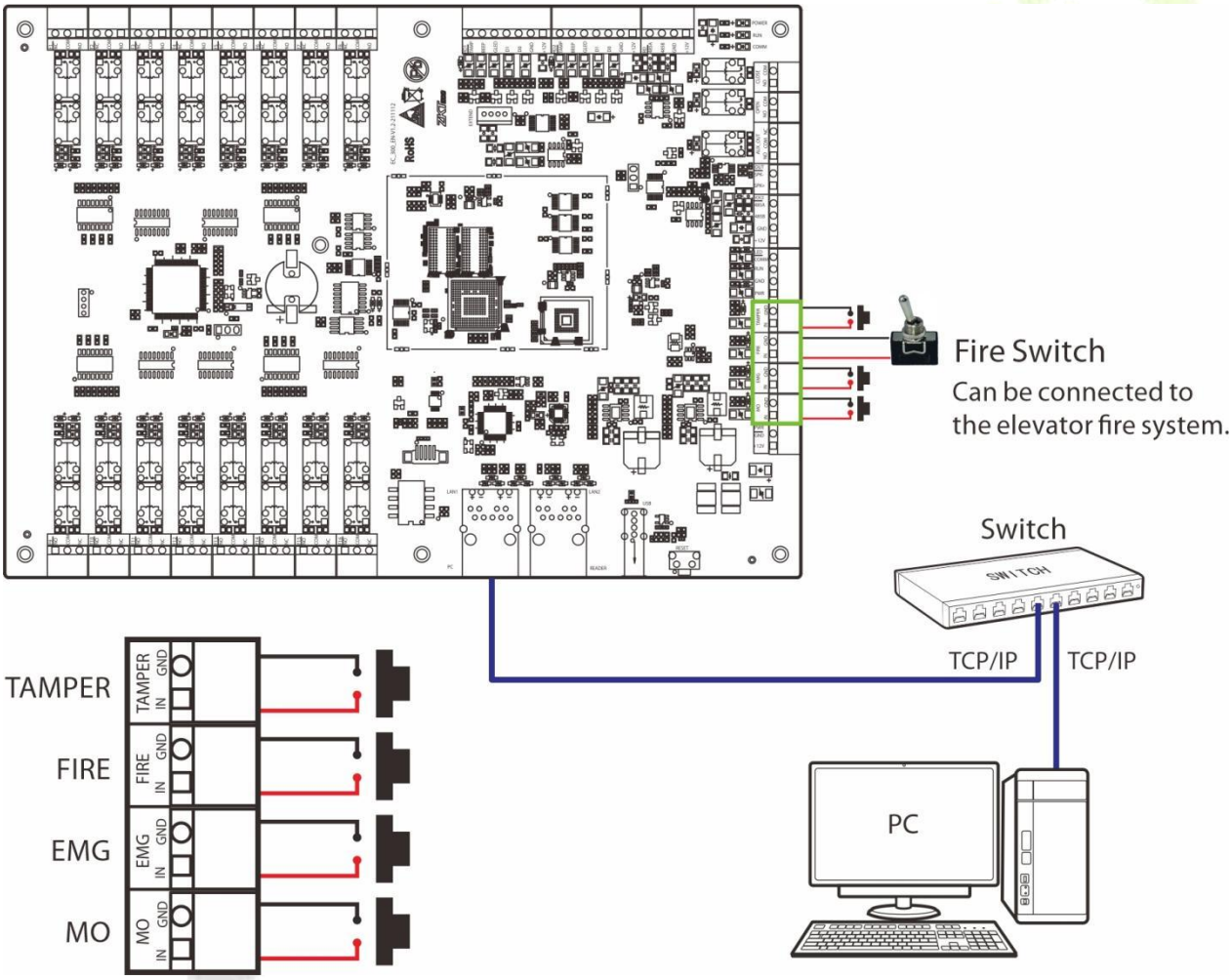
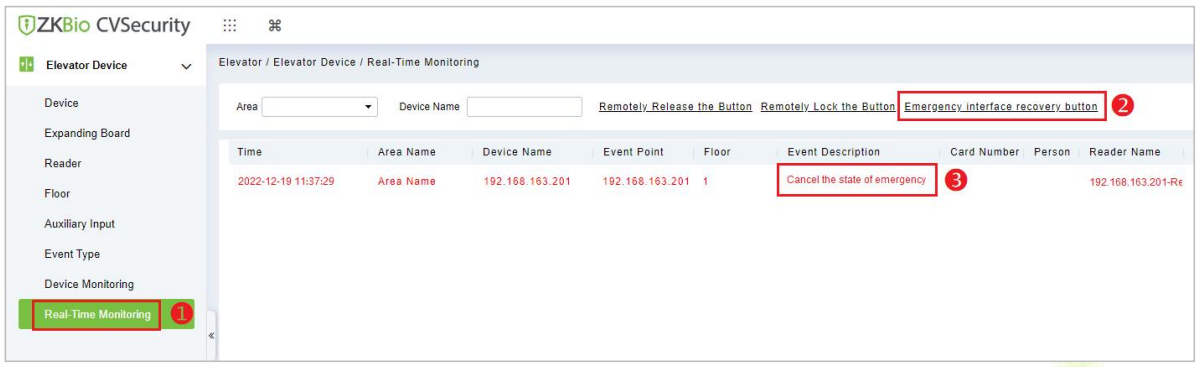


Figure 4-6 MO, EMG, FIRE, TAMPER interface wiring diagram

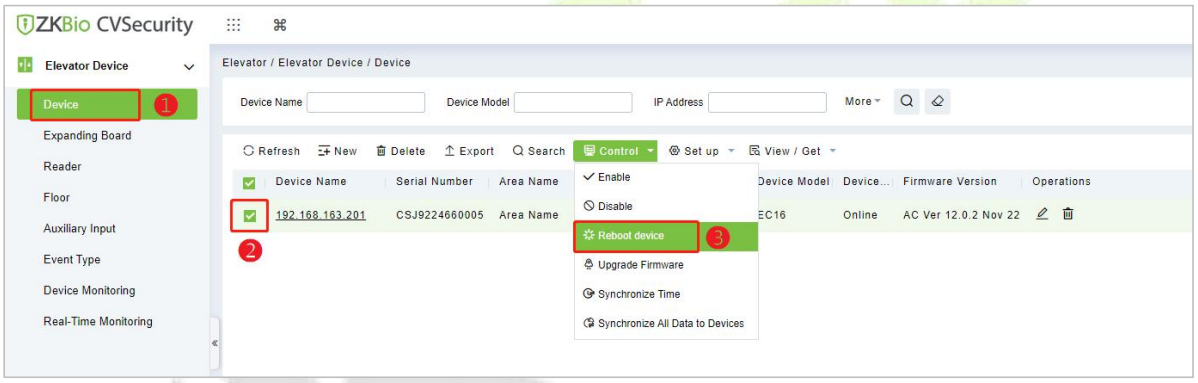
Instructions:

1. *When the **MO** interface becomes a short circuit, the elevator controller will cancel the control function of the floor button. At this time, the elevator buttons can be operated manually. The "manual" function can be canceled by directly changing the MO interface from short circuit to broken circuit.*

2. *When the **EMG** interface becomes short circuit, the elevator controller will cancel the key control of each floor. To cancel the "emergency" function, please log in ZKBio CVSecurity software, click [**Elevator**] > [**Elevator Device**] > [**Real-time Monitoring**] > [**Emergency interface recovery button**].*



3. *When the **FIRE** interface becomes a short circuit, all the keys of the elevator cannot be lit normally. If you want to cancel the "fire" function, please log in ZKBio CVSecurity software, click [**Elevator**] > [**Elevator Device**] > [**Device**] and then check the equipment that needs to restart, select [**Control**] > [**Restart device**] to complete the restart of the elevator control equipment, see the following figure for detailed steps.*



4. *When the **TAMPER** interface becomes a broken circuit, the system will push the tampering alarm information in real time and send an alarm sound.*
5. *Fire and emergency functions require no software setup, just a hardware connection for use.*
6. *In this elevator controller system, the fire interface has the highest level, followed by the emergency interface, and finally the manual interface.*
7. *When an alarm is connected to the auxiliary output of the controller, the status of the alarm and the event description of the software side after the interface is short circuit or broken circuit are as follows.*

Interface	Line Status	Auxiliary Output (Alarm)	Event description on the software
MO	Short circuit	Uninterrupted alarm	Real-time pushing of "manual button short circuit" information and one alarm sound
	Broken circuit	Stop alarm	Real-time pushing of "manual button short circuit" information and one alarm sound
	Note: The alarm can be canceled by disconnecting the "manual" interface of the elevator control equipment.		
EMG	Short circuit	Uninterrupted alarm	Real-time pushing of "emergency button short circuit" information and one alarm sound
	Broken circuit	Uninterrupted alarm	Real-time pushing of "emergency button short circuit" information and one alarm sound
	Note: The alarm can be cancelled by clicking the [**Emergency Interface Recovery**] button or by restarting the device on the software side.		

FIRE	Short circuit	Uninterrupted alarm	Real-time pushing of "fire button short circuit" information and one alarm sound
	Broken circuit	Uninterrupted alarm	Real-time pushing of "fire button break" information and one alarm sound
	Note: The alarm can be cancelled by restarting the device on the software side.		
TAMPER	Short circuit	No alarm	No information push and no alarm sound.
	Broken circuit	No alarm	Real-time pushing of "tamper alarm" information and one alarm sound

4.6 Wiring of Expansion Board

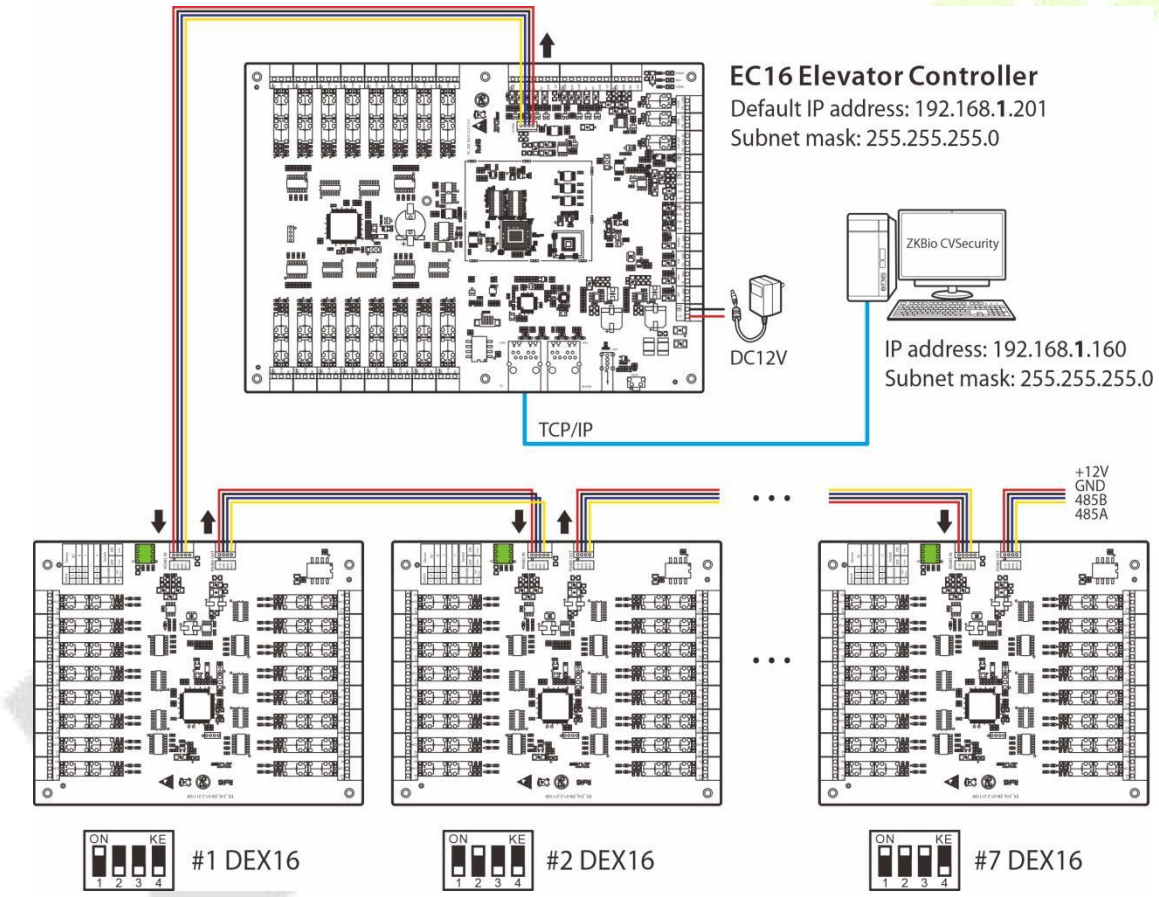


Figure 4-7 MO, EMG, FIRE, TAMPER interface wiring diagram

Note:

1. *Use the software setup after connecting the DEX16 module to the EC16 master controller.*
2. *A maximum of seven DEX16 extended boards can be connected to one EC16 controller.The total can be expanded to 128 layers at most.*
3. *Before power is supplied, use the DIP switch to set the RS-485 addresses of the DEX16s, following the order in which each DEX16 is connected.*
4. *The DIP switch needs to be set with the control board powered off and takes effect after restart. After setting, the DIP switch does not need to be set back to its original position.*

4.7 Installation of Elevator Management System

The elevator management system consists of two parts, which are the management workstation (PC) and the elevator controller. The management workstation and elevator controller adopt TCP/IP communication mode. The communication line is as far away from the high-voltage electric line as possible, and should not be wired in parallel with the power line, let alone bundled together.

The management workstation is a PC connected to the network, and the elevator manager can realize various remote management functions, including adding/removing users, viewing various event records, entering/exiting elevators and monitoring the status of each elevator in real time, etc. just by running the elevator control management software on it.

The following diagram shows the installation of EC16 elevator controller system.

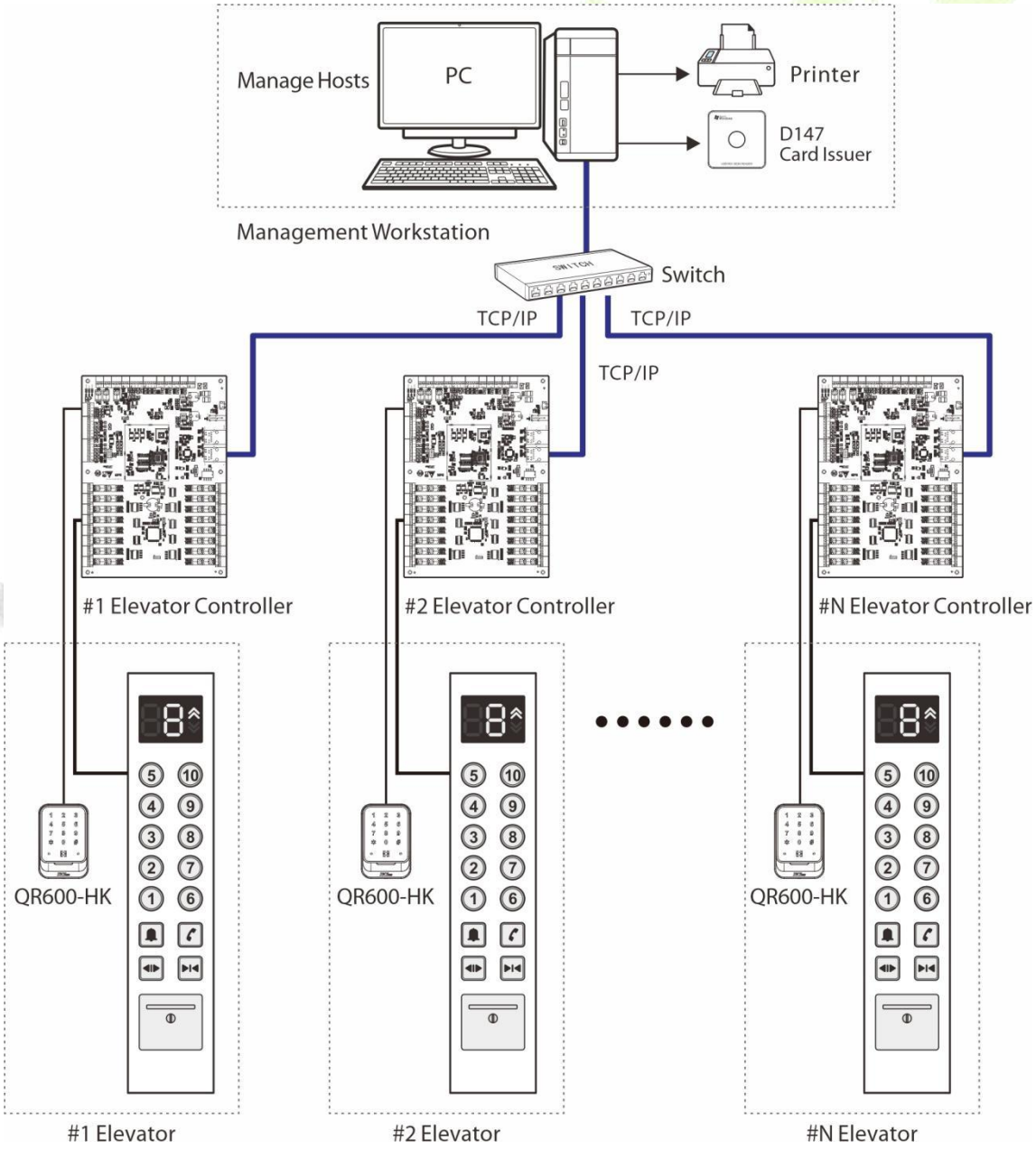


Figure 4-8 Diagram of elevator management system

4.8 Elevator Controller System Power Supply Structure

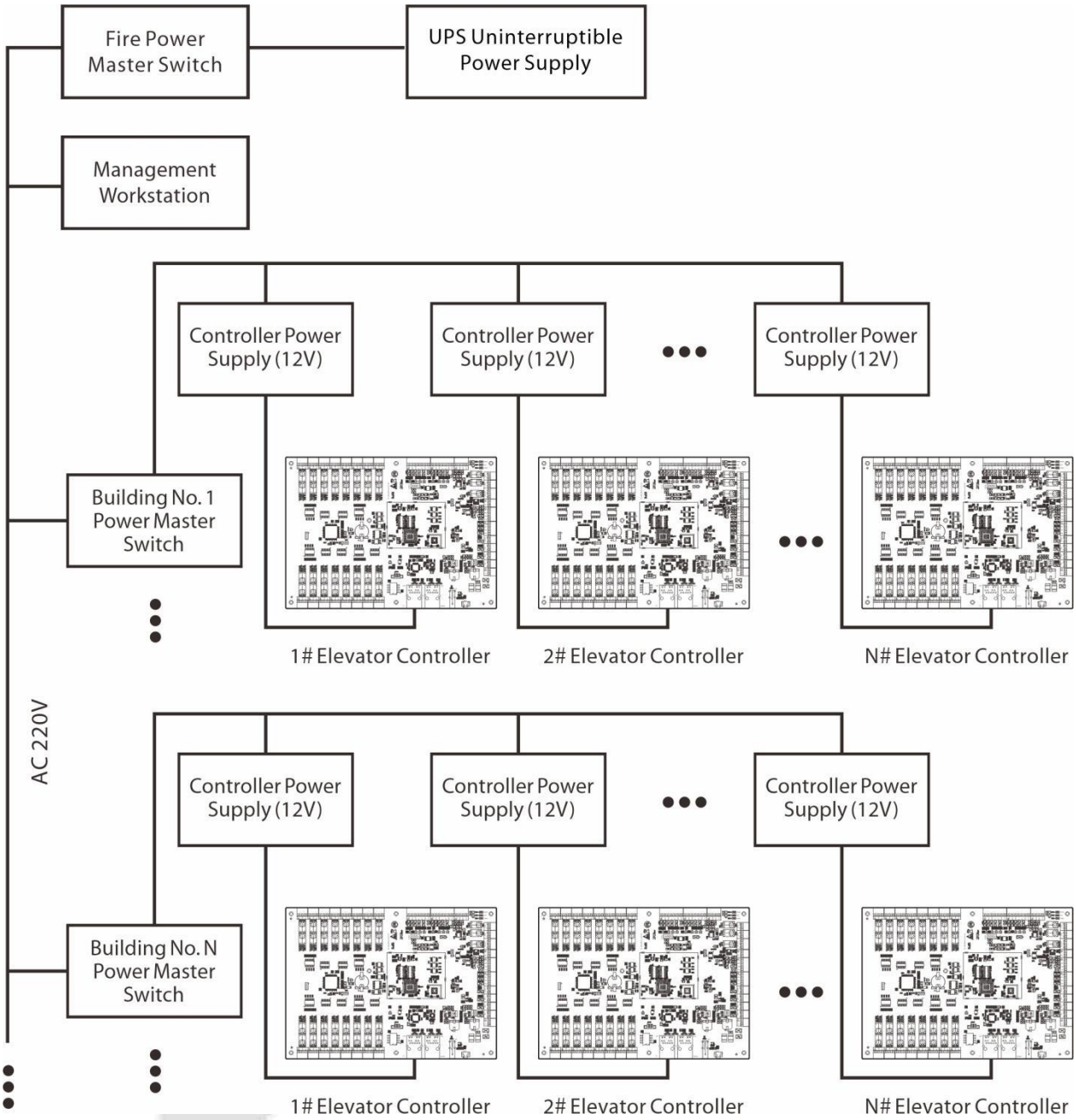


Figure 4-9 Diagram of elevator controller system power supply structure

The EC16 elevator controller is powered by +12V DC power supply.

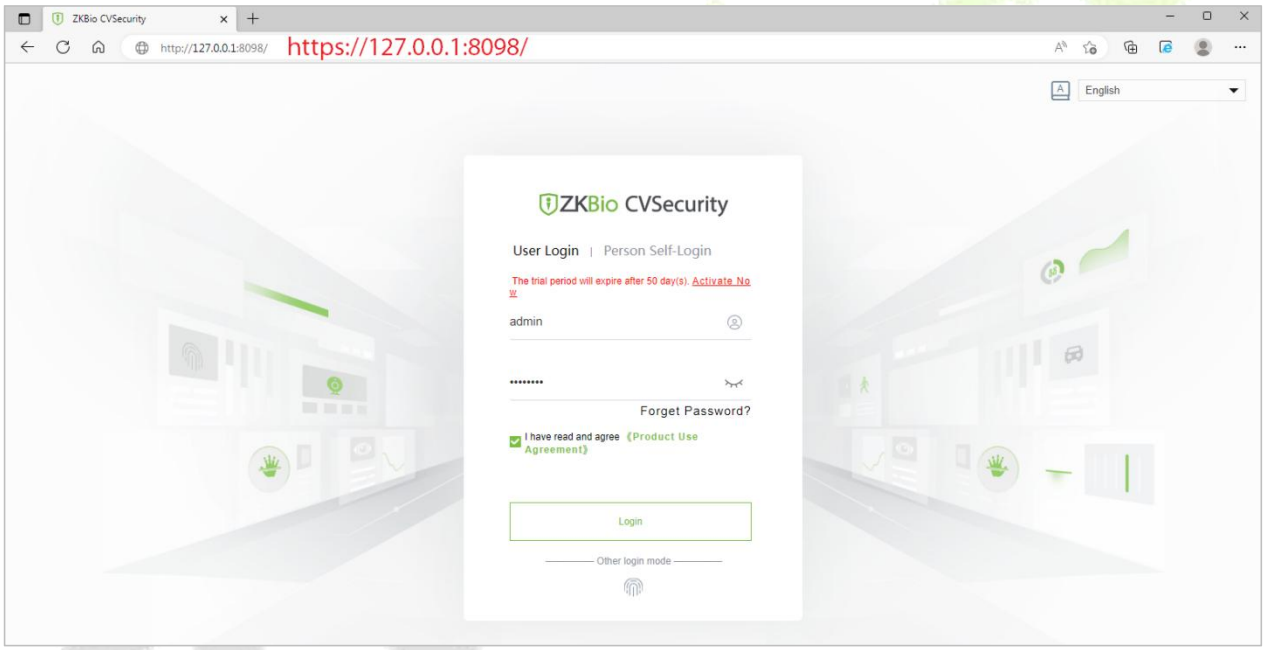
When using +12V DC power supply, generally speaking, in order to reduce the influence of power interference between elevator controllers, each elevator controller should be powered separately. In order to prevent the loss of power to the elevator controller and cause the whole system to fail to work normally, the elevator management system is generally required to be equipped with at least one UPS uninterruptible power supply.

5 Elevator control operating instructions

5.1 Connect to ZKBio CVSecurity Software

The elevator controller needs to be connected to the software and set the corresponding parameters to use the elevator control function in the software system, and can manage the equipment through the system, upload the user's elevator control data, download the configuration information and output various reterminals to realize the digital management of the enterprise.

5.1.1 Login Software



1. Open your browser, enter the server IP address and terminal number (e.g. https://127.0.0.1:8098/) in the address bar, click **Enter** to enter the login page.
2. Or double-click the desktop the ZKBio CVSecurity icon to bring up the system login page.
3. For the first time to use this system, default user name admin and password admin, click **[Login]**, or click **[Fingerprint Login]** on the interface, then press the administrator finger on the fingerprint device to enter the system home page.
4. To use this system for the first time, enter the default user name **admin** and password **admin** and click [**Login**]. Or click the icon of **Other login mode** on the interface, then press admin finger on the fingerprint device to enter the system home page.

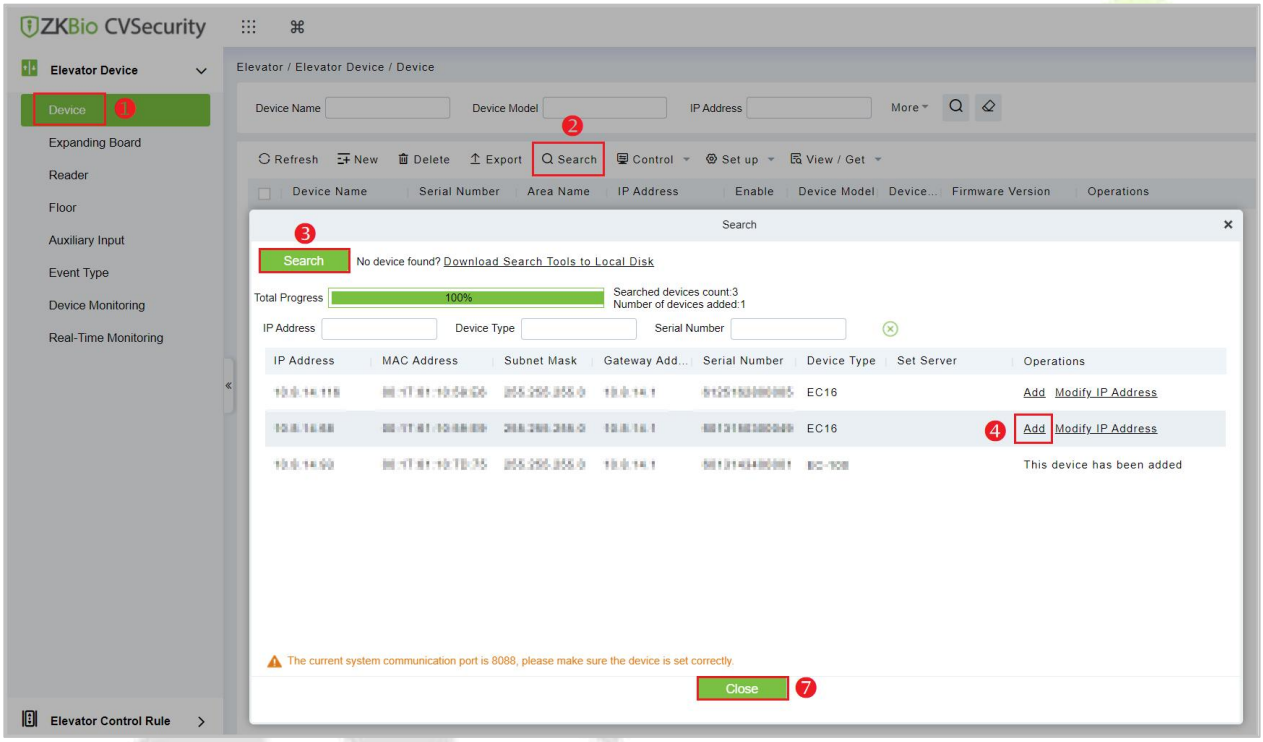
Note:

1. *To ensure the safety of using the system, you must change the default password after logging into the system.*
2. *For more details, please refer to the ZKBio CVSecurity User Manual.*

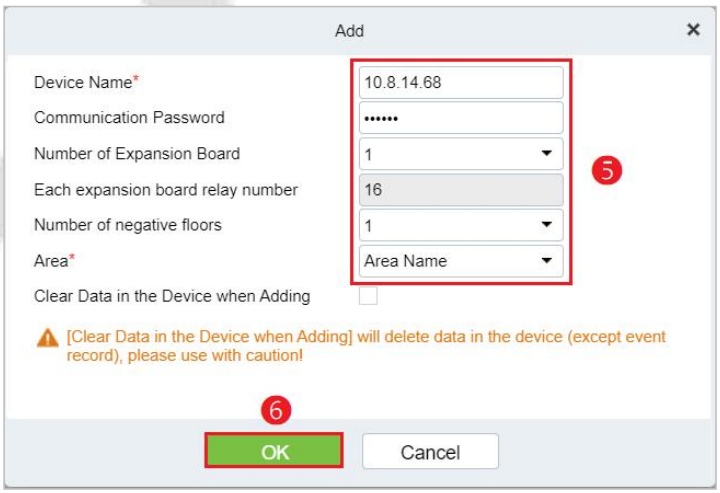
5.1.2 Add Device on the Software

Add elevator control device by searching, the operation process is as follows.

1. Click [**Elevator**] > [**ElevatorDevice**] > [**Device**] > [**Search**], to open the Search interface in the software.
2. Click [**Search**] on the pop-up search page.
3. After the search is completed, the list and total number of elevator controllers will be displayed.



4. Click the [**Add**] button after the device and make sure to finish adding it.



5. Set the relevant parameters.
6. Click [**OK**] to complete the operation of adding elevator control device.
7. Click [**Close**] to close the Device Search Add interface.

Note:

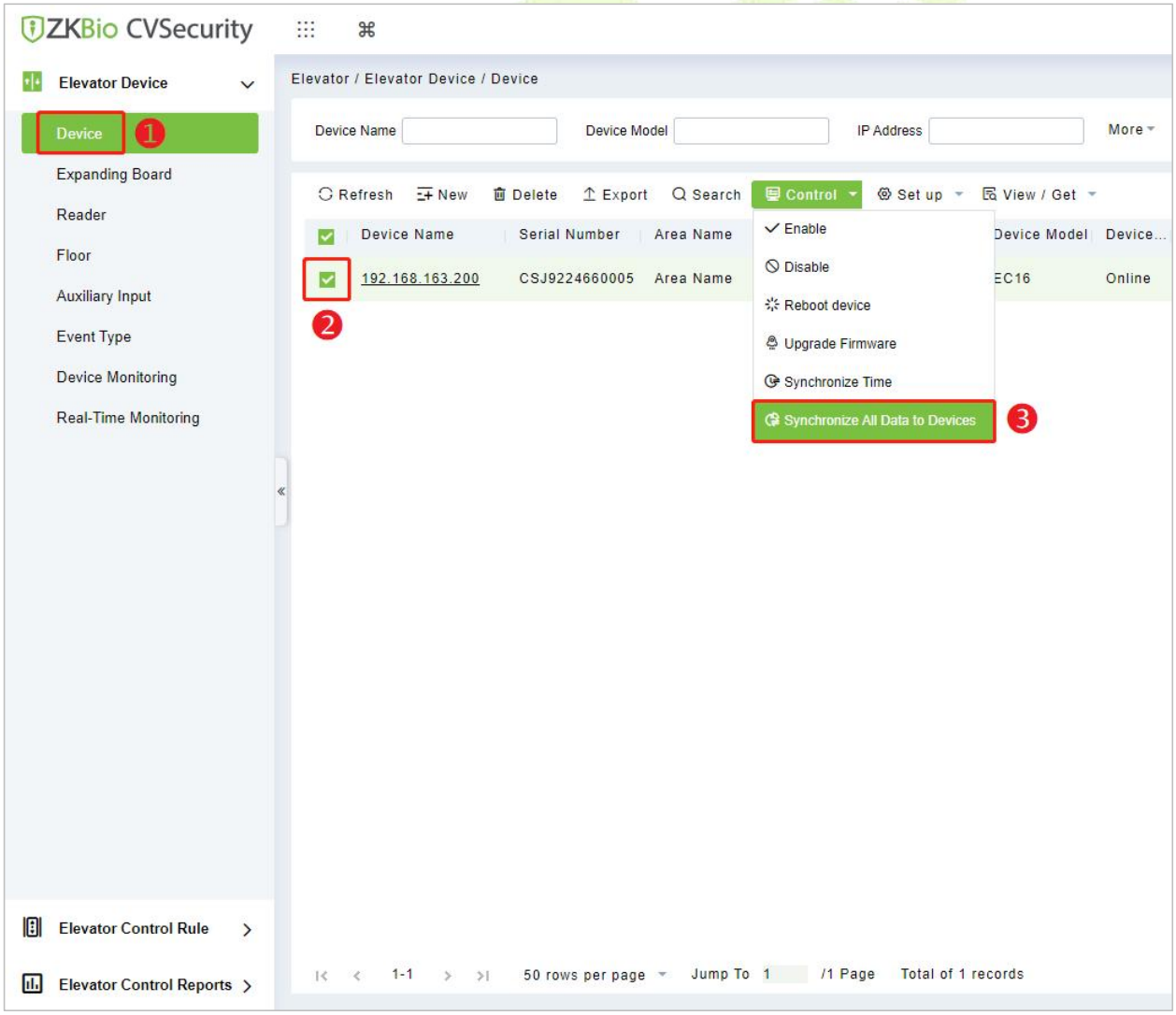
When the device cannot be added to the software, please check the following information.

1. *When the device can not be added, please check whether the communication is HTTP or HTTPS.*
2. *Whether PC and Elevator control device can PING through.*
3. *Whether the corresponding server IP of the device is correct.*

5.1.3 Synchronize All Data to Devices

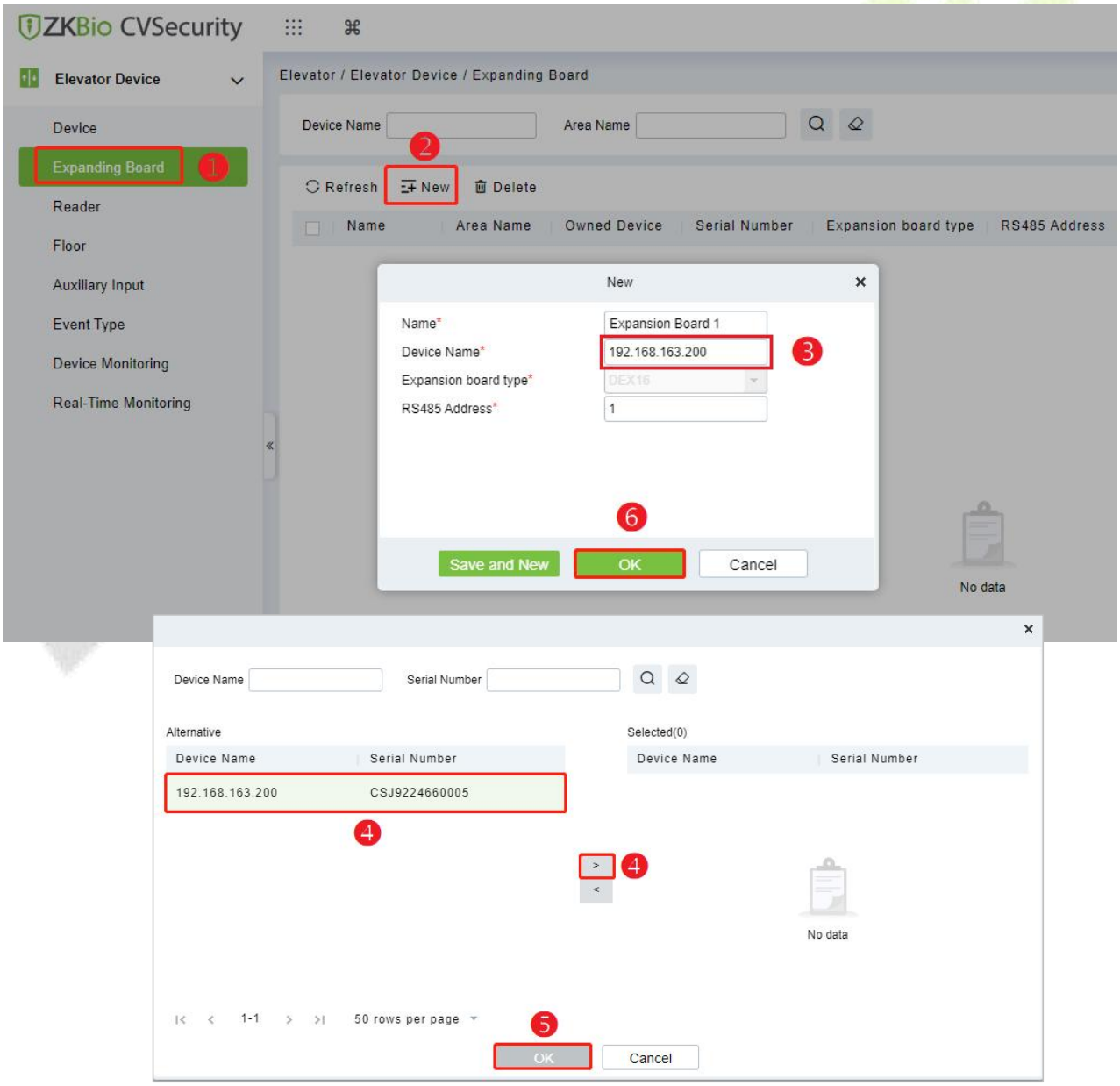
Register user and send to elevator control device. The operation steps are as follows.

1. Click [**Personnel**] > [**Personnel**] > [**Person**] > [**New**] to register users in the software.
2. Add users to elevator control level.
3. Click [**Elevator**] > [**Device**] > [**Control**] > [**Synchronize All Data to Devices**] to synchronize all data to the controller, including new users.



5.1.4 Add Expansion Board on the Software

1. Click [**Elevator**] > [**Elevator Device**] > [**Expanding Board**] to enter the setting interface.
2. Click[**New**] to add a expanding board.
3. Click [**Device Name**] and select the expansion board in the pop-up window.
4. Select the expansion board and then click > to move it to the selected column on the right.
5. Click [**OK**] to confirm and exit.
6. After setting all parameters, click [**OK**] on the New page, when the pop-up "The operation succeeded!" prompt means add expansion board is completed.



Note: *The RS485 address is input according to the dip switch setting of the expansion board, check the dip switch setting in [4.6 Wiring of Expansion Board](#) for details.*

5.1.5 Add Reader on the Software

EC16 elevator controller supterminals connecting Wiegand or RS-485 communication reader.

5.1.5.1 Connect RS-485 Reader via RS-485

1. Connect the VCC, GND, 485A and 485B terminals of the reader to the RS-485 communication terminal of the elevator controller, and the wiring is shown in the following figure.

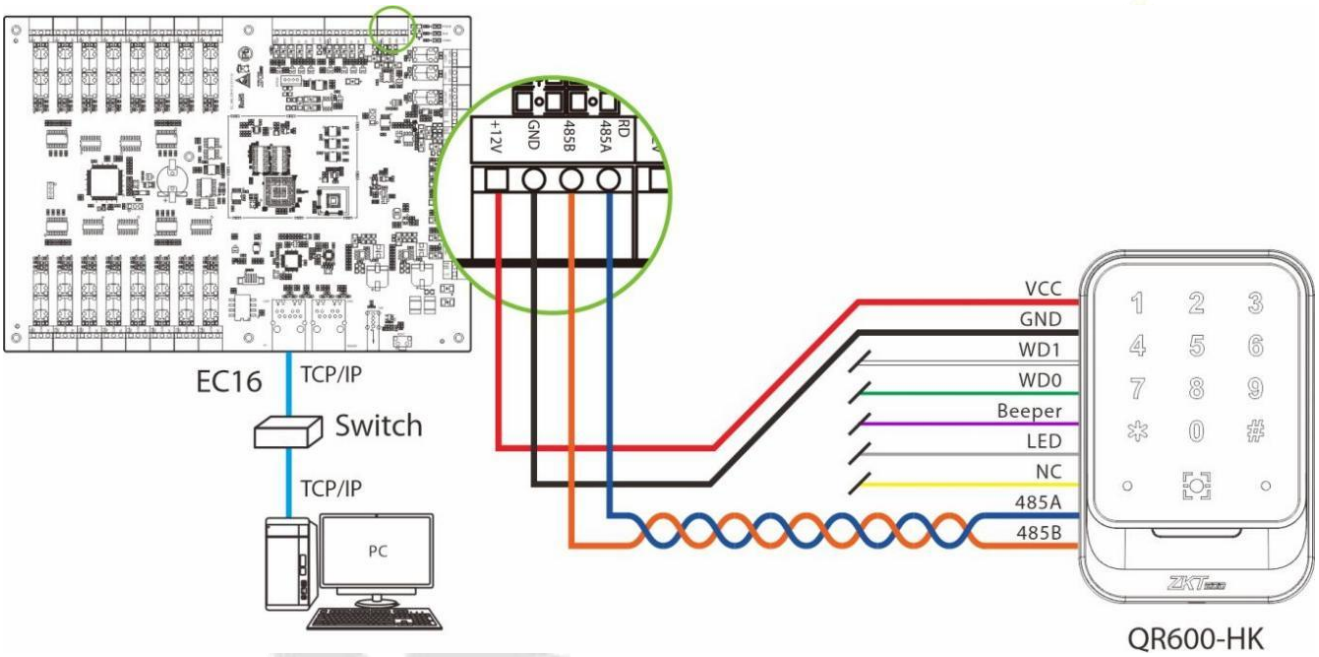


Figure 5- 1 Wiring Schematic of RS-485 Reader and EC16 Elevator Controller

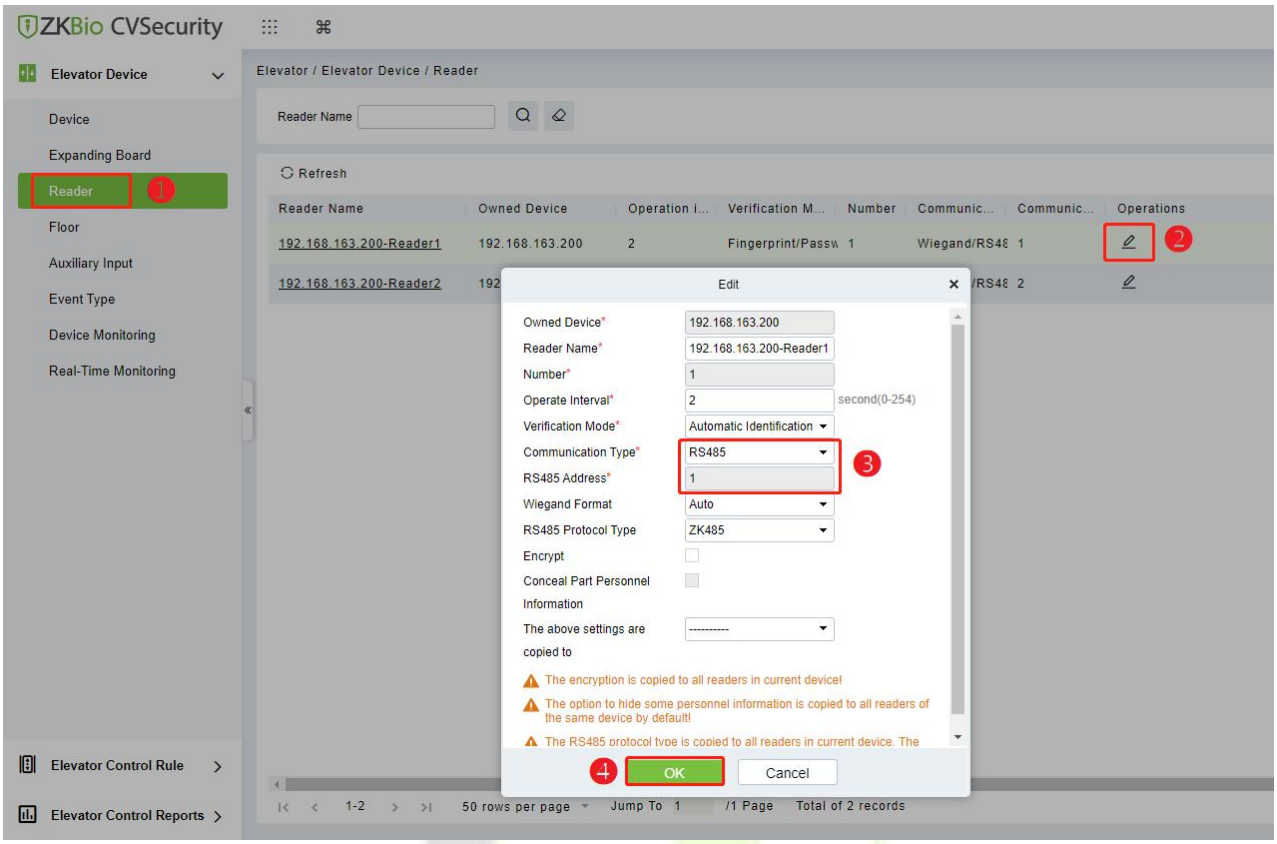
2. Set the 485 addresses (machine number) of the reader by software.

1) Click [**Elevator**] > [**Elevator Device**] > [**Reader**] to enter the setting interface.

2) Select the reader and click [**Edit**] icon behind it to enter the editing screen.

3) Change the communication type of the reader to RS485 in the edit window and enter the RS485 address.

4) Click [**OK**] to confirm and exit, as shown in the figure below.



3. Each EC16 can connect a maximum of two RS-485 readers, as shown in the figure below.

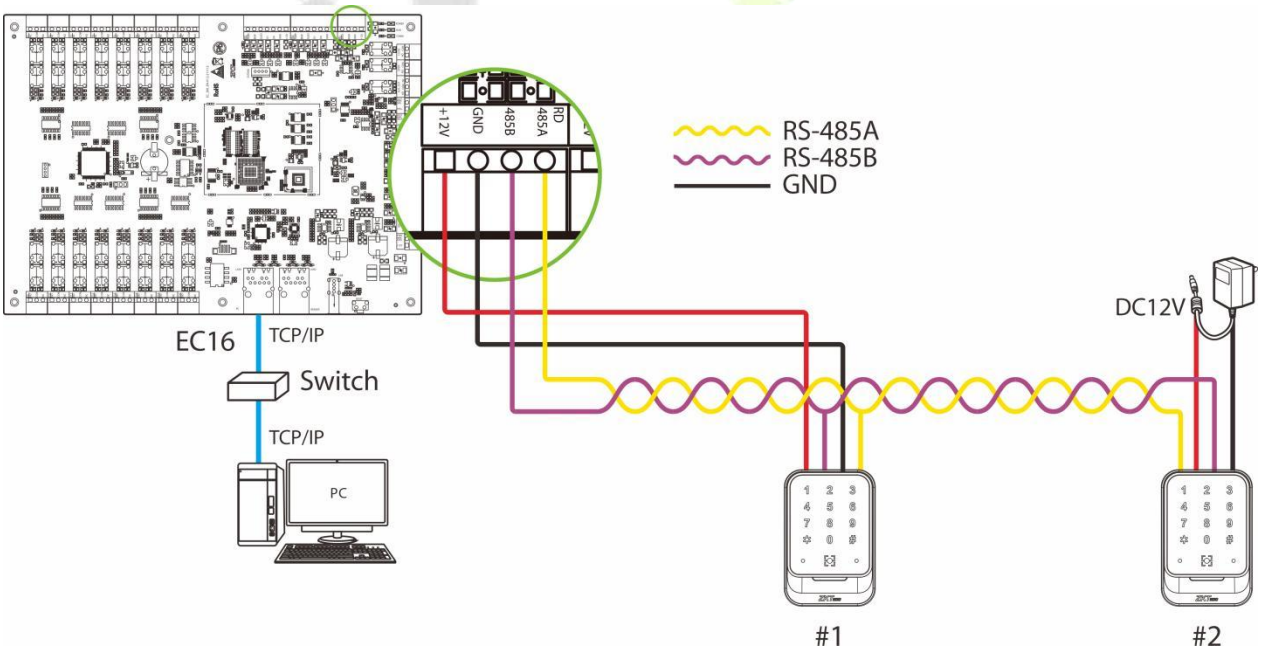


Figure 5- 2 Wiring diagram of elevator controller and multiple RS-485 readers

Remarks:

When connecting the RS-485 readers through the RS-485 communication terminal of the elevator controller, it can provide a maximum current output of 3A (12V), so when using the power output of the RS-485 communication terminal to supply power to multiple readers, the overall working current of the reader cannot exceed this value and should be left with sufficient margin. In the calculation, the

maximum current for each reader is calculated (**Note:** the instantaneous current of the device at the time of start-up is the largest, which can be more than twice the normal work, and this situation must be considered when calculating). In addition, if the reader shares power with the device, it is recommended that the RS-485 communication terminal and the RS-485 reader should not be connected to more than 3937 ft (100m), otherwise it is recommended that a separate power supply be used.

Note: *For devices with high power consumption, it is recommended to use separate power supply to ensure stable operation of the device.*

5.1.5.2 Connect Wiegand Reader via Wiegand

EC16 elevator controller can connect two Wiegand readers.

The elevator controller provides Wiegand interface for the readers, which can be connected to different types of readers. If your reader uses a voltage other than DC 12V, an external power supply device is required. The reader should be installed about **55 inches (1.4m)** from the ground and **0.1 inches to 0.2 inches (30 to 50mm)** from the door edge frame.

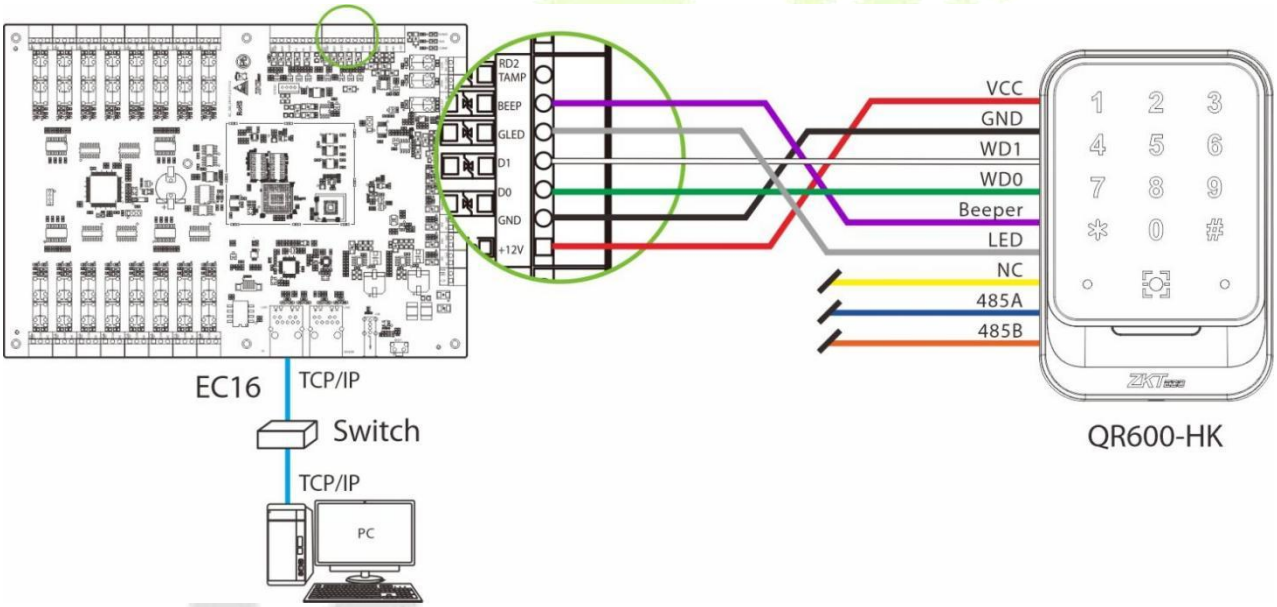


Figure 5- 3 Wiring Diagram of EC16 Elevator Controller and Wiegand Reader

5.1.6 Set Elevator Control Rules on Software

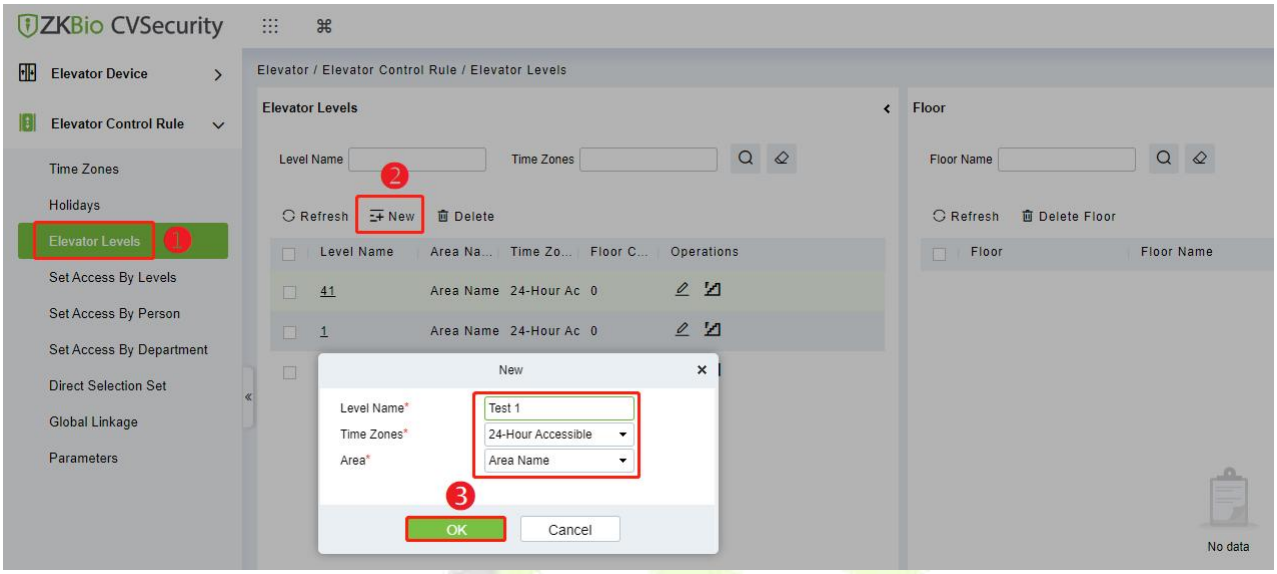
Note that when setting elevator control rules, when the "Direct Selection Set" function is set, other floor permissions such as those set in "Elevator Levels", "Set Access By Levels", "Set Access By Person", "Set Access By Department" will be invalid, when the "Direct Selection Set" function is canceled, the floor permissions set will be valid again.

Note:

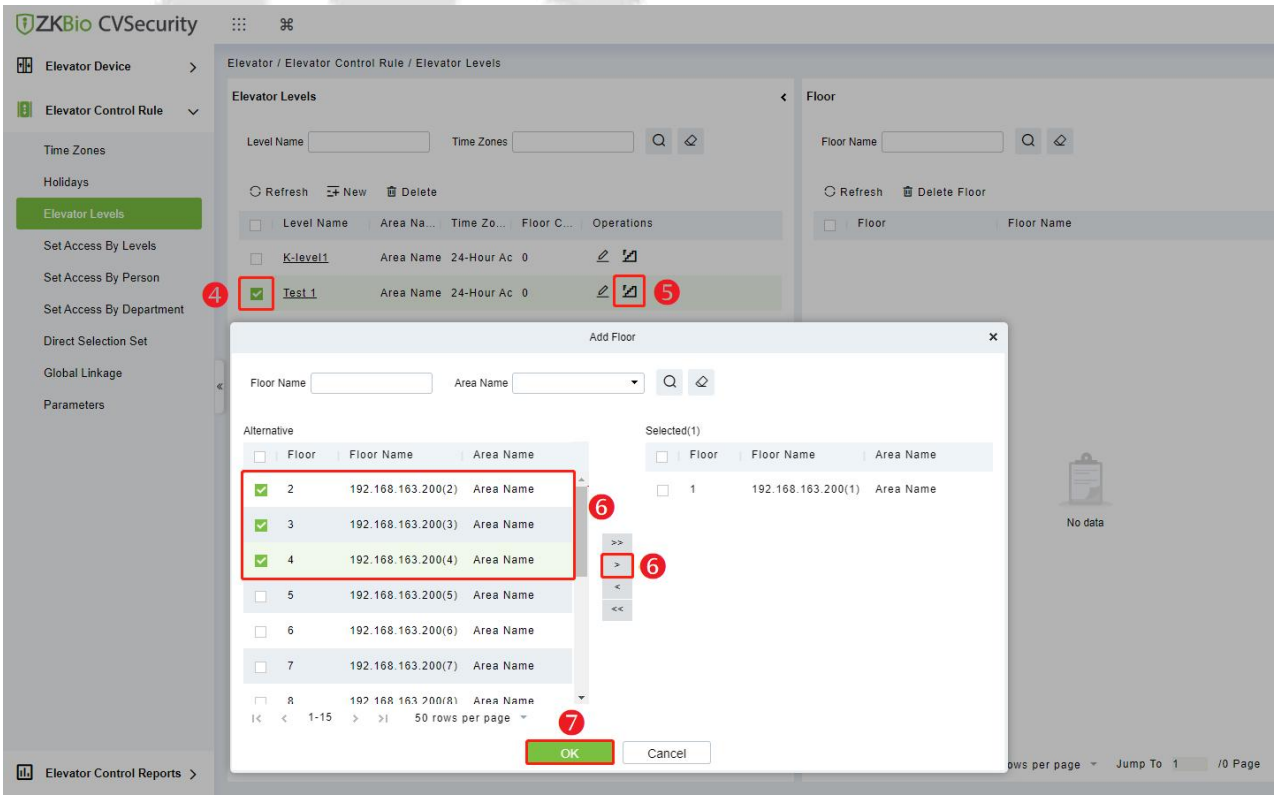
Elevator Levels, Set Access By Levels, Set Access By Person and Set Access By Department function are mainly used as visitor authority.

5.1.6.1 Set Elevator Control Levels Group

1. Click [**Elevator**] > [**Elevator Control Rule**] > [**Elevator Levels**] to enter the setting interface.
2. Click [**New**] to add a new elevator control level group.
3. Enter the level name, time zones and setting area, then click [**OK**] to confirm and exit.



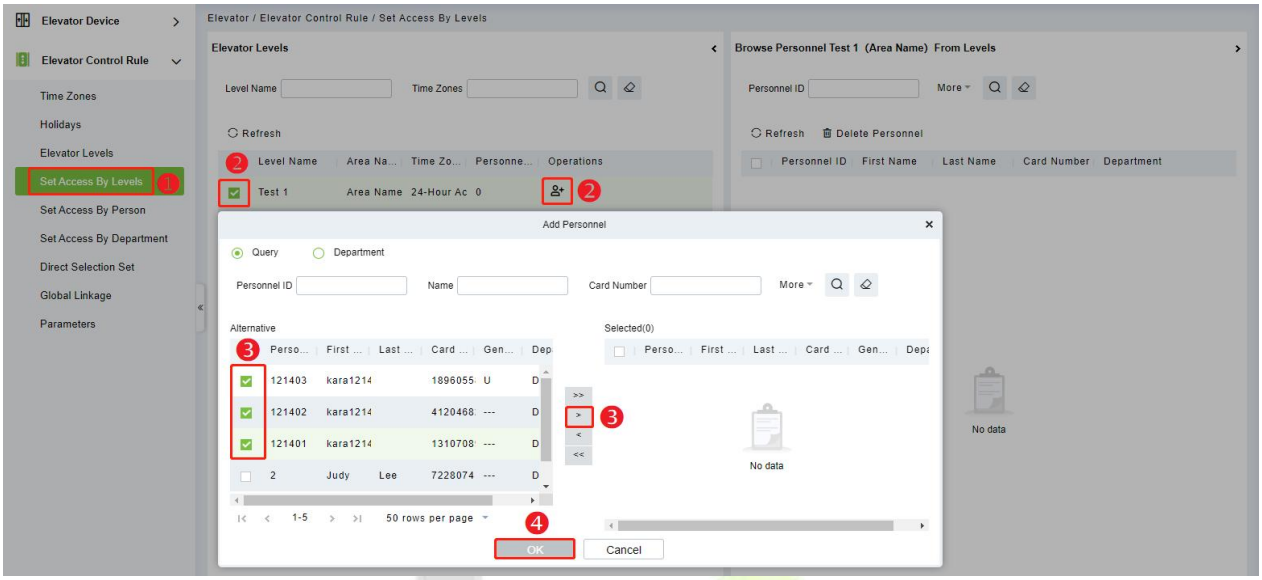
4. After adding successfully, check the levels group.
5. Click [**Add Floor**] icon in the levels group bar to open the settings window.
6. Select the floor and then click > to move it to the selected column on the right.
7. Click [**OK**] to confirm and exit.



5.1.6.2 Set Access by Levels

Add personnel to the elevator control level group.

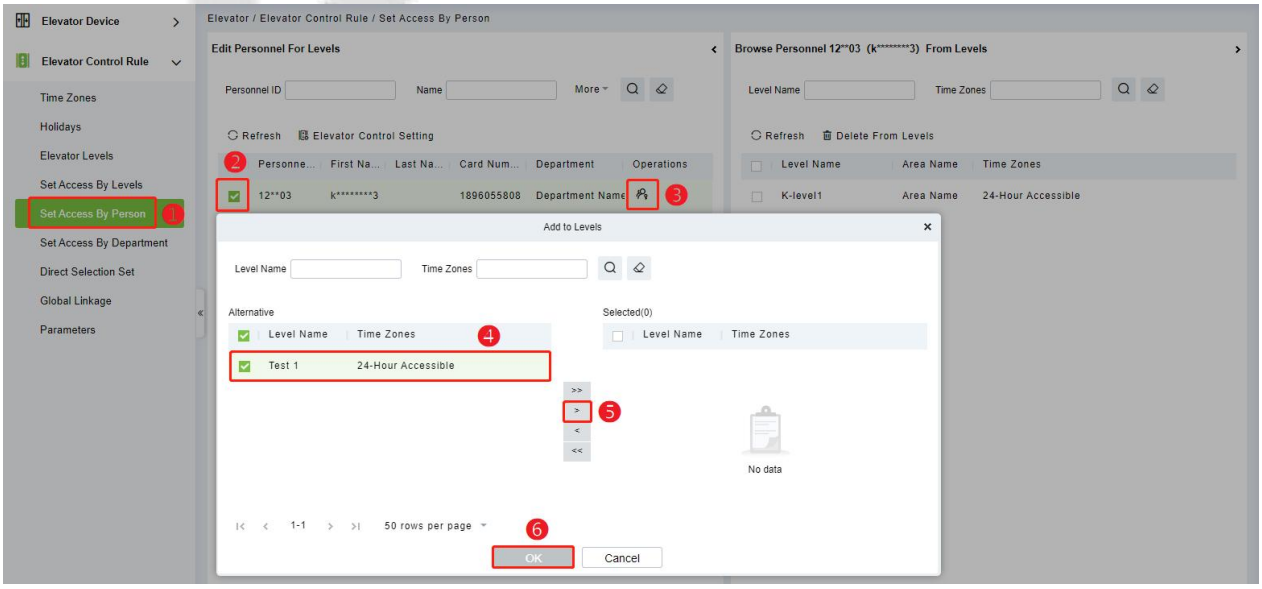
1. Click [**Elevator**] > [**Elevator Control Rule**] > [**Set Access By Levels**] to enter the setting interface.
2. Check the levels group and click the [**Add Personnel**] icon in its bar to open the settings window.
3. Select the person and then click to move it to the selected column on the right.
4. Click [**OK**] to confirm and exit.



5.1.6.3 Set Access By Person

Edit the elevator control level group for personnel.

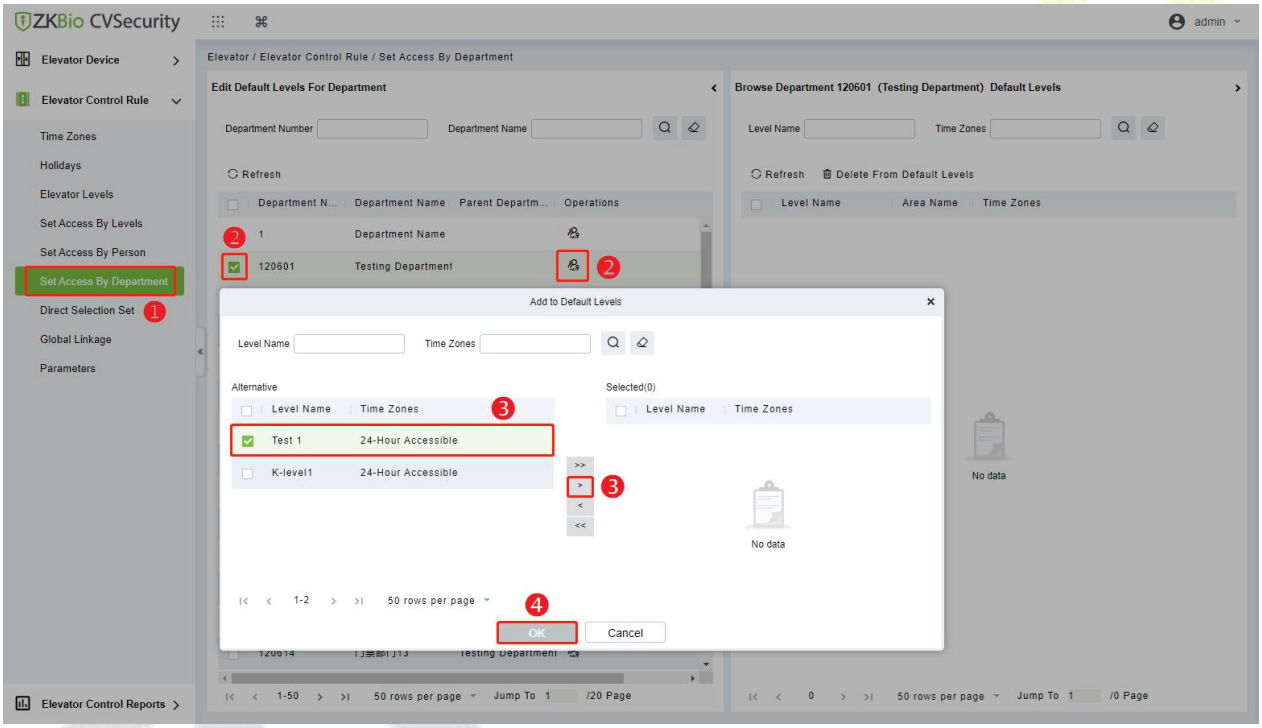
1. Click [**Elevator**] > [**Elevator Control Rule**] > [**Set Access By Person**] to enter the setting interface.
2. Check the levels group and click the [**Add to Levels**] icon in its bar to open the settings window.
3. Select the levels group and then click to move it to the selected column on the right.
4. Click [**OK**] to confirm and exit.



5.1.6.4 Set Access By Department

Edit the elevator control level group for the department.

1. Click [**Elevator**] > [**Elevator Control Rule**] > [**Set Access By Department**] to enter the setting interface.
2. Check the department and click the [**Add to Default Levels**] icon in its bar to open the settings window.
3. Select the levels group and then click > to move it to the selected column on the right.
4. Click [**OK**] to confirm and exit.

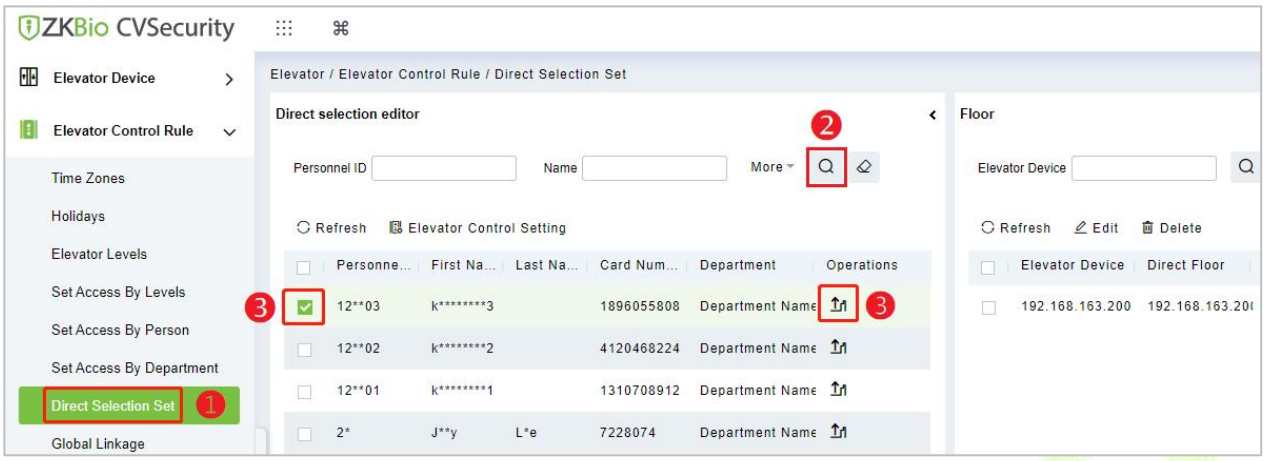


5.1.6.5 Direct Selection Floor Setting

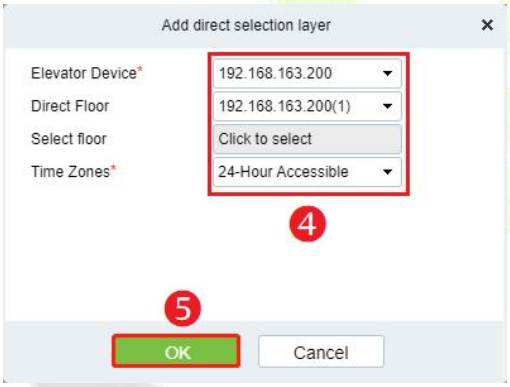
You can set a direct selection floor for users or visitors here; or set other floors that can be selected in addition to the direct selection floor.

- **Direct Selection Floor**

1. Click [**Elevator**] > [**Elevator Control Rule**] > [**Direct Selection Set**] to set the floor that can be reached directly for personnel.
2. Click the query icon to search the list of editable personnel.
3. Check the people you need to set in the list, and click icon to add direct access to the floor for the people.



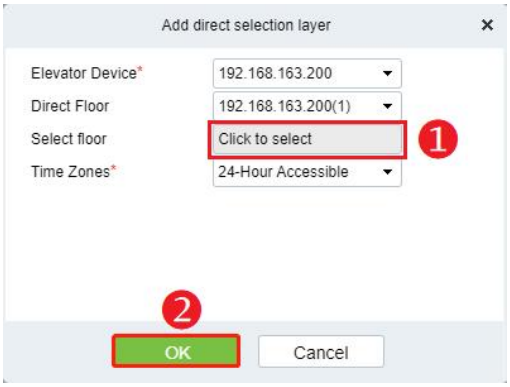
4. In the **Add direct selection layer** pop-up window, click on the drop-down menu to select the elevator device, direct floor and time zones.



5. Click [**OK**] to save and exit.

Select Floor

1. In the pop-up window of **Add direct selection layer**, click [**Click to select**] in the select floor column to select the floor.
2. Once the setup is complete, the user is allowed to access the authorized floor. Once the user is authenticated at the reader, he/she can press his/her authorized floor button directly on the floor panel to light up that floor.



Note: *Unauthorized floor buttons will not respond when pressed.*

5.2 User Verification on the QR-600 Series Readers

When the QR-600 Series Reader successfully communicates with the elevator controller (see 5.1.5 Add Reader on the Software for details on the connection method), the user can verify on the QR-600 series reader.

Users can authenticate with passwords, cards and QR codes on the QR-600 series reader. When the verification is successful, the user can reach the authorized floor.

When a user or visitor is authorized to go straight to the floor, the authorized floor is directly lit when he verifies successfully.

When a user or visitor is authorized to reach multiple floors, when he verifies successfully, he needs to manually light up the authorized floor to reach it.

Note: *Unauthorized floors will not respond when the user presses the floor button.*

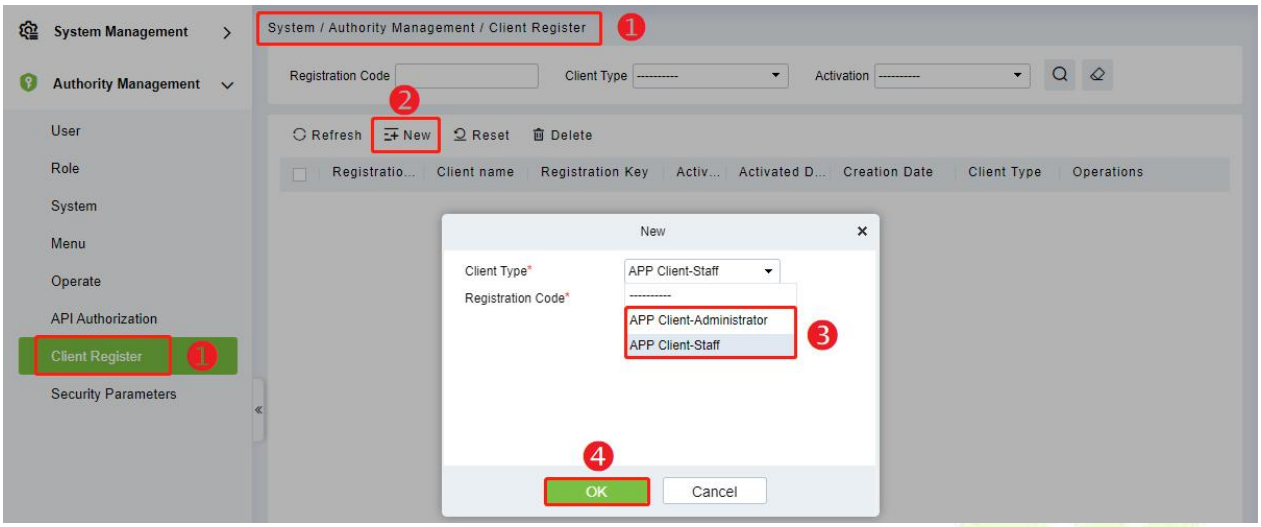
5.3 Connect to ZKBioSecurity Mobile App

Employees can install ZKBioSecurity Mobile App on the mobile phone, and can use the QR code of the electronic work card on the app to verify on QR-600 series reader to automatically light up the direct floor or manually light up the optional floor. The specific operation steps are as follows.

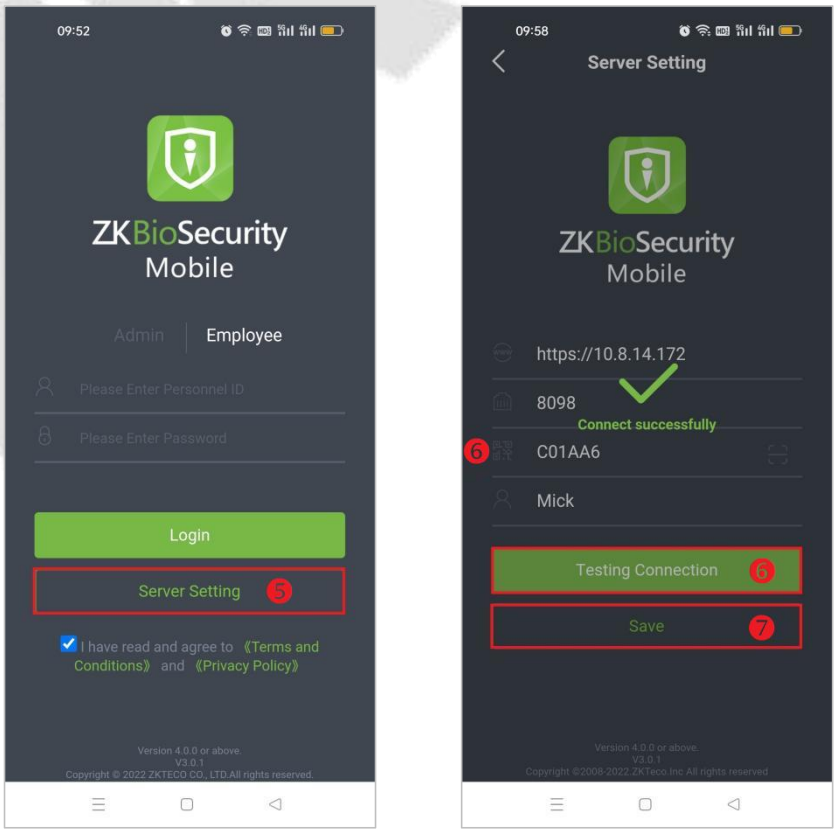
5.3.1 Mobile App Configuration

After downloading and installing the App, the user needs to set the Server before login. The steps are given below:

1. On the Server, choose [**System**] > [**Authority Management**] > [**Client Register**] to enter the Client Register interface.
2. Click [**New**] to add a registered App client.
3. Select the Registration Code. If the app is used by an administrator, register "**APP Client-Administrator**", and the mobile phone using the registration code can login to the administrator account and employee account. If the app is used by an employee, register "**APP Client-Staff**" and the mobile phone with the registration code can only login to the employee account.
4. Click [**OK**] to save and exit.



5. Open the App on the Smartphone. On the login screen, tap [**Server Setting**] and type the IP Address or the Domain Name of the Server, and its Port Number.
6. Tap the **QR Code icon** to scan the QR code of the new App client. After the client is identified successfully, set the Client Name and tap [**Testing Connection**].
7. After the network is connected successfully, tap [**Save**].

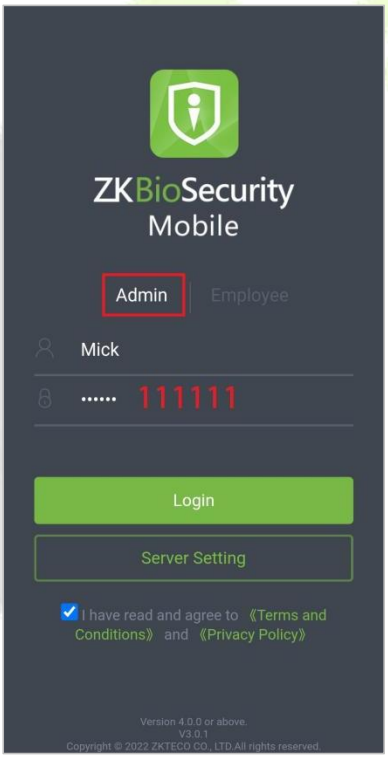


Note: *The APP's network connection and the server's network connection need to be in the same LAN, otherwise the network will be unavailable.*

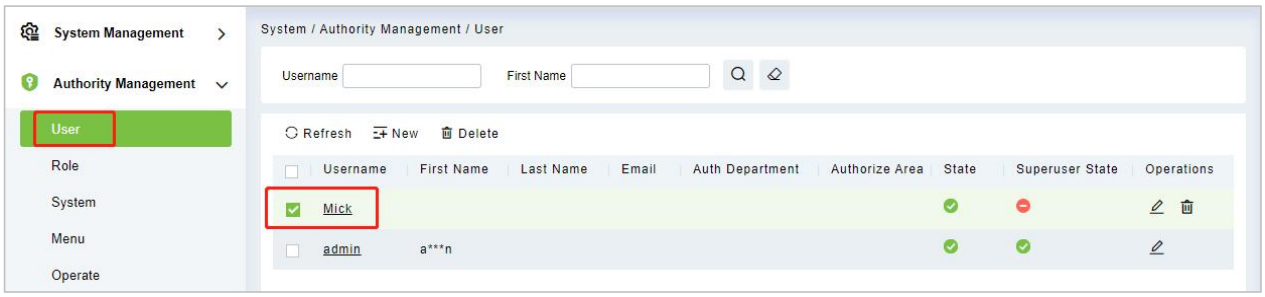
5.3.2 Login

Initially, it is required to configure the Server Settings before login. After the Server settings are successfully saved, it will automatically return to the login screen.

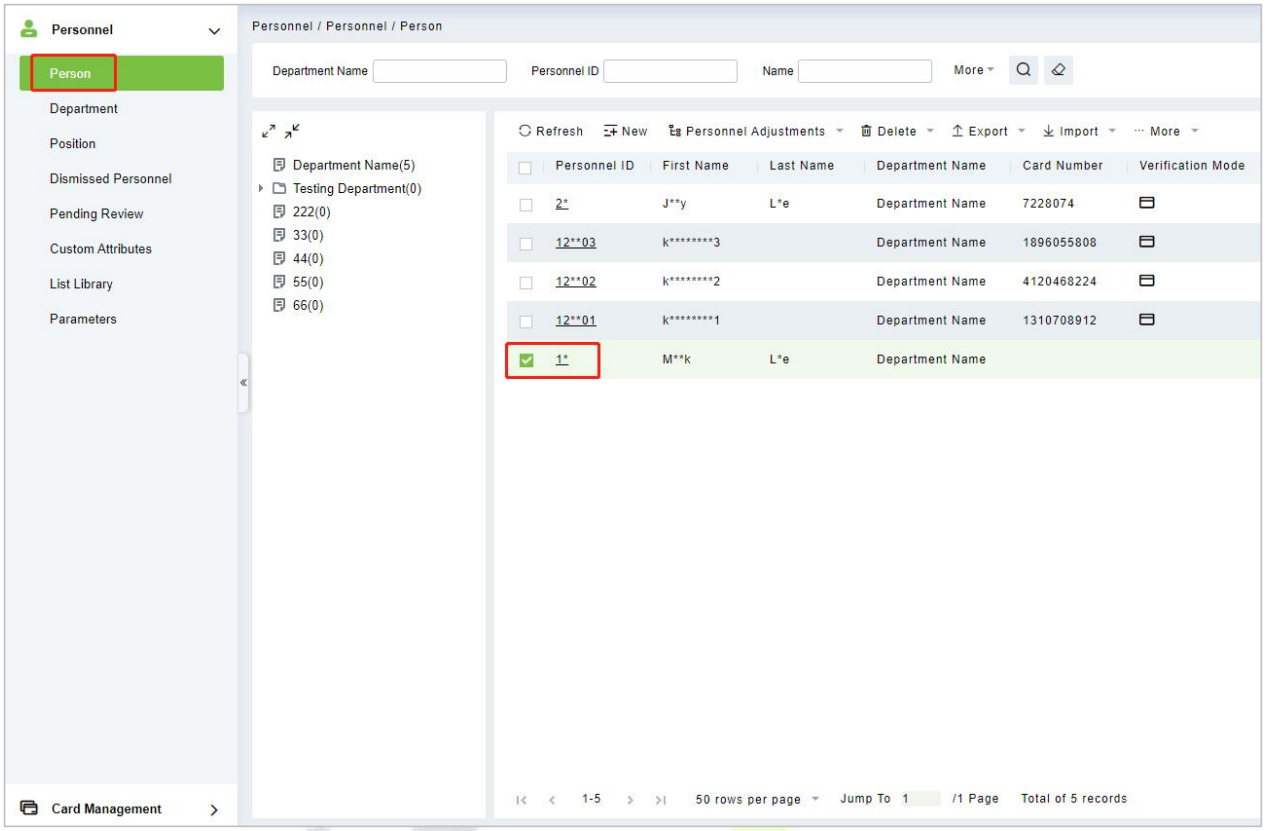
1. Select the login identity which includes **Administrator** login and **Employee** login.
2. The default is "Admin". When the Employee needs to login, tap on **Employee** to switch to Employee login screen.



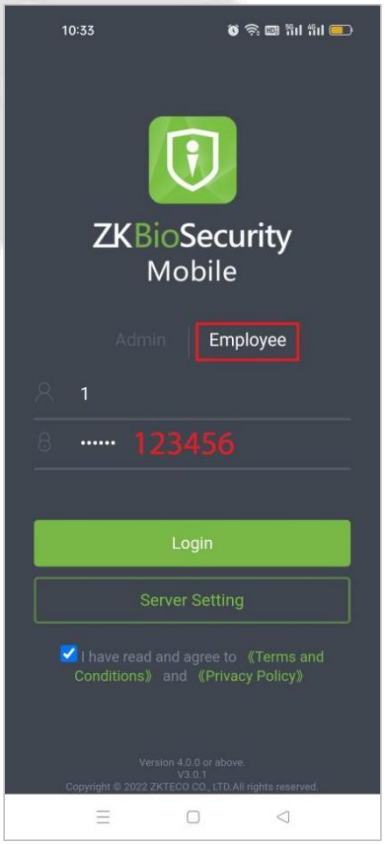
3. The administrator can login with the username in [**System**] > [**Authority Management**] > [**User**] and self-service password. The default self-service password is **111111**.



4. Employees can login with the Personnel ID in [**Personnel**] > [**Personnel**] > [**Person**] and self-service password. The default self-service password is **123456**.

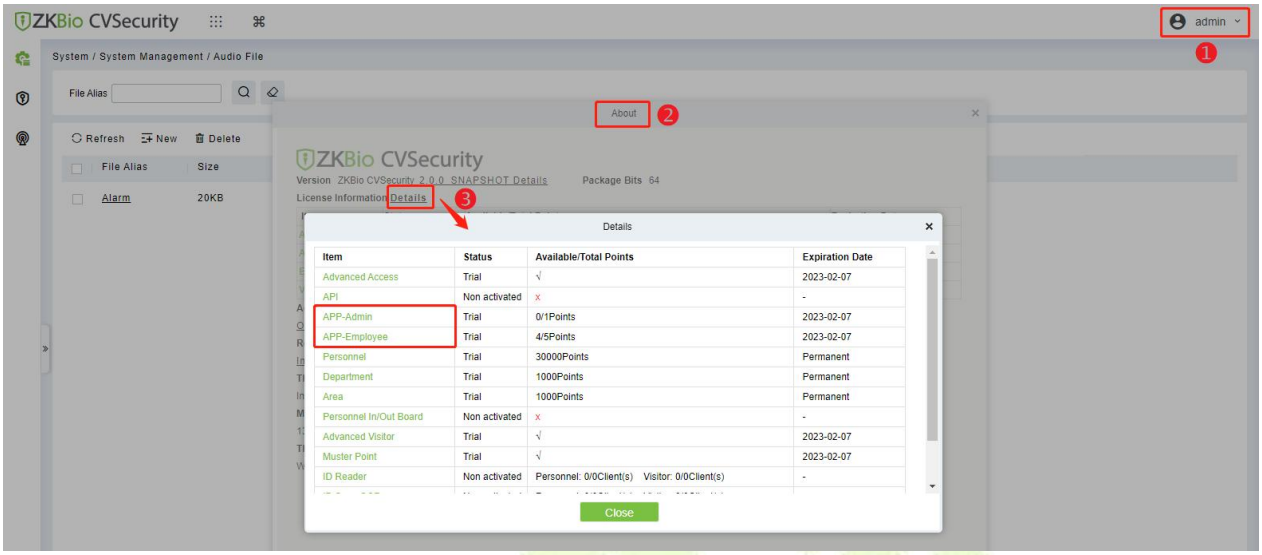


5. The employee login diagram is shown in the figure:



6. The Administrator and Employee can change the Password in the App System Settings.

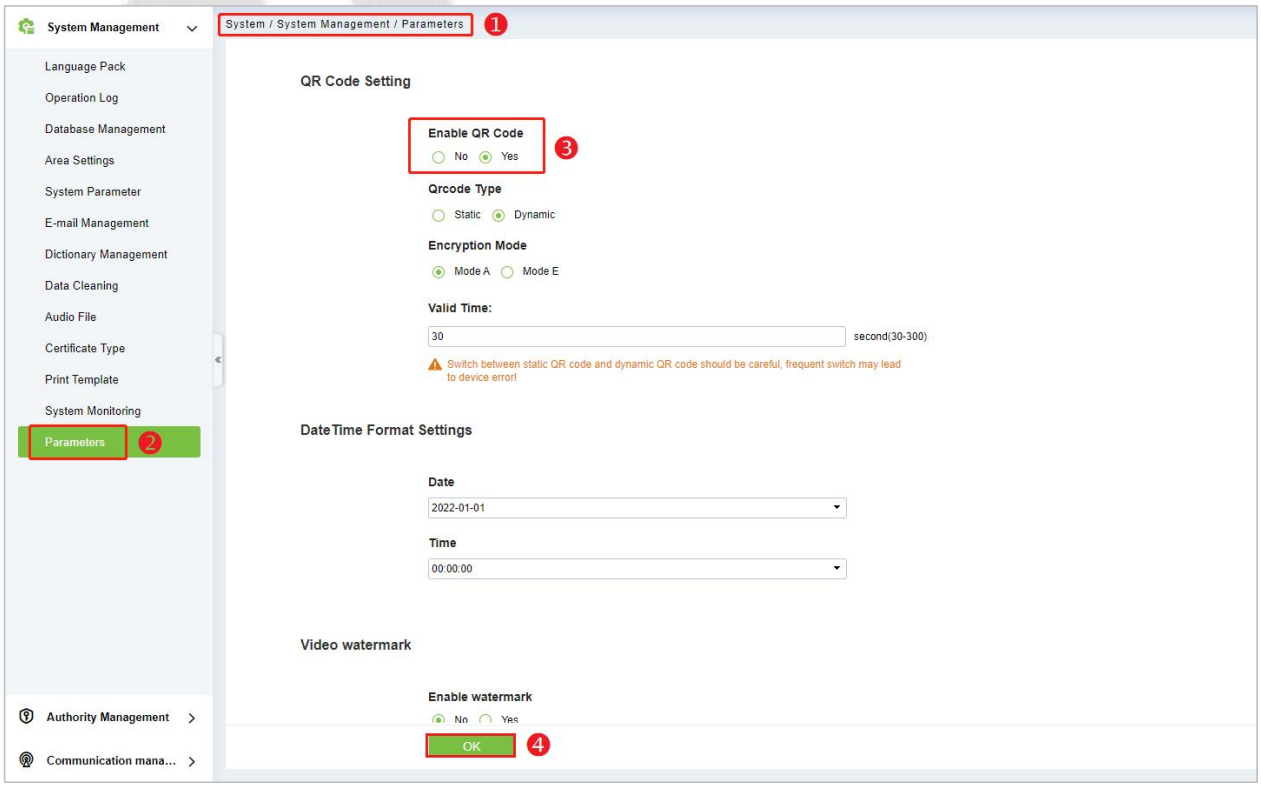
Notes: *The license determines the number of available Mobile App connections. Users can view it by clicking [**Personal Information**] > [**About Path**], as shown below.*



7. Each registration code consumes a licensed App point and can only be assigned to one mobile phone.

5.3.3 Enable the Dynamic QR Code on the Software

Open ZKBio CVSecurity software, click [**System**] > [**System Management**] > [**Parameters**] to enable the dynamic QR code. Set the relevant parameters in the page, click **OK** to save and exit. As shown in the figure below.



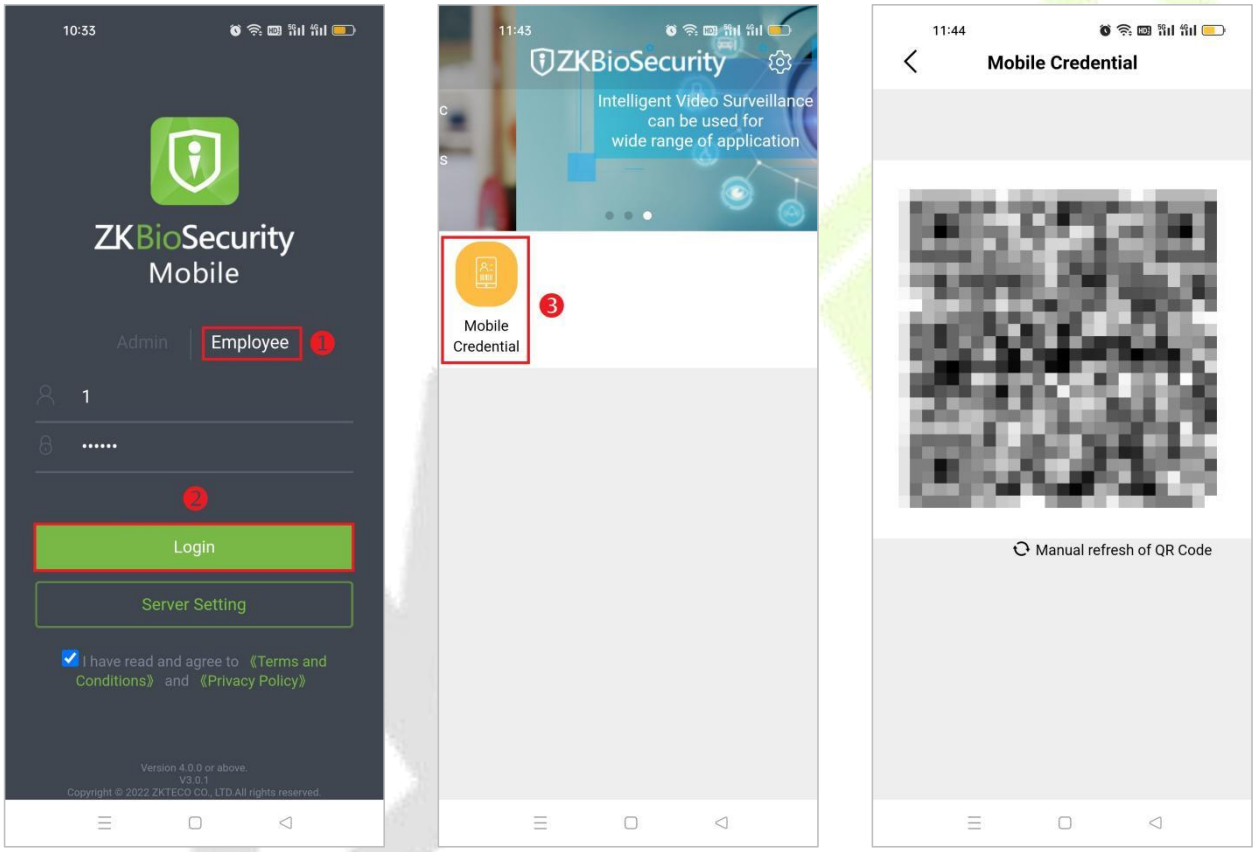
5.3.4 Verification QR Code

After logging into the ZKBioSecurity Mobile App as an employee, click on the mobile credential icon and bring up the QR code to verify on the reader. After successful verification, you can go straight to the authorized floor or you can light up the authorized floor manually.

1. Select **Employee** and enter the account information, then click **Login** to enter the App.

2. Click the **Mobile Credential** icon to enter the QR Code interface.

3. Place this QR code in front of the QR code collector of the reader for verification.



6 Communication Connection

The backend PC software is able to communicate with the system via TCP/IP for data exchange and remote management. Communication lines are as far away from high-voltage power lines as possible, and should not be wired in parallel with power lines, let alone bundled together.

6.1 Access Control Networking Wires and Wiring

1. The power supply is 12V DC converted from 220V or POE.
2. The Wiegand readers use 6-core communication shielded wires (RVVSP 6×0.5mm) (usually there are different types of wires available, namely, 6-core, 8-core, and 10-core for users to select according to the ports) to reduce interference during transmission.
3. As an electronic lock produces a big current, it generates strong interference signals during an action. To reduce the effect of an electronic lock during an action on other elements, 4-core wires (RVVP 4×0.75mm^2, two for a power supply and two for a door sensor) are recommended.
4. "EXT RS485" interface use 4-core communication shielded wires (RVVSP 4*0.5mm).
5. Other control cables like exit switches are all made of 2-core wires (RVVSP 2×0.5mm^2).
6. Notes for wiring:
   - ✧ Signal wires (like network cables) can neither run in parallel with nor share one casing pipe with large-power electric wires (like electronic lock wires and power cables). If parallel wiring is unavoidable for environmental reasons, the distance must be over 50cm.
   - ✧ Try to avoid using any conductor with a connector during distribution. When a connector is indispensable, it must be crimped or welded. No mechanical force can be applied to the joint or branch of conductors.
   - ✧ In a building, distribution lines must be installed horizontally or vertically. They should be protected in casing pipes (like plastic or iron water pipes, to be selected according to the technical requirements of indoor distribution). Metal hoses are applicable to ceiling wiring, but must be secure and good-looking.
   - ✧ Shielding measures and shielding connection: If the electromagnetic interference in the wring environment is found strong in the survey before construction, it is necessary to consider shielding protection for data cables when designing a construction scheme. Overall shielding protection is required if there is a large radioactive interference source or wiring has to be parallel with a large-current power supply on the construction site. Generally, shielding measures include: keeping a maximum distance from any interference source, and using metal wiring troughs or galvanized metal water pipes to ensure reliable grounding of the connection between the shielding layers of data cables and the metal troughs or pipes. Note that a shielding enclosure can have a shielding effect only when it is grounded reliably.
   - ✧ Ground wire connection method: Reliable large-diameter ground wires in compliance with applicable national standards are needed on the wiring site and should be connected in a tree form to avoid DC loop. These ground wires must be kept far away from lightning fields. To ensure that there is no lightning current through any ground wire when there is lightning, no lightning conductors can be used. Metal wiring troughs and pipes must be connected continuously and reliably and linked to ground wires through large-diameter wires. The impedance of this section of wire cannot exceed 2ohm. The shielding layer also must be connected reliably and grounded at one end to guarantee uniform current direction. The ground wire of the shielding layer must be connected through a wire with large-diameter (not smaller than 2.5mm^2).

6.2 TCP/IP Communication

The Ethernet 10/100Base-T Crossover Cable, a type of crossover network cable, is mainly used for cascade hubs and switches, or used to connect two Ethernet end-points directly without a hub. Both 10Base-T and 100Base-T are supterminaled.

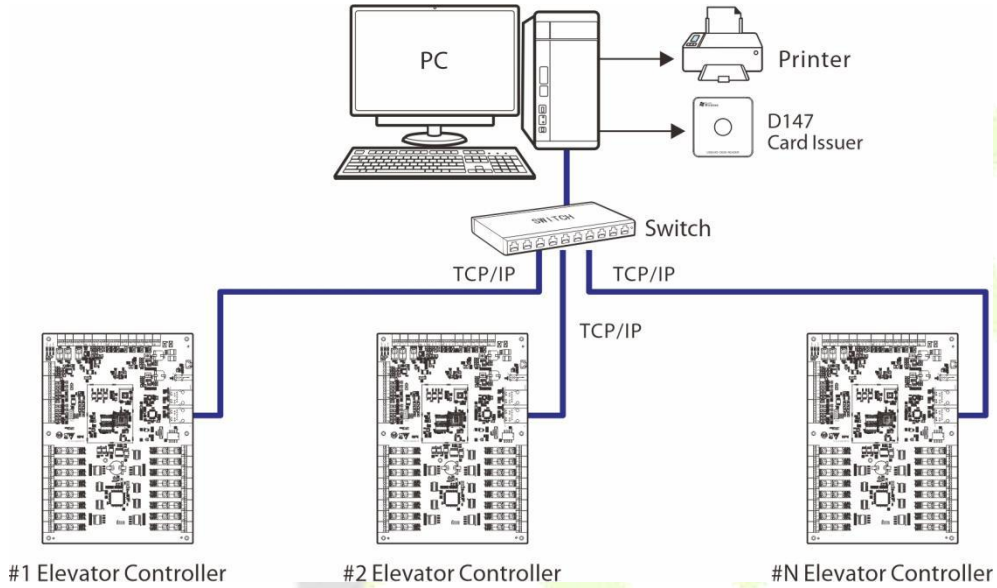
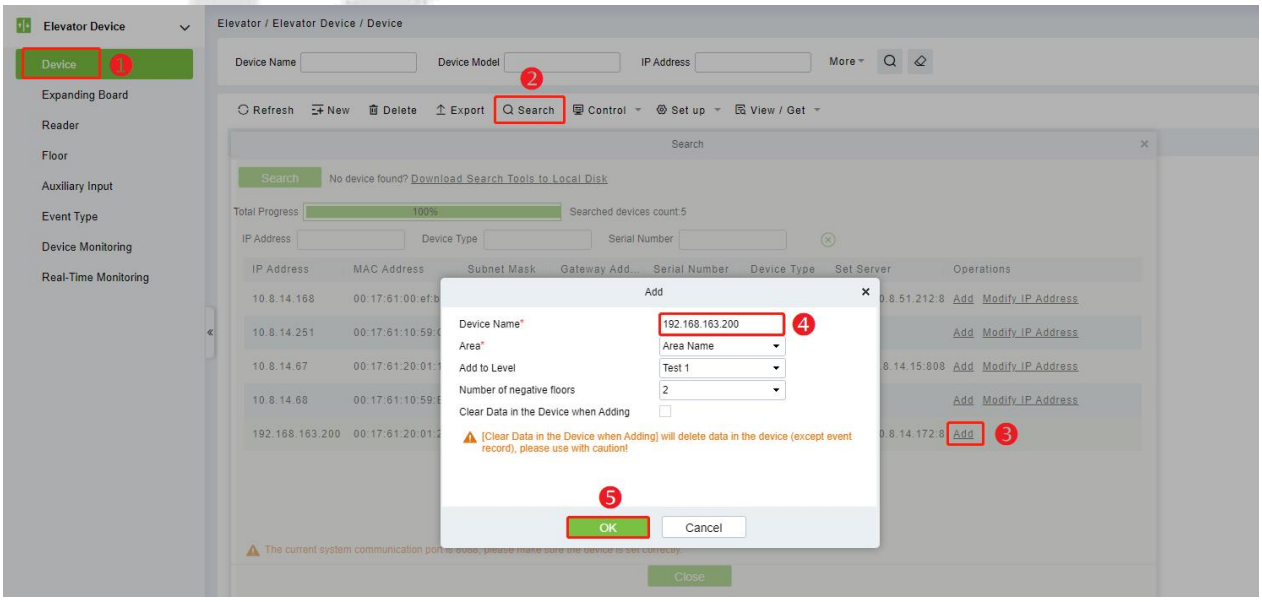


Figure 6-1 Diagram of TCP/IP communication

1. In ZKBio CVSecurity software, click [**Elevator**] > [**Elevator Device**] >[**Device**] to enter the setting interface.
2. Click [**Search**] to open the Search interface in the software.
3. After the search is completed, a list of controllers will be displayed. Select the controller in the list and click [**Add**] behind the action bar.
4. In the Add window, enter the relevant parameters for the controller.
5. Click [**OK**] to save and exit.



6. The factory default IP address of the device is: 192.168.1.201, after the device is added successfully, you can modify the IP address of the device in the communication column. Select the device, click **[Elevator] > [Elevator Device] > [Set up] > [Modify IP Address]**, modify the IP address of NIC 1 and click [**OK**].

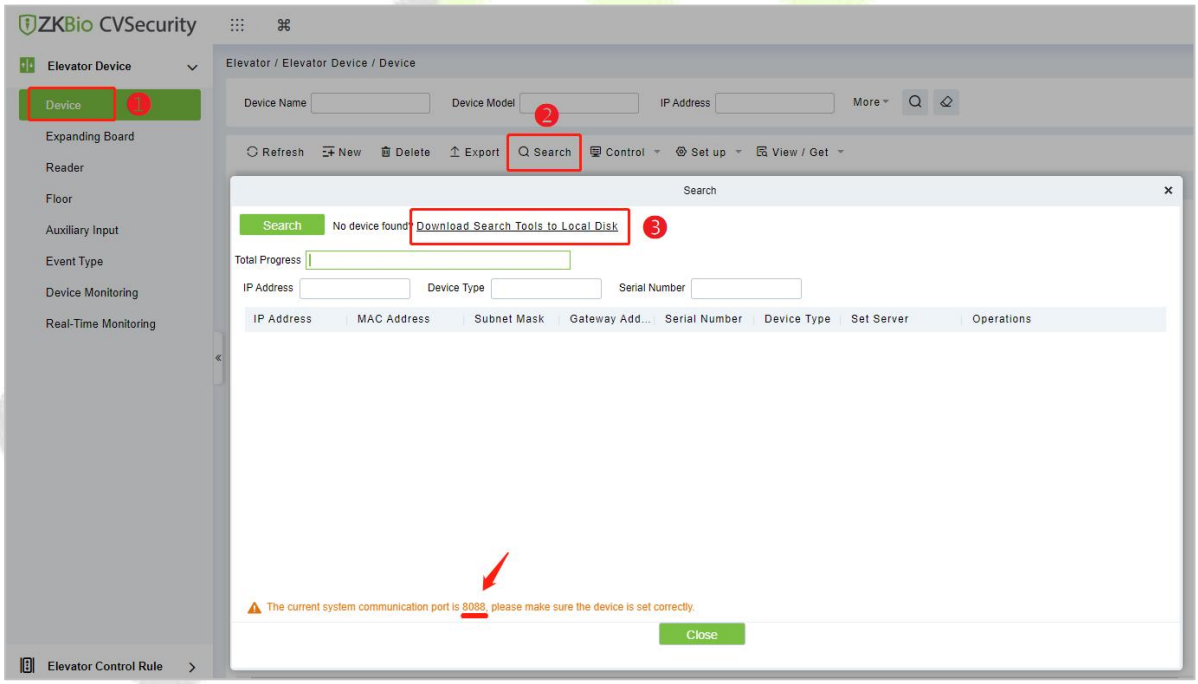
6.3 Modify the IP address

The default IP address of the primary NIC when the elevator controller is shipped is 192.168.1.201. It may conflict with the IP of other devices in the network, so the new device needs to modify the IP address before use. It can be modified by the following ways.

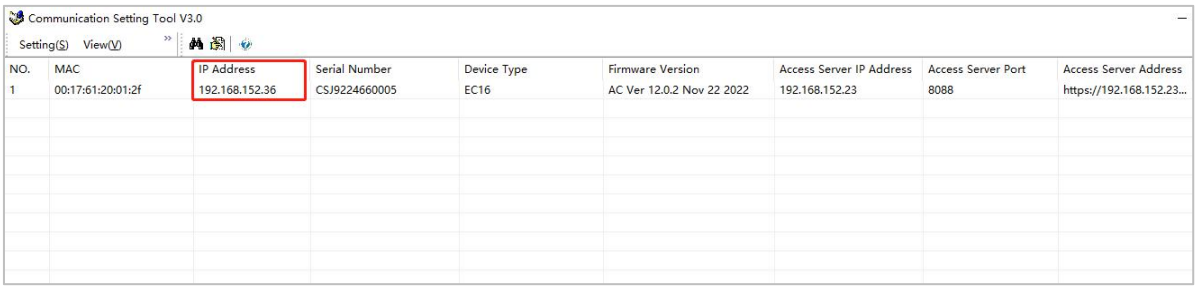
- **Modify by Search Tool**

1. After logging in the ZKBio CVSecurity software, click [**Elevator**] > [**ElevatorDevice**] > [**Device**] > [**Search**], click [**Download Search Tools to Local Disk**] in the search device window, download the search tool *deviceSettingTool_overseas.exe* to your computer.

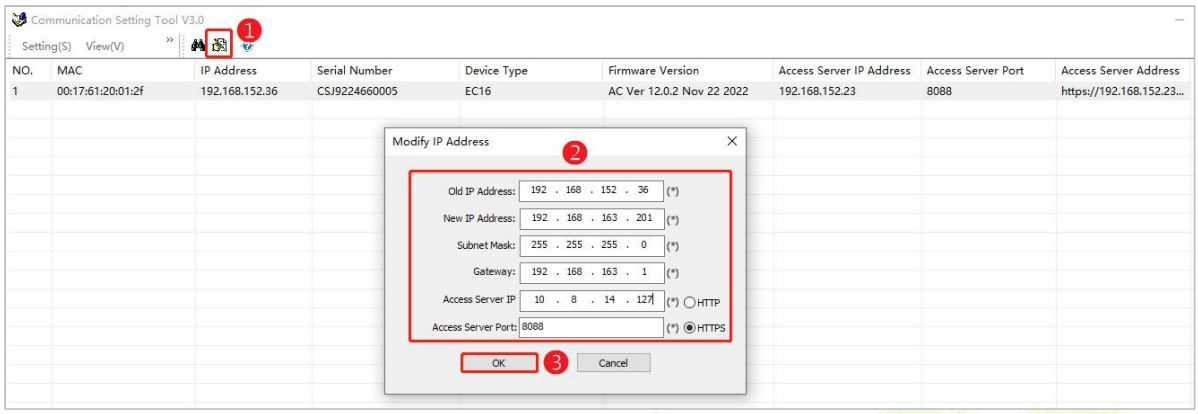
   Note: *At the bottom of the search device interface will prompt the current system communication terminal number.*



2. Double-click deviceSettingTool_overseas.exe to open the search screen, and click the icon to search for the device, then the IP address of the controller is displayed.



3. Select the device to be modified, click the icon to modify the IP address of the device, click [**OK**] after setting the parameters, as the following figure shows.

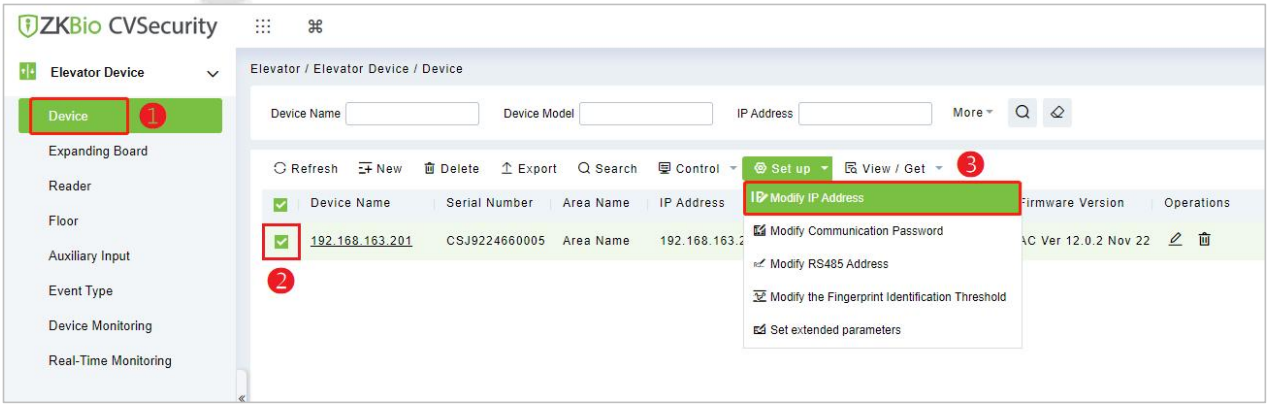


- **Old IP Address:** The IP address of the device. The factory default IP address of the device is: 192.168.1.201.
- **New IP Address:** The new IP address of the device. ***Note:*** *The IP address of the device and the IP address of the computer must be in the same network segment.*
- **Subnet Mask:** Default subnet mask 255.255.255.0, can be modified as needed.
- **Gateway:** Default gateway address 0.0.0.0, can be modified as needed. ***Note:*** *The gateway and the IP address must be in the same network segment.*
- **Access Server IP:** The IP address of the ZKBio CVSecurity software server.
- **Access Server Port:** Enter the communication terminal number of the current system, which is indicated under the "Search" pop-up window.

Modify the IP Address in the software

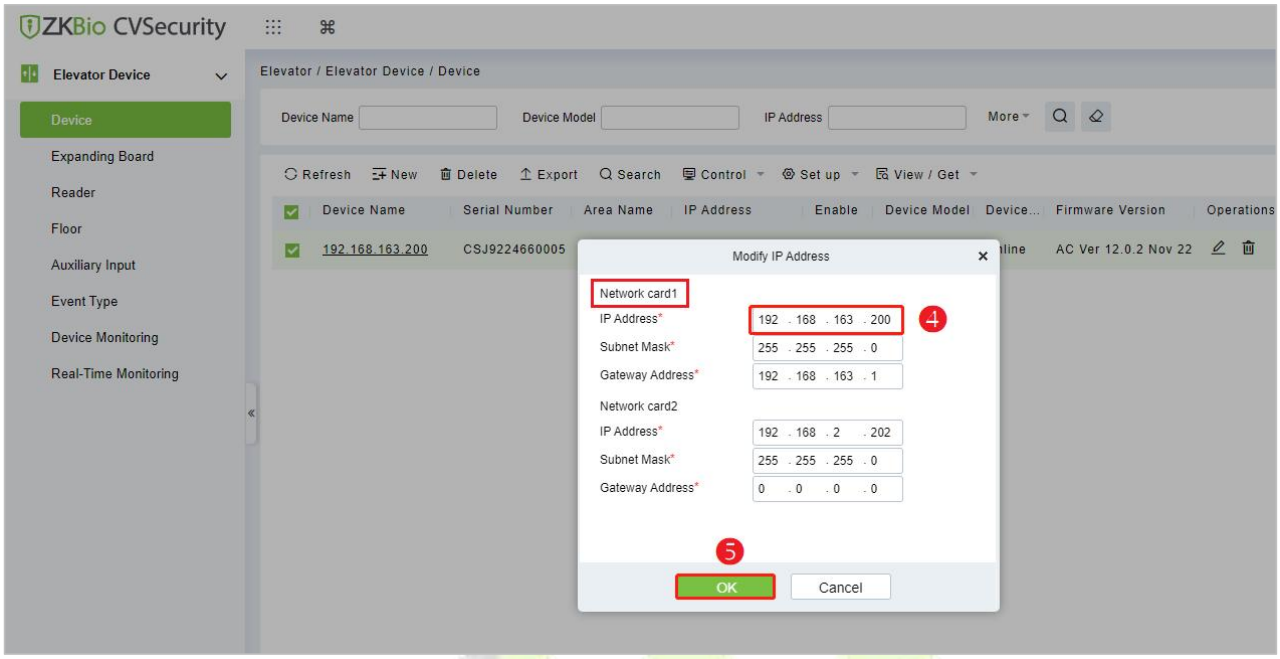
After adding devices successfully in the software (see 5.1.2 Add Device on the Software), you can change the IP address in the device list field.

1. Click [**Elevator**] > [**Elevator Device**] > [**Device**] to enter the setting interface.
2. Check the added device in the device list.
3. Click [**Set up**] > [**Modify IP address**] to bring up the settings window.



4. Modify the IP address of **Network card 1** in the pop-up window.

5. Click [**OK**] to save and exit.



Note: *Network card 1 is the IP address of the primary NIC of the elevator controller, and Network card 2 is the IP address of the extended NIC of the elevator controller.*

7 Others

7.1 USB Disk Upgrade

USB interface can be used to upgrade the elevator controller, the usage is as follows.

1. First, create a new "Udisk" folder in the USB disk, and put the upgrade file into "Udisk".
2. Under the normal operation of the elevator controller, insert the U disk, press the [**Reset**] key for 1 to 5 seconds (the operation light will flash) and release it.
3. The operation light will keep flashing during the upgrade process (no power failure during the upgrade, no unplugging of the U disk), and the elevator controller will restart automatically after the upgrade is successful.
4. If the upgrade is unsuccessful, the elevator controller will return to normal operation.

7.2 Restore Factory Settings

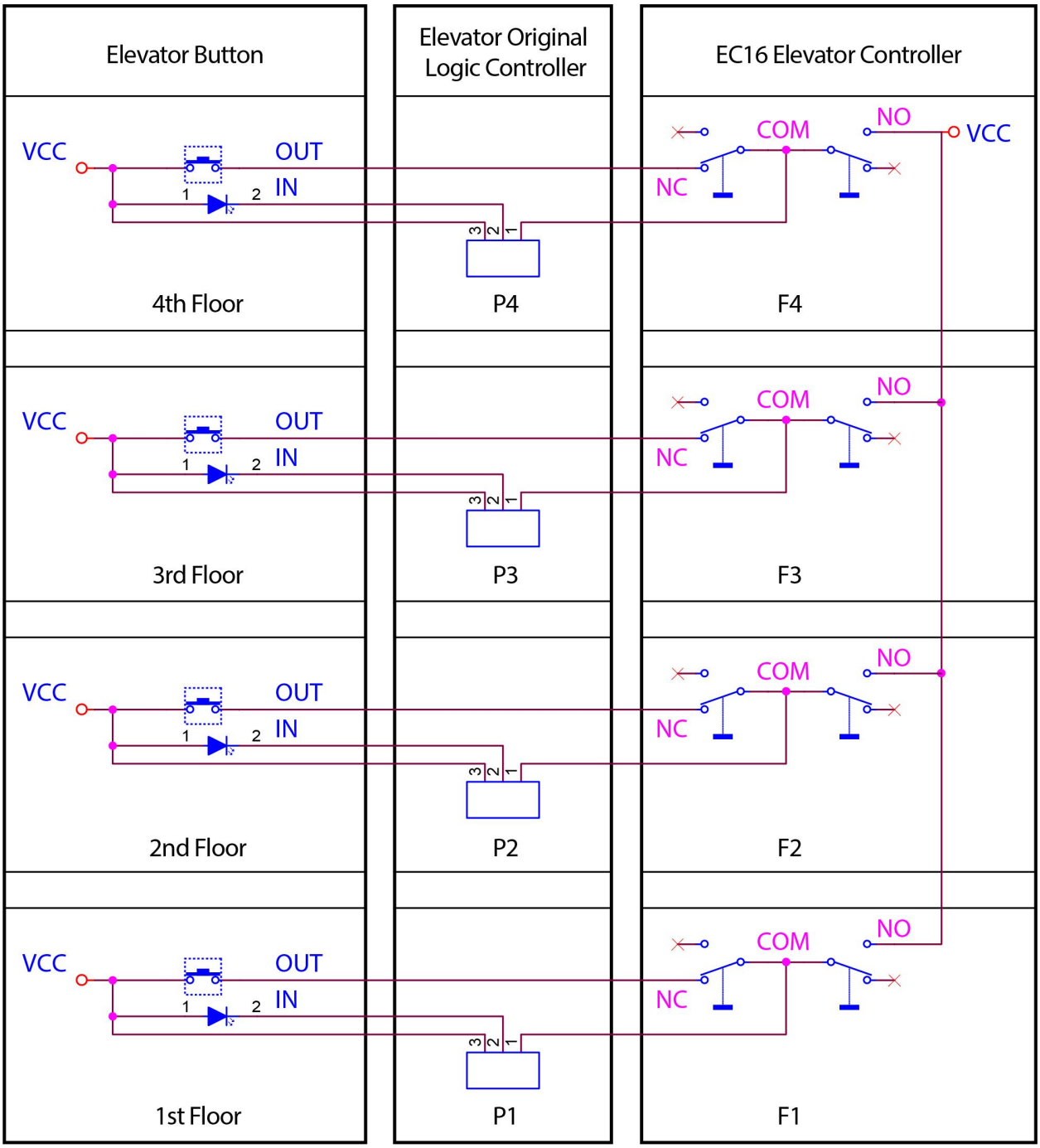
The EC16 elevator controller can be restored to factory settings by [**RESET**] key. Press the [**RESET**] button, 1 to 5 seconds to upgrade with USB disk, 5 to 10 seconds to restart the controller, 10 seconds or more to restore the factory settings.

Note: When restoring the factory settings, only the network configuration of the device is restored, and other data is not restored.

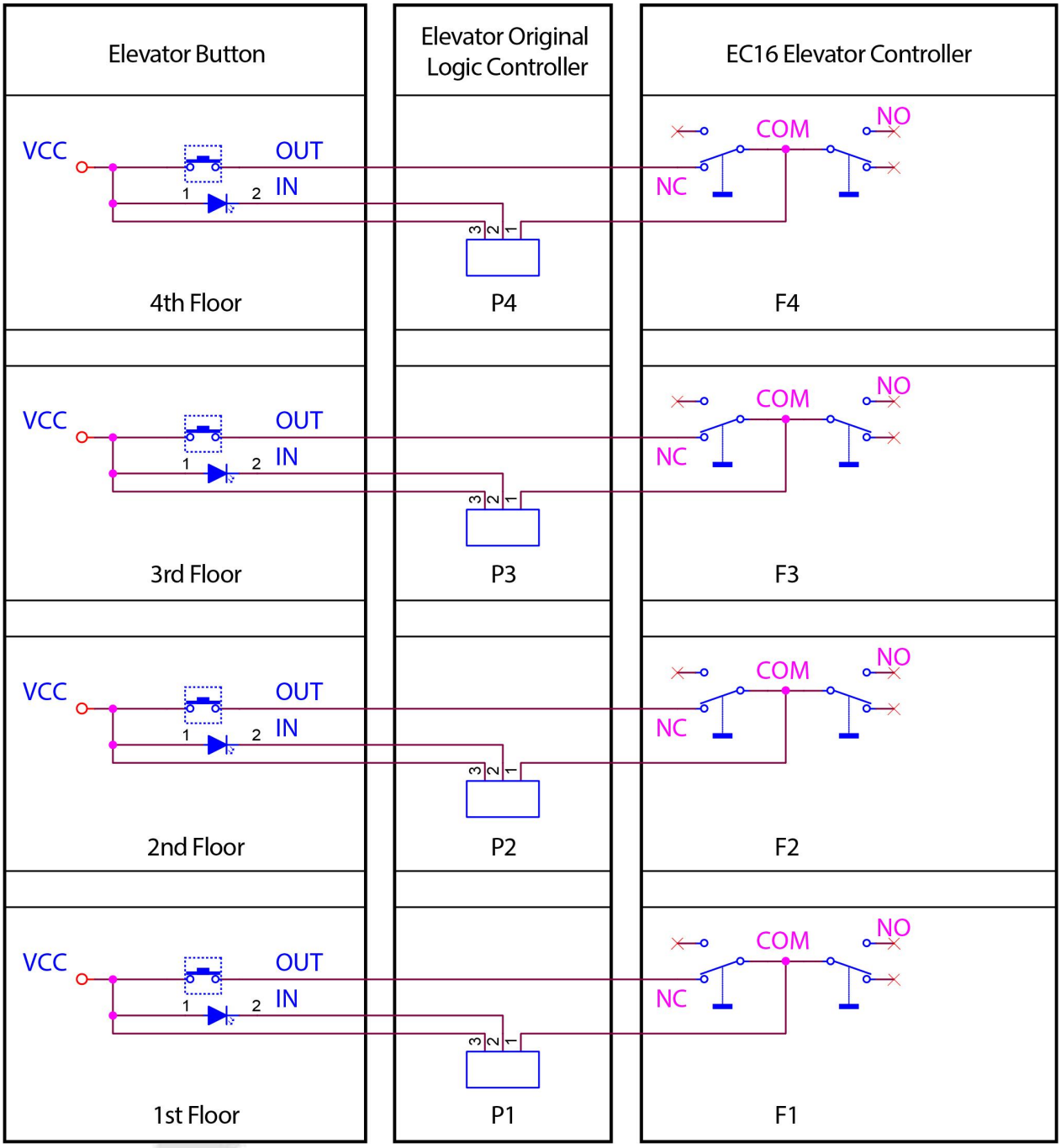
Appendix 1 Elevator Control and Elevator Button Wiring

Method 1 Common Anode Button Connection

1. Supports for floor selection and direct floor selection

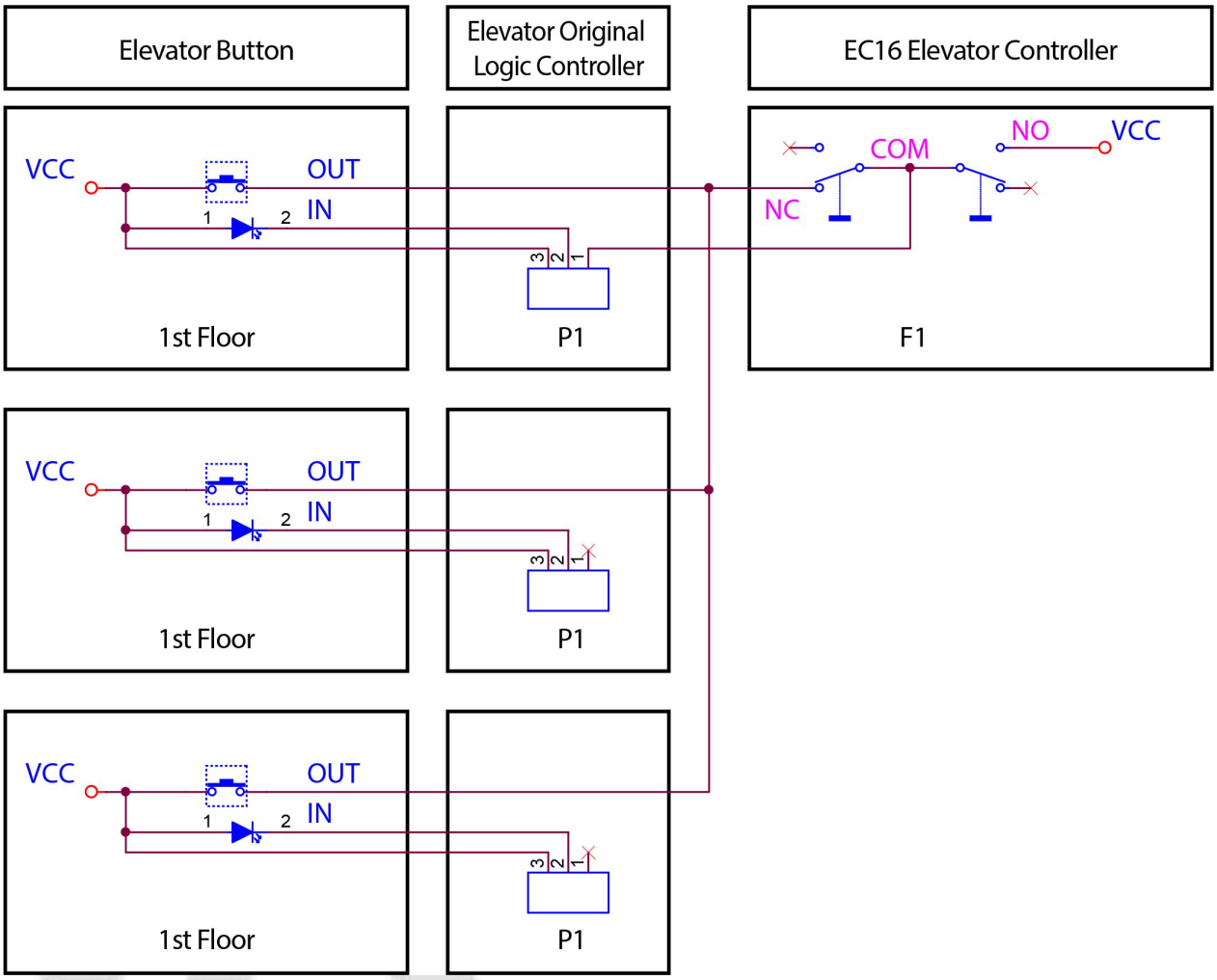


2. Supports floor selection only



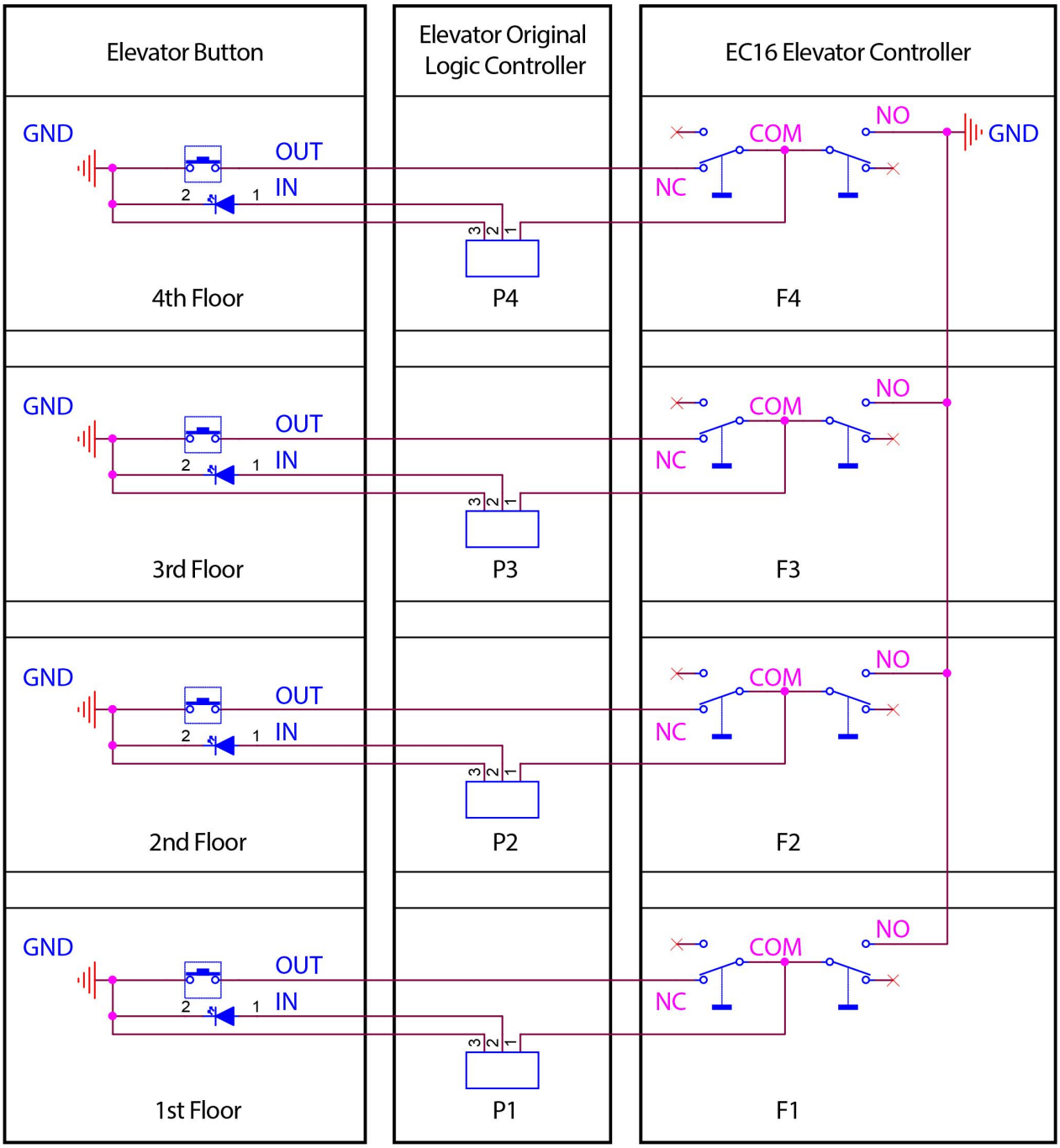
3. Wiring method when there are multiple identical buttons on the same floor

The following figure shows the wiring method for an elevator with three button boards, and this connection method avoids button cancellation exceptions.

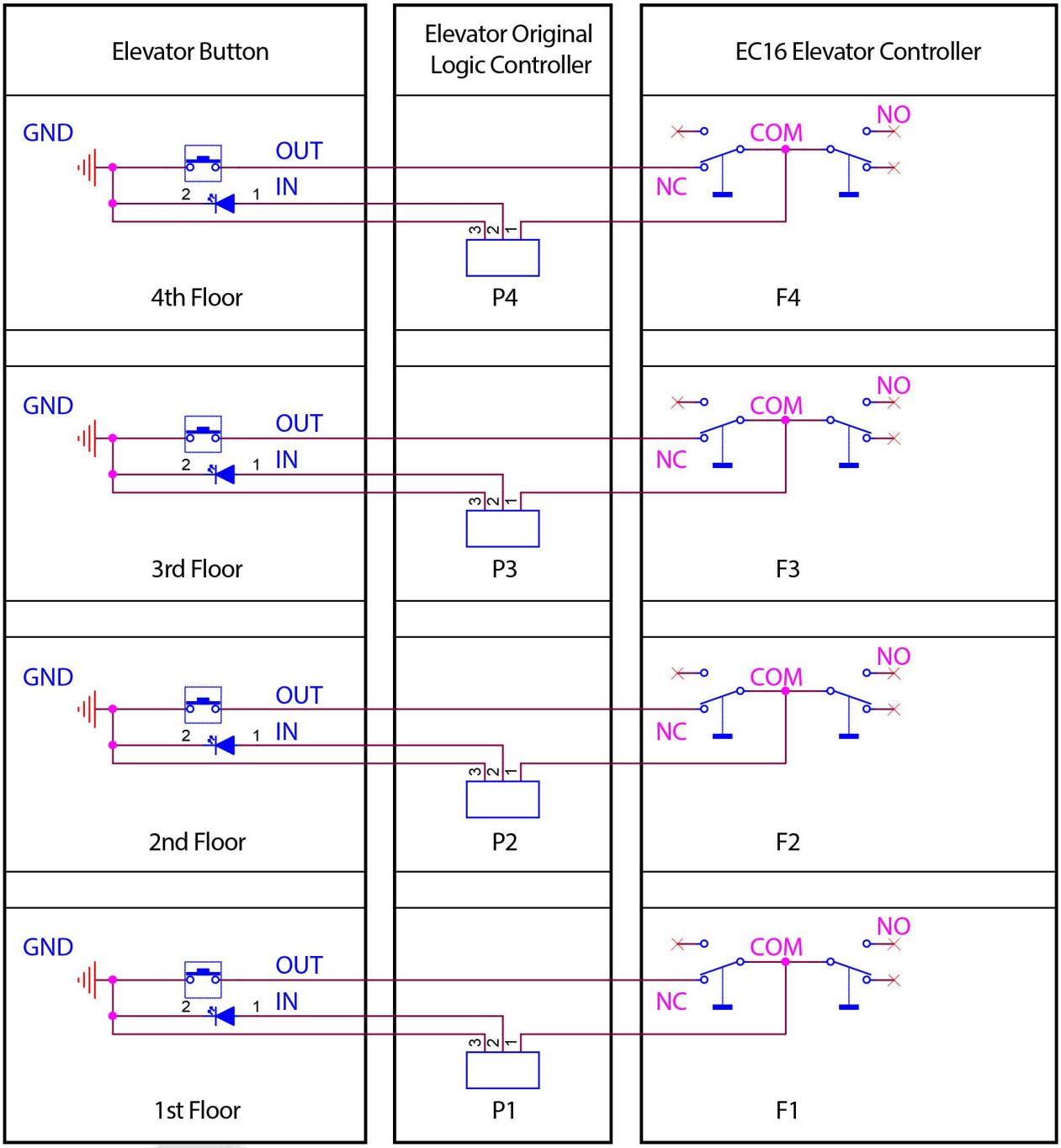


Method 2 Common Cathode Button Connection

1. Supports for floor selection and direct floor selection

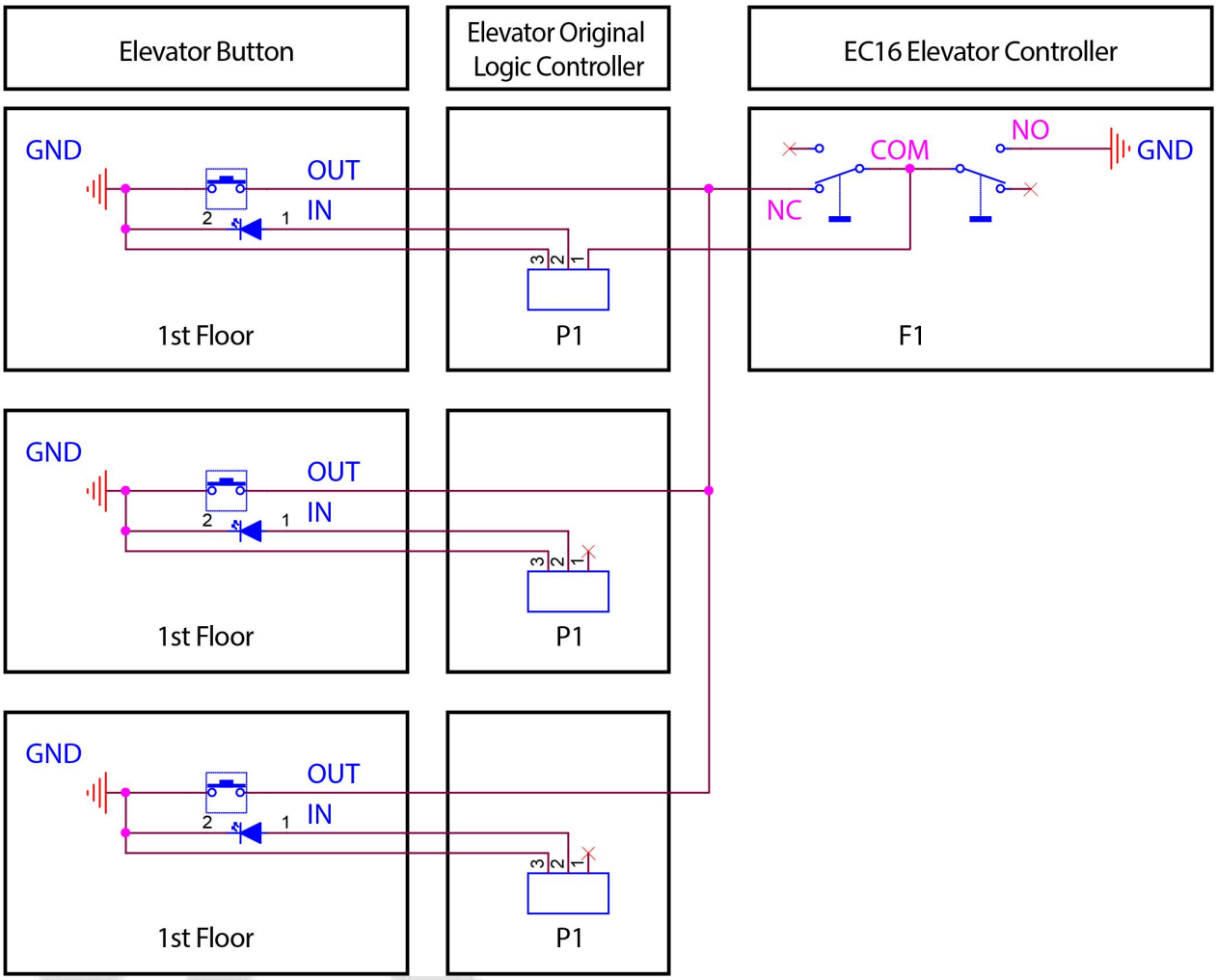


2. Supports floor selection only



3. Wiring method when there are multiple identical buttons on the same floor

The following figure shows the wiring method for an elevator with three button boards, and this connection method avoids button cancellation exceptions.



Appendix 2 Buzzer, Indicator Light Prompt Instructions

EC16 elevator controller works normally online, when the user verifies the RFID card in RS-485 reader and Wiegand reader, the buzzer and indicator prompts are shown in the following table.

Working Status	Buzzer	Indicator Light
Verification Success	1 short sound	LED indicator lights green.
Verification Failure (swipe unregistered card)	2 short sound	LED indicator (red) lights up briefly twice.
Validation method error	2 short sound 1 long sound	LED indicator (red) lights up twice short and then once long.
Data transfer error (Wiegand format error)	1 short sound 1 long sound	LED indicator (red) lights up one short and then once long.
No permission (person has expired, the operation interval is too short, door is not valid time period verification open, illegal time period, illegal access, wrong verification method, block list)	3 short sound	LED indicator (red) lights up briefly three times.
Continue validation during combination validation	/	Flashing green light three times.
Combined verification is not completed	4 short sound (timeout time of 10s)	LED indicator (red) lights up briefly four times.
Timeout	4 short sound (timeout time of 8s)	LED indicator (red) lights up briefly four times.

Appendix 3 Privacy Policy

Notice:

To help you better use the products and services of ZKTeco and its affiliates, hereinafter referred as "we", "our", or "us", the smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified)**.

2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface)**.

4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks**.

5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.

6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

IV. Others

You can visit https://www.zkteco.com/cn/index/Index/privacy_protection.html to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

Appendix 4 Eco-friendly Operation

The product's "eco-friendly operational period" refers to the time during which this product will not discharge any toxic or hazardous substances when used in accordance with the prerequisites in this manual.

The eco-friendly operational period specified for this product does not include batteries or other components that are easily worn down and must be periodically replaced. The battery's eco-friendly operational period is 5 years.

Hazardous or Toxic substances and their quantities

Component Name	Hazardous/Toxic Substance/Element					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
Chip Resistor	×	○	○	○	○	○
Chip Capacitor	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diode	×	○	○	○	○	○
ESD component	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in SJ/T 11363—2006.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in SJ/T 11363—2006.

Note: 80% of this product's components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

www.zkteco.eu