



Conventional Fire Alarm Control Panel

User's Manual



Foreword

General

This manual introduces the functions and operations of the Conventional Fire Alarm Control Panel (hereinafter referred to as "the Device").

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	Modify output.	March 2026
V1.0.0	First release.	December 2025

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please

contact the customer service for the latest program and supplementary documentation.

- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, comply with the guidelines when using it, and keep the manual safe for future reference.

Operation Requirements



- Make sure that the power supply of the device works properly before use.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.

Installation Requirements



WARNING

- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.



- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.

Maintenance Requirements



- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- Clean the device with a soft dry cloth or a clean soft cloth dipped in neutral detergent.
- Contact your local dealer or the service center nearest to you if the device needs internal configuration or maintenance. Do not dismantle or modify the device without a qualified professional present to avoid the risk of danger or damage to the device. We will assume no responsibility for any problems caused by unauthorized modifications or maintenance.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1. Product Information.....	1
2. Technical Information.....	2
3. Structure	3
3.1 Dimensions	3
3.2 Composition.....	3
3.3 Front Panel	4
4. Device Installation and Debug.....	7
4.1 Packing List.....	7
4.2 Inspection.....	7
4.3 Installation.....	7
4.3.1 Principle.....	7
4.3.2 Wiring.....	8
4.3.3 Power connection.....	11
4.3.4 Battery.....	11
4.4 System Debugging	12
4.4.1 Communication Mode.....	12
4.4.2 Alarm Test	13
4.4.3 Disconnection Test	14
4.4.4 Update Firmware By U Disk.....	14
4.4.5 Import Configurations By U Disk.....	14
4.4.6 RS485 Networking.....	15
4.4.7 Consequences of Faults.....	15
5. Compatibility List	16
6. FAQ.....	18
7. Maintenance	19
Appendix 1 Cybersecurity Recommendations	20

1.Product Information

Conventional Fire Alarm Control Panel (DHI-HY-C102-4/6/8) is designed and manufactured in compliance with EN54 Parts 2 & 4 requirements. It provides the advanced capabilities of a cutting-edge conventional fire alarm system, combined with the ease of use and effective installation that building users and installers require. As the core of a conventional fire alarm system, it cooperates with a comprehensive range of auxiliary devices, including smoke detectors, heat detectors, sounder strobes, and manual call points, to construct a fire alarm control system. With Ethernet, RS-485, and other IoT ports, it can integrate with other panels and connect to platforms.

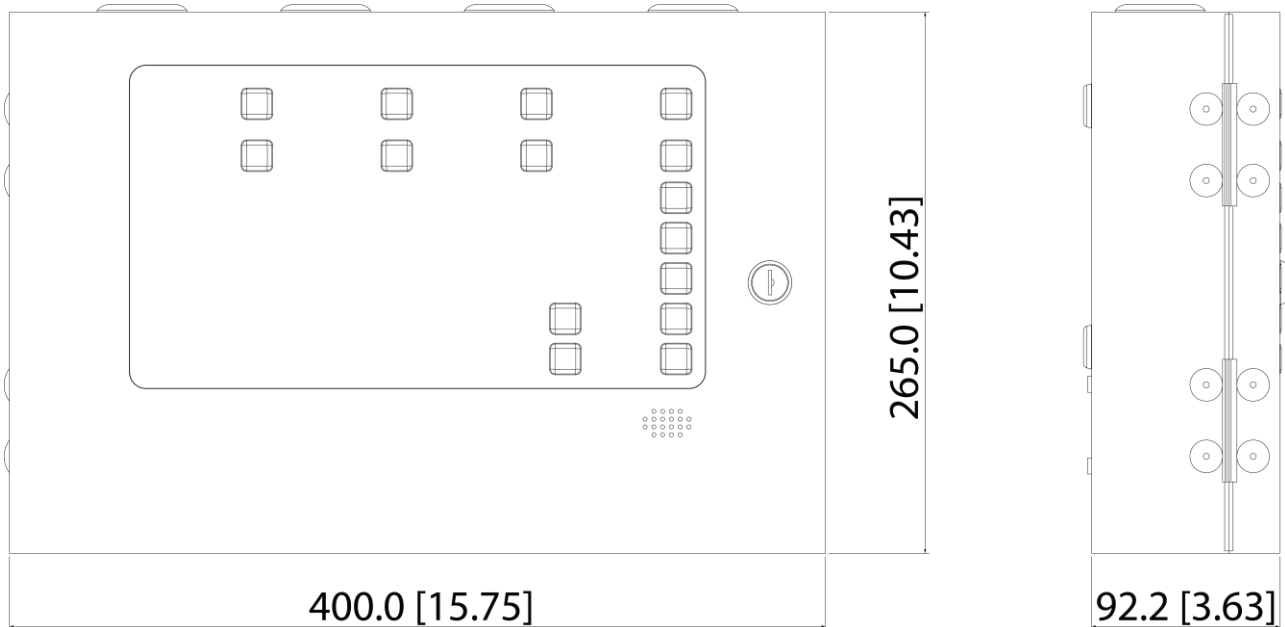
2. Technical Information

Parameter	Introduction
Main Power Supply	AC 100-240V/50Hz, 60Hz
Rated Power	28W
Working Voltage	DC24V
Backup Power Supply	2 lead-acid batteries (12V/7Ah each)
Dimensions	400.0 mm×92.2 mm×265.0 mm (15.75" × 3.63" × 10.43")
Operating Temperature	-10°C to +40°C (+14°F to +104°F)
Operating Humidity	≤ 95% RH (no condensation)
Protection	IP30
PSE	● Output: DC 28V ● I max. a: 1.0A max ● I max. b: 1.0A max ● I min: 0.2A max ● Battery: 2 x RT1270 ● Output: 24Vdc, 0.5A max
Internal Battery	● Model: RT1270 ● Type: Rechargeable lead-acid battery ● Life: 6~8 years ● Rated voltage: 12V ● Rated capacity: 7.0Ah ● Final voltage: 10.5V ● Max charging current: 2.1A ● Ri max(maximum internal resistance): 100 Ω ● Max discharging current: 1.0A

3. Structure

3.1 Dimensions

Figure 3-1 Dimensions (mm[inch])



3.2 Composition

- zones: Max. 25 conventional devices in one zone
- 2 alarm bell outputs: Output DC 28V/500mA or DC 12V/500mA(in terms of product specification)
- 1 fire alarm output: Output closing switch during a fire alarm
- 1 fault output: Output closing switch during a fault alarm
- 4 input detection lines: Detect external input switch
- 1 RS-485: Enable networking with control panels
- 1 RS-232: Reserved port
- 1 USB: Configure and upgrade the panel with USB
- 1 RJ45: Communicate with platform

3.3 Front Panel

Figure 3-2 Front panel



Table 3-1 Front panel introduction

Name	Introduction
Indicator	● Fire: Remain lit after this zone receiving fire information. The LED turns off when the panel is reset. ● Fault: Remain lit after this zone detecting fault. The LED turns off when the panel is reset or the fault is addressed. ● Disable: Remain lit when this zone is disabled. ● FIRE: Remain lit after receiving fire information. ● Mains Supply: Remain lit when FACP is powered by main power. ● Aux.-n (n=1~4): Remain lit when switch is closed. ● Mains Fault: Remain lit when the main voltage is low. ● Low Battery: Remain lit when the battery voltage is under 24V. ● Communication: Remain lit when control panel connects to network, and flash when a fire occurs ● Battery: Remain lit when FACP working voltage is supplied by battery only. ● Battery Fault: Remain lit when backup voltage is under 22V. ● Sounder Active: Remain lit when light and audible alarm is triggered. ● General Fault: Remain lit when FACP receives fault information. (Press Reset button to turn off General Fault indicator) ● Manual Call Point: Remain lit after receiving fire information from manual call point. ● System Fault: Remain lit when the system is not functioning properly. ● Sounder Fault: Remain lit when sounder strobe fails to start. ● General Disable: Remain lit when any zone is disabled. ● Debug: Remain lit when the panel is in debug mode. ● Accumulate: Press Accumulate and Panel Buzzer Silence button to enter level-2, Accumulate indicator remains lit. If permission is insufficient, the light flashes. ● Admin Control: Press Admin Control and Panel Buzzer Silence button to enter level-3, Admin Control indicator remains lit. When both level-2 and level-3 lights are off, it enters level-1. Press and hold Admin Control button under level-3 permission to debug the device. ● Reset: Remain lit when the panel is in reset mode. ● Disconnection Test: Remain lit when the panel is in disconnection test mode. ● Alarm Test: Remain lit when the panel is in alarm test mode. ● Panel Buzzer Silence: Remain lit when the buzzer is silenced. ● Remote Sounder Silence: Remain lit when remote sounder silence is disabled.

Name	Introduction
Functionality Button	● Accumulate: Press Accumulate and Panel Buzzer Silence button to enter level-2, Accumulate indicator remains lit. If permission is insufficient, the light flashes. Press and hold Accumulate button to enter the main-sub registration. Functions that can be used in level-2 include Reset, Remote Sounder Silence, Disable/Disable cancelled, Disconnection Test, Alarm Test, main-sub registration. ● Admin Control: Press Admin Control and Panel Buzzer Silence button to enter level-3, Admin Control indicator remains lit. When both level-2 and level-3 lights are off, it enters level-1. Press and hold Admin Control button under level-3 permission to debug the device. Functions that can be used in level-3 include Device debug, Update Firmware By U Disk, Import Configurations by U Disk. ● Reset: During reset, Reset indicator remains lit, and is off after the reset is completed. Press the Reset button, FACP will reset within 20 seconds, the existing status and related information will be re-established within 20 seconds, and the fault information will be re-established within 100 seconds. Press and hold Reset button at level 2, the system will enter the self-test state. ● Disconnection Test: Press Disconnection Test and Zone Disable, the system enters disconnection test, the Disconnection Test indicator remains lit. After completing disconnection test, press Reset to stop test. Press and hold the button to trigger the communication to the PC.  Disconnection test does not affect FACP's normal operation. ● Alarm Test: Press Alarm Test and Zone Disable, the system enters alarm test, the Alarm Test indicator remains lit. Press Zone Disable button in different zones, its Fire indicator is on, FIRE indicator lights up, buzzer beeps, alarm signal and bell outputs. You can reset to clear alarm information. During the test, if a real fire occurs, FACP stops test automatically and addresses alarm. ● Panel Buzzer Silence: When FACP sends out alarm signal, buzzer beeps. Press Panel Buzzer Silence to temporarily mute alarm. When a new alarm occurs, the buzzer activates again. ● Remote Sounder Silence: Press and hold Remote Sounder Silence to block the equipment; Under a fire alarm condition, press Remote Sounder Silence to mute and reset the equipment.
Buzzer	Alarm sound outlet.

4. Device Installation and Debug

4.1 Packing List

Check the package according to the following checklist. If you find anything damaged or lost, contact customer service.



Keep accessories properly for future use.

Table 4-1 Checklist

Item	Quantity
Conventional fire alarm control panel	1
User's manual	1
Key	2
Backup battery fuse	2

4.2 Inspection

- Disconnect all sources of power prior to installing or removing devices, connecting or disconnecting wiring.
- The Conventional Fire Alarm Control Panel receives main power from AC100V-240V supply. The positive and negative poles of the backup battery are correctly connected.
- Carry out self-test to check whether all parts are successfully inspected.
- The defective detectors should be dealt with according to "FAQ" and "Maintenance", and then test again. If it still fails to pass the test, it should be returned to the factory for repair.

4.3 Installation

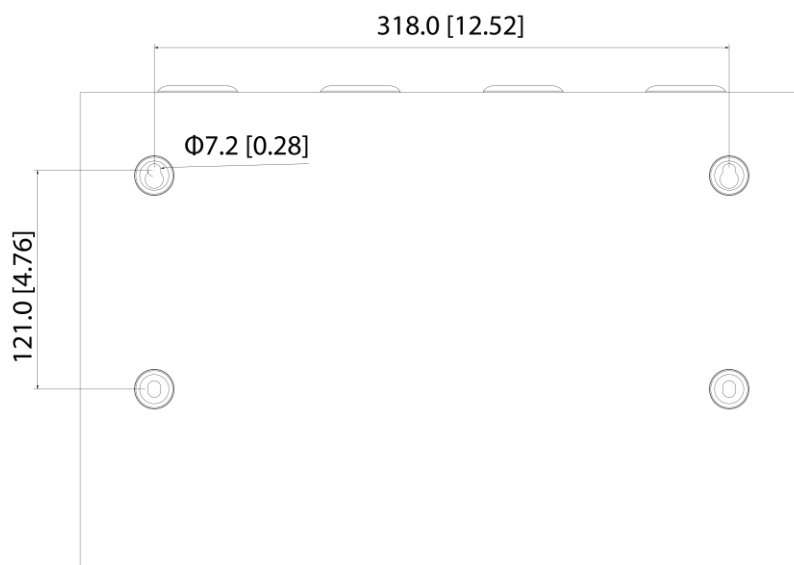
4.3.1 Principle

- The FACP supports wall-mounted installation. It should be installed in the fire control room or the place where people are on duty. Keep away from the environment with electromagnetic interference.
- The design should be strictly implemented in accordance with relevant provisions and regulations, and connect the device correctly according to the construction drawing.
- During the system debugging process, please do not remove the dust cover of the device in advance to avoid false alarms during the decoration process.

Step 1 Choose suitable place with convenient height for visual and manual access to FACP.

Step 2 Drill four holes (Φ10 mm) on the wall and screw bolts.

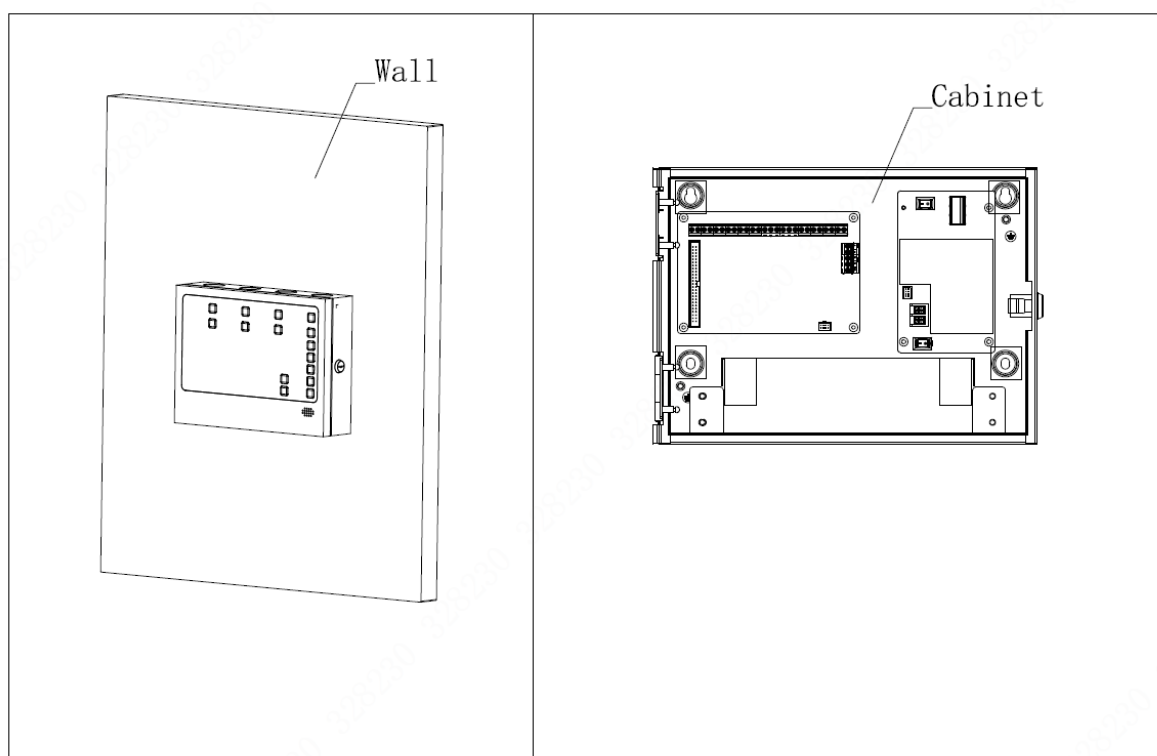
Figure 4-1 Installation (1)



Step 3 Place the cabinet over the four bolts.

Step 4 Open the cabinet, tighten all four bolts securely against the back wall of the cabinet.

Figure 4-2 Installation (2)



4.3.2 Wiring

Before connecting the signal line and direct control line to the FACP, the insulation test should be carried out.

The insulation resistance between loops is more than 10 KΩ, and insulation resistance between loops and ground is more than 10 MΩ.



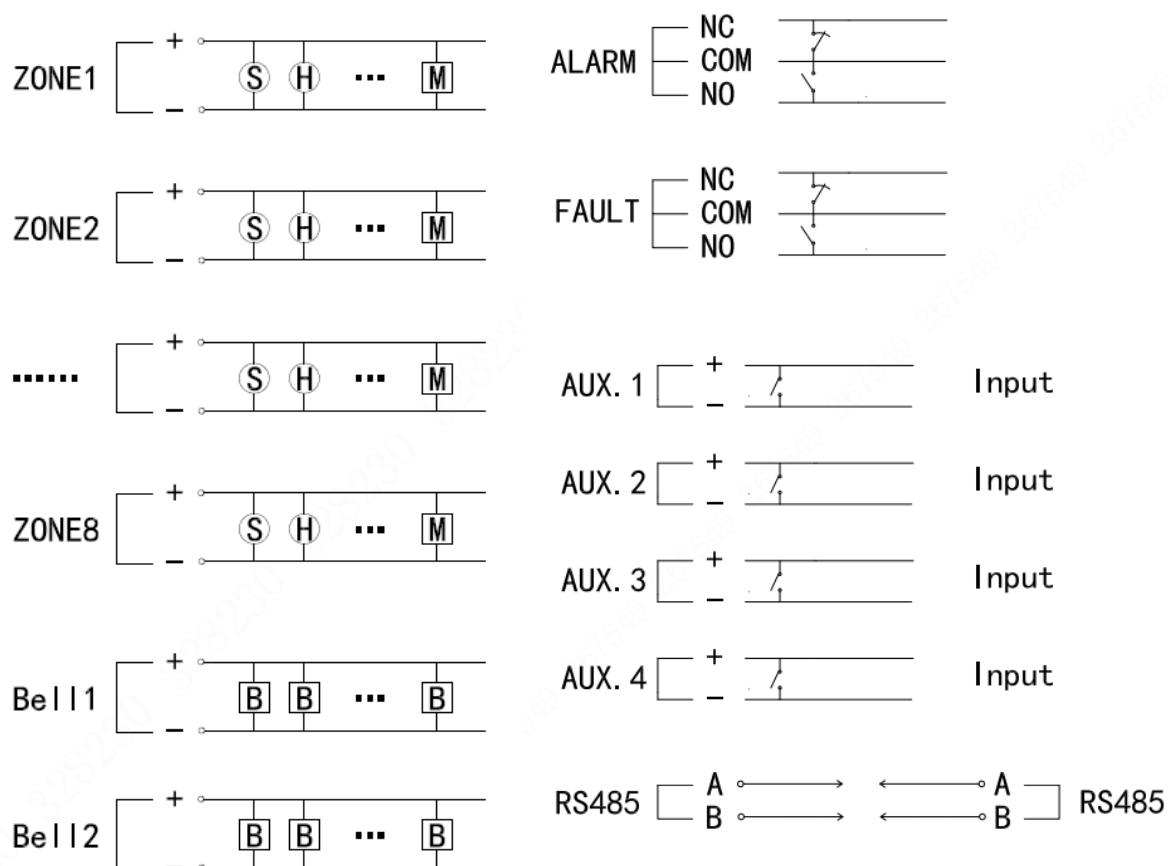
This system does not require external end line resistors.

- Wiring should comply with the construction drawing and relevant regulations.
- Wires with different voltages and types should not be co-managed.
- Use RVS twisted pairs with a section area of 1.5 mm² or 1.0 mm² for the polarity-free signal buses with a communication distance of less than 1500 m.
- RS-485 BUS: Use RVS twisted pairs with a section area of 1.5 mm² with a communication distance of less than 1200 m.
- AC power cord (L, N, $\perp$): Use a flame-retardant 3-core insulated wire with a withstand voltage of more than 750V.
- Grounding wire: Use a 4 mm² copper wire with a grounding resistance of less than 4Ω.

Figure 4-3 Wiring terminal

ZONE1		ZONE2		ZONE3		ZONE4		ZONE5		ZONE6		ZONE7		ZONE8		BELL1		BELL2		FIRE			FAULT		
+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	NC	COM	NO	NC	COM	NO

1	2	AUX1
1	2	
1	2	AUX2
1	2	
1	2	AUX3
1	2	
1	2	AUX4
1	2	
A	B	RS485
RX	TX	
GND		RS232



ZONE terminal

ZONE_n (n=1-8): Connect smoke detector, heat detector, manual call point, etc.



If it is connected to Dahua detector, there is no need to add a end of resistor at each zone.

If it is connected to a detector of any other brand, you need to add a 10kΩ terminal resistor at each zone.

Alarm bell terminal

Bell1, Bell2: Power output terminal of alarm bell, output DC28V/DC12V (in terms of product specification) during fire alarm.

Other terminal

- **FAULT:** Fault output. When the FACP receives fault information, the normally open switch of the terminal becomes the normally closed switch.
- **ALARM:** Alarm output. When the FACP receives alarm information, the normally open switch of the terminal becomes the normally closed switch.
- **AUX_n (n=1-4):** Receive input passive switching from other devices in the system. The maximum

output is 1.0mA.

- 232TX, 232RX, GND: Reserved port.
- 485A1, 485B1: RS-485 networking port for communication among control panels.

Main electrical terminal

L、N、 $\perp$: AC 100V~240V power supply.



Supply Connection-Type: permanent connection

Please ensure it is firm. The disconnect device will be provided with building.

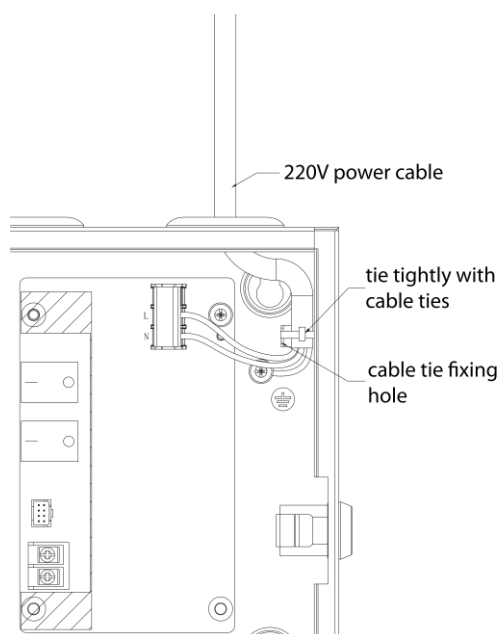
4.3.3 Power connection

Press the L, N, and PE labels to connect the AC 100V~240V power supply. After connecting the power supply, use cable ties to tighten the cable holes as shown in the figure.



AC power cord (L, N, $\perp$): Use a power cable with a cable diameter of no less than 2.5mm. Cut about 10 mm off the cable cover at the end of the cable. After the cable is secured, the copper cover is exposed no more than 2mm and pull to check whether the cable is securely secured.

Figure 4-4 Power connection



4.3.4 Battery



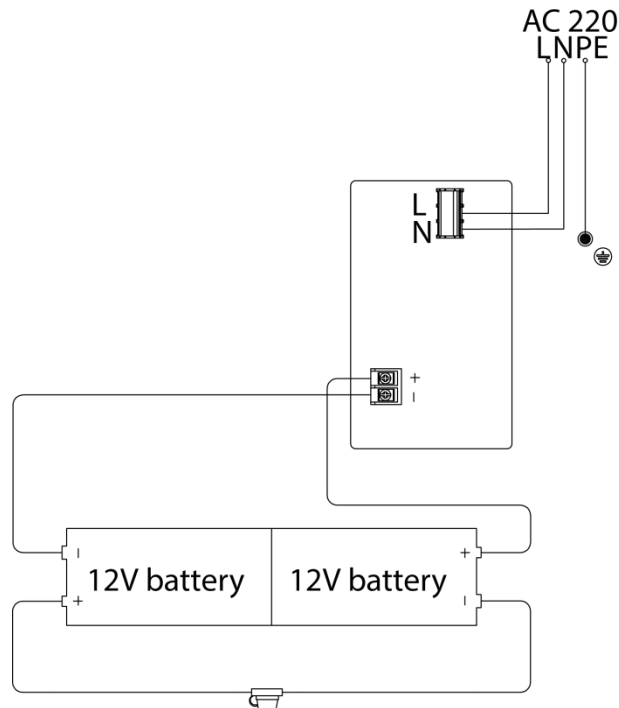
The batteries contained in the product, if any, have been tested in compliance with Regulation (EU) 2023/1542.

Connect the final battery after completing installation.

Step 1 Connect fuse.

Step 2 Connect the red and black power wires reserved in the wire slot to the positive and negative terminals of the battery respectively.

Figure 4-4 Battery



4.4 System Debugging

4.4.1 Communication Mode

- Normal Mode (Default)
 1. Supports connection with third-party detectors.
 2. Plug and play, the detector can be used in conjunction with the panel immediately after being connected to the zone.
 3. Factory default setting is normal mode.
- Protocol Mode
 1. Don't support connection with third-party detectors.
 2. Registration process is required to establish communication between the panel and the detector.
 3. Low current consumption, supports larger number of detectors, two-wire and non-polarized connection.
- How to Switch Modes
 1. Switch to Protocol Mode from Normal Mode: Connect the detectors to zone terminals, press Admin Control and Panel Buzzer Silence to enter level-3, press and hold Admin

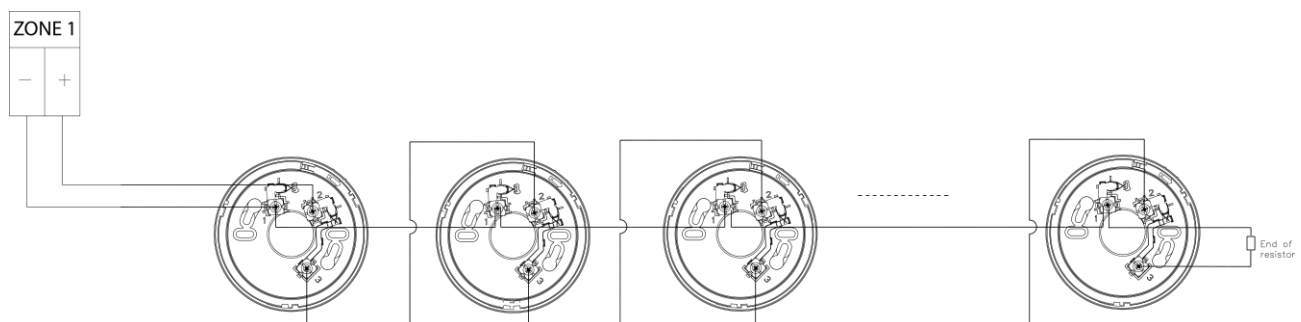
Control to register device automatically. When registration, the Debug indicator lights up, and it turns off after registration.

2. Switch to Normal Mode from Protocol Mode: Disconnect all the detectors from zone terminals, press Admin Control and Panel Buzzer Silence to enter level-3, press and hold Admin Control to register device again. When registration, the Debug indicator lights up, and it turns off after registration, then the communication mode is changed back to normal mode.

- 2-Wire Detector Wiring for Different Modes

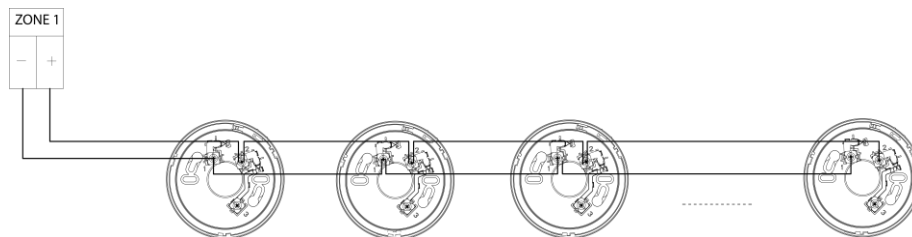
1. 2-Wire Detector + 3-Wire Base Wiring for Normal Mode

Figure 4-5 Wiring



2. 2-Wire Detector + 3-Wire Base Detector Wiring for Protocol Mode

Figure 4-6 Wiring



NOTE

If the panel is switched to protocol mode, it may not function properly with most third-party detectors. In such cases, you need to switch it back to normal mode.

4.4.2 Alarm Test

- Press **Alarm Test** and **Zone Disable** to simulate alarm.
During the test, Alarm Test indicator lights up.
Press **Zone Disable** button in different zone, its Fire indicator is on, FIRE indicator lights up, buzzer beeps, and alarm signal outputs. You can reset to clear alarm information. During the test, if a real fire occurs, FACP stops test automatically and addresses alarm.
- Manual call point test
Press the manual call point to activate the alarm. After the test is completed, reset the manual call point, and then press the **Reset** button in the FACP to reset to stop the fire alarm test.

4.4.3 Disconnection Test

Press **Disconnection Test** and **Zone Disable** to simulate disconnection fault.

During the test, the Disconnection Test indicator lights up.

Press **Zone Disable** button in different zone, its Zone Fault indicator is on, General Fault indicator lights up, buzzer beeps, and fault signal outputs. Press **Reset** to stop the disconnection test.

4.4.4 Update Firmware By U Disk

Step 1 Place the upgraded BIN file named "DHIC102" in the root directory of the U Disk.

Step 2 Use the key to open the chassis and insert the U Disk into the U Disk port.

Step 3 Press **Admin Control** and **Panel Buzzer Silence** button to enter level-3.

Step 4 Press **Accumulate** and **Admin Control** button at level-3 to perform a U Disk upgrade.

Step 5 After 3 seconds, the Debug indicator is always on, indicating that the upgrade process has begun.

During the upgrade, the System Fault indicator will be on, it is normal.

Step 6 After the upgrade is complete, the Debug and System Fault indicators are off, and the control panel returns to the standby state



If the U Disk is not recognized, the Debug indicator will always be on. If the file is incorrect or the import fails, the Debug indicator will turn off until the Manual Reset is released.

4.4.5 Import Configurations By U Disk

Configure the RS485 networking between the host and the networking function between the host and the platform by the computer software named "ControlConfig".

Step 1 Configure the settings on the ControlConfig and export the file renamed to "DHIC102.cfg" to the root directory of the U Disk.

Step 2 Use the key to open the chassis and insert the U Disk into the U Disk port.

Step 3 Press **Admin Control** and **Panel Buzzer Silence** button to enter level-3.

Step 4 Press **Admin Control** and **Remote Sounder Silence** button at level-3 to perform a U Disk import.

Step 5 After 3 seconds, the Debug indicator is always on, indicating that the import process has begun.

Step 6 After the import is complete, the Debug indicator is off, and the control panel returns to the standby state.



If the U Disk is not recognized, the Debug indicator will always be on. If the file is incorrect or the import fails, the Debug indicator will turn off until the Manual Reset is released.

4.4.6 RS485 Networking

Realize the networking of RS485 main and sub devices.

Step 1 Complete the configuration of main-sub mode on the ControlConfig.

Step 2 Connect the main and sub devices through RS485A and RS485B terminals.

Step 3 Press **Accumulate** and **Panel Buzzer Silence** button to enter level-2.

Step 4 Press and hold **Accumulate** button at level-2 to enter the main-sub registration.

Step 5 After 3 seconds, the Debug indicator is always on, indicating that the registration process has begun.

Step 6 After the registration is complete, the Debug indicator is off, and the control panel returns to the standby state.



Only one main and a maximum of 128 sub devices can exist on a same RS485 circuit, and the addresses of the sub devices must be different.

4.4.7 Consequences of Faults

Fault event type	Cause	Host response time
BELL output short circuit	Description The BELL output (28V port) is short-circuited	The response time of a control panel in normal monitoring state and after the panel is reset (or powered on) is 3s.
BELL output open circuit	Description When the BELL output (28V port) is disconnected, an event is generated	
Bus short	An event is generated when the controller BUS is short-circuited.	The response time of the control panel in normal monitoring state is 40s, and the response time after the panel is reset is 15 seconds.
Bus break	An event is generated when a registered device in the LOOP is disconnected	The response time of the control panel under normal monitoring condition is 80s, and the response time after reset is 16s.

5.

6.Compatibility List

Product	Dahua Panel with Protocol Mode		Dahua Panel with Normal Mode and Third Party Panel		Sounder Strobe Base	Remote Indicator	Detector Model	Notes
	DHI-HY-C102-4/6/8		DHI-HY-C102-1/4/6/8/12/16/20		DHI-HY-SDZ	DHI-HY-R1151		
	Power On	Report Offline	Power On	Report Offline	Compatibility	Compatibility		
2-Wire Sensor + 2-Wire Base	√	√	√	×	×	×	DHI-HY-C131 DHI-HY-C132	The base of baseline product number has been switched to a 3-wire base already
2-Wire Sensor + 3-Wire Base	√	√	√	√	×	×	DHI-HY-C131 DHI-HY-C132	2-wire wiring for protocol mode 3-wire wiring for normal mode

4-Wire Sensor + 4-Wire Base Remote Indicator Version	×	×	✓	✓	✓	✓	DHI-HY-C1 34 DHI-HY-C1 36	one detect or can only connect one remote indicator or one sounder strobe base in the same time
4-Wire Sensor + 4-Wire Base Relay Version	×	×	✓	✓	×	×	DHI-HY-C1 34-RE DHI-HY-C1 36-RE	Selectable NO/NC relay output
2-Wire Manual Call Point	✓	✓	✓	×	\	\	\	\
2-Wire Sounder Strobe	✓	×	✓	×	\	\	DHI-HY-C1 51	\
4-Wire Sounder Strobe	✓	✓	✓	✓	\	\	DHI-HY-C1 56 DHI-HY-C0 542	\

7.FAQ

Problem	Analysis	Solutions
Fails to work normally after starting up	Abnormal power supply	● Check mains power supply ● Check the connection cable
Mains Fault indicator is constantly on after starting up	● No mains power supply ● The fuse of mains power is blown out	● Check and connect the cables ● Replace the fuse
Battery Fault indicator is constantly on after starting up	● Wrong connection of backup power cable ● The backup power supply is out of power or damaged	● Check the relevant backup electrical plug-ins to ensure that the backup electrical connection is normal ● In the case of AC power supply, turn it on for more than 24 hours. If the fault cannot be eliminated, the backup power supply needs to be replaced
Fault indicator of zone is constantly on	● Devices disconnected ● Devices damaged ● Poor contact between device and base ● Bus short circuit ● The third-party has not been connected to terminal resistor.	● Check the connection ● Replace the device ● Re-install the device and make sure the proper installation ● Check the circuit. After the short circuit fault is addressed, FACP will reset after 1 minute ● Add a 10kΩ resistor in corresponding zone.
No alarm sound	● Loose connection with Buzzer terminals ● Buzzer damaged	● Insert the Buzzer terminals again ● Replace Buzzer

8.Maintenance

To keep your device in good working condition, please follow these requirements.

- Simulate alarm test: Test the device once half a year (recommended).
- Battery check: A visual inspection should be made once a quarter and discharging once half a year to ensure they are in good serviceable condition.



When reporting a backup power failure, check the connection and wiring of the backup battery. When the backup battery continuously works for more than 8 hours, it may also report a backup power failure due to low voltage.

- Fuse maintenance: Check the fuse when the main and backup power supply is abnormal. If the fuse is burnt out, replace the fuse with same specification.

Fuse	Fuse	Use location
Fuse -TMDT2AL250V-2A-250VAC- Slow Melt Glass Tube - Φ5.2x20mm	250V-2A	Main power
Fuse -32V-3A	32V-3A	Battery connection

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords.

- The length should not be less than 8 characters.
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
- Do not contain the account name or the account name in reverse order.
- Do not use continuous characters, such as 123, abc, etc.
- Do not use overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are

using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. Disable Unnecessary Services and Choose Secure Modes

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

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

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

10. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. Network Log

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

13. Construct a Safe Network Environment

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883