Addressable Input Module

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.2

Foreword

General

This manual introduces the functions and operations of the Addressable Input Module (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
V1.0.2	Modify specification.	December 2023
V1.0.1	Modify installation.	August 2022
V1.0.0	First release.	March 2022

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

1 Product Information

1.1 Introduction

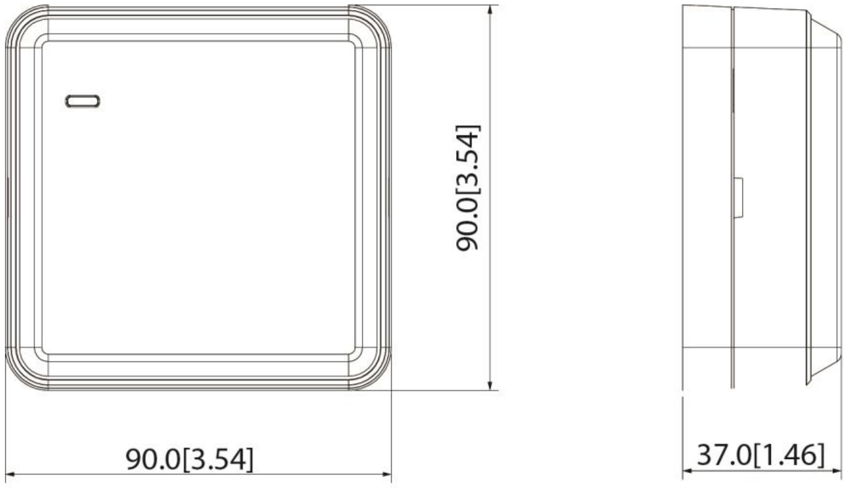
DHI-HY-1400 Addressable Input Module is a mated product of the Addressable Fire Alarm Control Panel, regulating the normal operation of external fire protection device. When the external device is abnormal, the Addressable Fire Alarm Control Panel will confirm a fire alarm according to the received message sent from the module. It can be connected with various passive, normally open on-off pieces of equipment, such as water flow indicators, pressure switches and other firefighting equipment.

1.2 Features

- Convenient wiring: Two-wire, polarity-free
- Reliable communication: Built-in microprocessor, stable performance
- Ultra-low power consumption: Ultra-low monitoring current and operating current
- Simple installation: With a plug-in structure, easy to install and construct

1.3 Dimensions

Figure 1-1 Dimension [mm (inch)]



2 Technical Information

Parameter	Introduction
Electrical	
Working Voltage	DC24V
Rated Power	0.04W
Current	● Monitoring current: ≤ 220μA ● Operating current: ≤280μA
Indicator	Red indicator flashes once every 6 seconds, and flashes once every 2 seconds when malfunctioned
Communication Wiring	
Wiring	Two-wire, polarity-free
Addressing Method	Encoder
Address Range	1–254
Communication Distance	≤ 1500 m
Environment	
Operating Temperature	–10°C to +55°C (+14°F to +131°F)
Storage Temperature	–20°C to +65°C (–4°F to +149°F)
Operating Humidity	≤ 95% RH (no condensation)
Construction	
Color	White
Dimensions (with base)	90 mm × 90 mm × 37 mm (3.54" × 3.54" × 1.46")
Weight (with base)	103 g (0.23 lb)
Certification	EN54-18:2005

3 Device Installation

3.1 Packing List

Check the quantity and model. If you find device damage or any loss, contact the after-sales service.

3.2 Installation Steps

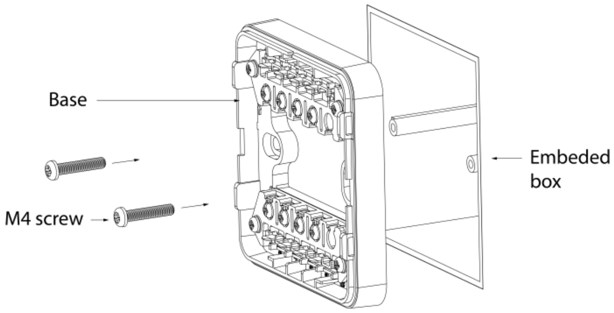
Prerequisites

- Determine the location, mounting distance and numbers for mounting the device in the protection area according to relevant provisions and regulations of the GB50166-2007 *Code for Installation and Acceptance of Fire Alarm System*, and connect the device correctly according to the construction drawing.
- Disconnect the power supply of the device before installation.
- The insulation resistance between buses should be greater than 20KΩ, and the insulation resistance of the bus to ground should be greater than 20MΩ.
- Use RVS twisted pairs with a section area of 1.5 mm^2 or 1.0 mm^2 for the signal buses.

Procedure

Step 1 Use two M4 screws to fix the device base on the embedded box or designated position, and make sure the matched mounting base has been firmly installed.

Figure 3-1 Installation (1)



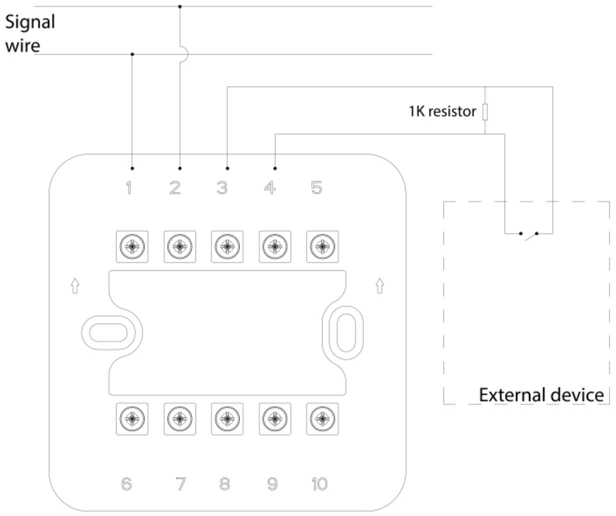
Step 2 Wiring the base. Connect terminals and fix on the base.

There are two wiring methods: Normally open input and normally closed input. The former is adopted by default. Please choose the corresponding wiring method according to realities.

- 1, 2: Access terminal for the bus signal, polarity-free.
- 3, 4: Access terminal for the feedback equipment, connected to the equipment such as fire damper, signal butterfly valve, water flow indicator, pressure switch, and flow switch.

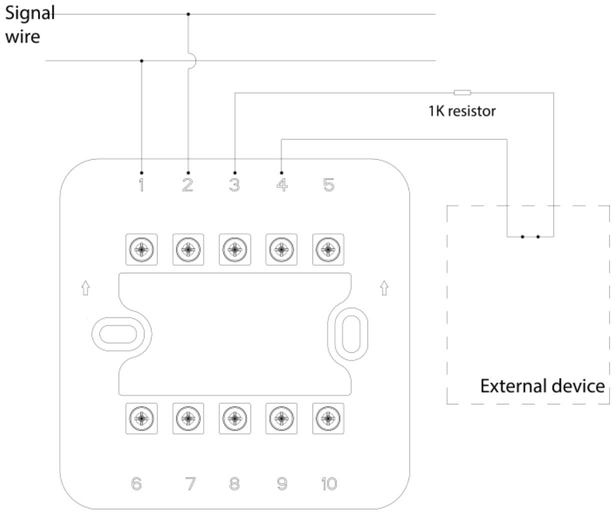
- Normally open input: The end of the input line of the module must be connected in parallel with a 1KΩ resistor.

Figure 3-2 Normally open input



- Normally closed input: The end of the input line of the module must be connected in series with a 1KΩ resistor.

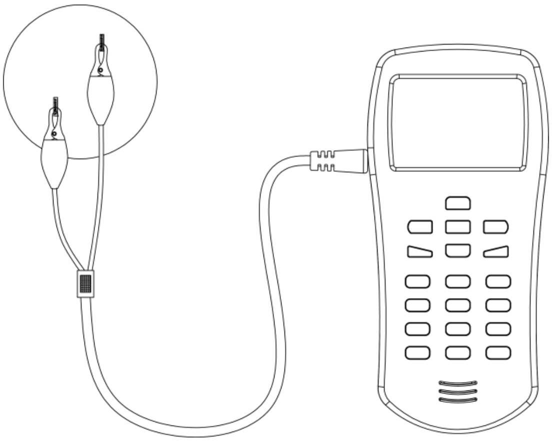
Figure 3-3 Normally closed input



<u>Step 3</u> Code address.

1) Use a coder to make the device coded according to the device address on the construction drawing.
2) Press the number key to enter the address number, and then press **OK** to write the corresponding address to the device.
3) After writing the address successfully, there will be a "Di" tone, and the address will be automatically increased by one.

Figure 3-4 Coding



Step 4 Mount the device into the base by aligning them together until it is firmly locked.

Figure 3-5 Installation (2)

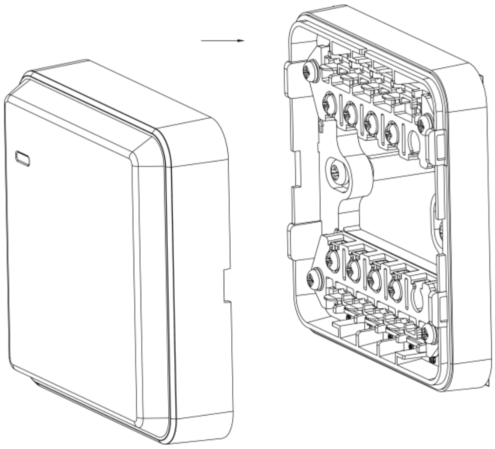
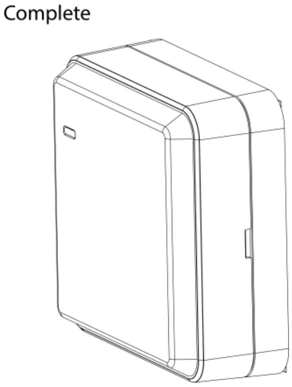


Figure 3-6 Installation (3)



Step 5 After all devices are installed and checked, connect the power supply of the Addressable Fire Alarm Control Panel and conduct automatic register. The equipment shall be powered by a limited power source or PS2 circuit.

4 FAQ

Problem	Solutions
The indicator light of the module flashes quickly, and the screen of Fire Alarm Control Panel displays "Add or replace equipment"	While adding or replacing equipment, re-register in the **System Debugging** menu on the Fire Alarm Control Panel
The indicator light of the module flashes quickly, and the screen of Fire Alarm Control Panel displays "LA repeated equipment information"	Find and take off the wrong coding device, rewrite the code with the encoder, and re-register on the Fire Alarm Control Panel after installation
The indicator light of the module does not light up, and the screen of Fire Alarm Control Panel displays "Registered device is offline"	Check whether the device is installed in place; if it is installed correctly, check the circuit, measure and ensure that the voltage of the equipment signal line is between BUS 16V and BUS 28V
The indicator light of the module flashes quickly, and the screen of Fire Alarm Control Panel displays "Open Circuit (Short Circuit) Fault"	Terminal 3 and 4 should be connected with 1 KΩ resistor

5 Test and Maintenance

5.1 Test

- After installation and register, inspect the operation status of module. When the external device works properly, the indicator of input module flashes 6 seconds.
- Trigger the input switch to activate a fire alarm signal, the LED should be constant on.
- After completing the alarm test, reset the Fire Alarm Control Panel and restore to the normal operation.

5.2 Maintenance

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

- Simulate alarm test: Test the device once half a year (recommended).
- Before testing or maintaining, inform the proper authorities that the system is undergoing maintenance and will temporarily be put out of service. Disable the system to prevent unwanted alarms.

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