



No. DH - IPC - HDEW-Um-01-2021

# Explosion-Proof Camera

## Quick Start Guide



# Foreword

## General




This manual introduces the installation and operations of explosion-proof camera (hereinafter referred to as "the Camera").

## Model

DH-IPC-HDEW series

## Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable result.
 NOTE	Provides additional information as a supplement to the text.

## Revision History

Version	Revision Content	Release Time
V1.0.3	Updated the installation procedure.	February 2024
V1.0.2	Updated the cable description.	October 2021
V1.0.1	Updated "3.3 (Optional) Installing SD Card".	September 2021
V1.0.0	First release.	July 2021

## Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited to: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

## About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

## Important Safeguards and Warnings

The manual will help you to use the Camera properly. Read the manual carefully before using the Camera, and keep it well for future reference.



- Avoid heavy stress, violent vibration, and water splash during transportation, storage, and installation. Complete package is necessary during the transportation when the Camera is delivered or is returned to the manufacturer for repair. We will assume no responsibility for any damage or problem caused by the incomplete package during the transportation.
- Protect the Camera from falling down or heavy vibration.
- Buckle the safety hook before installing the Camera if it is included.
- To avoid damage, keep the Camera away from televisions, radio transmitters, electromagnetic devices, electric machine, transformers, and speakers; do not install the Camera in places with smoke or vapor, high temperature, and lots of dust; do not install the Camera near the heating furnace and other heat sources, such as spotlight, kitchen, and boiler room.
- Do not disassemble the Camera; otherwise it might cause dangers or device damage. Contact your local retailer or customer service center for internal setup or maintenance requirements.
- Do not aim the lens at strong light (such as lamplight, sunlight) for focusing; otherwise, it might cause over brightness or flickering (which is not because of device error), impacting sensor lifespan (CCD or CMOS).
- When using a laser beam device, avoid exposing the device surface to laser beam radiation.
- Do not place the device in the humid, dusty, extremely hot and cold site with strong electromagnetic radiation or unstable illumination.
- Avoid liquids entering the device and then damaging the components.
- Keep the Camera well ventilated to avoid heat gathering.
- Install the device in a place where only professionals with relevant safety protection and warning knowledge can enter. When the device is working normally, non-professionals entering the Camera installation area might cause injury.
- Make sure that there is no metal, or inflammable, explosive substance in the Camera; otherwise it might cause fire, short-circuit, or other damage. Power off the Camera and disconnect the power cable immediately if there is water or other liquid falling into the Camera. And contact your local retailer or after-sales service center. Avoid sea water or rain eroding the Camera.
- Avoid the lens aiming at intense light source, including sunlight, and incandescent light; otherwise the lens might be damaged.
- To avoid the risk of discharge caused by static electricity on the surface of the product, the ground terminal of the product body must be reliably connected to the ground terminal of the installation site. The dome of the product body is treated with conductive coating hardening to reduce the risk of static electricity accumulation. Avoid exposing the device to ultraviolet rays. Typical ambient temperature range is -40°C to 85°C, and humidity is 85% RH.
- There might be a risk of electrostatic discharge seeping on the dome cover. After adjusting the camera, cut off the power before installing the top cover of the dome. Avoid directly exposing the dome cover of the Camera to other equipments and human bodies.
- The Camera uses G 3/4 thread (for external connection) at the outlet of the bottom shell.



- Use the power adapter recommended by the manufacturer.
- For the Camera that supports laser, do not aim the laser directly at eyes. And keep a proper distance from the flammable to avoid fire.

- Do not connect several cameras to one power adapter; otherwise it might result in overheat or fire if it exceeds the rated load.
- If there is any smoke, disgusting smell, or noise from the Camera, power off the Camera and disconnect the power cord immediately, and contact your local retailer or customer service center.
- We will assume no responsibility for any problems (such as water intrusion or loose cables) caused by unauthorized modifications, disassembly or repair, incorrect installation or use, and overuse of certain components.

## Requirements for Installation and Maintenance Personnel

- Hold certificates or experiences related to installation and maintenance of the closed-circuit television (CCTV), and have certificates related to working at height.
- Have basic knowledge and installation skills of CCTV system.
- Have basic knowledge and operation technique for low-voltage wiring and low-voltage electronic circuit connection.
- Have the ability to read and understand the manual.
- Have explosion-proof related certificates.

## Requirements for Lifting the Camera

- Select appropriate tools and place to lift the Camera.
- Make sure that the selected tools reach the installation height.
- Make sure that the selected tools have high safety performance.

## Storage Requirements

- The warehouse should be well ventilated and free from corrosive gases; the ambient temperature should be: T5/T100°C: -40 °C to 55 °C; T6/T80°C: -40 °C to +55 °C. The relative humidity should be no more than 85%; there should be no strong mechanical vibration, impact or strong magnetic field.
- Keep the Camera away from fire source, and do not store it with corrosive, inflammable and explosive materials.
- If the Camera has been stored for more than 18 months, it should be resubmitted for inspection and confirmation.

## Transportation Requirements

- Handle the Camera with care, and do not throw, roll or trample it.
- Avoid damp, extrusion and rain during transportation.
- Do not ship the Camera with corrosive, inflammable and explosive materials.

# Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Overview.....	1
1.1 Introduction.....	1
1.2 Naming Rule.....	1
1.3 Application.....	2
1.4 Mechanical Structure.....	3
1.4.1 Mechanical Specification.....	3
1.4.2 Explosion-proof Structure.....	3
1.5 Electric Specification.....	4
1.6 Environment Requirements.....	4
1.7 Repair and Maintenance.....	6
1.7.1 Notes to Maintenance.....	6
1.7.2 Preparation.....	6
2 Installation Preparation.....	7
2.1 Packing List.....	7
2.2 Dimensions.....	8
2.3 Cable Connection.....	8
2.3.1 Cable Description.....	8
2.3.2 Connecting the Alarm Cable.....	10
2.3.3 Connecting the Explosion-Proof Flexible Tube.....	11
2.3.4 Grounding Description.....	12
2.4 Cable Preparation.....	13
3 Device Installation.....	15
3.1 Installation Conditions.....	15
3.1.1 Installation Accessories and Tools.....	15
3.1.2 Precautions before Installation.....	16
3.2 Installation Method.....	17
3.3 (Optional) Installing SD Card.....	17
3.4 Installation Procedure.....	18
3.4.1 Wall Mount.....	18
3.4.2 Ceiling Mount.....	21
3.4.3 Adjusting Lens Angle.....	22
4 Network Configuration.....	23
4.1 Initializing Device.....	23
4.2 Modifying Device IP Address.....	24
4.3 Logging in to Web Interface.....	25

---

<b>5 Troubleshooting.....</b>	<b>26</b>
<b>Appendix 1 Thunder-Poof and Surge Protection.....</b>	<b>27</b>
<b>Appendix 2 RS-485 Cable.....</b>	<b>29</b>
<b>Appendix 2.1 Basic Features.....</b>	<b>29</b>
<b>Appendix 2.2 Common Issues in Use.....</b>	<b>29</b>
<b>Appendix 2.3 FAQ on RS-485 Cable.....</b>	<b>30</b>
<b>Appendix 3 Wire Gauge Reference Sheet.....</b>	<b>31</b>
<b>Appendix 4 Security Commitment and Recommendation.....</b>	<b>32</b>

# 1 Overview

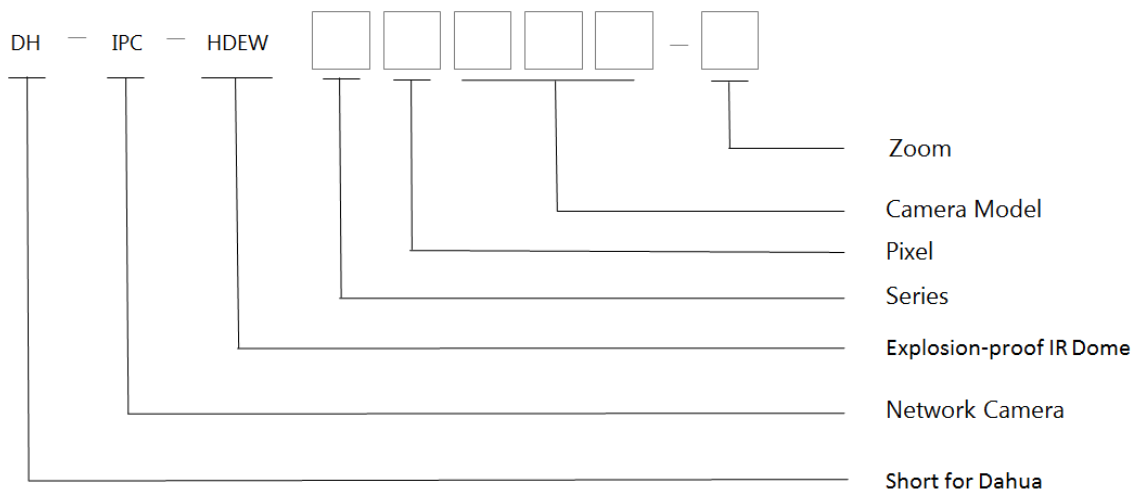
## 1.1 Introduction

As a new generation of explosion-proof monitoring device, the Camera uses more advanced manufacturing technology, so that the quality, performance and appearance outperform the competitors. It adopts new design in structure and the engineering construction is simple. Moreover, the installation will not affect the overall aesthetic look of the monitoring site. The Camera has features such as clear image, digitization, intelligence, and easy installation.

The Camera is designed and manufactured in strict accordance with standards such as IEC60079-0:2017, IEC60079-1:2014, IEC60079-31:2013, EN60079-0:2018, EN 60079-1:2014, EN 60079-31:2014. The enclosure is rated IP68. The Camera can be widely used in oil, chemical engineering, wharf, port, mine, aerospace, food processing, and other sites.

## 1.2 Naming Rule

Figure 1-1 Naming rule



Model	Description
DH-IPC-HDEW8441R-Z	Dahua 4MP Camera
IPC-HDEW8441R-Z	General 4MP Camera
DH-IPC-HDEW8441RP-Z	Dahua 4MP Camera (PAL standard)
IPC-HDEW8441RP-Z	General 4MP Camera (PAL standard)
DH-IPC-HDEW8441RN-Z	Dahua 4MP Camera (NTSC standard)
IPC-HDEW8441RN-Z	General 4MP Camera (NTSC standard)
DH-IPC-HDEW8241R-Z	Dahua 2MP Camera
IPC-HDEW8241R-Z	General 2MP Camera
DH-IPC-HDEW8241RP-Z	Dahua 2MP Camera (PAL standard)
IPC-HDEW8241RP-Z	General 2MP Camera (PAL standard)
DH-IPC-HDEW8241RN-Z	Dahua 2MP Camera (NTSC standard)



Model	Description
IPC-HDEW8241RN-Z	General 2MP Camera (NTSC standard)
DH-IPC-HDEW8841R-Z	Dahua 8MP Camera
IPC-HDEW8841R-Z	General 8MP Camera
DH-IPC-HDEW8841RP-Z	Dahua 8MP Camera (PAL standard)
IPC-HDEW8841RP-Z	General 8MP Camera (PAL standard)
DH-IPC-HDEW8841RN-Z	Dahua 8MP Camera (NTSC standard)
IPC-HDEW8841RN-Z	General 8MP Camera (NTSC standard)
IPC-HDEW8441R-Z-27135-316	General 4MP Camera (Model for Eastern Europe)
IPC-HDEW8441R-Z-27135-316-CER	General 4MP Camera (Model for Eastern Europe with certification sign)

### 1.3 Application

#### Explosion-Proof Sign and Application


- IECEx mark:
  - ◇ Ex db IIC T6/T5 Gb
  - ◇ Ex tb IIIC T80 °C /T100 °C Db
  - ◇ T5/T100 °C: -40 °C ≤ Tamb ≤ +60 °C
  - ◇ T6/T80 °C: -40 °C ≤ Tamb ≤ +55 °C
- ATEX mark:
  - ◇  II 2 G D
  - ◇ Ex db IIC T6/T5 Gb
  - ◇ Ex tb IIIC T80 °C /T100 °C Db
  - ◇ T5/T100 °C: -40 °C ≤ Tamb ≤ +60 °C
  - ◇ T6/T80 °C: -40 °C ≤ Tamb ≤ +55 °C

Figure 1-2 Explosion proof sign information (1)

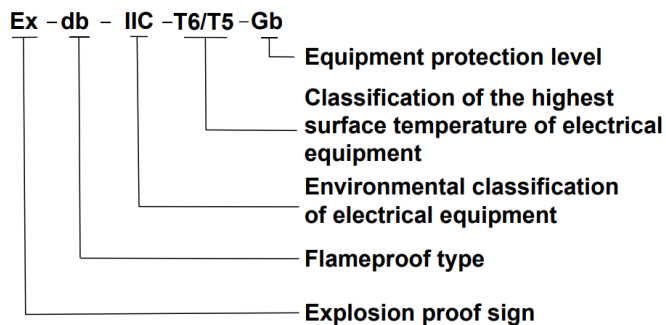
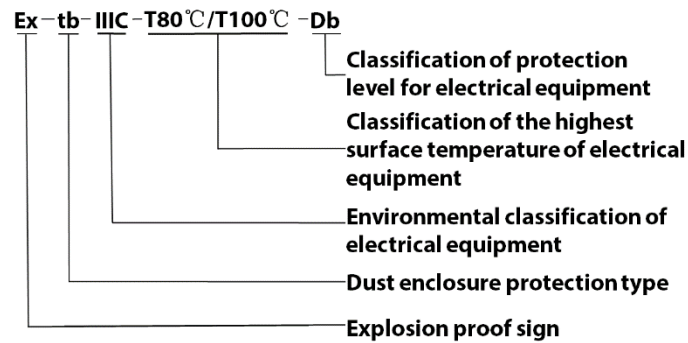


Figure 1-3 Explosion proof sign information (2)



Suitable for area 1&2 with explosive gas (IIA, IIB, IIC), and area 21 & 22 with explosive dust (IIIA, IIIB, IIIC).



Do not open the camera when power is on or under the environment with explosive gas.

## 1.4 Mechanical Structure

### 1.4.1 Mechanical Specification

Table 1-1 Mechanical specification

Parameter	Description
Material	316L stainless steel by default; stainless steel 304 customizable
IP rating	IP68
Cable outlet hole	1
Cable outlet hole thread	G 3/4 thread (for external connection)

### 1.4.2 Explosion-proof Structure

- The enclosure design of the Camera guarantees that no external explosion, caused by internal operation when explosive gas mixture gets inside, can happen. Several factors have been considered to guarantee the explosion-proof performance, such as enclosure intensity, junction surface gap and length among components, and maximum surface temperature of the enclosure.
- After the welding and finish machining, the enclosure can sustain the severe hydrostatic test. With 10 s –20 s 2 Mpa test pressure, there is no water dripping and deformation.
- When the Camera is working normally, the maximum surface temperature of the enclosure is no more than:
  - ◇ 80°C; under the environment with T6 explosive gas and ambient temperature: -40°C to +55°C;
  - ◇ 100°C; under the environment with T5 explosive gas and ambient temperature: -40°C to +60°C;

- The observation window is made of tempered glass, and it has passed impulse test and thermal shock test.
- (IP) degree of protection of enclosure: IP68 (1 m/1 h).
- The Camera adopts gland packings to lead the cable in, which makes the cable fully compressed without loosen.

## 1.5 Electric Specification

Table 1-2 Electric specification

Parameter	Description
Input voltage	12 VDC
Maximum current	≤ 0.7 A
Power consumption	≤ 8.4 W
Electrical connection	Power, Ethernet, audio ports, alarm and RS-485 port on the control cable by default.

### Power Standard

- Make sure that the power supply is correct before operating the device. Strictly follow the local electrical safety standards.
- Strictly follow the power supply requirements of the device.
  - ◇ Use the power adapter of a regular brand with UL, CE\FCC and other related certifications passed.
 

Input the rated voltage 12 VDC ( $\pm 10\%$  voltage) and input the rated current 2A power adapter to supply power to the device.
  - ◇ Provide stable long-time power supply.
  - ◇ The power adapter provided with the Camera is recommended.
  - ◇ If power adapter does not come with the Camera, select a power source that complies with IEC62368-1/IEC60950-1. IEC62368-1 requires compliance with ES1 (Electrical Energy Source Class 1) and PS1/PS2 (Power Source Class 1 or 2) classification standards and Limited Power Source Standards. IEC60950-1 requires compliance with SELV (Safety Extra-low Voltage Circuit) and Limited Power Source standards.
- Install cables with easy-to-use circuit breaker, which is for emergent power off when necessary.
- Do not tread or put pressure on the power cable, especially the plug, the outlet and the connection point where the cable comes out.

## 1.6 Environment Requirements

Table 1-3 Environment requirements

Parameter	Description
Air pressure	80 kPa–110 kPa
Operating temperature	T5/T100 °C: $-40\text{ }^{\circ}\text{C}$ to $+60\text{ }^{\circ}\text{C}$ ; T6/T80°C: $-40\text{ }^{\circ}\text{C}$ to $+55\text{ }^{\circ}\text{C}$
Operating humidity	≤ 85% (RH)

Special conditions of use:

1. End user shall comply with the manufacture's User manual to minimize the risk from electrostatic discharge: Conductors and live parts are prohibited from contacting the non-metallic enclosure during normal operation of the equipment. Use insulators to contact non-metallic enclosures during maintenance.
2. Tamb1: -40°C to +60°C.  
Tamb2: -40°C to +55°C.

Other Notes:

- Special temperature range: T5/T100°C:  $-40\text{ °C} \leq T_{amb} \leq +60\text{ °C}$ , T6/T80°C:  $-40\text{ °C} \leq T_{amb} \leq +55\text{ °C}$ . You can use a soft damp cloth to wipe the body of the device. While using the device, do not touch metal objects to prevent electrostatic discharge.
- The Camera is delivered with an eight-meter control cable. The external wiring of the Camera should be carried out with the device that meets explosion-proof requirements or under safe area environment. The wire diameter size for external wiring allowed for 8.5mm (Do not replace the cable randomly. Confirm with the manufacturer if you do need to replace it).
- Tightening torque of the compression component  $\geq 25.5\text{ Nm}$ .
- Yield strength of fastening bolt:  $> 450\text{ MPa}$ .
- Make sure that all the explosion-proof components are complete without any cracks and defects.
- Install the Camera in a stable place that does not shake and does not have shock vibrations or insulation-break vapor. Securely install the Camera to make sure that it remains still and does not move in either direction.
- Do not touch the heat dissipation components of the Camera to avoid getting burnt.
- Do not disassemble the Camera unprofessionally. Otherwise, it might cause water leakage or bad image. If you find that the lens is foggy or the desiccant turns green after disassembling the device, contact the after-sales service to replace the desiccant. (Some model may not have the desiccant particles, and the actual conditions shall prevail.)
- It is recommended to use the Lightning Protector for better lightning-proof effect.
- Do not touch the image sensor (CMOS) directly. Dust and dirt could be removed with soft cloth that is moistened with alcohol.
- Clean the device body with soft dry cloth, and for stubborn stains, use the cloth with mild detergent. To avoid possible damage on device body coating which could cause performance to decrease, do not use volatile solvent such as alcohol, benzene, diluent and so on to clean the device body, nor can strong, abrasive detergent be used.
- Dome cover is an optical component. Do not touch or wipe the cover with your hands directly during installation or operation. To remove dust, grease or fingerprints, wipe gently with oil-free cotton moistened with diethyl or moistened soft cloth. You can also remove dust with an air blower.
- Use a wet cloth to clean the transparent cover. The transparent cover has a potential electrostatic charge hazard.
- Strengthen the protection of network, device data and personal information by adopting measures which include but not limited to using strong password, changing password regularly, upgrading firmware to the latest version, and isolating computer network. For some devices with old firmware versions, the ONVIF password will not be changed automatically along with the change of the system password, and you need to upgrade the firmware or manually update the ONVIF password. Updating firmware will optimize the functions of the Camera without consuming more power.
- Use standard components or accessories provided by manufacturer and make sure that the device is installed and maintained by professional engineers.

## 1.7 Repair and Maintenance

### 1.7.1 Notes to Maintenance

- Equipment maintenance units or individuals must have relevant explosion-proof qualifications and should understand the requirements of national regulations and standards related to maintenance work.
- You should understand whether the repair unit meets related conditions, especially the conditions of the processing equipment and personnel directly related to the repair work. If you repair the device by yourself, learn relevant regulations and standards first.
- The inspection and repair of the flameproof enclosure should be carried out in accordance with the current national technical regulations. Do not modify and replace the shell structure, the materials and dimensions of the main components, such as explosion-proof joint surfaces, dome cover and encapsulation components, cable entry devices, fasteners. Destruction of explosion-proof performance, such as drilling holes in the shell, shall not be carried out without the agreement of the inspection agency and the manufacturer.
- If there are any doubts about the repair method, ask the manufacturer or the explosion-proof inspection unit.
- Cut off the power before camera maintenance and overhaul, and consult after-sales service to make sure that the device installation area is safe.
- Make sure that the power is off when you connect the cables, install or uninstall the Camera.
- If the Camera will not be used for a long time, unplug the power cable.
- Keep the packing box well for future transportation.

### 1.7.2 Preparation

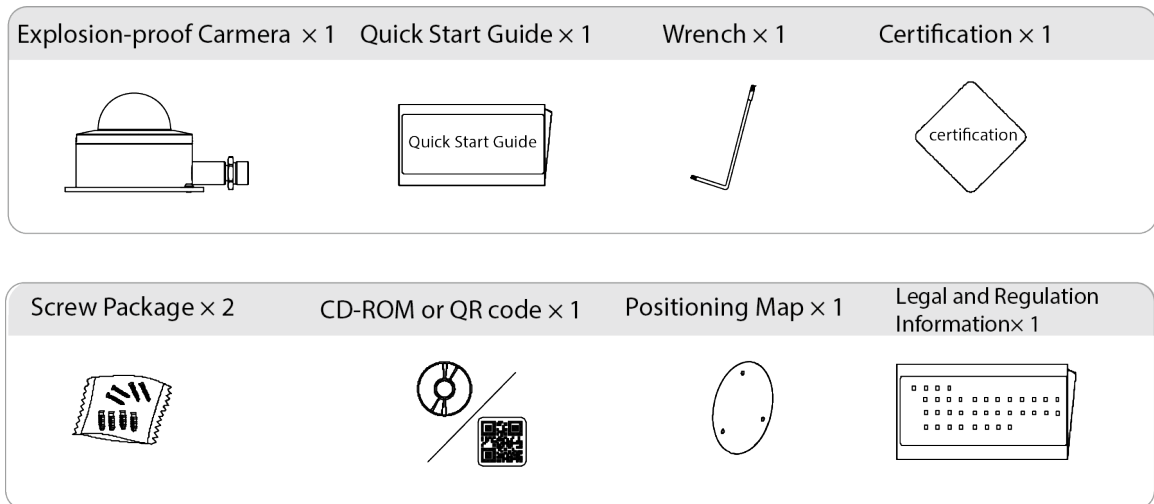
- Before repair: Clarify the maintenance content and prepare the tools, materials and instrument needed; cut off the power first and confirm the scope of the power outage; distinguish the nature of the overhaul site, the degree of danger in the explosion hazard place, and category of hazardous area.
- When inspecting and repairing in explosion-hazardous area, the specified explosion-proof tools are needed. The instruments used for inspection and repair must also be explosion-proof.
- In allowed conditions, move the explosion-proof cameras that need to be overhauled away from the original area for repair.
- When disassembling and assembling parts related to explosion-proof performance, the explosion-proof performance of other parts must not be damaged. Explosion-proof surface cannot have any scratches.
- Carry out a comprehensive inspection and debugging before putting the device into use after maintenance. In case of restoring electrical performance, the Camera can be put into operation only if the explosion-proof performance is restored.

## 2 Installation Preparation

### 2.1 Packing List

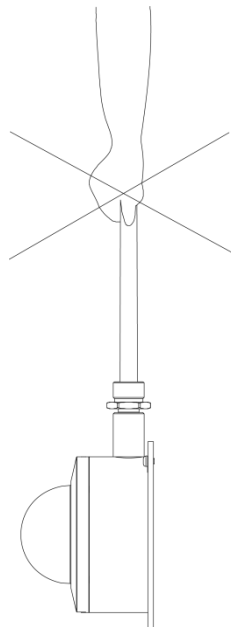
After unpacking, check whether there is obvious damage to the appearance, and check whether the accessories are complete against the packing list. If everything is fine, you can start to install the Camera.

Figure 2-1 Packing list



Do not drag or pull the cables to lift the Camera when carrying it.

Figure 2-2 Wrong way of carrying the camera

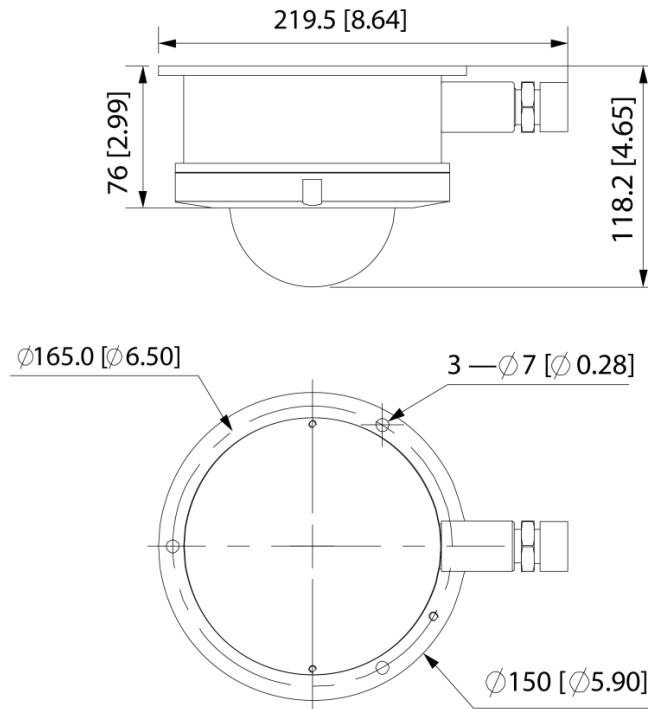


## 2.2 Dimensions



The following figure is for reference only, and the actual product shall prevail.

Figure 2-3 Dimensions (mm [inch])



## 2.3 Cable Connection

### 2.3.1 Cable Description

When delivered out of factory, the Camera is connected with a composite cable. The cable threads out from the outlet hole at the Camera rear, and it is 8 m by default. The diameter of the cable is 8.5 mm.



The cables vary with the product models, and the actual cables shall prevail. The manual will introduce the cables as complete as possible.

Figure 2-4 Cables

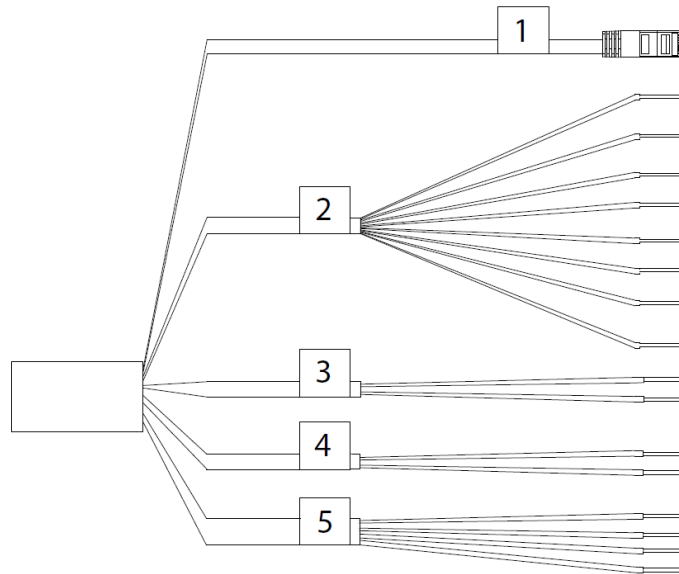


Table 2-1 Cable description

No.	Description	No.	Description
1	Ethernet port.	4	Power port. <ul style="list-style-type: none"> <li>● Red: 12 VDC+</li> <li>● Black: 12 VDC-</li> </ul>
2	Alarm I/O port. <ul style="list-style-type: none"> <li>● Brown: Alarm output 1</li> <li>● Green: Alarm output 1 ground</li> <li>● Blue: Alarm input 1</li> <li>● White: Alarm input 2</li> <li>● Gray: Alarm input ground</li> <li>● White-yellow: Alarm input 3</li> <li>● Red: Alarm output 2</li> <li>● Black: Alarm output 2 ground</li> </ul>	5	Audio port. <ul style="list-style-type: none"> <li>● White-Red: Audio input+</li> <li>● White-orange: Audio input-</li> <li>● Pink: Audio output+</li> <li>● Purple: Audio output-</li> </ul>
3	RS-485 port. <ul style="list-style-type: none"> <li>● Yellow-black: A+</li> <li>● Yellow: B-</li> </ul>	—	—

Table 2-2 Cable information

No.	Port name	Description
1	Ethernet port	Connects to network with network cable.
2	Alarm I/O	Includes alarm signal input and output ports, the number of I/O ports might vary on different devices.
3	RS-485	Controls external devices, such as PTZ.







No.	Port name	Description
4	12 VDC power input	Inputs 12 VDC power. Be sure to supply power as instructed in the manual.  Device abnormality or damage might occur if power is not supplied correctly.
5	Audio input/output	Connects to sound pickups to receive audio signal, or connect to speaker to output audio signal.  Audio input/output is available on select models.

Table 2-3 Alarm information

Port	Port Name	Description
Alarm I/O	ALARM_IN	Receives the switch signal of external alarm source.
	ALARM_GND	 Connect different alarm input devices to the same ALARM_IN_GND port.
	ALARM_OUT	Outputs alarm signal to alarm device.
	ALARM_OUT_GND	 When connecting to alarm device, only the ALARM_OUT port and ALARM_OUT_GND port with the same number can be used together.

## 2.3.2 Connecting the Alarm Cable



Alarm input/output is available on select models.

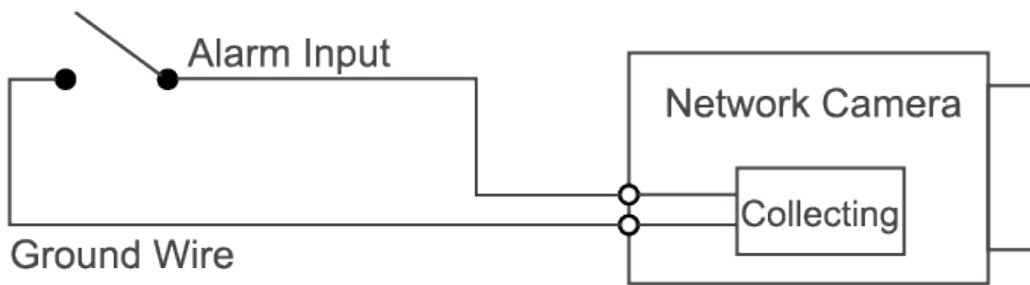
### Procedure

**Step 1** Connect alarm input device to the alarm input end of the I/O port.

Device collects different states of alarm input port when the input signal is idling and being grounded.

- Device collects logic "1" when input signal is connected to +3 V to +5 V or idling.
- Device collects logic "0" when input signal is grounded.

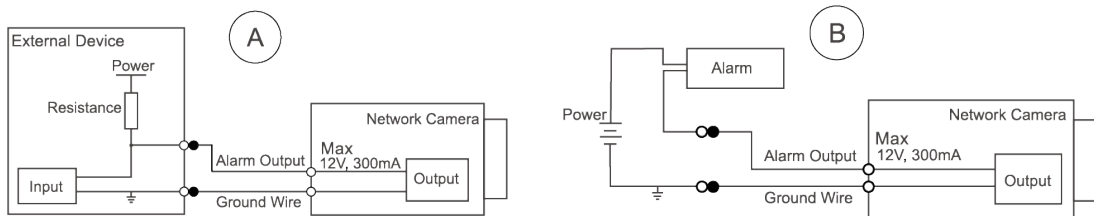
Figure 2-5 Alarm input



**Step 2** Connect alarm output device to the alarm output end of the I/O port. The alarm output is open-drain output, which works in the following modes.

- **Mode A: Level application.** Alarm outputs high and low level, and the alarm outlet is OD, which requires external pull-up resistance (10K Ohm typical) to work. The maximum external pull-up level is 12 V, maximum port current is 300mA and the default output signal is high-level (external pull-up voltage). The default output signal switches to low- level when there is alarm output.
- **Mode B: Switch application.** Alarm output is used to drive external circuit, the maximum voltage is 12 V and the maximum current is 300 mA. If the voltage is higher than 12 V, please use an additional electric relay.

Figure 2-6 Alarm output



**Step 3** Log in to web interface, and configure alarm input and alarm output in alarm setting.

- The alarm input on the web interface is corresponding to the alarm input end of the I/O port. There will be high level and low level alarm signal generated by the alarm input device when alarm occurs, set the input mode to "NO" (default) if the alarm input signal is logic "0" and to "NC" if the alarm input signal is logic "1".
- The alarm output on the web interface is corresponding to the alarm output end of the device, which is also alarm output end of the I/O port.

### 2.3.3 Connecting the Explosion-Proof Flexible Tube

Before connecting the composite cable, you need to make it explosion-proof. The common method is to cover the cable with an explosion-proof flexible tube.

#### Procedure

- Step 1** Cover the cable with the explosion-proof flexible tube, remove the compression nut, and fix explosion-proof flexible tube to external 3/4 thread.

Figure 2-7 Installation of explosion-proof flexible tube (1)

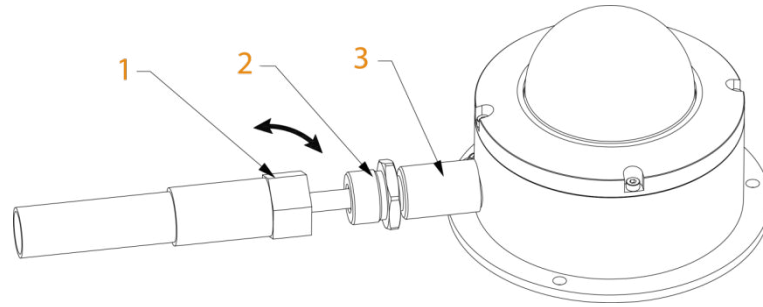


Table 2-4 Flexible tube installation (1)

No.	Description
1	Explosion-proof flexible tube
2	Ex certified compression nut
3	Outlet hole

**Step 2** Tighten the thread connector and then the explosion flexible tube.

Figure 2-8 Installation of explosion-proof flexible tube (2)

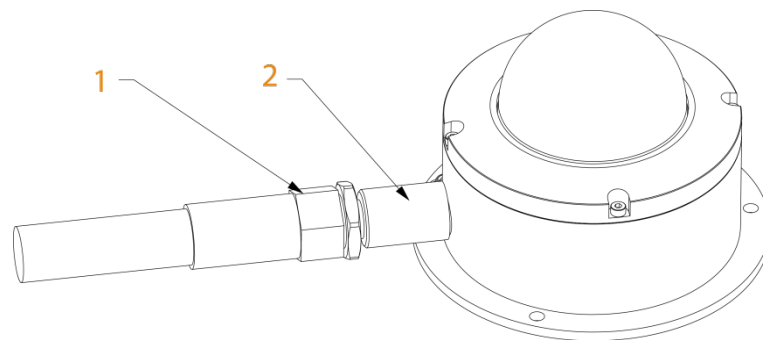


Table 2-5 Flexible tube installation (2)

No.	Description
1	Explosion-proof flexible tube
2	Outlet hole

### 2.3.4 Grounding Description

Make sure that the Camera is properly grounded. Grounding wire of external bonding should meet the requirements in IEC60079-0:17 sheet 12.

Figure 2-9 External grounding mark

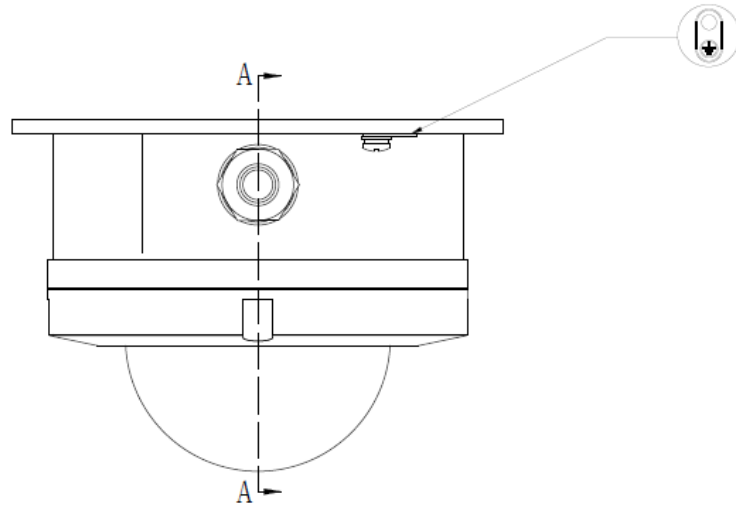
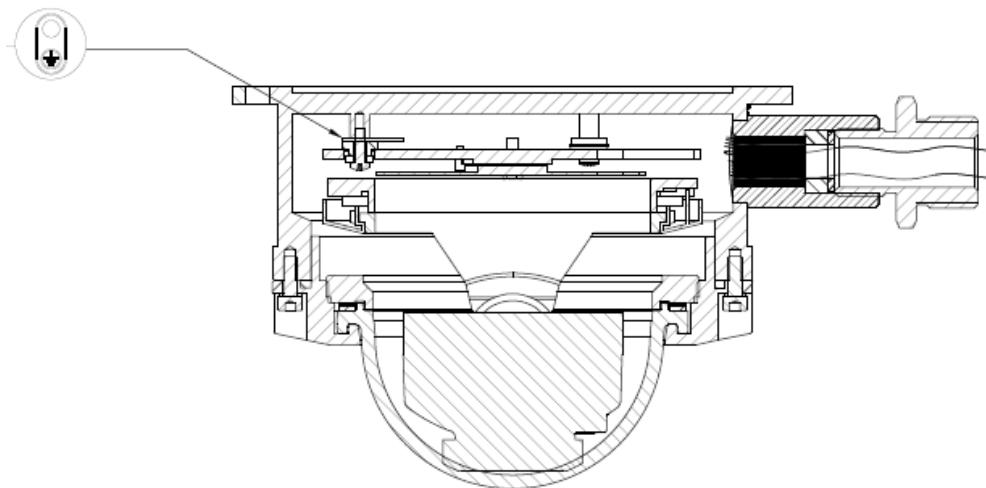


Figure 2-10 Internal grounding mark



## 2.4 Cable Preparation

Select the cables depending on the transmission distance.

RS-485 cable requirement: When using the 0.56 mm (24 AWG) twisted-pair line, depending on different baud rates, the theoretical maximum transmission distance are different. For details, see Table 2-6 .

Table 2-6 Theoretical maximum transmission distance

Baud Rate	Maximum Transmission Distance
2400 bps	1800 m
4800 bps	1200 m
9600 bps	800 m

The maximum transmission distance will be reduced in the following conditions: When thinner communication cables are used; the Camera is used in places with intense electromagnetic interference; too many devices are connected to the RS-485 cable.

## 3 Device Installation



- Equipment maintenance units or individuals must have relevant explosion-proof qualifications and should understand the requirements of national regulations and standards related to maintenance work.
- Make sure that the power is off when you connect the cables, install or uninstall the Camera.
- In allowed conditions, move the explosion-proof cameras that need to be overhauled away from the original area for repair.
- When disassembling and assembling parts related to explosion-proof performance, the explosion-proof performance of other parts must not be damaged. Explosion-proof surface cannot have any scratches.

### 3.1 Installation Conditions

#### 3.1.1 Installation Accessories and Tools

For the installation accessories and tools, see Figure 3-1 . For the wall mount bracket, see Figure 3-2 .

Figure 3-1 Accessories and tools

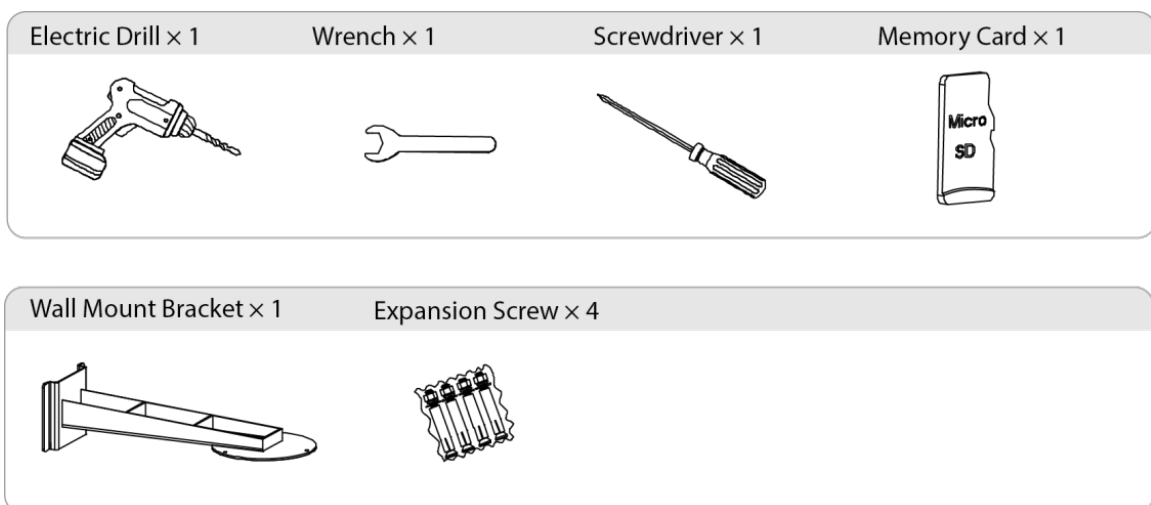
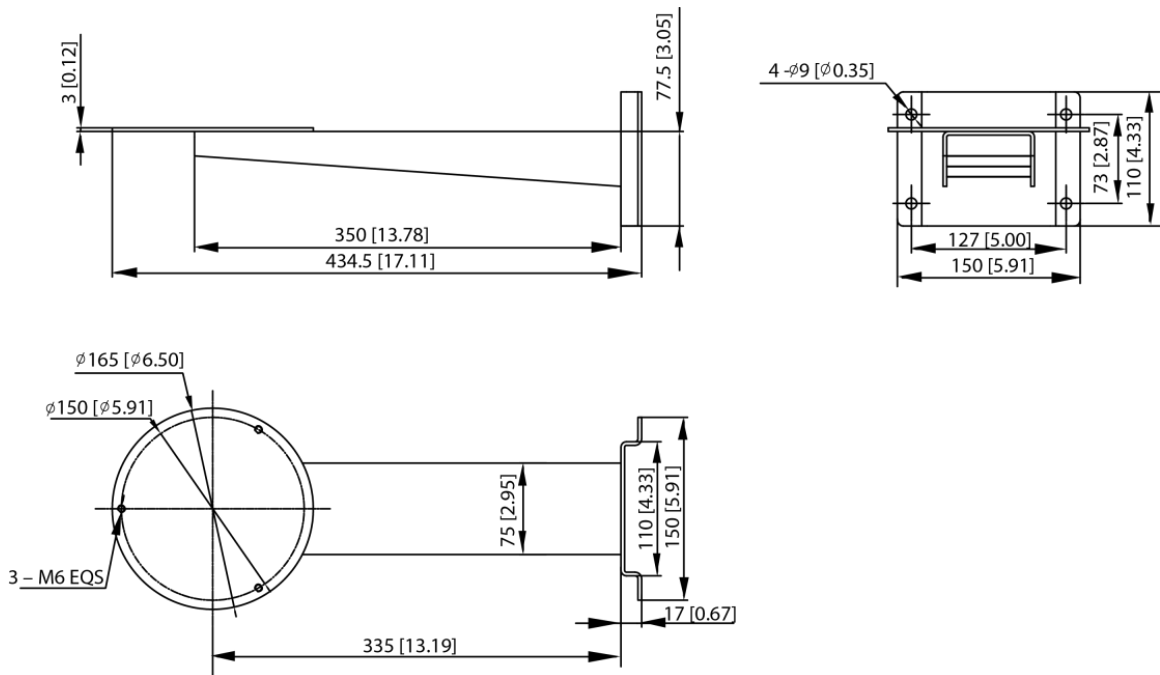


Figure 3-2 Wall mount bracket (mm [inch])

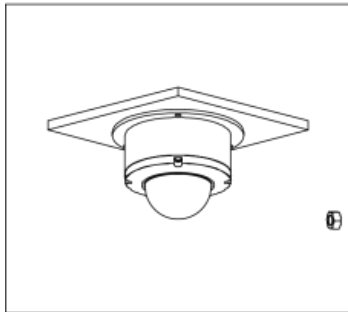


### 3.1.2 Precautions before Installation

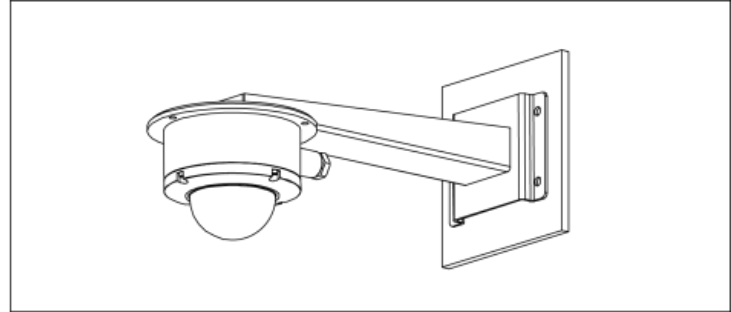
- Use the power supply specified in "1.5 Electric Specification".
- Always use the Camera under the air pressure, operating temperature and operating humidity specified in "1.6 Environment Requirements".
- Explosion-proof cameras are special. Power and debug them indoors, and familiarize the features of them before installation.
- Keep the original packing material well because you might need it to pack the Camera and send it back for repair if any problem arise.
- Make sure that the place where the Camera is installed has enough space to hold the Camera and its mounting accessories.
- Make sure that the ceiling and wall can sustain 8 times the weight of the Camera and its mounting accessories.
- Make sure that the wall is thick enough to install expansion bolts (Users need to buy expansion bolts separately).

## 3.2 Installation Method

Figure 3-3 Installation method



Wall Mount



Ceiling Mount

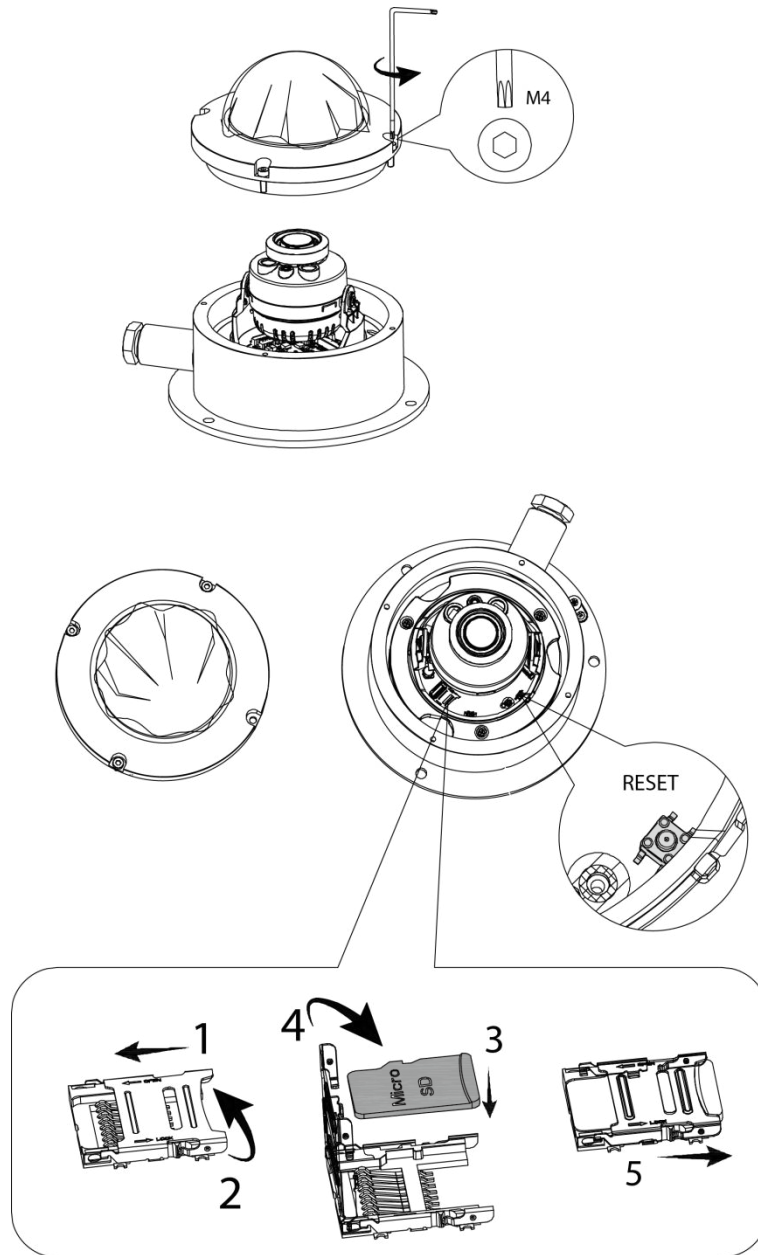
## 3.3 (Optional) Installing SD Card



- SD card slot is available on select models.
- Disconnect the power before installing or removing the SD card.
- Do not open the cover for more than 30 min to avoid spray in cameras.
- Press and hold the reset button for 10 seconds to default the device.



Figure 3-4 Installing SD card



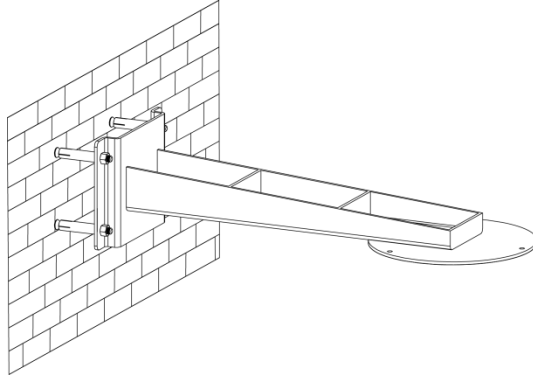
## 3.4 Installation Procedure

### 3.4.1 Wall Mount

#### Procedure

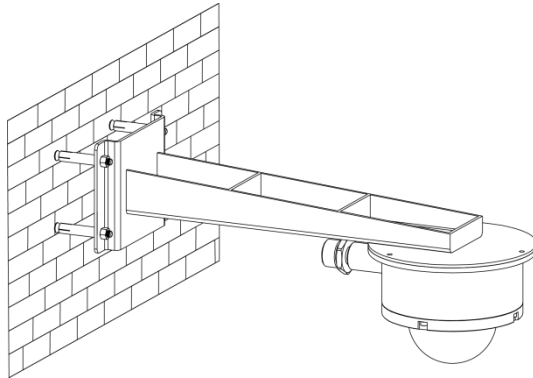
Step 1 Fix the wall mount bracket on the wall through 4 expansion screws.

Figure 3-5 Install the wall mount bracket



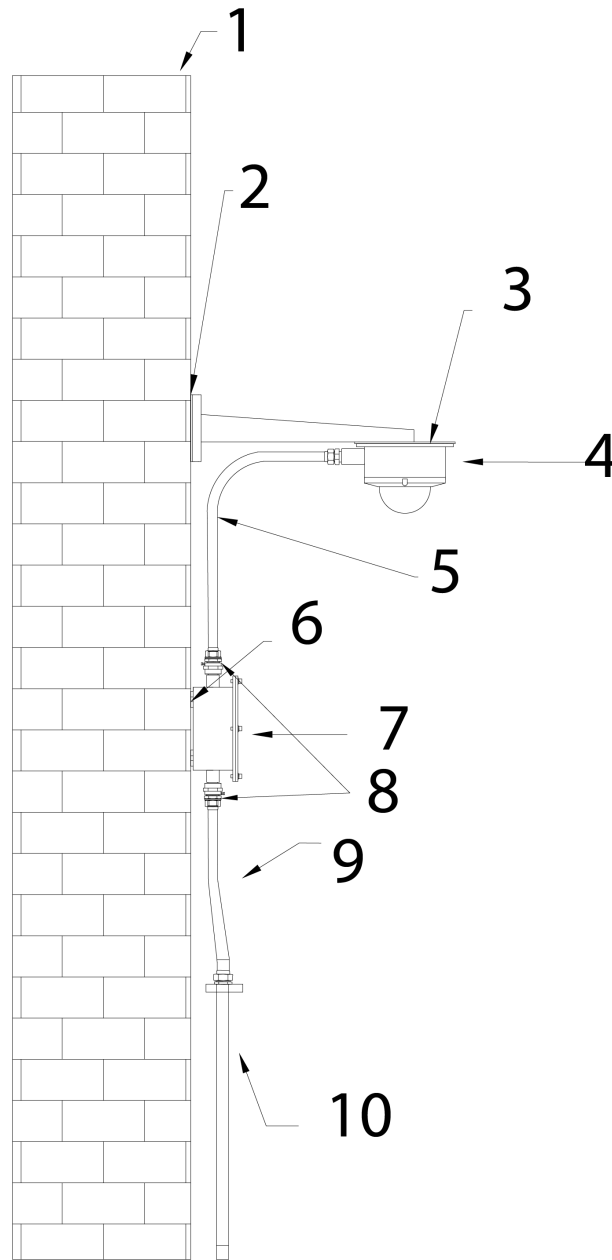
Step 2 Use 3 M6×14 inner hexagon screws and nuts to fix the universal joint on the bracket.

Figure 3-6 Install the universal joint



Step 3 Connect the cables among the Camera, bracket, flexible tube, and control cabinet.

Figure 3-7 Cable layout



For the details of connecting explosion-proof flexible tube, see "2.3.3 Connecting the Explosion-Proof Flexible Tube". For the cable connection, see "2.3.1 Cable Description".



Make sure that the installation surface can withstand at least three times the combined weight of the bracket and the device to be installed.

Table 3-1 Cable layout description

No.	Description
1	Wall
2	4 screws used to fix the bracket on the wall

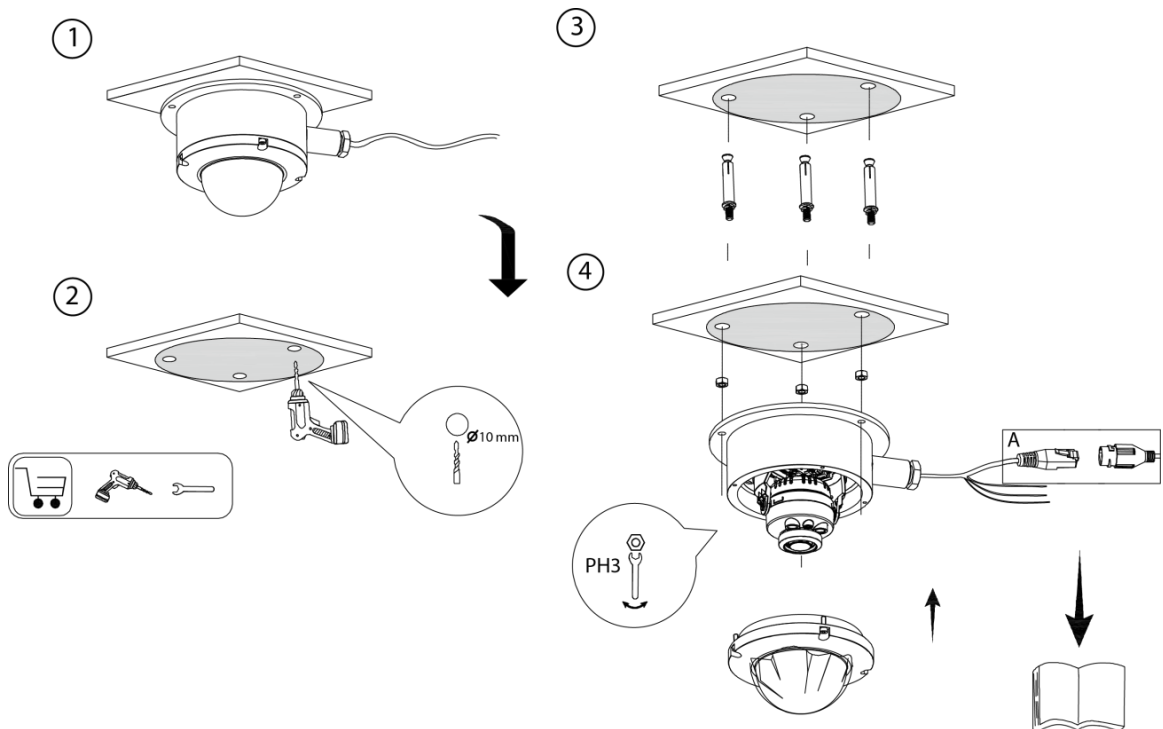
No.	Description
3	3-M6 inner hexagon screws
4	Explosion-proof camera
5	Explosion-proof flexible tube
6	4 screws used to fix the bracket on the wall
7	Explosion-proof flexible box
8	Explosion-proof stuffing box
9	Explosion-proof flexible tube
10	Galvanized steel pipe connected to the terminal

### 3.4.2 Ceiling Mount

#### Procedure

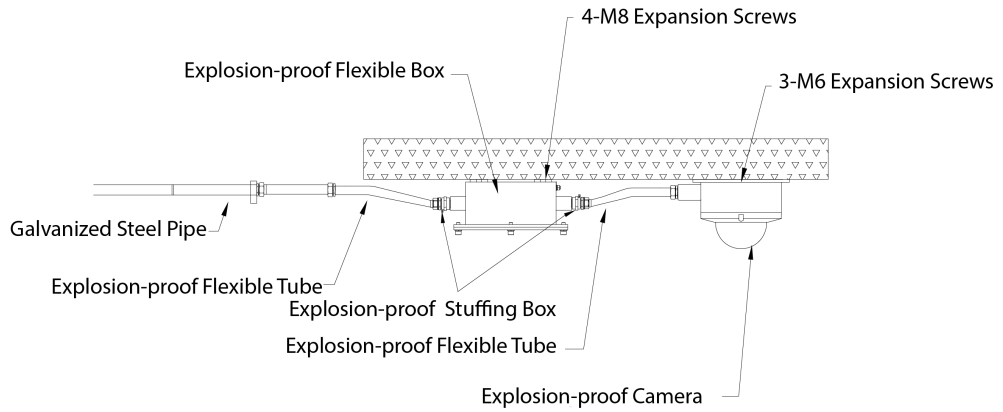
**Step 1** Fix the explosion-proof camera on the wall through 3 expansion screws.

Figure 3-8 Install the camera



**Step 2** Connect the cables among the Camera, bracket, flexible tube, and control cabinet.

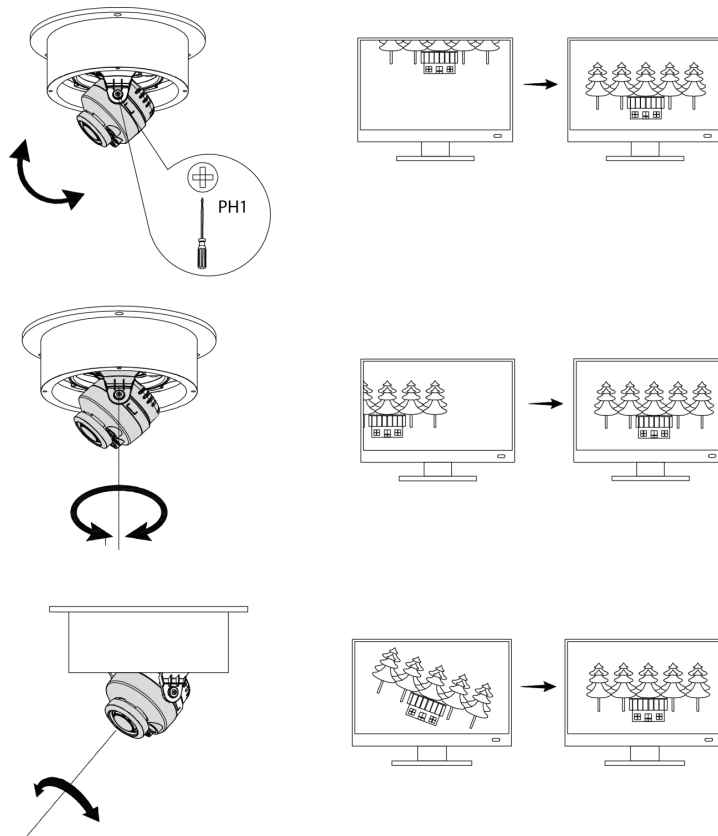
Figure 3-9 Ceiling mount



Use the wet cloth to clean the transparent cover. The transparent cover has a potential electrostatic charge hazard.

### 3.4.3 Adjusting Lens Angle

Figure 3-10 Adjusting Lens Angle



# 4 Network Configuration

Device initialization and IP setting can be finished with the **ConfigTool** or on web interface. For more information, see the Web Operation Manual.



- Device initialization is available on select models, and it is required at first-time use and after device is being reset.
- Device initialization is available only when the IP addresses of the device (192.168.1.108 by default) and the PC stay in the same network segment.
- Plan usable network segment properly to connect the device to the network.
- The following figures and interfaces are for reference only, and the actual product shall prevail.

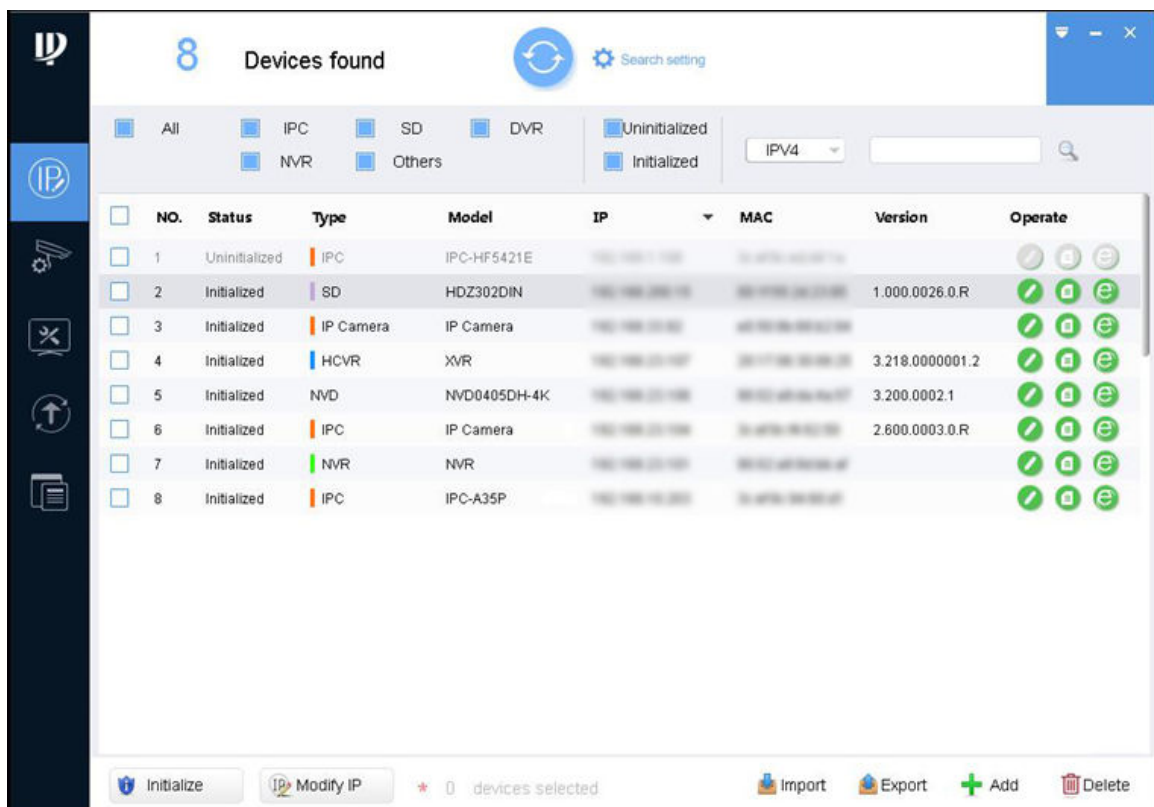
## 4.1 Initializing Device

### Procedure

**Step 1** Double-click **ConfigTool.exe** to open the tool.

**Step 2** Click .

Figure 4-1 Modify IP



**Step 3** Click **Search setting**.

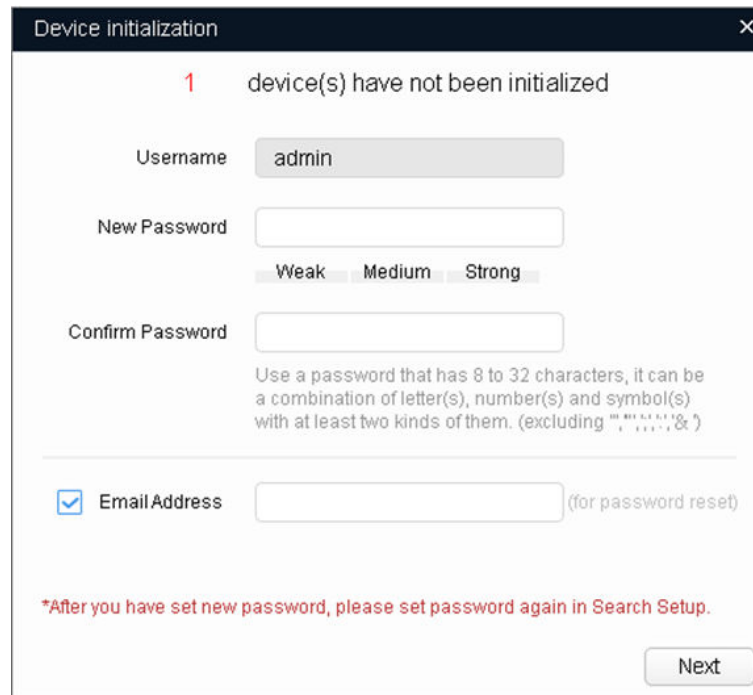
**Step 4** Enter the start IP address and end IP address of the network segment in which you want to search devices, and then click **OK**.

All the devices found in the network segment are listed.

**Step 5** Select one or several devices in uninitialized status, and then click **Initialize**.

**Step 6** Select the devices that need initialization, and then click **Initialize**.

Figure 4-2 Password setting



**Step 7** Set and confirm the password of the devices, then enter a valid email address, and then click **Next**.

The final setting interface is displayed.



Password can be modified or reset in **System Settings**.

**Step 8** Select the options according to your needs, and then click **OK**.

The **Initialization** interface is displayed after initialization is completed. Click the success icon (✓) or the failure icon (⚠) for the details.

**Step 9** Click **Finish**.

The device status on the **Modify IP** interface turns to **Initialized**.

## 4.2 Modifying Device IP Address

### Prerequisites

- You can modify IP address of one or multiple devices at one time. This section is based on modifying IP addresses in batches.
- Modifying IP addresses in batches is available only when the corresponding devices have the same login password.

### Procedure

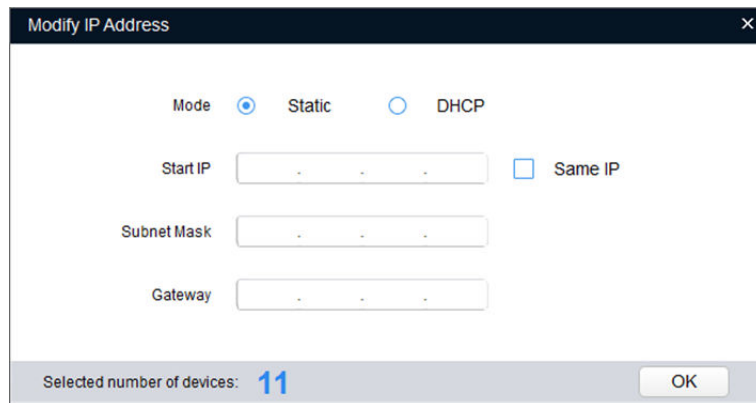
**Step 1** Do **Step 1** to **Step 4** in "4.1 Initializing Device" to search devices in your network segment.



After clicking **Search setting**, enter the username and password, and make sure that they are the same as what you set during initialization; otherwise there will be wrong password notice.

Step 2 Select the devices whose IP addresses need to be modified, and then click **Modify IP**.

Figure 4-3 Modify IP address



Step 3 Select **Static** mode, and then enter start IP, subnet mask, and gateway.



- IP addresses of multiple devices will be set to the same if you select the **Same IP** check box.
- If DHCP server is available in the network, devices will automatically obtain IP addresses from DHCP server when you select **DHCP**.

Step 4 Click **OK**.

## 4.3 Logging in to Web Interface

### Procedure

Step 1 Open IE browser, enter the IP address of the device in the address bar, and then press **Enter** key.

If the setup wizard is displayed, finish the settings as instructed.

Step 2 Enter the username and password in the login box, and then click **Login**.

Step 3 For the first-time login, click **Click Here to Download Plugin**, and then install the plugin as instructed.

The main interface is displayed when the installation is finished.



## 5 Troubleshooting

For the malfunctions, possible reasons and solutions, see Table 5-1 .

Table 5-1 Troubleshooting

Malfunction	Possible Reason	Solution
After being powered on, the Camera does not perform self-check, and there is no image.	<p>If the red LED light on power board is off:</p> <p>The power supply is not connected to the socket of the power board or the contact is poor.</p> <p>Mains electricity is cut off or there is transformer failure.</p>	<p>Check whether the power supply is connected, and make sure that the socket body is in good contact.</p> <p>Check whether the mains electricity is normal, and whether the transformer is working normally.</p>
	<p>If the red LED light on the power board is on:</p> <p>The Camera is damaged.</p> <p>There is power board failure.</p>	<p>Use another camera.</p> <p>Contact the supplier to replace the power board.</p>
Self-check cannot be performed, or there is noise when the self-check is performed.	Insufficient power supply.	Use the power supply meeting requirement.
	There is mechanical fault.	Contact after-sales service for overhaul.
Unstable image.	Poor contact between the cables.	Connect the cables again.
Blurry video	The focus is in manual status.	Operate the Camera and adjust the focus.
	The glass is dirty.	Clean the glass.

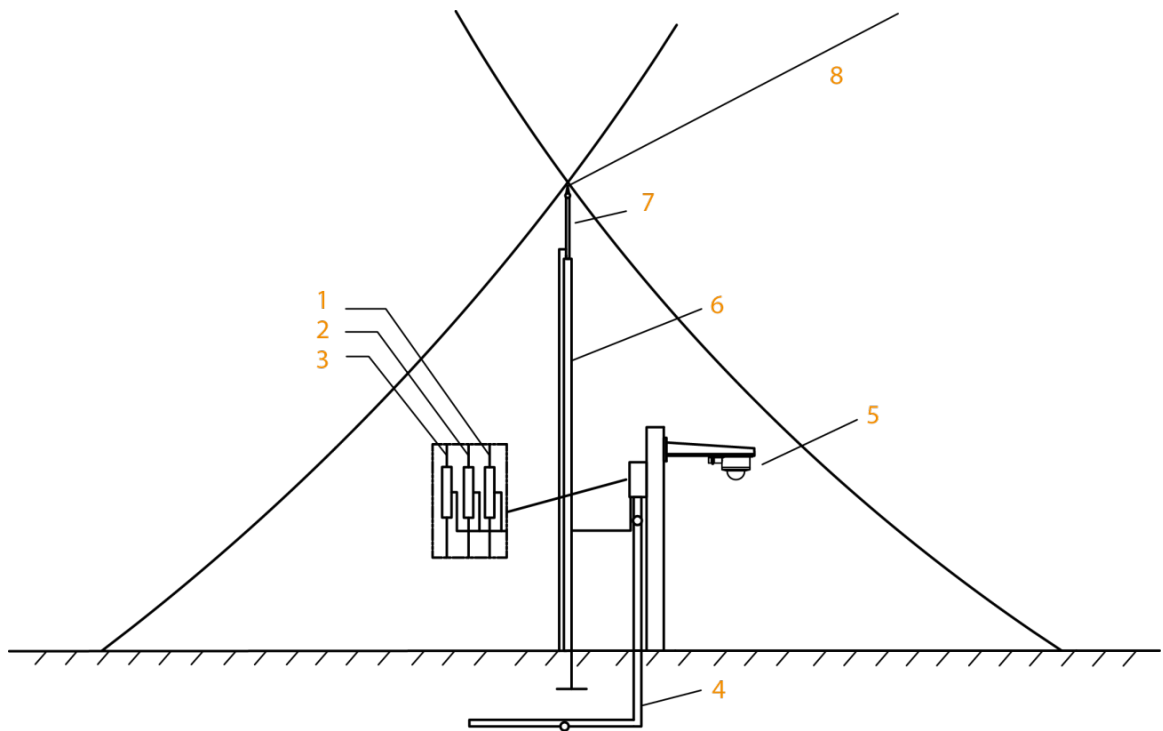
# Appendix 1 Thunder-Poof and Surge Protection

Transient voltage suppressor (TVS) is applied to protect the Camera against voltage spikes and overvoltage below 2 KV (cable to ground) and 1 KV (cable to cable). However, it is still necessary to do operations to protect the Camera depending on local electrical safety regulations.

- The signal transmission cable must stay at least 50 m away from high voltage devices and high voltage wire.
- When laying cables outdoors, try to lay them under the eaves.
- At open places, lay cables underground by means of hermetic steel tube, and then do equipotential grounding to both ends of steel tubes. Laying overhead power cables is prohibited.
- At places with severe thunderstorms and induced voltage (like substation), you need to prepare high-powered lightning protection devices and lightning conductors.
- The thunder protection and earth grounding of the outdoor devices and cables shall be considered based on the whole thunder protection of the building and conform to local or industry standards.
- You must do equipotential grounding to the electric system. The grounding device must meet the demand of anti-jamming and also conforms to your local electrical safety code. The grounding device shall not form short circuit to N (neutral) line of high voltage power grid or be mixed with other wires. When the electrical system is connected to the ground cable, the impedance cannot exceed 4Ω, and the cross-sectional area of the earth lead cannot exceed 25 mm<sup>2</sup>.

For the installation of lightning protection devices outdoors, see Appendix Figure 1-1 .

Appendix Figure 1-1 Install lightning protection devices outdoors (1)

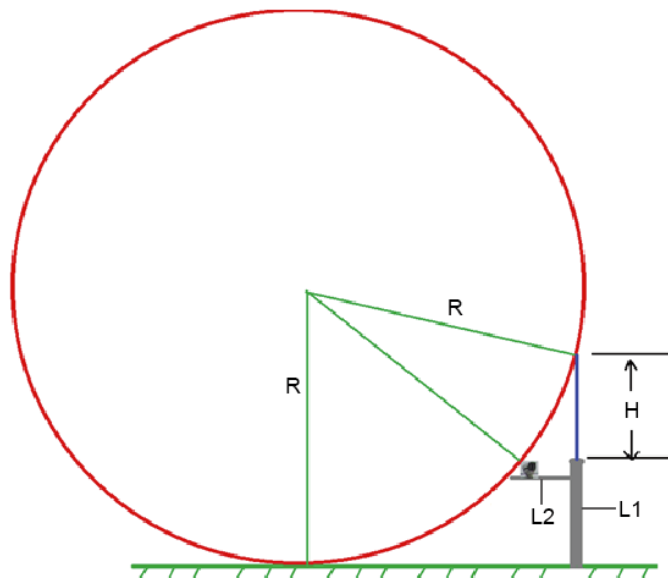


Appendix Table 1-1 Installing lightning protection devices outdoors

No.	Description
1	Video lightning conductor.

No.	Description
2	Communication lightning conductor.
3	Power supply lightning conductor.
4	Steel tube.
5	Explosion-proof camera: Must be installed in the arc formed by the 60-m circle, the lightning conductor top and the ground.
6	Impedance of the cable connected to the grounding wire should be less than 4 $\Omega$ .
7	Lightning conductor.
8	The radius is 60 m.

Appendix Figure 1-2 Installing lightning protection devices outdoors (2)



- R: The radius of the circle, and R=60 m.
- L1: The length of the pole that holds the lightning conductor.
- L2: The length of the rail that holds the Camera.
- H: The length of the lightning conductor.

To get the value of L1, you need to use the formula:  $\left(\sqrt{R^2 - [R - (L1 + H)]^2} - L2\right)^2 + (R - L1)^2 = R^2$

## Appendix 2 RS-485 Cable

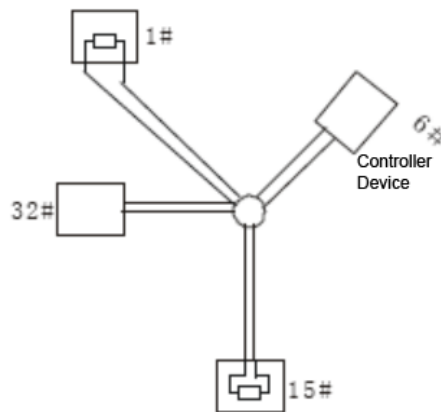
### Appendix 2.1 Basic Features

RS-485 industrial buses are half-duplex communication buses whose characteristic impedance is 120 Ω. Its maximum load is 32 payloads (including controller devices and controlled devices).

### Appendix 2.2 Common Issues in Use

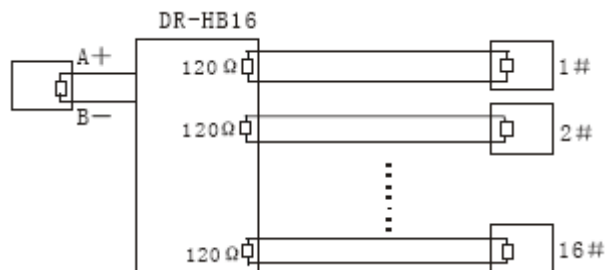
Users tend to connect devices in the way displayed in Appendix Figure 2-1 . In this case, the terminal resistance must be connected to the two devices whose cable length is the longest among all the devices (in Appendix Figure 2-1 , cable length between 1# and 15# is the longest). However, this connection does not comply with the RS-485 industry standard. As a result, common issues like signal reflection and anti-interference capability reduction will occur. And the reliability of the control signal will decrease. Therefore, the Camera will be out of control or cannot stop.

Appendix Figure 2-1 Common method to connect devices



To fix the issues, we recommended to use RS-485 distributors. The RS-485 distributor can help avoid the common connection method to improve transmission reliability. See Appendix Figure 2-2 .

Appendix Figure 2-2 Connecting method with RS-485 distributors



## Appendix 2.3 FAQ on RS-485 Cable

Appendix Table 2-1 Malfunction, possible reason and solution

Malfunction	Possible Reason	Solution
The Camera can perform self-check, but is out of control.	Baud rate/address of the host and Camera are not matched.	Modify the baud rate/address of the host or Camera to be matched.
	Positive electrode and negative electrode of RS-485 cable are misconnected.	Connect cables to the positive electrode and negative electrode correctly.
	Loose connection.	Connect the cables firmly.
	RS-485 cable is broken.	Replace RS-485 cable.
The Camera can be controlled, but the operation is not smooth.	RS-485 cable is in poor contact.	Connect the RS-485 cable firmly.
	A RS-485 cable is broken.	Replace RS-485 cable.
	The distance between the host and Camera is too long.	Install terminal resistance.
	Too many cameras are connected parallelly.	Install RS-485 distributors.

## Appendix 3 Wire Gauge Reference Sheet

Appendix Table 3-1 Wire gauge reference sheet

Metric Bare Wire Diameter (mm)	AWG	SWG	Bare Wire Cross Section Area (mm <sup>2</sup> )
0.050	43	47	0.00196
0.060	42	46	0.00283
0.070	41	45	0.00385
0.080	40	44	0.00503
0.090	39	43	0.00636
0.100	38	42	0.00785
0.110	37	41	0.00950
0.130	36	39	0.01327
0.140	35	/	0.01539
0.160	34	37	0.02011
0.180	33	/	0.02545
0.200	32	35	0.03142
0.230	31	/	0.04115
0.250	30	33	0.04909
0.290	29	31	0.06605
0.330	28	30	0.08553
0.350	27	29	0.09621
0.400	26	28	0.1257
0.450	25	/	0.1602
0.560	24	24	0.2463
0.600	23	23	0.2827
0.710	22	22	0.3958
0.750	21	/	0.4417
0.800	20	21	0.5027
0.900	19	20	0.6362
1.000	18	19	0.7854
1.250	16	18	1.2266
1.500	15	/	1.7663
2.000	12	14	3.1420
2.500	/	/	4.9080
3.000	/	/	7.0683

## Appendix 4 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

### Account Management

#### 1. Use complex passwords

Please refer to the following suggestions to set passwords:

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

#### 2. Change passwords periodically

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

#### 3. Allocate accounts and permissions appropriately

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

#### 4. Enable account lockout function

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

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

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

## Service Configuration

### 1. Enable HTTPS

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

### 2. Encrypted transmission of audio and video

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

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

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

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

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

### 4. Change HTTP and other default service ports

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

## Network Configuration

### 1. Enable Allow list

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

### 2. MAC address binding

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

### 3. Build a secure network environment

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

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

## Security Auditing

### 1. Check online users

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

### 2. Check device log



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

3. **Configure network log**

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

## Software Security

1. **Update firmware in time**

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

2. **5.2 Update client software in time**

We recommend you to download and use the latest client software.

## Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: [www.dahuasecurity.com](http://www.dahuasecurity.com) | Postcode: 310053

Email: [dhoverseas@dhvisiontech.com](mailto:dhoverseas@dhvisiontech.com) | Tel: +86-571-87688888 28933188