

Thermal Explosion-proof Bullet Camera

User's Manual



V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the thermal explosion-proof bullet camera (hereinafter referred to as "the Camera"). Read carefully before using the device, and keep the manual safe for future reference.

Models

Type/model description:

aTPC-AEBFxy0mn

a: Can be DHI- or blank to represent the brand of the manufacture;

x: Can be 1 to 9 to represent the series of the product;

y: Can be 1 to 9 or A to represent the resolution of image;

m: Can be 1 to 9 for commercial use;

n: Can be A to Z or blank for commercial use;

Ex Marking

 II 2 G Ex db IIC T6 Gb
II 2 D Ex tb IIIC T80°C Db IP68

Safety Instructions

The following signal words 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, reductions in performance, or unpredictable results.
 LASER RADIATION	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	November 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, 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: 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

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

Transportation Requirements



- Do not place heavy stress on the device, allow it to fall, violently vibrate or immerse it in liquid during transportation. Handle the device with care to avoid damaging the internal precision parts.
- The complete package is necessary for transportation and storage. It is strictly forbidden to transport the device without full packaging. Whether it is delivered by the contractor or returned to the factory for repair, we will assume no responsibility for any damage or problems caused during transportation due to the incomplete package being sent.

Storage Requirements



- Store the device under allowed humidity and temperature conditions.
- Do not place the device in a humid, dusty, extremely hot or cold site that has strong electromagnetic radiation or poor ventilation.
- Do not place heavy stress on the device, allow it to fall or collide with other objects, violently vibrate or immerse it in liquid during storage.

Installation Requirements



DANGER

- All service personnel must have required certification or qualified training for performing installations and maintenance of electric apparatuses in environments that have explosive gas. They must also be trained and certified to work at heights, and must have knowledge and skills in the following areas:
 - ◇ Basic knowledge and skills in installing CCTV system and components.
 - ◇ Basic knowledge and skills in low-voltage wiring and in connecting low-voltage electronic circuits.
- All installation and operations must conform to the local electrical safety code and standards.
- Strictly comply with the local electrical safety code and standards, and check whether the power supply is correct before operating the device.
 - ◇ When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.
 - ◇ We recommend using the power adapter provided with the device.
 - ◇ The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- Make sure that the power is off when you connect the cables, install or disassemble the device.

- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- Protect the power cord and wires from being walked on or squeezed particularly at plugs, power sockets, and the point where they exit from the device.
- Do not expose the device to heat sources such as a radiator, heater, stove or other types of heating equipment. This is to avoid the risk of fire.
- Do not connect multiple devices to the same power adapter to avoid the risk of overheating or fire if the rated load is exceeded. Please use the power adapter provided by the manufacturer.

 WARNING

- A high joule surge protector must be installed when using the device in environments with strong thunder storms or high induced voltage, such as in high voltage transformer substations.
- We recommend you use the device with a lightning protection device for stronger protection against lightning. For outdoor scenarios, strictly comply with the lightning protection regulations. The device must be installed by a certified lightning protection contractor.
- The lightning protection standards of buildings must be taken into consideration when designing the lightning protection and grounding for outdoor circuits. They must conform to the related national and industrial standards. The grounding device must meet the dual requirements of system anti-interference and electrical safety, and must not be short-circuited or mixed with the neutral line of the strong power grid.



- Appropriate brackets must be installed when the device cannot be used alone.
- Do not pull on the cable to avoid damaging the device.
- Do not place heavy stress on the device, allow it to collide with other objects, and do not violently vibrate or immerse it in liquid during installation.
- Do not connect the device to two or more kinds of power supplies, to avoid safety risks and damage to the device.
- Do not expose the device to environments with strong magnetic fields to avoid damage to the device.
- Do not install the device in an environment that has strong vibrations, such as in a vehicle or ship.
- Remove the electrostatic film from the visible window and the thermal imaging lens cover after installation is complete.
- Do not block the ventilation opening near the device to avoid the device being damaged from heat accumulation.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- Make sure a durable and reliable waterproof treatment has been applied to the connectors of the network and power cables, to avoid damaging the device.
- Protect the accessories that come with the device for future maintenance and debugging.
- Make sure that the device is installed horizontally (the bubble inside the spirit level stays in the middle), and on a stable surface that is resistant to deformation.
- Power on the device for inspection of basic functions before installing it in a high location. This is to avoid reinstalling it if it behaves abnormally.
- Do not place the device in environments with smoke, vapor, heavy dust, or that have high temperatures to avoid damage to the device.
- If a circular connector comes with the device, make sure it is securely screwed in place. Otherwise,

the device might behave abnormally due to erosions or oxidation of the connector or the pins.

- Make sure the wire diameter of the cables meets the requirements of the corresponding distance to avoid equipment damage caused by undervoltage and overcurrent.
- Do not aim the lens at intense radiation sources (such as the sun, lasers and molten steel) to avoid damage to the thermal detector and the visible lens.
- After unpacking, even if the packing bag is damaged or leaking air, and the desiccant particles are different colors, the normal use of the device will not be affected.
- Around 2.5 m control cable is provided when the device is delivered out of factory. When connected to the explosion-proof control cabinet, the control cable should be protected by explosion-proof flexible tube or armor cable.

Operation Requirements



DANGER

- Apply the following information when the device is being used in the environment of area 21 and 22 with explosive dust, and area 1 and 2 with explosive air. Applicable air pressure: 86 kPa–116 kPa; ambient temperature: –40 °C to +60 °C; relative humidity: No more than 95% (+25 °C).
- Do not insert foreign matter into the device to avoid the risk of short circuits, damaging the device and injuring people.



WARNING

- Make sure the explosion-proof components are complete without any cracks or defects.
- Do not touch the heat dissipation component of the device to avoid getting burnt.



- Do not use a temperature measuring device to measure temperatures that extend beyond its measuring range.
- Do not stain or damage optical components such as the lens and glass.
- Prevent liquid from flowing into the device to avoid damage to its internal components.
- Do not place the device in a highly humid, extremely hot or cold site.
- Use the device within the allowed humidity (less than 95% RH) and altitude (less than 3000 m) conditions.
- The operating temperature of the device must meet the requirements. Refer to the device specifications for information on the allowed temperature and humidity conditions.
- Do not expose the device to corrosive environments such as coastal areas, sea areas with thick salt fog, environments with acid gas, chemical plants and the seaside.
- There is a limit to the life cycle of the quick-wear parts. Make sure to use them correctly, and follow the manufacturer's recommendations and guidance. Log in to the official website for instructions on using the quick-wear parts.
- Devices suitable for low temperature environments automatically preheat before they start to work when placed in a low temperature environment. The preheat time depends on the ambient temperature. When it heats to a suitable temperature, the device starts to work normally.
- Rating: 12 VDC, 1 A, 3 W Max.

Maintenance Requirements



WARNING

- The maintenance personnel of the camera must have required certification or qualified training

for installing closed-circuit television (CCTV) systems. They must also be trained and certified to work at heights, and must have knowledge and skills in the following areas:

- ◇ Basic knowledge and skills in installing CCTV systems and components.
- ◇ Basic knowledge and skills in low-voltage wiring and in connecting low-voltage electronic circuits.
- Cut off the power before cleaning the device to avoid the risk of electrocution.
- Do not turn on the device in the environment with explosive gas.
- The cover must not be opened while the device is powered on.



- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- Clean the device body with a soft dry cloth. If there are any stubborn stains, clean them away with a soft cloth dipped in a neutral detergent, and then wipe the surface dry. Do not use volatile solvents such as ethyl alcohol, benzene, diluent, or abrasive detergents on the device to avoid damaging the coating and degrading the performance of the device.
- Use a clean cloth or lens wipe to gently wipe off the dust on the visible window. Dried stains can be washed with clean water or ordinary diluted detergent. Do not use alkaline detergents to clean the device, and do not vigorously wipe the device with a damp cloth to avoid permanently damaging the glass.

Repair Requirements



WARNING

Do not allow liquid to get into the device to avoid damage to the internal components. If any liquid flows into the device, immediately disconnect the power supply, unplug all the cables connected to the device, and contact after-sales service.



- Use the accessories suggested by the manufacturer. Repair must be performed by qualified professionals.
- If the device produces smoke, an odd odor, noise, or behaves faulty, cut the power immediately, and contact the local dealer or service center at your earliest convenience. Do not disassemble the device. We assume no responsibility for issues caused by uninstructed maintenance.

Laser Requirements



LASER RADIATION

If the device is equipped with a laser beam, pay extra attention to the following:

- The laser can cause permanent damage to human eyes and skin within safe distance. Keep the device a safe distance away from humans while installing or operating the device.
- Do not use the distance measurer to measure the distance of targets that are within 50 m of the laser. The laser can permanently damage the device.
- Laser radiation can ignite flammables. Do not directly expose objects (excluding scattered or absorber) to the laser beam, and do not place volatile flammables (such as alcohol) in the working area of laser radiation products, to avoid producing laser beams or fire caused by sparks from high voltage discharge.
- Clear all the reflective objects from the working area of laser radiation products. The reflected or

scattered beam of a laser can cause severe damage to eyes. Take necessary precautions when reflective objects are required for use, to minimize its reflecting and scattering range.

- Before dismantling or moving the device to another location, wait 5 minutes after the laser distance measurer finishes operating, so that the accumulated electrons inside the device can be fully discharged. This is to avoid the risk of electrocution.
- Do not touch the circuit of the distance measurer while the device is in a working state, especially the power supply of the laser, which possesses thousands of volts of voltage.
- Install the device with laser function within 3 m of distance, and make sure there are no objects obstructing it to avoid the risk of laser burn and fire.
- When using a laser beam device, avoid exposing the device surface to laser beam radiation.

Explosion-Proof Structure Declarations

- The casing is designed to not cause external explosions due to the operation of its internal electric apparatus even if an explosive gas mixture were to enter the device. Several factors were considered in designing the camera to guarantee that it is explosion-proof, such as the maximum surface temperature of the casing, casing intensity, the length between the components and the junction surface gap.
- Due to its welding and the finish machining of the casing, the device passed the hydrostatic test in IEC 60079-1:2014. The test pressure was 1.55 Mpa, lasting 10 s–12 s, and the result was no water leakage or deformation.
- When the device is working normally, the maximum surface temperature of the casing cannot exceed 80 °C.
- The casing is IP68 rated.
- The device uses compression nut equipment to lead the cable in, and fully compresses the cable without allowing it to become loose.

Special Use Condition

- Specific guidance noted to contact the original manufacturer for information on the dimension of the flameproof joints.
- CAUTION – USE FASTENERS WITH YIELD STRESS $\geq 450\text{Mpa}$.
- The external cable connections and plugs shall be protected by a type of Ex protection, and the installation shall comply with requirements of IEC 60079-14:2013.

Table of Contents

- ForewordI
- Important Safeguards and Warnings..... III
- 1 Packing List..... 1
- 2 Component Structure..... 2
 - 2.1 Dimensions 2
 - 2.2 Cables 3
- 3 Installing Cameras..... 4
 - 3.1 Cable Preparation..... 4
 - 3.2 Installation Site..... 5
 - 3.3 Installation Procedures..... 5
- 4 Basic Configuration 9
 - 4.1 Initializing Camera..... 9
 - 4.2 Modifying IP Address..... 9
 - 4.3 Live Video 10
- 5 Alarm Configuration 11
- Appendix 1 Lightning and Surge Protection..... 13
- Appendix 2 Cybersecurity Recommendations 14

1 Packing List

Check the package according to the following checklist. If you find something has been damaged or is missing, contact customer service.



Keep accessories safe for future use.

Table 1-1 Packing list

Name	Quantity
Thermal Explosion-proof Bullet Camera	1
Accessory Bag	1
Quick Start Guide	1
Legal and Regulatory Information	1

2 Component Structure

2.1 Dimensions



- The figures are for reference only, and might differ from the actual product.
- The mounting bracket does not come with the delivery. Please buy them if they are needed.

Figure 2-1 Component dimensions (mm [inch])

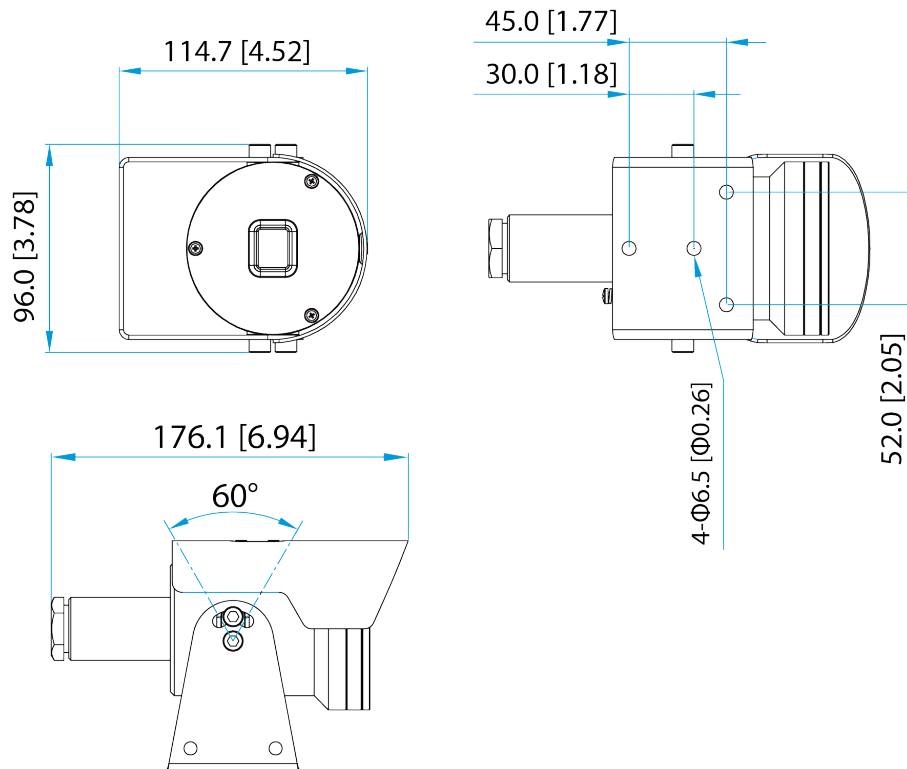
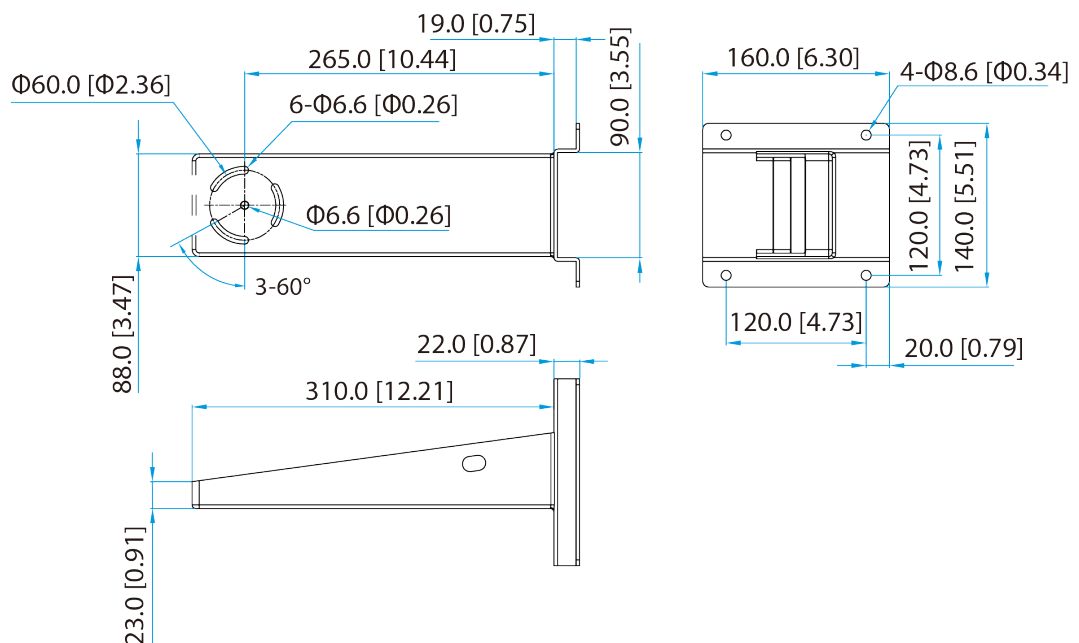


Figure 2-2 Dimensions of bracket (mm [inch])



2.2 Cables

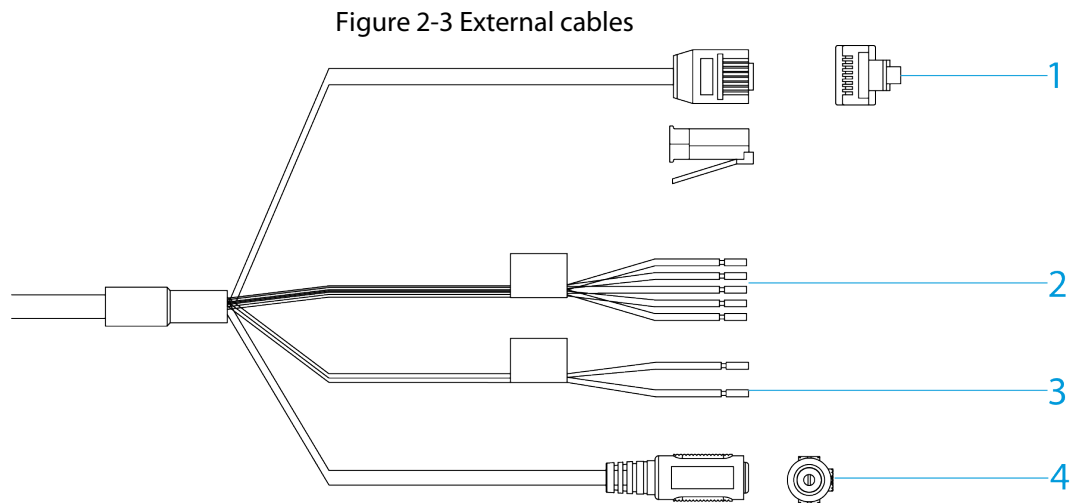


Table 2-1 Cable description

No.	Port	Port Name	Connector	Description
1	LAN	Network port	Ethernet port	Connects to standard Ethernet cable.
2	I/O	I/O port	—	Inputs and outputs alarm signals. For details, see Table 2-2
3	RS-485	RS-485_A	—	RS-485 port, controls external PTZs.
		RS-485_B		
4	POWER	Power input port	—	Power input port. Inputs 12 VDC.  Supply power to the Camera according to the label description.

Table 2-2 I/O port description

Port Name	No.	Cable port name	Description
I/O port	1	ALARM_IN1	Alarm input port, receives on-off signal from the external alarm devices.
	2	ALARM_IN0	
	3	ALARM_NO	Alarm output port, outputs alarm signal to alarm devices.  ALARM_NO can only be used together with ALARM_COM when connecting to alarm devices.
	4	ALARM_COM	
	5	GND	Ground terminal.

3 Installing Cameras



The figures are for reference only, and might differ from the actual cameras.

3.1 Cable Preparation

Power Cord

To extend the power cord you have received, evaluate the distance you want to extend to and select the appropriate cord diameter.

Table 3-1 Power cord description

Wire Diameter [inch (mm)]	Distance [ft (m)]
0.031 (0.80)	32.81 (10.00)
0.039 (1.00)	55.77 (17.00)
0.049 (1.25)	91.86 (28.00)
0.079 (2.00)	249.34 (76.00)
0.098 (2.50)	390.42 (119.00)

RS-485 Cable

When using a twisted pair that has a diameter of 0.56 mm (24AWG) as the communication cable, the value of the maximum transmission distance is different depending on the baud rate.

Table 3-2 Maximum transmission distance

Baud Rate (bps)	Maximum Transmission Distance [ft (m)]
2400	5905.51 (1800)
4800	3937.01 (1200)
9600	2624.67 (800)

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; many devices are connected to the RS-485 cable. Otherwise, maximum transmission distance will be increased.

Video Cable

- 75 Ω impedance.
- Full cable with copper conductor.
- 95% knitted copper shield.

Table 3-3 Video cable description

International Model	Maximum Transmission Distance [ft (m)]
RG59/U	750 (229)

International Model	Maximum Transmission Distance [ft (m)]
RG6/U	1000 (305)
RG11/U	1500 (457)

3.2 Installation Site

WARNING

- Make sure the mounting platform can sustain at least 8 times the weight of the Camera and its mounting structural components. The load bearing is at least 30 kg.
- Avoid dropping objects such as parts and tools of the Camera from high altitudes during installation to avoid people getting hurt and the Camera being damaged.
- For the explosion-proof products, power on the Camera indoor firstly and get familiar with the operation, and then install the Camera.

Figure 3-1 Installation site

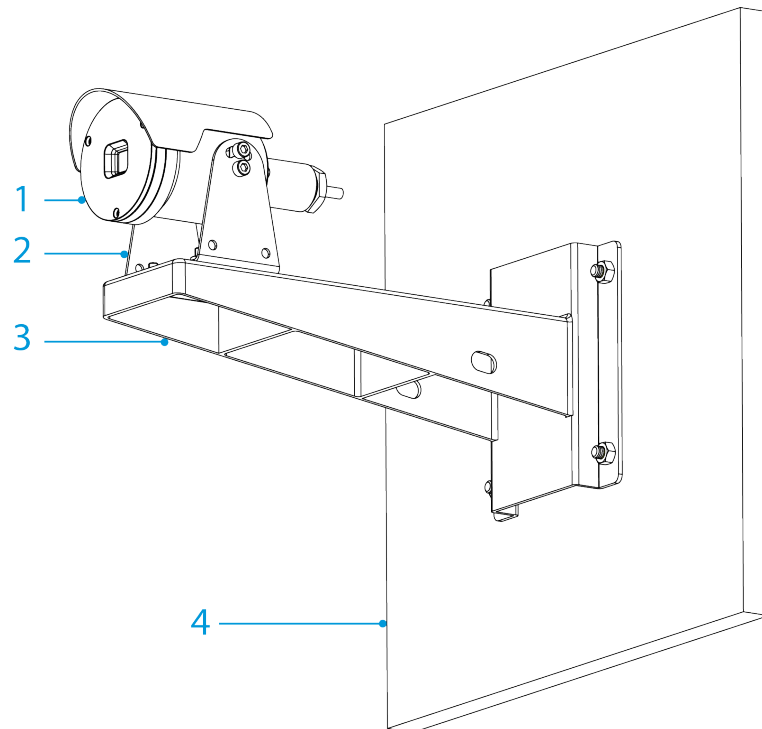


Table 3-4 Component description

No.	Name
1	Thermal explosion-proof bullet camera
2	Fixing bracket
3	Mounting bracket
4	Mounting surface

3.3 Installation Procedures

Step 1 Use the explosion-proof flexible tube connecting Cables.



- Choose between the explosion-proof flexible tube and the armored cable depending on the actual situation.
 - Two methods are needed with proper optional cables. The diameter of the lead-in cable needs to match that of the sealed rubber ring. You need to select the minimum diameter of lead-in cable according to the label of the sealed rubber ring. The thread specification of outlet hole of the lead-in device at the bullet rear is G-3/4. After tightening compression nut, make sure that the gap between sealed rubber ring and cable, and the gap between sealed rubber ring and lead-in device meet the explosion-proof requirements.
- 1) Wrap the cable with the explosion-proof flexible tube, remove the compression nut, and then save the gasket and the rubber ring.

Figure 3-2 Install explosion-proof flexible tube (1)

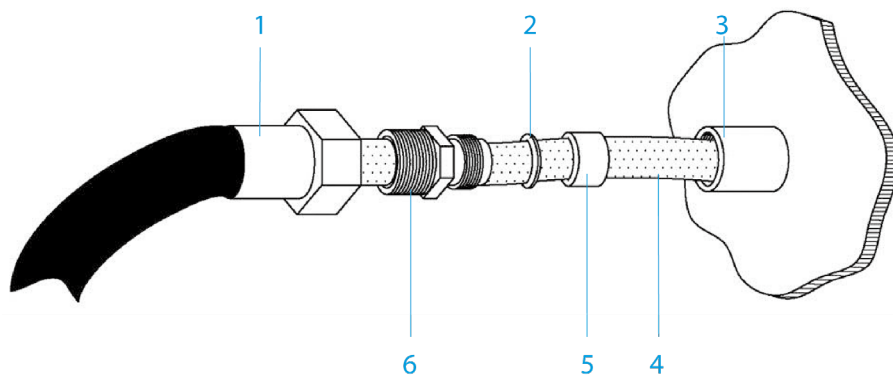


Table 3-5 Component description (1)

No.	Name
1	Explosion-proof flexible tube
2	Washer
3	Cable outlet hole
4	Threaded joint
5	Rubber ring
6	Outgoing cable

- 2) Tighten the thread connector and then the explosion-proof flexible tube.

Figure 3-3 Install explosion-proof flexible tube (2)

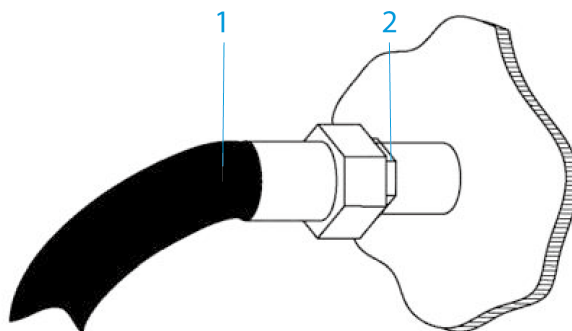


Table 3-6 Component description (2)

No.	Name
1	Explosion-proof flexible tube
2	Cable outlet hole

Step 2 Use armored cable.



You can directly connect the armored cable with explosion-proof gran to various explosion-proof equipment firmly.

- 1) You need to peel off the protective cover for a proper length to expose the armored cable (steel band). Then, you need to save a certain length of the steel band and remove the excessive part.

Figure 3-4 Install armored cable (1)

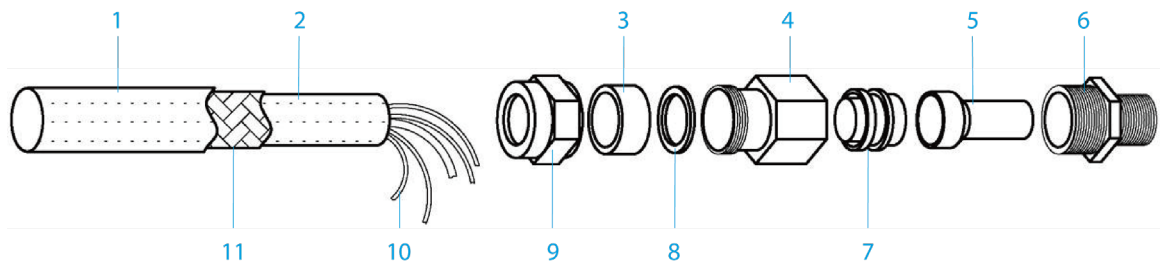


Table 3-7 Component description (3)

No.	Name
1	Protective cover of armored cable
2	Cable internal part
3	Rubber sealing ring
4	Stuffing box
5	Stuffing bush
6	Adapter
7	Cone and shrink ring
8	Gasket
9	Nut
10	Cable core
11	Steel band

- 2) Install the explosion-proof gran to the armored cable.

Figure 3-5 Install armored cable (2)

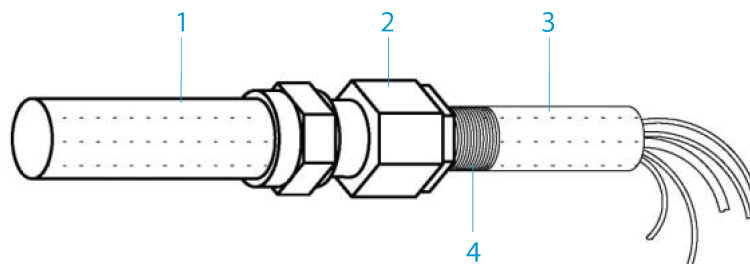


Table 3-8 Component description (4)

No.	Name
1	Protective cover of the armored cable
2	Installed explosion-proof gran
3	Inner of the cable
4	Thread

Step 3 Fix the Camera on the bracket.

- 1) Adjust the angle of the universal joint, install it on the bracket, and then tighten the screws.
- 2) Install the Camera on the universal joint, adjust the angle and tighten the screws, and then fix the Camera on the bracket.

Step 4 Fix the bracket on the installation surface.

- 1) Drill holes on the installation surface (wall or ceiling) according to the bottom holes of the installation bracket.



The size and depth of the holes must be matched with the expansion bolts. Make sure that there is no deviation.

- 2) Open the accessory bag, take out the expansion bolts and hammer them into the holes. Make sure the external terminals of the expansion bolts are parallel with the installation surface.
- 3) Open the accessory bag and take out the installation screws. Align the four bottom holes of the installation bracket with the installation holes of the four expansion bolts. Pass the installation screws through the bottom holes of bracket and screw them into the mounting holes of expansion bolts. Firmly tighten the four installation screws and fix the installation bracket on the installation surface.

Step 5 Connect the external cables of the Camera according to your requirements.

Step 6 Slightly adjust the shooting direction of the Camera.

- 1) Slightly loosen the fixing screws or the adjusting screws on the both sides of the universal joint, to adjust the Camera from four directions (up, down, left, right). Set the shooting direction according to your personal requirement.
- 2) Tighten the fixing screws or the adjusting screws on the both sides of the universal joint.

4 Basic Configuration

Set user password when logging in for the first time (the username is admin by default).



The figures in this manual are for reference only, and might differ from the actual interface. For more details, see *Thermal Camera_Web Operation Manual*.

4.1 Initializing Camera

You can initialize the Camera by the ConfigTool, or by connecting the computer to the Camera and logging in to the web page with the default IP address.

- To initialize multiple devices at the same time in batches, use the ConfigTool.
- To initialize one device at a time, log in to the web page.

This section uses single camera initialization on the web for an example.



- Initialize the Camera for first-time use after performing a factory reset.
- To secure the data on the Camera, keep the admin password after initialization and regularly change it.
- Make sure the Camera IP address (192.168.1.108 by default) and the IP address of the computer are on the same network segment.

Step 1 Open IE browser, enter the Camera default IP address in the address bar, and then press Enter.

Step 2 Set the login password of admin and the email address.



- The email address is for password reset.
- We recommend entering the email address in case you forget the password and reset the password.

Step 3 Click **Save**.

4.2 Modifying IP Address

Set the IP address for the network segment to allow the Camera to access the network.

Step 1 Log in to the Camera web page.

Step 2 Select **Setup > Network > TCP/IP**.

Figure 4-1 TCP/IP

TCP/IP

Host Name: TPCDome

Ethernet Card: Wire(Default) ▼

Mode: ☒ Static ☐ DHCP

MAC Address: [][][][][][]

IP Version: [][] ▼

IP Address: [][][][]

Subnet Mask: [][][][]

Default Gateway: [][][][]

Preferred DNS: [][][][]

Alternate DNS: [][][][]

☒ Enable ARP/Ping to set IP address service

Default Refresh Save

Step 3 Configure IP related parameters.

Step 4 Click **Save**.

4.3 Live Video



Make sure that the Camera can access the network and check the video after configuring the network.

Step 1 Log in to the web interface of the Camera.



The default username is admin, and the password is the one that was set during initialization.

Step 2 Click **Login** and then the system will display the web main interface.



You will be prompted to install a plug-in for first-time system login. Please download and install the plug-in. The web interface will refresh automatically after the plug-in is installed, and then the live video will be displayed.

5 Alarm Configuration



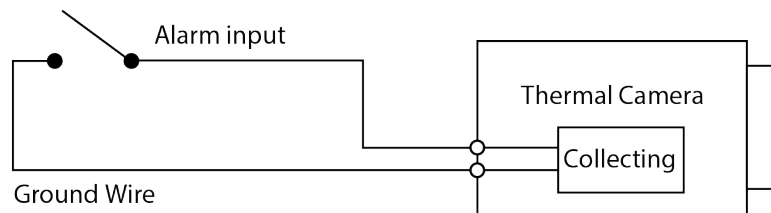
Cut off power before connecting cables.

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

Alarm input: input signal is idle or grounded and the device can collect different states of alarm input port.

- When input signal is 3.3 V or idle, the Camera collects logic "1".
- When input signal is grounded, the Camera collects logic "0".

Figure 5-1 Alarm input



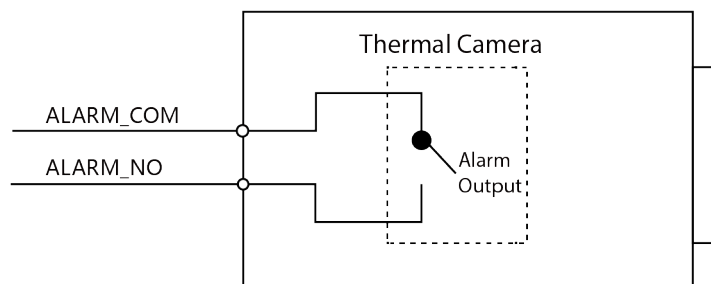
Step 2 Connect alarm output device to alarm output port of I/O cable. Alarm output is a relay switch output. The alarm output port can only be connected to NO alarm device.

Alarm output: Port ALARM_NO and ALARM_COM form a switch to provide alarm output. Normally the switch is on. The switch will be turned off when there is an alarm output.



ALARM_NO can only be used together with ALARM_COM when connecting to alarm devices.

Figure 5-2 Alarm output



Step 3 Open web interface, select **Setting > Event > Alarm**.

Step 4 Configure the settings for alarm input and output in the alarm setup interface, and then click **Save**.

- Alarm input is corresponding to the alarm input port of device I/O cable. It is to set corresponding NO and NC according to the high and low level signal generated by alarm input devices when an alarm is triggered.
- The alarm output corresponds to the alarm output port of device I/O cable.

Figure 5-3 Alarm settings

Alarm

☐ Enable

Relay-inAlarm1

PeriodSetting

Anti-Dither0Sec. (0~100)Sensor TypeNO

☒ Record

Record Delay10Sec. (10~300)

☒ Relay-out

Alarm Delay10Sec. (10~300)

☐ Send Email

☐ PTZ

☐ Snapshot

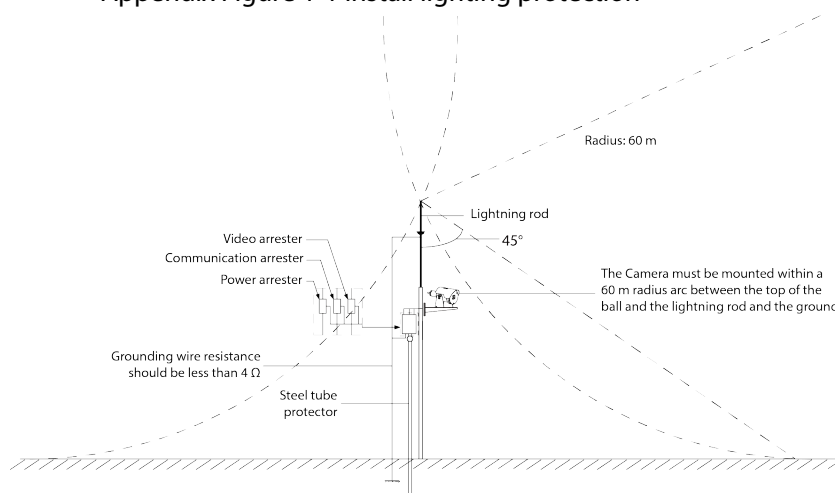
DefaultRefreshSave

Appendix 1 Lightning and Surge Protection

The Camera adopts TVS lightning protection technology. It can effectively prevent damage from various pulse signals below 6000 V, such as a sudden lighting and surge. However, you still need to take necessary precaution measures in accordance with your local electrical safety code when installing the Camera in outdoor environment.

- The distance between the signal transmission cable and high-voltage device (or high-voltage cable) shall be at least 50 m.
- Outdoor cable layout shall go under the penthouse if possible.
- For vast land, use sealing steel tube under the land to implement cable layout and make sure that both ends of the tube are equipotentially grounded. Open floor cable layout is forbidden.
- For vast land, install a 10 KA lightning rod near the Camera's power input port and Ethernet port. For Camera with AC to DC power adapter, install a 10 KA lightning rod near the output port of the adapter.
- For Camera installed on iron tower, if there is a high-performance grounding bar on the tower, connect the Camera grounding wire to the bar. If there is no grounding bar, use multiple copper cable whose cross-sectional area are not less than 16 mm² to connect the Camera grounding wire into the ground.
- Make sure that the Camera is over 3 m away from the top point of tower lightning rod and within protection area against direct lighting.
- In area of strong thunderstorm or near high sensitive voltage (such as near high-voltage transformer substation), install additional high-power thunder protection device or lightning rod.
- 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 your local or industry standards.
- The system shall adopt equal-potential wiring. The grounding devices shall meet anti-jamming requirements and at the same time conforms to your local electrical safety code.
- The grounding devices shall not be connected to N (neutral) line of high voltage power grid or mixed with other wires. When you connect the system to the ground alone, the grounding resistance shall not be more than 4Ω and the cross-sectional area of grounding cable shall be no less than 25 mm².

Appendix Figure 1-1 Install lightning protection



Appendix 2 Cybersecurity Recommendations

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 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.