网络摄像机（H 型半球）

快速操作手册

V1.0.0

前言

符号约定

在本文档中可能出现下列标识，代表的含义如下。

标识	说明
 注意	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 说明	表示是正文的附加信息，是对正文的强调和补充。

修订记录

版本号	修订内容	发布日期
V1.0.0	首次发布。	2021.06

使用安全须知

下面是关于产品的正确使用方法、为预防危险、防止财产受到损失等内容，使用设备前请仔细阅读本说明书并在使用时严格遵守，阅读后请妥善保存说明书。

电源要求

- 请严格遵守当地各项电气安全标准，并在设备运行之前检查供电电源是否正确。
- 请严格遵循以下供电要求为设备供电。
  - ◇ 选用电源适配器时，请使用满足 SELV（安全超低电压）要求的电源，并按照 GB8898（IEC60065）或 GB4943.1（IEC60950-1 或 IEC62368-1 符合 Limited Power Source（受限制电源））标准额定电压供电，具体供电要求以设备标签为准。
  - ◇ 若设备出厂时随带电源适配器，推荐使用随带电源适配器。
- 请在安装配线时装入易于使用的断电设备，以便必要时进行紧急断电。
- 请保护电源软线免受踩踏或紧压，特别是插头、电源插座和从装置引出的接点处。
- 如非特殊说明，请勿同时对设备提供两种及以上供电方式，否则可能导致设备损坏。

使用环境要求

- 请勿将设备对准强光（如灯光照明、阳光等）聚焦，否则容易引起过亮或拉光现象（这并非设备故障），也将影响感光器件 CMOS（Complementary Metal Oxide Semiconductor，互补金属氧化物半导体）的寿命。
- 请在使用激光束设备时，避免使设备表面受到激光束的辐射。
- 请在允许的湿度和温度范围内运输、使用和存储设备。不建议将设备置于长期潮湿、多尘、极热、极冷、强电磁辐射或照明条件不稳定等场所。
- 请在运送设备时以出厂时的包装或同等品质的材质进行包装，且勿在运输、存储及安装过程中重压、剧烈振动、浸泡设备。
- 请勿将任何液体流入设备，以免内部元件受损。
- 请勿让室内设备受到雨淋或受潮，以免发生火灾或电击危险。
- 请勿阻挡设备附近的通风口，以免热量积蓄。
- 设备需安装于仅专业人员（专业人员需明确了解使用本设备的安全注意事项）可触及的场所，非专业人员在设备正常工作时进入设备安装区域可能会造成意外伤害。

操作与保养要求

- 请勿碰触设备散热部件，以免烫伤。
- 设备相关的拆卸操作请严格参照本文档进行。违规拆卸，可能会导致设备漏水或者图像不良。

涉及拆卸操作的设备在合盖前请务必检查密封圈是否平整并处于安装槽内。如开箱发现镜头有凝雾或拆卸设备后发现干燥剂变绿，请及时联系售后更换干燥剂。（部分型号不包含干燥剂，具体情况以实际为准。）

- 建议配合防雷器使用本设备，提高防雷效果。
- 建议设备上的接地孔⏚接地，提高设备的可靠性。（部分型号无接地孔，具体情况以实际为准。）
- 请勿直接碰触到感光器件 CMOS，可用气枪除去镜头表面的灰尘或污垢。若有必要清洁，请将干净的软布用酒精稍微润湿，轻轻拭去尘污。
- 清洁机身可用干净的软布擦拭，若遇污垢难以清除，请用干净的软布蘸取少量中性清洁剂轻轻拭去，之后再擦干。请勿使用如酒精、苯或稀释剂等挥发性溶剂，或者强烈的、带有研磨性的清洁剂，否则会损坏表面涂层，或降低设备工作性能。
- 半球球罩是光学器件，安装及使用时请勿直接碰触及擦拭球罩表面，如沾染灰尘、油脂或指纹，可使用脱脂棉花沾少许乙醚或干净的软布沾水后轻轻擦拭。如沾染灰尘，也可使用气枪轻轻拭去。
- 不锈钢材质的摄像机在强腐蚀环境中（如海边、化工厂等）使用一段时间后，表面有锈迹属正常现象，可使用带有磨砂功能的软布蘸取少量酸性溶液（建议食醋）轻轻拭去，之后再擦干。
- 请加强网络、设备数据和个人信息等的保护，采取保障设备网络安全的必要措施，包括但不限于使用强密码、定期修改密码、将固件更新至最新版本、隔离电脑网络等。部分老版本的 IP 摄像机固件，系统的主密码更改后，ONVIF（Open Network Video Interface Forum，开放型网络视频接口论坛）密码不会自动跟着更改，您需要更新摄像机的固件或者手动更新 ONVIF 密码。
- 请使用生产厂商规定的配件或附件，并由专业服务人员进行安装和维修。

目录

第 1 章 设备结构

1.1 设备外接线缆

对接线缆时，建议使用绝缘胶带和防水胶带，以免造成线路短路和漏水。具体处理方法请参见对应的常见问题说明书。

图1-1 外接线缆示意图

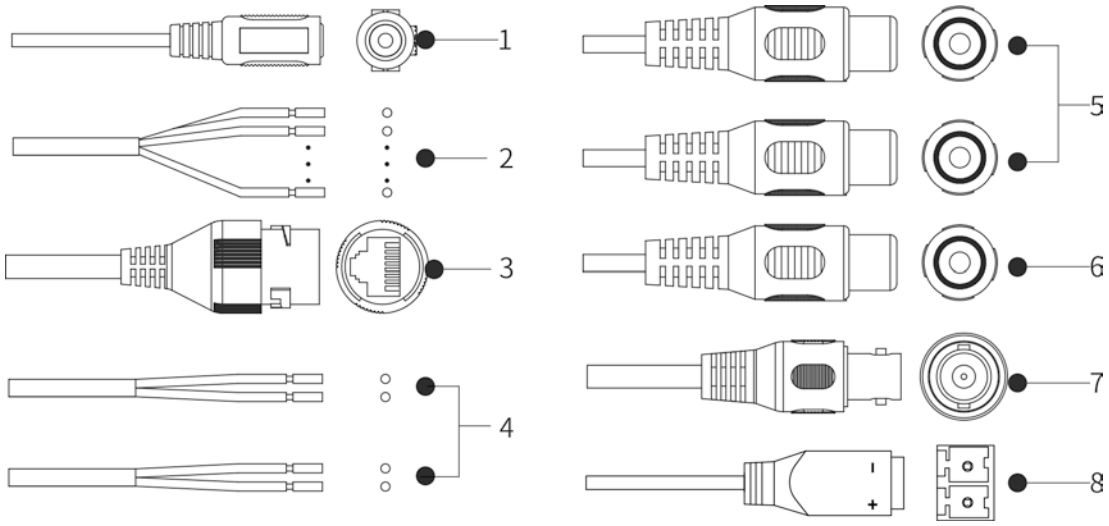


表1-1 外接线缆功能介绍

序号	接口	接口名称	功能描述
1	POWER	电源输入接口	输入 DC 12 V 或 AC 24 V 电源。 **注意** 使用时请务必按照标签对设备供电，否则将导致设备损坏。
2	I/O	I/O 端口	包括报警信号输入和输出，不同设备的 I/O 端口数不同，请根据设备标签参见表 1-2 使用。
3	LAN	网络接口	连接标准以太网线，提供 PoE 供电功能。
4	RS-485	RS-485 接口	控制外部云台等。
5	AUDIO IN	音频输入接口	RCA 接口，输入音频信号，接收拾音器等设备的模拟音频信号。
6	AUDIO OUT	音频输出接口	RCA 接口，输出音频信号，提供给音箱等设备。
7	VIDEO OUT	视频输出接口	BNC 接口，输出模拟视频信号，可接 TV 监视器观看图像。
8	DC 12V Out	电源返送输出接口	输出 DC 12 V 电源，额定功率 2 W。用于给拾音器等供电。

表1-2 I/O 端口功能介绍

接口	线缆接口名称	功能描述
I/O 端口	ALARM_OUT	报警输出接口，输出报警信号给报警设备。 **说明** 连接报警输出设备时，ALARM_OUT 只能和数字相同的 ALARM_OUT_GND 配合使用。
	ALARM_OUT_GND	
	ALARM_IN	报警输入接口，接收外部报警源的开关量信号。 **说明** 不同的报警输入设备连接到同一个接地端，即 ALARM_IN_GND。
	ALARM_IN_GND	

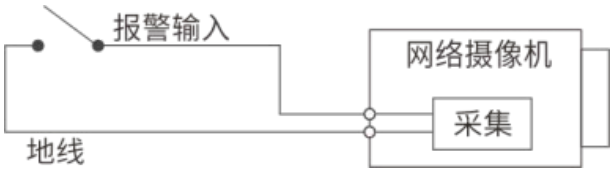
1.2 报警设置

步骤1　连接报警输入设备，如图 1-2 所示。

输入信号悬空或者接地，设备可以采集到报警输入口的不同状态。

- 输入信号接+3 V–+5 V 或者悬空，设备采集到逻辑“1”。
- 输入信号接地，设备采集到逻辑“0”。

图1-2 报警输入示意图

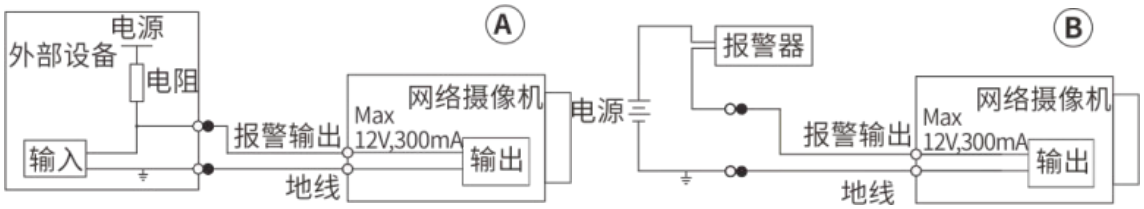


步骤2　连接报警输出设备，如图 1-3 所示。

报警输出为漏极开路输出。

- 方式 A：电平应用。报警输出高低电平，报警输出口为 OD 门，需要外部增加上拉电阻（典型值 10 KΩ）才能正常工作。外部上拉电平最大为 12 V，端口电流最大为 300 mA，增加外部上拉电阻，输出信号默认为高电平（外部上拉电压），当有报警输出的时候，输出信号变为低电平。
- 方式 B：开关应用。报警输出用于驱动外部电路，最高电压为 12 V，最大电流为 300 mA（峰值），超出此值时建议外加继电器。

图1-3 报警输出示意图



步骤3　登录 WEB 界面，在报警设置里对报警输入、输出做相应的设置。

- WEB 端的报警输入对应 I/O 端口线缆上的报警输入接口。如果报警输入信号在报警发生时产生的信号为逻辑“0”，则设置为常开型输入（默认状态）；如果报警输入信号在报警发生时产生的信号为逻辑“1”，则设置为常闭型输入。
- WEB 端设置报警输出，报警输出对应 I/O 端口线缆上的报警输出接口。

第 2 章 网络配置

您可以通过 ConfigTool 工具和 WEB 界面初始化设备以及修改 IP 地址，本文档以 ConfigTool 举例说明。WEB 界面相关操作请参见配套的使用说明书。

说明

- 设备初次使用或恢复出厂设置后，需进行初始化。
- 初始化、修改 IP 地址、登录设备等功能，需确保设备（默认 IP 为 192.168.0.10）与 PC 处于同一网络。
- 为使设备能顺利接入网络，请根据实际网络环境，合理规划可用的 IP 网段。
- 以下图示仅做参考，不同型号设备的界面显示不同，请以实际为准。

2.1 初始化设备

步骤1　通过 ConfigTool 搜索到需要初始化的设备。

1. 双击“ConfigTool”，打开快速配置工具。
2. 选择“  > 搜索设置”，系统弹出“设置”对话框。
3. 设置设备所在网段，单击“确定”，开始搜索设备。

步骤2　在设备列表中选择未初始化的设备，单击“初始化”。

系统显示未初始化设备列表。

步骤3　选择需要初始化的设备，单击“初始化”。

系统显示“设备初始化”界面，如图 2-1 所示。

图2-1 设备初始化

步骤4　设置密码和预留手机，单击“初始化”。

系统显示自动检测等功能设置界面。

预留手机用于重置密码，请根据实际需要设置“预留手机”。

步骤5　根据实际需求选择自动检测等功能，单击“确定”。

系统开始初始化设备。表示初始化成功；表示初始化失败。单击图标可查看详细信息。

步骤6　单击“完成”，完成设备初始化。

2.2 修改 IP 地址

步骤1　参考“初始化设备”的步骤 1，搜索到设备。

说明

“搜索设置”中的用户名及密码需与设备初始化的用户名及密码一致，否则修改 IP 地址会提示密码错误。

步骤2　选择需要修改 IP 的设备，单击“批量修改 IP”。

系统弹出“修改 IP”对话框，如图 2-2 所示。

图2-2 修改 IP 对话框

步骤3　修改设备 IP 地址，支持静态模式和 DHCP 模式。

- 静态模式：设置“模式”为“静态”，并输入规划的起始 IP、子网掩码和网关。
- DHCP 模式：当网络存在 DHCP 服务器时，设置“模式”为“DHCP”，设备自动从 DHCP 服务器获取 IP 地址。

说明

选择“同一 IP”，将选中的多个设备设置为同一个 IP 地址，建议统一设置出厂默认 IP 时使用。

步骤4　单击“确定”，完成设备 IP 地址修改。

2.3 登录 WEB 界面

步骤1　打开 IE 浏览器，在地址栏里输入设置的设备 IP 地址，按【Enter】键。

说明

若界面显示设置向导，请根据界面提示操作。

步骤2　输入用户名和密码，单击“登录”。

说明

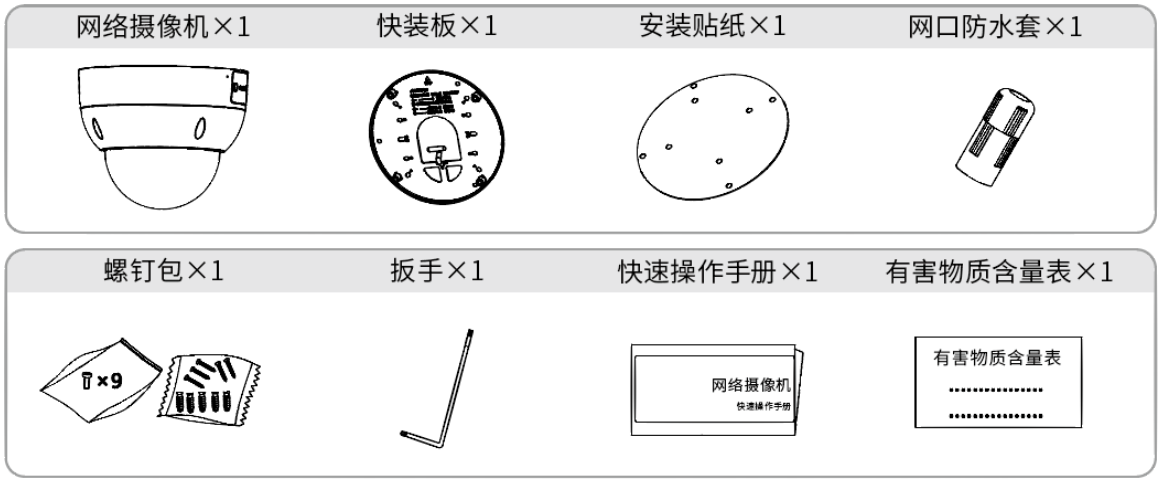
- 首次登录需单击“请点击此处下载插件”，根据系统提示安装控件。
- 如果您遗忘了密码，可以在登录界面单击“忘记密码”进行重置。

第 3 章 设备安装

3.1 开箱检查

开箱未提及的工具或配件，请用户自行按需购买。

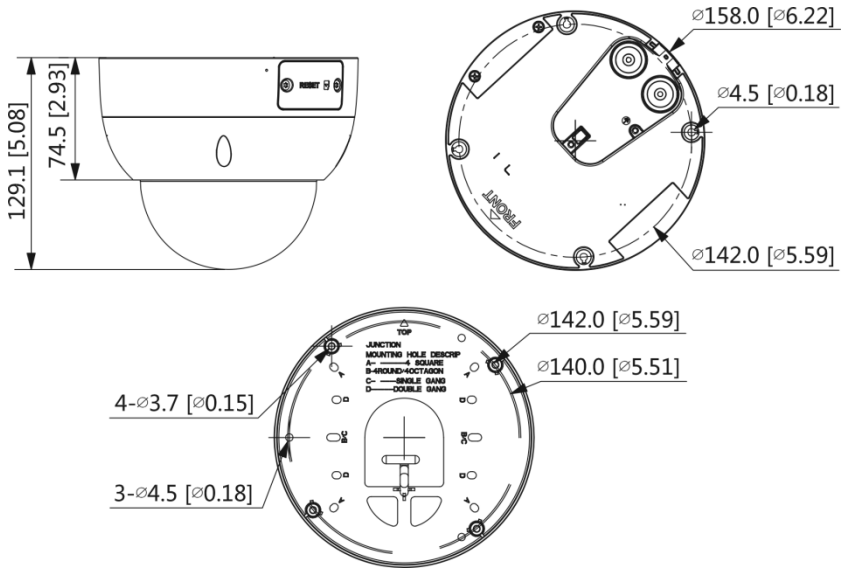
图3-1 开箱检查



3.2 结构尺寸

结构尺寸单位为 mm[inch]。

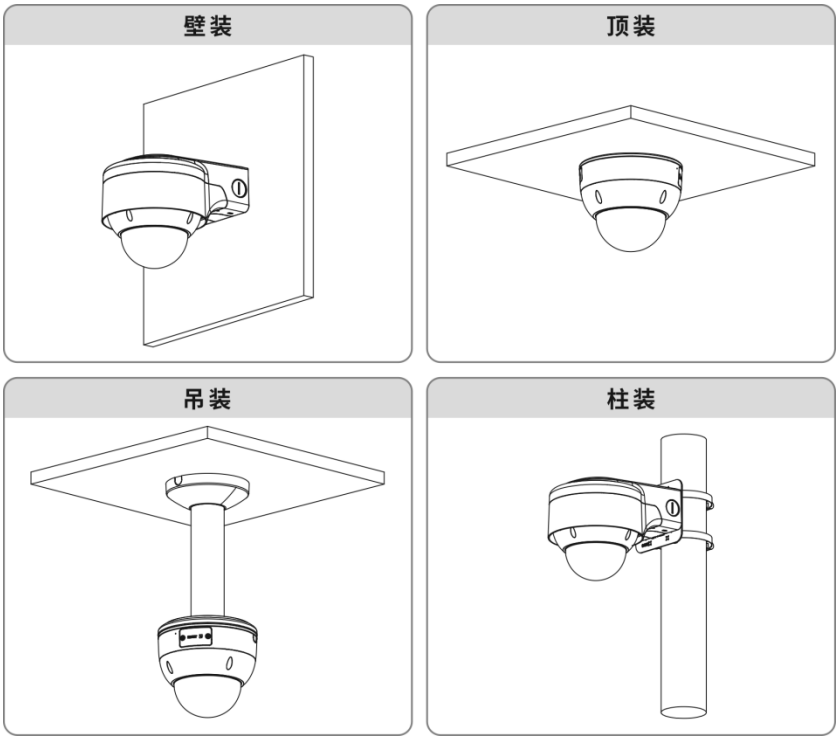
图3-2 结构尺寸示意图



3.3 安装设备

3.3.1 安装场景

图3-3 安装场景示意图



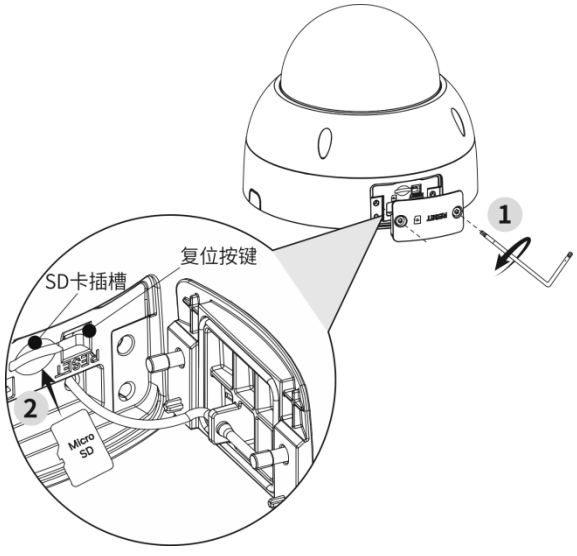
3.3.2 （可选）安装 SD 卡

当设备有 SD 卡插槽且需要使用 SD 卡存储录像时，请先安装 SD 卡。安装或取下 SD 卡时，请先切断设备电源再操作。

说明

设备正常工作情况下长按复位按键 10 秒钟，恢复系统配置信息到出厂默认设置。

图3-4 安装 SD 卡示意图



3.3.3 固定设备

设备支持带快装板安装和不带快装板安装，两种安装方式均支持墙体出线和出线槽出线，下面带快装板以墙体出线为例，不带快装板以出线槽出线为例介绍。

注意

设备安装面需要至少能够承受 3 倍于支架和设备的总重量。

图3-5 带快装板（墙体出线）安装示意图

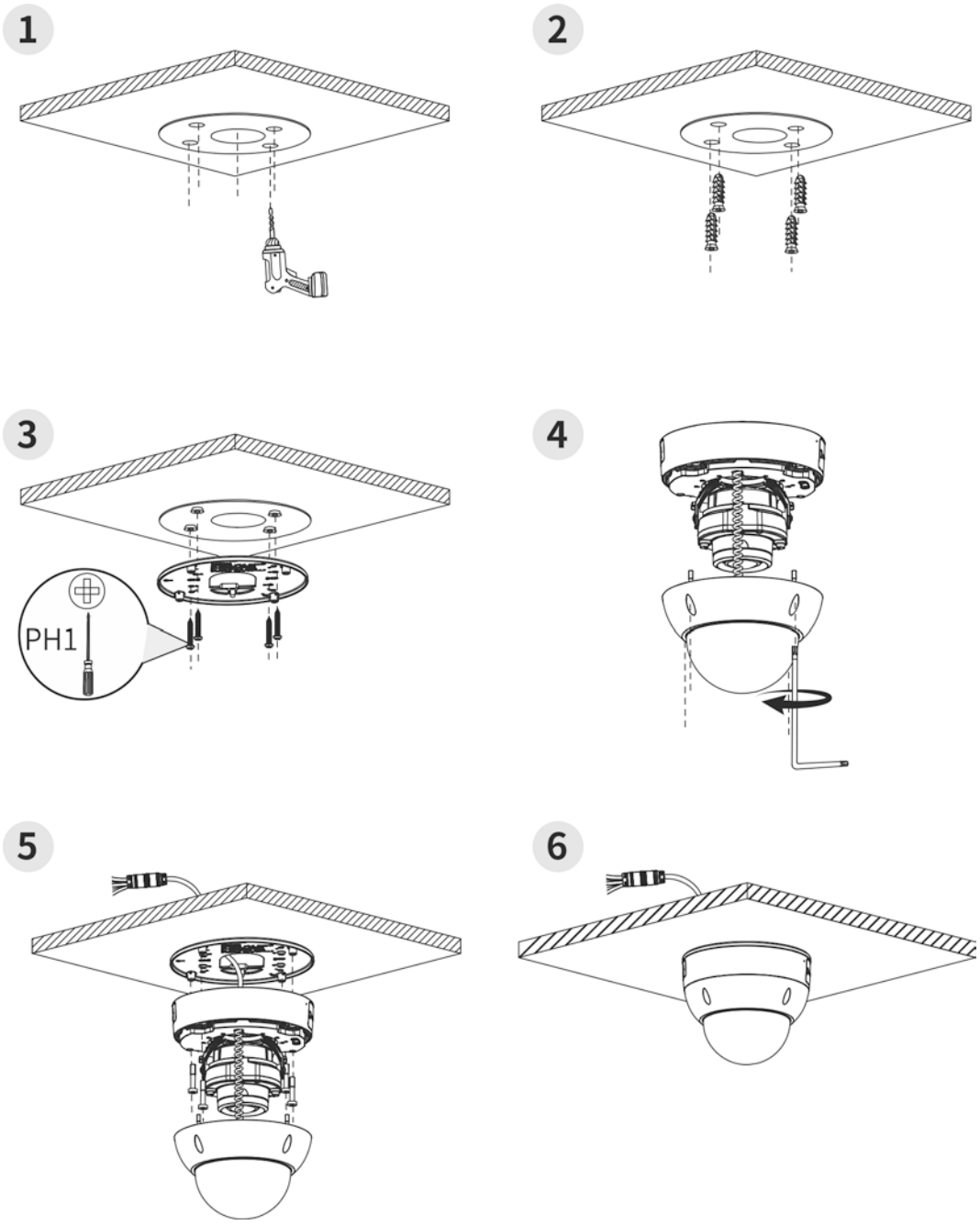
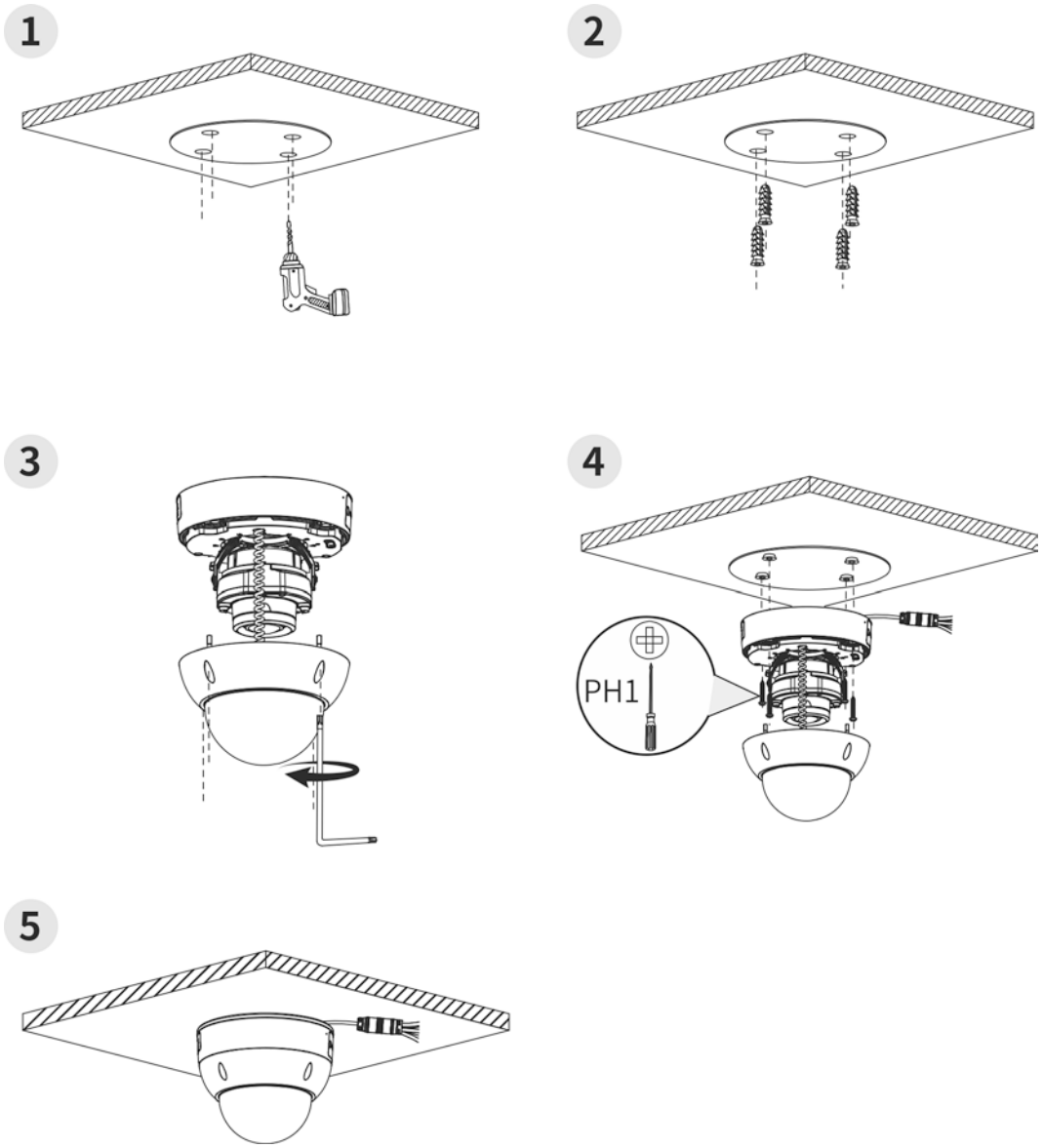


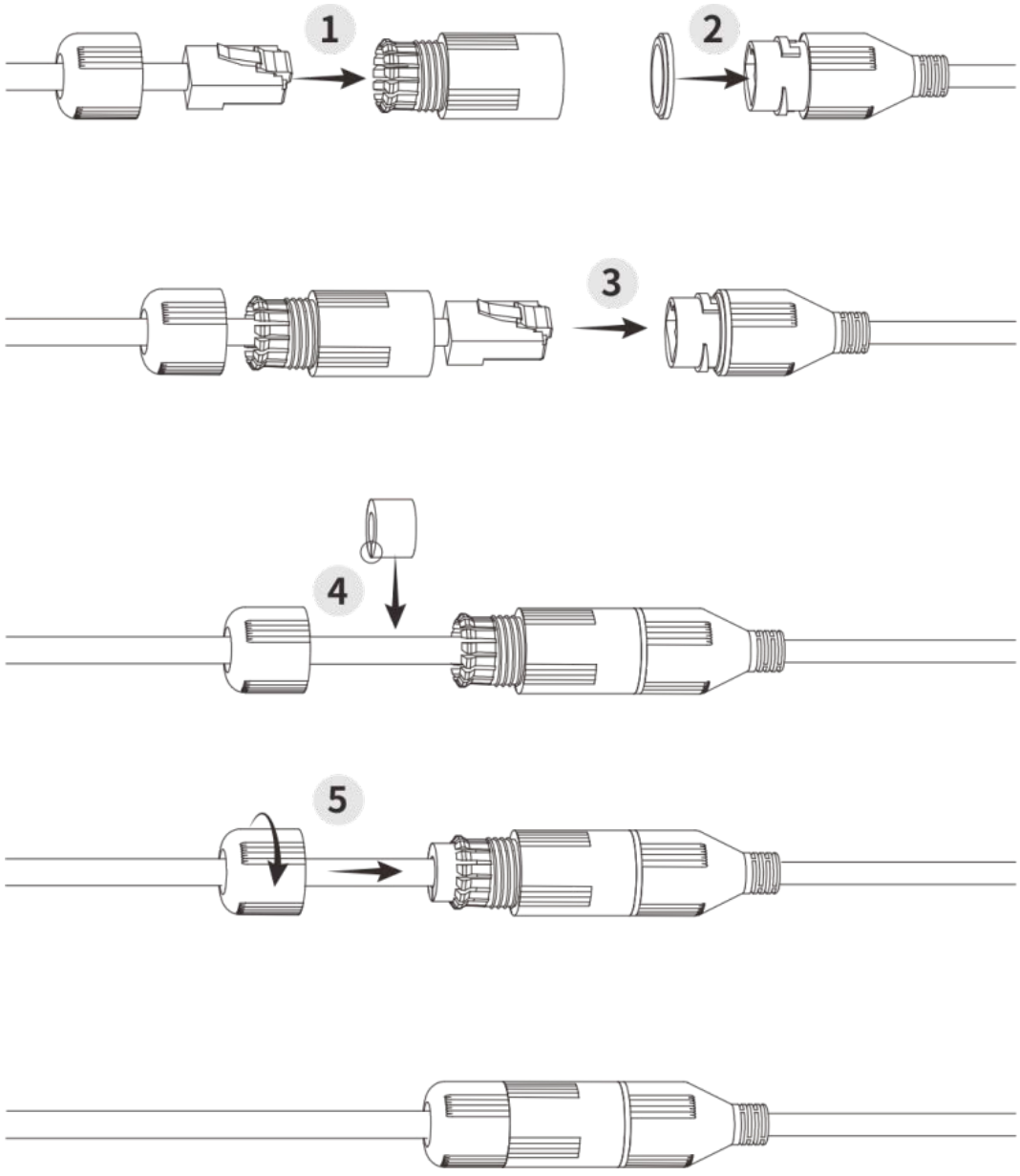
图3-6 不带快装板（出线槽出线）安装示意图



3.3.4 （可选）安装网口防水套

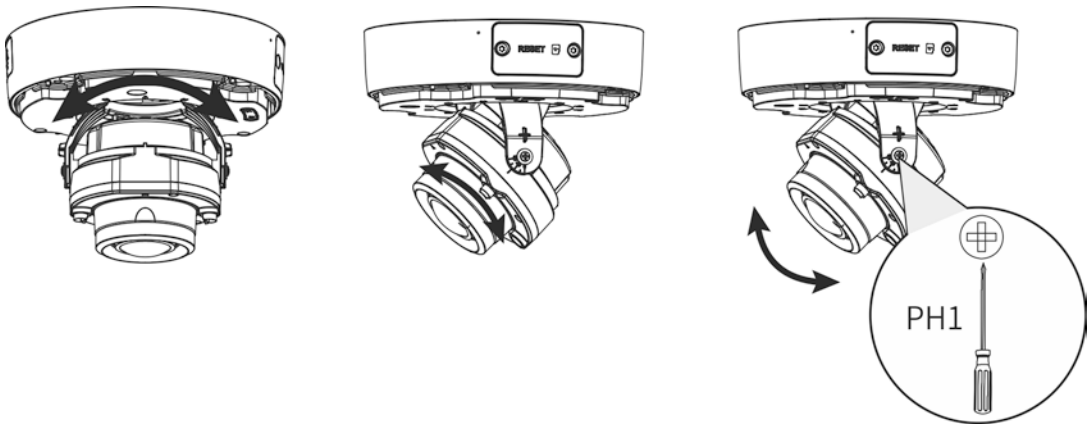
当设备配有网口防水套且在室外使用时，需要执行此操作。

图3-7 安装网口防水套示意图



3.3.5 调节角度

图3-8 调节角度示意图



附录 1 法律声明

商标声明

- VGA 是 IBM 公司的商标。
- Windows 标识和 Windows 是微软公司的商标或注册商标。
- 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

责任声明

- 在适用法律允许的范围内，在任何情况下，本公司都不对因本文档中相关内容及描述的产品而产生任何特殊的、附随的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉、文档丢失或预期节约的损失进行赔偿。
- 本文档中描述的产品均“按照现状”提供，除非适用法律要求，本公司对文档中的所有内容不提供任何明示或暗示的保证，包括但不限于适销性、质量满意度、适合特定目的、不侵犯第三方权利等保证。

隐私保护提醒

您安装了我们的产品，您可能会采集人脸、指纹、车牌等个人信息。在使用产品过程中，您需要遵守所在地区或国家的隐私保护法律法规要求，保障他人的合法权益。如，提供清晰、可见的标牌，告知相关权利人视频监控区域的存在，并提供相应的联系方式。

关于本文档

- 本文档供多个型号产品使用，产品外观和功能请以实物为准。
- 如果不按照本文档中的指导进行操作而造成的任何损失由使用方自己承担。
- 本文档会实时根据相关地区的法律法规更新内容，具体请参见产品的纸质、电子光盘、二维码或官网，如果纸质与电子档内容不一致，请以电子档为准。
- 本公司保留随时修改本文档中任何信息的权利，修改的内容将会在本文档的新版本中加入，恕不另行通知。
- 本文档可能包含技术上不准确的地方、或与产品功能及操作不相符的地方、或印刷错误，以公司最终解释为准。
- 如果获取到的 PDF 文档无法打开，请使用最新版本或最主流的阅读工具。

附录 2 网络安全建议

保障设备基本网络安全的必须措施：

1. **使用复杂密码**

   请参考如下建议进行密码设置：

   - 长度不小于 8 个字符。
   - 至少包含两种字符类型，字符类型包括大小写字母、数字和符号。
   - 不包含账户名称或账户名称的倒序。
   - 不要使用连续字符，如 123、abc 等。
   - 不要使用重叠字符，如 111、aaa 等。

2. **及时更新固件和客户端软件**

   - 按科技行业的标准作业规范，设备的固件需要及时更新至最新版本，以保证设备具有最新的功能和安全性。设备接入公网情况下，建议开启在线升级自动检测功能，便于及时获知厂商发布的固件更新信息。
   - 建议您下载和使用最新版本客户端软件。

增强设备网络安全的建议措施：

1. **物理防护**

   建议您对设备（尤其是存储类设备）进行物理防护，比如将设备放置在专用机房、机柜，并做好门禁权限和钥匙管理，防止未经授权的人员进行破坏硬件、外接设备（例如 U 盘、串口）等物理接触行为。

2. **定期修改密码**

   建议您定期修改密码，以降低被猜测或破解的风险。

3. **及时设置、更新密码重置信息**

   设备支持密码重置功能，为了降低该功能被攻击者利用的风险，请您及时设置密码重置相关信息，包含预留手机号/邮箱、密保问题，如有信息变更，请及时修改。设置密保问题时，建议不要使用容易猜测的答案。

4. **开启账户锁定**

   出厂默认开启账户锁定功能，建议您保持开启状态，以保护账户安全。在攻击者多次密码尝试失败后，其对应账户及源 IP 将会被锁定。

5. **更改 HTTP 及其他服务默认端口**

   建议您将 HTTP 及其他服务默认端口更改为 1024～65535 间的任意端口，以减小被攻击者猜测服务端口的风险。

6. **使能 HTTPS**

   建议您开启 HTTPS，通过安全的通道访问 Web 服务。

7. **MAC 地址绑定**

   建议您在设备端将其网关设备的 IP 与 MAC 地址进行绑定，以降低 ARP 欺骗风险。

8. **合理分配账户及权限**

根据业务和管理需要，合理新增用户，并合理为其分配最小权限集合。

9. **关闭非必需服务，使用安全的模式**

- 如果没有需要，建议您关闭 SNMP、SMTP、UPnP 等功能，以降低设备面临的风险。
- 如果有需要，强烈建议您使用安全的模式，包括但不限于：
  - ◇ SNMP：选择 SNMP v3，并设置复杂的加密密码和鉴权密码。
  - ◇ SMTP：选择 TLS 方式接入邮箱服务器。
  - ◇ FTP：选择 SFTP，并设置复杂密码。
  - ◇ AP 热点：选择 WPA2-PSK 加密模式，并设置复杂密码。

10. **音视频加密传输**

如果您的音视频数据包含重要或敏感内容，建议启用加密传输功能，以降低音视频数据传输过程中被窃取的风险。

11. **安全审计**

- 查看在线用户：建议您不定期查看在线用户，识别是否有非法用户登录。
- 查看设备日志：通过查看日志，可以获知尝试登录设备的 IP 信息，以及已登录用户的关键操作信息。

12. **网络日志**

由于设备存储容量限制，日志存储能力有限，如果您需要长期保存日志，建议您启用网络日志功能，确保关键日志同步至网络日志服务器，便于问题回溯。

13. **安全网络环境的搭建**

为了更好地保障设备的安全性，降低网络安全风险，建议您：

- 关闭路由器端口映射功能，避免外部网络直接访问路由器内网设备的服务。
- 根据实际网络需要，对网络进行划区隔离：若两个子网间没有通信需求，建议使用 VLAN、网闸等方式对其进行网络分割，达到网络隔离效果。
- 建立 802.1x 接入认证体系，以降低非法终端接入专网的风险。
- 开启设备 IP/MAC 地址过滤功能，限制允许访问设备的主机范围。