总线防盗报警控制器

使用说明书

V1.1.1

浙江大华技术股份有限公司

法律声明

版权声明

商标声明

- alhua、alhua、alhua、HDCVI是浙江大华技术股份有限公司的商标或注册商标。
- HDMI 标识、HDMI 和 High-Definition Multimedia Interface 是 HDMI Licensing LLC 的商标或注册商标。本产品已经获得 HDMI Licensing LLC 授权使用 HDMI 技术。
- 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。

出口管制合规声明

大华遵守适用的出口管制法律法规，并且贯彻执行与硬件、软件、技术的出口、再出口及转让相关的要求。就本手册所描述的产品，请您全面理解并严格遵守国内外适用的出口管制法律法规。

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、邮箱、电话、GPS 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。

网络安全声明和建议

安全声明

- 若您将产品接入互联网需自担风险，包括但不限于可能遭受网络攻击、黑客攻击、病毒感染等，请您加强网络、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，包括但不限于修改出厂默认密码并使用强密码、定期修改密码、将固件更新至最新版本等。本公司不对因此造成的产品工作异常、信息泄露等问题承担任何责任，但本公司会提供产品相关安全维护。
- 在适用法律未明令禁止的程度下，对于因使用或无法使用本产品或服务而引起的任何利润、收入、销售损失、数据丢失或采购替代商品或服务的成本、财产损害、人身伤害、业务中断、商业信息损失，或者任何特殊的、直接的、间接的、附带的、经济性、覆盖性、惩罚性、特殊或从属损害，无论是基于何种责任理论（合同、侵权、过失或其他），本公司及其员工、许可方或附属公司都不承担赔偿责任，即使其已被告知存在此种损害的可能性也是如此。某些司法管辖区不允许对人身伤害、附带或从属损害等进行责任限制，则此限制可能不适用于您。
- 本公司对您的所有损害承担的总责任限额（除了因本公司过失导致人身伤亡的情况，需遵循适用法律规定）不超过您购买本公司产品所支付的价款。

安全建议

保障设备基本网络安全的必须措施：

1.修改出厂默认密码并使用强密码

没有更改出厂默认密码或使用弱密码的设备是最容易被“黑”的。建议用户必须修改默认密码，并尽可能使用强密码（最少有 8 个字符，包括大写、小写、数字和符号）。

2.更新固件

按科技行业的标准作业规范，NVR、DVR 和 IP 摄像机的固件应该要更新到最新版本，以保证设备享有最新的功能和安全性。请访问大华官网获取最新版本的固件。

以下建议可以增强设备的网络安全程度：

1.定期修改密码

定期修改登录凭证可以确保获得授权的用户才能登录设备。

2.更改默认 HTTP 和 TCP 端口

- 更改设备的默认 HTTP 和 TCP 端口这两个端口是用来进行远程通讯和视频浏览的。
- 这两个端口可以设置成 1025～65535 间的任意数字。更改默认端口后，减小了被入侵者猜到你使用哪些端口的风险。

3.使能 HTTPS/SSL 加密

设置一个 SSL 证书来使能 HTTPS 加密传输。使前端设备与录像设备间的信息传输被全部加密。

4.使能 IP 过滤

使能 IP 过滤后，只有指定 IP 地址的设备才能访问系统。

5.更改 ONVIF 密码

部分老版本的 IP 摄像机固件，系统的主密码更改后，ONVIF 密码不会自动跟着更改。你需要更新摄像机的固件或者手动更新 ONVIF 密码。

6.只转发必须使用的端口

- 只转发必须使用的网络端口。避免转发一段很长的端口区。不要把设备的 IP 地址设置成 DMZ。
- 如果摄像机是连接到本地的 NVR，你不需要为每一台摄像机转发端口，只有 NVR 的端口需要被转发。

7.关闭 SmartPSS 的自动登录功能

如果你使用 SmartPSS 来监控你的系统而你的电脑是有多个用户，请必须把自动登录功能关闭。增加一道防线来防止未经授权的人访问系统。

8.在 SmartPSS 上使用不同于其他设备的用户名和密码

万一你的社交媒体账户，银行，电邮等账户信息被泄漏，获得这些账户信息的人也无法入侵你的视频监控系统。

9.限制普通账户的权限

如果你的系统是为多个用户服务的，请确保每一个用户只获得它的作业中必须的权限。

10. UPnP

- 启用 UPnP 协议以后，路由器将会自动将内网端口进行映射。从功能上来说，这是方便用户使用，但是却会导致系统自动的转发相应端口的数据，从而导致本应该受限的数据被他人窃取。
- 如果已在路由器上手工打开了 HTTP 和 TCP 端口映射，我们强烈建议您关闭此功能。在实际的使用场景中，我们强烈建议您不开启此功能。

11. SNMP

如果您不使用 SNMP 功能，我们强烈建议您关闭此功能。SNMP 功能限于以测试为目的的临时使用。

12. 组播

组播技术适用于将视频数据在多个视频存储设备中进行传递的技术手段。当前为止尚未发现有过任何涉及组播技术的已知漏洞，但是如果您没有使用这个特性，我们建议您将网络中的组播功能关闭。

13. 检查日志

如果您想知道您的设备是否安全，可以通过检查日志来发现一些异常的访问操作。设备日志将会告知您哪个 IP 地址曾经尝试过登录或者用户做过何种操作。

14. 对您的设备进行物理保护

为了您的设备安全，我们强烈建议您对设备进行物理保护，防止未经授权的物理操作。我们建议您将设备放在有锁的房间内，并且放在有锁的机柜，配合有锁的盒子。

15. 强烈建议您使用 PoE 的方式连接 IP 摄像机和 NVR

使用 PoE 方式连接到 NVR 的 IP 摄像机，将会与其它网络隔离，使其不能被直接访问到。

16. 对 NVR 和 IP 摄像机进行网络隔离

我们建议将您的 NVR 和 IP 摄像机与您的电脑网络进行隔离。这将会保护您的电脑网络中的未经授权的用户没有机会访问到这些设备。

更多内容

请访问大华官网安全应急响应中心，获取安全公告和最新的安全建议。

适用型号

DH-ARC9016C、DH-ARC9016C-G

符号约定

在本文档中可能出现下列标识，代表的含义如下。

符号	说明
 危险	表示有高度潜在危险，如果不能避免，会导致人员伤亡或严重伤害。
 警告	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 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。
 电击防护	表示高压危险。
 激光辐射	表示强激光辐射。
 防静电	表示静电敏感的设备。
 窍门	表示能帮助您解决某个问题或节省您的时间。
 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

编号	版本号	修订内容	发布日期
1	V1.0.0	首次发布	2017.5
2	V1.1.0	基线功能修改	2018.5
3	V1.1.1	删除 GPRS 相关描述	2019.5

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。

使用要求

- 请在设备布控后及时修改用户的默认密码，以免被人盗用。
- 请不要将设备放置和安装在阳光直射的地方或发热设备附近。
- 请不要将设备安装在潮湿、有灰尘或煤烟的场所。
- 请保持设备的水平安装，或安装在稳定的场所，注意防止本产品坠落。
- 请勿将液体滴到或溅到设备上，并确保设备上不能放置装满液体的物品，防止液体流入设备。
- 请安装在通风良好的场所，切勿堵塞设备的通风口。
- 仅可在额定输入输出范围内使用设备。
- 请不要随意拆卸设备。
- 请在允许的湿度和温度范围内运输、使用和存储设备。

电源要求

- 请务必按照要求使用电池，否则可能导致电池起火、爆炸或燃烧的危险！
- 更换电池时只能使用同样类型的电池！
- 产品必须使用本地区推荐使用的电线组件（电源线），并在其额定规格内使用。
- 请使用满足 SELV（安全超低电压）要求的电源，并按照 IEC60950-1 符合 Limited Power Source（受限制电源）的额定电压供电，具体供电要求以设备标签为准。
- 请将 I 类结构的产品连接到带保护接地连接的电网电源输出插座上。
- 如果使用电源插头或器具耦合器等作为断开装置，请保持断开装置可以方便的操作。

系统使用须知

报警系统须知

总线防盗报警控制器构成的报警系统，虽然具有稳定可靠的性能，但是也可能由于以下原因发生失效，请认真阅读并知晓。

- 入侵者的入侵区域未加防护，或者入侵者通过足够的技术使系统故障或失灵。
- 警号设备安装位置不当，未能及时起到示警作用。
- 探测器发生如断电等意外故障，导致探测器未能响应。
- 探测器安装位置不当，无法探测到实际需要探测的区域。
- 用于传输报警信号的传输系统有问题，如被停掉服务、被恶意攻击等，导致系统未能及时报警。
- 由于没有定期维护和检查报警系统，导致其失效。

安装人员须知

- 安装人员需要对系统进行定期检查和维护，建议每月一次，以保证系统长期稳定地工作。
- 安装人员需要对系统进行定期测试，建议每周一次。
- 安装人员可以对用户进行培训，让用户了解系统并能熟练操作系统。

系统测试须知

- 安装完成后，您可以连接交流和直流电源进行测试。
- 您也可以完成所需设置，测试报警控制器的所有操作。

目录

1 产品概述

1.1 产品简介

本产品是专为大型报警方案应用设计的一款高性能报警控制器产品，采用嵌入式 Linux 操作系统，依托嵌入式平台开发支撑，系统运行稳定，具有先进的控制技术和强大的数据传输能力。

本产品采用嵌入式设计，安全性高、可靠性好。既可以本地独立工作，也可以联网组成一个强大的安全监控网，配合专业报警平台软件使用，可以充分体现其强大的组网和远程监控能力。

本产品可应用于学校、商铺、工厂、智能小区等各领域的安全防范。

1.1 产品功能

- 支持本地 16 路开关量输入，可扩展至 256 路开关量输入采集；支持接入常开或常闭型探测器；支持探测器防拆功能。
- 支持本地 8 路报警输出，并可扩展至 64 路报警输出控制；支持强制开启、强制关闭、自动控制功能。
- 支持扩展单防区、双防区。
- 支持多路继电器开关量报警输出，便捷实现报警联动及现场的灯光控制。
- 报警输入及报警输出接口皆具有保护电路，确保主控制器不受损坏。
- 支持异常报警，包括断网报警、PSTN 掉线报警、控制器防拆报警、蓄电池掉电报警、蓄电池欠压报警、电源故障报警、IP 冲突报警、MAC 冲突报警。
- 具备 RS485 接口，实现 RS485 报警键盘接入。键盘支持紧急报警，包括火警、匪警、医疗紧急报警、胁迫报警。
- 具备 PSTN 接口，实现报警事件上报功能，支持 Contact ID 协议。
- 具备 GSM 网络接口，实现报警事件短信发送功能。
- 具备标准以太网接口，实现网络远程访问功能。
- 支持单防区和子系统布撤防功能。
- 支持远程配置及远程查询。

2 开箱检查

运输公司将您所需的总线防盗报警控制器送到您手中时，请对照下表进行开箱检查，若有任何问题，请及时联系公司的售后服务人员。

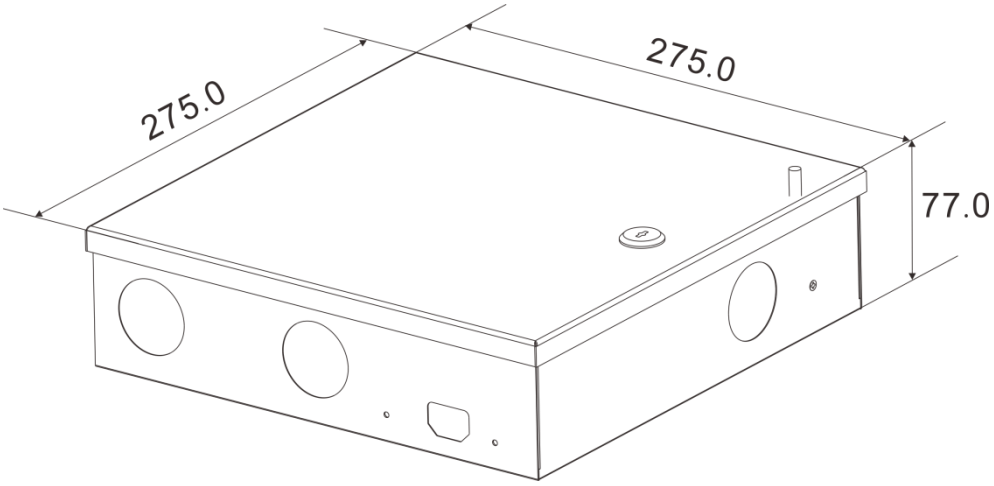
检查顺序	检查项		检查内容
1	整体包装	外观	有无明显的损坏
		包装	有无意外撞击
		配件（保修卡上的配件清单）	是否齐全
2	前后面板	前面板贴膜上的型号	是否与订货合同一致
		后面板上所贴的标签	有无撕毁 **说明** ● 不要撕毁、丢弃，否则不保证提供保修服务。 ● 您在拨打公司的售后电话时，需要您提供产品的序列号。
3	机壳	外观	有无明显的损坏
		数据线、电源线和主板	连接是否松动 **说明** 若有松动，请及时联系公司的售后服务人员。

3 安装与接线

3.1 整机外观

总线防盗报警控制器的外观如图 3-1 所示。

图3-1 整机外观（mm）



3.2 控制器安装

安装注意事项如下：

- 确保房间气温低于 35℃。
- 保持控制器周围有 15 厘米空间，以便于空气流通。

壁挂式安装的具体步骤如下：

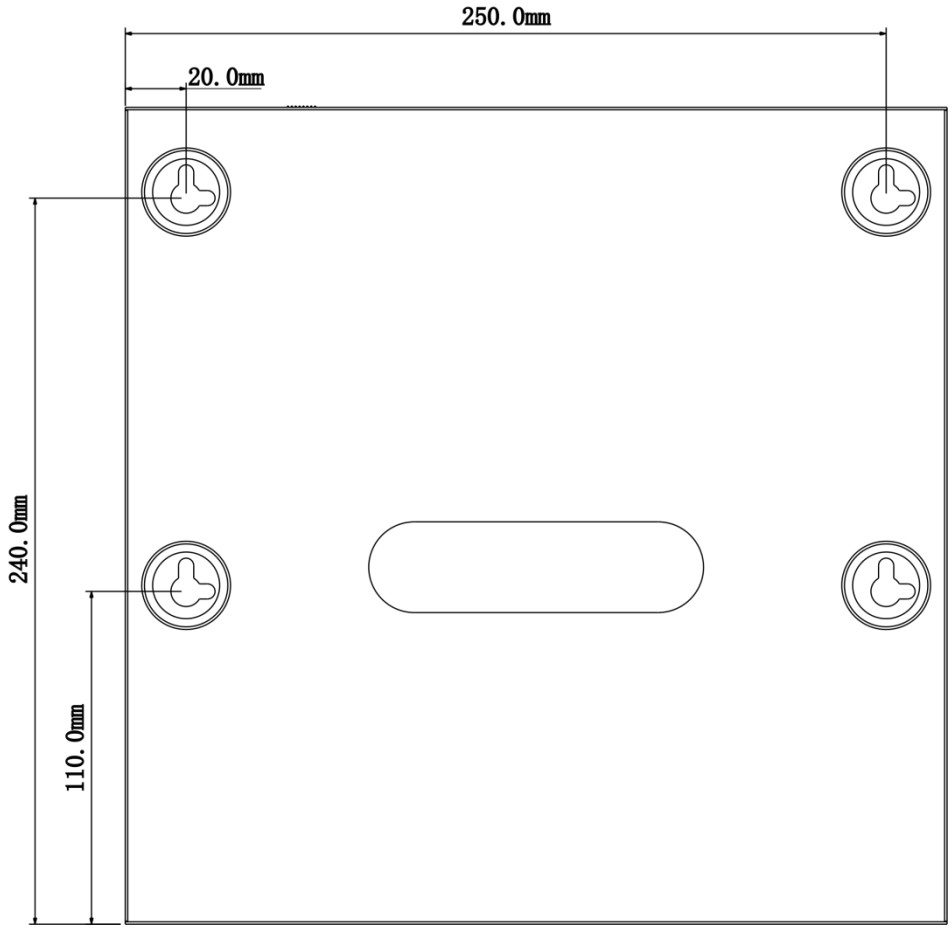
步骤1　请打开包装，取出“塑料膨胀螺栓”和“自攻螺钉”。

步骤2　按图 3-2 所示，在墙上打 4 个孔。

步骤3　放入“塑料膨胀螺栓”，拧入 4 个“自攻螺钉”。

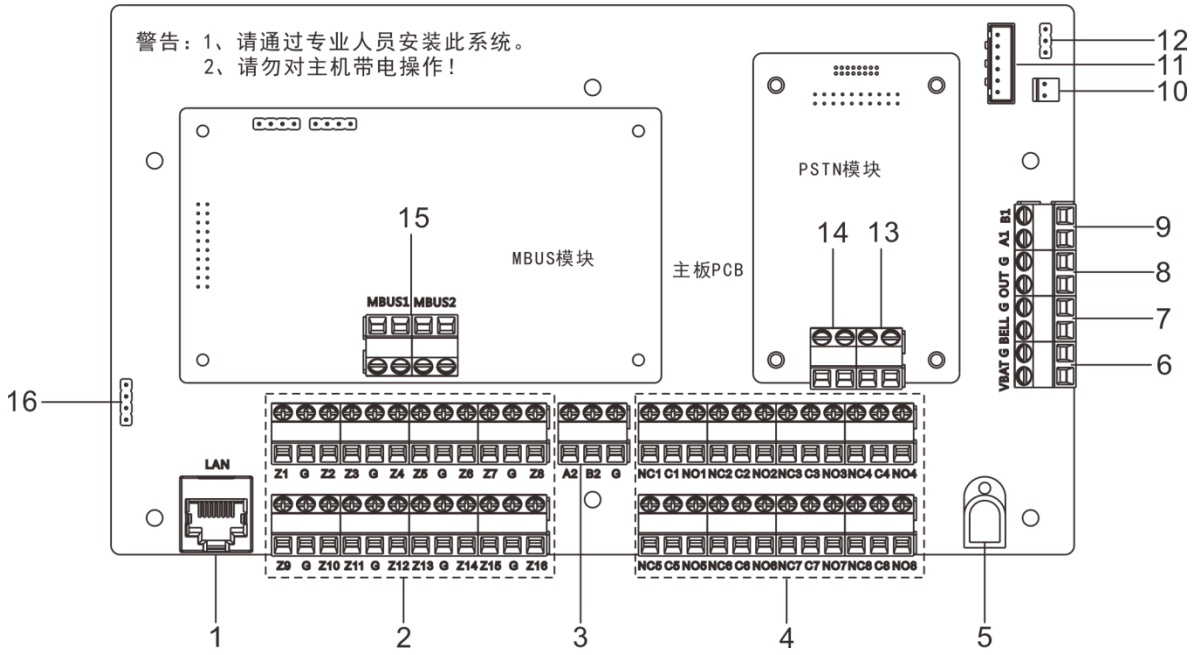
步骤4　将控制器挂在螺钉上。

图3-2 安装示意图



3.3 主板接口

图3-3 主板接口示意图



主板的接口说明如表 3-1 所示。

表3-1 主板接口说明

序号	说明
1	RJ45 网络接口。
2	本地报警输入接口，支持 16 路报警输入。
3	RS485 接口，接入 RS485 设备。
4	本地报警输出接口，支持 8 路报警输出。
5	DC 14.5V 电源接口。
6	DC 12V 铅酸蓄电池接口。
7	警号输出接口。
8	DC 12V 常电输出。
9	RS485 接口，接入报警编程键盘。
10	防拆开关接口。
11	2G 模块接口。
12	恢复出厂设置接口。
13	用户线接口。
14	电话机接口。
15	M-BUS 总线接口，支持 2 路扩展模块接入。
16	调试串口。

3.4 安装接线

3.4.1 线缆要求

线缆要求请参见表 3-2。

表3-2 线缆要求

设备	线材	单芯截面积	备注
网线	五类八芯屏蔽双绞线	≥0.22mm^2	最长距离≤100m
探测器	22AWG	≥0.32mm^2	最长距离≤2400m
编程键盘	22AWG	≥0.32mm^2	最长距离≤1000m
警号	22AWG	≥0.32mm^2	最长距离≤200m
电话入户线	HYX2×1	≥0.25mm^2	最长距离≤100m

3.4.2 本地报警输入接线

支持 16 路报警输入，对应接口为 Z1～Z16，支持常开、常闭探测器的四态接法和两态接法，连接示意图如图 3-4 和图 3-5 所示。若需要支持探测器的防拆时，需要将控制器配置成四态接法；若无须接入探测器的防拆时，需要将控制器配置成两态接法。

图3-4 探测器接线（常开类型）

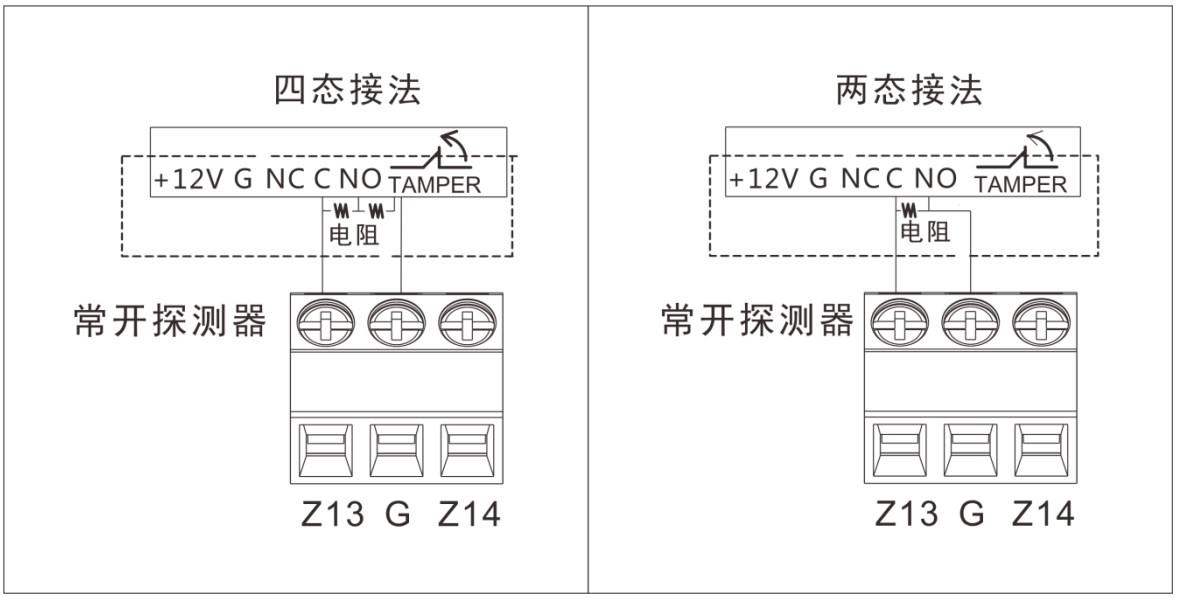
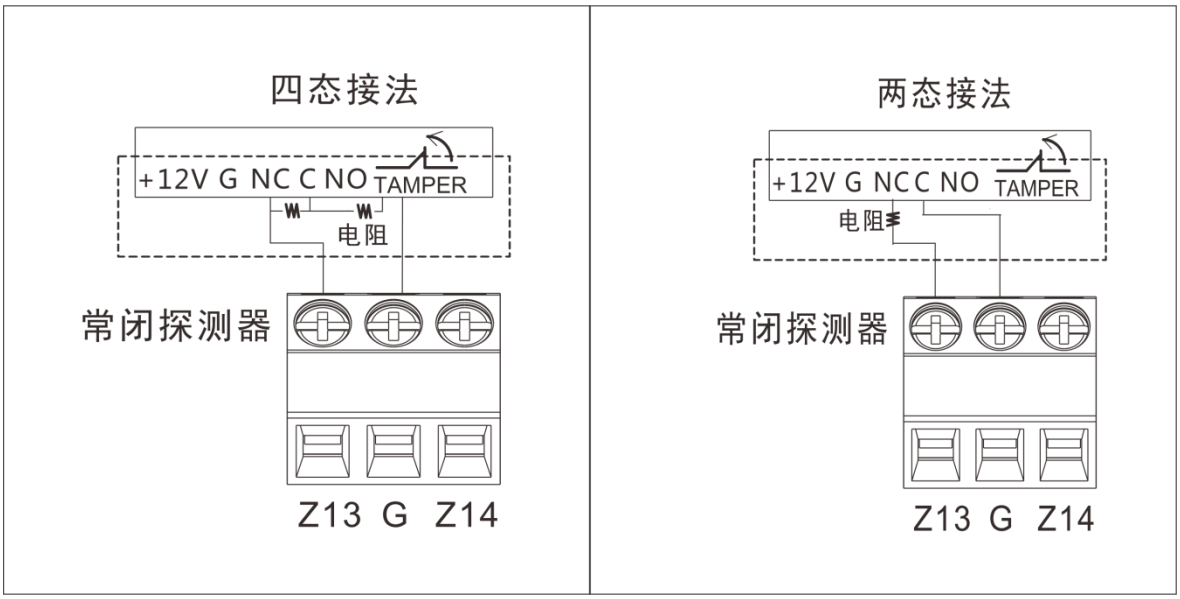


图3-5 探测器接线（常闭类型）



3.4.3 本地报警输出接线

注意

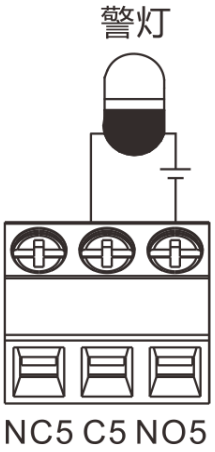
- 总线防盗报警控制器的报警输出不能连接大功率负载（不超过 1A），防止电流过大导致继电器的损毁，使用大功率负载需要用接触器隔离。
- 为避免过载而损坏主机，连接时请参阅继电器相关参数，相关的继电器说明请参见“附录 1 继电器参数表”。

支持 8 路报警输出，对应接口为（NC1、C1、NO1）～（NC8、C8、NO8）。

- NC：常闭端
- C：公共端（COM）
- NO：常开端

以常开类型的警号为例，连接示意图如图 3-6 所示

图3-6 本地报警输出接口



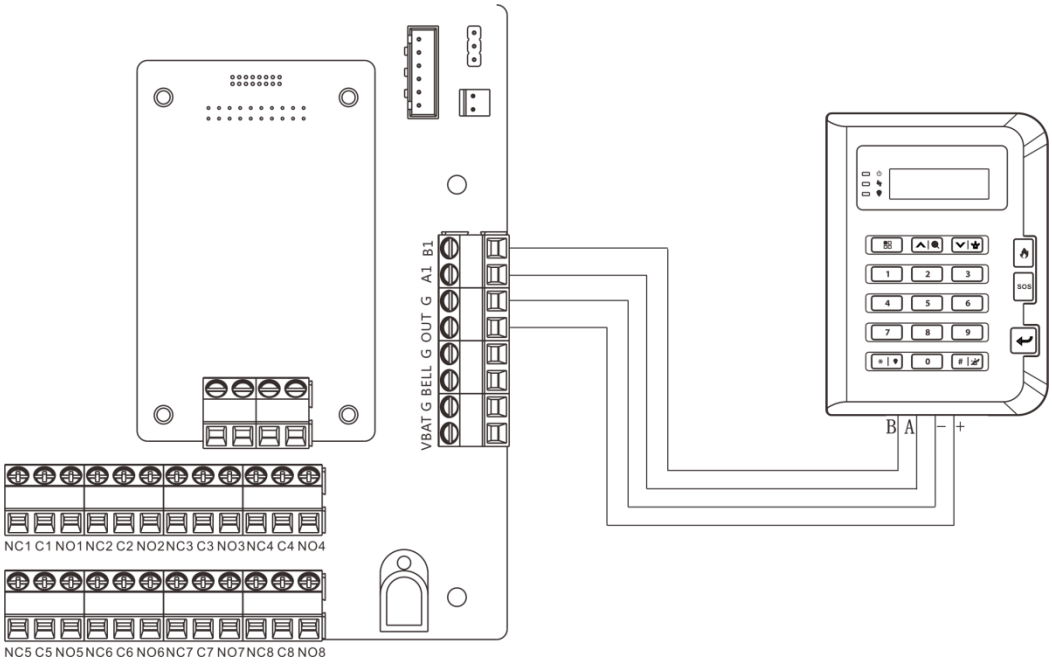
说明

外部报警设备（例如：警灯）需要外部电源供电。

3.4.4 键盘接线

键盘的“B”和“A”接口分别连接总线报警控制器的 B1、A1 接口（用于 485 通信），“－”和“＋”接口分别连接总线报警控制器的接地端 G 口和 OUT 接口，示意图如图 3-7 所示。

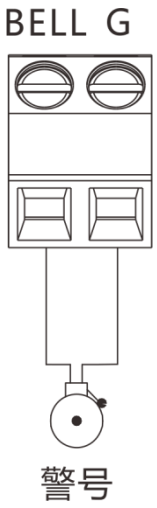
图3-7 键盘连接示意图



3.4.5 警号接线

警号连示意图如图 3-8 所示。

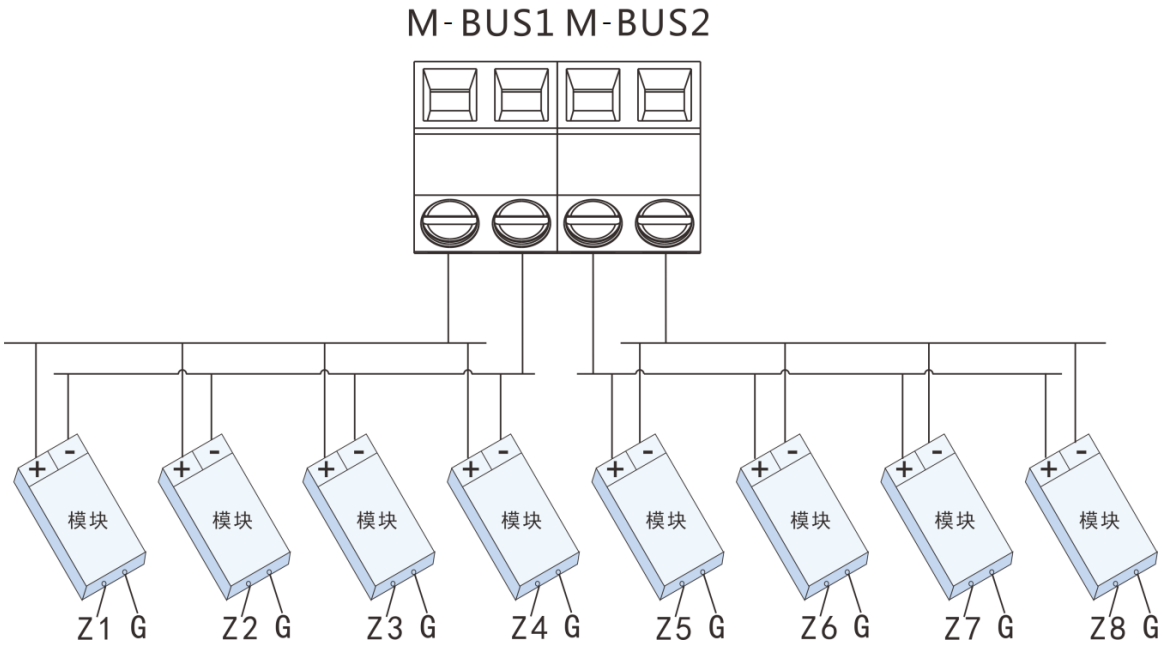
图3-8 警号接口



3.4.6 扩展模块接线

提供 2 路 M-BUS 总线接口，连接示意图如图 3-9 所示。

图3-9 扩展模块接线



说明

- 扩展模块输入线尾电阻阻值为 10kΩ。
- 扩展模块的地址拨码范围为 0～254，结合扩展模块（ARM801、ARM802、ARM911、ARM921、ARM808）使用，推荐接线要求请参见表 3-2，单路 M-BUS 模块可以支持 2.4km 通信距离。
- 每路 M-BUS 最多可接入的模块为：801 模块可接入 120 个，802 模块可接入 90 个，911 模块可接入 60 个，921 模块可接入 60 个，808 模块可接入 15 个。
- 扩展模块地址不能重复，否则控制器无法检测到扩展模块。

4 ARCConfig 工具操作

通过 ARCConfig 工具，可以实现控制器的初始化、升级，以及在忘记密码时重置密码。

ARRConfig 工具安装包的获取请联系技术支持，获取后请双击“.exe”文件，根据界面提示安装。

4.1 初始化控制器

首次使用控制器或恢复出厂设置后，需要通过 ARCConfig 工具初始化。

说明

- 请确保 PC 与控制器的默认 IP 在同一个网段内，出厂默认 IP 地址为 192.168.1.108。
- 初始化前请确保已有 ARCConfig 工具。

步骤1　搜索控制器。

1. 在 ARCConfig 工具中，单击“ > 搜索设置”。

   系统显示“设置”界面，如图 4-1 所示。

图4-1 设置

2. 根据实际情况选择搜索控制器的方式。
   - ◇ 当前网段搜索：选择“当前网段搜索”，并设置“用户名”和“密码”，系统搜索当前网段的设备。系统出厂默认为当前网段搜索。
   - ◇ 其他网段搜索：选择“其他网段搜索”，并设置“起始 IP”、“结束 IP”、“用户名”和“密码”，系统搜索设置网段的设备。

   说明

   - 当同时选择“当前网段搜索”和“其他网段搜索”时，系统同时搜索当前网段和设置网段的设备。
   - “用户名”和“密码”是修改 IP、配置系统参数信息和升级设备时登录设备的用户名和密码。
3. 单击“确定”，系统开始搜索设备。

   搜索完成后，系统显示搜索的设备，如图 4-2 所示。

图4-2 搜索结果

步骤2 初始化控制器。

1. 选择未初始化的控制器。
2. 单击 初始化 。

   系统显示“设备初始化”界面，如图 4-3 所示。

图4-3 控制器初始化（1）

3. 选择需要初始化的控制器，单击“初始化”。

   系统显示“设备初始化”界面，如图 4-4 所示。

图4-4 控制器初始化（2）

4. 设置控制器初始化参数，详细参数说明请参见表 4-1。

表4-1 控制器参数说明

参数	说明
用户名	用户名默认为 admin。
新密码	输入控制器的新密码，建议设置为 8 位～32 位，可以由数字、字母和特殊字符（除“'”、“"”、“;”、“:”、“&”外）三种类型中的两种组成。
确认密码	确认输入的新密码。
预留手机	默认是已选择状态，输入手机号码即可。预留的手机用于忘记密码时重置密码，建议设置。如果确定不需要预留手机，可以取消该选项。

5. 单击“初始化”。

初始化完成后，系统显示如图 4-5 所示。

表示初始化成功；表示初始化失败，单击图标可以查看详细信息。

图4-5 初始化完成

6. 单击“完成”，结束控制器初始化操作。
初始化完成后，工具主界面上控制器状态变为“已初始化”，控制器信息将显示在工具其他界面。

4.2 修改控制器 IP

通过 ARCConfig 工具将控制器 IP 修改为规划的 IP 地址。

4.2.1 单个修改

当控制器较少时或者控制器的登录密码不相同时，可以单个修改控制器的 IP 地址。

步骤1 单击  。

系统显示“修改 IP”界面，如图 4-6 所示。

图4-6 修改 IP

步骤2 单击需要修改 IP 的控制器对应的。

系统弹出“修改 IP”对话框，如图 4-7 所示。

说明

如果控制器没在设备列表中，请重新搜索控制器。

图4-7 修改 IP（1）

步骤3 根据实际情况选择设置 IP 地址的模式。

- DHCP 模式：当网络中存在 DHCP 服务器时，设置“模式”为“DHCP”，则控制器自动从 DHCP 服务器获取 IP 地址。
- 手动模式：设置“模式”为“静态”，并填写控制器的“目标 IP”、“子网掩码”和“网关”，则控制器的 IP 地址修改为设置的 IP 地址。

步骤4 单击“确定”，完成修改。

说明

如果修改失败，请确认搜索界面中的用户名和密码是否正确，用户名默认为 admin，密码

是初始化时设置的密码。

4.2.2 批量修改

当控制器较多且控制器的密码相同时，可以批量修改控制器的 IP 地址。

步骤1　单击  。

系统显示“修改 IP”界面。

步骤2　选择需要修改 IP 的控制器。

说明

如果控制器没在设备列表中，请重新搜索控制器。

步骤3　单击  。

系统弹出“修改 IP”对话框，如图 4-8 所示。

图4-8 修改 IP（2）

步骤4　根据实际情况选择设置 IP 地址的模式。

- DHCP 模式：当网络中存在 DHCP 服务器时，设置“模式”为“DHCP”，则控制器自动从 DHCP 服务器获取 IP 地址。
- 手动模式：设置“模式”为“静态”，并填写控制器的“起始 IP”、“子网掩码”和“网关”，则控制器的 IP 地址从起始 IP 开始依次递增修改。

说明

选择“同一 IP”，将选中的控制器设置为同一个 IP 地址。

步骤5　单击“确定”，完成修改。

说明

如果修改失败，请确认搜索界面中的用户名和密码是否正确，用户名默认为 admin，密码是初始化时设置的密码。

4.3 重置密码

通过扫描二维码或者 XML 文件重置密码。

说明

- 只能对局域网内的控制器进行密码重置。
- 若在初始化时没有设置预留信息，密码重置时只能通过 XML 文件方式。

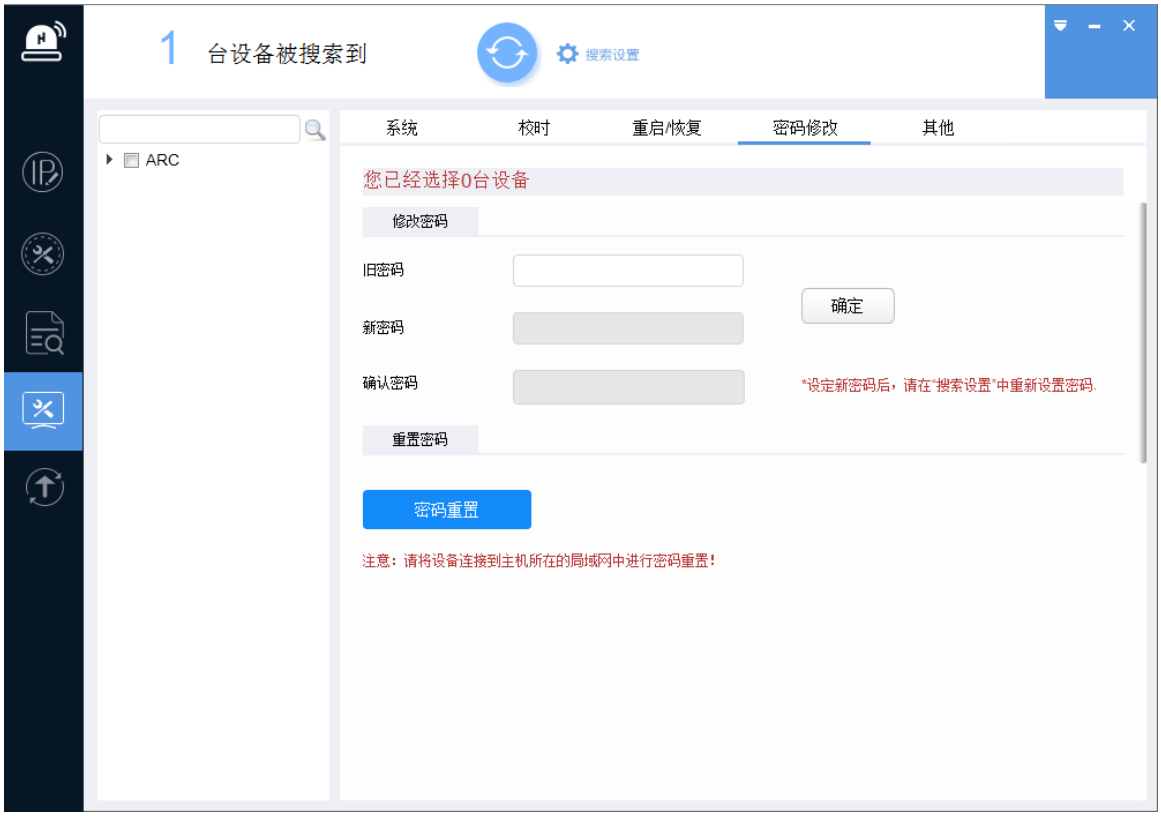
4.3.1 二维码重置密码

通过扫描界面上的二维码重置密码，仅支持单个控制器密码重置。

步骤1　选择“  > 密码修改”。

系统显示“密码修改”界面，如图 4-9 所示。

图4-9 密码重置（1）



步骤2　单击控制器类型前的▶，选择需要重置密码的单个控制器。

说明

如果控制器没在设备列表中，请重新搜索控制器。

步骤3　单击“密码重置”。

系统显示“密码重置”界面，如图 4-10 所示。

图4-10 密码重置（2）

步骤4　选择“重置方式”为“二维码”。

步骤5　根据实际界面指示操作，获取安全码。

注意

- 扫描二维码获取安全码时，一个二维码最多支持扫描获取两次安全码。
- 预留手机接收到安全码后，请在 24 小时内使用安全码重置密码，否则安全码将失效。

步骤6　输入“安全码”、“新密码”和“确认密码”。

新密码设置为 8 位～32 位，可以由数字、字母和特殊字符（除“'”、“"”、“;”、“:”、“&”外）三种类型中的两种组成。

说明

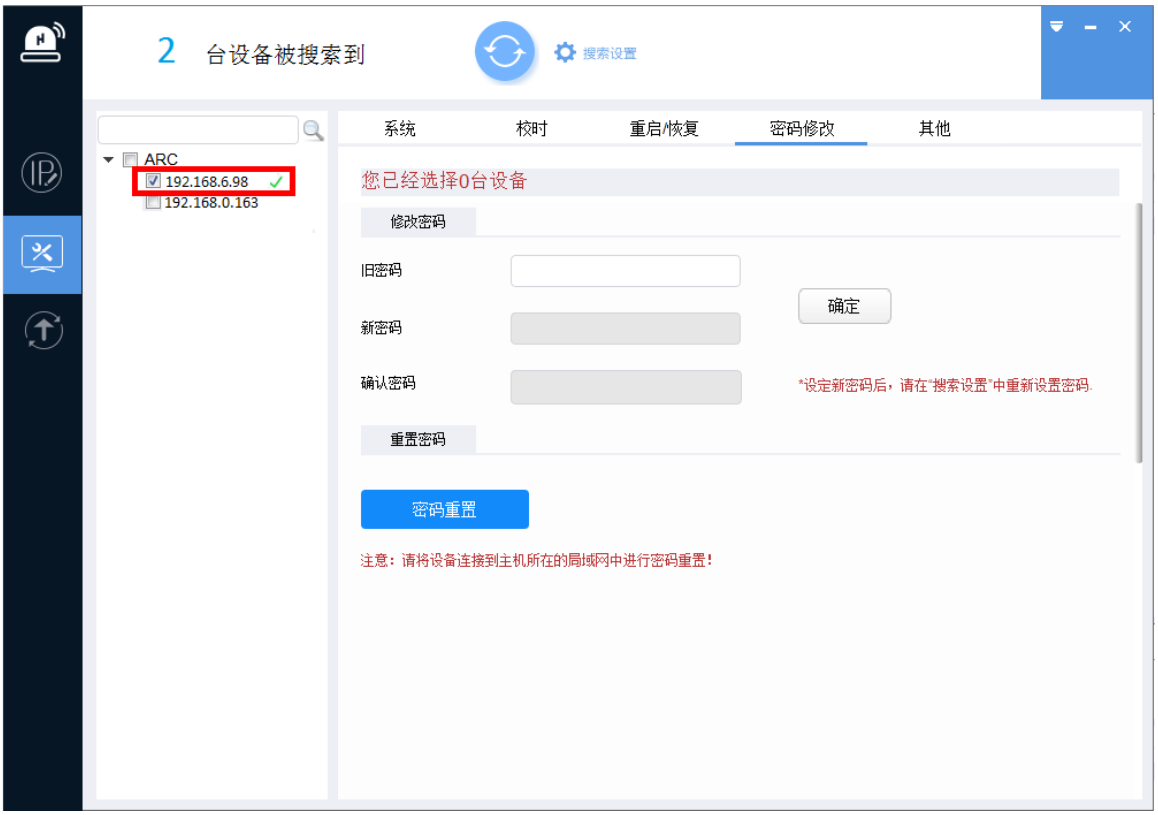
设置新密码后，在使用“搜索设置”搜索控制器时，请使用新密码登录控制器。

步骤7　单击“确定”，系统开始重置密码。

密码重置完成后，在设备处显示结果。

表示密码重置失败，表示密码重置成功。单击图标可以查看详细信息。

图4-11 密码重置结果



4.3.2 XML 文件重置密码

通过 XML 文件重置密码，仅支持单个控制器密码重置。

步骤1　在图 4-10 中，选择“重置方式”为“XML 文件”。

系统显示“密码重置-导出 XML”界面，如图 4-12 所示。

图4-12 密码重置-导出 XML

步骤2　导出 XML。

1. 单击“浏览”，选择导出 XML 文件的保存路径。
2. 单击“下一步”，开始导出。

   导出完成后，系统弹出提示对话框。
3. 单击“确定”，完成导出。

   导出 XML 文件成功后，系统自动进入“密码重置-导入 XML”界面。

步骤3　获取 result.xml 文件。

在 XML 文件的保存路径下找到 ExportFile.xml 文件，按照界面提示将此文件作为邮件附

件发送至指定邮箱。约几分钟后，您会收到附件形式的 result.xml 文件，将其保存至任意路径。

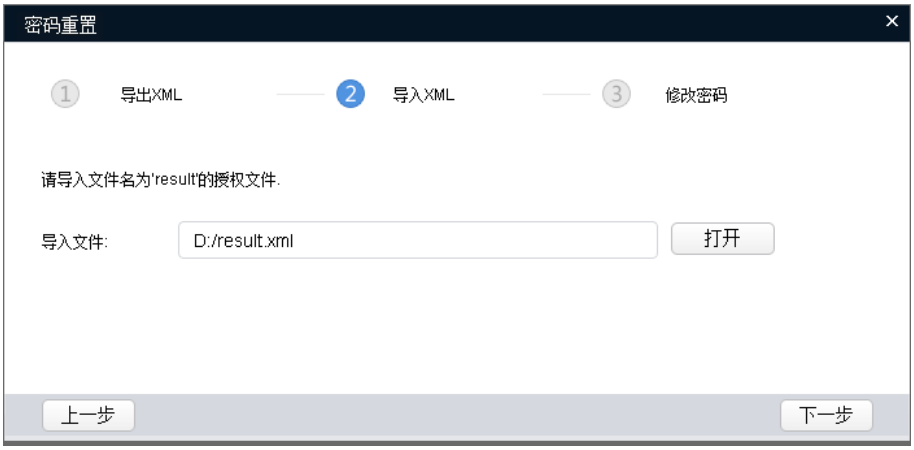
步骤4　导入 XML。

说明

若导入 XML 的窗口已关闭，可以选择“系统设置 > 密码重置”，在“密码重置”页签上，单击“继续上次修改密码操作，请导入 XML 文件”，以继续操作。

1. 单击“打开”，从保存路径导入 result.xml 文件，如图 4-13 所示。

图4-13 密码重置-导入 XML



2. 单击“下一步”，开始导入。

导入 XML 文件成功后，系统自动进入“密码重置-修改密码”界面，如图 4-14 所示。

图4-14 密码重置-修改密码

步骤5　修改密码。

输入“新密码”和“确认密码”。新密码设置为 8 位～32 位，可以由数字、字母和特殊字符（除“'”、“"”、“;”、“:”、“&”外）三种类型中的两种组成。

说明

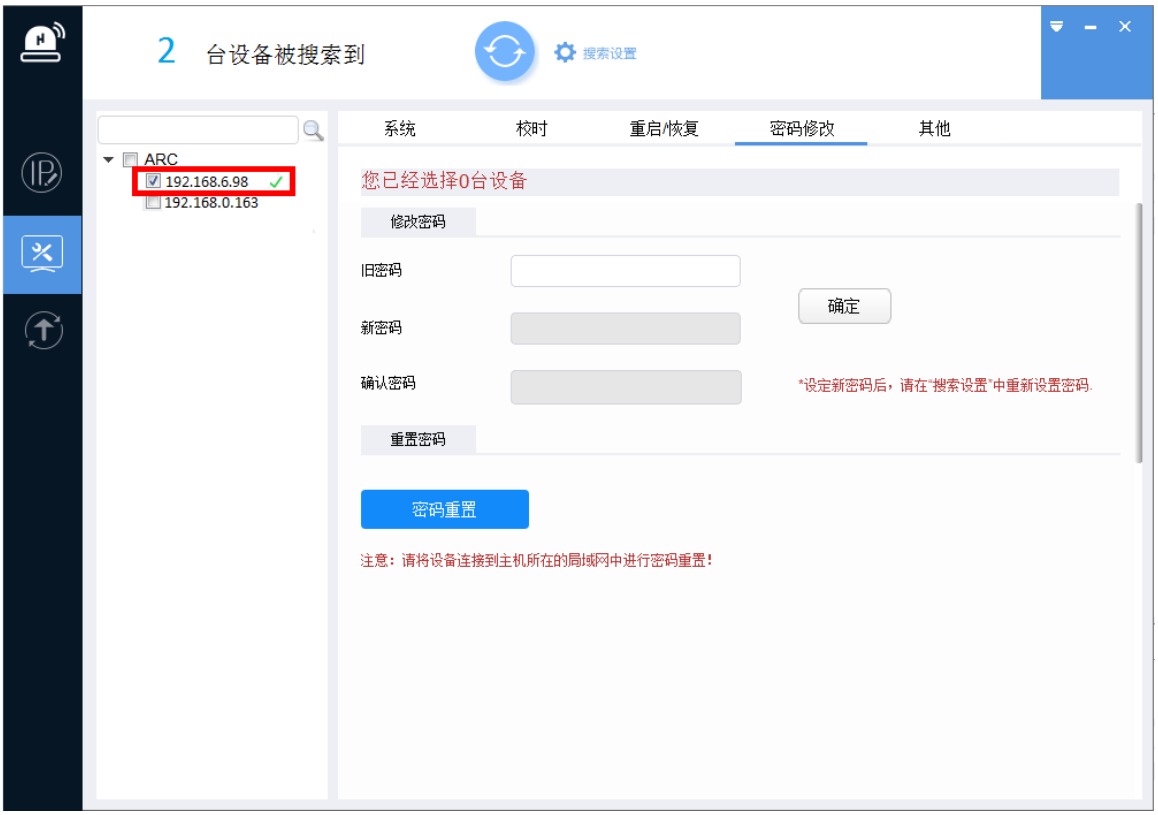
设置新密码后，在使用“搜索设置”搜索控制器时，请使用新密码登录控制器。

步骤6　单击“完成”，系统开始重置密码。

密码重置完成后，在控制器处显示结果，如图 4-15 所示界面。

表示参数均配置成功；表示有参数配置失败，单击图标可以查看详细信息。

图4-15 设置结果



4.4 升级控制器程序

通过 ARCConfig 工具升级控制器程序。

说明

升级过程中如果控制器断开连接，只要工具继续停留在升级界面，当再次连上网络时，会继续进行升级。

4.4.1 单个升级

对某一个控制器升级程序。

步骤1 单击 。

系统显示“升级”界面，如图 4-16 所示。

图4-16 升级

步骤2 单击需要升级控制器对应的“打开”，选择升级文件。

说明

如果控制器没在设备列表中，请重新搜索控制器。

步骤3 单击“升级”，系统开始升级并显示进度。

升级完成后，系统提示“升级成功”，控制器自动重新启动。

4.4.2 批量升级

将多个控制器批量升级到同一软件版本。

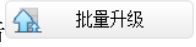
步骤1 单击  。

系统显示“升级”界面。

步骤2 选择需要升级控制器。

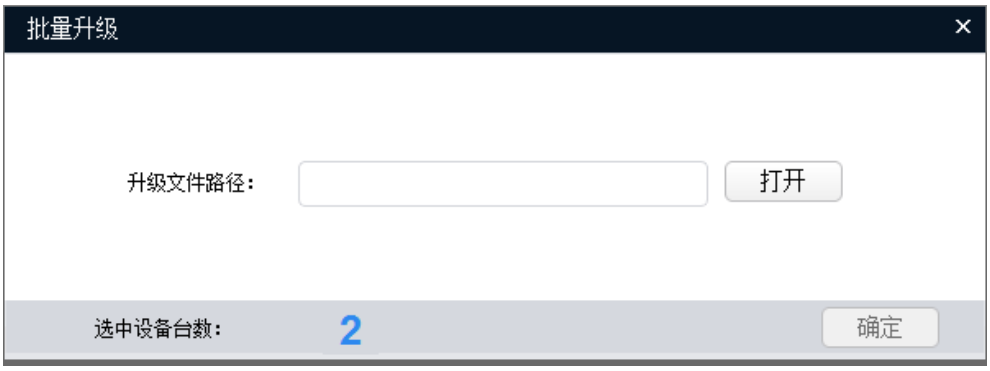
说明

- 如果控制器没在设备列表中，请重新搜索控制器。
- 选择的控制器必须是升级到同一个软件版本的控制器。

步骤3 单击  。

系统显示“批量升级”界面，如图 4-17 所示。

图4-17 批量升级



步骤4　单击“打开”，选择升级文件。

步骤5　单击“确定”，系统开始升级。

5 SDK 客户端操作

您可以通过登录报警控制器 SDK 客户端，查看和配置报警控制器参数。

5.1 登录

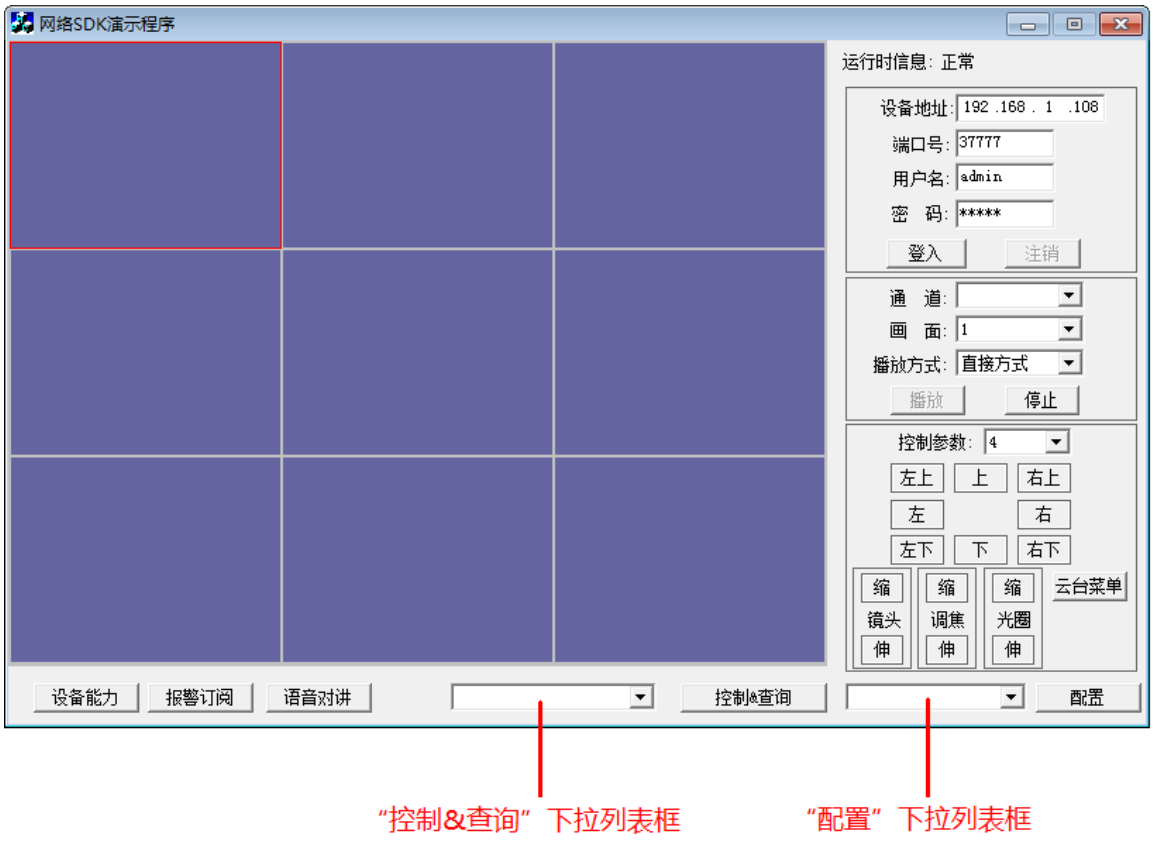
注意

请确认控制器已初始化，如果还未初始化，请先使用 ARCConfig 工具对其初始化，具体操作参见“4.1 初始化”。

步骤1　在“AlarmDeviceDemo\Bin”文件夹下，双击“AlarmDevice.exe”文件。

系统显示“网络 SDK 演示程序”界面，如图 5-1 所示。

图5-1 网络 SDK 客户端主界面



步骤2　输入“设备地址”、“端口号”、“用户名”和“密码”，单击“登入”，登录 SDK 客户端。

说明

- 首次登录前，必须确保所使用的 PC 与控制器处于同一网段内，控制器初始 IP 为 192.168.1.108。
- 默认端口号为 37777，默认用户名和密码均为 admin，首次登录后请及时修改密码，具体请参

见“5.2.18 修改密码”。

- 如果出现登录失败的情况，请查询“8 常见问题解答”。
- 如果同一个 PC 上需要同时打开多个 SDK 客户端，请在安装目录下复制多个 AlarmDevice.exe 文件并重命名，文件名不可相同，如 AlarmDevice1.exe、AlarmDevice2.exe。

5.2 控制器基本配置

5.2.1 网络配置

您可以通过网络设置，设置控制器 IP 地址、子网掩码和网关。

步骤1　在主界面“配置”下拉列表框中选择“网络设置”。

步骤2　单击“配置”。

系统显示“网络配置”界面，如图 5-2 所示。

图5-2 网络设置

步骤3　输入控制器“IP 地址”、“子网掩码”和“默认网关”。

步骤4　单击“设置”，完成配置。

说明

控制器出厂默认 IP 为 192.168.1.108，默认子网掩码为 255.255.255.0，默认网关为 192.168.1.1。

5.2.2 时间配置

5.2.2.1 设置和读取时间

您可以根据实际情况设置和读取时间。

步骤1　在主界面“控制&查询”下拉列表框中选择“设备时间”。

步骤2　单击“控制&查询”。

系统显示“设备时间设置”界面，如图 5-3 所示。单击“获取”，可查看控制器当前时间。

说明

首次进入该界面时，显示的是 PC 时间。

图5-3 设备时间设置

步骤3　设置日期和时间。

步骤4　单击“设置”，完成配置。

5.2.2.2 时间同步服务器

您可以设置时间同步服务器，使控制器时间与时间服务器同步。

步骤1　在主界面“配置”下拉列表中选择“时间同步服务器”。

步骤2　单击“配置”。

系统显示“时间同步配置”界面，如图 5-4 所示。单击“获取”，可查看当前设置的同步情况。

图5-4 时间同步服务器

步骤3　配置参数，详细参数说明请参见表 5-1。

表5-1 时间同步配置

参数	说明
使能开关	是否启用时间同步，选择“使能开关”，表示启用。
IP 地址或网络域名称	时间同步服务器的 IP 地址。
端口号	时间同步服务器的端口号。

参数	说明
更新周期	控制器与同步服务器同步的间隔时间。
时区	选择时区。
时区描述	自定义时区名称方便区分。

步骤4　单击“设置”，完成配置。

5.2.2.3 夏令时配置

您可以根据需要启用夏令时，控制器将根据夏令时运行。

步骤1　在主界面“配置”下拉列表中选择“夏令时、冬令时”。

步骤2　单击“配置”。

系统显示“夏令时、冬令时”界面，如图 5-5 所示。单击“获取”，查看控制器当前的设置情况。

图5-5 夏令时

步骤3　选择“夏令时”，选择设置类型。

- 若选择为“按日期”，则需要根据“年月日”和“时分”设置夏令时的开始和结束时间。
- 若选择为“按星期”，则需要根据“月份”、“周数”、“星期”、“时”和“分”设置夏令时的开始和结束时间。

步骤4　单击“设置”，完成配置。

启用夏令时后，如果当前控制器时间到达夏令时开始时间时，控制器时间会自动增加 1 小时。

5.2.3 传感器安装模式配置

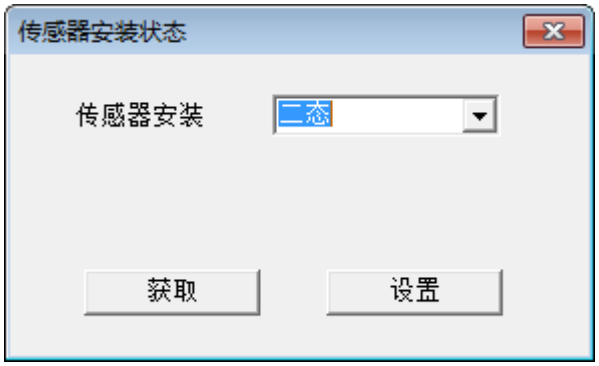
安装探测器后，您需要对探测器的安装模式进行配置。

步骤1　在主界面“配置”下拉列表框中选择“传感器安装模式配置”。

步骤2　单击“配置”。

系统显示“传感器安装状态”界面，如图 5-6 所示。单击“获取”，可查看控制器当前探测器的安装状态。

图5-6 传感器安装状态



步骤3　在下拉框中选择传感器安装状态，单击“设置”，完成配置。

安装状态包括二态和四态两种，具体安装模式请参见“3.4.2 本地报警输入接线”。

5.2.4 开关量防区配置

您可以配置本地报警输入通道、防区、传感器类型及报警联动等参数。

注意

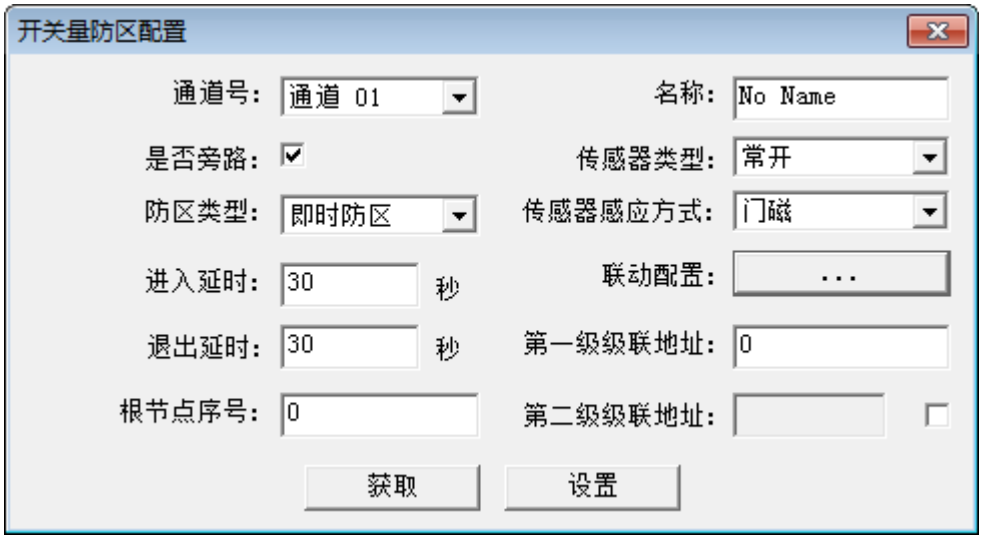
- 当防区一直有报警输入或者有报警触发时，则无法保存配置。
- 需要在撤防状态下设置。

步骤1　在主界面“配置”下拉列表框中选择“开关量防区配置”。

步骤2　单击“配置”。

系统显示“开关量防区配置”界面，如图 5-7 所示。选择“通道号”，单击“获取”，可查看该防区的配置情况。

图5-7 开关量防区配置



步骤3　配置参数，详细参数说明请参见表 5-2。

表5-2 开关量防区配置

参数	说明
通道号	本地报警输入通道号（1～256）。
名称	自定义通道名称，便于区别。

参数	说明
是否旁路	防区旁路设置请参见“5.4.4 旁路控制”。
防区类型	控制器支持以下防区类型。 ● 即时防区。 ● 延时防区。 ● 全天防区。
进入延时	进入防区的时间，当“防区类型”设置为“延时防区”时，若“进入延时”设置为 10s，触发该防区报警后，用户有 10s 时间来进行撤防。若 10s 内成功撤防，则不联动报警；若 10s 内未成功撤防，则联动报警。
退出延时	离开防区的时间，当“防区类型”设置为“延时防区”时，若“退出延时”设置为 10s，用户设置布防后，10s 之后布防开始生效。
传感器类型	根据传感器类型（即探测器类型），选择“常开”或者“常闭”。 **说明** ● 常开类型探测器触发防拆报警时，PSTN 会上报防区防拆事件，SDK 会上报开关量报警事件。 ● 常闭类型探测器触发短路报警时，PSTN 会上报防区短路事件，SDK 会上报开关量报警事件。
传感器感应方式	本主机不支持。
联动配置	当有报警输入时，可自动联动报警输出通道，详细请参见“步骤 4”。
根节点序号	0 代表本地防区，1 代表 M-BUS 扩展防区，2 代表 485 扩展防区。
第一级级联地址	根节点下面的防区序号或扩展模块地址（以本地防区 16 路为例）。 ● 如果根节点为 0，则第一级级联地址分别为 0～15，对应本地报警输入通道 Z1～Z16，第二级级联地址此时无意义，不需要使能。 ● 如果根节点为 1，则第一级级联地址为 M-BUS 扩展模块的地址（地址由模块上面的拨码开关决定，支持 0～254），第二级级联地址（0～7）代表该扩展模块的防区序号（Z1～Z8），第二级级联地址需要选择使能。 ● 如果根节点为 2，则第一级级联地址为 485 扩展模块的地址（地址由模块上面的拨码开关决定，支持 0～7），第二级级联地址（0～7）代表该扩展模块的防区序号（Z1～Z8），第二级级联地址需要选择使能。 **说明** 防区之间地址不能重复。即不同防区的根节点序号相同时，第一级联地址、第二级联地址及使能不能完全相同。

步骤4　单击联动配置后面的…。

系统显示“联动配置”界面，如图 5-8 所示。

图5-8 联动配置

步骤5 当根据时间段布防时，需要手动设置布防时间。以星期为周期，每天提供 6 个时间段，设置时间后选择“使能”复选框，表示启用该时间段。

步骤6 配置联动参数，详细说明请参见表 5-3。

表5-3 联动参数说明

参数	说明
报警输出	是否使能“报警输出”，选择表示启用。
报警输出通道	选择报警输出通道号。
MMS	是否发送短信，选择表示启用。
蜂鸣	是否启用“蜂鸣器”，选择表示启用。
警号	是否启用“警号”，选择表示启用。
电话报警中心	选择“是否上报”，表示启用。启用后，可以选择上报电话报警中心 1 或者电话报警中心 2。
警号延时	本主机不支持。
语音提示	
联动语音文件绝对路径	
上传报警服务器	
门禁	
门禁通道	
门禁操作	
语音呼叫使能	
语音呼叫发起方	
语音呼叫协议	

步骤7 单击“确定”，完成联动设置。

返回到“开关量防区配置”界面。

步骤8 单击“设置”，完成开关量防区所有配置。

说明

如果该防区有报警输入或者报警触发，则会提示配置失败。

5.2.5 单防区/子系统布撤防使能配置

注意

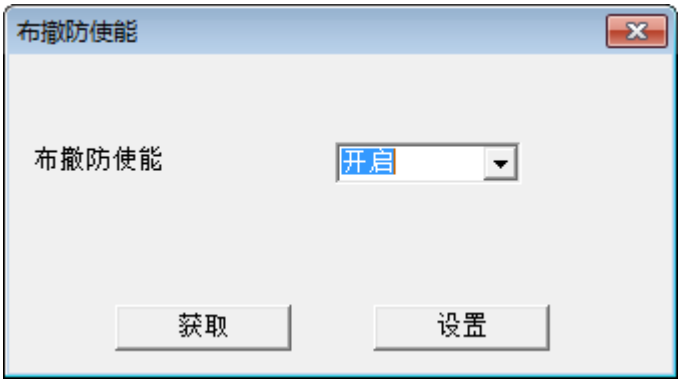
只有开启单防区/子系统布撤防使能后，才可以对某个防区或子系统进行布撤防操作。

步骤1　在主界面“配置”下拉列表框中选择“单防区/子系统布撤防使能”。

步骤2　单击“配置”。

系统显示“布撤防使能”界面，如图 5-9 所示。单击“获取”，可获得系统当前的使能状态。

图5-9 单防区/子系统布撤防使能



步骤3　在下拉框中选择使能状态。

“开启”表示可以进行单防区或子系统布撤防，“关闭”表示不可以进行单防区或子系统布撤防。

步骤4　单击“设置”，完成配置。

5.2.6 报警子系统配置

您可以对各个子系统进行防区配置。

注意

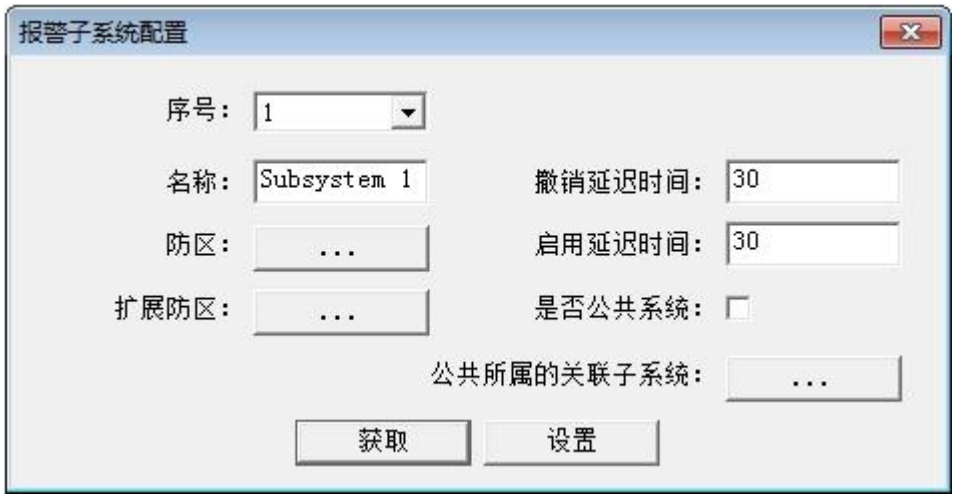
- 只有添加了防区的子系统可以进行子系统布撤防操作。
- 只有控制器撤防时，才能进行子系统配置。

步骤1　在主界面“配置”下拉列表框中选择“报警子系统”。

步骤2　单击“配置”。

系统显示“报警子系统配置”界面，如图 5-10 所示。单击“获取”，可获得系统当前的配置信息。

图5-10 报警子系统

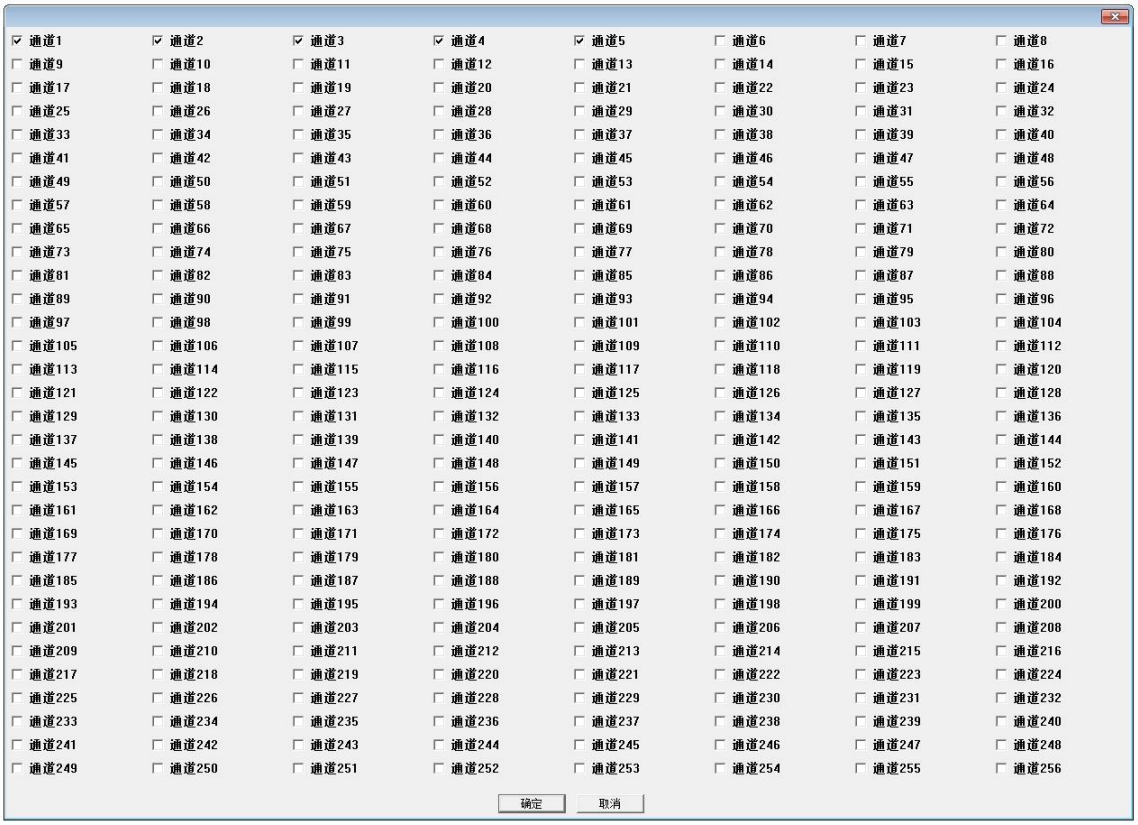


步骤3　配置相关参数，具体说明请参见表 5-4。

表5-4 子系统参数

参数	说明
序号	在下拉框中选择子系统序号。
名称	自定义子系统名称。
防区	单击 ··· ，弹出子系统防区界面，如图 5-11 所示。查看或设置当前子系统所分配的防区。 **说明** 子系统之间防区不能重复。
扩展防区	本主机不支持这些功能。
撤销延迟时间	
启用延迟时间	
是否公共系统	
公共所属的关联子系统	

图5-11 子系统防区



步骤4 单击“设置”，完成设置。

5.2.7 报警输出配置

您可以为每个报警输出通道配置相应的输出模式。

步骤1 在主界面“配置”下拉列表框中选择“报警输出配置”。

步骤2 单击“配置”。

系统显示“本地报警输出配置”界面，如图 5-12 所示。选择“通道号”，单击“获取”，可获得当前通道的配置信息。

图5-12 报警输出配置

步骤3　配置参数，详细参数请参见表 5-5。

表5-5 报警输出配置参数说明

参数	说明
通道号	选择报警输出通道号（1～64）。
通道名称	自定义通道名称，便于识别。
输出类型	自定义输出报警名称，便于识别。
输出模式	选择报警输出模式： ● 自动报警：自动模式。 ● 强制报警：强制该通道报警输出。 ● 关闭报警：关闭该通道报警输出。
脉冲模式输出时间	设置报警输出的持续时间，以分钟为单位。
Slot	0 代表本地防区，1 代表 M-BUS 扩展防区，2 代表 485 扩展防区。
Level1、Level2	根节点下面的防区序号或扩展模块地址（以本地 8 路报警输出通道为例）。 ● 如果根节点为 0，则第一级级联地址分别为 0～7，对应本地报警输出通道 NO1-COM1-NC1~NO8-COM8-NC8；第二级级联地址此时无意义，不需要使能。 ● 如果根节点为 1，则第一级级联地址为 M-BUS 扩展模块的地址（地址由模块上面的拨码开关决定，支持（0～254），第二级级联地址对应该模块上的报警输出通道（0～1），第二级级联地址需要选择使能。 ● 如果根节点为 2，则第一级级联地址为 485 扩展模块的地址（地址由模块上面的拨码开关决定，支持（0～7），第二级级联地址对应该模块上的报警输出通道（0～15），第二级级联地址需要选择使能。

步骤4　单击“设置”，完成配置。

5.2.8 警号配置

您可以设置各个通道的警号输出情况。

步骤1　在主界面“配置”下拉列表框中选择“警号控制”。

步骤2　单击“配置”。

系统显示“警号配置”界面，如图 5-13 所示。选择“通道号”，单击“获取”，可获得该通道的警号输出情况。

图5-13 警号配置

步骤3　选择“通道号”，输入“持续输出时间”。

步骤4　单击“设置”，完成警号输出配置。

5.2.9 电话报警中心配置

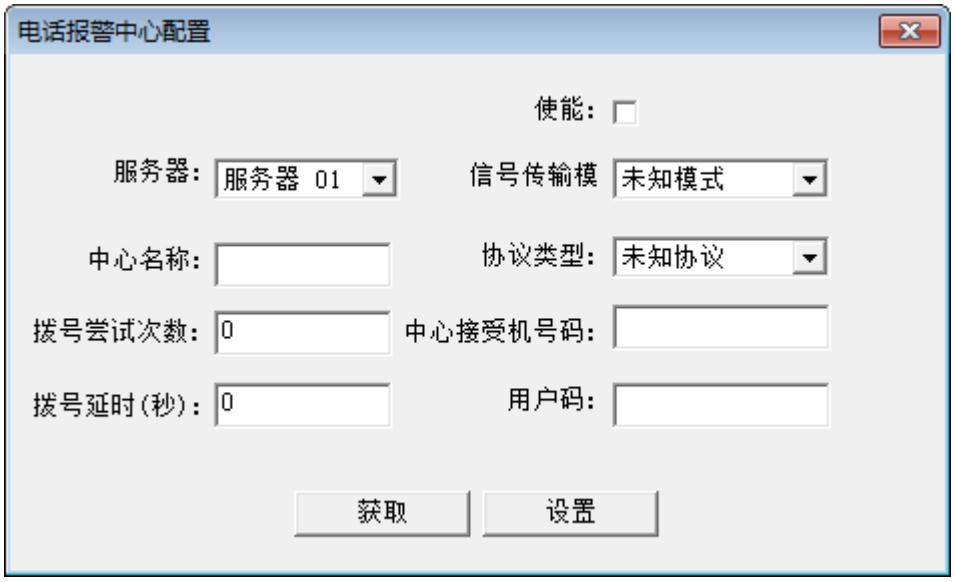
您可以设置电话中心参数，当有报警发生时，系统将报警信息发送给电话中心。

步骤1　在主界面“配置”下拉列表框中选择“电话报警中心配置”。

步骤2　单击“配置”。

系统显示“电话报警中心配置”界面，如图 5-14 所示。选择“服务器”，单击“获取”，可获得该服务器的使能情况。

图5-14 电话报警中心配置



步骤3　配置参数，详细参数说明请参见表 5-6。

表5-6 电话报警中心参数

参数	说明
使能	开启或关闭电话中心接警功能，选择“使能”表示开启。
服务器	电话中心服务器名称。
中心名称	自定义电话中心的名称。
拨号尝试次数	电话中心未接警时重拨的次数，范围为 1～9。

参数	说明
拨号延时	两次拨号尝试的时间间隔。
信号传输模	使用默认值，默认为 DTMF 5/S。
协议类型	使用默认值，默认为 CID。
中心接受机号码	电话中心的号码。
用户码	电话中心提供的用户码，系统支持 4 位数，由 0～9，b～f 组成，默认为 0000。

步骤4　单击“设置”，完成配置。

5.2.10 短信配置

控制器支持短信服务，您可以绑定手机号码。当发生蓄电池、电源、断网、报警等事件时，系统会发送短信给指定手机用户。

步骤1　在主界面“配置”下拉列表框中选择“移动业务配置”。

步骤2　单击“配置”。

系统显示“短信配置”界面，如图 5-15 所示。单击“获取”，可获取系统当前的配置信息。

图5-15 短信配置

步骤3　选择“使能开关”，表示启用移动业务。

步骤4　信息类型选择为“短信”，输入“信息标题”。

说明

信息标题最多支持 10 个汉字或者 30 个英文字符。

步骤5　设置指定手机用户号码。

在“收信号码”文本框中输入手机号码，单击 ，将号码添加到列表中；或者在列表中选

中某号码，单击，删除该号码。

说明

最多支持 5 组号码。

步骤6　单击“设置”，完成配置。

5.2.11 个人电话接机配置

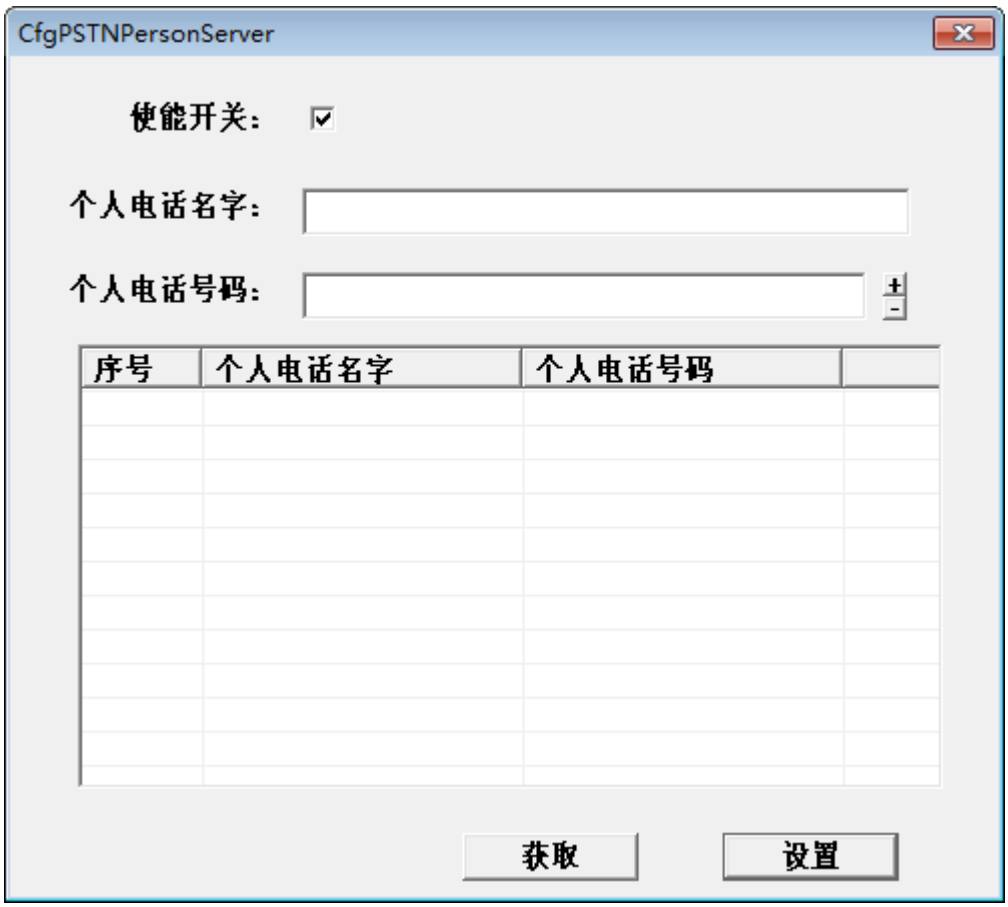
您可以使能并配置个人电话接机，当防区有报警时，个人电话会语音投放“防区报警”。

步骤1　在主界面“配置”下拉列表框中选择“个人电话接机配置”。

步骤2　单击“配置”。

系统显示“个人电话接机配置”界面，如图 5-16 所示。单击“获取”，可获取系统当前的配置信息。

图5-16 个人电话接机配置



步骤3　选择“使能开关”。

步骤4　输入“个人电话名字”和“个人电话号码”，单击“+”。

将个人电话信息加入列表中，最多个添加 3 组信息。

步骤5　单击“设置”，完成配置。

5.2.12 自动维护配置

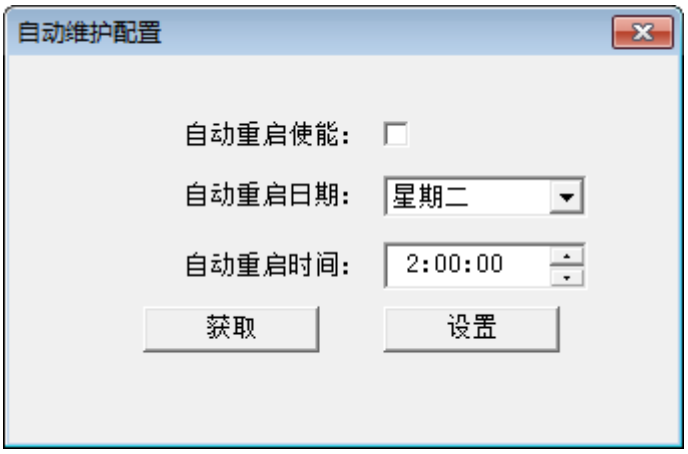
支持自动重启功能，您可以设置自动重启参数，控制器会在设置的时间点自动进行重启。

步骤1　在主界面“配置”下拉列表框中选择“自动维护配置”。

步骤2　单击“配置”。

系统显示“自动维护配置”界面，如图 5-17 所示。单击“获取”，可获取系统当前的配置信息。

图5-17 自动维护配置



步骤3　选择“自动重启日期”和“自动重启时间”。

说明

- 自动重启使能目前无效。
- “自动重启日期”选择为“永不”，表示不启用该功能。
- 只有设置整点的时间，才能成功保存。例如设置为 2:00:00，可以成功保存；设置为 2:30:00，则保存失败。

步骤4　单击“设置”，完成配置。

5.2.13 PSTN 测试计划配置

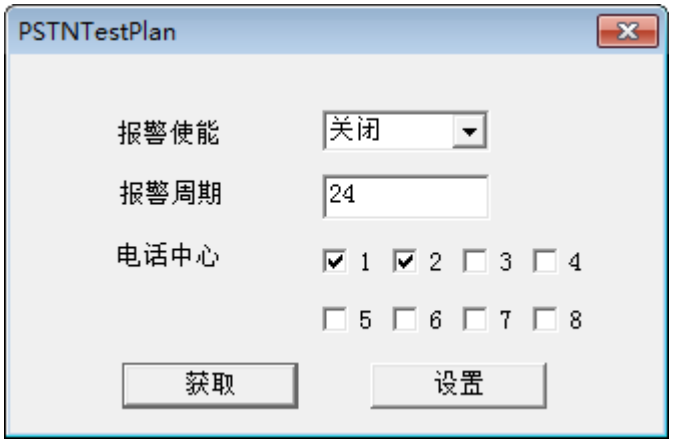
您可以开启 PSTN 的测试计划，定时检测控制器到电话接警中心的链路是否连通。

步骤1　在主界面“配置”下拉列表框中选择“PSTN 测试计划配置”。

步骤2　单击“配置”。

系统显示“PSTN 测试计划配置”界面，如图 5-18 所示。单击“获取”，可查看控制器当前的 PSTN 测试计划。

图5-18 PSTN 测试计划配置



步骤3　将“报警使能”选择为“开启”。

步骤4　输入“报警周期”，并选择电话中心。

说明

报警周期范围为 1~24，单位为小时。

步骤5　单击“设置”，开启 PSTN 测试计划。

5.2.14 手动测试 PSTN 连接状态

您可以通过 SDK 客户端，手动测试控制器到电话接警中心的链路是否连通。

步骤1　在主界面“控制&查询”下拉列表框中选择“手动测试 PSTN 连接状态”。

步骤2　单击“控制&查询”。

系统显示“手动测试 PSTN”界面，如图 5-19 所示。

图5-19 手动测试 PSTN

步骤3　单击“手动测试”。

系统将呼叫电话接警中心，检测是否能够呼通。

5.2.15 布撤防联动配置

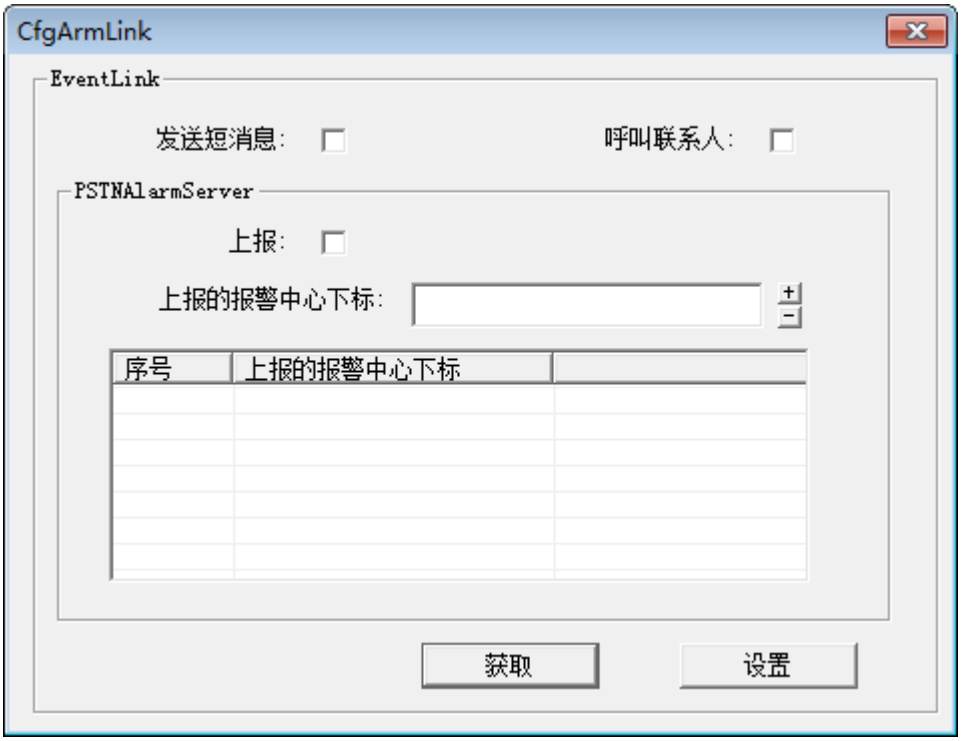
您可以配置布撤防联动参数，当布防或撤防操作发生时，系统会联动电话接警中心。

步骤1　在主界面“配置”下拉列表框中选择“布撤防联动配置”。

步骤2　单击“配置”。

系统显示“布撤防联动配置”界面，如图 5-20 所示。单击“获取”，可获取系统当前的配置信息。

图5-20 布撤防联动配置



步骤3 配置参数，详细参数说明请参见表 5-7。

表5-7 布撤防联动参数

参数	说明
发送短消息	本主机不支持。
呼叫联系人	
上报	1. 选择“上报”，开启联动电话报警中心功能。 2. 在“上报的报警中心下标”文本框中输入报警中心序号，单击“+”，添加到列表中。 说明 ● 设置前请确保已配置电话报警中心，具体请参见“5.2.9 电话报警中心配置”。 ● 输入 0 表示联动接警中心 1，输入 1 表示联动接警中心 2。 ● 选择列表中的报警中心，单击“-”，可删除。
上报报警中心下标	

步骤4 单击“设置”，完成配置。

5.2.16 配置导入导出

您可以将控制器中已配置的信息（控制器 IP 地址除外）导出并保存，或者将已导出的配置信息导入至其他控制器中。

说明

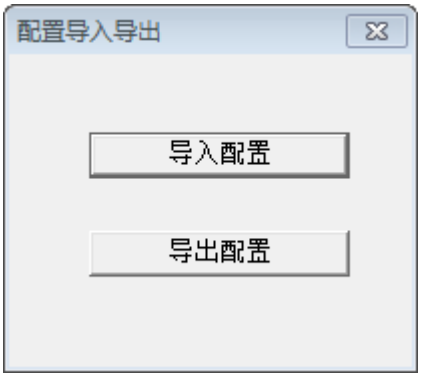
- 导出配置时，文件名请勿修改，默认为 config.tgz。
- 导入配置成功后，控制器会自动重启。

步骤1 在主界面“控制&查询”下拉列表框中选择“配置导入导出”。

步骤2 单击“控制&查询”。

系统显示“配置导入导出”界面，如图 5-21 所示。

图5-21 配置导入导出



- 导出配置
  单击“导出配置”，选择保存位置，进行保存。
- 导入配置
  单击“导入配置”，选择配置文件，进行导入。

5.2.17 恢复配置

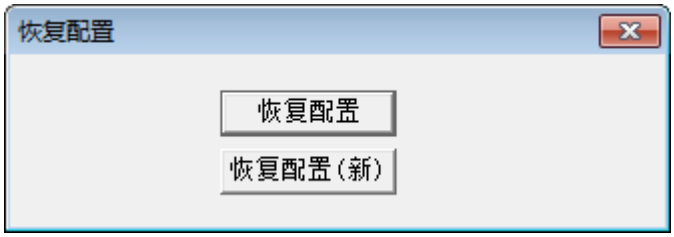
您可以对控制器执行恢复配置操作，使控制器恢复到出厂设置。

步骤1　在主界面“控制&查询”下拉列表框中选择“恢复配置”。

步骤2　单击“控制&查询”。

系统显示“恢复配置”界面，如图 5-22 所示。

图5-22 恢复配置



- 恢复配置
  单击“恢复配置”，提示“设置恢复配置成功!”，系统内除网络配置外的所有配置信息恢复为出厂默认状态。
- 恢复配置（新）
  单击“恢复配置（新）”，系统显示“恢复配置（新）”界面，如图 5-23 所示。选择需要恢复默认的参数，单击“确定”，将所选择的参数恢复为出厂默认状态。
  目前系统支持以下参数配置恢复默认。
  - ◇ Alarm：开关量防区配置。
  - ◇ AlarmOut：报警输出配置。
  - ◇ AlarmKeyboard：报警键盘配置。
  - ◇ PowerFault：电源故障配置。
  - ◇ BatteryLowPowerAlarm：蓄电池电压低配置。
  - ◇ ChassisIntrusion：防拆报警配置。
  - ◇ CommGlobal：全局布撤防配置。
  - ◇ PSTNAlarmServer：电话报警中心配置。

◇ AlarmSubSystem：子系统配置。

◇ PSTNBreakLine： PSTN 掉线报警配置

图5-23 恢复配置

5.2.18 修改密码

您可以根据需要修改系统密码。

步骤1 在主界面“控制&查询”下拉列表框中选择“修改密码”。

步骤2 单击“控制&查询”。

系统显示“密码修改”界面，如图 5-24 所示。

图5-24 修改密码

步骤3　输入“用户名”、“旧密码”、“新密码”和“确认”。

说明

密码建议设置为 8 位～32 位，可以由数字、字母和特殊字符（除“'”、“"”、“;”、“:”、“&”外）三种类型中的两种组成。

步骤4　单击“修改”，完成修改。

5.2.19 远程升级

5.2.19.1 控制器升级

您可以远程对控制器进行升级。

说明

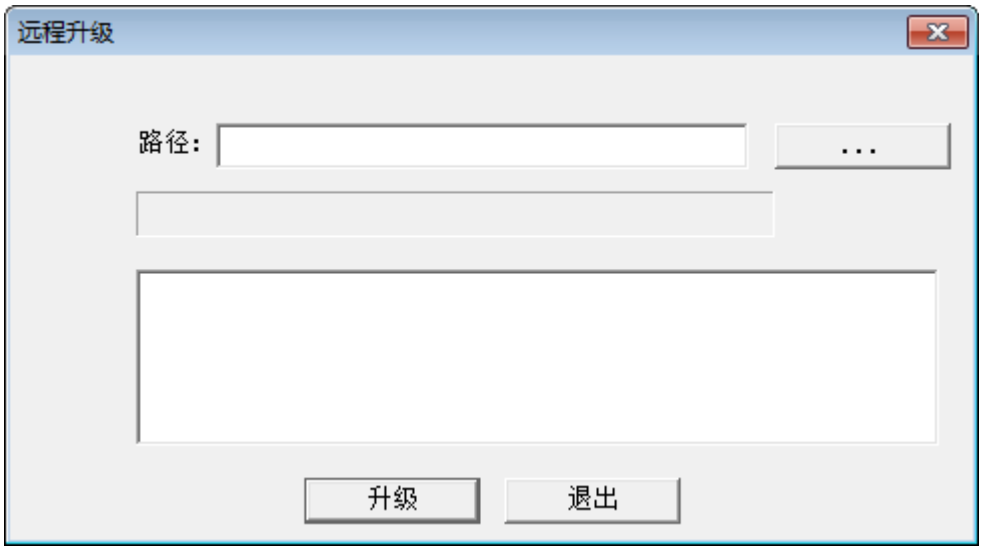
升级成功后时，控制器会自动重启，听到控制器蜂鸣，表示控制器重启完成；同时请通过“恢复配置”功能或者硬件初始化功能清除配置后再使用控制器。

步骤1　在主界面“控制&查询”下拉列表框中选择“远程升级”。

步骤2　单击“控制&查询”。

系统显示“远程升级”界面，如图 5-25 所示。

图5-25 远程升级



步骤3　单击 ...，选择升级文件。

步骤4　单击“升级”，开始对控制器或键盘进行远程升级。

说明

正常情况下，该过程大约需要 5～6 分钟，请耐心等待，中途不要断电。升级进度显示“升级成功”，表示升级完成。

5.2.19.2 键盘升级

您可以远程对键盘进行升级，具体升级步骤请参见“5.2.19.1 控制器升级”。

说明

升级成功后时，键盘会自动注册。

5.2.19.3 M-BUS 模块升级

您可以对 M-BUS 模块进行远程升级，具体升级步骤请参见“5.2.19.1 控制器升级”。

说明

升级成功后时，模块会自动重启。

5.2.20 重启控制器

您可以通过 SDK 客户端重启控制器。

步骤1　在主界面“控制&查询”下拉列表框中选择“重启设备”。

步骤2　单击“控制&查询”。

系统显示“重启”界面，如图 5-26 所示。

图5-26 重启设备

步骤3　单击“重启”，即可重新启动控制器。

5.3 控制器告警配置

5.3.1 机箱入侵报警配置

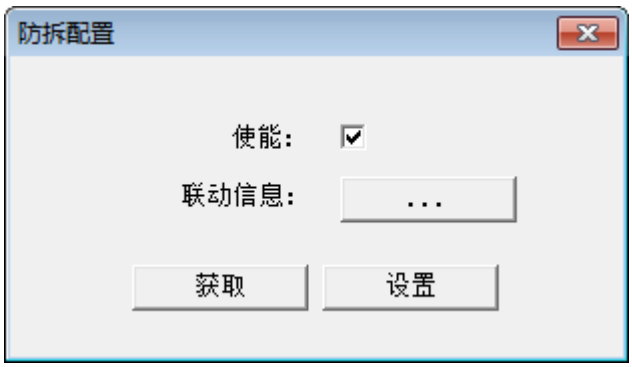
您可以对控制器进行机箱入侵报警配置，当机箱被入侵时会产生联动报警。

步骤1　在主界面“配置”下拉列表框中选择“机箱入侵报警（防拆配置）”。

步骤2　单击“配置”。

系统显示“防拆配置”界面，如图 5-27 所示。单击“获取”，可获取系统当前的配置信息。

图5-27 防拆配置



步骤3　选择“使能”，表示启用防拆报警。

步骤4　单击 ... 。

系统显示“联动参数”界面，具体的配置请参见“5.2.4 开关量防区配置”。

步骤5　配置完成后，单击“确定”进行保存，并返回到“防拆配置”界面。

步骤6　单击“设置”，保存配置。

说明

可以用“取消使能”、“防拆恢复”、或者“撤防”等操作来消除报警。

5.3.2 电源故障配置

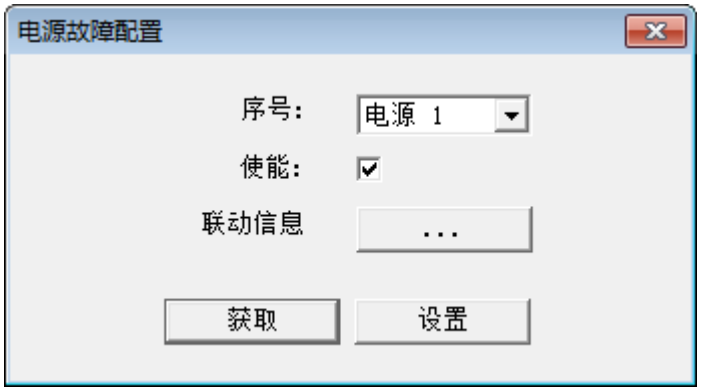
您可以对控制器进行电源故障配置，当电源发生故障时会产生联动报警。

步骤1　在主界面“配置”下拉列表框中选择“电源故障配置”。

步骤2　单击“配置”。

系统显示“电源故障配置”界面，如图 5-28 所示。单击“获取”，可获取系统当前的配置信息。

图5-28 电源故障配置



步骤3　选择电源序号，选择“使能”，表示该电源开启故障报警。

步骤4　单击 ... 。

系统显示“联动参数”界面，具体的配置请参见“5.2.4 开关量防区配置”。

步骤5　配置完成后，单击“确定”进行保存，并返回到“电源故障配置”界面。

步骤6　单击“设置”，保存配置。

说明

可以用“取消使能”、“故障恢复”、或者“撤防”等操作来消除报警。

5.3.3 蓄电池电压低配置

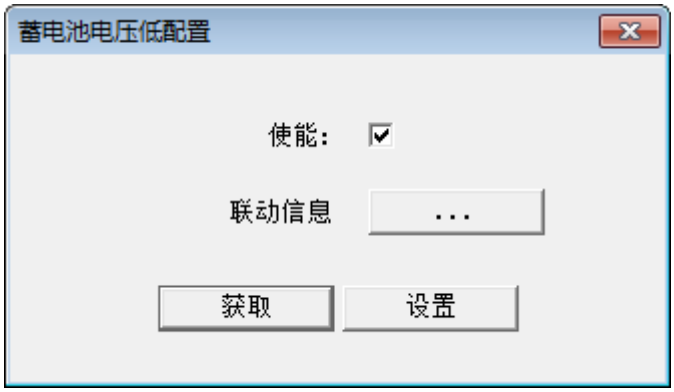
您可以对控制器进行蓄电池电压配置，当蓄电池电量小于 11.8V 时会产生蓄电池低压联动报警。

步骤1　在主界面“配置”下拉列表框中选择“蓄电池电压低配置”。

步骤2　单击“配置”。

系统显示“蓄电池电压低配置”界面，如图 5-29 所示。单击“获取”，可获取系统当前的配置信息。

图5-29 蓄电池电压低配置



步骤3　选择“使能”，表示开启蓄电池电压低报警。

步骤4　单击 

。

系统显示“联动参数”界面，具体的配置请参见“5.2.4 开关量防区配置”。

步骤5　配置完成后，单击“确定”进行保存，并返回到“蓄电池电压低配置”界面。

步骤6　单击“设置”，保存配置。

说明

可以用“取消使能”、“控制器主电恢复至蓄电池电压大于等于 11.8+0.5V”、或者“撤防”等操作来消除报警。

5.3.4 断网事件配置

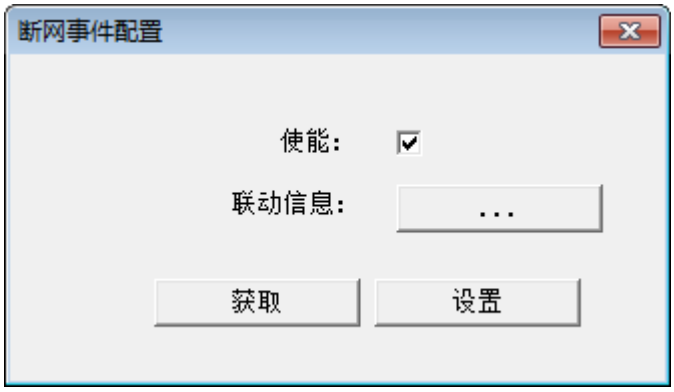
您可以对控制器进行断网事件配置，当发生断网情况时会产生联动报警。

步骤1　在主界面“配置”下拉列表框中选择“断网事件配置”。

步骤2　单击“配置”。

系统显示“断网事件配置”界面，如图 5-30 所示。单击“获取”，可获取系统当前的配置信息。

图5-30 断网事件配置



步骤3　选择“使能”，表示开启断网报警。

步骤4　单击 ... 。

系统显示“联动参数”界面，具体的配置请参见“5.2.4 开关量防区配置”。

步骤5　配置完成后，单击“确定”进行保存，并返回到“断网事件配置”界面。

步骤6　单击“设置”，保存配置。

说明

可以用“取消使能”、“断网事件恢复”、或者“撤防”等操作来消除报警。

5.3.5 IP 冲突事件配置

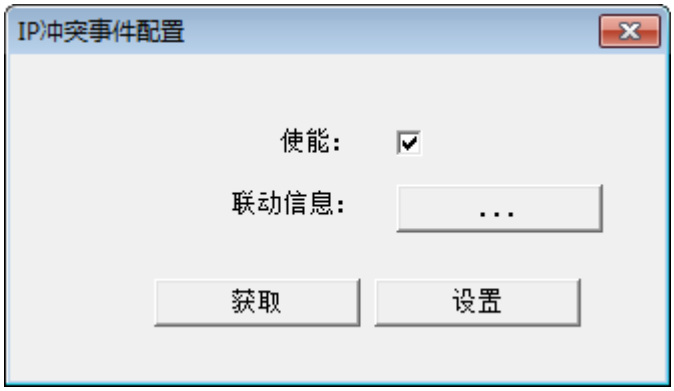
您可以对控制器进行 IP 冲突配置，当发生 IP 冲突时会产生联动报警。

步骤1　在主界面“配置”下拉列表框中选择“IP 冲突事件配置”。

步骤2　单击“配置”。

系统显示“IP 冲突事件配置”界面，如图 5-31 所示。单击“获取”，可获取系统当前的配置信息。

图5-31 IP 冲突事件配置



步骤3　选择“使能”，表示开启 IP 冲突报警。

步骤4　单击 ... 。

系统显示“联动参数”界面，具体的配置请参见“5.2.4 开关量防区配置”。

步骤5　配置完成后，单击“确定”进行保存，并返回到“IP 冲突事件配置”界面。

步骤6　单击“设置”，保存配置。

说明

可以用“取消使能”、“IP 冲突恢复”、或者“撤防”等操作来消除报警。

5.3.6 MAC 冲突事件配置

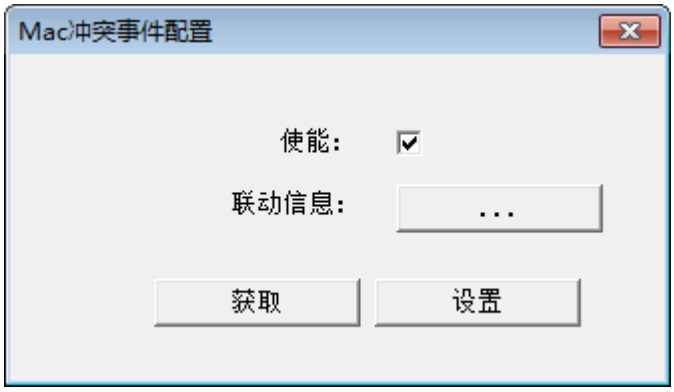
您可以对控制器进行 Mac 冲突事件配置，当发生 MAC 冲突时会产生联动报警。

步骤1　在主界面“配置”下拉列表框中选择“Mac 冲突事件配置”。

步骤2　单击“配置”。

系统显示“Mac 冲突事件配置”界面，如图 5-32 所示。单击“获取”，可获取系统当前的配置信息。

图5-32 Mac 冲突事件配置



步骤3　选择“使能”，表示开启 MAC 冲突报警。

步骤4　单击 

。

系统显示“联动参数”界面，具体的配置请参见“5.2.4 开关量防区配置”。

步骤5　配置完成后，单击“确定”进行保存，并返回到“Mac 冲突事件配置”界面。

步骤6　单击“设置”，保存配置。

说明

可以用“取消使能”、“MAC 冲突恢复”、或者“撤防”等操作来消除报警。

5.3.7 PSTN 掉线事件配置

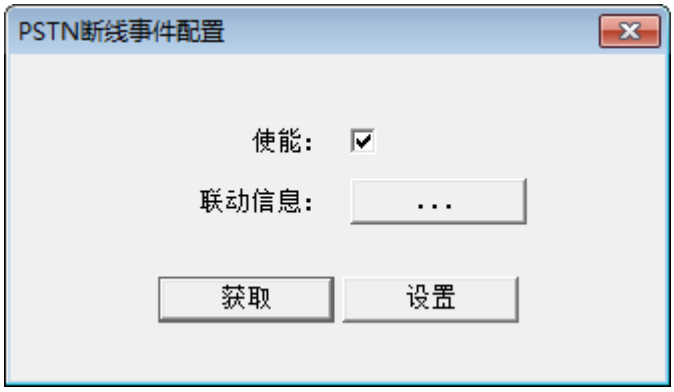
您可以对控制器进行 PSTN 掉线事件配置，当发生 PSTN 掉线时会产生联动报警。

步骤1　在主界面“配置”下拉列表框中选择“PSTN 掉线事件配置”。

步骤2　单击“配置”。

系统显示“PSTN 断线事件配置”界面，如图 5-33 所示。单击“获取”，可获取系统当前的配置信息。

图5-33 PSTN 掉线事件配置



步骤3　选择“使能”，表示启用 PSTN 掉线报警。

步骤4　单击 ... 。

系统显示“联动参数”界面，具体的配置请参见“5.2.4 开关量防区配置”。

步骤5　配置完成后，单击“确定”进行保存，并返回到“PSTN 掉线事件配置”界面。

步骤6　单击“设置”，保存配置。

说明

可以用“取消使能”、“接电话交换机的电话线恢复连接”、或者“撤防”等操作来消除报警。

5.3.8 紧急呼叫报警事件配置

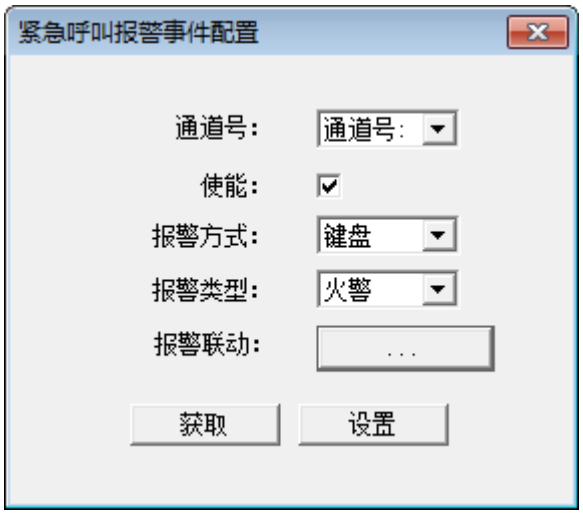
您可以对控制器进行紧急呼叫报警事件配置，当有紧急报警时会产生联动报警。

步骤1　在主界面“配置”下拉列表框中选择“紧急呼叫报警事件配置”。

步骤2　单击“配置”。

系统显示“紧急呼叫报警事件配置”界面，如图 5-34 所示。单击“获取”，可获取系统当前的配置信息。

图5-34 紧急呼叫报警事件配置



步骤3　选择“通道号”。

说明

- 选择“通道号”后，系统自动显示报警方式和报警类型，“报警方式”暂只支持键盘。

- 通道 1 对应火警，通道 2 对应胁迫报警，通道 3 对应匪警，通道 4 对应医疗紧急报警。

步骤4　选择“使能”，表示启用“紧急呼叫报警”。

步骤5　单击 ... 。

系统显示“联动参数”界面，具体的配置请参见“5.2.4 开关量防区配置”。

步骤6　配置完成后，单击“确定”进行保存，并返回到“紧急呼叫报警事件配置”界面。

步骤7　单击“设置”，保存配置。

说明

撤防可以进行消警。

5.4 布撤防

5.4.1 全局布撤防

您可以对所有防区进行全局布防和撤防。

步骤1　在主界面“控制&查询”下拉列表框中选择“布撤防控制”。

步骤2　单击“控制&查询”。

系统显示“布撤防”界面，如图 5-35 所示。

图5-35 布撤防

步骤3　选择布撤防模式和情景模式，并输入密码。

说明

- 布撤防模式选择“布防”或者“撤防”。
- 情景模式选择“在家”或者“外出”，如果选择“未知”，布防时会提示失败。

步骤4　单击“设置”，完成布撤防。

当有防区报警输入时，单击“设置”，控制器会布防失败。此时可以单击“有报警源输入的防区”的 ... ，查看当前异常防区。可以手动将异常防区旁路，使控制器成

功布防。旁路操作请具体参见“5.4.4 旁路控制”。

说明

如果出现布防失败，请确认检查以下几个方面。

- 防区是否有报警输入，如果有请执行撤防操作，清除各防区的报警激活状态，对一直有报警输入的防区进行旁路或者隔离即可。
- 串联或并联的 2.2kΩ线尾电阻是否连接正确，具体请参见“3.4.2 本地报警输入接线”。
- 探测器与主机之间的接线是否有松动，如果有重新接线。
- 如果上述检查后还是布防失败，请用 2.2kΩ线尾电阻与防区并联，开启 SDK 客户端的订阅界面，如果没有防区源事件，表示防区正常；如果有防区源开始事件，表示防区异常，需要维修。

5.4.2 单防区布撤防

您可以对单个防区进行布防和撤防。

注意

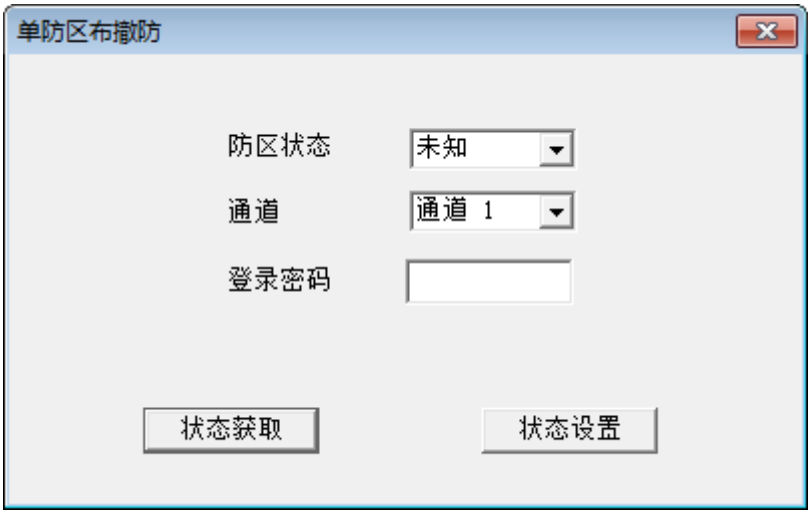
只有开启单防区/子系统布撤防使能后，才可以对某个防区进行布撤防操作，开启使能步骤请参见“5.2.5 单防区/子系统布撤防使能配置”。

步骤1　在主界面“控制&查询”下拉列表框中选择“单防区布撤防控制”。

步骤2　单击“控制&查询”。

系统显示“单防区布撤防”界面，如图 5-36 所示。选择“通道号”，单击“状态获取”，可查看该防区的布撤防状态。

图5-36 单防区布撤防



步骤3　选择“通道”和“防区状态”，并输入“登录密码”。

防区状态即布撤防模式，包括布防和撤防。

步骤4　单击“状态设置”，完成布撤防。

说明

如果出现布防失败，请确认检查以下几个方面。

- 防区是否有报警输入，如果有请执行撤防操作，清除各防区的报警激活状态，对一直有报警输入的防区进行旁路或者隔离即可。
- 串联或并联的 2.2kΩ线尾电阻是否连接正确，具体请参见“3.4.2 本地报警输入接线”。

- 探测器与主机之间的接线是否有松动，如果有重新接线。
- 如果上述检查后还是布防失败，请用 2.2kΩ线尾电阻与防区并联，开启 SDK 客户端的订阅界面，如果没有防区源事件，表示防区正常；如果有防区源开始事件，表示防区异常，需要维修。

5.4.3 子系统布撤防

您可以对子系统进行布防和撤防。

注意

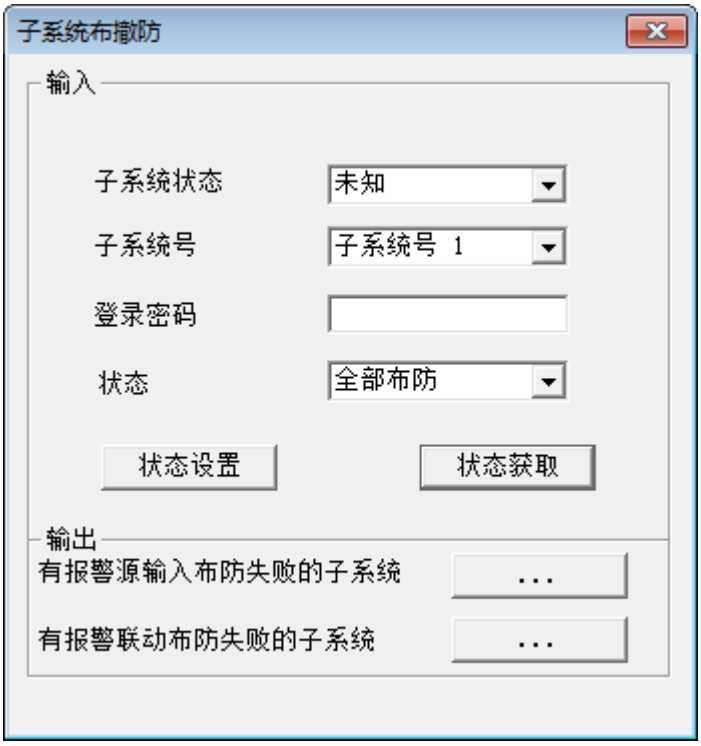
只有开启了单防区/子系统布撤防使能，且已配置了子系统。使能请参见“5.2.5 单防区/子系统布撤防使能配置”，配置请参见“5.2.6 报警子系统配置”。

步骤1　在主界面“控制&查询”下拉列表框中选择“子系统布撤防控制”。

步骤2　单击“控制&查询”。

系统显示“子系统布撤防”界面，如图 5-37 所示。选择“子系统号”，单击“状态获取”，可查看子系统的布撤防状态。

图5-37 子系统布撤防



步骤3　选择“子系统号”和“子系统状态”，并输入“登录密码”。

子系统状态即子系统布撤防模式，包括布防和撤防。

步骤4　单击“状态设置”，完成布撤防。

当有防区输入时，单击“状态设置”，控制器会布防失败。此时可以单击“有报警源输入布防失败的防区”的 ...，查看当前异常防区。可以手动将异常防区旁路，使控制器成功布防。旁路操作请具体参见“5.4.4 旁路控制”。

说明

如果出现布防失败，请确认检查以下几个方面。

- 防区是否有报警输入，如果有请执行撤防操作，清除各防区的报警激活状态，对一直有报警输入的防区进行旁路或者隔离即可。
- 串联或并联的 2.2kΩ线尾电阻是否连接正确，具体请参见“3.4.2 本地报警输入接线”。
- 探测器与主机之间的接线是否有松动，如果有重新接线。
- 如果上述检查后还是布防失败，请用 2.2kΩ线尾电阻与防区并联，开启 SDK 客户端的订阅界面，如果没有防区源事件，表示防区正常；如果有防区源开始事件，表示防区异常，需要维修。

5.4.4 旁路控制

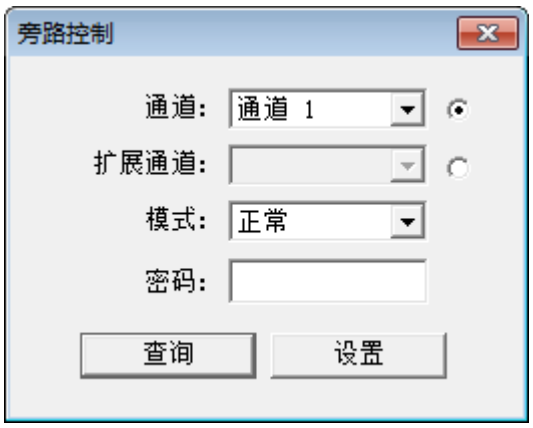
您可以在控制器处于布防状态时进行旁路操作，旁路的防区仍然会对外部探测器进行监听并做记录，但不会转发给用户。在控制器撤防后，防区将恢复为非旁路状态。

步骤1　在主界面“控制&查询”下拉列表框中选择“旁路”。

步骤2　单击“控制&查询”。

系统显示“旁路控制”界面，如图 5-38 所示。选择“通道号”，单击“查询”，可查看该防区的旁路状态。

图5-38 旁路控制



步骤3　单击单选框，激活“通道”。

步骤4　选择“通道号”和“模式”，输入“密码”。

说明

- 正常：该防区在布防状态下可以正常报警。
- 旁路：该防区在此次布防时被屏蔽，当控制器撤防时，防区将恢复为正常状态。
- 隔离：该防区被停用，在控制器撤防再布防时，该隔离的防区仍为停用。

步骤5　单击“设置”。

说明

如果防区被触发，则修改旁路状态后，在下一次报警产生时生效。

5.5 状态查询

5.5.1 蓄电池查询

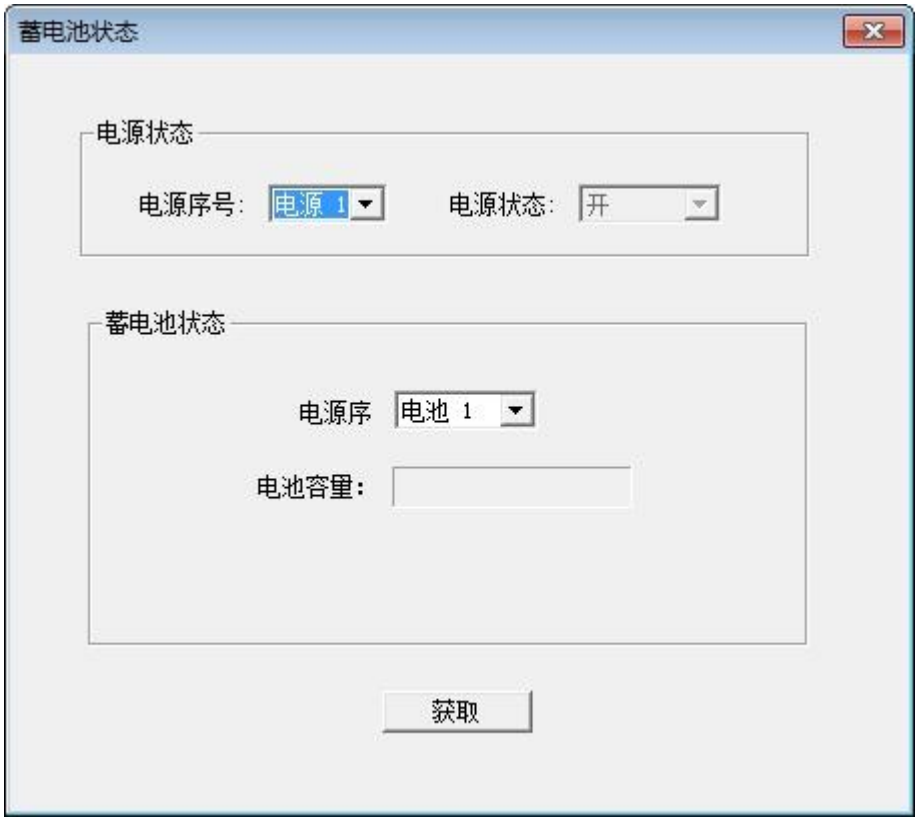
您可以查询蓄电池的电源和电池状态。

步骤1　在主界面“控制&查询”下拉列表框中选择“电源电池”。

步骤2　单击“控制&查询”。

系统显示“蓄电池状态”界面，如图 5-39 所示。

图5-39 蓄电池查询



步骤3　单击“获取”即可查询。

说明

- 电源序号：电源 1 代表主电源（AC 220V）。
- 电源状态：“开”代表主电源正常，“关”代表主电源掉电，相应产生主电掉电报警事件。
- 电池序号：电池 1 代表备用电池。
- 电池容量状态条：指示电池当前容量，当电池电压小于 11.8V，状态条为 0，产生欠压报警事件。

5.5.2 获取报警通道状态

您可以根据需要查询各报警通道的状态。

步骤1　在主界面“控制&查询”下拉列表框中选择“通道状态”。

步骤2　单击“控制&查询”。

系统显示“通道状态获取”界面，如图 5-40 所示。

图5-40 通道状态

步骤3　选择“查询类型”，并填写相应查询通道数量，单击“获取状态”，获取各个通道及状态。

说明

- 报警输入通道：对应报警源，“状态”选中代表有防区异常。
- 报警输出通道：对应报警输出通道，选中代表该通道有输出，常开情况下，选中代表继电器闭合。
- 警号通道：对应警号，选中代表警号在输出。
- 本主机不支持扩展模块报警输入和扩展模块报警输出查询。
- 如果状态查询失败，请检查“需要查询个数”是否设置正确。

5.5.3 获取激活防区状态

您可以根据需要查询各防区是否激活。

步骤1　在主界面“控制&查询”下拉列表框中选取“获取激活防区”。

步骤2　单击“控制&查询”。

系统显示“激活防区”界面，如图 5-41 所示。

图5-41 激活防区

步骤3　填写报警输入查询个数，单击“获取”。

报警输入激活防区表会显示相应激活防区通道号和激活时间，您可以根据该激活防区信息进行相应的消警操作。

5.5.4 获取扩展模块状态

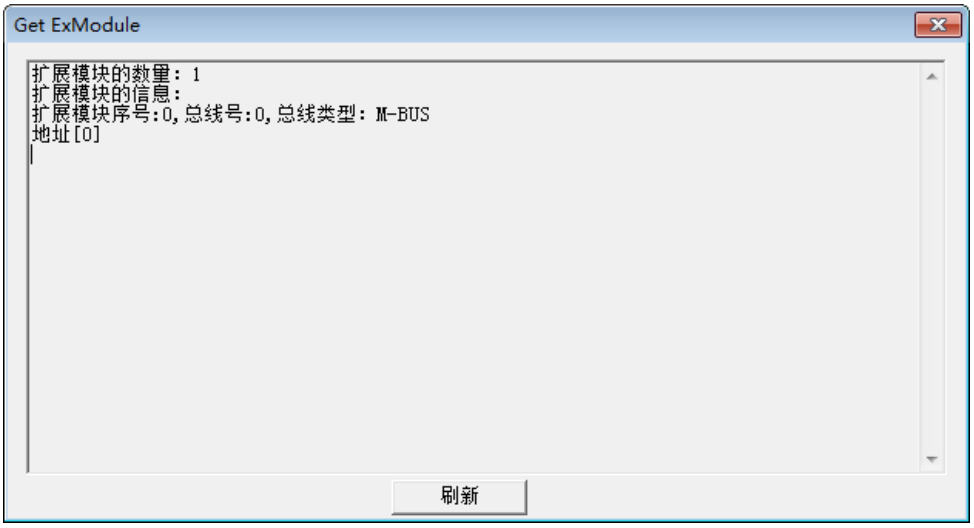
您可以根据需要获取控制器接入的扩展模块状态信息。

步骤1　在主界面“控制&查询”下拉列表框中选取“获取扩展模块状态”。

步骤2　单击“控制&查询”。

系统显示“获取扩展模块状态”界面，如图 5-42 所示。

图5-42 扩展模块状态



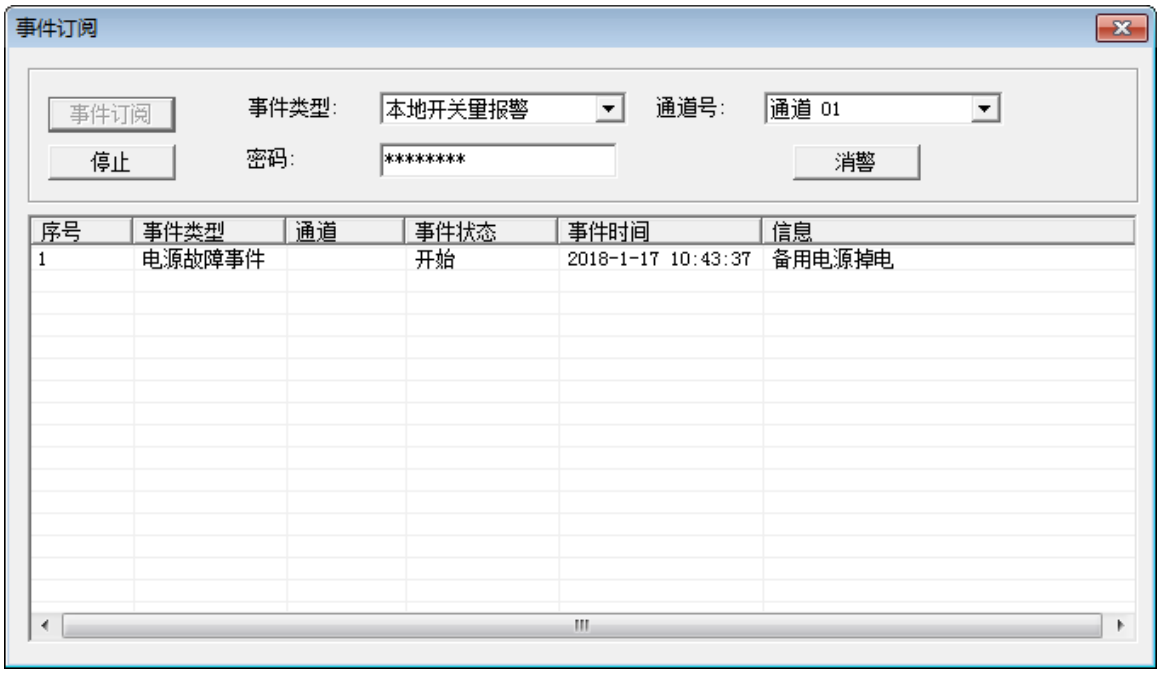
5.6 设备管理

5.6.1 报警信息订阅

您可以根据需要订阅报警事件以及对报警通道进行消警处理。

在主界面单击“报警订阅”，如图 5-43 所示。

图5-43 订阅报警



订阅报警

单击“事件订阅”，控制器会将当前处于报警或异常的事件逐一上报。

说明

- 订阅后，如果“报警输入”有触发。在触发开始，控制器会主动上报对应通道和时间的 Start 事件，在触发结束后，控制器会再次主动上报该通道当前时间的 Stop 事件。
- 电源故障或防拆开关触发，均会上报对应事件。

消除报警

选择需要消警的“通道号”和“事件类型”，输入登录密码，单击“消警”，可对该通道的此类事件进行消警处理。

说明

- 仅支持本地开关量报警消除。
- 消警对报警源触发并联动输出后进行复核，消警操作后，控制器关闭对应报警源的联动输出。

5.6.2 日志管理

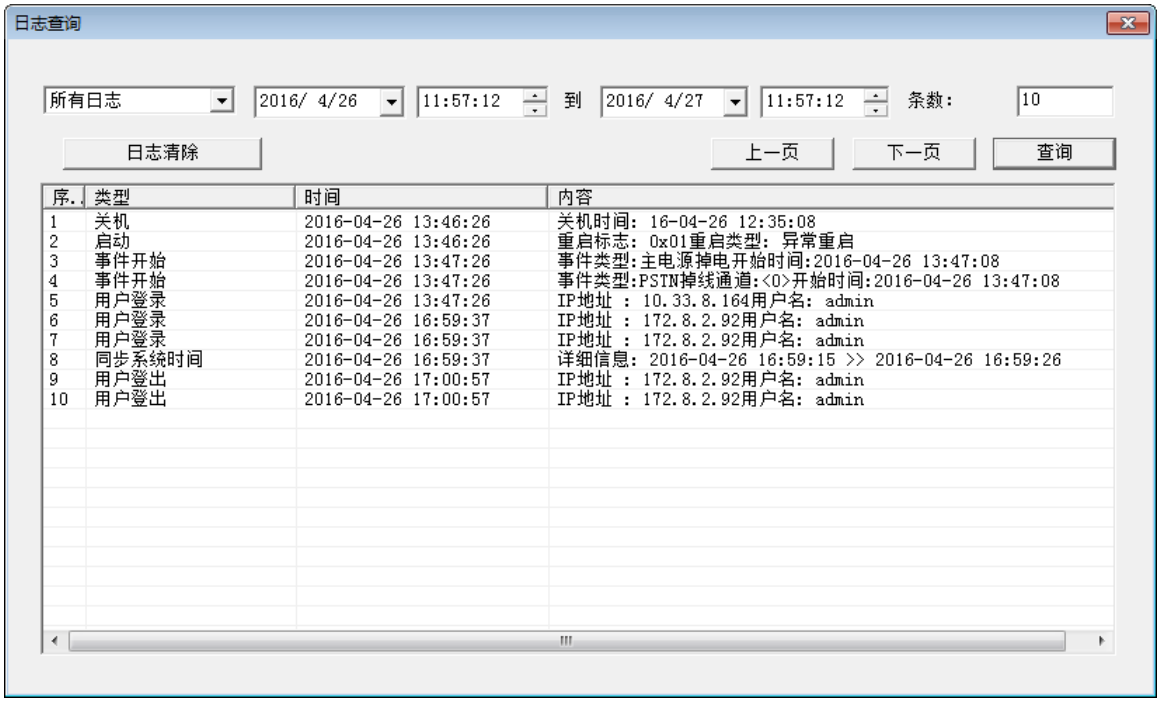
您可以通过日志管理，来查看日志信息。

步骤1　在主界面“控制&查询”下拉列表框中选取“日志管理”。

步骤2　单击“控制&查询”。

系统显示“日志查询”界面，如图 5-44 所示。

图5-44 日志查询



步骤3　选择日志类型、时间和条数，开始查询日志信息。

说明

- 系统支持最多可查询 100 条日志，若条数较多，查询时间也较长，例如查询 100 条日志大约需要 15s。
- 日志不支持清除。

5.6.3 设备能力查看

在主界面单击“设备能力”，如图 5-45 所示，您可以在此界面中查看报警控制器处理报警输入/输出以及相关功能的能力。

图5-45 设备能力

5.6.4 版本信息查看

您可以在版本信息界面中查看控制器和 M-BUS 主模块的版本信息。

步骤1　在主界面“控制&查询”下拉列表框中选取“版本信息”。

步骤2　单击“控制&查询”。

系统显示“版本信息”界面，如图 5-46 所示。

图5-46 版本信息


版本信息
序列号：2D01DFFYAQ00012
软件版本：2.616.0001.5
软件生成日期：2017-11-20
单片机序号
1
软件版本
2017-10-27 V1.2
刷新

6 LCD 报警键盘操作说明

6.1 型号选择和 485 地址设置

注意

设备支持热插拔功能。在报警主机正常运行情况下，将键盘的线缆接入报警主机的对应端子，通讯指示灯闪烁即可正常使用。

当报警键盘首次接入报警主机时，需要选择操作语言及报警主机的型号，方可注册到该报警主机并进入相应的操作界面。

具体启动步骤如下所示。

步骤1　将连接线的一端接入键盘的线缆接口。

步骤2　按住ENTER键，同时将连接线另一端的两对接线端子分别插入报警主机的键盘接口和供电接口，键盘界面点亮并显示操作语言选项（中文和 English）。

步骤3　通过  或  键，选择适合的语言，按ENTER键。

步骤4　通过  或  键，选择“6-485 Addr”，按ENTER键，输入键盘地址，再按ENTER键。

返回到型号选择与地址设置界面。

说明

- 485 地址以十进制形式呈现，范围为 00～15。
- 多台键盘连接时 485 地址不能重复。

步骤5　通过  或  键，选择对应的产品型号，按ENTER键，键盘发出“滴”一声，显示主界面且通讯指示灯绿灯常亮，表示自动注册成功，键盘与报警主机可以进行正常通讯。

说明

若报警主机型号选择错误，则注册失败，通讯指示灯红灯常亮。

6.2 操作前必看说明

6.2.1 前面板按键说明

图6-1 前面板

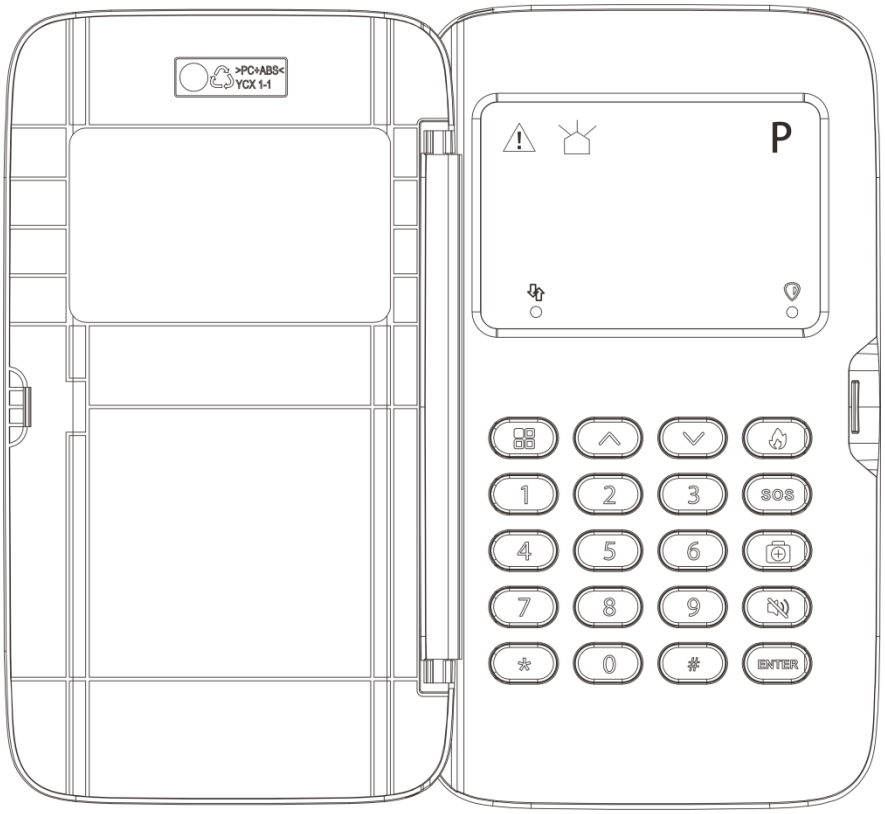
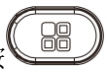


表6-1 前面板说明

按键或图标	名称	说明
	通讯指示灯	● 绿色常亮：键盘成功注册到报警主机 ● 红色常亮：键盘未注册到报警主机
	布撤防指示灯	● 绿色常亮：处于布防状态 ● 红色常亮：处于撤防状态
	故障图标	显示该图标，表示设备有异常故障，您可以在全局模式下，长按  3s，查询设备故障状态
	报警图标	显示该图标，表示设备有报警，您可以在全局模式下，长按  3s，查询当前设备的报警情况
P	部分布防图标	显示该图标，表示设备存在部分布防，您可以在全局模式下，长按  3s，查询当前已经布防的子系统编号
	菜单键	● 进入主菜单界面 ● 返回上一级菜单 ● 短按此键，清除上一个输入的编码

按键或图标	名称	说明
		● 全局模式下，长按此键 3s，显示各模块的状态，复选框显示为黑，表示该模块故障；复选框显示为白时，代表该模块正常，如图 6-2 所示
^	上翻页键	● 在菜单中，按此键可向上翻阅 ● 全局模式下，长按此键 3s，显示所有防区的旁路状态，防区后的复选框显示为黑，表示该防区旁路或者隔离
v	下翻页键	● 在菜单中，按此键可向下翻阅 ● 全局模式下，长按此键 3s，显示所有的告警防区，防区后的复选框显示为黑，表示该防区有告警
0～9	数字符号键	● 输入数字（0～9） ● 任何模式下，【1】 + ENTER，查询当前模式
*	*号键	● 符号键（*） ● 全局模式下，长按此键 3s，查询当前已经布防的子系统编号，显示所有子系统的布撤防状态，防区后的复选框显示为黑，表示该子系统处于布防状态
#	#号键	符号键（#）
火	火警键	长按此键 3s，蜂鸣器开始报警，设备向报警控制器发送火警信息 **说明** 任何模式下都可操作。
SOS	匪警键	长按此键 3s，蜂鸣器开始报警，设备向报警控制器机发送匪警信息 **说明** 任何模式下都可操作。
+	医疗键	长按此键 3s，蜂鸣器开始报警，设备向报警主机发送医疗报警信息 **说明** 任何模式下都可操作。
无声	无声紧急报警键	长按此键 3s，设备向报警主机发送无声紧急报警信息 **说明** 任何模式下都可操作。
ENTER	确认键	● 确认设置按键 ● 全局模式下，长按此键 3s，显示所有防区异常状态，防区后的复选框显示为黑，表示该该防区异常

图6-2 报警主机状态

主电□	电池□	防拆□
网络□	电话□	2G■

6.2.2 操作模式及功能说明

进入操作模式后，直接输入编码指令进行操作。操作模式分为全局模式、单一子系统模式、编程

模式、查询模式和步测模式，五种模式不可同时登录，默认为全局模式。当在其他四种模式下 5 分钟内没有任何操作或者退出操作时，系统自动返回全局模式。每个模式下可操作的功能介绍如图 6-3 所示。

图6-3 模式及功能介绍

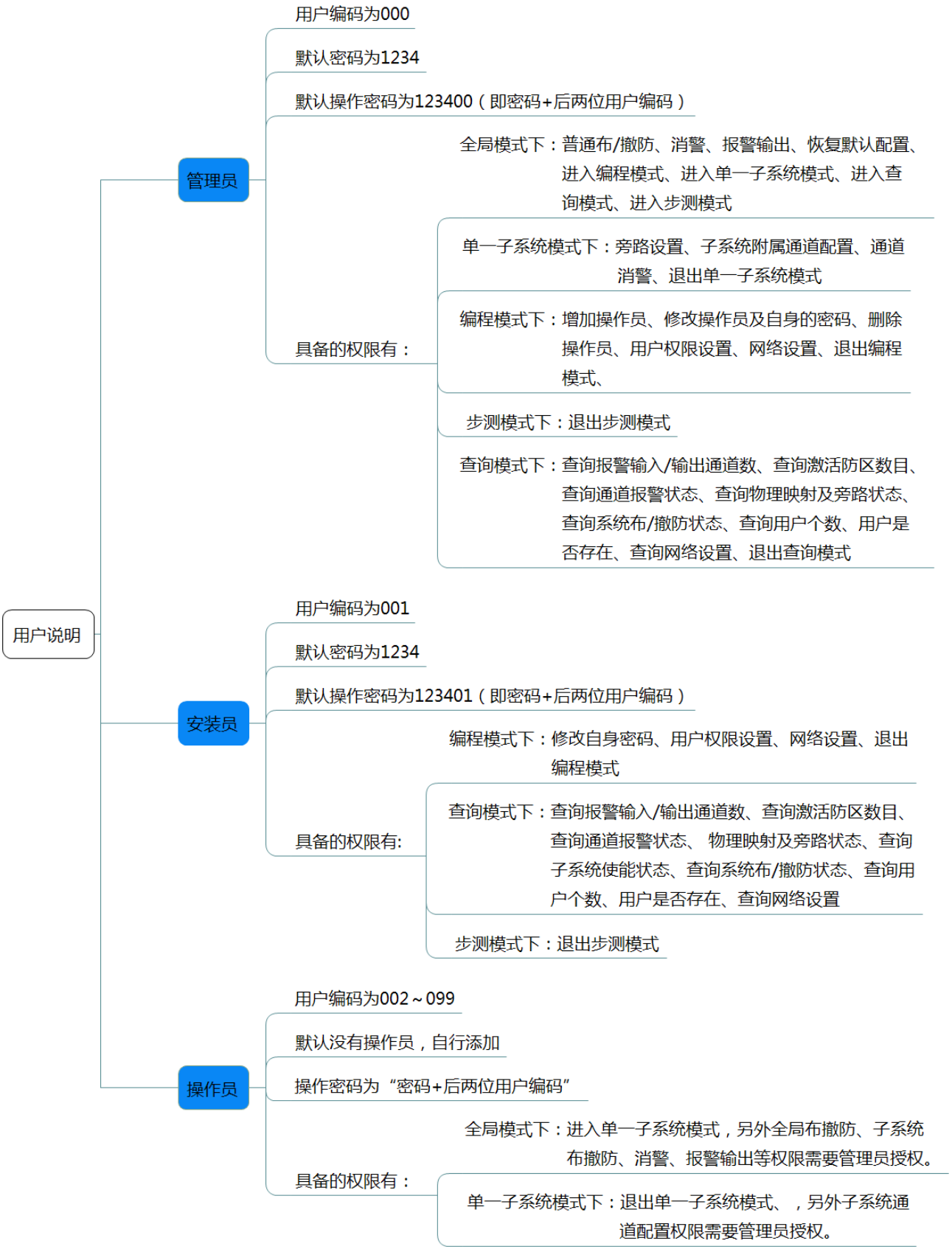
6.2.3 用户权限及密码说明

用户类型分为管理员、安装员和操作员，不同用户的用户编码、默认密码、操作密码、具备的权限都不同，具体如图 6-4 所示。

注意

- 用户操作密码由“用户密码+用户编号”组成。例如：02 用户的密码是 2345，那么 02 用户的操作密码为 234502。
- 胁迫密码由“用户密码尾数加 1（遇 10 为 0）+用户编号”，只要输入的操作密码为胁迫密码，即可产生胁迫事件。例如：03 用户的密码是 5678，那么 03 用户的胁迫密码为 567903，输入该胁迫密码，即会产生胁迫事件。
- 操作员权限授权操作请参见“6.4.4 设置权限”。

图6-4 操作用户介绍


用户说明
管理员
用户编码为000
默认密码为1234
默认操作密码为123400（即密码+后两位用户编码）
具备的权限有：
全局模式下：普通布/撤防、消警、报警输出、恢复默认配置、进入编程模式、进入单一子系统模式、进入查询模式、进入步测模式
单一子系统模式下：旁路设置、子系统附属通道配置、通道消警、退出单一子系统模式
编程模式下：增加操作员、修改操作员及自身的密码、删除操作员、用户权限设置、网络设置、退出编程模式、
步测模式下：退出步测模式
查询模式下：查询报警输入/输出通道数、查询激活防区数目、查询通道报警状态、查询物理映射及旁路状态、查询系统布/撤防状态、查询用户个数、用户是否存在、查询网络设置、退出查询模式
安装员
用户编码为001
默认密码为1234
默认操作密码为123401（即密码+后两位用户编码）
具备的权限有:
编程模式下：修改自身密码、用户权限设置、网络设置、退出编程模式
查询模式下：查询报警输入/输出通道数、查询激活防区数目、查询通道报警状态、 物理映射及旁路状态、查询子系统使能状态、查询系统布/撤防状态、查询用户个数、用户是否存在、查询网络设置
步测模式下：退出步测模式
操作员
用户编码为002～099
默认没有操作员，自行添加
操作密码为“密码+后两位用户编码”
具备的权限有：
全局模式下：进入单一子系统模式，另外全局布撤防、子系统布撤防、消警、报警输出等权限需要管理员授权。
单一子系统模式下：退出单一子系统模式、 ，另外子系统通道配置权限需要管理员授权。

6.3 全局模式

6.3.1 全局布/撤防

6.3.1.1 布防

功能说明

当报警主机和探测器均正常工作时，对防区进行全局布防后，报警主机将对防区内的报警信号做出响应。

授权用户

管理员或者带布撤防权限的操作员

编码指令

［管理员操作密码/带布撤防权限的操作员操作密码］ + 【*】 + 【00】

举例

管理员（操作密码为 123400）实现全局布防。

步骤1　在全局模式下，输入编码指令为 123400*00。

步骤2　按【确认键】。

6.3.1.2 撤防

功能说明

当有防区处于布防状态时，使防区退出布防状态。

授权用户

管理员或者带布撤防权限的操作员

编码指令

［管理员操作密码/带布撤防权限的操作员操作密码］ + 【*】 + 【01】

举例

管理员（操作密码为 123400）实现全局撤防。

步骤1　在全局模式下，输入编码指令为 123400*01。

步骤2　按【确认键】。

6.3.2 子系统布/撤防

6.3.2.1 布防

功能说明

当报警主机和探测器均正常工作时，对子系统内的防区进行布防后，报警主机将对防区内的报警信号做出响应。

注意

只有开启子系统布撤防使能后，才可以对子系统进行布撤防操作，开启使能步骤请参见配套的报警主机说明书。

授权用户

管理员或者带布撤防权限的操作员

编码指令

［管理员操作密码/带布撤防权限的操作员操作密码］ + ［2 位子系统号］ + 【**】 + 【0】

说明

2 位子系统号为 01～64。

举例

管理员（操作密码为 123400）对子系统 01 实现布防。

步骤1　在全局模式下，输入编码指令为 12340001**0。

步骤2　按【确认键】。

6.3.2.2 撤防

功能说明

当子系统内有防区处于布防状态时，使子系统内的防区退出布防状态。

授权用户

管理员或者带布撤防权限的操作员

编码指令

［管理员操作密码/带布撤防权限的操作员操作密码］ + ［2 位子系统号］ + 【**】 + 【1】

说明

2 位子系统号为 01～64。

举例

管理员（操作密码为 123400）对子系统 01 实现撤防。

步骤1　在全局模式下，输入编码指令为 12340001**1。

步骤2　按【确认键】。

6.3.3 单防区布撤防

6.3.3.1 布防

功能说明

当报警主机和探测器均正常工作时，对某个防区单独布防后，报警主机将对防区内的报警信号做出响应。

注意

只有开启单防区/子系统布撤防使能后，才可以对某个防区进行布撤防操作，开启使能步骤请参见

配套的报警主机说明书。

授权用户

管理员或者带布撤防权限的操作员

编码指令

［管理员操作密码/带布撤防权限的操作员操作密码］ + ［3 位防区号］ + 【**】 + 【2】

说明

3 位防区号为 001～256。

举例

管理员（操作密码为 123400）对防区 1 实现布防。

步骤1　在全局模式下，输入编码指令为 123400001**2。

步骤2　按【确认键】。

6.3.3.2 撤防

功能说明

当某个防区处于布防状态时，单独使该防区退出布防状态。

授权用户

管理员或者带布撤防权限的操作员

编码指令

［管理员操作密码/带布撤防权限的操作员操作密码］ + ［3 位防区号］ + 【**】 + 【3】

说明

3 位防区号为 001～256。

举例

管理员（操作密码为 123400）对防区 1 实现撤防。

步骤1　在全局模式下，输入编码指令为 12340001**3。

步骤2　按【确认键】。

6.3.4 消警

功能说明

当报警被触发后，通过键盘消除报警。

授权用户

管理员或者带消警权限的操作员

编码指令

［管理员操作密码/带消警权限的操作员操作密码］ + 【*】 + 【1】

举例

管理员（操作密码为 123400）实现消警。

步骤1　在全局模式下，输入编码指令为 123400*1。

步骤2　按【确认键】。

6.3.5 设置报警输出

功能说明

报警输出模式分为自动报警、强制报警和关闭报警三种。强制报警产生的报警输出，可以通过设置自动报警和关闭报警来关闭。

授权用户

管理员或者带报警输出设置权限的操作员

编码指令

［管理员操作密码/带报警输出设置权限的操作员操作密码］ + 【*】 + 【2】+【n1】+【n2】

说明

- n1 表示输出通道号，范围为 001～064。
- n2 表示模式：0-自动报警、1-强制报警、2-关闭。

举例

管理员（操作密码为 123400）对输出通道 1 打开强制报警功能。

步骤1　在全局模式下，输入编码指令为 123400*20011。

步骤2　按【确认键】。

6.3.6 恢复默认配置

功能说明

恢复默认配置包括报警、报警输出、报警子系统、键盘、布撤防、主电掉电、欠压、防拆、电话报警中心、PSTN 掉线、子系统状态、断网、IP 冲突、Mac 冲突、紧急报警等参数的恢复。

授权用户

管理员

编码指令

［管理员操作密码］ + 【*】 + 【3】

举例

管理员（操作密码为 123400）恢复默认配置。

步骤3　在全局模式下，输入编码指令为 123400*3。

步骤4　按【确认键】。

6.3.7 设置 PSTN 测试

6.3.7.1 手动测试

功能说明

输入测试命令后，直接呼叫电话接警中心。

授权用户

安装员或者管理员

编码指令

［安装员操作密码/管理员操作密码］ + 【*】 + 【8】

举例

管理员（操作密码为 123400）手动测试 PSTN。

步骤1　在全局模式下，输入编码指令为 123400*8。

步骤2　按【确认键】。

6.3.7.2 开启定时测试

功能说明

输入测试命令后，开启定时测试功能。

注意

开启前需要在报警主机端配置测试计划，具体请参见相关的报警主机说明书。

授权用户

安装员或者管理员

编码指令

［安装员操作密码/管理员操作密码］ + 【*】 + 【9】

举例

管理员（操作密码为 123400）开启自动测试 PSTN。

步骤1　在全局模式下，输入编码指令为 123400*9。

步骤2　按【确认键】。

6.3.7.3 关闭定时测试

功能说明

输入测试命令后，关闭定时测试功能。

授权用户

安装员或者管理员

编码指令

［安装员操作密码/管理员操作密码］ + 【*】 + 【10】

举例

管理员（操作密码为 123400）关闭自动测试 PSTN。

步骤1　在全局模式下，输入编码指令为 123400*10。

步骤2　按【确认键】。

6.4 编程模式

在编程模式下，您可以进行用户管理和网络设置。

6.4.1 进入编程模式

功能说明

进入编程模式后，可以实现用户管理、报警主机网络设置和清除 CID 缓存功能。

授权用户

安装员或者管理员

编码指令

［安装员操作密码/管理员操作密码］ + 【*】 + 【4】

举例

管理员（操作密码为 123400）进入编码模式。

步骤1　在全局模式下，输入编码指令为 123400*4。

步骤2　按【确认键】。

屏幕显示：进入编程模式。

6.4.2 增加用户/修改密码

功能说明

增加新的操作员，或者修改用户密码。

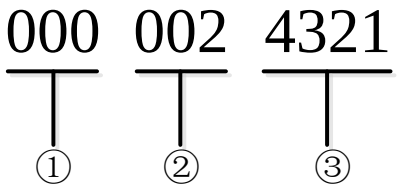
授权用户

安装员或者管理员

说明

- 仅管理员可以增加操作员。
- 管理员不可以修改安装员密码。
- 安装员用户只能修改自身密码。

编码指令



序号	说明
①	编码地址，表示此操作是增加用户或修改用户密码，默认为 000
②	用户编号，共支持 100 个用户。000 代表管理员，001 代表安装员，002～099 代表操作员
③	用户密码，密码长度为 4 位数字

举例

管理员（操作密码为 123400）增加新的操作员 002，用户密码为 4321。

步骤1　管理员在编码模式下，输入编码指令为 0000024321。

步骤2　按【确认键】。

6.4.3 删除用户

功能说明

删除操作员。

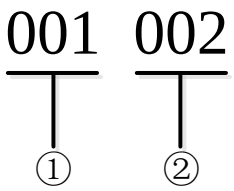
授权用户

管理员

说明

- 只有管理员才能删除操作员。
- 管理员和安装员不能被删除。

编码指令



序号	说明
①	编码地址，表示此操作是删除用户，默认为 001
②	操作员编号，范围为 002～099

举例

管理员（操作密码为 123400）删除操作员 002。

步骤1　管理员在编码模式下，输入编码指令为 001002。

步骤2　按【确认键】。

6.4.4 设置权限

功能说明

给操作员分配操作权限。

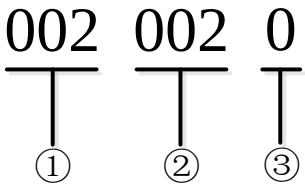
说明

管理员拥有所有权限，安装员仅具备编程和查询权限。

授权用户

管理员或安装员

编码指令



序号	说明
①	编码地址，表示此操作是设置用户权限，默认为 002
②	操作员编号，范围为 002～099

序号	说明
③	权限编码，共有 8 类权限

权限编码	权限内容	权限编码	权限内容
0	表示具备子系统布撤防权限	01～64	设置子系统附属通道，如：01 代表具备在子系统 1 添加或删除通道的权限
（*+01）～（*+64）	子系统布撤防，如：*+01 代表具备子系统 1 的布撤防权限	129	表示具备全局模式下的消警权限
130	表示具备全局模式下的报警输出设置权限		

举例

管理员（操作密码为 123400）给操作员 002 增加布撤防权限。

步骤1　管理员在编码模式下，输入编码指令为 0020020。

步骤2　按【确认键】。

6.4.5 设置主机网络

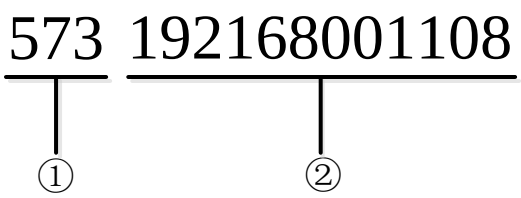
功能说明

设置报警主机的 IP 地址、子网掩码、网关和端口号。

授权用户

管理员或安装员

编码指令



序号	说明
①	编码地址，573－IP 地址，574－端口号，575－子网掩码，576－网关
②	● IP 地址、子网掩码和网关的地址编码，由四个单元组成，每单元采用三位设置方式，不足三位的补零 ● 端口号，范围为 1025～65535，默认为 37777

举例

管理员（操作密码为 123400）设置报警主机的 IP 地址为 192.168.1.108。

步骤1　管理员在编码模式下，输入编码指令为 573192168001108。

步骤2　按【确认键】。

6.4.6 清除 CID 缓存

功能说明

清除 CID 缓存。

授权用户

管理员或安装员

编码指令

600

举例

管理员（操作密码为 123400）清除 CID 缓存。

步骤1　管理员在编码模式下，输入编码指令为 600。

步骤2　按【确认键】。

6.4.7 退出编程模式

功能说明

退出编程模式。

说明

- 如果 5 分钟内没有任何操作，系统会自动退出编程模式并进入全局模式。
- 若要换成其他模式前，必须先退出编程模式。

授权用户

管理员或安装员

编码指令

*

举例

管理员（操作密码为 123400）退出编程模式。

步骤1　管理员在编码模式下，输入编码指令为*。

步骤2　按【确认键】。

屏幕显示：退出编程模式。

6.5 单一子系统模式

6.5.1 进入子系统模式

功能说明

进入单一子系统模式后，可以实现子系统下属通道旁路、子系统下属通道消警和子系统附属通道配置功能，操作员能否操作需确认是否具备该操作权限。

授权用户

管理员或带权限的操作员

编码指令

［管理员操作密码/带权限的操作员操作密码］ + 【*】 + 【5】 + 【n1】

说明

支持 64 个子系统，n1 表示子系统号 01～64。

举例

管理员（操作密码为 123400）进入子系统 01 模式。

步骤1　在全局模式下，输入编码指令为 123400*501。

步骤2　按【确认键】。

屏幕显示：进入子系统模式。

6.5.2 设置旁路

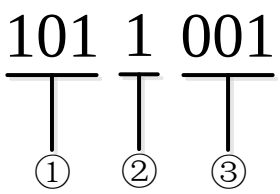
功能说明

将子系统中的下属通道设置旁路或隔离。

授权用户

管理员或带权限的操作员

编码指令



序号	说明
①	编码地址，表示此操作是旁路设置，默认为 101
②	旁路模式：0－正常，1－旁路，2－隔离
③	当前子系统下属通道号，范围为 001～256

举例

管理员（操作密码为 123400）将子系统 01 中的下属通道 001 设置为旁路。

步骤1　管理员在子系统 01 模式下，输入编码指令为 1011001。

步骤2　按【确认键】。

6.5.3 设置子系统附属通道

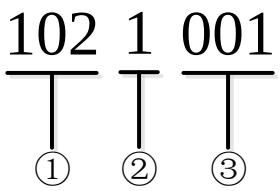
功能说明

在子系统中添加或删除子系统附属通道。

授权用户

管理员或带权限的操作员

编码指令



序号	说明
①	编码地址，表示此操作是设置子系统附属通道，默认为 102
②	添加/删除：0－删除，1－添加
③	子系统附属通道号，范围为 001～256

说明

- 通道不能重复。
- 通道的添加根据实际通道总数来决定，超出会提示操作失败。

举例

管理员（操作密码为 123400）在子系统 01 中添加新通道 002。

步骤1　管理员在子系统 01 模式下，输入编码指令为 1021002。

步骤2　按【确认键】。

6.5.4 通道消警

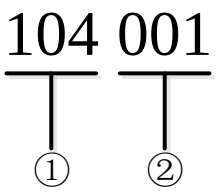
功能说明

消除子系统中某一通道的报警。

授权用户

管理员或带权限的操作员

编码指令



序号	说明
①	编码地址，表示此操作是取消通道报警，默认为 104
②	当前子系统下属通道号，范围为 001～256

举例

管理员（操作密码为 123400）消除子系统 01 中下属通道 001 的报警。。

步骤1　管理员在子系统 01 模式下，输入编码指令为 104001。

步骤2　按【确认键】。

6.5.5 退出子系统模式

功能说明

退出子系统模式。

说明

- 如果 5 分钟内没有任何操作，系统会自动退出子系统模式并进入全局模式。
- 若要换成其他模式前，必须先退出子系统模式。

授权用户

管理员或带权限的操作员

编码指令

*

举例

管理员（操作密码为 123400）退出子系统 01 模式。

步骤1　管理员在子系统 01 模式下，输入编码指令为*。

步骤2　按【确认键】。

屏幕显示：退出子系统模式。

6.6 系统查询模式

6.6.1 进入系统查询模式

功能说明

进入系统查询模式后，可以实现各类查询功能。

授权用户

管理员或安装员用户

编码指令

［安装员操作密码/管理员操作密码］ + 【*】 + 【6】

举例

管理员（操作密码为 123400）进入系统查询模式。

步骤1　在全局模式下，输入编码指令为 123400*6。

步骤2　按【确认键】。

屏幕显示：进入系统查询模式。

6.6.2 查询报警输入/输出通道数

功能说明

查询报警输入/输出通道数。

授权用户

管理员或安装员用户

编码指令

200

举例

管理员（操作密码为 123400）查询报警输入/输出通道数。

步骤1　管理员在系统查询模式下，输入编码指令为 200。

步骤2　按【确认键】。

屏幕显示：**200 0016/0008**，0016/0008 表示报警输入通道是 16 个，报警输出通道是 8 个。

6.6.3 查询激活防区数

功能说明

查询有触发报警的防区个数。

授权用户

管理员或安装员用户

编码指令

201

举例

管理员（操作密码为 123400）查询激活防区数。

步骤1　管理员在系统查询模式下，输入编码指令为 201。

步骤2　按【确认键】。

屏幕显示：**201 001**，001 表示激活防区个数为 1 个。

6.6.4 查询通道报警状态

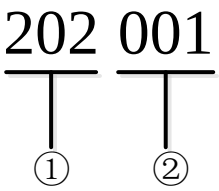
功能说明

查询通道报警状态。

授权用户

管理员或安装员用户

编码指令



序号	说明
①	编码地址，表示此操作是查询通道报警状态，默认为 202
②	通道号，范围为 001～256

举例

管理员（操作密码为 123400）查询通道 001 的报警状态。

步骤1　管理员在系统查询模式下，输入编码指令为 202001。

步骤2　按【确认键】。

屏幕显示：**202 0**，0 表示未报警，1 表示报警。

6.6.5 查询通道物理映射地址

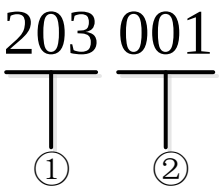
功能说明

查询通道物理映射地址。

授权用户

管理员或安装员用户

编码指令



序号	说明
①	编程地址，表示此操作是查询通道物理映射地址，默认为 203
②	通道号，范围为 001～256

举例

管理员（操作密码为 123400）查询通道 001 的物理映射地址。

步骤1　管理员在系统查询模式下，输入编码指令为 203001。

步骤2　按【确认键】。

屏幕显示：**203 0/000/00**，0/000/00 表示物理映射地址 slot/level1/level2，slot 表示根节点序号，level1 为第一级级联地址，level2 为第二级级联地址。

6.6.6 查询通道旁路状态

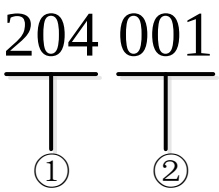
功能说明

查询通道旁路状态。

授权用户

管理员或安装员用户

编码指令



序号	说明
①	编码地址，表示此操作是查询通道旁路状态，默认为 204
②	通道号，范围为 001～256

举例

管理员（操作密码为 123400）查询通道 001 的旁路状态。

步骤1　管理员在系统查询模式下，输入编码指令为 204001。

步骤2　按【确认键】。

屏幕显示：**204 0**，0 表示正常，1 表示旁路，2 表示隔离。

6.6.7 查询系统布/撤防状态

功能说明

查询系统布撤防状态。

授权用户

管理员或安装员用户

编码指令

206

举例

管理员（操作密码为 123400）查询系统布撤防状态。

步骤1　管理员在系统查询模式下，输入编码指令为 206。

步骤2　按【确认键】。

屏幕显示：**206 0**，0 表示撤防，1 表示布防，2 表示部分布防。

6.6.8 查询用户个数

功能说明

查询查询用户个数。

授权用户

管理员或安装员用户

编码指令

207

举例

管理员（操作密码为 123400）查询用户个数。

步骤1　管理员在系统查询模式下，输入编码指令为 207。

步骤2　按【确认键】。

屏幕显示：**207 000**，000 表示用户个数为 0。

6.6.9 查询用户是否存在

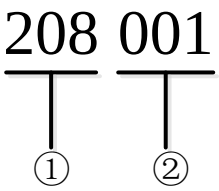
功能说明

查询用户是否存在。

授权用户

管理员或安装员用户

编码指令



序号	说明
①	编码地址，表示此操作是查询用户是否存在，默认为 208
②	用户编号，范围为 000～099

举例

管理员（操作密码为 123400）查询用户 001 是否存在。

步骤1　管理员在系统查询模式下，输入编码指令为 208001。

步骤2　按【确认键】。

屏幕显示：**208 0**，0 表示用户不存在，1 表示用户存在。

6.6.10 查询端口号

功能说明

查询报警主机的端口号。

授权用户

管理员或安装员用户

编码指令

209

举例

管理员（操作密码为 123400）查询报警主机的端口号。

步骤1　管理员在系统查询模式下，输入编码指令为 209。

步骤2　按【确认键】。

屏幕显示：**209 37777**，37777 是系统默认端口号。

6.6.11 查询 IP 地址

功能说明

查询报警主机的 IP 地址。

授权用户

管理员或安装员用户

编码指令

210

举例

管理员（操作密码为 123400）查询报警主机的 IP 地址。

步骤1　管理员在系统查询模式下，输入编码指令为 210。

步骤2　按【确认键】。

屏幕显示：**210 192.168.1.108**，显示的 IP 地址以实际控制器为准。

6.6.12 查询子网掩码

功能说明

查询报警主机的子网掩码。

授权用户

管理员或安装员用户

编码指令

211

举例

管理员（操作密码为 123400）查询报警主机的子网掩码。

步骤1　管理员在系统查询模式下，输入编码指令为 211。

步骤2　按【确认键】。

屏幕显示：**211 255.255.0.0**，显示的子网掩码以实际控制器为准。

6.6.13 查询网关

功能说明

查询报警主机的网关地址。

授权用户

管理员或安装员用户

编码指令

212

举例

管理员（操作密码为 123400）查询报警主机的网关地址。

步骤1　管理员在系统查询模式下，输入编码指令为 212。

步骤2　按【确认键】。

屏幕显示：**212 192.168.1.1**，显示的网关以实际控制器为准。

6.6.14 退出系统查询模式

功能说明

退出子系统模式。

说明

- 如果 5 分钟内没有任何操作，系统会自动退出系统查询模式并进入全局模式。
- 若要换成其他模式前，必须先退出系统查询模式。

授权用户

管理员或安装员用户

编码指令

*

举例

管理员（操作密码为 123400）退出系统查询模式。

步骤1　管理员在系统查询模式下，输入编码指令为*。

步骤2　按【确认键】。

屏幕显示：退出系统查询模式。

6.7 步测模式

6.7.1 进入步测模式

功能说明

在全局模式下，通过管理员或安装员用户操作密码可进入步测模式，对防区进行调试。若防区异常会直接上报警情给键盘，退出步测模式后，会自动清除键盘上的防区报警符号。

说明

- 进入测试模式后，防区将不再受布撤防、旁路、子系统、防区类型等限制。
- 防区被触发，只上报警情给键盘，没有其他报警联动输出。
- 扩展模块仍需要通过开关量防区配置进行设置。
- 隔离的防区不会上报警情给键盘。
- 若要换成其他模式，必须先退出步测模式。

授权用户

管理员或安装员用户

编码指令

［安装员操作密码/管理员操作密码］ + 【*】 + 【7】

举例

管理员（操作密码为 123400）进入步测模式。

步骤1　管理员在全局模式下，输入编码指令为 123400*7。

步骤2　按【确认键】。

屏幕显示：进入步测模式。

6.7.2 退出步测模式

功能说明

退出步测模式。

说明

- 如果 5 分钟内没有任何操作，系统会自动退出步测模式并进入全局模式。
- 若要换成其他模式前，必须先退出步测模式。

授权用户

管理员或安装员用户

编码指令

*

举例

管理员（操作密码为 123400）退出步测模式。

步骤1　管理员在步测模式下，输入编码指令为*。

步骤2　按【确认键】。

屏幕显示：退出步测模式。

7 控制器维护

- 电路板上的灰尘受潮后会引起短路，从而影响总线防盗报警控制器正常工作，甚至损坏报警控制器。为了使报警控制器能长期稳定工作，请定期用刷子对电路板、接插件、机箱风机、机箱等进行除尘。
- 请确保控制器良好接地，以免报警信号受到干扰，同时避免总线防盗报警控制器被静电或感应电压损坏。
- 请不要带电插拔报警信号线以及 RS232、RS485 等接口，否则容易损坏这些端口。
- 请确保总线防盗报警控制器远离高温的热源及场所。
- 请保持总线防盗报警控制器机箱周围通风良好，以利于散热。
- 请定期进行系统检查及维护。

8 常见问题解答

若您所遇到的问题不在以下的内容中，请与您所在地客服人员联系或致电总部客服咨询，我们将竭诚为您服务。

1　问：开机后，总线防盗报警控制器无法正常启动？

答：可能原因如下：

a） 输入电源不正确。
b） 开关电源线接触不好。
c） 开关电源损坏。
d） 程序升级错误。
e） 总线防盗报警控制器主板损坏。

2　问：总线防盗报警控制器启动几分钟后会自动重启或经常死机？

答：可能原因如下：

a） 输入电压不稳定或过低。
b） 开关电源功率不够。
c） 散热不良，灰尘太多，机器运行环境太恶劣。
d） 总线防盗报警控制器硬件故障。

3　问：时间显示不对？

答：可能原因如下：

a） 设置错误。
b） 电池接触不良或电压偏低。
c） 晶振不良。

4　问：客户端不能登录？

答：可能原因如下：

a） 如果客户端无法安装或者无法正常显示，且操作系统是 win98 或 win me，推荐将操作系统更新到 win2000sp4 以上版本，或者安装低版本的客户端软件。
b） ActiveX 控件被阻止。
c） 没有安装 dx8.1 或以上版本，升级显卡驱动。
d） 网络连接故障。
e） 网络设置问题。
f） 用名和密码不正确。
g） 客户端版本与总线防盗报警控制器程序版本不匹配。

5　问：网络连接不稳定？

答：可能原因如下：

a） 网络不稳定。
b） IP 地址冲突。
c） MAC 地址冲突。
d） 计算机或总线防盗报警控制器网卡不好。

6　问：报警信号无法布防？

答：可能原因如下：

a） 报警设置不正确。

b） 输入控制器故障或连接不正确。

c） 程序版本不对，升级程序可以解决。

7 问：报警不起作用？

答：可能原因如下：

a） 报警设置不正确。

b） 报警接线不正确。

c） 报警输入信号不正确。

d） 一个报警控制器同时接入 2 个回路。

8 问：本地菜单操作高级密码或网络密码忘记？

答：解决办法如下：

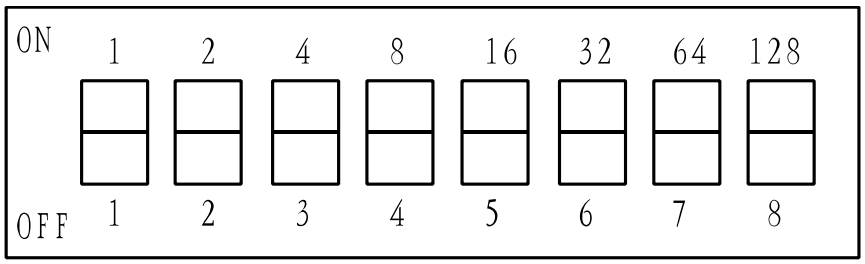
请与您所在地客服人员联系或致电总部客服电话，我们将根据您提供的机器型号及程序版本指导您如何解决。

附录1 继电器参数表

型号		HFD23/005-1ZS	HRB1-S-DC5V
触点材料		AgNi+镀金	AuAg10/AgNi10/CuNi30
额定值 (电阻负载)	额定开关容量	30V DC 1A/125V AC 0.5A	24V DC 1A/125V AC 2A
	最大开关功率	62.5VA/30W	250VA/48W
	最大开关电压	125V AC/60V DC	125V AC/60V DC
	最大开关电流	2A	2A
绝缘	触点间	400VAC 1 分钟	500VAC 1 分钟
	触点与线圈之间	1000VAC 1 分钟	1000VAC 1 分钟
开通时间		5ms max	5ms max
关断时间		5ms max	5ms max
寿命	机械	1×107 次(300 次/MIN)	1×106(300 次/MIN)
	电气	1×105 次(30 次/MIN)	2.5×104 次(30 次/MIN)
工作环境温度		-30℃～+70℃	-40℃～+70℃

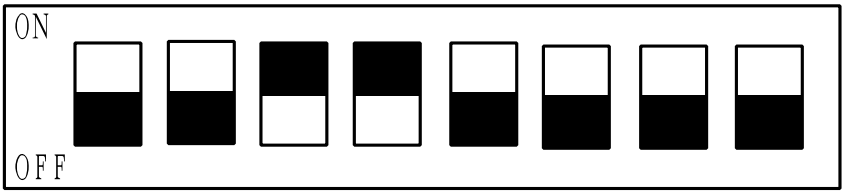
附录2 扩展模块拨码与地址对应关系

拨码开关从左到右为 1～8，即最低位到最高位，对应的数字如下所示：

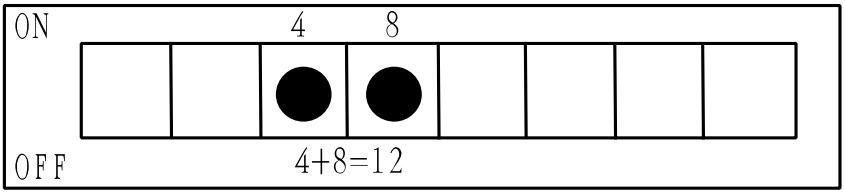


黑色在 on 的一端表示 1，如  ；黑色在 off 的一端表示 0，如  。

例如：当拨码开关为下图所示时，



则对应的二进制为：



表示的十进制为：地址=12。

附录3 键盘编码指令表

命令		操作指令	含义
全局模式下	布防	123400*00+确认键	管理员全局布防
	撤防	123400*01+确认键	管理员全局撤防
	子系统布防	12340001**0+确认键	管理员子系统 1 布防
	子系统撤防	12340001**1+确认键	管理员子系统 1 撤防
	单防区布防	123400001**2+确认键	管理员防区 1 布防
	单防区撤防	123400001**3+确认键	管理员防区 1 撤防
	消警	123400*1+确认键	管理员消除报警
	报警输出设置	123400*20011+确认键	管理员对报警输出 1 打开强制报警功能
	恢复默认配置	123400*3+确认键	管理员恢复默认配置
	PSTN 手动测试	123400*8+确认键	管理员进行 PSTN 手动测试
	PSTN 开启定时测试	123400*9+确认键	管理员开启 PSTN 定时测试
	PSTN 关闭定时测试	123400*10+确认键	管理员关闭 PSTN 定时测试
编程模式下	进入编程模式	123400*4+确认键	管理员进入编程模式
	增加用户	0000028888+确认键	增加操作员用户 002，密码 8888
	修改密码	0000026666+确认键	修改操作员用户 002 的密码为 6666
	删除用户	001002+确认键	删除操作员用户 002
	设置权限	0020020+确认键	设置操作员用户 002 具有布撤防权限
	本地 IP 地址设置	573010015022105+确认键	设置报警主机 IP 地址为 10.15.22.105
	本地端口号设置	57437777+确认键	设置报警主机端口号为 37777
	子网掩码设置	575255255000000+确认键	设置报警主机子网掩码为 255.255.0.0
	网关设置	576010015000001+确认键	设置报警主机网关为 10.15.0.1
	清除 CID 缓存	600+确认键	清除 CID 缓存
	退出当前模式	*	退出当前模式
单一子系统模式下	进入子系统模式	123400*501+确认键	管理员进入子系统 1
	旁路设置	1012003+确认键	隔离防区 3
	子系统附属通道配置	1021001+确认键	添加防区 1 到子系统 1
	通道消警	104001+确认键	取消防区 1 报警
	退出当前模式	*+确认键	退出当前模式
查询模式下	进入系统查询模式	123400*6+确认键	管理员进入查询模式
	查询报警输入/输出通道数	200+确认键	查询报警输入/输出通道数
	查询激活防区数	201+确认键	查询总报警防区数
	查询通道报警状态	202001+确认键	查询防区 1 报警状态
	查询通道物理映射地址	203001+确认键	查询防区 1 物理映射地址
	查询通道旁路状态	204001+确认键	查询防区 1 是否旁路

命令		操作指令	含义
	查询系统布撤防状态	206+确认键	查询系统布撤防状态
	查询用户个数	207+确认键	查询用户个数
	查询用户是否存在	208001+确认键	查询用户是否存在
	查询端口号	209+确认键	查询端口号
	查询 IP 地址	210+确认键	查询 IP 地址
	查询子网掩码	211+确认键	查询子网掩码
	查询网关	212+确认键	查询网关
	退出当前模式	*+确认键	退出当前模式
步测模式下	进入步测模式	123400*7+确认键	进入步测模式
	退出当前模式	*+确认键	退出当前模式