Modbus 转 GPRS 网关

MGS-801

产品手册

V2.4

Rev A

上海泗博自动化技术有限公司

SiboTech Automation Co., Ltd.

技术支持热线：021-3126 5138

E-mail: support@sibotech.net

目　录

一、产品概述

1.1 产品功能

MGS-801 是基于 RS232/485 通讯、支持 Modbus 总线协议和 GPRS 无线数据通讯的工业物联网网关，可实现无线远程监控和连接博凯云（工业设备云）的功能，主要针对需要无人值守和远程监控要求的工业监控现场。MGS-801 可用于 Modbus 从站设备通过 GPRS 进行远程监控，可将设备数据上传到博凯云，广泛应用于环保设备监控、空气产品设备监控、供水等多种领域。

1.2 产品特点

- 通信模式：Modbus 主站模式，串口作为 Modbus 主站进行数据采集和控制，通过 GPRS 连接博凯云，与博凯云进行数据交换
- GPRS 支持永远在线，自动重连功能
- 主动连接博凯云，并有连接探测和自动重连功能
- 对数据进行 AES 加密，确保数据安全
- 采用新数据推送机制或周期发送机制，数据发送间隔可设置，以节省客户流量费用；
- 通过 GPRS 传递有效的 Modbus 寄存器数据，节约 GPRS 流量
- 可随时通过 GPRS 数据监控设备端运行状态
- 自动监测 GPRS 信号，具有 GPRS 信号强度指示功能
- 工业级的可靠性，实时监控模块状态，故障自复位
- 扩展型号可支持 OPC 服务器与第三方云服务器

1.3 技术指标

[1] GPRS 模块

支持协议及工作频段：支持 GSM 900 MHz/1800 MHz，协议兼容 GSM/GPRS Phase2/2+；

最大发射功率：EGSM900 Class 4 (2 W)，GSM1800 Class 1 (1 W)；

接收灵敏度： ＜-107 dBm；

SIM 卡：支持 3V/1.8V SIM 卡；

天线：支持 Hirose U.FL-R-SMT-1(80) 50 ohm 天线连接器；

[2] 串行端口

接口类型：三针端子及五针端子；

支持调试；

波特率：1200 - 115200bps；

隔离设计：1kV 光电隔离；

串口支持 RS485 或 RS232 接口，半双工，奇偶校验支持无校验、奇校验、偶校验、标记、空格，停止位支持 1 位和 2 位；

串口支持的协议类型：Modbus RTU 主站、Modbus ASCII 主站；

[3] 整机供电及防护安装

供电：DC 24V（11-30V）；

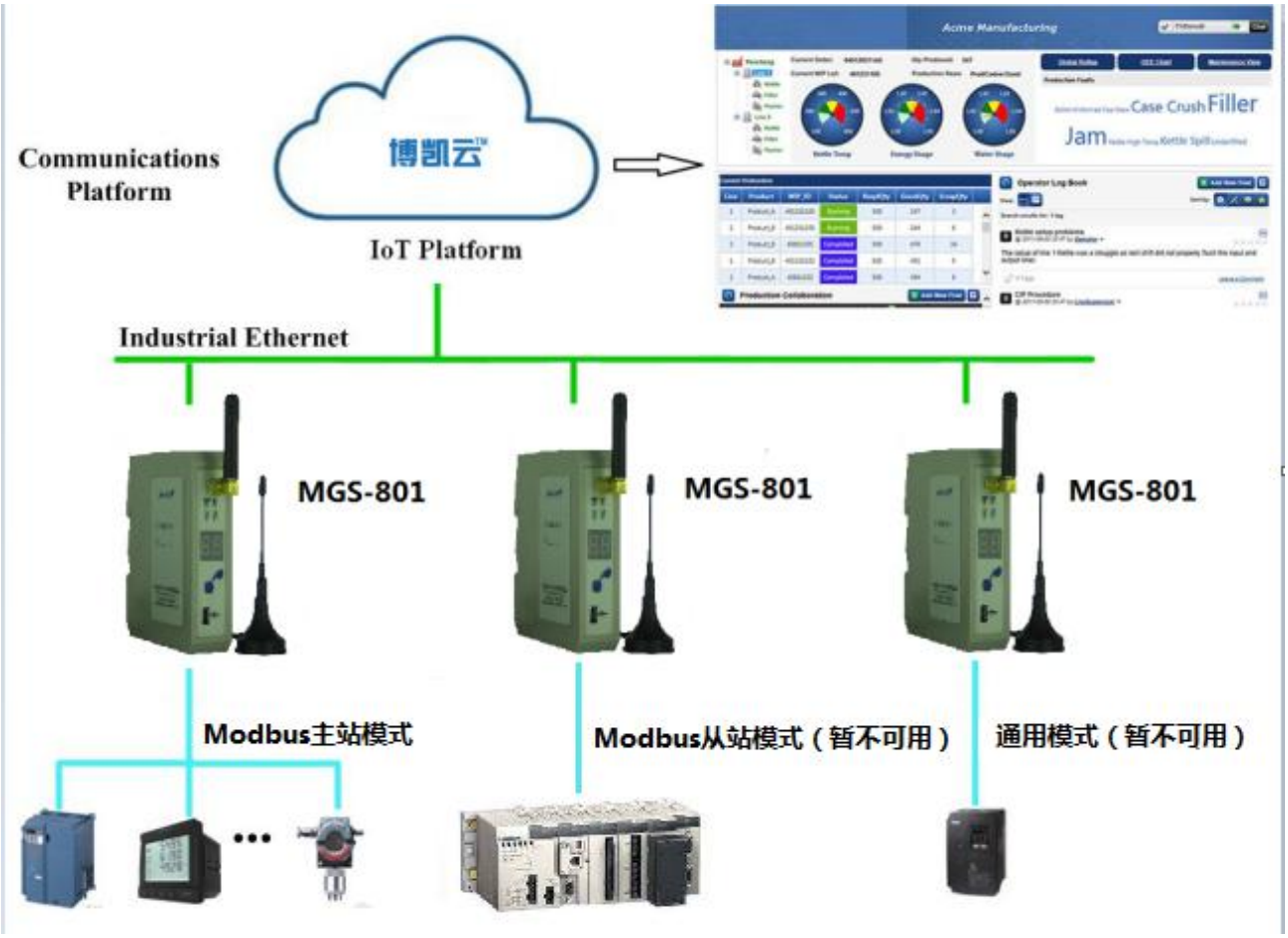
工作环境温度：-30℃ ～60℃，相对湿度：5%～95%（无凝露）；

机械尺寸：25mm（宽）× 100mm（高）× 90mm（深）；

安装方式：35mm 导轨；

防护等级：IP20。

二、应用案例



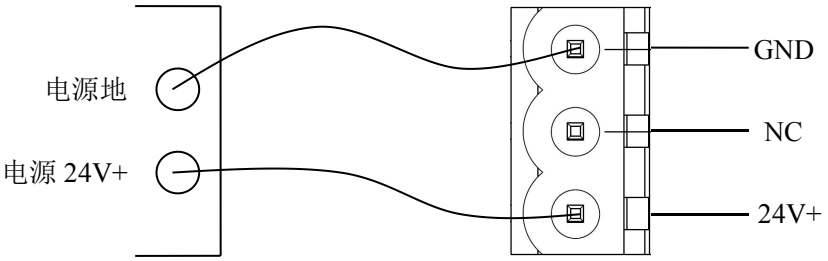
MGS-801 可做为 Modbus 主站与博凯云连接，通过 GPRS 将采集的设备数据推送至博凯云，同时在博凯云的界面也可以控制设备的运行。

目前 Modbus 从站与通用模式暂不可用，后续会开通相应功能。

三、快速应用指南

3.1 连接电源

使用直流 24V 电源供电，电源接线如下图：



直流+24V 电源　　MGS-801 的电源接口

3.2 连接 PC

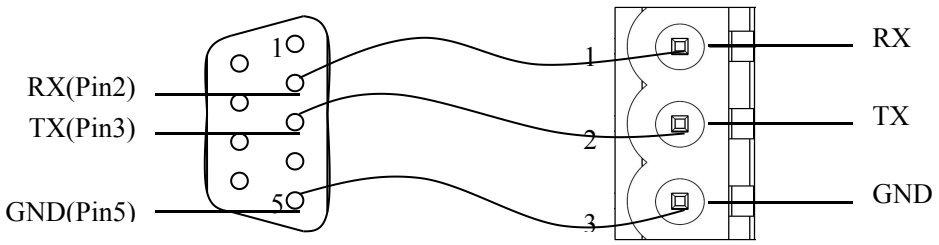
安装 USB 驱动，将网关的 USB 接口与 PC 的 USB 接口相连接。

3.3 安装软件并配置 MGS-801

将产品 CD 光盘放入计算机的光驱中，打开光盘，安装配置软件 **MGC-123** 。按照提示即可轻松完成安装。给 MGS-801 上电, 通过配置软件进入配置模式，数码管显示 CF 并闪烁。打开已安装好的配置软件 **MGC-123** 即可对 MGS-801 进行配置。

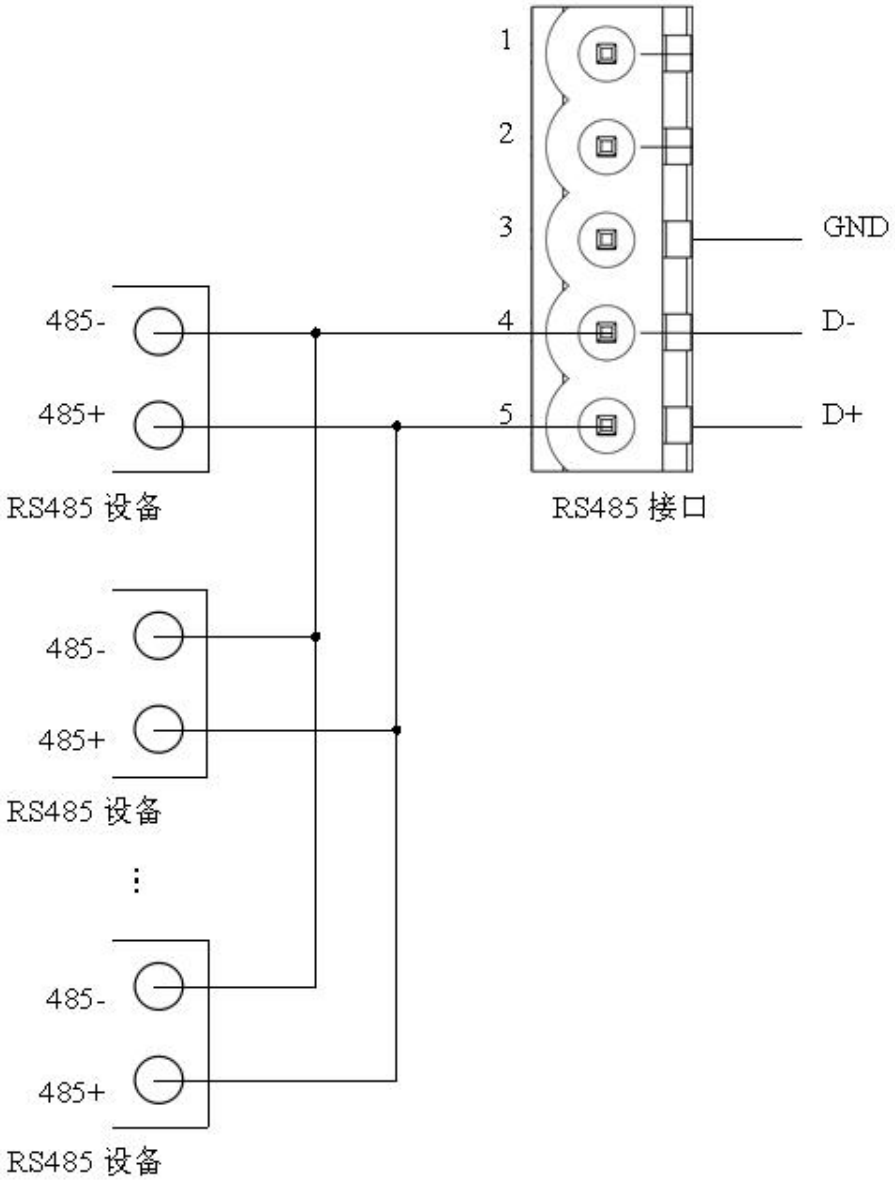
3.4 连接串口设备

配置完成后，连接通信接口，RS-232 接口的接线如下图：

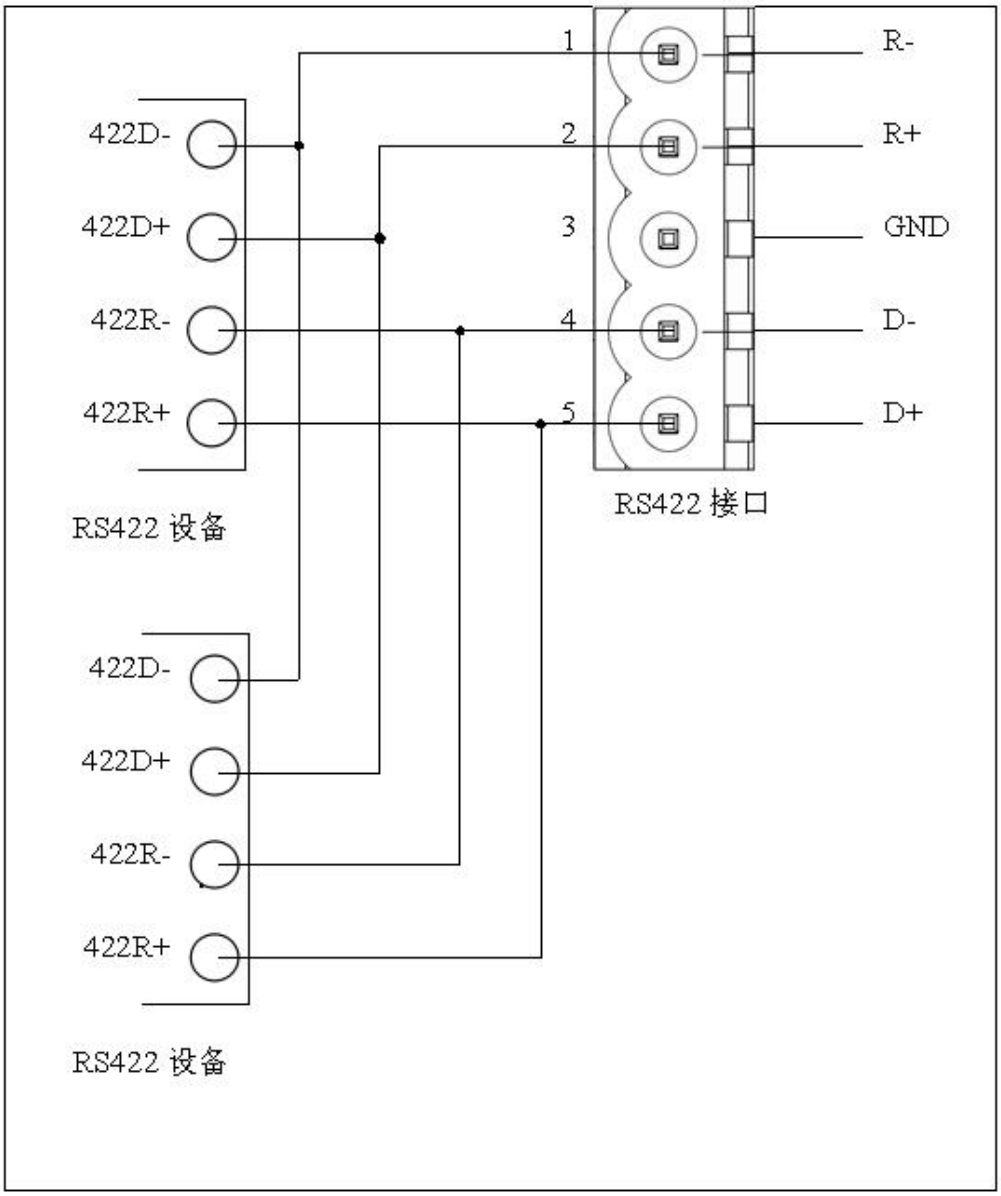


设备的 RS232 接口　　MGS-801 的 RS232 接口

RS-485 接口的接线如下图：



RS-422 接口的接线如下图：



RS-485/RS-422 在点到多点通信时，为了防止信号的反射和干扰，需在线路的最远两端各接一个终端电阻，参数为 120Ω 1/2W。

注：MGS-801 的 RS-485/RS-422 接口内部无终端电阻。

3.5 调试

MGS-801 支持调试功能，方便用户调试 Modbus 网络数据通信。

四、硬件说明

4.1 产品外观

注：此图仅供参考，产品外观应以实物为准。

4.2 指示灯

状态		说明
PWR	常亮	有电源
	常灭	无电源
STA	常灭	睡眠模式
	闪烁周期 1s，亮 0.1s	搜网状态或无网络时（含无 SIM 卡或未解 PIN 码时）
	闪烁周期 3s，亮 0.1s	已注册上 2G 网络
	闪烁周期 0.125s，亮 0.1s	GPRS 数据业务
TX	绿灯闪烁	RS-485/232 口有数据在发送
	绿灯灭	RS-485/232 口无数据发送
RX	绿灯闪烁	RS-485/232 口有数据在接收
	绿灯灭	RS-485/232 口无数据接收

4.3 数码管及按钮

数码管位于产品的正面。

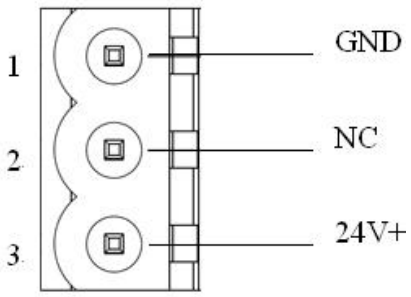
数码管的显示有三种情况：

数码管显示	说明
88	上电瞬间/Boot 成功瞬间(Boot 状态)
三条横条动态变化	正在搜索 GPRS 信号(Boot 状态/运行状态)
中间横条固定不变	没有插 SIM 卡或没有搜索到 GPRS 信号(Boot 状态)
EE	Boot 结束瞬间(Boot 状态)
SG	表示网关正处于运行模式(运行状态)

CF	表示网关正处于配置模式(运行状态)
具体数字	表示网关正处于运行模式，数字表示信号强度值(运行状态)

4.4 接口

4.4.1 电源接口



引脚	功能
1	GND，电源地
2	NC，无连接
3	24V+，直流正 24V

4.4.2 RS-485/RS-422 接口

MGS-801 产品的 RS-485 接口是标准的 RS-485 接口，以下简述本产品 RS-485 特性：

4.4.2.1 RS-485 传输技术基本特征

① 网络拓扑：线性总线，两端有有源的总线终端电阻；

② 传输速率：1200 bit/s~115.2Kbit/s；

③ 介质：屏蔽双绞电缆，也可取消屏蔽，取决于环境条件（EMC）；

④ 站点数：每分段 32 个站（不带中继），可多到 127 个站（带中继）；

⑤ 插头连接：3/5 针可插拔端子。

4.4.2.2 RS-485 传输设备安装要点

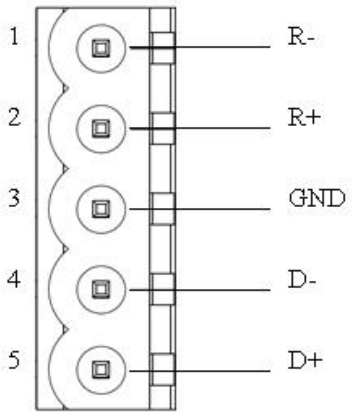
① 全部设备均与 RS-485 总线连接；

② 每个分段上最多可接 32 个站；

③ 总线的最远两端各有一个总线终端电阻，120Ω 1/2W 确保网络可靠运行。

串行接口采用开放式 5 针可插拔端子，用户可以根据面板上的指示进行接线。

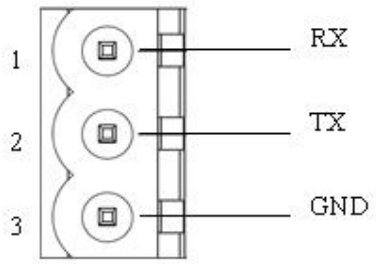
五针端子：



引脚	功能
1	R-，RS-422 接收-
2	R+，RS-422 接收+
3	GND（RS-485 或 RS-422 的通讯信号地）
4	D-，RS-485-/RS-422 发送-
5	D+，RS-485+/RS-422 发送+

4.4.3 RS-232 接口

MGS-801 产品的 RS-232 接口采用开放式 3 针可插拔端子，其引脚描述如下：



引脚	功能
1	RX，接用户设备 RS-232 的 RX
2	TX，接用户设备 RS-232 的 TX
3	GND，接用户设备 RS-232 的 GND

五、配置软件使用说明

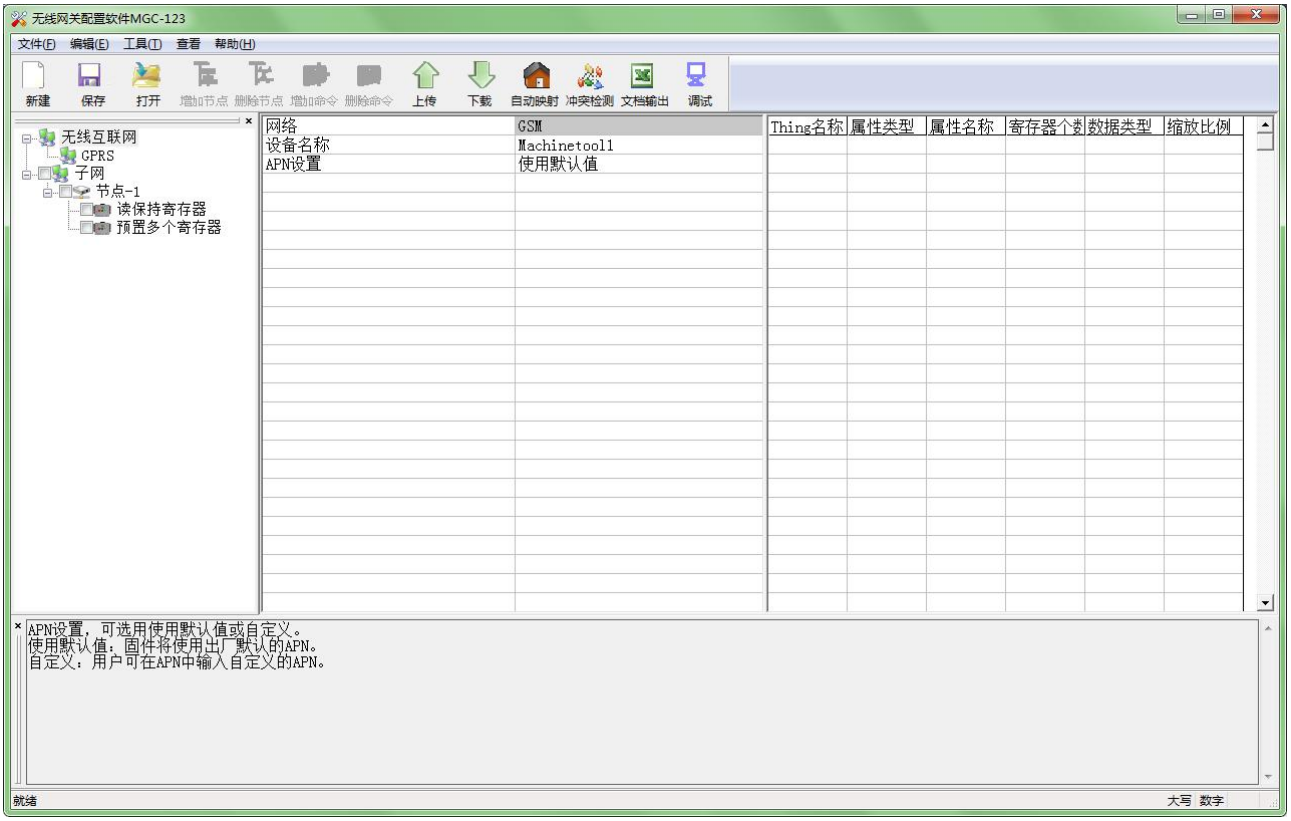
5.1 配置前注意事项

MGC-123 是一款基于 Windows 平台，用来配置 MGS-801 相关参数及命令的配置软件。

本说明书描述了网关配置软件 MGC-123 的具体使用方法和注意事项，方便工程人员的操作运用。在使用本软件前，请仔细阅读本说明书。

本软件通过 PC 机的 USB 接口和 MGS-801 的 USB 接口连接通讯，上载或下载配置文件。

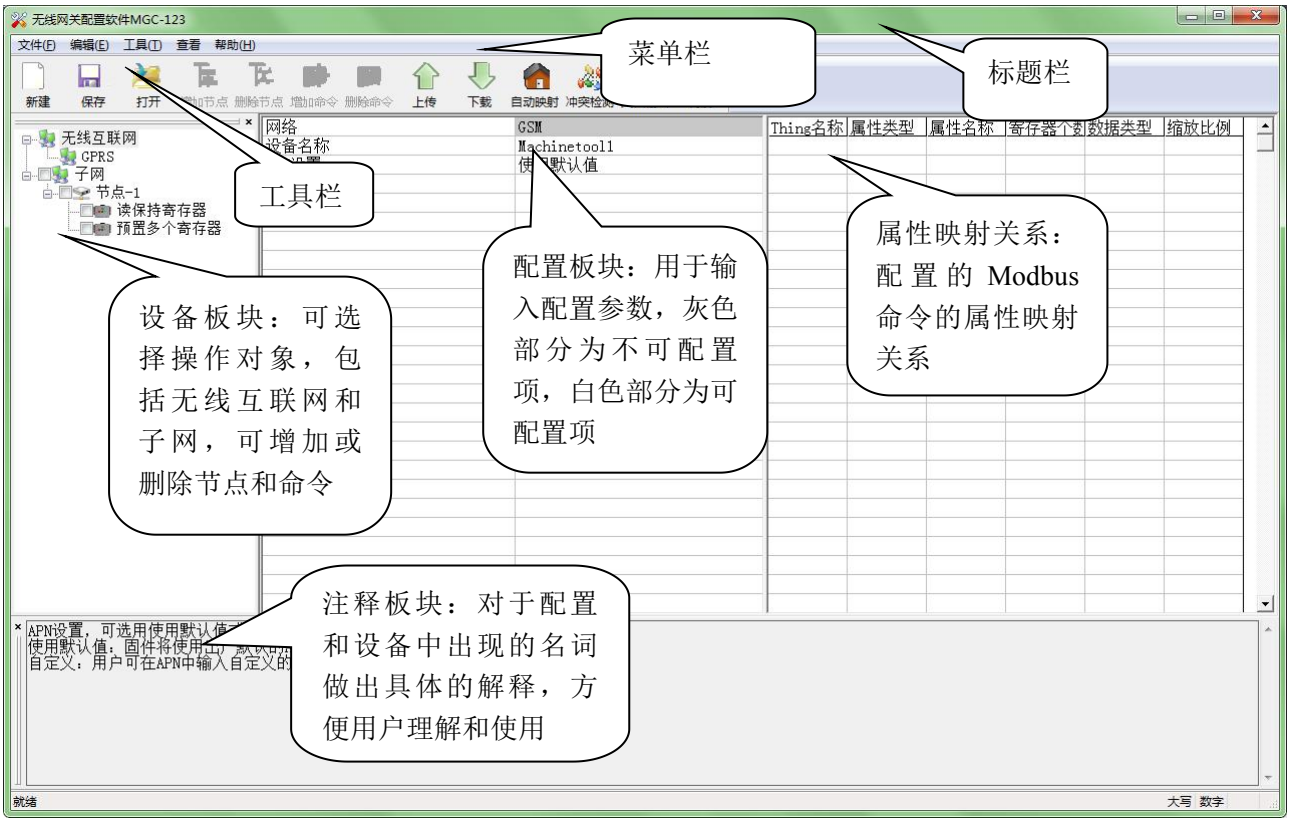
双击软件图标即可打开配置软件, 配置软件 MGC-123 主界面如下：



5.2 用户界面

界面包括：标题栏、菜单栏、工具栏、状态栏、设备板块、配置板块和注释板块。

备注：在该软件中，所有的灰色部分为不可更改项。



工具栏：

工具栏如下图所示：

从左至右的功能分别是：新建、保存、打开、增加节点、删除节点、增加命令、删除命令、上载配置信息、下载配置信息、自动映射、冲突检测、Excel 配置文档输出、通信调试。

：新建一个配置工程

：保存当前配置

：打开一个配置工程

：增加一个 Modbus 从站（协议类型：Modbus 主站）节点

：删除一个 Modbus 从站（协议类型：Modbus 主站）节点

：增加一条 Modbus 命令

：删除一条 Modbus 命令或者通用命令

：将配置信息从模块中读取上来，并且显示在软件中

：将配置信息从软件中下载到模块

：软件自动计算并填写每条命令的内存映射起始地址参数

：检测配置好的命令在网关内存数据缓冲区中是否有冲突

：将当前配置输出到本地硬盘，以.xls 文件格式保存

：监视 I/O 口数据和网络状态

5.3 设备视图操作

5.3.1 设备视图界面

5.3.2 设备视图操作方式

对于设备视图，子网部分支持如下三种操作方式：编辑菜单、快捷工具栏和右键编辑菜单，无线互联网部分仅支持右键编辑菜单操作。

编辑菜单

快捷工具栏

右键编辑菜单

5.3.3 设备视图操作种类

1）增加节点操作：在子网上单击鼠标左键，选中该节点，然后执行增加节点操作。在子网下增加一个名字为“节点-1”的节点。

2）删除节点操作：单击鼠标左键，选中待删除节点，然后执行删除节点操作。该节点及其下所有命令全部删除。

3）增加命令操作：在节点上单击鼠标左键，然后执行增加命令操作，为该节点添加命令。

子网协议类型为 Modbus 主站时，弹出如下选择命令对话框，供用户选择，如下图所示：

目前支持的命令号：01，02，03，04，05，06，15，16 号命令

选择命令：双击命令条目即可将选中的命令添加到当前选中节点下

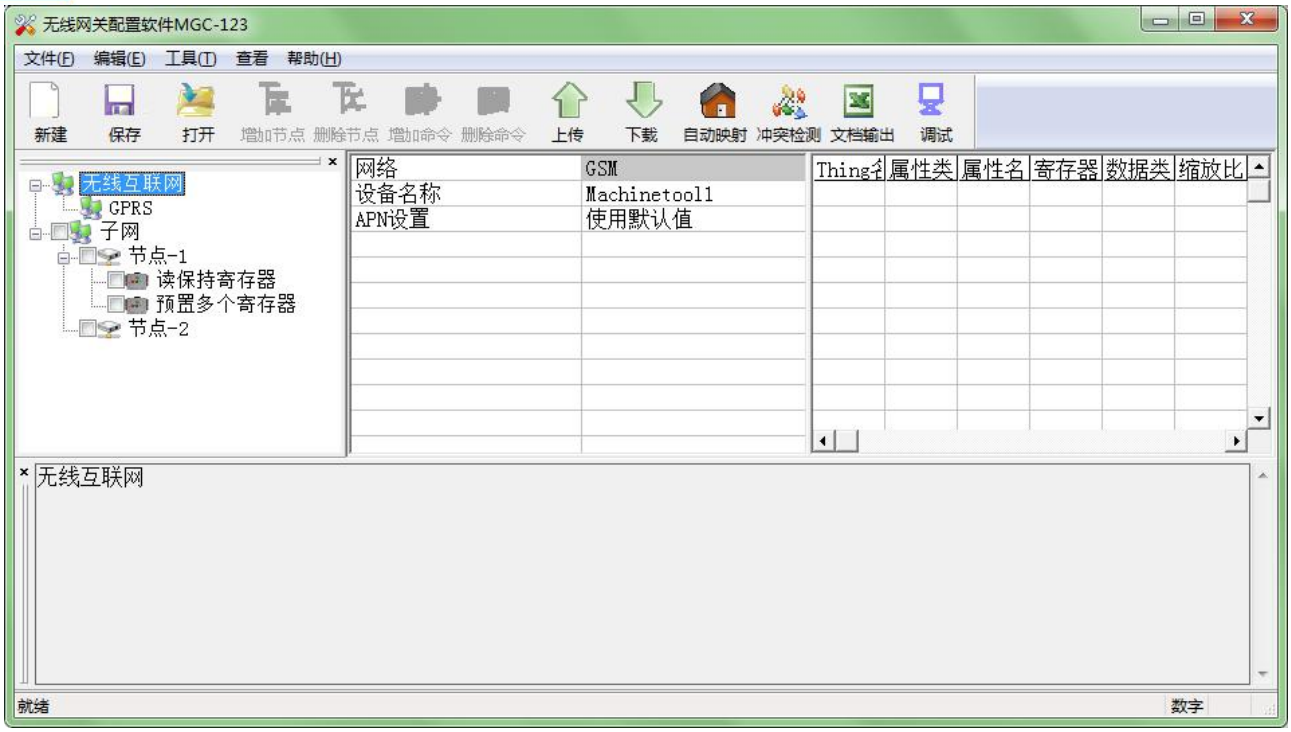
4）删除命令操作：单击鼠标左键，选中待删除命令，然后执行删除命令操作，该命令即被删除。

5）节点重命名操作：在需要重命名的节点上单击鼠标左键，在右侧配置板块，更改从地址参数即可对节点重命名。

5.4 配置视图操作

5.4.1 无线互联网配置视图界面

“无线互联网”可配置参数：设配名称、APN。

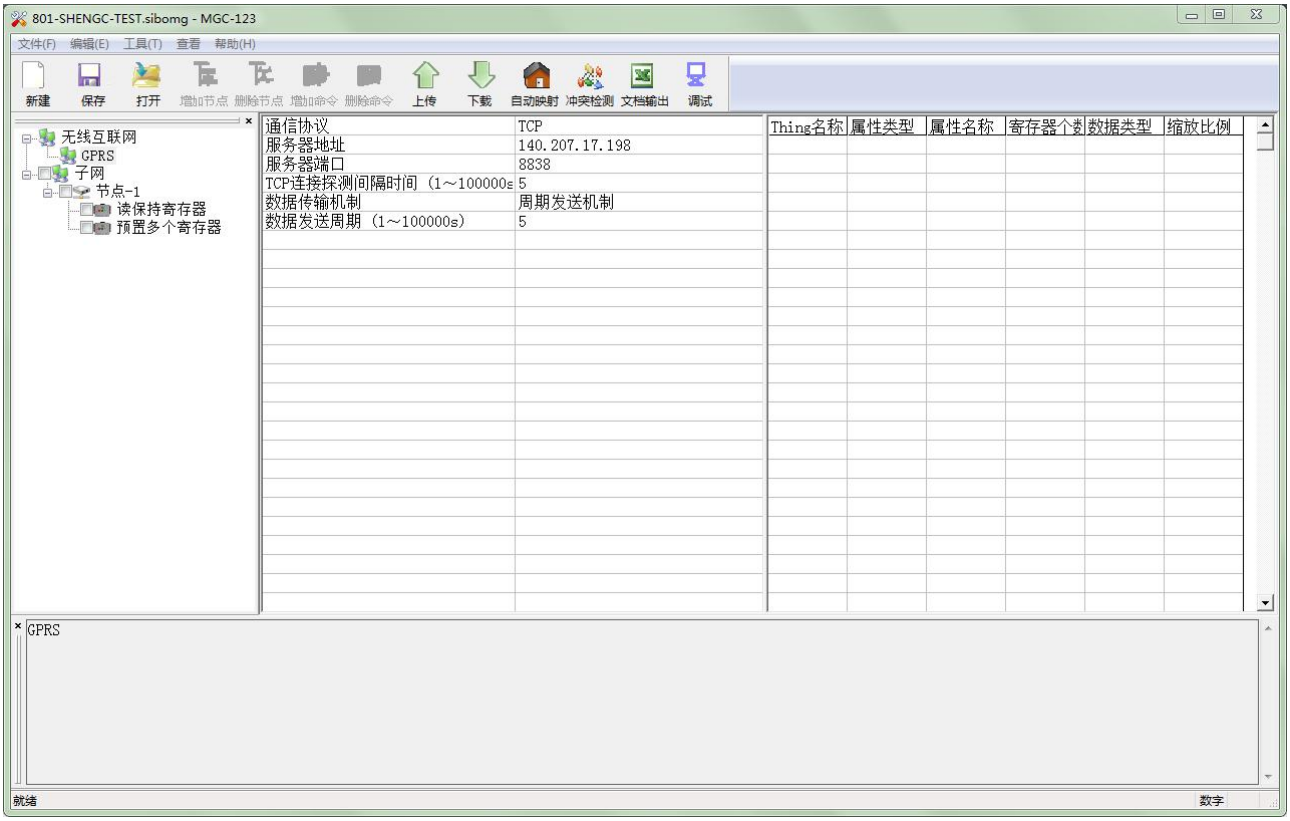


设备名称：用户所用设备的名称, 方便用户管理多台 MGS-801 设备

APN 设置：APN 设置，可选用使用默认值或自定义。使用默认值：固件将使用出厂默认的 APN。自定义：用户可在 APN 中输入自定义的 APN。

APN：（国内专网或国外使用）网络接入点名称，需咨询当地运营商。

“GPRS”可配置参数：通信协议、服务器地址、服务器端口、TCP 连接探测间隔时间、数据传输机制、数据发送周期。



通信协议：TCP，可以双向传输数据。

服务器地址：远端服务器的 IP 地址。

服务器端口：远端服务器的端口号，理论支持范围 0~65535，建议使用 8000~65535；

TCP 连接探测间隔时间：可选关闭或输入时间值，范围 1~100000s；

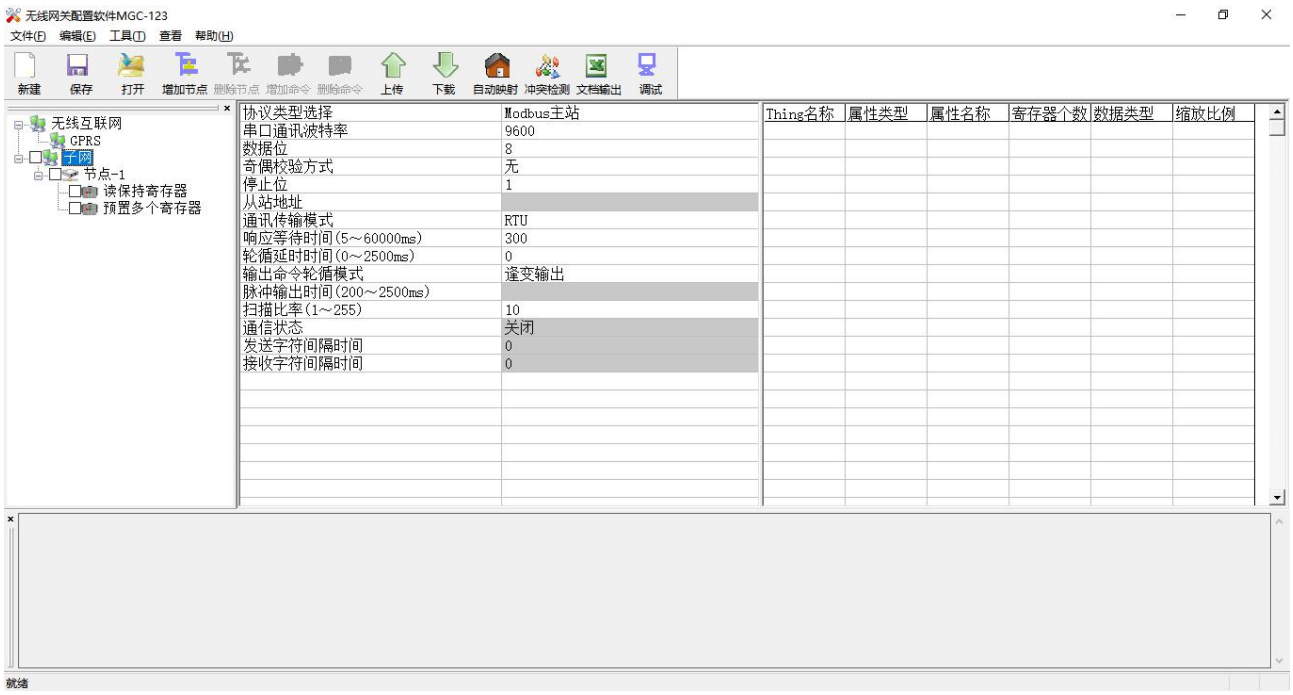
数据传输机制：提供“新数据推送机制”和“周期发送机制”两种选项，“新数据推送机制”是指有数据变化时 MGS-801 发送数据给远端服务器；“周期发送机制”是指按照指定的周期发生数据，无论数据是否发生变化；

数据发送周期：“周期发送数据机制”的数据发送周期时间，范围 1~100000s。

5.4.2 子网配置视图界面

可配置参数为：串口通讯波特率、数据位、奇偶校验方式、停止位、通讯传输模式、响应等待时间、轮询延时时间、输出命令轮询模式、扫描比率。

配置视图界面显示如下：



串口通讯波特率：300，600，1200，2400，4800, 9600，19200，38400，57600，115200bps 可选

数据位：8 位

奇偶校验方式：无、奇校验、偶校验、标记、空格可选

停止位：1、2 可选

通讯传输模式：RTU、ASCII 可选

响应等待时间：当 Modbus 主站发送命令后，等待从站响应的时间，范围：5～60000ms

轮询延时时间：一条 Modbus 命令发完并收到正确响应或响应超时之后，发送下一条 Modbus 命令之前，延迟的时间，范围：0～2500ms。实际轮询延时时间为输入值除以 10 之后取整，再乘以 10，单位 ms。假如输入值为 9，则实际轮询延时时间为 0ms；假如输入值为 15，则实际轮询延迟时间为 10ms。

输出命令轮询模式：

Modbus 写命令（输出命令），有三种输出模式：连续输出，禁止输出，逢变输出

连续输出：与 Modbus 读命令输出方式相同，根据扫描比率进行扫描输出

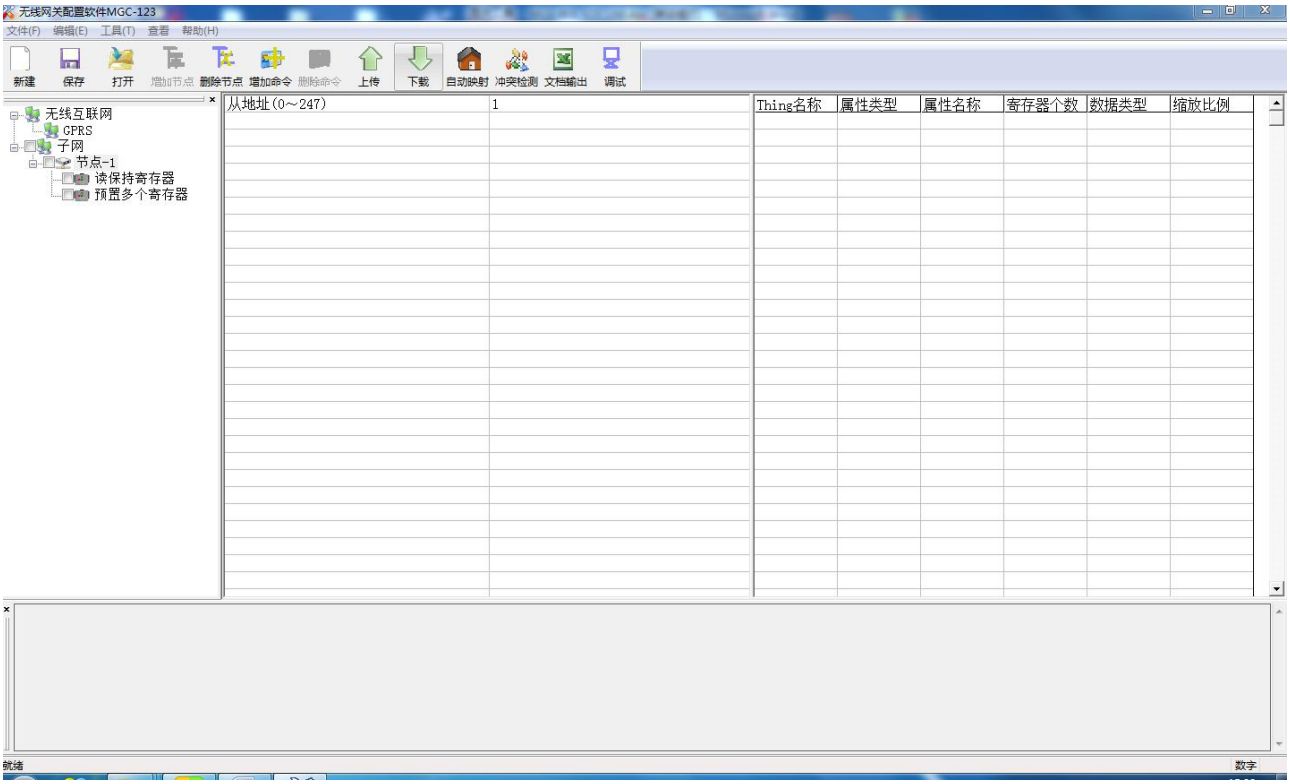
禁止输出：禁止输出 Modbus 写命令

逢变输出：输出数据有变化时，输出写命令，并在接收到正确响应后停止输出

扫描比率：快速扫描周期与慢速扫描周期的比值，如果该值设为 10，那么快速扫描命令发出 10 次，慢速扫描命令发出 1 次

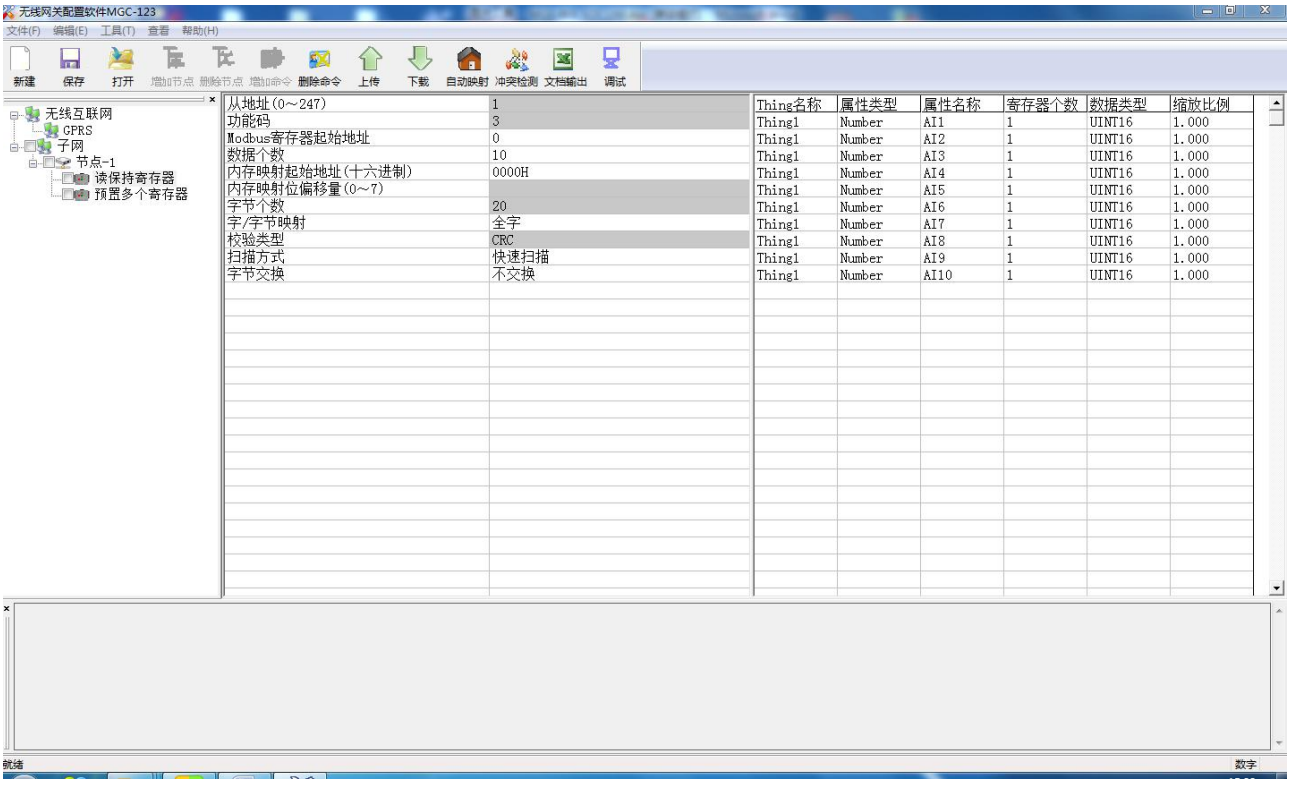
5.4.3 节点配置视图界面

在“Modbus 主站”模式下，在设备视图界面，单击新建的节点，配置视图界面显示如下：



5.4.4 命令配置视图界面

在设备视图界面，协议类型选择 Modbus 主站时，单击新建的命令，配置视图界面显示如下：



Modbus 寄存器起始地址：Modbus 从站设备中寄存器/开关量/线圈等起始地址，范围是 0～65535

注：配置软件 MG-123 中该条目指的是协议地址，当用户输入 PLC 地址时，确定后会自动弹出如下图说示的对话框，点击确定后，用户输入的 PLC 地址会被转换成协议地址。

PLC 地址与对应的协议地址举例如下表所示：

命令	PLC 地址举例	对应的协议地址
线圈状态	00001～00010	00000～00009
输入状态	10001～10010	00000～00009
保持寄存器	40001～40010	00000～00009
输入寄存器	30001～30010	00000～00009

例如：当配置的 Modbus 命令为 03H（读保持寄存器），当用户在这一条目中（Modbus 寄存器起始地

址）输入 40001，确定后会弹出上图所示的对话框，当点击确定后，输入的 PLC 地址 40001 会被转换成协议地址 0。

数据个数：Modbus 从站设备中寄存器/开关量/线圈的个数

内存映射起始地址（十六进制）：在模块内存缓冲区中数据的起始地址

数据在模块内存中映射的地址范围：

读命令：0x0000~0x01FF

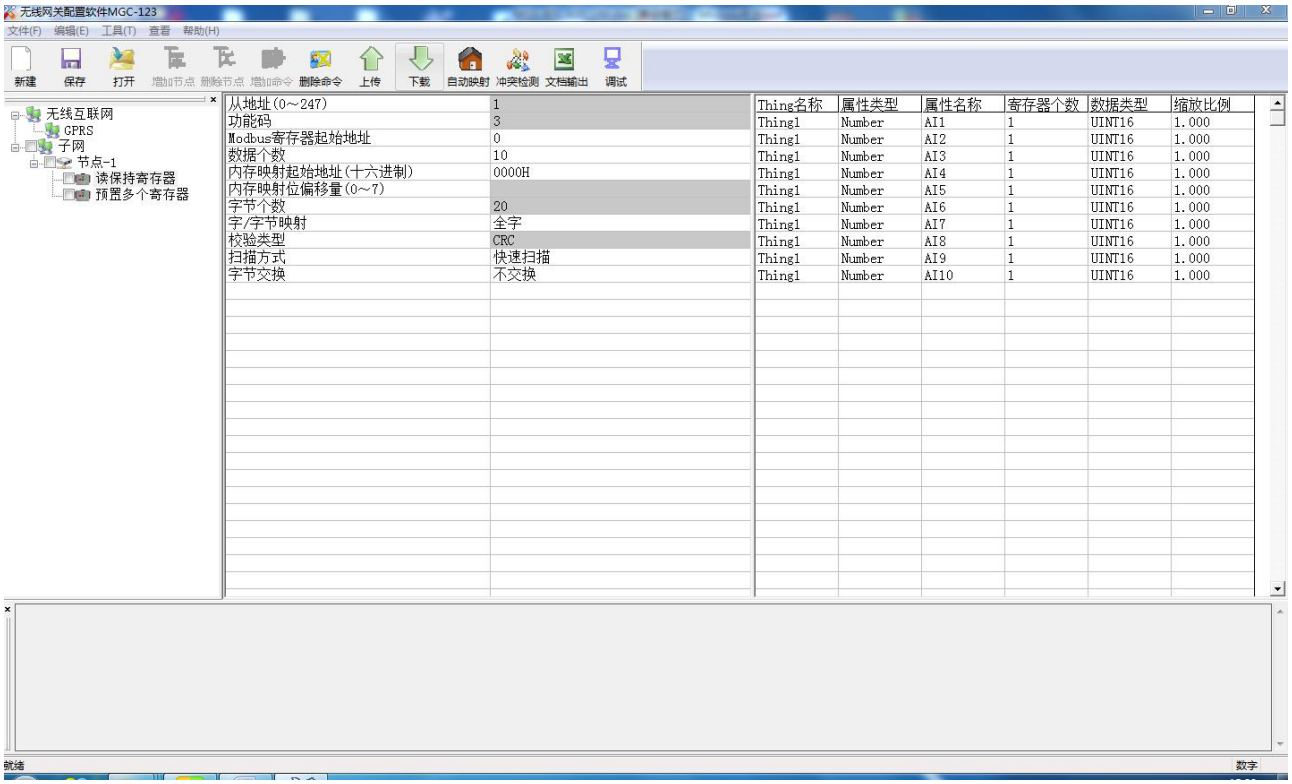
写命令：0x4000~0x41FF

写命令作为本地数据交换也可使用区域：0x0000~0x01FF

内存映射位偏移量（0～7）：对于位操作指令，起始位在字节中的位置，范围是 0～7

扫描方式：有两种扫描方式，快速扫描和慢速扫描，适应用户对不同的命令的快速扫描或慢速扫描的要求。扫描比率等于慢速扫描周期除以快速扫描周期，一般扫描比率为 10（在“子网”设置界面中设置）

5.4.5 属性配置视图



Thing 名称：可根据 Thing 命名规则，由用户自定义 Thing 的名称；

1. 直接点击 Thing 名称可单个更改：

Thing名称	属性类型	属性名称	寄存器个数	数据类型	缩放比例
UsrThing	Number	Property1	1	UINT16	1.000
Thing1	Number	Property2	1	UINT16	1.000
Thing1	Number	Property3	1	UINT16	1.000
Thing1	Number	Property4	1	UINT16	1.000
Thing1	Number	Property5	1	UINT16	1.000
Thing1	Number	Property6	1	UINT16	1.000
Thing1	Number	Property7	1	UINT16	1.000
Thing1	Number	Property8	1	UINT16	1.000
Thing1	Number	Property9	1	UINT16	1.000
Thing1	Number	Property10	1	UINT16	1.000

2. 勾选命令前的方框，可实现批量更改 Thing 名称：

Thing名称	属性类型	属性名称	寄存器个数	数据类型	缩放比例
Usr1Thing	Number	AI1	1	UINT16	1.000
Usr1Thing	Number	AI2	1	UINT16	1.000
Usr1Thing	Number	AI3	1	UINT16	1.000
Usr1Thing	Number	AI4	1	UINT16	1.000
Usr1Thing	Number	AI5	1	UINT16	1.000
Usr1Thing	Number	AI6	1	UINT16	1.000
Usr1Thing	Number	AI7	1	UINT16	1.000
Usr1Thing	Number	AI8	1	UINT16	1.000
Usr1Thing	Number	AI9	1	UINT16	1.000
Usr1Thing	Number	AI10	1	UINT16	1.000

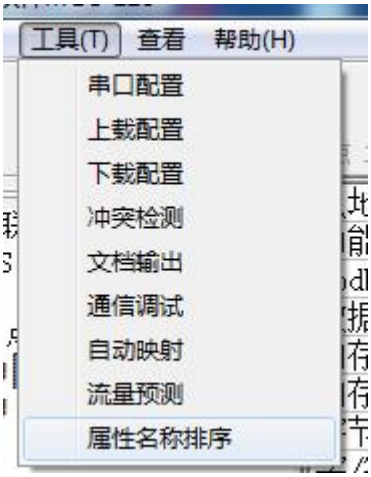
属性类型：不可更改。

属性名称：可根据属性命名规则，用户自定义属性名称；

1. 直接点击属性名称，修改单个属性名称

Thing名称	属性类型	属性名称	寄存器个数	数据类型	缩放比例
Usr1Thing	Number	userAI1	1	UINT16	1.000
Usr1Thing	Number	AI2	1	UINT16	1.000
Usr1Thing	Number	AI3	1	UINT16	1.000
Usr1Thing	Number	AI4	1	UINT16	1.000
Usr1Thing	Number	AI5	1	UINT16	1.000
Usr1Thing	Number	AI6	1	UINT16	1.000
Usr1Thing	Number	AI7	1	UINT16	1.000
Usr1Thing	Number	AI8	1	UINT16	1.000
Usr1Thing	Number	AI9	1	UINT16	1.000
Usr1Thing	Number	AI10	1	UINT16	1.000

2. 利用工具->属性名称排序



注：设备名称、Thing 名称以及保存的配置文件应当保持一致，命名规则为：

接入名称-客户公司首字母简写-设备类型-设备编号（或名称简写）。

请使用大写字母来表示，不可使用中文。公司首字母在 3-5 个大写字母，设备类型使用 3-5 个大写字母表示，设备编号默认从 1 开始。

如：801-KQHG-ZDJ-1 代表的是 801 接入，KQHG 公司 试用博凯云，设备类型是 ZDJ,设备编号是 1。

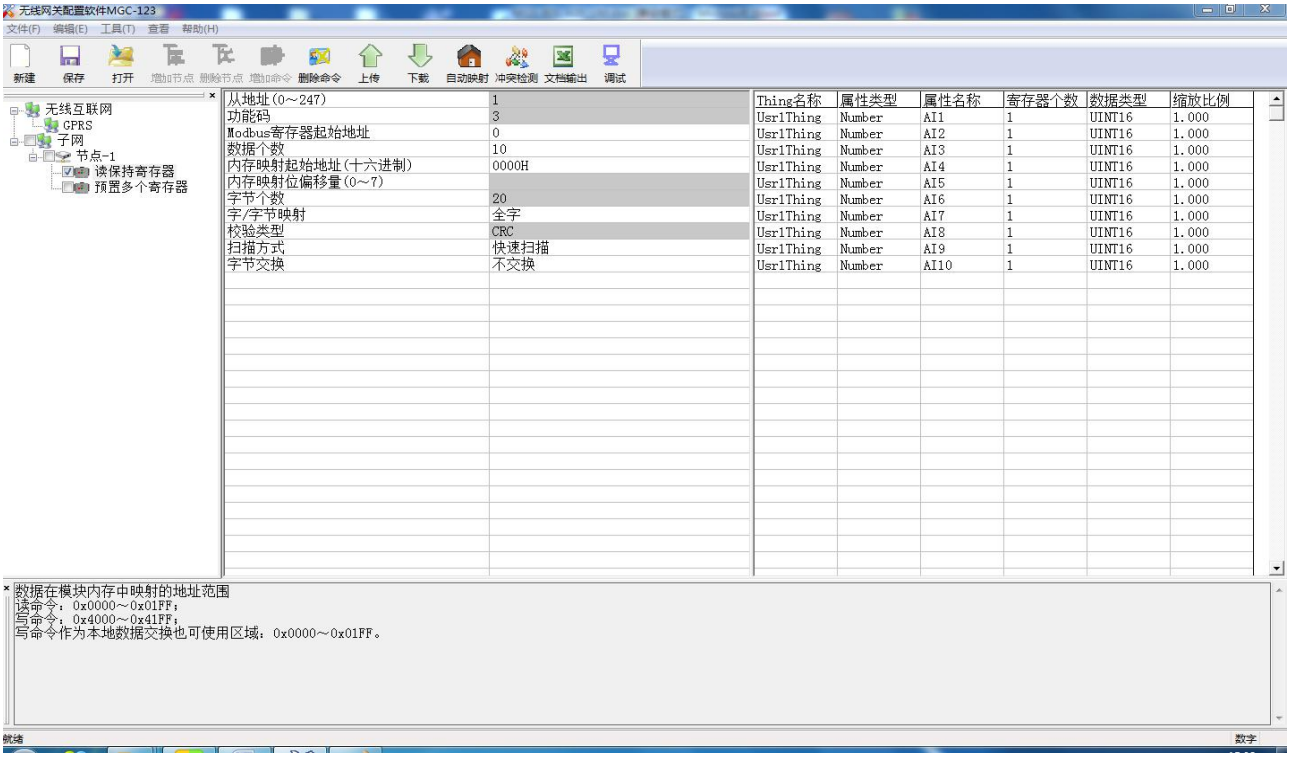
寄存器个数：可选择每个属性的寄存器个数。

数据类型：可选择每个属性的数据类型，暂时支持无符号 16 位与有符号 16 位。

缩放比例：可由用户根据实际情况的单位来确定缩放比例。

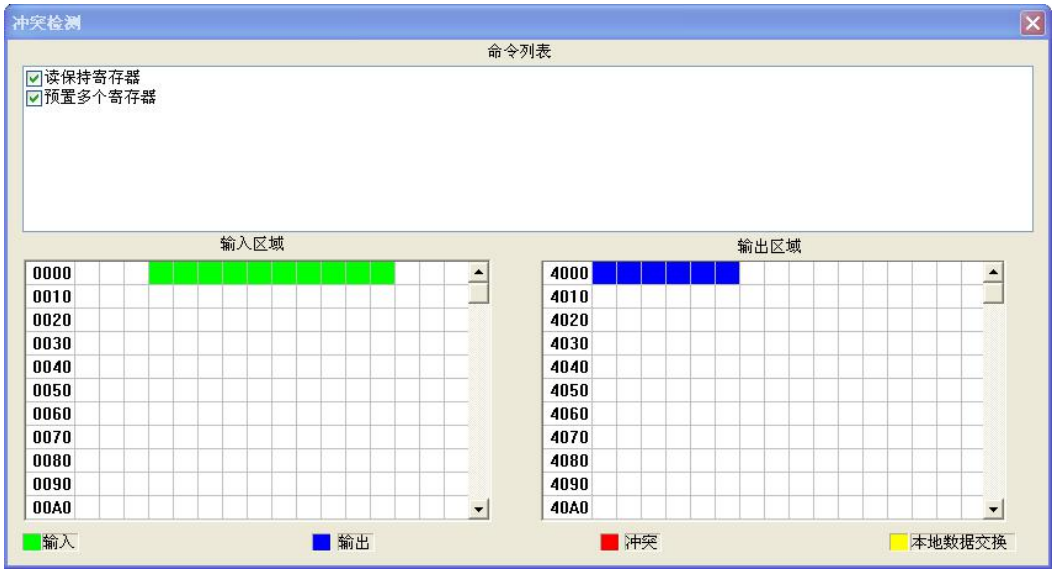
5.4.6 注释视图

注释视图显示相应配置项的解释。如配置内存映射起始地址时，注释视图显示如下：



5.5 冲突检测

用于检测“内存映射数据”是否有冲突，若发现冲突的情况，可及时做调整。视图显示如下：



5.5.1 命令列表操作

在命令列表视图显示所有配置的命令，每条命令前的选中框，用于在内存映射区检查该条命令所占内存映射位置。单击某条命令，使选中框打勾，在内存映射区会显示相应命令所占空间位置，再次单击该命令，去掉选中框勾，命令不在映射区显示所占空间。该功能可用于命令间内存映射区的冲突检测。

5.5.2 内存映射区操作

内存映射区分输入区域和输出区域：

输入映射地址从 0x0000～0x3FFF；

输出映射地址从 0x4000～0x7FFF。

每个方格代表一个字节地址。

绿色：读命令在输入映射区显示，无冲突时呈绿色；

黄色：写命令当地址映射区位于输入区，无冲突时呈黄色；

蓝色：当地址映射区位于输出区，无冲突时呈蓝色；

红色：在输入区或输出区，不同命令占用同一字节地址，该字节区域呈红色。

对于位操作指令，以上色格显示含义同样适用。

单击输入输出区域方格，该方格对应字节的各个位显示是否被占用，如下图所示：

上图指的是第二个字节中的第一位数据有冲突。

5.6 上载下载配置

硬件通讯菜单项如下：

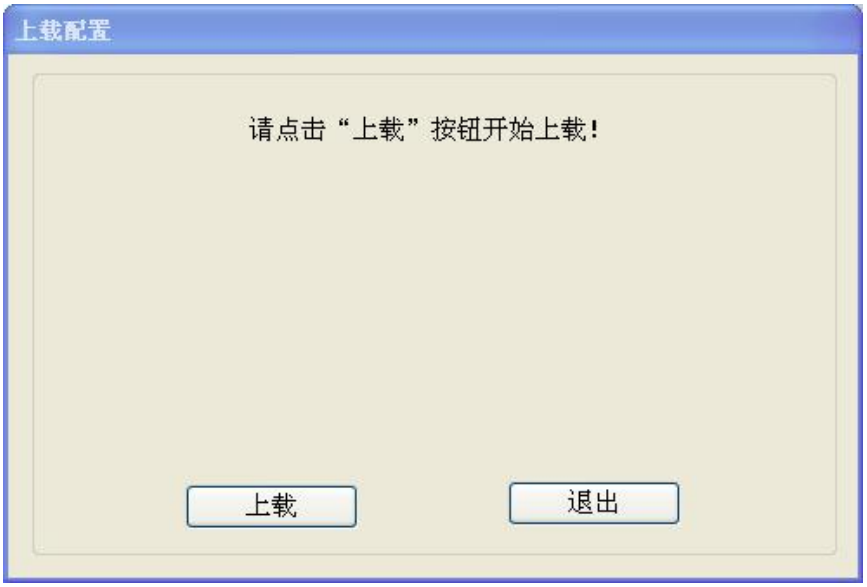
5.6.1 串口配置

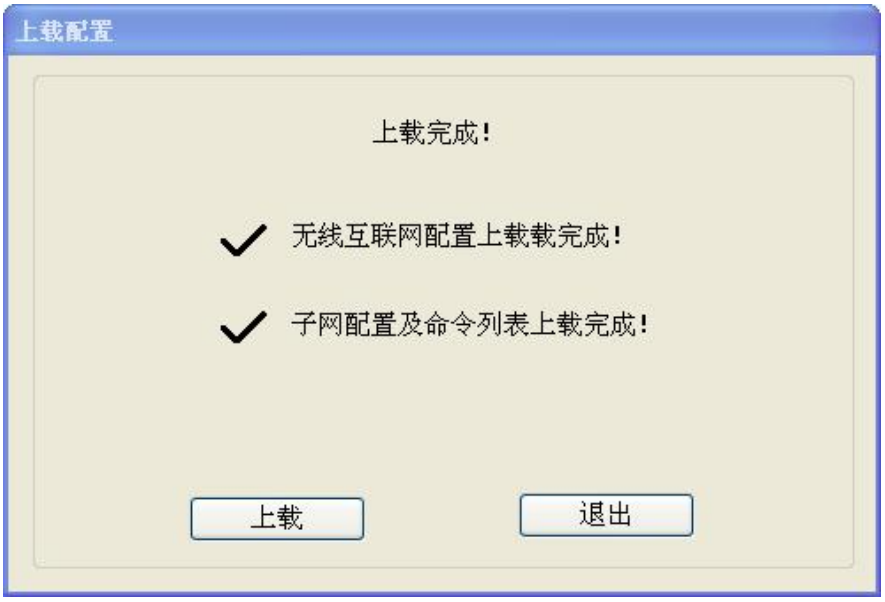
本软件自动扫描系统可用串口，并在串口列表中列出可用串口。修改完所有设置项后，按“确定”保存设置。

备注：除端口号以外，其余参数为固定数值：115200，无，8，1。

5.6.2 上载配置

选择上载配置，将网关配置信息从设备上载到软件中，显示界面如下：



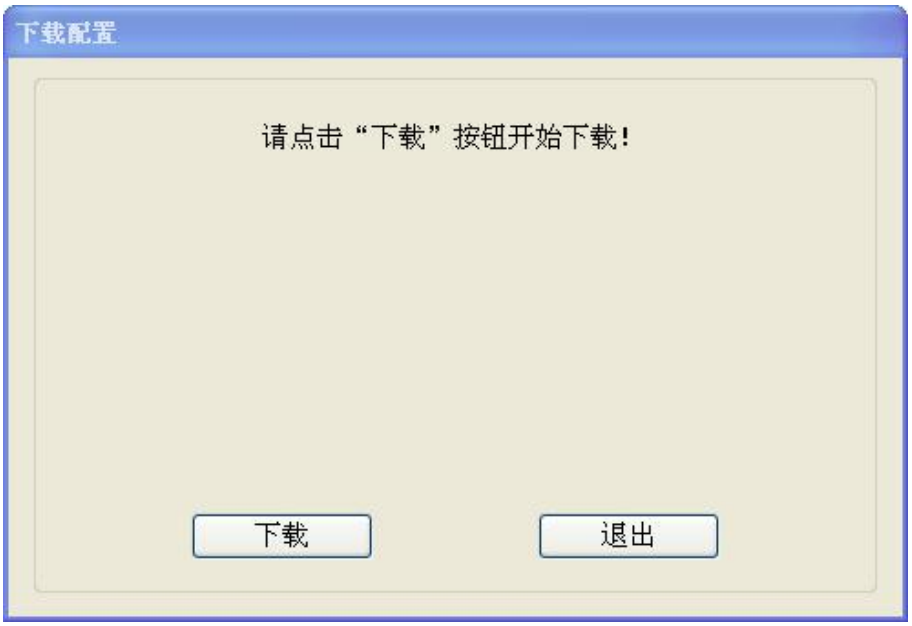


备注：在上载配置之前，请先检查“串口配置”中端口号是否为正在使用的串口。

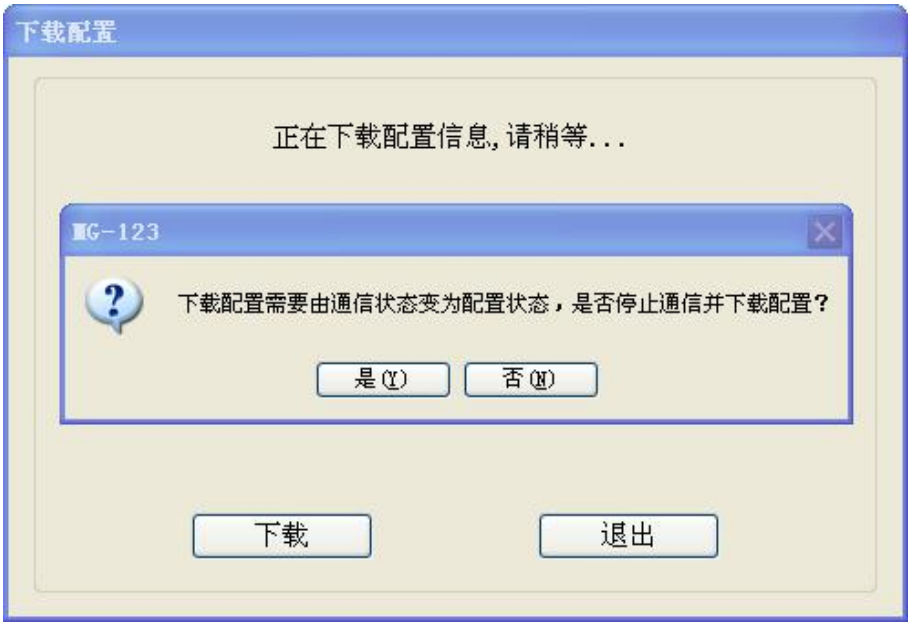
5.6.3 下载配置

选择下载配置，将配置好的网关信息下载到网关设备，显示界面如下：

选择正确的端口，点击确定：

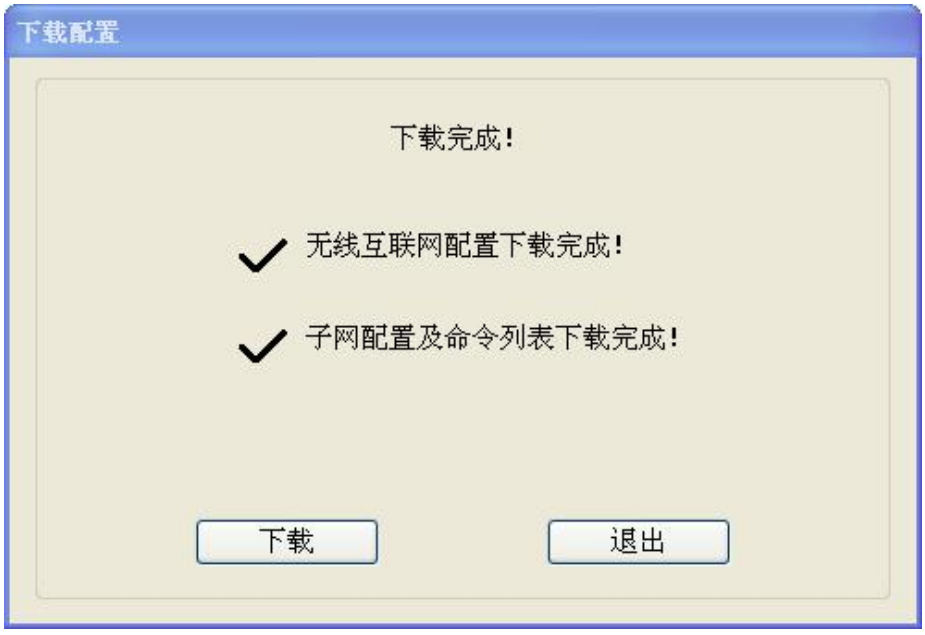


点击下载：



点击是：

点击是：



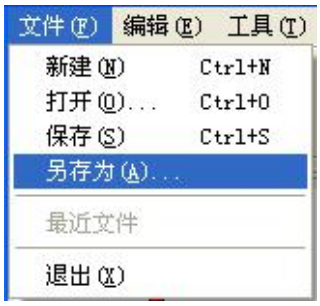
备注 1：在下载配置之前，请先检查“串口配置”中端口号是否为正在使用的串口。

备注 2：在下载之前，请先确认所有的配置已经完成。

5.7 加载和保存配置

5.7.1 保存配置工程

选择“保存”，可以将配置好的工程以.sibomg 文档保存。

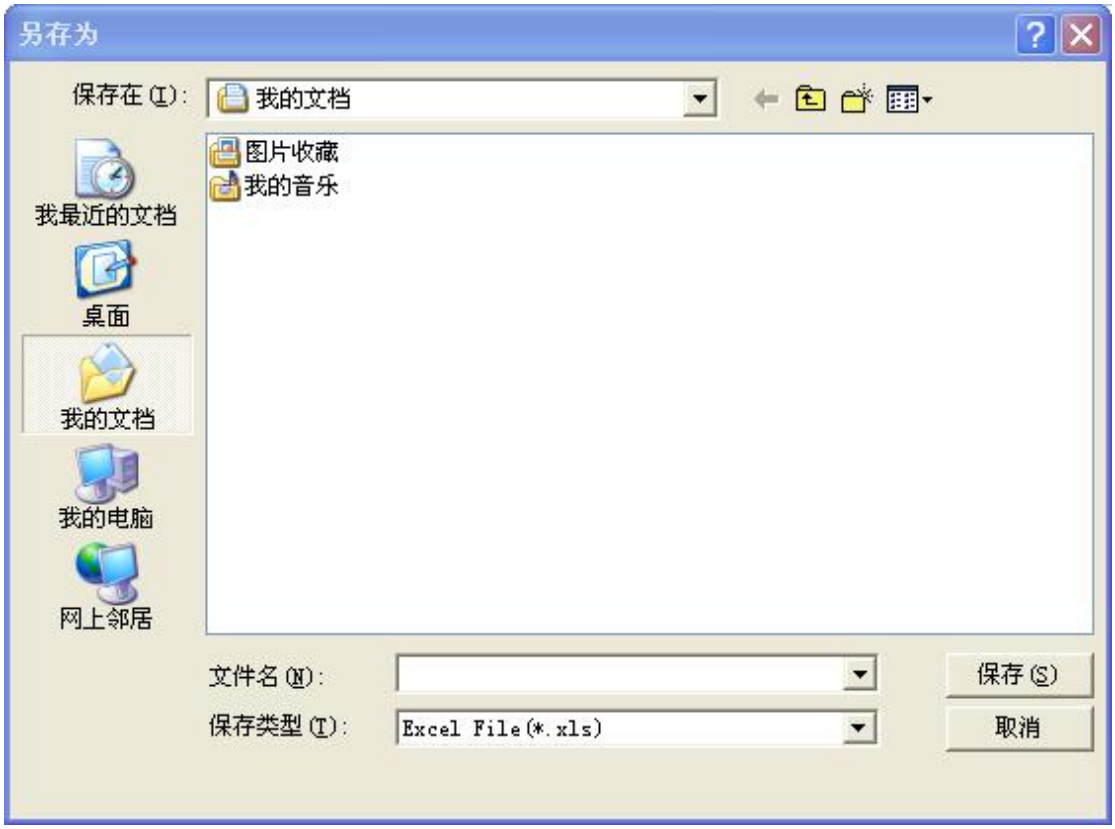


5.7.2 加载配置工程

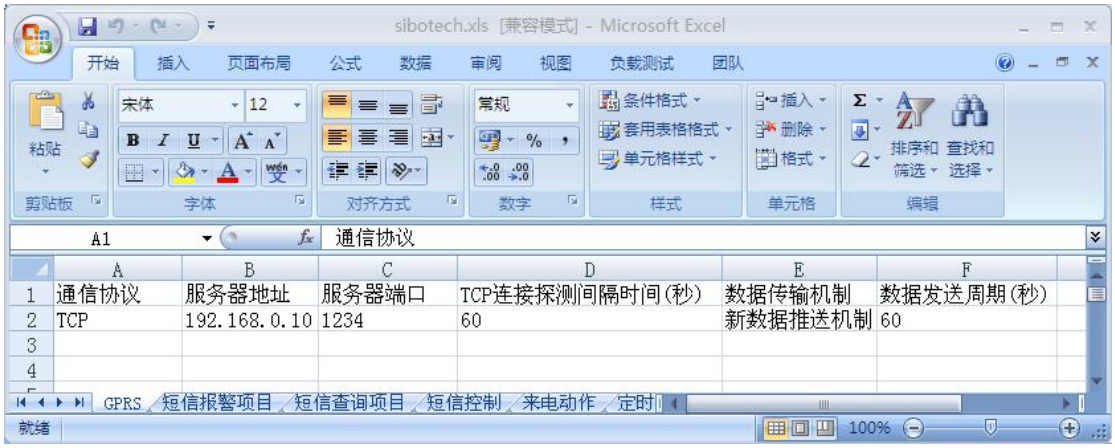
选择“打开”，可以将以保存的.sibomg 文件打开。

5.8 EXCEL 文档输出

配置文档输出有助于用户查看相关配置, 使用此功能前请确保电脑上安装有 Microsoft Excel。



保存成功后将自动打开, 如下所示：



保存的 xls 有 GPRS、子网、主站命令、属性 4 个部分

GPRS：无线互联网，GPRS 参数

子网：Modbus 通信参数

主站命令：Modbus 命令及相关参数

5.9 自动映射

自动映射功能是软件自动计算并填写每条命令的内存映射起始地址参数，自动映射后内存映射起始地址没有冲突。

5.10 调试功能

状态：显示与从站的通信状态，响应正确、响应超时、响应异常、响应错误

从站地址：配置文件中配置的从站地址（仅主站、十六进制）

功能码（命令）：配置文件中配置的 Modbus 命令（仅主站、十六进制）

起始地址：配置文件中配置的“Modbus 寄存器起始地址”（仅主站、十六进制）

数据/异常代码：显示读取到的从站数据或异常代码（十六进制）

注：当配置为 Modbus 主站时，才会显示从站地址、功能码、起始地址。

读取到的数据：显示最新接收到的数据（十六进制）

内存映射地址：数据写入网关内存的起始地址（十六进制）

数据：要写入网关内存的数据（十六进制）

当用户填充正确的“内存映射地址”和“数据”后，可以点击“发送”按钮把数据包发送出去。

保存内容/停止保存：软件支持用户将调试数据保存到本地硬盘，当保存结束时，需要点击“停止保存”使保存生效。

停止显示/继续显示：软件支持动态或者静态显示调试数据。

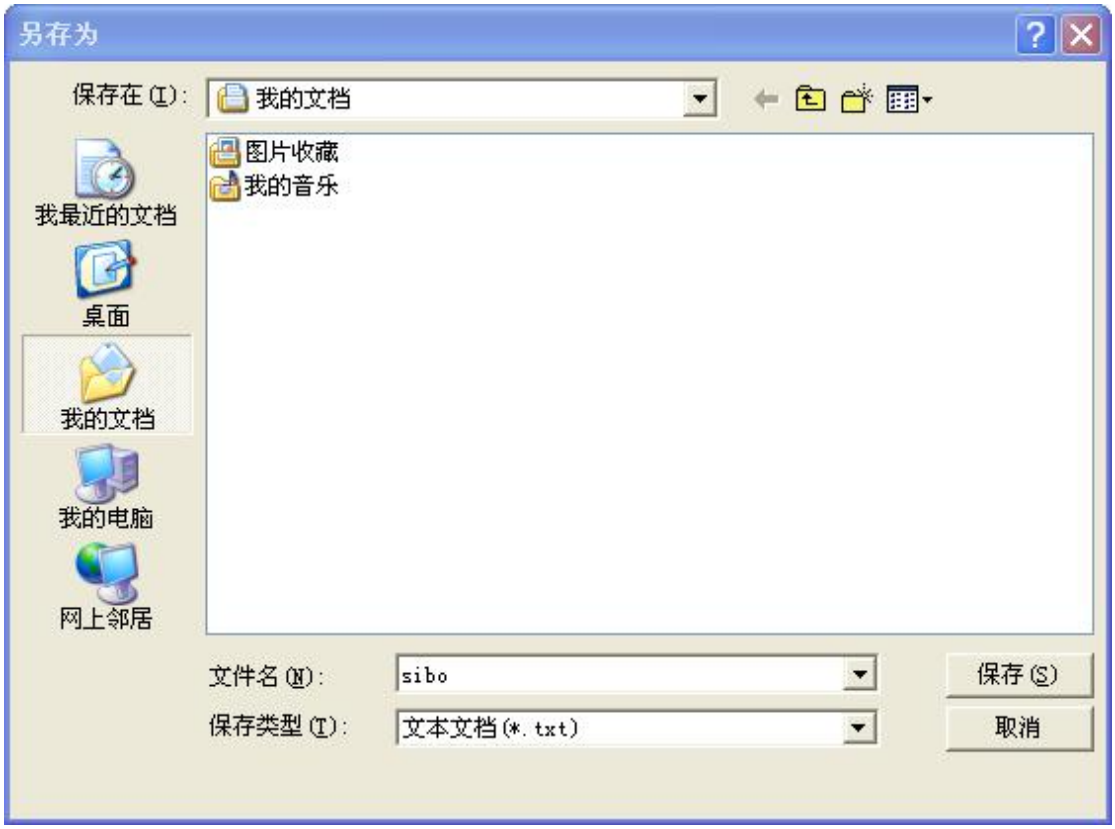
清空数据：点击该按钮，则将当前调试界面的数据清空。

结束调试并退出：点击该按钮或者调试界面的关闭按钮，即可将当前调试界面关闭。

强制退出：当软件不能区分调试信息是否结束时的一种退出机制。如调试过程中网关被断电等其它情况。

响应正确

保存数据功能可以将监视到的数据保存到文本文档，以供需要时查看。



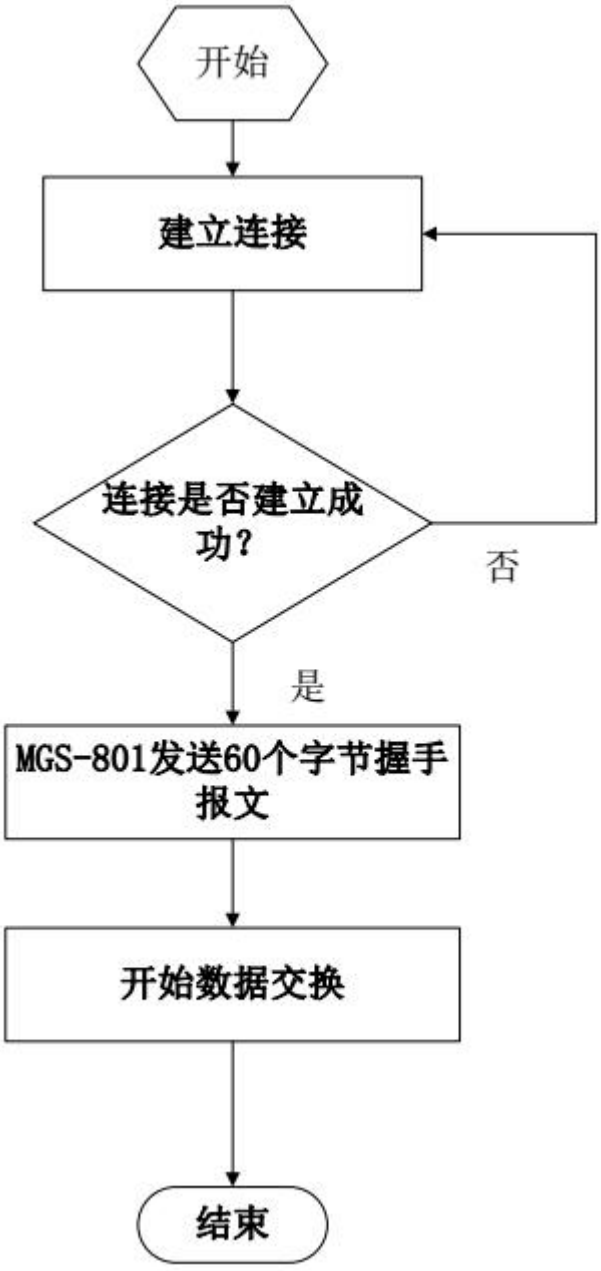
手动打开保存的 txt 文档查看内容：

注意： 当完成配置后，需要将配置文件（扩展名.sibomg）保存后登录到泗博的文件提交管理平台并上传-申请运行，设备即可与博凯云建立连接并进行数据交换。

六、数据传输

6.1 握手报文

握手报文流程图，内容如下：

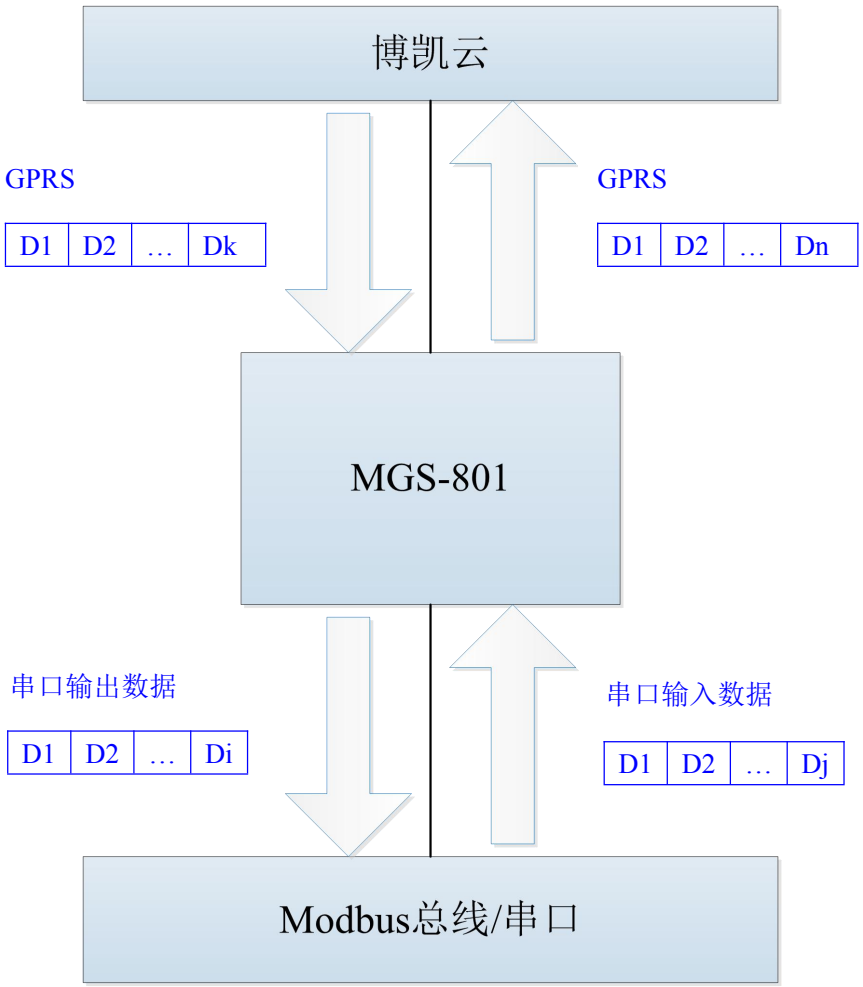


MGS-801 与博凯云（服务端）建立 TCP 连接后，MGS-801 就会发送握手报文进行身份验证，握手报文采用 AES 加密。

6.2 数据交换

本网关实现串口（Modbus）与 GPRS 之间的数据交换。

数据交换如下图所示：

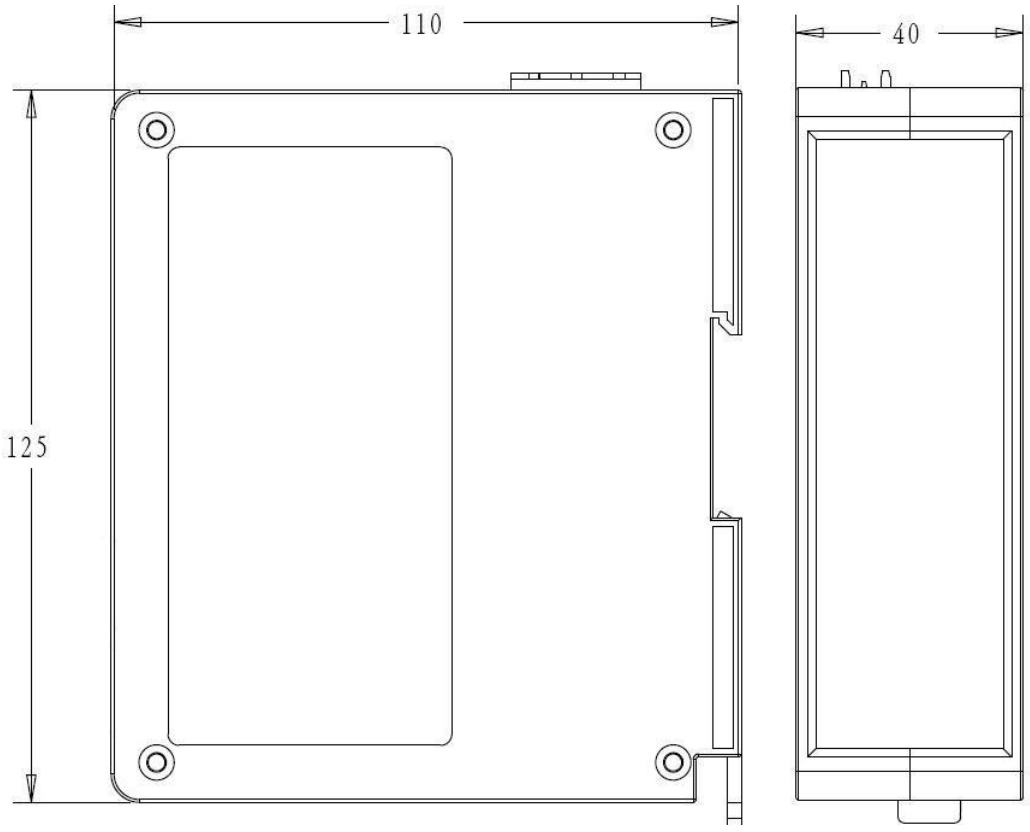


D1 ~ Di 是串口发送数据； D1 ~ Dj 是串口接收数据。为了 GPRS 节省流量，Modbus 主站模式的 GPRS 数据带有帧头，用于识别和控制数据，通过 GPRS 传输的数据采用 AES 加密，且密钥是动态的。

七、安装

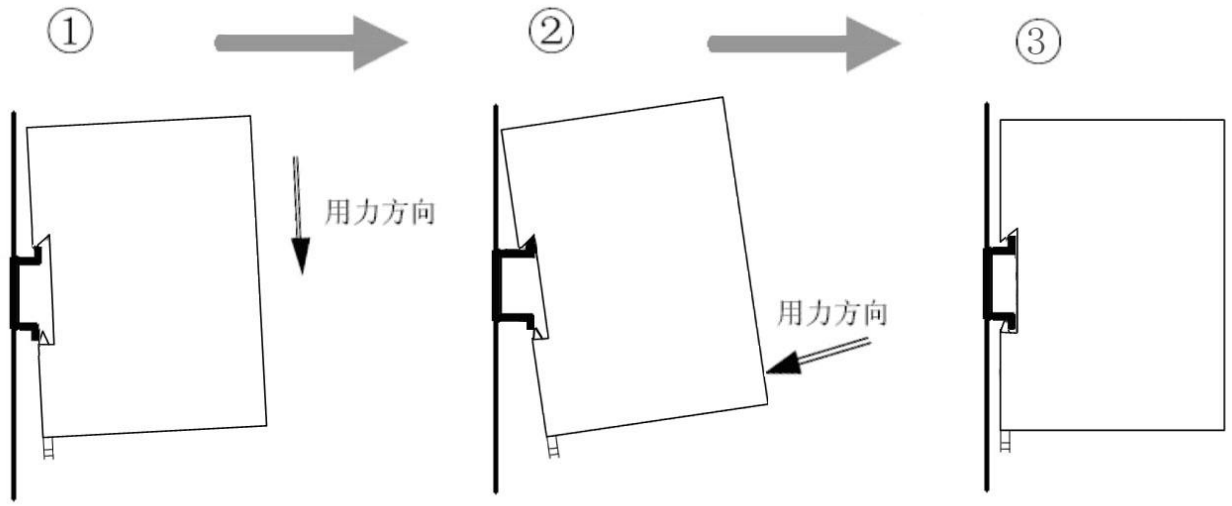
7.1 机械尺寸

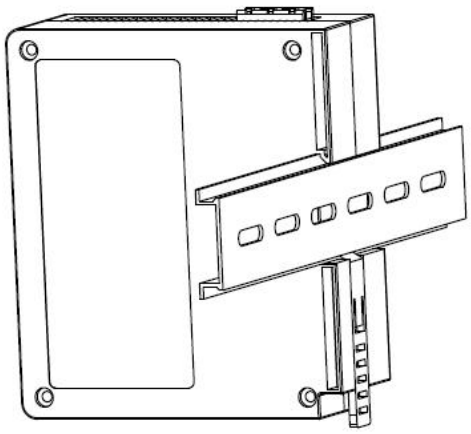
尺寸： 40mm（宽）×125mm（高）×110mm（深）



7.2 安装方法

35mm DIN 导轨安装





八、运行维护及注意事项

- 模块需防止重压，以防面板损坏；
- 模块需防止撞击，有可能会损坏内部器件；
- 供电电压控制在说明书的要求范围内，以防模块烧坏；
- 模块需防止进水，进水后将影响正常工作；
- 上电前请检查接线，有无错接或者短路。

九、修订记录

时间	修订版本	修改内容
2017-12-06	A	V2.1_Rev A 新发布，支持接入到博凯云、支持远程更新程序。
2018-8-8	A	修改主版本为产品版本，删除“仅限”，上一个版本 V2.1_Rev A
2019-07-30	A	版本升级为 V2.4,；修改内容为：无线物联网配置参数中增加 APN 设置。

十、版权信息

本说明书中提及的数据和案例未经授权不可复制。泗博公司在产品的发展过程中，有可能在不通知用户的情况下对产品进行改版。

SiboTech® 是上海泗博自动化技术有限公司的注册商标。

该产品有许多应用，使用者必须确认所有的操作步骤和结果符合相应场合的安全性，包括法律方面，规章，编码和标准。

十一、相关产品

本公司其它相关产品包括：

GMT-881，MGS-803，IOT-860，IOT-861 等

获得以上几款产品的说明，请访问公司网站 www.sibotech.net，或者拨打技术支持热线：021-3126 5138。

上海泗博自动化技术有限公司
SiboTech Automation Co., Ltd.
技术支持热线：021-3126 5138
E-mail: support@sibotech.net
网址：www.sibotech.net

附录 A：Modbus 协议

Modbus RTU 协议:

说明：与本产品通讯的设备必须带有 Modbus 接口，同时设备 Modbus 协议必须符合下面的规定，本公司提供用户定制服务。

1.协议概述

物理层：传输方式：RS-485

通讯地址：0-247

通讯波特率： 可设定

通讯介质：屏蔽双绞线

传输方式：主从半双工方式。

协议在一根通讯线上使用应答式连接（半双工），这意味着在一根单独的通讯线上信号沿着相反的两个方向传输。首先，主计算机的信号寻址到一台唯一的终端设备（从机），然后，在相反的方向上终端设备发出的应答信号传输给主机。

协议只允许在主计算机和终端设备之间，而不允许独立的设备之间的数据交换，这就不会在使它们初始化时占据通讯线路，而只响应到达本机的查询信号。

一个数据帧格式:

1 位起始位，8 位数据，1 位停止位。

一个数据包格式

地址	功能码	数据	校验码
8-Bits	8-Bits	N x 8-Bits	16-Bits

协议详细定义了校验码、数据序列等，这些都是特定数据交换的必要内容。

当数据帧到达终端设备时，它通过一个简单的“口”进入寻址到的设备，该设备去掉数据帧的“信封”（数据头），读取数据，如果没有错误，就执行数据所请求的任务，然后，它将自己生成的数据加入到取得的“信封”中，把数据帧返回给发送者。返回的响应数据中包含了以下内容：终端从机地(Address)、被执行了的命令(Function)、执行命令生成的被请求数据(Data)和一个校验码(Check)。发生任何错误都不会有成功的响应。

地址（Address）域

地址域在帧的开始部分，由 8 位（0～255）组成，这些位标明了用户指定的终端设备的地址，该设备将接收来自与之相连的主机数据。每个终端设备的地址必须是唯一的，仅仅被寻址到的终端会响应包含了该地址的查询。当终端发送回一个响应，响应中的从机地址数据便告诉了主机哪台终端正与之进行通信。

功能（Function）域

功能域代码告诉了被寻址到的终端执行何种功能。表 1－1 列出了所有的功能码、它们的意义及它们的初始功能。

表 1－1 功能码

代码	意义	行为
03	读数据	获得一个或多个寄存器的当前二进制值
06	预置单寄存器	放置一个特定的二进制值到一个单寄存器中
16	预置多寄存器	放置特定的二进制值到一系列多寄存器中

数据域

数据域包含了终端执行特定功能所需要的数据或者终端响应查询时采集到的数据。这些数据的内容可能是数值、参考地址或者极限值。例如：功能域码告诉终端读取一个寄存器，数据域则需要指明从哪个寄存器开始及读取多少个数据，内嵌的地址和数据依照类型和从机之间的不同能力而有所不同。

错误校验域

该域允许主机和终端检查传输过程中的错误。有时，由于电噪声和其它干扰，一组数据在从一个设备传输到另一个设备时在线路上可能会发生一些改变，出错校验能够保证主机或者终端不去响应那些传输过程中发生了改变的数据，这就提高了系统的安全性和效率，出错校验使用了 16 位循环冗余的方法。

[注] 发送序列总是相同的 – 地址、功能码、数据和与方向相关的出错校验。

错误检测

循环冗余校验（CRC）域占用两个字节，包含了一个 16 位的二进制值。CRC 值由传送设备计算出来，然后附加到数据帧上，接收设备在接收数据时重新计算 CRC 值，然后与接收到的 CRC 域中的值进行比较，如果这两个值不相等，就发生了错误。

CRC 运算时，首先将一个 16 位的寄存器预置为全 1，然后连续把数据帧中的 8 位字节与该寄存器的当前值进行运算，仅仅每个字节的 8 个数据位参与生成 CRC，起始位和终止位以及可能使用的奇偶位都不影响 CRC。

在生成 CRC 时，每个 8 位字节与寄存器中的内容进行异或，然后将结果向低位移位，高位则用“0”补充，最低位（LSB）移出并检测，如果是 1，该寄存器就与一个预设的固定值进行一次异或运算，如果最低位为 0，不作任何处理。

上述处理重复进行，知道执行完了 8 次移位操作，当最后一位（第 8 位）移完以后，下一个 8 位字节与寄存器材的当前值进行异或运算，同样进行上述的另一个 8 次移位异或操作，当数据帧中的所有字节都作了处理，生成的最终值就是 CRC 值。

生成一个 CRC 的流程为：

预置一个 16 位寄存器为 0FFFFH（全 1），称之为 CRC 寄存器。

把数据帧中的第一个 8 位字节与 CRC 寄存器中的低字节进行异或运算，结果存回 CRC 寄存器。将 CRC 寄存器向右移一位，最高位填以 0，最低位移出并检测。

如果最低位为 0：重复第三步（下一次移位）。

如果最低位为 1：将 CRC 寄存器与一个预设的固定值（0A001H）进行异或运算。

重复第三步和第四步直到 8 次移位。这样处理完了一个完整的八位。

重复第 2 步到第 5 步来处理下一个八位，直到所有的字节处理结束。

最终 CRC 寄存器得值就是 CRC 的值。

2．应用层功能详解

第一章已经简述了协议和数据帧，使用此软件的程序员可以使用下述的方法以便通过协议正确的建立他们的特定应用程序。

本章所述协议将尽可能的使用如图 2－1 所示的格式，（数字为 16 进制）。

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量的个数高字节	变量的个数低字节	校对验码低字节	校对验码高字节
03H	03H	00H	01H	00H	03H	55H	E9H

图 2－1 协议例述

2.1 读保持寄存器（功能码 03）

查询

图 2－2 的例子是从 03 号从机读 3 个采集到的基本数据 U1，U2，U3，U1 的地址为 0001H，U2 的地址为 0002H，U3 的地址为 0003H

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量的个数高字节	变量的个数低字节	校对验码低字节	校对验码高字节
03H	03H	00H	01H	00H	03H	55H	E9H

图 2－2 读 Uca 和 Ia 的查询数据帧

响应

响应包含从机地址、功能码、数据的数量和 CRC 错误校验。

图 2－3 的例子是读取 U1，U2，U3 的响应。

地址	功能码	变量的总字节数	变量值高字节	变量值低字节	变量值高字节	变量值低字节	变量值高字节	变量值低字节	校对验码低字节	校对验码高字节
03H	03H	06H	01H	7CH	01H	7DH	01H	7CH	F9H	9BH

图 2－3 读 U1,U2,U3 的响应数据帧

2.2 预置多寄存器（功能码 10）

查询

功能码 10H 允许用户改变多个寄存器的内容，设备可从任何地址开始设置最多 16 个变量的值。控制器是以动态扫描方式工作的，任何时刻都可以改变寄存器内容。

图 2-4 是修改 3 号从站设备的负载监控 1 和负载监控 2 的动作及延时时间的设定值，其中负载监控 1 的动作设定值寄存器地址为 00 2AH，设定值为 0x07 D0，延时时间的设定值寄存器地址为 00 2BH，设定值为 0x00 0A，负载监控 2 的动作设定值寄存器地址为 00 2CH，设定值为 0x07 0D，延时时间的设定值寄存器地址为 00 2DH，设定值为 0x00 0A。

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量的个数高字节	变量的个数低字节	变量的总字节数	变量值高字节	变量值低字节	变量值高字节	变量值低字节	变量值高字节	变量值低字节	变量值高字节	变量值低字节	校对验码低字节	校对验码高字节
03H	10H	00H	2AH	00H	04H	08H	07H	D0H	00H	0AH	07H	0D0H	00H	0AH	25H	7CH

图示 2-4修改负载监控 1 和负载监控 2 的动作值及延时时间的设定值

响应

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量的个数高字节	变量的个数低字节	校对验码低字节	校对验码高字节
03	10H	00H	2AH	00H	04H	EBH	8DH

图示 2-5 修改负载监控 1 和负载监控 2 的动作值及延时时间的设定值的响应

2.3 预置单寄存器（功能码 06）

查询

功能码 06 允许用户改变单个寄存器的内容，DAE 系统内部的任何单寄存器都可以使用此命令来改变其值。既然仪器是以动态扫描方式工作的，任何时刻都可以改变单寄存器内容。

下面的例子是请求 03 号从机修改过载动作设定值 Ir1，Ir1 地址是 002EH。

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量值高字节	变量值低字节	校对验码低字节	校对验码高字节
03H	06H	00H	2EH	07H	0D0H	EBH	8DH

图示 2-6 修改过载动作设定值 Ir1

响应

对于预置单寄存器请求的正常响应是在寄存器值改变以后将接收到的数据传送回去。

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量值高字节	变量值低字节	校对验码低字节	校对验码高字节
03H	06H	00H	2EH	07H	0D0H	EBH	8DH

图示 2-7 修改过载动作设定值 Ir1