HART/ MODBUS 网关
HTM-611

产品手册
REV 1.3

上海泗博自动化技术有限公司

SiboTech Automation Co., Ltd

技术支持热线:021-5102 8348
E-mail: support@sibotech.net

目 录

1 产品概述 ..... - 4 -
1.1 产品功能 ..... - 4 -
1.2 产品特点 ..... - 4 -
1.3 技术指标 ..... - 4 -
1.4 本安防爆特性 ..... - 5 -
1.5 相关产品 ..... - 5 -
2 快速应用举例 ..... - 6 -
2.1 网关参数配置 ..... - 6 -
2.1.1 配置前连接设置 ..... - 6 -
2.1.2 软件配置 ..... - 6 -
2.2 功能演示 ..... - 9 -
3 硬件说明 ..... - 10 -
3.1 产品外观 ..... - 10 -
3.2 指示灯 ..... - 11 -
3.3 配置开关/按钮 ..... - 11 -
3.3.1 状态设置开关 ..... - 11 -
3.3.2 MODBUS 地址设置按钮 ..... - 12 -
3.3.3 内/外采样电阻切换开关 ..... - 12 -
3.4 接口 ..... - 13 -
3.4.1 电源接口 ..... - 13 -
3.4.2 RS-485/RS-422 接口 ..... - 13 -
3.4.3 RS232 接口 ..... - 14 -
3.4.4 HART 接口 ..... - 15 -
3.5 HTM-611 与现场设备的拓扑 ..... - 16 -
4 软件使用说明 ..... - 18 -
4.1 软件界面说明 ..... - 18 -
4.2 软件功能说明 ..... - 20 -
4.2.1 与硬件的连接 ..... - 20 -
4.2.2 上载网关配置 ..... - 20 -
4.2.3 配置现场总线 ..... - 20 -
4.2.4 配置 HART 总线 ..... - 22 -
4.2.5 冲突检测 ..... - 25 -
4.2.6 自动内存映射 ..... - 26 -
4.2.7 下载配置 ..... - 27 -
4.2.8 内存数据显示功能 ..... - 27 -
4.2.9 诊断 ..... - 27 -
4.2.10 串口调试 ..... - 30 -

4.2.11 转换工具 ..... - 31 -
5 工作原理 ..... - 33 -
5.1 执行一条 HART 命令的流程图 ..... - 36 -
5.2 通用收发数据 ..... - 36 -
5.3 触发命令 ..... - 37 -
5.4 与 MODBUS 的数据交换 ..... - 37 -
6 安装 ..... - 38 -
6.1 机械尺寸 ..... - 38 -
6.2 安装方法 ..... - 38 -
7 运行维护及注意事项 ..... - 40 -
8 版权信息 ..... - 41 -
附录 A：MODBUS 协议 ..... - 42 -
附录 B：HART 协议 ..... - 46 -
物理层 ..... - 46 -
数据链路层 ..... - 46 -
帧结构 ..... - 47 -
应用层 ..... - 48 -
附录 C：HART 常用命令 ..... - 49 -

1 产品概述

1.1 产品功能

HTM-611 是一款实现 HART 与 MODBUS 数据通信的网关。HART 一侧可配置为第一主站或第二主站，MODBUS 一侧做从站。

1.2 产品特点

- 应用简单：用户只需参考产品手册及应用实例，根据要求配置即可在短时间内实现通信。
- 功能强大：支持 HART 与 MODBUS 之间的互联、HART 与串口数据的透明传输。
- 丰富的调试功能：数据交换的直观显示、HART 从站的命令诊断以及通用调试等功能极大的方便了用户的通信测试。

1.3 技术指标

[1] HART 可作为第一主站或第二主站

[2] 支持 1 个 HART 通道，多点模式下使用网关内置电阻支持连接 13 台仪表，使用外部电阻（250Ω）支持连接 15 台仪表

[3] 支持 HART 单点工作模式和多点工作模式

[4] 单点工作模式下，支持从站设备数据的突发操作

[5] 支持 HART 协议所有命令

[6] 每条 HART 命令可配置为逢变输出、轮询输出、初始化输出或不输出

[7] HART 每通道最多支持 128 条用户命令，HART 输出数据缓冲区高达 1000 字节，输入数据缓冲区高达 1600 字节

[8] 可选择使用内部或外部采样电阻

[9] 串口是 RS232、RS485、RS232 可选，波特率：300、600、1200、2400、9600、19.2K、38.4K、57.6K、

115.2Kbps 可选

[10] 串口侧可配置为 MODBUS 从站，支持功能码：03H、04H、06H、10H

[11] MODBUS 从站支持 RTU 和 ASCII 通信方式

[12] 串口可配置为通用模式，能够与 HART 从站设备进行数据透明传输。

[13] **供电：24VDC（9V-30V），80mA（24V DC）；**

[14] 工作环境温度：-20℃～60℃，相对湿度 5%～95%（无凝露）；

[15] 外形尺寸：40mm（宽）×125mm（高）×110mm（深）；

[16] 安装：35mm 导轨；

[17] 防护等级：IP20；

1.4 本安防爆特性

HTM-611 为非本安防爆产品，使用时请放置于控制室内。

1.5 相关产品

本公司其它相关产品包括：

HPM-610，PM-160，EPS-320MP 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：021-5102 8348

2 快速应用举例

以下以“MODBUS 主站模拟软件通过 HTM-611 读取设备短地址为 0 的主变量的瞬时值（PV）”为例介绍网关 HTM-611 的使用过程。

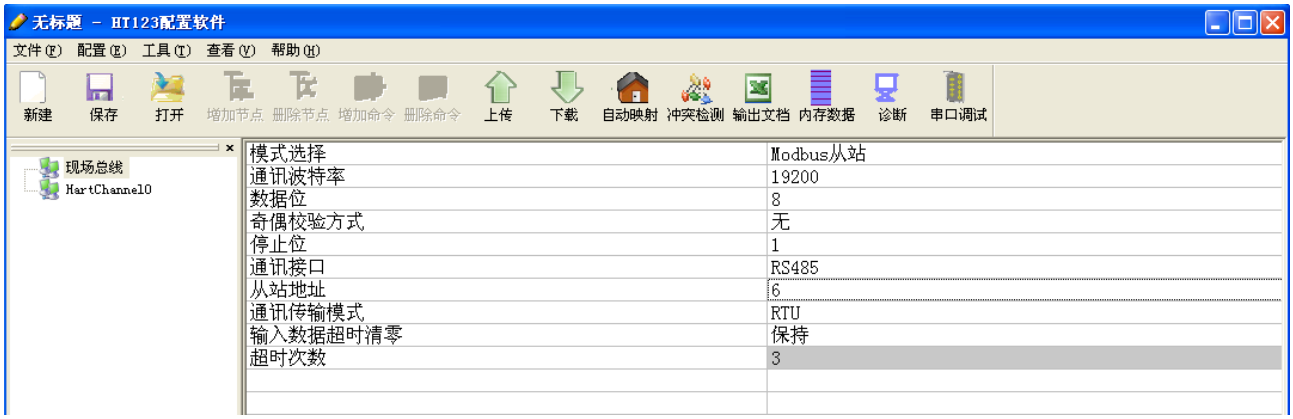
2.1 网关参数配置

2.1.1 配置前连接设置

1. 将网关的配置拨码开关拨至“ON”；
2. 用串口线将网关的 232 接口和电脑的串口相连，接线方法请见本说明书 3.4.3 章节；
3. 给网关上电，此时数码管显示“CF”，表明网关处于配置状态。双击已安装的软件图标 HT-123 即可开始对网关进行配置。

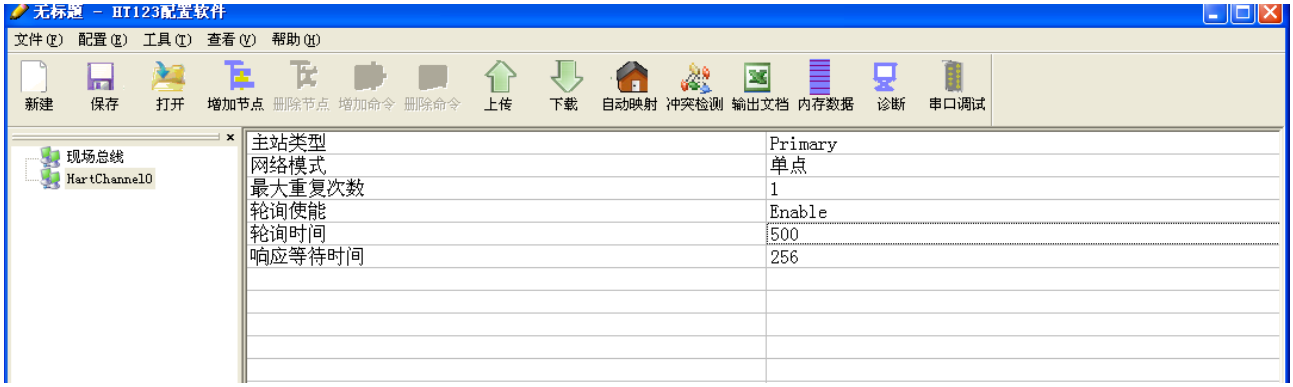
2.1.2 软件配置

1. 打开电脑内安装的 HT-123 软件。
2. 点击左侧树视图中的“现场总线”， 右侧出现的配置表按下图所配：



配置完成后按回车确认。

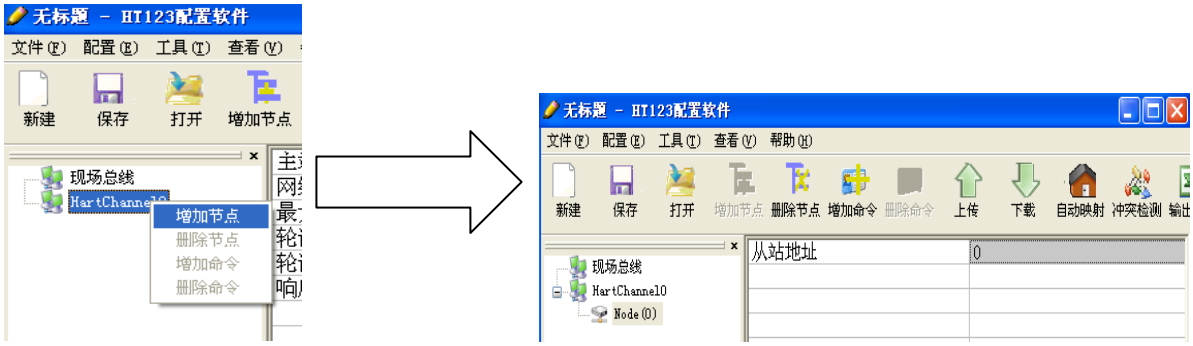
3. 单击左侧树视图的 HartChannel0，右侧出现的配置表按下图所配：



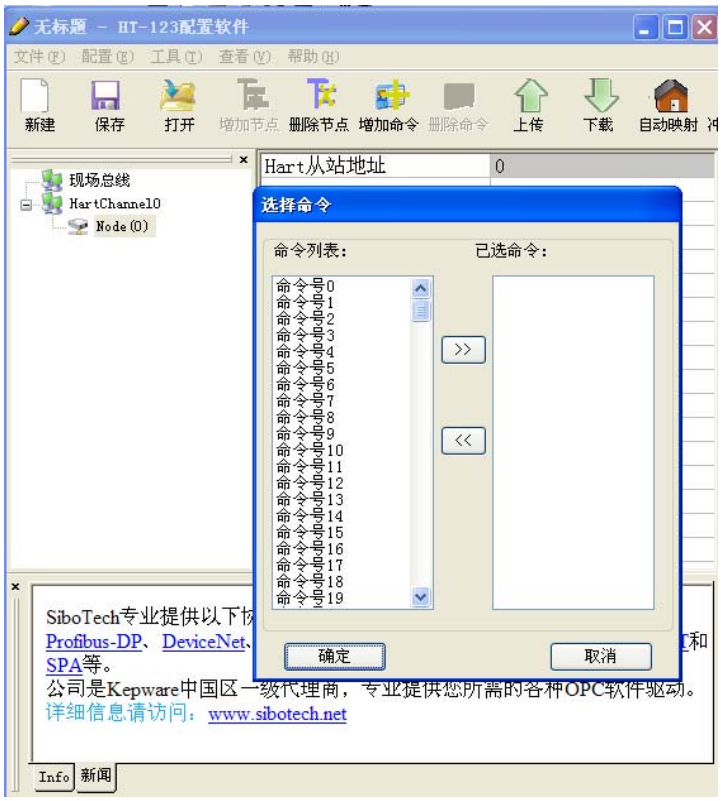
配置完成后，按回车键确认。

注：HART 协议中，规定从站地址为 0 的设备工作在单点模式，此时允许数字通讯和模拟通讯同时存在。从站地址为 1~15 的设备工作在多点模式，此时设备的模拟输出为最小值（如 4mA），只能进行数字通讯。协议同时规定现场设备出厂前的地址默认配置为 0 号。

4． 右击 HartChannel0，在弹出的菜单中选择“增加节点”，如下图：



5． 右击：“Node（0）”，在弹出的菜单中选择增加命令，在弹出的对话框中添加 1 号命令（命令号 1），然后确定返回。



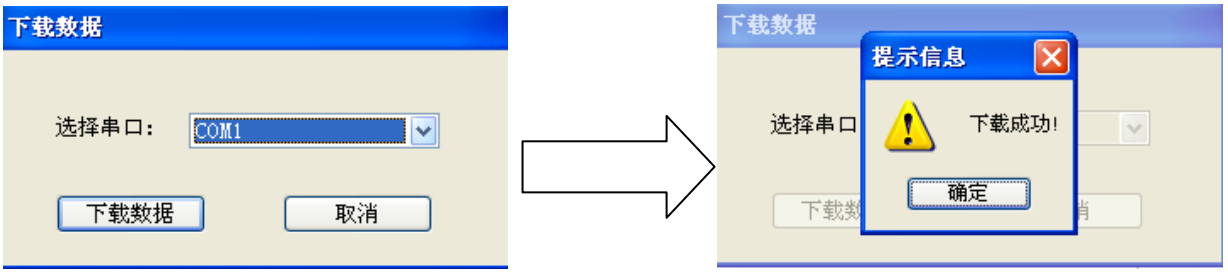
6. 点击“命令号 1”, 右侧出现的配置表按下图所配：

输出方式	轮询输出
发送数据内存起始地址	3000
发送数据的Modbus寄存器起始地址	0
发送数据长度(BYTE)	0
发送数据长度(WORD)	0
接收数据内存起始地址	0
接收数据的Modbus寄存器地址	0
接收数据长度(BYTE)	7
接收数据长度(WORD)	3
命令索引值	0

然后按回车确定。

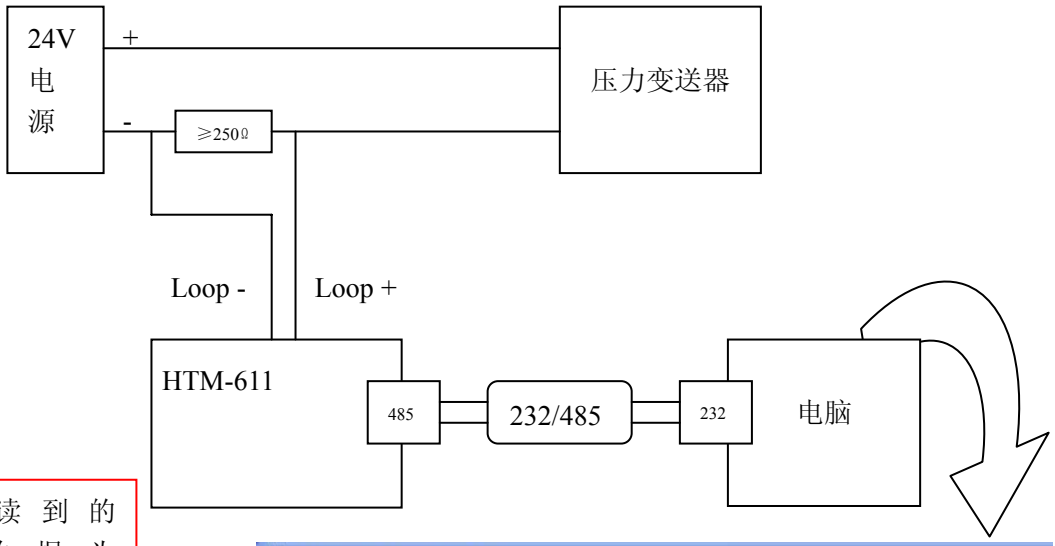
7. 点击

图标，在弹出的对话框选择网关所连接的电脑串口，然后点击下载：

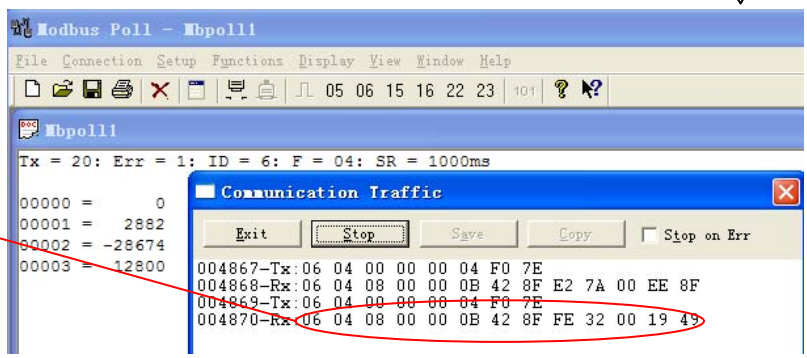


2.2 功能演示

网关的 HART 接口连接一台从站地址为 0 的 2 线制压力变送器，485 接口通过 485/232 转换器连接到电脑，电脑中用设置好的 MODBUS POLL 软件来模拟一个 MODBUS 主站，这样在数据交换窗口中即可看到压力变送器的主变量值：

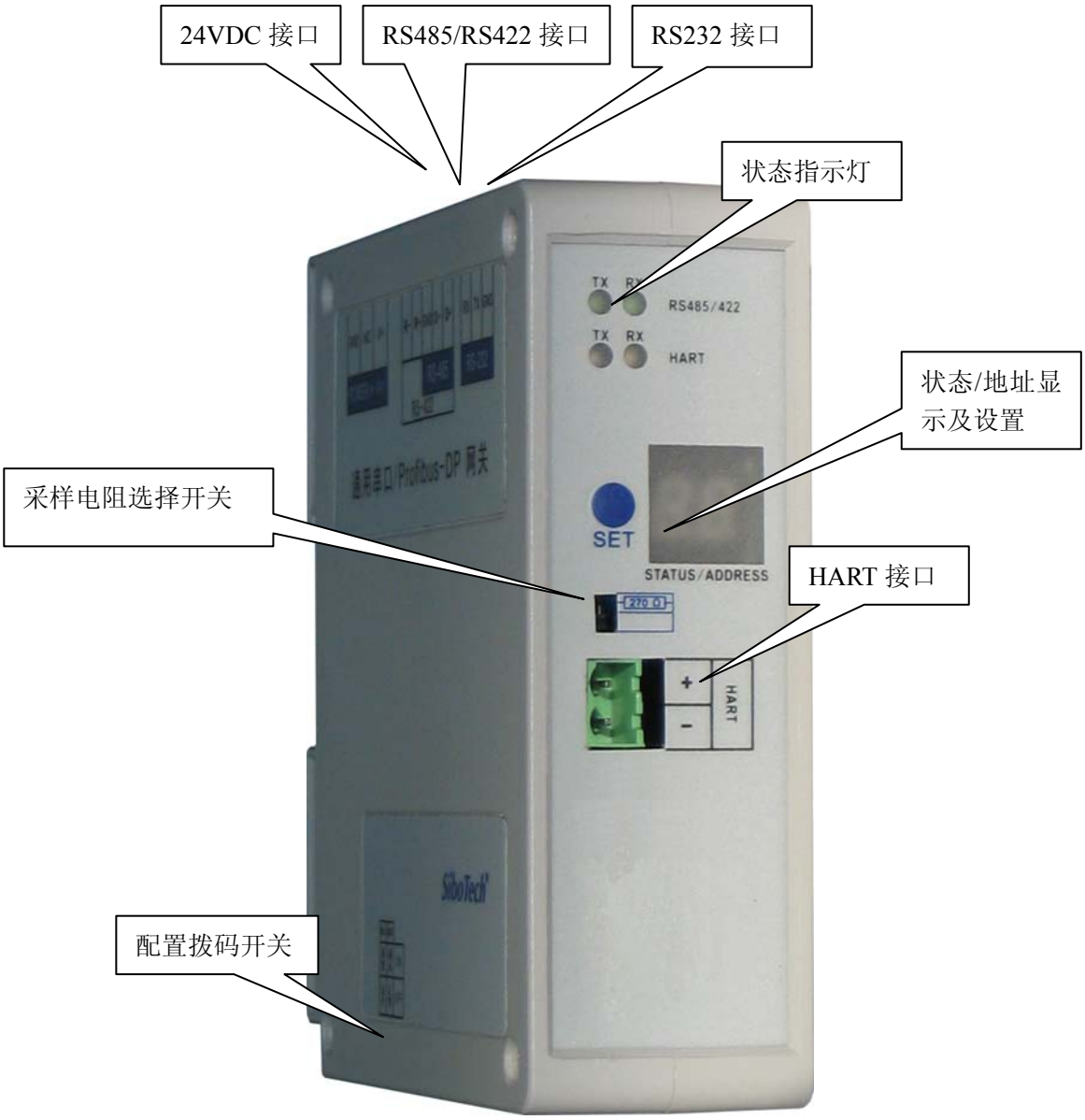


Modbus 读到的 HART 数据为“00,00,0B,42,8F,FE,32”其中前面两个“00”表示设备状态为正常，”0B”表明压力单位是 psi，“42,8F,FE,32”表示压力值，大小为 71.9964752197266（psi）。



3 硬件说明

3.1 产品外观



注：此图仅供参考，产品外观应以实物为准。

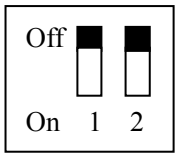
3.2 指示灯

指示灯	状态	状态说明
PBF	保留	保留
	保留	保留
STA	保留	保留
	保留	保留
TX	闪烁	总线有数据在发送
	灭	无数据发送
RX	闪烁	总线有数据在接收
	灭	无数据接收

3.3 配置开关/按钮

3.3.1 状态设置开关

配置开关位于产品下方，位 1 为调试位，位 2 为配置位。



调试（位 1）	配置（位 2）	说明
Off	Off	运行模式
Off	On	配置模式
On	Off	调试模式
On	On	配置模式

注意：①重新设置配置开关后须重新启动 HTM-611，使设置生效！

②设置为调试模式之后，“MODBUS 从站”或“通用模式”将被强制指定 RS485 接口为通信口，RS232 接口为调试接口。

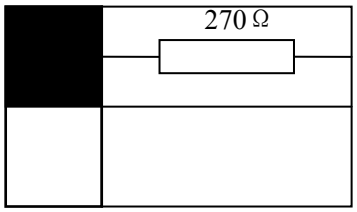
③配置接口使用 RS232 接口。

3.3.2 MODBUS 地址设置按钮

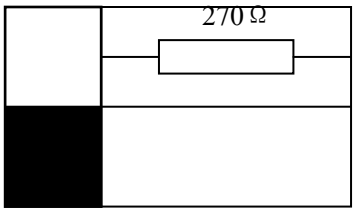
在 HTM-611 正常工作状态下，快速按两次按键，此时数码管显示的地址高位开始闪烁，单按按键即可设置 MODBUS 地址的高位；再长按按键 3 秒，数码管显示的地址低位开始闪烁，单按按键即可设置 MODBUS 地址的低位。最后长按按键 3 秒，地址闪烁三次表明设置成功。在进入设置地址状态后，如果十秒内没有按下按键则自动退出设置地址状态并继续显示原来的地址。MODBUS 地址的可设置范围为：0~99（十进制）。

3.3.3 内/外采样电阻切换开关

HPM-610 产品可供用户选择使用内部采样电阻还是外部采样电阻来取得 HART 信号，内部电阻规格为 270Ω，2W。当采样电阻上的功率超过 2W 时，必须使用外部电阻。



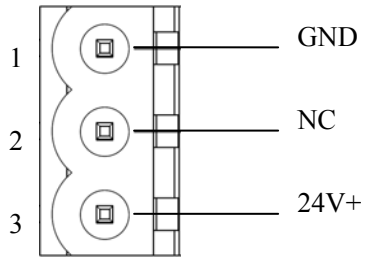
开关拨至上方，使用内部采样电阻



开关拨至下方，使用外部采样电阻

3.4 接口

3.4.1 电源接口



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

3.4.2 RS-485/RS-422 接口

HTM-611 产品的 485 接口是标准的 RS-485 接口，以下简述本产品 RS-485 特性：

3.4.2.1 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。

3.4.2.2 RS-485 传输设备安装要点

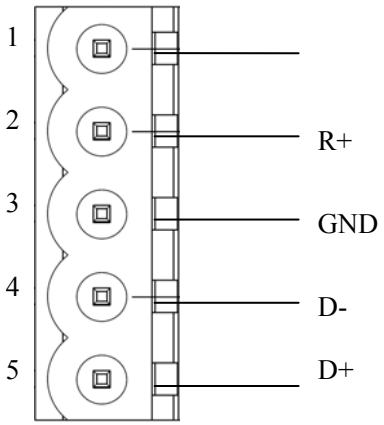
① 全部设备均与 RS-485 总线连接；

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。

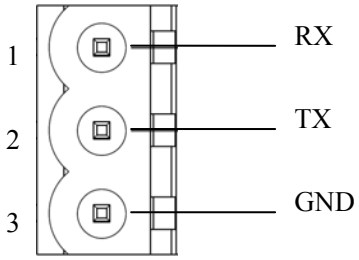
五针端子：



引脚	功能
1	R-，RS-422 接收-
2	R+，RS-422 接收+
3	GND
4	D-，RS-485/RS-422 发送-
5	D+，RS-485/RS-422 发送+

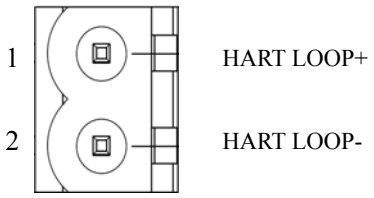
3.4.3 RS232 接口

HTM-611 产品的 RS232 接口采用开放式 3 针可插拔端子，其引脚描述如下：



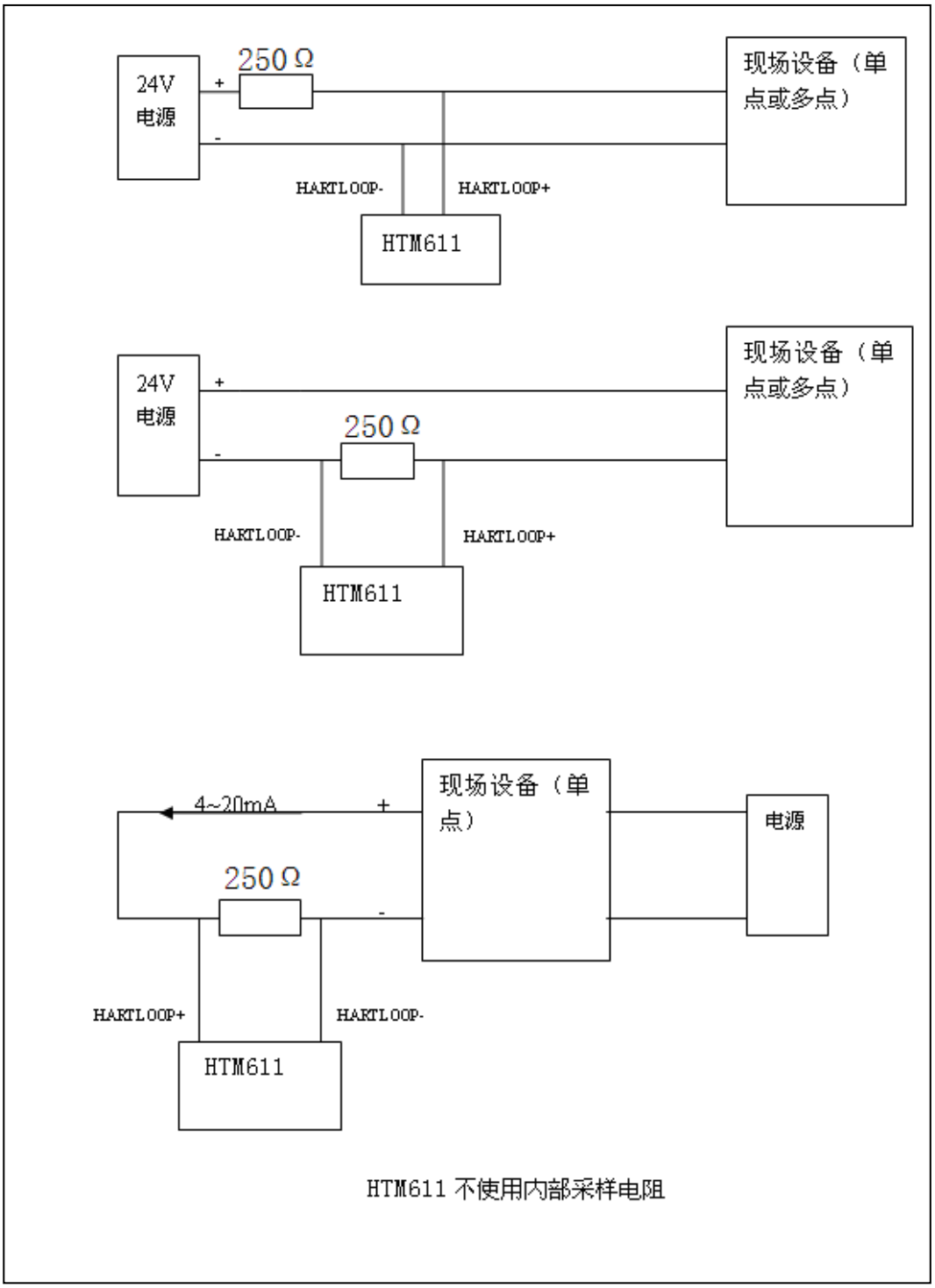
引脚	功能
1	RX，接用户设备 RS232 的 RX
2	TX，接用户设备 RS232 的 TX
3	GND，接用户设备 RS232 的 GND

3.4.4 HART 接口

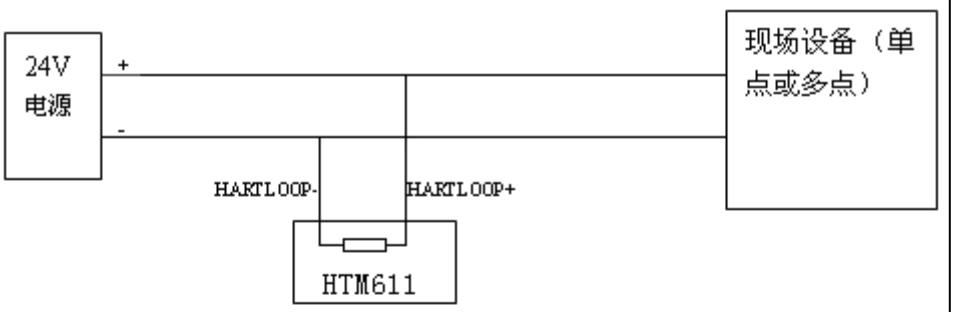


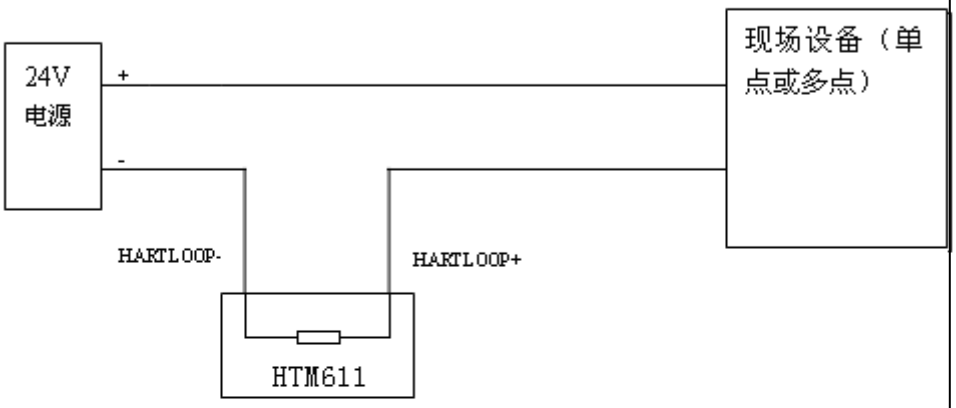
引脚	功能
1	接 HART 信号的正极
2	接 HART 信号的负极

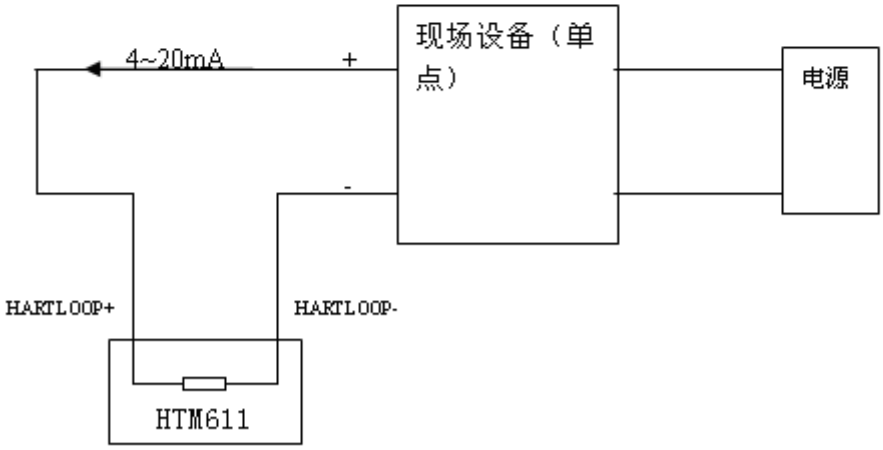
3.5 HTM-611 与现场设备的拓扑



HTM611 不使用内部采样电阻







HTM611 使用内部采样电阻

4 软件使用说明

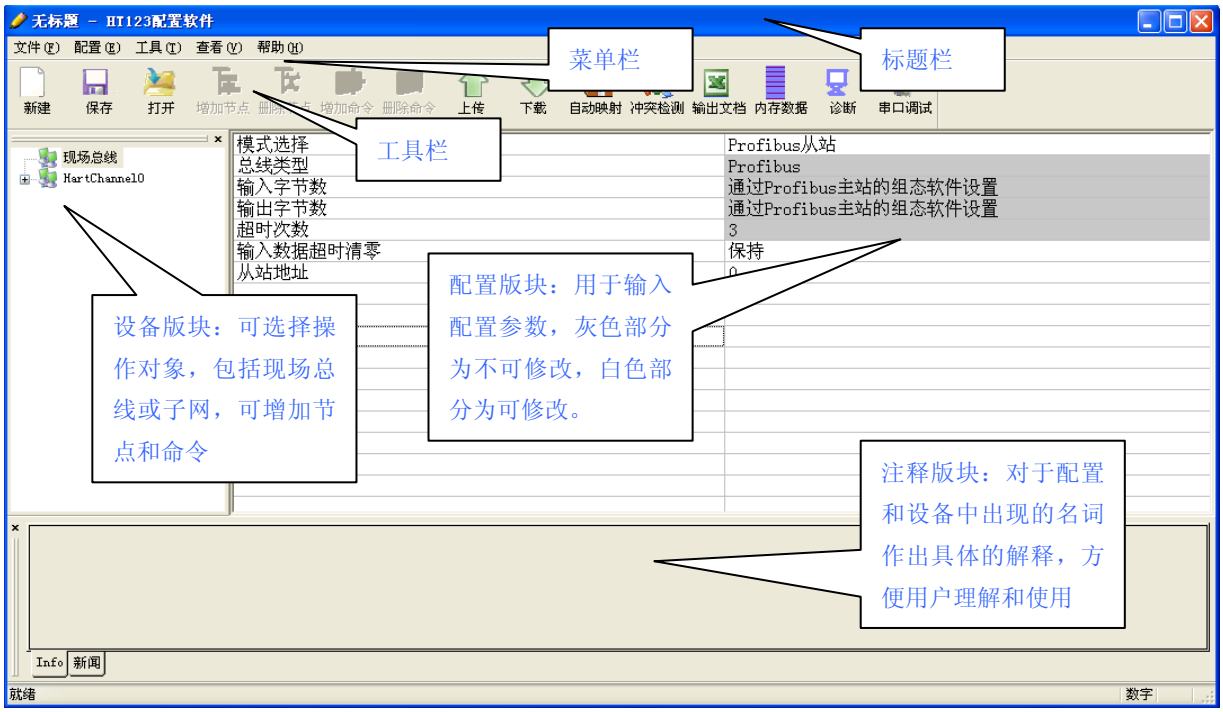
4.1 软件界面说明

HT-123 是一款基于 Windows 平台，用来配置 HART 系列网关设备的配置软件。

本部分简要介绍如何使用 HT-123 及配置 HTM-611 的方法。 详细的使用方法请看软件说明书。

双击图标

即可进入软件主界面：



工具栏：

工具栏如下图所示：

从左至右的功能分别是：新建、打开、保存、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、冲突检测、自动计算映射地址、Excel 配置文档输出、内存数据显示、诊断和串口调试。

新建：新建一个配置工程

打开：打开一个配置工程

保存：保存当前配置

增加节点：增加一个 HART 从站节点

删除节点：删除一个 HART 从站节点

增加命令：增加一条 HART 命令

删除命令：删除一条 HART 命令

上载配置信息：将配置信息从模块中读取上来，并且显示在软件中

下载配置信息：将配置信息从软件中下载到模块

冲突检测：检测配置好的命令在网关内存数据缓冲区中是否有冲突

自动计算映射地址：用于自动计算所配置命令的无冲突内存映射地址

Excel 配置文档输出：将当前配置输出到本地硬盘，以.xls 文件格式保存

内存数据显示窗口：显示网关的内部数据交换情况。

诊断窗口：诊断窗口可以用来分析现场设备的运行情况，还可以进行一定的分析。

串口调试助手：该功能可以向 HART 总线发任意帧，并可显示 HART 收到的数据，方便调试。

4.2 软件功能说明

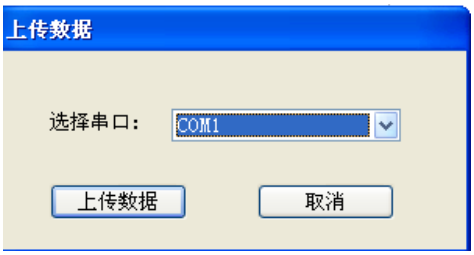
4.2.1 与硬件的连接

将网关的配置拨码开关拨至“ON”，用串口线连接网关的 RS232 接口和电脑的串口，给网关上电。此时网关的数码管显示“CF”表明处于配置状态。

4.2.2 上载网关配置

打开 HT-123，点击上载图标

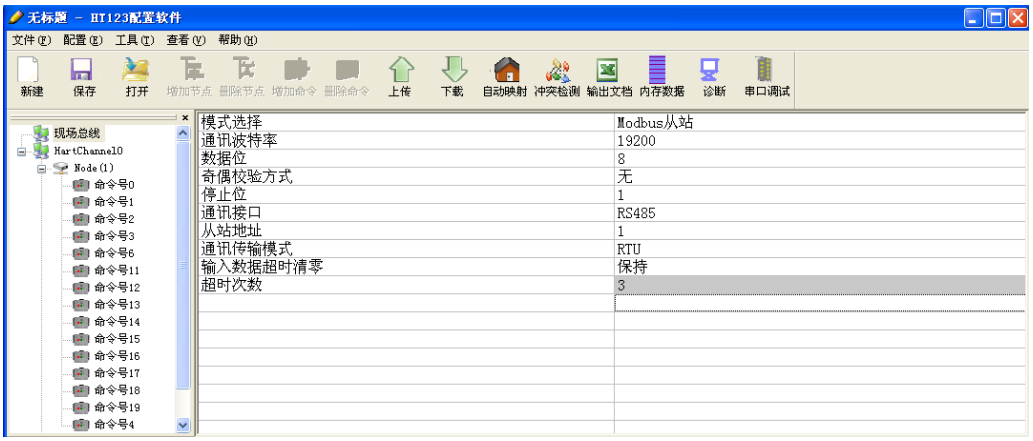
，在随后弹出的对话框里先选择网关所连接的电脑串口，再点击上传数据，当显示“上传成功”即表示网关里的配置已上传到 HT-123 中。



4.2.3 配置现场总线

4.2.3.1 配置现场总线为 MODBUS SLAVE

点击树视图中的“现场总线”，在右侧的配置板块里将“模式选择”选为“Modbus 从站”，然后按回车确定，将出现下图：



在这个界面里可以设置 从站的一些参数：

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

数据位：8 位

奇偶校验方式：无、奇、偶、标记、空格可选

停止位：1、2 可选

通讯传输模式：RTU、ASCII 可选

从站地址：范围是 0～247

通信接口：RS232、RS485 可选。当串口需要使用 RS422 通信时，此时请选择“RS485”

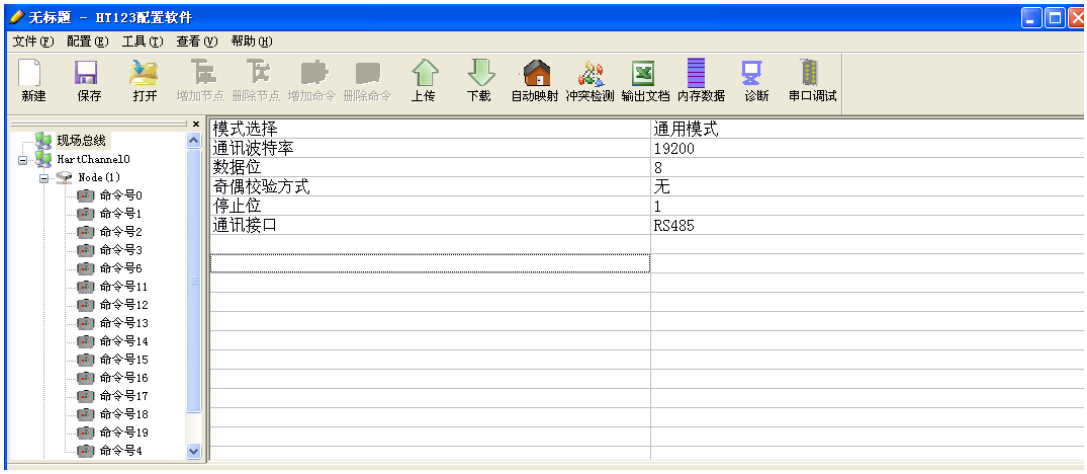
输入数据超时清零/保持：在 HART 命令超过所设的无应答次数之后，是否清零 HART 输入数据缓冲区。

超时次数：设定超时清零的次数

4.2.3.2 配置现场总线为通用模式

通用模式（透明传输模式）指可以通过串口（RS232/RS485/RS422）直接向 HART 总线发 HART 帧，同时网关也会将在 HART 总线接收到的数据通过串口（RS232/RS485/RS422）发送出去。在这个过程中数据没有任何增减。

点击树视图中的“现场总线”，在右侧的配置板块里将“模式选择”选为“通用模式”，然后按回车确定，将出现下图：

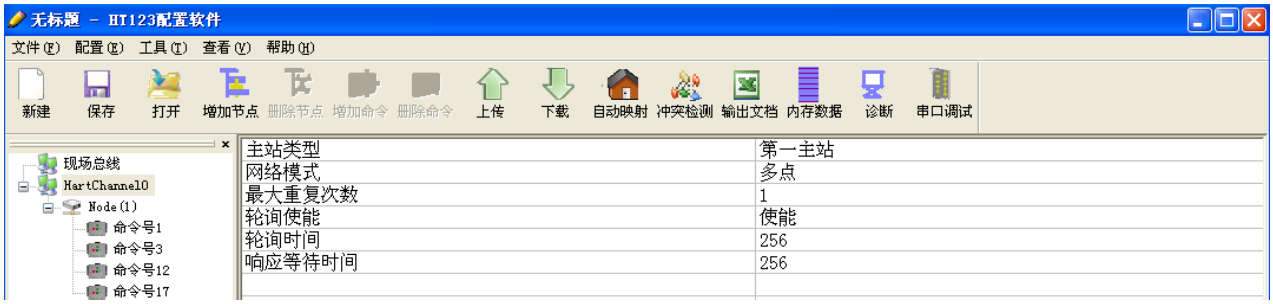


通用模式中的参数范围和意义同 “Modbus 从站”。

4.2.4 配置 HART 总线

4.2.4.1 配置 HART 通道参数

点击树视图中的“HartChannel0”，在右侧将出现配置板块：



主站类型：可以选择网关作为 HART 的第一主站还是第二主站；

网络模式：可以选择 HART 的网络连接为单点还是多点，在单点模式中只能与地址为 0 的从站设备通讯；

最大重复次数：选择命令重发的次数，范围 0~5；

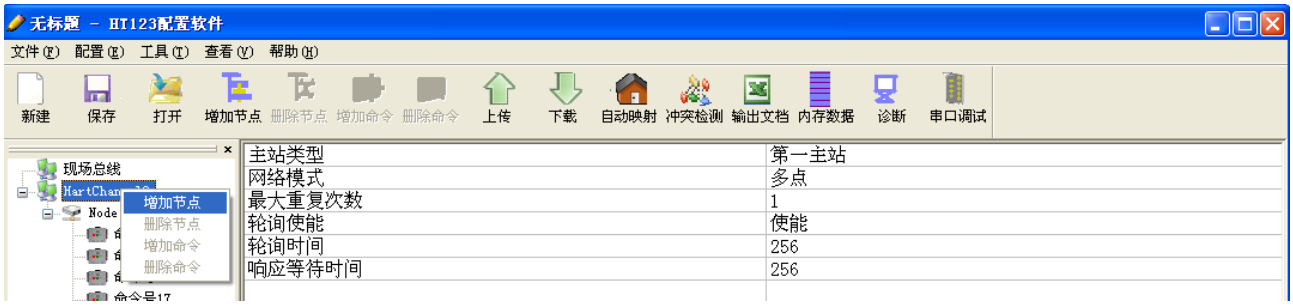
轮询使能：是否使用轮询功能，“Enable”表示使用轮询功能；

轮询时间：设定轮询命令的时间（一条命令发送开始到开始发送下一条命令的时间间隔），范围 256~65535ms；

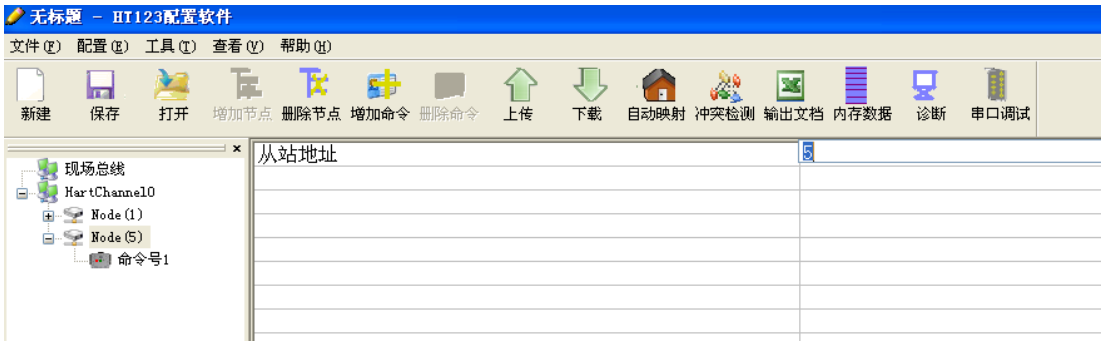
响应等待时间：设定网关等待从站设备应答的最大时间，范围是 256~65535ms

4.2.4.2 增加一个从站节点

点击所选的 HART 通道，点击鼠标右键，在弹出的菜单中选择增加节点。



点击所增加的节点，在右侧的配置板块中设定从站的地址，注意当 HART 通道选为单点时只能有一个地址为 0 的从站节点。



4.2.4.3 增加一条命令

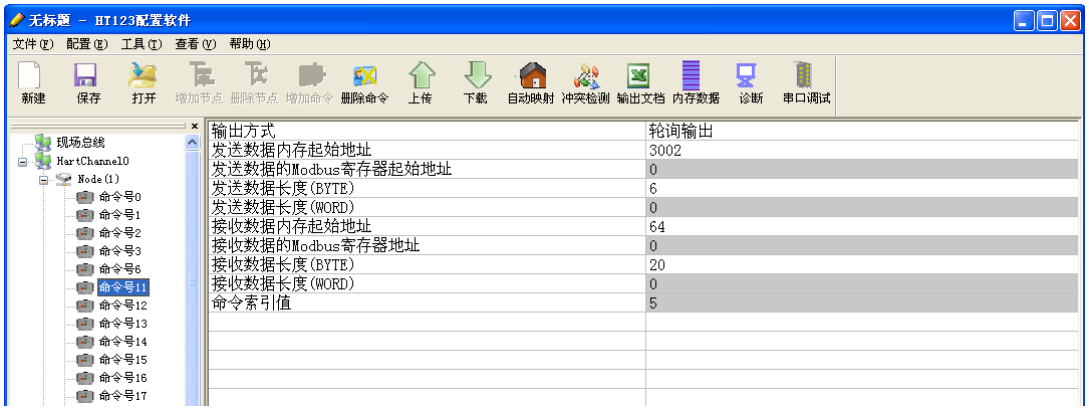
鼠标点击选择的从站节点，点击鼠标右键，在弹出的菜单中选择增加命令

在弹出的对话框中选择欲增加的命令，然后点击确定退出

注意，同一个命令在一个节点里只能配置一个。

4.2.4.4 配置从站命令

点击树视图中的相应命令号，在右侧将出现命令的配置板块：



输出方式：可以选择此命令的执行方式，可以选择为逢变输出，轮询输出，初始化输出，不输出；

- 逢变输出：当该命令的 HART 发送数据缓冲区内的数据发生变化时才执行此命令
- 轮询输出：该命令将放在轮询队列里，定时被执行
- 初始化输出：该命令在上电的时候只执行一次
- 不输出：该命令不输出

发送数据内存起始地址：设定该命令输出数据的内存起始地址，范围 3000~3999；

发送数据的寄存器起始地址：该属性为网关自动算出的，主要为方便用户进行寄存器寻址；

发送数据长度（byte）：用来设定该命令输出数据的长度；

发送数据长度（word）：该属性为网关自动算出，主要为方便用户查看输出数据长度，1word=2byte；

接收数据内存起始地址：设定该命令输入数据的内存地址。响应数据仅包括 HART 帧中的数据域，关于 HART 的帧结构请参考附录 B；

接收数据的寄存器起始地址：该属性为网关自动算出的，主要为方便用户进行寄存器寻址；

接收数据长度（byte）：用来设定该命令输入数据的长度；

接收数据长度（word）：该属性为网关自动算出，主要为方便用户查看输出数据长度，1word=2byte；

命令索引值：为配置软件自动算出，表明该命令在所配置的命令表中的索引值。

4.2.4.5 删除一条命令

先选择欲删除的命令，然后单击鼠标右键，选择删除命令即可；通过菜单命令也可进行相同的操作。

4.2.4.6 删除一个节点

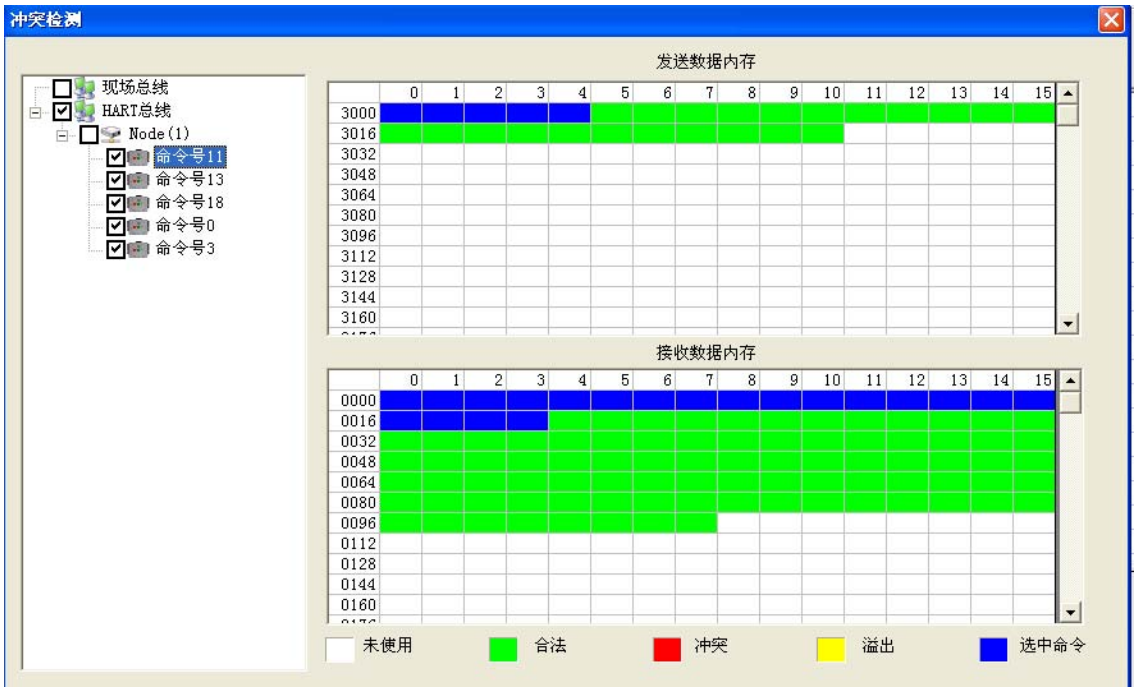
先选择欲删除的节点，然后单击鼠标右键，选择删除节点即可；通过菜单命令也可进行相同的操作。删除节点时，该节点下的所有命令也都被删除。

4.2.5 冲突检测

用来查看所有命令的输入输出数据在内存中的分布情况。

点击

图标将会弹出冲突检测界面：



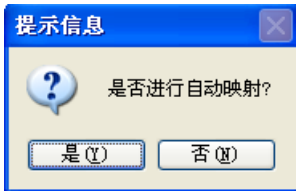
其中左侧的树视图中显示所配的命令，右侧为内存分配图。上面的内存分配图表示 HART 发送数据的内存分配，下面的表示 HART 接收数据的内存分配。当某一内存单元被两个或两个以上的命令所占用时，该内存单元将显示红色，当命令所分配的内存地址超出网关所规定的范围时，那么超出的部分将显示黄色，白色的区域表示可用的内存，绿色的区域表示已经被占用的内存。点击某一条命令，右侧的内存分配图将会以蓝色来表示该命令的输入数据和输出数据所在的存储位置。

4.2.6 自动内存映射

自动内存映射功能将自动根据用户命令所要求的输入输出字节数来无冲突分配内存。

首先要为每条命令设置正确的输入输出字节数，然后点击

图标，在弹出的对话框中选择“是”即可。



4.2.7 下载配置

点击

图标即可将配置下载到网关内。

4.2.8 内存数据显示功能

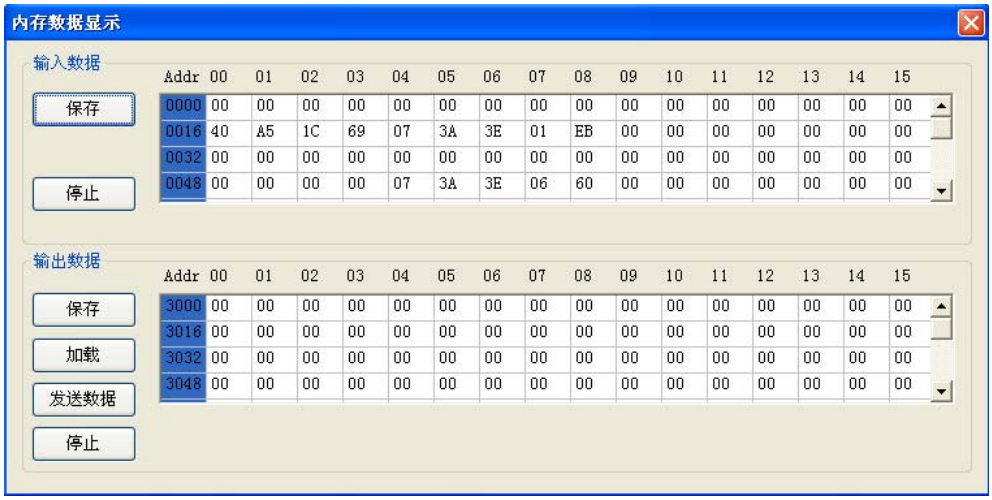
内存数据显示功能使用户可查看网关内部的数据交换情况，并可修改 HART 的输出数据。方便用户在 MODBUS 侧没有连接的情况下进行 HART 总线及设备的调试。使用该功能的步骤如下：

1) 首先将 HTM-611 的调试拨码开关拨至“ON”，然后重新上电。这时 HTM-611 运行于调试模式。

2) 将 HTM-611 的 RS232 接口连接到电脑上，打开 HT-123 软件，点击“配置->设置串口”，选择正确的串口号。

3) 点击“工具->内存数据显示”或单击“

”图标，打开如下窗口：



如图所示，上面表格显示的是 HART 输入数据在内存中的分布，下面表格显示的是 HART 输出数据在内存中的分布。当要修改输出数据时，先点击“停止”，再修改相应数据，或者加载已经保存过的数据表，最后点击“发送数据”即可。

4.2.9 诊断

设备诊断功能可以使用户知道哪些设备没有进行正常通信、所配命令的执行情况、网关的数据收发

状态和特定命令的显示。操作步骤如下：

1) 首先将 HTM-611 的调试拨码开关拨至“ON”，然后重新上电。这时 HTM-611 运行于调试模式。

2) 将 HTM-611 的 RS232 接口连接到电脑上，打开 HT-123 软件，点击“配置->设置串口”，选择正确的串口号。

3) 点击“工具->诊断”或点击图标“

”，软件先弹出一个对话框用来上载网关的配置，如下图：

4) 点击“上传数据”弹出下图：

5) 点击“确定”进入诊断界面：

在这个界面中点击“HartChannel0”，右侧就会显示网关在 HART 总线部分的状态，单击“更新”会刷新一次数据，单击“重置”会清零系统状态，单击“周期更新”，软件会 500ms 更新一次数据。

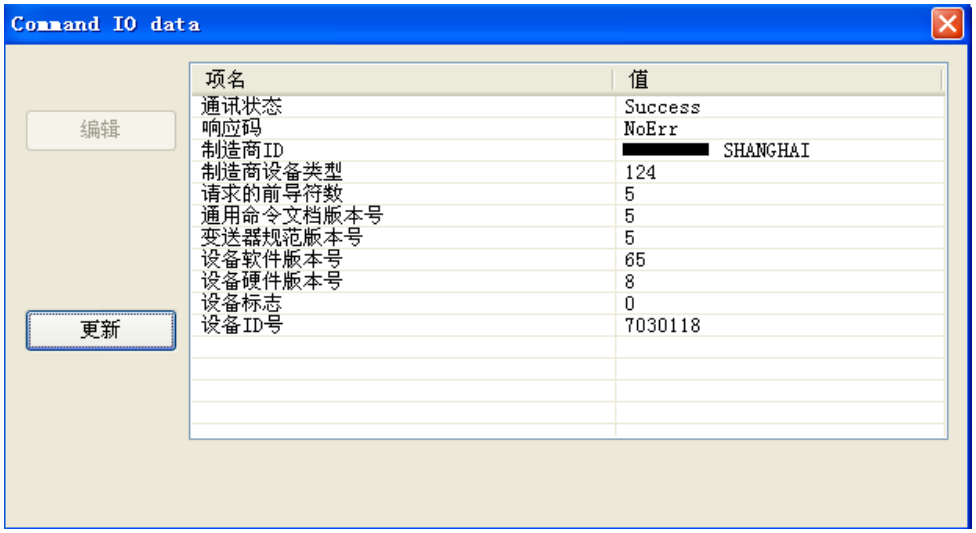
6) 单击 Node（x）出现下图：

这个界面显示的是所配置命令的响应状态。

点击“更新”会刷新这些命令状态，“周期更新”会 500ms 更新一次命令状态。

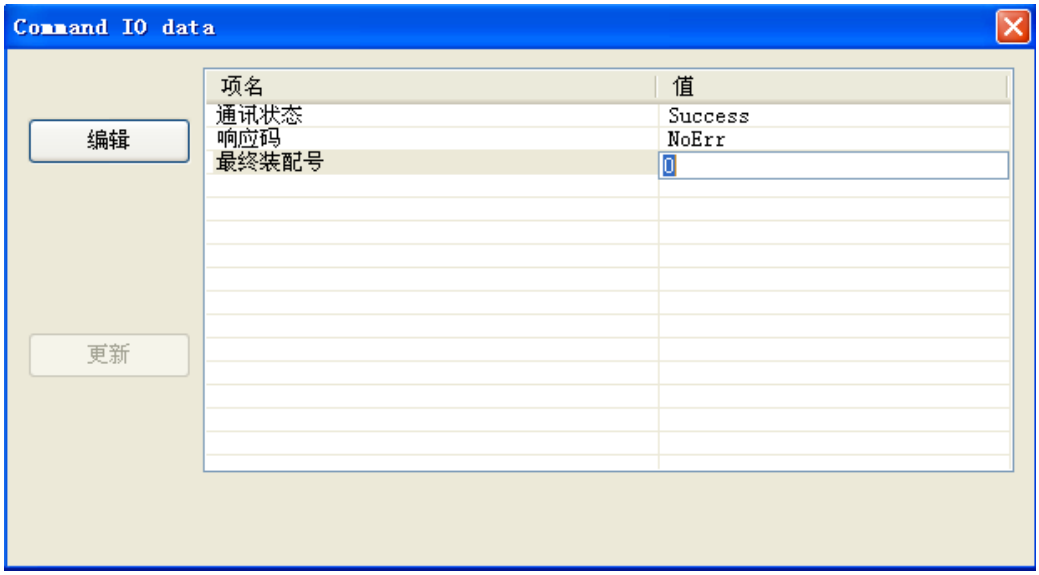
7) 双击 0、1、2、3、6、11、12、13、1、15、16、17、18、19 号命令会弹出它们的命令信息，对 6、17、18、19 号命令可以进行数据的输入。

如双击“CMD0”则弹出如下窗口：



点击“Update”即可更新数据，“Modify”在只读的命令里不起作用。

双击“CMD19”弹出如下窗口：



单击想要改变的变量或属性，如“Final Assembly Number”，改变相应的数值，然后单击“Modify”即可执行本次的写命令操作。

4.2.10 串口调试

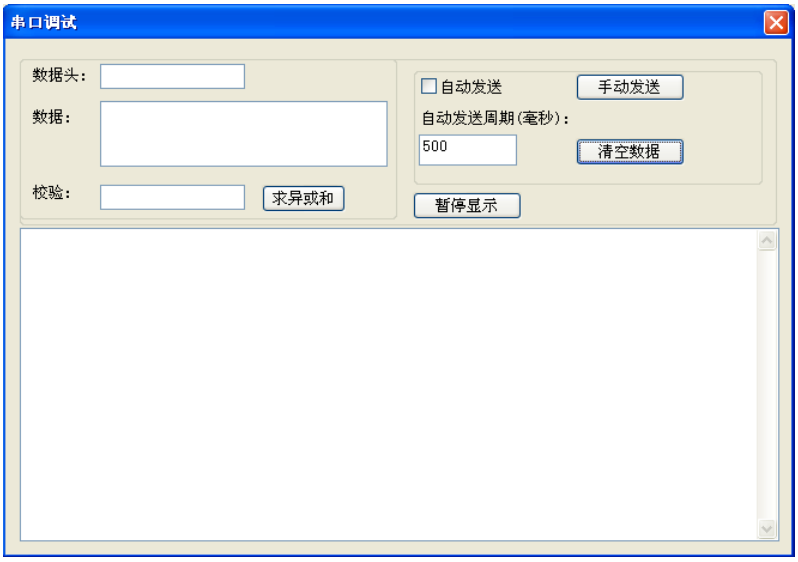
串口通用体调试功能可以向 HART 总线发送任何报文，还可监测网关在 HART 总线上收到的数据。具体操作如下：

1) 首先将 HTM-611 的调试拨码开关拨至“ON”，然后重新上电。这时 HTM-611 运行于调试模式。

2) 将 HTM-611 的 232 接口连接到电脑上，打开 HT-123 软件，点击“配置->设置串口“，选择正确的串口号。

3) 点击“工具->串口调试助手”或点击图标“

”，弹出串口调试助手界面：



在此界面中，点击“自动发送”或“手动发送”就会将数据头、数据和校验组成一帧发出去，网关在HART 总线接收到的数据会在下面空白处显示。其中“求异或和”按钮只对数据部分进行校验。举例如下：

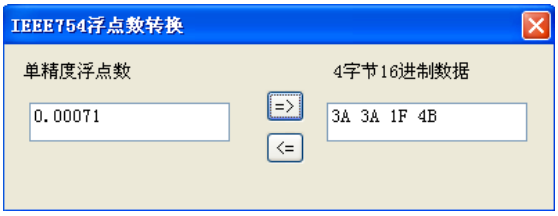
示例中由数据头，数据和校验组成了一个 HART 的 0 号命令，使用的是短地址，点击“手动发送”后，在下方便得到了该命令的响应数据。

注：在此功能下，网关将停止执行所配置的命令，关闭此功能，网关将恢复执行所配置的命令。

4.2.11 转换工具

在“工具”菜单里有两个实用的工具，用来方便的进行 IEEE754 和 PACKED ASCII 的转换：

Packed ASCII Translate
未压缩的数据
TECH
ASCII码
<=
=>
压缩后的数据
50 50 C8
16进制


IEEE754浮点数转换
单精度浮点数
0.00071
=>
<=
4字节16进制数据
3A 3A 1F 4B

5 工作原理

网关内部开辟了一个长度为 5000 字节的内存作为数据交换的输入输出缓冲区。其中 0~2999 的内存作为 HART 的输入数据和设备状态的存放区域。3000~4999 的内存作为 HART 的输出数据和控制变量的存放区域。具体的分配如下表所示：

	网关内存地址	对应 MODBUS 寄存器地址	描述
只读部分	0-1599	0-799	HART 数据输入区
	1600-1619	800-809	Device 0_cmd0 数据
	1620-1639	810-819	Device 1_cmd0 数据
	……	……	……Device 15_cmd0 数据
	1920	960H	网关状态
	1921	960L	网关 HART 口发送次数
	1922	961H	网关 HART 口接收次数
	1923	961L	HART 通讯错误次数
	1924-1943	962-971	保留
	1944	972H	Device 0_cmd0 的响应状态
	1945	972L	Device 1_cmd0 的响应状态
	……	……	……Device15 _cmd0 的响应状态
	1960-2119	980-1059	用户命令的响应状态
	2120-2391	1060-1195	保留
	2392	1196H	通用接收标号
	2393	1196L	通用接收错误计数器
	2394-2395	1197	通用接收数据长度
	2396-2695	1198-1347	通用接收数据
	2696-2999		保留
可读可写部分	3000-3999	0000-0499	HART 数据输出区
	4000	0500H	复位发送、接收、出错计数器
	4001	0500L	轮询使能

	4002	0501H	触发标号
	4003	0501L	触发命令号
	4004-4269	0502-0634	保留
	4270	0635H	通用发送标号
	4271	0635L	通用模式使能
	4272-4273	0636	通用发送数据长度
	4274-4573	0637-0786	通用发送数据

- HART 数据输入区：存放 HART 从站设备发给网关的数据。
- HART 数据输出区：存放网关发给 HART 从站的数据。
- Device 0_cmd0~ Device 15_cmd0：在第一次执行某个从站命令时，网关内部会自动执行 0 号命令来获取设备信息（取得长地址）。这些内部命令的响应数据存放在该区域内
- 网关状态：网关状态表明网关在 HART 网络所处的状态，其定义为：

  0----没有 HART 通讯在进行

  1----发送中

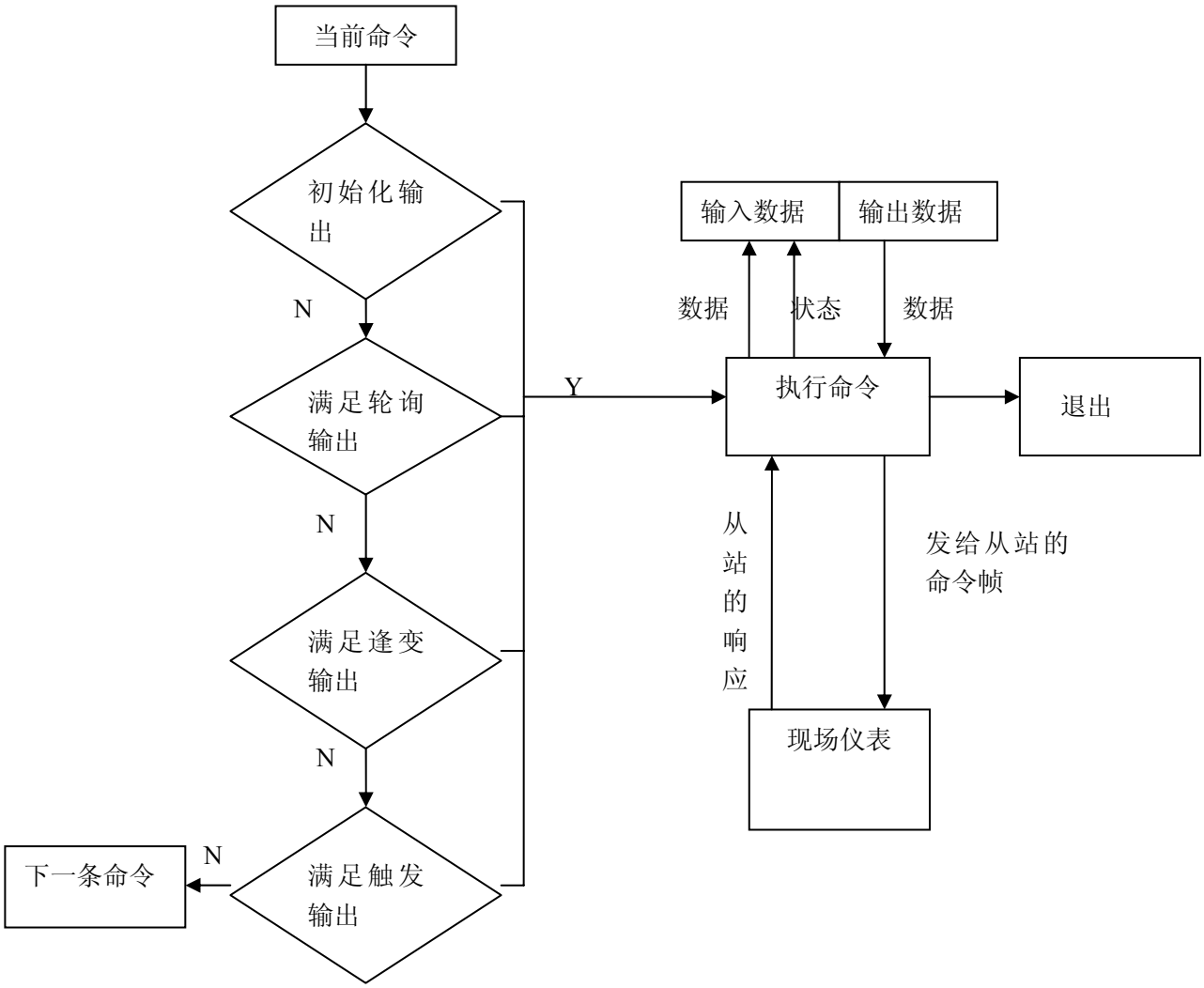
  2----等待应答

  3----处理应答
- 网关 HART 口发送次数： HART 发送计数器
- 网关 HART 口接收次数： HART 接收计数器
- HART 通讯错误次数：HART 接收错误计数器
- Device 0_cmd0~ Device 15_cmd0 的响应状态：表明各内部命令的响应状态
- 用户命令的响应状态：表明用户命令的响应状态

  命令状态定义：
  0----没执行过
  1----正确响应
  2----校验错误
  3----无应答
  4----协议中定义的错误
  5----没有连接
- 通用接收标号：通用模式下的接收标号，此值变化一次即表明 HART 端接收到了一个 HART 帧
- 通用接收数据长度：表明通用模式下所接收到的数据长度

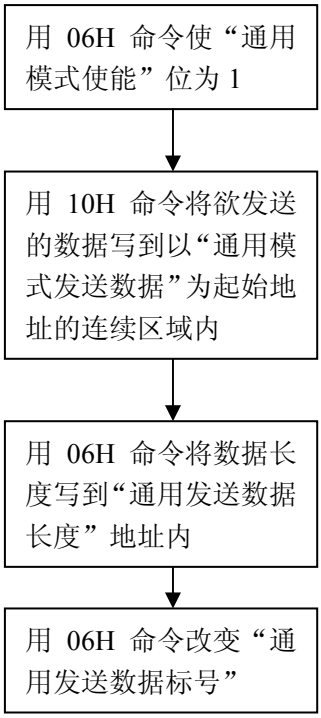
- 通用接收错误计数器：表明通用接收错误次数
- 通用接收数据：存放通用模式下 HART 端所接收到的数据
- 复位发送、接收、出错计数器：为网关的控制信号，该内存的值发生变化则网关会使各计数器为 0
- 轮询使能：此位可读可写，当写 1 时可使能轮询输出，写 0 时可禁止轮询输出；读 1 表明轮询为使能状态，为 0 表明轮询为禁止状态
- 触发标号：用户改变该值将导致一次触发操作
- 触发命令号：触发操作所执行的命令号
- 通用模式使能：该值为 1 表明使能了通用传输功能，否则为禁止了通用传输功能
- 通用发送标号：通用模式下的发送标号，此值变化一次将导致发送一个 HART 帧
- 通用发送数据长度：通用模式发送数据的长度
- 通用发送数据：通用模式要发送的数据

5.1 执行一条 HART 命令的流程图



5.2 通用收发数据

有两种通用方式供用户选择：一个是将现场总线定义为通用模式，此时网关将会以 3.5 个字符超时断帧的方式接收串口的数据，并不加修改地由 HART 接口发送出去。网关也会将 HART 接口接收到的数据不加修改地由串口发出。字符超时时间根据波特率而定，如波特率为 19200，那么字符超时时间被认为是(1/19200)*10*3.5≈2ms。另一种是通过 MODBUS 命令间接的进行 HART 通用帧的收发，举例如下：



网关将接收到 HART 帧存放在以“通用接收数据”为起始地址的连续区域内，并将接收的数据长度填写到“通用接收数据长度”内，然后改变“通用接收标号”的值。如果在响应等待时间内没有接收到任何数据，则会令“通用接收错误计数器”加 1。 所以用户在发送通用帧之前应先读取通用接收标号和错误计数器，在发完通用帧后需不断的读取这两个值，直到其中一个发生变化为止。

5.3 触发命令

用户可以用 MODBUS 命令来触发任意一条网关所配置的 HART 命令，具体做法为用 MODBUS 的 6 号命令将欲触发的用户命令号（在用 HT-123 配置命令时软件会自动算出并显示）写到“触发命令号”内，然后改写“触发标号”使其数值变化即可触发网关进行一次触发操作。设备响应中的数据部分会存放到以该命令号所指定的“接收数据内存”中。

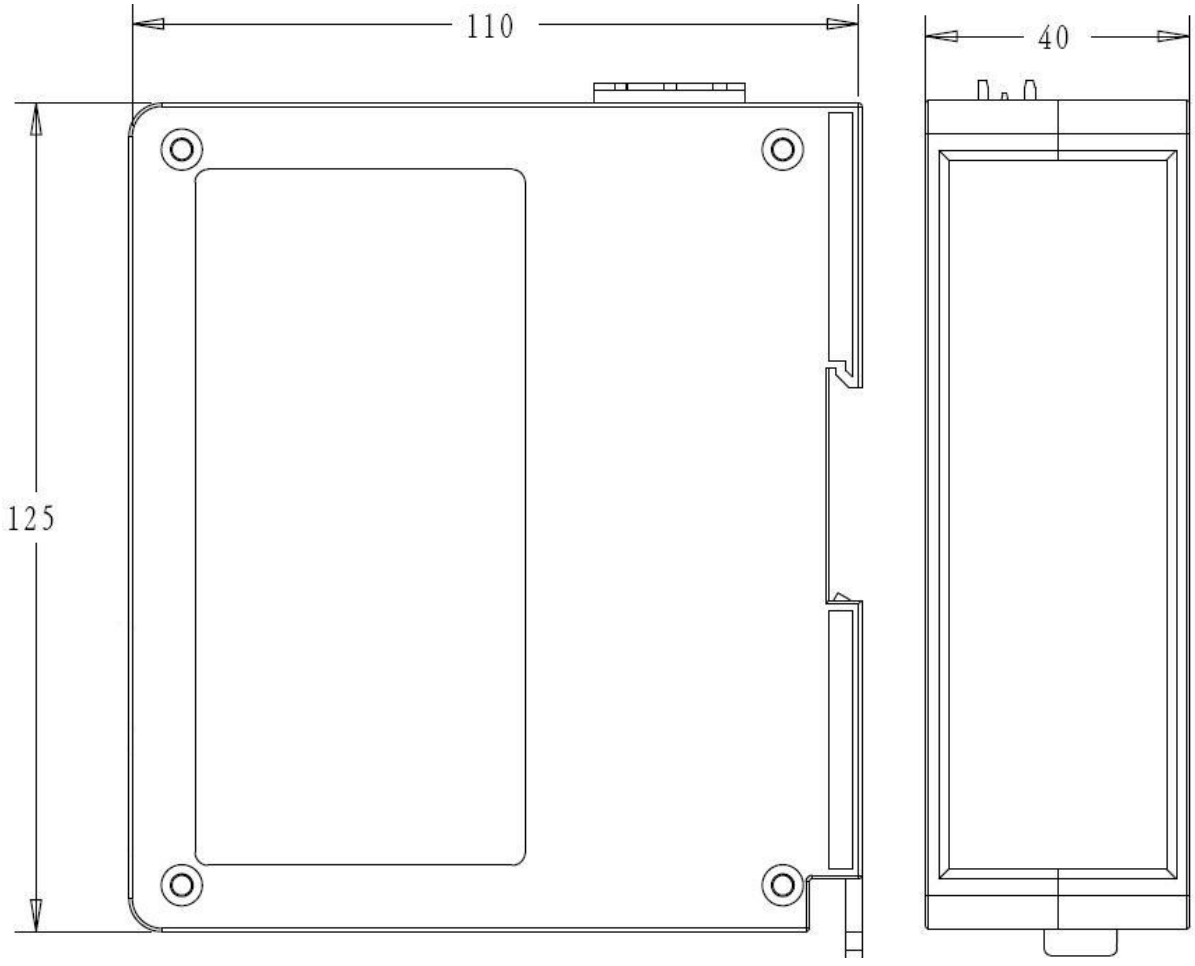
5.4 与 MODBUS 的数据交换

现场总线配置为“Modbus 从站”时，用户可以根据网关内部输入输出缓冲区所对应的地址来进行数据交换、进行网关的状态查询及管理，还可进行触发操作和通用帧的收发。

6 安装

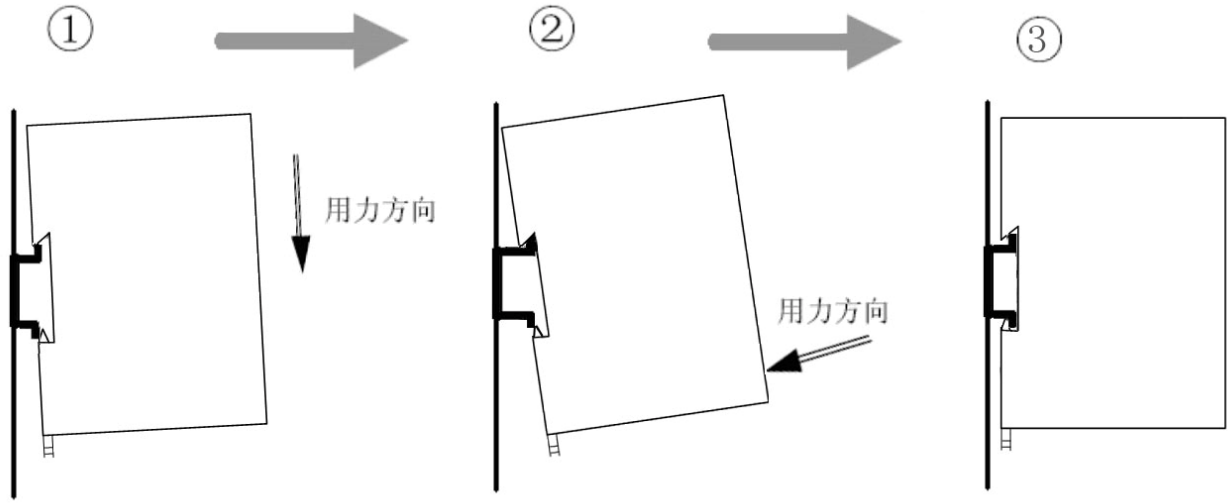
6.1 机械尺寸

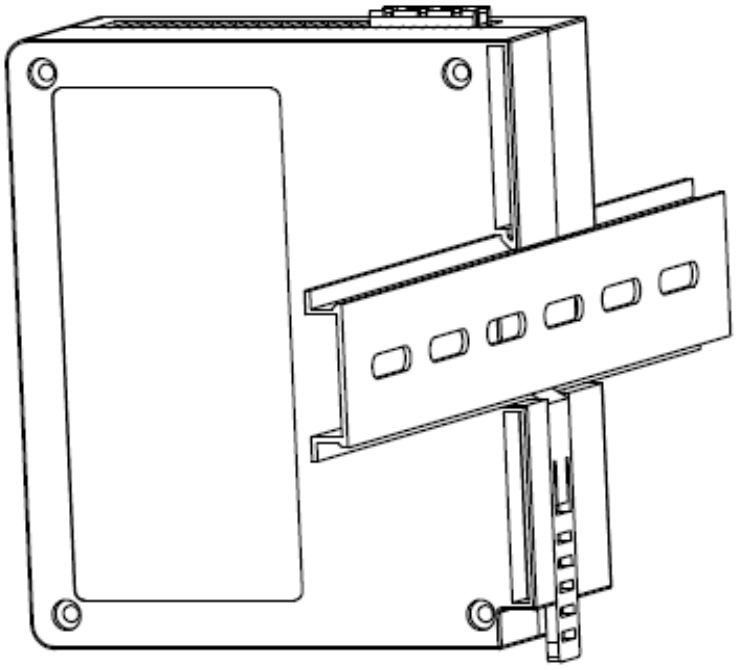
尺寸： 40mm（宽）×125mm（高）×110mm（深）



6.2 安装方法

35mm DIN 导轨安装


①
②
③
用力方向
用力方向



7 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。

8 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。

附录 A：MODBUS 协议

1.协议概述

物理层：传输方式：RS485

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，这就不会在它们初始化时占据通讯线路，而仅限于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 位或者无奇偶检验位、1 位或者 2 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、数据格式、功能码等，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：终端从机地址(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 列出了部分常用的功能码、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	读保持寄存器	获得一个或多个寄存器的当前二进制值
06	预置单个寄存器	放置一个特定的二进制值到一个寄存器中
16	预置多个寄存器	放置特定的二进制值到一系列寄存器中

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：功能域代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。

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，起始位和停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，直到执行完了 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：

1) 预置一个 16 位寄存器为 0FFFFH（全 1），称之为 CRC 寄存器。
2) 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。
3) 如果最低位为 0：重复第 2 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。
4) 重复第 2 步和第 3 步直到 8 次移位。这样处理完了一个完整的八位。
5) 重复第 2 步到第 4 步来处理下一个八位，直到所有的字节处理结束。

6) 最终 CRC 寄存器的值就是 CRC 的值。

2．应用层功能详解

2.1 读保持寄存器（功能码 03）

查询

功能码 03H 允许用户读取多个保持寄存器的内容。主站设备可设从保持寄存器的任何起始地址读取多个寄存器的值。表 2 – 1 的例子是从 03 号从机读 3 个数据 U1,U2,U3, 其中 U1 的地址为 0001H, U2 的地址为 0002H, U3 的地址为 0003H，即寄存器起始地址为 0001H，数据个数为 0003H。

表 2 – 1 读 U1、U2、U3 的查询数据帧

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

响应

响应包含从机地址、功能码、数据的数量和 CRC 错误校验。表 2 – 2 的例子是读取 U1,U2,U3 的响应。

表 2 – 2 读 U1,U2,U3 的响应数据帧

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

2．2 预置多个寄存器（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多个变量的值。表 2-3 的例子是修改 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 的动作设定值地址为 2AH，延时时间的设定值为 2BH，负载监控 2 的动作设定值地址为 2CH，延时时间的设定值为 2DH。

表 2-3 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

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	D0H	00H	0AH	25H	7CH

响应

响应包含从机地址、功能码、数据的数量和 CRC 错误校验。表 2 – 4 的例子是修改负载监控 1 和负载监控 2 的动作值及延时时间的设定值的响应。

表 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的响应

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

2．3 预置单个寄存器（功能码 06）

查询

功能码 06 允许用户改变单个寄存器的内容。表 2-5 的例子是修改 03 号从机过载动作设定值 Ir1，其中 Ir1 地址是 002EH.

表 2-5 修改过载动作设定值 Ir1

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	D0H	EBH	8DH

响应

对于预置单个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。

表 2-6 修改过载动作设定值 Ir1 响应

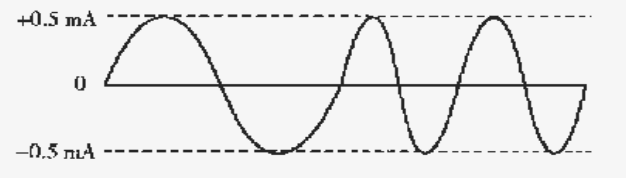
地址	功能码	变量起始地址高字节	变量起始地址低字节	变量值高字节	变量值低字节	校对验码低字节	校对验码高字节
03H	06H	00H	2EH	07H	D0H	EBH	8DH

附录 B：HART 协议

现代工业生产中存在着多种不同的主机和现场设备，要想很好地使用他们，完善的通讯协议是必须的。**HART** 协议最初是由美国 **Rosemount** 公司开发，已应用了多年。**HART** 协议使用 **FSK** 技术，在 **4~20mA** 信号过程量上叠加一个频率信号，成功地把模拟信号和数字信号双向同时通讯，而不互相干扰。**HART** 协议参照了国际标准化组织的开放性互连模型，使用 **OSI** 标准的物理层、数据链路层、应用层。HART 协议规定了传输的物理形式、消息结构、数据格式和一系列操作命令，**是一种主从协议**。当通讯模式为“问答式”的时候，一个现场设备只做出被要求的应答。HART 协议允许系统中存在 2 个主机（比如说，一个用于系统控制，另一个用于 HART 通信的手操仪），如果不需要模拟信号，多点系统中的一对电缆线上最多可以连接 15 个从设备。

物理层

物理层规定了信号的传输方法、传输介质。采用 **Bell202** 标准的 **FSK** 频移键控信号，在低频的 **4～20mA** 模拟信号上叠加一个频率数字信号进行双向数字通信。数字信号的幅度为 **0.5mA**，数据传输率为 **1200bps**，**1200Hz** 代表逻辑“**1**”，**2200Hz** 代表逻辑“**0**”。数字信号波形如上图所示。



数据链路层

数据链路层规定 **HART** 协议帧的格式，可寻址范围 0～15，“0”时，处于 4～20mA 及数字信号单点模式，现场仪表与两个数字通信主设备（也称作通信设备或主设备）之间采用特定的串行通信，主设备包括 PC 机、控制室系统、网关和手持通信器。单点操作中，主变量（过程变量）可以以模拟形式输出，也可以以数字通信方式读出，以数字方式读出时，轮询地址始终为 0。也就是说，单站模式时数字信号和 4～20mA 模拟信号同时有效。“1～15”处于全数字通信状态，工作在多点模式，通信模式有“问答”式、“突发”式(点对点、自动连续地发送信息)。按问答方式工作时的数据更新速率为 2～3 次 / s，按突发方式工作时的数据更新速率为 3～4 次 / s。在本质安全要求下，只使用一个电源，至多能连接 15 台现场仪表，每个现场设备可有 256 个变量，每个信息最大可包含 4 个变量。这就是所谓的多点（多站）操作模式。这种工作方式尤其适用于远程监控，如管道系统和油罐储存场地。采用多点模式，4～20mA 的模拟输出信号不再有效（输出设在 4mA 使功耗最小，主要是为变送器供电，各个现场装置并联连接 ），系统以数字通信方式依次读取并

联到一对传输线上的多台现场仪表的测量值（或其它数据）。如果以这种方式构成控制系统，可以显著地降低现场布线的费用和减少主设备输入接口电路，这对于控制系统有重要价值。

HART 协议根据冗余检错码信息，采用自动重复请求发送机制，消除由于线路噪声或其他干扰引起的数据误码，实现数据无差错传送。能利用总线供电，可满足本质安全防爆要求。

HART 协议采用 **UART**（通用异步接收/发送器）来完成字节的传输，格式为：1 个起始位，8 个数据位，一个奇校验位，一个停止位，波特率为 1200。

帧结构

PREAMBLE	START	ADDR	COM	BCNT	STATUS	DATA	PARITY
序文	定界符	地址	命令号	数据长度	响应码	数据字节	奇偶校验

（1）PREAMBLE　导言字节，一般是 5～20 个 FF 十六进制字节。他实际上是同步信号，各通讯设备可以据此略做调整，保证信息的同步。从机应答 0 信号时将告之主机他“希望”接收几个字节的导言，另外主机也可以用 59 号命令告诉从机应答时应用几位导言。

（2）START　起始字节，他将告之使用的结构为“长”还是“短”、消息源、是否是“突发”模式消息。主机到从机为短结构时，起始位为 02，长帧时为 82。从机到主机的短结构值为 06，长结构值为 86。而为“突发”模式的短结构值为 01，长结构为 81。

（3）ADDR　地址字节，他包含了主机地址和从机地址，从机地址分为短地址和长地址。短结构中占 1 字节，长结构中占 5 字节。无论长结构还是短结构，因为 HART 协议中允许 2 个主机存在，所以我们用首字节的最高位来进行区分，值为 1 表示第一主机地址，第二主机用 0 表示。次高位为 1 表示从站处于“突发”模式。短结构用首字节的 0～4 位表示值为 0～15 的从机地址，第 5，6 位赋 0；而长结构用首字节的后 6 位表示从机的生产厂商的代码，第 2 个字节表示从机设备型号代码，后 3～5 个字节表示从机的设备序列号，这五个字节构成“唯一”标志码，即长地址。另外，长结构的低 38 位如果都是 0 的话表示的是广播地址，即消息发送给所有的设备。

（4）COM　命令字节，他的范围为 253 个，用 HEX 的 0～FD 表示。

（5）BCNT　数据总长度，他的值表示的是 BCNT 下一个字节到最后（不包括校验字节）的字节数。接收设备用他可以鉴别出校验字节，也可以知道消息的结束。他的取值范围是 0~255

（6）STATUS　状态字节，他也叫做“响应码”，顾名思义，他只存在于从机响应主机消息的时候，用 2 字节表示。他将报告通讯中的错误、接收命令的状态（如：设备忙、无法识别命令等）和从机的操作状态。

如果我们在通讯过程中发现了错误，首字节的最高位（第 7 位）将置 1，其余的 7 位将汇报出错误的细节，而第 2 个字节全为 0。否则，当首字节的最高位为 0 时，表示通讯正常，其余的 7 位表示命令响应

情况，第 2 个字节表示场设备状态的信息。

UART 发现的通讯错误一般有：奇偶校验、溢出和结构错误等。命令响应码可以有 128 个，表示错误和警告，他们可以是单一的意义，也可以有多种意义，我们通过特殊命令进行定义、规定。现场设备状态信息用来表示故障和非正常操作模式。

（7）DATA　数据字节，并非所有的命令和响应都包含数据字节。数据的形式可以是无符号的整数（可以是 8，16，24，32 b），浮点数（用 IEEE754 单精浮点格式）或 ASCII 字符串，还有预先制定的单位数据列表。具体的数据个数根据不同的命令而定。

（8）CHK　奇偶校验，方式是纵向奇偶校验，从起始字节开始到奇偶校验前一个字节为止。另外，每一个字节都有 1 位的校验位，这两者的结合可以检测出 3 位的突发错误。

应用层

操作命令处于应用层，包括通用命令、普通命令和特殊命令。

附录 C：HART 常用命令

注意：实际的响应数据单元前两个字节为设备的现场状态信息，后面的数据才是响应字节。

命令 0：读标识码

返回设备类型代码，版本和设备标识码。

请求：无

响应：

字节 0：　　254
字节 1：　　制造商 ID
字节 2：　　制造商设备类型
字节 3：　　请求的前导符数
字节 4：　　通用命令文档版本号
字节 5：　　变送器规范版本号
字节 6：　　设备软件版本号
字节 7：　　设备硬件版本号
字节 8：　　设备标志
字节 9-11：　　设备 ID 号

命令 1：读主变量（PV）

以浮点类型返回主变量的值。

请求：无

响应：

字节 0：　　主变量单位代码
字节 1-4：　　主变量

命令 2：读主变量电流值和百分比

读主变量电流和百分比，主变量电流总是匹配设备的 AO 输出电流。百分比没有限制在 0-100%之间，如果超过了主变量的范围，会跟踪到传感器的上下限。

请求：无

响应：

字节 0-3：　　主变量电流，单位毫安
字节 4-7：　　主变量量程百分比

命令 3：读动态变量和主变量电流

读主变量电流和 4 个（最多）预先定义的动态变量，主变量电流总是匹配设备的 AO 输出电流。每种设备

类型都定义的第二、第三和第四变量，如第二变量是传感器温度等。

请求：无

响应：

字节 0-3：　主变量电流，单位毫安

字节 4：　主变量单位代码

字节 5-8：　主变量

字节 9：　第二变量单位代码

字节 10-13：　第二变量

字节 14：　第三变量单位代码

字节 15-18：　第三变量

字节 19：　第四变量单位代码

字节 20-23：　第四变量

命令 4：保留

命令 5：保留

命令 6：写 POLLING 地址

这是数据链路层管理命令。这个命令写 Polling 地址到设备，该地址用于控制主变量 AO 输出和提供设备标识。

只有当设备的 Polling 地址被设成 0 时，设备的主变量 AO 才能输出，如果地址是 1~15 则 AO 处于不活动状态也不响应应用过程，此时 AO 被设成最小；并设置传输状态第三位——主变量模拟输出固定；上限/下限报警无效。如果 Polling 地址被改回 0，则主变量 AO 重新处于活动状态，也能够响应应用过程。

请求：

字节 0：　设备的 Polling 地址

响应：

字节 0：　设备的 Polling 地址

命令 11：用设备的 Tag 读设备的标识 读与工位号相关的唯一标示符

这是一个数据链路层管理命令。这个命令返回符合该 Tag 的设备的扩展类型代码、版本和设备标识码。该命令可以用长地址或广播地址来寻址。响应消息中的扩展地址和请求的相同。

请求：

字节 0-5：　设备的 Tag，ASCII 码

响应：

字节 0：　254

字节 1：　制造商 ID 代码

字节 2：　制造商设备类型代码

字节 3：　请求的前导符数

字节 4：　通用命令文档版本号

字节 5：　　变送器版本号
字节 6：　　本设备的软件版本号
字节 7：　　本设备的硬件版本号
字节 8：　　设备的 Flags
字节 9-11：　设备的标识号

命令 12：读消息（Message）

读设备含有的消息。
请求：无
响应：
字节 0-23：　设备消息，ASCII

命名 13：读标签 Tag，描述符 Description 和日期 Date

读设备的 Tag，Description and Date。
请求：无
响应：
字节 0-5：　标签 Tag，ASCII
字节 6-17：　描述符，ASCII
字节 18-20：日期，分别是日、月、年-1900

命令 14：读主变量传感器信息

读主变量传感器序列号、传感器极限/最小精度（Span）单位代码、主变量传感器上限、主变量传感器下限和传感器最小精度。传感器极限/最小精度（Span）单位和主变量的单位相同。
请求：无
响应：
字节 0-2：　主变量传感器序列号
字节 3：　　主变量传感器上下限和最小精度单位代码
字节 4-7：　主变量传感器上限
字节 8-11：　主变量传感器下限
字节 12-15：主变量最小精度

命令 15：读主变量输出信息

读主变量报警选择代码、主变量传递（Transfer）功能代码、主变量量程单位代码、主变量上限值、主变量下限值、主变量阻尼值、写保护代码和主发行商代码。
请求：无
响应：
字节 0：　　主变量报警选择代码
字节 1：　　主变量传递 Transfer 功能代码

字节 2：　　主变量上下量程值单位代码
字节 3-6：　　主变量上限值
字节 7-10：　　主变量下限值
字节 11-14：　主变量阻尼值，单位秒
字节 15：　　写保护代码
字节 16：　　商标发行商代码 Private Label Distributor Code

命令 16：读最终装配号

读设备的最终装配号。
请求：无
响应：
字节 0-2：　　最终装配号

命令 17：写消息

写消息到设备。
请求：
　　字节 0-23：　设备消息，ASCII
响应：
　　字节 0-23：　设备消息，ASCII

命令 18：写标签、描述符和日期

写标签、描述符和日期到设备。
请求：
　　字节 0-5：　　标签 Tag，ASCII
　　字节 6-17：　描述符 Descriptor，ASCII
　　字节 18-20：日期
响应：
　　字节 0-5：　　标签 Tag，ASCII
　　字节 6-17：　描述符 Descriptor，ASCII
　　字节 18-20：日期

命令 19：写最后装配号

写最后装配号到设备。
请求：
　　字节 0-2：　　最终装配号
响应：
　　字节 0-2：　　最终装配号

命令 105：读突发模式配置

请求：无

响应：

字节 0：　　突发模式控制代码

字节 1：　　突发命令号

字节 2：　　分配给 slot1 的变量代码

字节 3：　　分配给 slot2 的变量代码

字节 4：　　分配给 slot3 的变量代码

字节 5：　　分配给 slot4 的变量代码

命令 108：写突发命令号

设定设备突发的命令号

请求：

字节 0：　HART 命令号

响应：

字节 0：　HART 命令号

命令 109：突发模式控制

开启或关闭突发模式。

请求：

字节 0：　突发模式控制代码（0 关，1 开）

响应：

字节 0：　突发模式控制代码