

大延牌智能仪表 ModBus 通讯协议说明

本公司的ModBus 通讯协议为ModBus RTU 协议。数据通讯采用Master/Slave 方式,Master 端发出数据请求消息,Slave 端接收到正确消息后就可以发送数据到 Master 端以响应请求;Master 端也可以直接发消息修改 Slave 端的数据,实现双向读写。

ModBus RTU 协议采用 16 位 CRC 校验,Modbus 采用主从方式定时收发数据,在实际使用中如果某 Slave 站点断开后(如故障或关机),Master 端可以诊断出来,而当故障修复后,网络又可自动接通。因此,Modbus 协议的可靠性较好。

1 接口标准:

此协议支持传统的 RS-232、RS-422、RS-485 设备。许多工业设备,包括 PLC,DCS,智能仪表等都在使用 Modbus 协议作为他们之间的通讯标准。

2 通讯数据格式:

采用主从控制方式,上位机为主站,仪表为从站。通信数据格式采用数据链格式,数据链包括设备地址、命令、数据、校验等内容:

主机发送帧格式:

仪表号(站号)(1 字节) 命令字(1 字节) 起始地址(2 字节) 数据的数量(2 字节) CRC 校验

从机应答帧格式:

仪表号 命令字 返回的数据长度(1 字节) 数据 1 高字节 数据 1 低字节..... CRC 校验

(1) 仪表号: 仪表的地址

(2) 命令字: 03 为读,06 为写

(3) 数据高字节:16 位 2 进制数的高 8 位 数据低字节:16 位 2 进制的低 8 位

(4) 起始地址: 32 位 2 进制数 数据的数量:32 位 2 进制数

(5) 返回的数据长度: 数据的数量*2 (数据= 数据高字节+数据低字节)

(6) CRC 校验: 16 位

3 通讯波特率:

波特率设置: 1200baud, 2400baud, 4800baud 和 9600baud 可选。

通讯发送命令字范例

读命令:

主机需要查询下位机的数据,下位机的站号(即下位机的地址)为 1;首先主机通过串行口向下位机发送以下数据:

0x01 0x03 0x00 0x00 0x00 0x05 0x85 0xC9

参数含义: 0x01 仪表号(即菜单 CPA 设置中的站号)

0x03 主机读取从机的数据

0x00 起始地址的高字节

0x00 起始地址的低字节(起始地址一般为 0x0000 表示从地址 0 开始读)

0x00 读取数据个数的高字节

0x05 读取数据个数的低字节(这里是 5 个数据,10 个为 0x0A)

0x85C9 CRC 校验

下位机收到经上主机发送的数据后,向主机发送以下数据:

0x01 0x03 0x0A 0x01 0x02.....0x0A CRC 校验字

站号 命令字 数据长度 仪表数据

0x01 0x02 为状态字 PSW

0x03 0x04 为 PV 值

.....根据各个仪表的不同的(读出的)通讯参数地址分别为不同的参数.

写命令:

主机向下位机写入数据,下位机的站号(即下位机的地址)为 2. 主机通过串行口向下位机发送如下数据:

0x01 0x06 0x00 0x01 0x03 0x20 0xD9 0x22

站号 写命令字 写入的地址 写入的数据 CRC 校验

写入的地址要根据各个仪表不同的(可写入的)通讯参数地址分别为不同的参数.(注: 例: 在自整定 PID 仪表中.写入的地址 01 为目标值.(SU 值),而读的地址 01 却是过程值(PV 值).读和写的地址代表的意义是不同的,这点请注意.在通讯参数和名称中也有区分开来.)

写入的数据为 10 进制转化的 16 进制数,上例中 0x0320 为 10 进制数的 800.

下位机收到经上主机发送的数据后, 会向主机发送同样的数据.