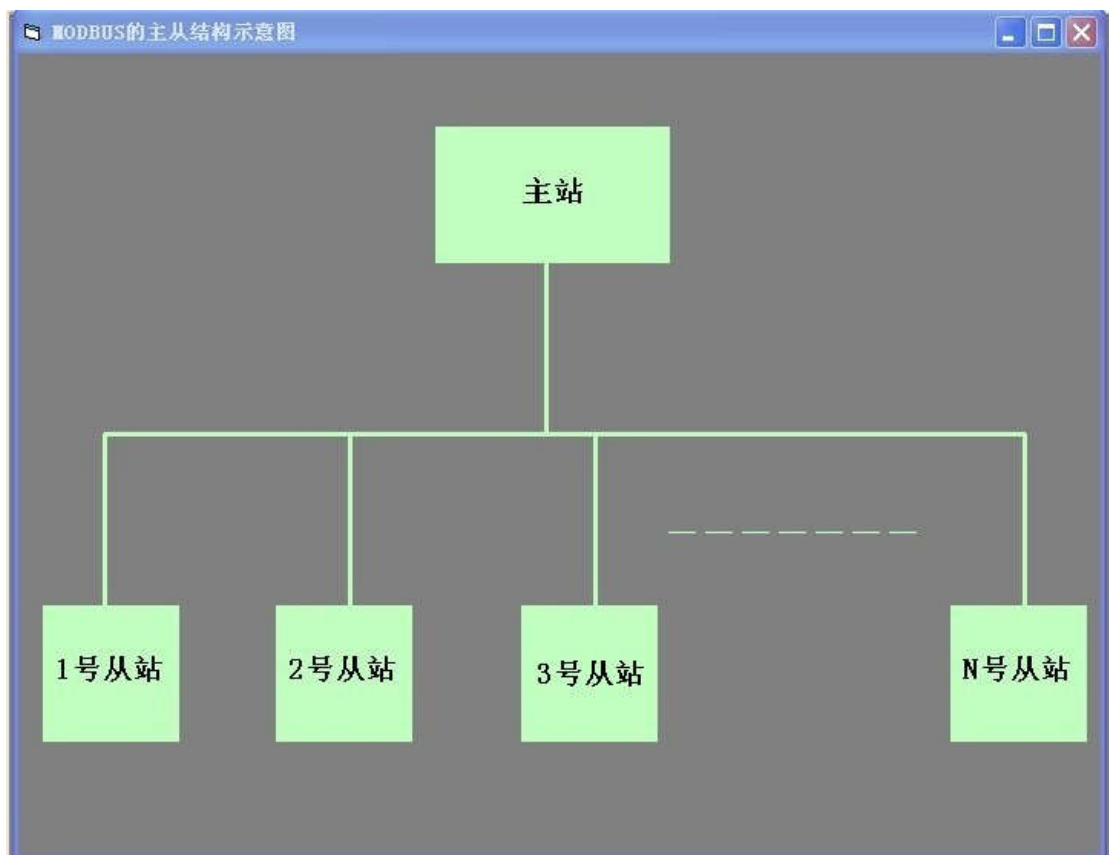


MODBUS协议、通讯格式、传输方式

MODBUS简介

MODBUS 是一种单主站的主/从通信模式。**MODBUS** 网络上只能有一个主站存在，主站在 **MODBUS** 网络上没有地址，从站的地址范围为 0 - 247，其中 0 为广播地址，从站的实际地址范围为 1 - 247。



MODBUS 通信标准协议可以通过各种传输方式传播，如 RS232C、RS485、光纤、无线电等。

MODBUS 具有两种串行传输模式，**ASCII** 和 **RTU**。它们定义了数据如何打包、解码的不同方式。支持 **MODBUS** 协议的设备一般都支持 **RTU** 格式。通信双方必须同时支持上述模式中的一种。

实际也就是发送与接收双方商量一下，定好规则，发送方想要接收方做某件事，就发送某种格式的信息给接收方，接收方收到信息后，按照事先约定好的规则分析信息，执行命令。

您如果愿意，也可以自己定义一个通讯规范，用PLC 或是VB 语言按照您自

已定义的这个规范处理,如果您定义的这个规范可靠性、便于分析性超过MODBUS,那您的通讯规范就是最流行的了!

MODBUS 的通讯规范:

起始符 + 设备地址 + 功能代码 + 数据 + 校验和 + 结束符

通讯格式

通讯格式设置举例：9600，o，8，1 即：
波特率为9600；
校验方式为奇校验；
数据位为八位；
停止位为一位；

1、波特率：

波特率是每秒钟传输的**数据位数**；什么是位数呢？

计算机处理的语言是“0”和“1”组合而成的信息，即机器语言！
一个“0”或是一个“1”就是一个位；

设置波特率的作用？

如果把波特率设为9600，即一秒钟之内能够传输9600个“0”或是“1”，它决定了通讯的数据传输速度。

常用的波特率数值有：**2400、4800、9600、19200、38400、57600、115200**；

其值越大，通讯传输速度越高，那么是不是把波特率的数值设置的越大越好呢？

当然不是，它要根据现场传输条件来决定，波特率设置的越大，要承担的通讯失败风险越大。

2、数据位：

前面说过，计算机处理的语言是“0”和“1”组合而成的信息，即机器语言！

01000001 ， 01000010 ， 01000011 ， 01000100 ， 01000101， 01000110

A B C D E F

上面一组机器码分别代表的字符是 A，B，C，D，E，F；

如A：是用01000001表示，共八个“0”或“1”，即数据位为八位；

数据位的含义：是一个字符可以用多少个位的组合来表示；

为什么要设置数据位呢？

其一，设置数据位后，我们就知道了数据长度，然后可以根据波特率(9600)计算出传输一个字符A需要多少时间。

如果数据位设为8, 则:

$$8/9600=0.00083\text{秒}$$

即传输一个字符“A”需要0.83毫秒的时间（这不是正确的计算，原因在停止位的解释中再论述!）

其二，定义一个标准，方便通讯双方分析。

合法的数据位值：4、5、6、7、8

目前常用的数据位是8位与7位。

3、停止位：

设置了数据位，就可以正常通讯了吗？不是！接收方何时才知道一个字符传输结束了呢？

这就需要有一个停止位，有停止位当然还需要一个**起始位**来告诉接收方一个字符的传输开始！

为什么要设置停止位呢？

上面解释过了，即，知道一个字符何时传输结束！

目前常用的停止位是一位与二位。

还有一个问题，为什么在通讯格式中不用设置起始位？

我所知道的是：

停止位是一个高电平(1)，当接收方接收到连续的高电平时，表示一个字符传输结束。

起始位是一个低电平(0)，当接收方接收连续的低电平时，表示下一个字符的传输开始。

如果停止位可靠(1位或是2位)，那么干扰造成低电平起始位假象的可能性就不大，所以不用设置起始位！

在数据位的解释中，我计算过传输一个数据位设为八位的字符“A”的传输时间， $8/9600=0.00083$ 秒，即0.83 毫秒的时间传输一个字符A，现在您应该知道了，这个计算并不正确，因为没有加上起始位数和停止位数！

现在我们重新计算：

假如设置停止位为2，则一个起始位，两个停止位，8个数据位，总位数为11。

$11/9600=0.0011$ 秒，即传输一个字符“A”需要1.1毫秒的时间（这还不是正确的计算，原因在校验方式的解释中再论述!）

4、校验方式:

朋友们都知道,干扰是无处不在的,如果抗干扰处理的不理想,在通讯传输过程中,"0"可能会变成"1",或是将"1"干扰成"0",造成传输错误.

干扰是消除不了的,提高抗干扰能力也只是提高而已,并不能完全防止干扰。所以因为干扰造成的传输错误一定会发生。接收方如何知道接收到字符是否正确呢?

解决方式就是加上一个校验,即在传输的数据中再加上一个校验位!

目前所用的校验方式为:

偶校验(even):简单表示为"e";

奇校验(odd):简单表示为"o";

无校验(none):简单表示为"n";

偶校验: 如果一个字符中"1"的个数是奇数那么校验位就置为"1";

如果一个字符中"1"的个数是偶数,那么校验位就置为0;

从而保证总的1的个数是偶数;

比如设置数据位为8位,字符"A"是: 0100 0001

其"1"的个数是2个,为偶数。那么校验位则为"0" 真正发送的信息为:

0100 0001 0

奇校验: 如果一个字符中"1"的个数是偶数,那么校验位就置为1;

如果一个字符中"1"的个数是奇数,那么校验位就置为0;

从而保证总的"1"的个数是奇数;

比如设置数据位为8位,字符"A"是: 0100 0001

其"1"的个数是2个,为偶数。那么校验位则为"1" 真正发送的信息为:

0100 0001 1

无校验: 没有校验位;

校验位的作用:

如果在传输过程中,由于干扰将某个"0"变成了"1",

偶校验时,"1"的个数因为干扰变成奇数,

奇校验时,"1"的个数因为干扰变成偶数,

接收方会返回一个奇偶校验错误信息给发送方。

比如：

当采用奇校验时，发送“A”字符的

0100 0001 1

当传输到接收方，由于干扰变成了

0100 0011 1

接收方接收到四个“1”，是偶数，不符合奇校验的“1”的个数为奇数的规定，所以返回一个奇偶校验错误信息给发送方！

注意：

奇偶校验方式不可能完全校验一个字符发送是否正确！

比如采用奇校验方式时，

发送“A”字符时

0100 0001 1

由于干扰接收方接收到的是

0100 0010 1 （是“B”）

由于只是“1”的位置改变了，“1”的个数还是奇数，虽然发送的是A，接收到的是B，但是奇校验还认为是正确的字符；

为了解决奇偶校验方式的上述缺陷，每种标准协议都会要求校验和计算，

比如 MODBUS通讯协议的 RTU 方式是 CRC 校验计算；

MODBUS通讯协议的 ASCII 方式是 LRC 校验计算；

有些朋友对于奇偶校验 与 校验和计算 这两个概念分不清楚。

奇偶校验：判断一个字符传输的是否正确；

校验和：判断一组字符传输的是否正确；

在停止位的解释中，我计算过传输一个数据位设为八位，停止位设为2位的字符“A”的传输时间，一个起始位，两个停止位，8 个数据位，总位数为11。

$11/9600=0.0011$ 秒，即1.1 毫秒传输一个字符A，现在您应该知道了，这个计算并不正确，因为没有加上校验位！

现在我们重新计算：

通讯格式为：9600，0，8，2

一个起始位，八个数据位，一个校验位，两个停止位，总位数为12。

$12/9600=0.00125$ 秒，传输一个字符“A”需要1.25毫秒的时间；

这个计算值才是最后的理论计算值！可以大致评估传输一组字符需要的时间！当然，选用无校验方式，计算传输方式不需要加上校验位

需要永远记住的是：*****参预通讯的双方设定的通讯格式必须一样的*****

传输方式

传输方式没什么好讲，只是有初学者询问我问题时，我问采用的通讯协议是什么，对方回答是**485**通讯，这明显是搞乱了**传输方式**与**通讯协议**两个概念，所以用一两句话大致说一下：

485通讯，**232**通讯，这讲的是采用何种传输方式！既然是传输方式，重要就是“传输”两字，不管是**232**还是**485**，只是起到传输作用，可以传输**MODBUS**通讯协议信息，也可以传输**其他通讯协议**信息！

或者说：

MODBUS通信标准协议可以通过各种传输方式传播，如**232**、**485**等！

顺便说一下**终端电阻**的作用：

光从空气进入水面时，水面从反射回一些光线，这是因为空气与水的媒质不同。光进入不同的媒质时，会在临界点反射。

电信号传输也一样，在传输过程中如果传输末端阻抗突然减小甚至没有，信号就会在此产生反射，这种反射会造成传输线路数据混乱，所以加一个偏置电阻，人为地保持阻抗平衡，减弱信号反射对线路的影响！

海为 plc 伺服驱动器 modbus 通讯相关程序

信捷 plc modbus 通讯例子程序

西门子 SMART 200 PLC modbus 通讯程序

烟台信科电气有限公司

电话 微信 13396452298