



# 其实，Modbus通讯很简单！——手把手教你



叶子的时候回来 图书馆



6 馆藏 106

2017-12-04 叶子的时候... 来源 阅 10219 转 38

分享： 微信 转藏到我的图书馆

## 主要内容：

S7-200 PLC Modbus通讯概述

S7-200 PLC Modbus通讯指令

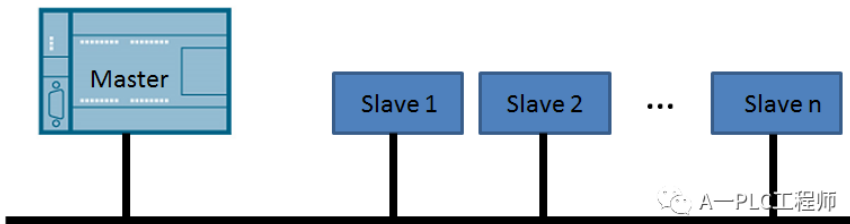
S7-200 PLC Modbus通讯常见问题

## (1) Modbus通讯

S7-200的Modbus通讯：

S7-200只支持Modbus RTU协议，不支持Modbus ASCII协议；

Modbus是一种单主站的主/从通信模式。一条Modbus网络上同时只能有一台主站，从站可以有若干个（如下图所示）。从站的地址范围为1-247；



一个Modbus通讯的传输字符应包括一个起始位，8个数据位，1个或0个校验位（奇偶校验或无校验可选择），以及一个停止位

在S7-200 CPU通信口上实现的是RS485半双工通信，使用的是S7-200的自由口功能。

Mode	FC	Meaning
RD ('0')	01	读取单个/多个线圈 (DO) 状态
	02	读取单个/多个线圈 (DI) 状态
	03	读取单个/多个保存寄存器
	04	读取单个/多个输入寄存器 (AI) 状态
WR ('1')	05	写单个线圈 (DO)
	06	写单个保存寄存器
	15	写多个线圈
	16	写多个保存寄存器

Modbus		S7-200	
Data area	MB-Address	Data area	PLC Address
Output	1-128	DO	Q0.0-Q15.7
Input	10001-10128	DI	I0.0-I15.7
Input	30001-30032	AI	AIW0-AIW62
Holding Reg.	40001-4xxxx	Holding Reg.	T-T+2*(xxxx-1)

## TA的最新馆藏

空调换万能板求助

手把手教你更换空调万能板，你也...

三菱FX3U系列PLC扩展232通讯口...

威纶通触摸屏与三菱PLC通信的接...

区分威纶触摸屏串口RS485 2W与R...

三菱PLC圆头8针的rs422接口定义



喜欢该文的人也喜欢

更多

归类总结卤味香料的调香技巧及香...

学科 | 最易误读的32个文史常识，...

麻烦通常是跟着女人一起来的，尤...

中药记忆口诀，先记住慢慢理解

光锥之外，皆是虚无；光锥之内，...

《增广贤文》：40句至理名言，40...

跟领导去喝酒，作为下属应该怎么...

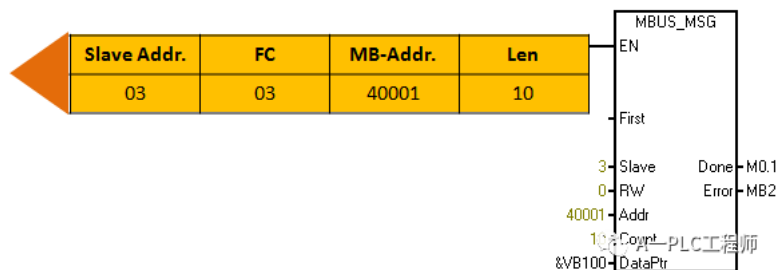
2017年度党政领导班子履行党风廉...

传世秘方100个

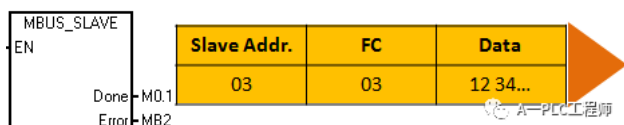


上图是一个典型的主站和从站的网络结构，对于Modbus主站而言可以对从站进行读或者写的操作，其中它所支持的功能码（FC，Function Code）包括主站左侧表格中所述功能，例如功能码为'01'时表示读取单个/多个线圈（DO）状态或功能码为'04'时表示读取单个/多个输入寄存器（AI）状态。而对于从站，我们只需要把Modbus的标准地址和从站的地址对应关系建立好就可以了，S7-200的从站与Modbus标准的对应关系如从站右侧表格所示。表中左侧是Modbus标准地址码，其中1-128对应于S7-200的Q0.0-Q15.7，10001-10128对应于S7-200的I0.0-I15.7，30001-30032对应于AIW0-AIW62，40001-4xxx对应的是S7-200的保持寄存器（V区），它的范围是T-T+2\*(xxxx-1)，T表示的是V区的起始地址，这一点由Modbus从站的指令所决定的。

1 硅胶垫圈	7 电路板设计	13 免费云服务器
2 尼龙垫片垫圈	8 橡胶现货价格	14 免费的网页游
3 高级软件工程	9 包装设计网	15 免费云主机
4 ui设计工程师	10 电机	16 硅胶垫圈
5 尼龙垫圈	11 电路板	17 尼龙垫片垫圈
6 软件工程师待	12 最火的网页游	18 高级软件工程

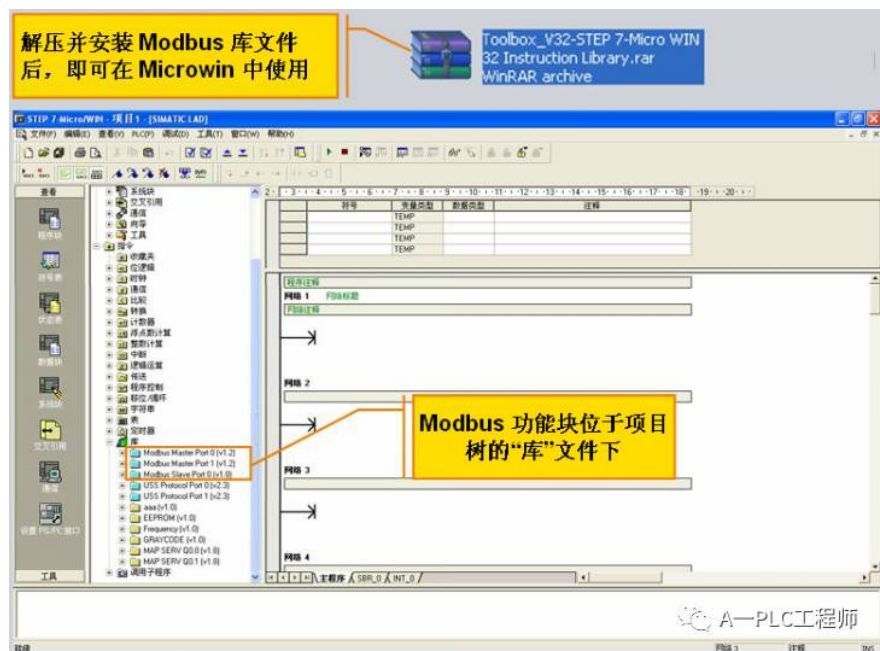


Modbus的主站指令叫做MBUS\_MSG，通过这条指令可以将Modbus的标准报文发给从站，例如在上图例子当中从站的第一个字节是03，表示的是从站的地址，FC功能码为03，表示的是读取单个/多个保存寄存器，Modbus标准地址是40001，长度是10。随着功能码的不同，报文的格式会发生相应的变化，具体的报文格式需要去参阅Modbus的通讯手册。



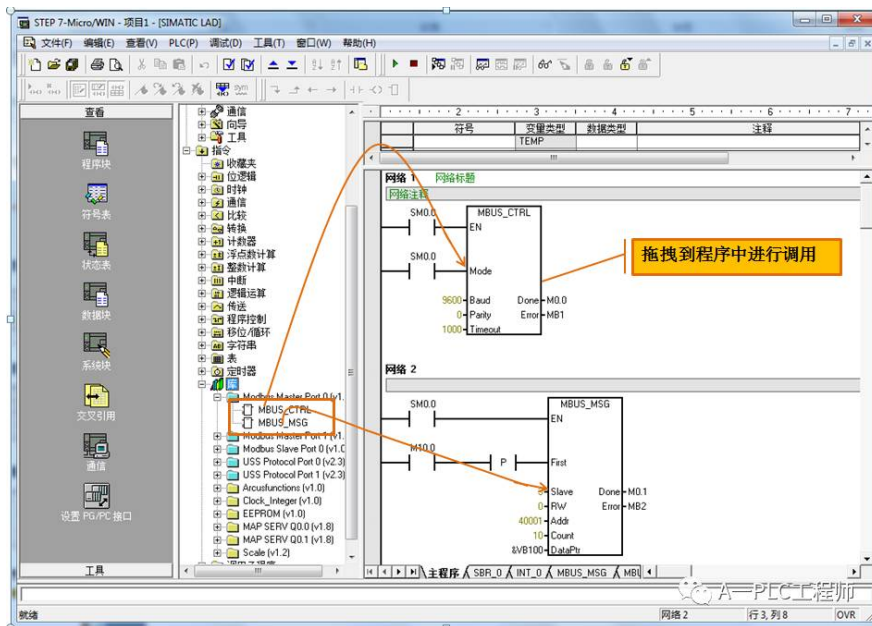
从站的指令时MBUS\_SLAVE，在接到主站发给它的报文后会根据报文的需求返回报文，比如在上图例子中返回的格式是第一个字节为从站的地址，第二个为功能码，第三个是数据返回给主站，这样就完成了一次Modbus通讯的请求与应答的过程。

## (2) Modbus库文件的安装和调用

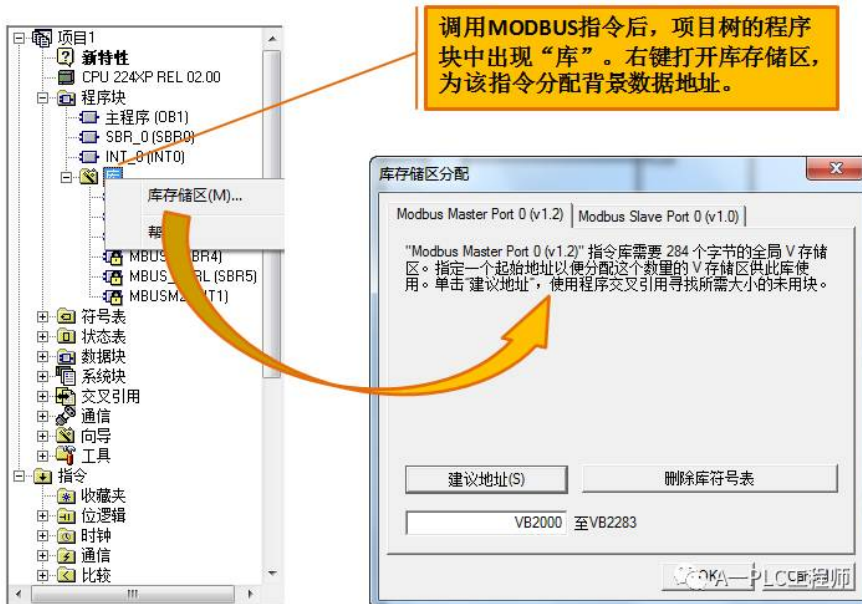


如果想要应用Modbus指令库，那么首先需要到因特网上或者向西门子的客服人员申请名称为'Toolbox\_V32-STEP 7-Micro WIN'的指令库，将它解压并且安装到Micro WIN当中就可以使用了，安装后会在Micro WIN的库文件当中出现上图标记的三个库，其中Port0和Port1都可以做Modbus Master，而Slave只有Port0口可以做。

## (3) Modbus库文件的使用

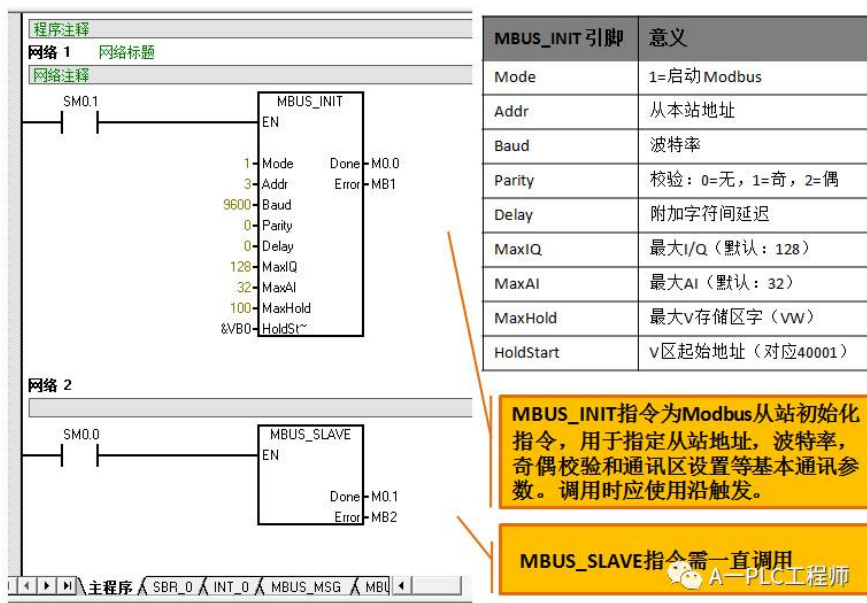


使用方法很简单，打开Modbus主站指令库会有相应的指令块出现，直接把指令块拖拽到程序当中进行调用就可以了。



在调用Modbus库指令的时候，需要注意一定记得为Modbus库文件分配库存储区。具体的方法是右键单击库，然后选择库存储区，在弹出来的对话框当中可以选择建议地址，自动分配一个程序里面不会用到的地址区间，也可以人为地手动填写起始地址，这个区间在程序当中不可以和其他的数据区相冲突，否则Modbus功能将不正常。所谓的库存储区其实就是Modbus指令库能够正常工作所必须的一部分背景数据，只要给它分配好区间并保证不与程序当中其他的地址相冲突就可以了。

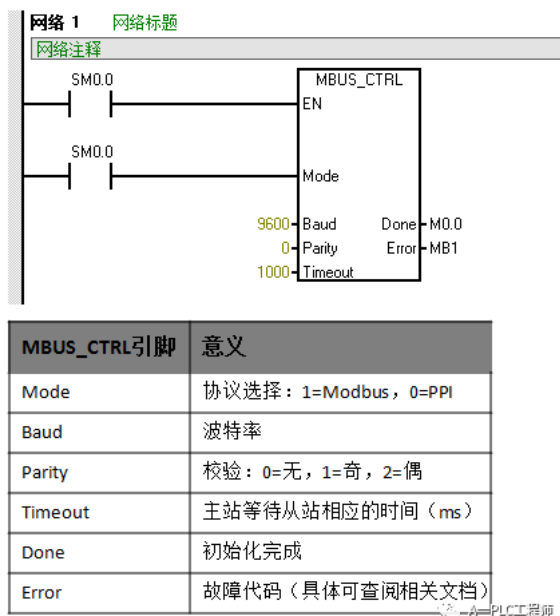
#### (4) Modbus从站指令



从站指令一共有两条，第一条是从站的初始化指令（MBUS\_INIT），另一条是MBUS\_SLAVE从站指令，在Modbus从站的初始化指令当中涉及哪些内容呢？首先，第一个引脚Mode表示等于1的时候是启动Modbus，等于0的时候是关闭Modbus，Addr表示的是这个从站的从站地址，Baud表示波特率，Parity是奇偶校验，0是无校验，1是奇校验，2是偶校验，Delay是附加字符之间的延迟，MaxIQ表示的是最大I/Q地址（默认128），MaxAI表示的是最大AI长度（默认32），MaxHold表示的是最大的V存储区（VW），最关键的是HoldStart，表示的是V区起始地址（对应40001），在之前已经提到过S7-200作为从站的时候，它的V区地址对应于Modbus标准地址的起始地址是可更改的，那么就在这里进行设定，在本例中如果HoldStart写的是VB0，那么40001对应的地址就是VW0，40002对应的地址是VW2，40003对应的地址是VW4，以此类推，每一个标准的Modbus地址码对应的是一个Word，以字为单位，同样如果这里设的是VB100，那么40001对应的就是VW100，40002对应的是VW102，以此类推。这一条初始化指令只需要调用一次就可以了，所以在上图中用的是SM0.1在上电的时候执行一次就可以了。

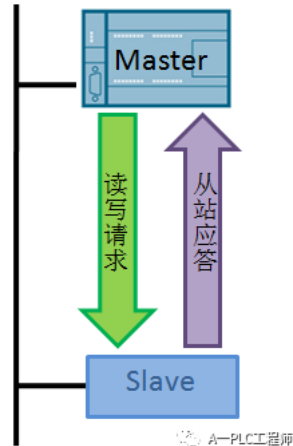
MBUS\_SLAVE这个功能块必须要用前面的条件必须是一直为1的，上图中用SM0.0。

## (5) Modbus主站指令

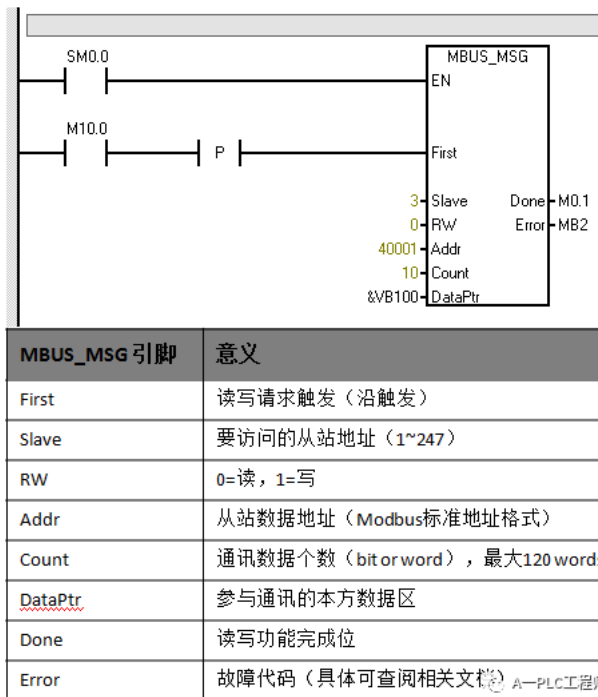


Modbus主站指令当中的第一个块叫做MBUS\_CTRL，MBUS\_CTRL有哪些内容呢？我们来看一下引脚定义的说明：首先Mode写1的时候是选择Modbus，写0的时候是选择PPI；Baud表示波特率；Parity是奇偶校验，0是无校验，1是奇校验，2是偶校验，这与从站的设置相类似；Timeout表示的是主站等待从站响应的的时间（ms）；Done位是初始化完成；Error位表示的是故障代码。其中值得一提的是Timeout这个时间，主站等待从站响应的的时间指的是什么呢？让我们来看一下主站和从站之间通讯的过程：

主站的读写请求发出后，从站应当在Timeout指定的时间内返回应答



首先，主站会发一帧读写请求给从站，在主站的读写请求发出后，从站应当在Timeout指定的时间内返回应答；如果在此时间内从站没有应答，则主站发第2次读写请求，第2次还不行发第3次读写请求，如果连续3次在此时间内从站没有应答，则主站认定从站无相应，放弃该从站并报错。



下面来看主站的读写命令（MBUS\_MSG），看一下引脚说明：首先First指的是读写请求触发（沿触发），每当First这一端来了一个沿，Modbus指令便会做出一次读或者写请求，RW标示的是这一次的命令是读还是写，0表示读，1表示写；Addr表示的是从站数据地址（Modbus标准地址格式），0开头、1开头、3开头和4开头的；Count指的是通讯数据的长度，最大120个字，单位可能是bit或word；DataPtr指的是参与通讯的本方数据区，如果是读指令标示的是读回来的指令放在本地的哪一块数据区，如果是写命令表示的是把本地的哪一块数据发给对方；Done位和Error位分别是功能完成和故障代码。

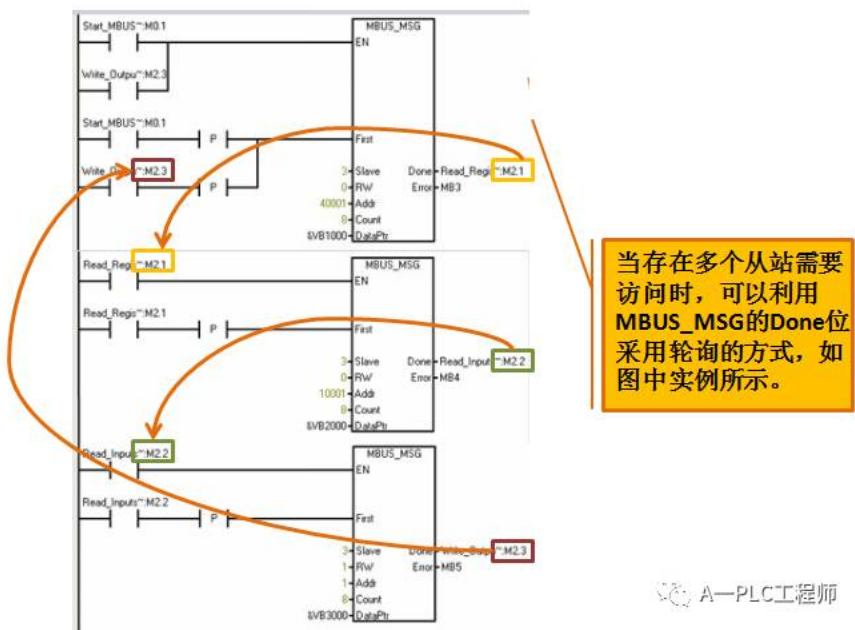


当Count的单位是Bit时，需要注意，此时Count的数字应当为8的整数倍。否则会出错，这是因为一个基本传输字符是包含8个数据位的，没有办法只传送一个Bit。

MBUS_MSG引脚	意义	MB-Address	Data area (for S7-200)	Count unit
First	读写请求触发（沿触发）	1-128	DO	Bit
Slave	要访问的从站地址（1~247）	10001-10128	DI	Bit
RW	0=读，1=写	30001-30032	AI	Word
Addr	从站数据地址（Modbus地址格式）	40001-4xxxx	寄存器	寄存器
Count	通讯数据个数（bit or word），最大120 words			
DataPtr	参与通讯的本方数据区			
Done	读写功能完成位			
Error	故障代码（具体可查阅相关文档）			

其中值得一提的是Count，刚才讲过它的单位可能是bit或word，究竟是bit或word取决于当时所用的Modbus标准的地址码是用的哪一块，如果对于1-128而言这是一个DO的输出，对于1开头的的是一个DI的输入点，这个时候Count的单位指的是bit，而对于3开头和4开头的，那么是AI和寄存器，它们的单位是word，需要注意的是当Count的单位是Bit时，一定Count

(6) Modbus主从站轮询



当存在Modbus多主站轮询的时候，在程序当中我们应当如何处理呢？上图中展示了这种方法。例如第一个MBUS\_MSG指令我们可以利用它的Done位（本例中为M2.1），把它作为第二条MBUS\_MSG指令的First前面的激活端，也就是说第一个MBUS\_MSG完成的时候才会去激活下一条MBUS\_MSG指令，那么同样，第二条指令完成时我们把它作为第三条MBUS\_MSG指令的激活条件，在最后又把第三条指令的完成位还给第一条网络，这样的话就构成了一个循环的轮询方式。

(7) Modbus FAQ

- Q1: S7-200是否支持Modbus ASCII模式？
- 答: S7-200可以支持上述模式，但是没有现成的指令库，需要用户自己利用自由口的方式编程。
- Q2: 项目编译后为何出现很多错误？

宏碁 (Acer) S...

罗技 (Lo

罗技 (Lo

答：使用指令库时，若编译后出现很多错误，一般是因为未指定库指令数据存储区。

Q3：Modbus从站的网络地址与S7-200的CPU网络地址有何关系？

答：没有关系。支持网络通信的通信协议必须有其自己的网络寻址规定。Modbus从站的地址只是它在Modbus网络上的地址，而通常所说的S7-200 CPU地址是CPU在西门子的PPI网络上的站地址。

Q4：MBUS\_MSG指令中代表数据长度的COUNT引脚单位是什么？


答：对于Modbus地址=0xxxx或1xxxx的，引脚单位为Bit；对于Modbus地址=3xxxx或4xxxx的，引脚单位为Word。

Q5：如何访问大于9999的保持寄存器地址？

答：Modbus Master协议库支持超过9999的保持寄存器地址。地址范围为400001-465536。只需在调用MBUS\_MSG子程序时给Addr参数赋相应的值即可，如416768。

Q6：为何有些HMI软件使用Modbus RTU读取S7-200中的实数会出现错误？

答：不同的厂家关于浮点数格式定义的不同，西门子的PLC遵循的是高位低存的规律，和其他的厂家有可能会不一样，这样读回来的实数或整数的高低字节会发生反转，这个时候可以通过监控 判断。在程序当中把它掉过来就可以了。

 **个人图书馆**  
360doc.com

千万人在用的知识管理与分享平台

我的图书馆

搜文章 找馆友

留言交流

答：Error 0#表示Modbus正在忙于其他请求。MBUS\_MSG指令同时只能允许有一个读写操作处于运行过程，如果在一个读写操作尚未完成时启用另外一个读写请求，就会发生Error 6 #。利用Done位可以对规避这一问题。

Q8：MBUS\_MSG显示Error 3#？

答：Error 3#表示从站无应答。即主站的读写请求发出后，从站没有在Timeout时间内返回报文。多种原因可以引起此故障，包括：

硬件故障（线路，端口等问题）。

错误的从站地址，波特率，奇偶校验。

从站不支持此功能码，或不能被从站识别的从站数据地址。

Timeout时间过短（从站响应较慢），通过延长Timeout可以解决这个问题。

关注本公众号，可提高PLC技术，拓宽PLC知识。

转载到我的图书馆      献花 (0)      分享：      微信 ▼

来自： [叶子的时候回来](#) > 《文件夹1》

[以文找文](#) | [举报](#)

上一篇：[据说使用PLC有9大原则，来看看对不对](#)

下一篇：[以太网通讯必须懂的技能——网线的制作与应用](#)

#### 猜你喜欢

				
管道疏通机器人	男孩早熟怎么办	综合布线	碳纤维布加固	磁翻板
				
伺服电动缸	不锈钢把手	电气控制柜	rs485通讯电缆	东方 马达

#### 类似文章

[更多](#)

#### 精选文章

[分分钟玩转通讯！智能控制的语言之——M...](#)

[西门子S7-200系列PLC的MODBUS通信功能（...](#)

[【玩转485】17.modbus通讯概述【连载17】...](#)

[谨记做人之大忌](#)

[降血压有四个特效穴位——不花一分钱?您不妨...](#)

[豆腐的多种吃法（附图）\\*](#)



aGV

  
宏碁（Acer）S...

  
罗技（Lo

  
罗技（Lo

  
罗技（Lo

- S7-200与变频器的MODBUS RTU通讯

Modbus RTU 主站指令库

问题详情

S7-200做主站S7-300 CP341做从站的Modbu...

USS通讯是“神马”？看完你就懂。

1 磁翻板液位计

2 通达泵业

3 男孩早熟怎么办

4 陪玩
- 苏共垮台对中共的警示

史上最全Excel键

5种中药零食乱吃会伤身

鸡蛋的艺术创意

白岩松：信仰缺失下的迷茫

1 博易大师博易大师,2018智能..

2 自闭症怎么解决,先评估再训..

3 今日诊股\_行情查询\_大盘趋..

发表评论

请 [登录](#) 或者 [注册](#) 后再进行评论

社交帐号登录：



**aGV**













宏碁（Acer）S...



罗技（Lo



六象（DXWRIT...



罗技（Lo