UN 200 SMART Modbus RTU 快速入门

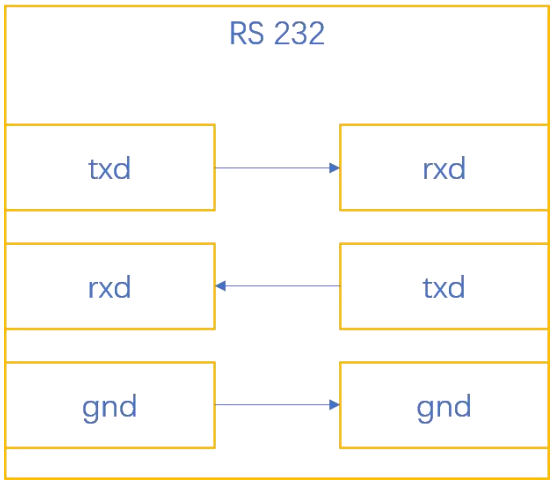
0. 阅读提示

本文旨在帮助读者初步了解 UN 200 SMART Modbus 通讯，笔者认知有限，文中难免有误，欢迎来电交流，联系方式：4000300890。
文中内容涉及硬件连线、地址、功能码及报文、编程几个方面，可初步的了解 Modbus。阅读全文约需 20 分钟，可对 Modbus 有一个初步的了解。对 Modbus 不了解的，实操约需 1 小时。阅读&实操后，可应对 80%的 UN 200 SMART Modbus 通信问题。

1. 硬件连线

1.1. 串口接口

Modbus 通讯原理：Modbus 通讯为主从通讯，即一问一答的方式进行通讯。主站发送响应的数据给某个从站，从站响应；主站没有数据发送时，从站不响应。
这个通讯机制，贯彻到编程思路，后文编程章节中会讲到。
Modbus 协议是运行在串口接口上，常见的串口接口有 RS-232,RS-485,RS-422。Modbus 常用 RS-485 接口。
一般 RS-232 三条通讯线即可完成通讯链路。如图 1 所示，RS232 的设备 1 的 txd 接到设备 2 的 rxd，rxd 接到 txd，可以同时接受或发送，这是全双工模式。因 RS-232 特性限制，只能一对一连接，即一个主站连接一个从站。因此在 Modbus 通讯上 RS-232 接口不多见。



图一 RS-232

RS-485 两条通讯线即可完成通讯链路。如图 2 所示，多台设备的 A 短接为一条线路，B 短接为另一条线路。同一时间只能发送或者接受，此为半双工。多台设备可以挂载同一链路，可实现一台主站、多台从站之间进行通信。此应用场景最为多见。

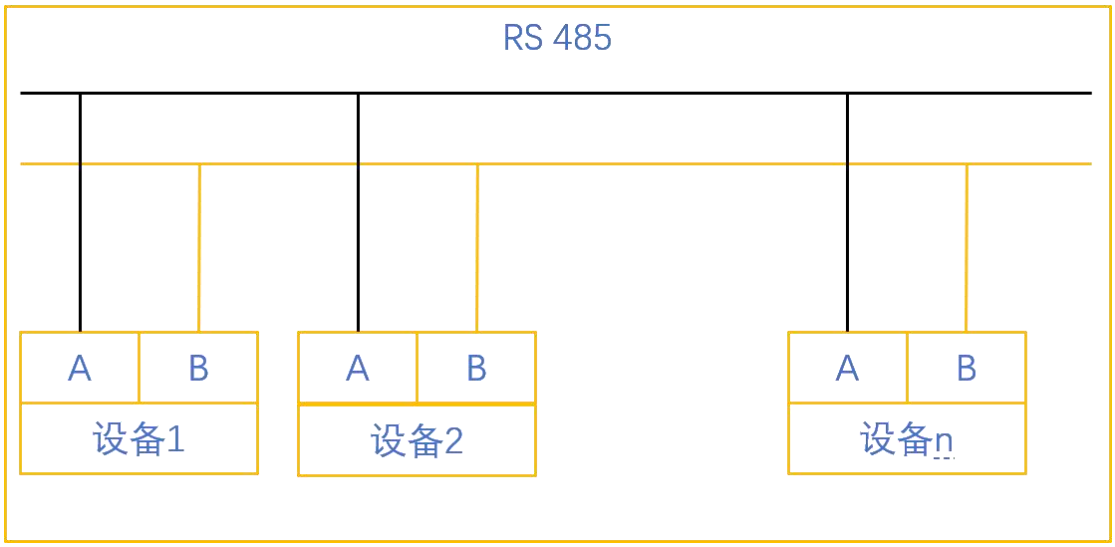


图 2 RS-485

UN 200 SMART 串行接口为 RS-485,引脚示意图如表 3.

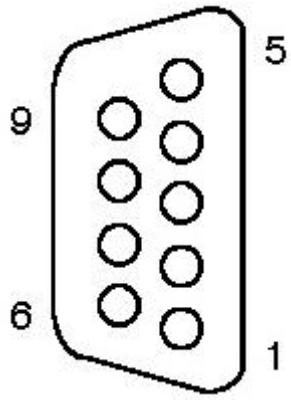
连接器	引脚标号	信号	引脚定义
	1	屏蔽	机壳接地
	2	24V 返回	逻辑公共端
	3	RS-485 信号 B	RS-485 信号 B
	4	发送请求	RTS （TTL）
	5	5V 返回	逻辑公共端
	6	+ 5V	+5 V，100 Ω 串联电阻
	7	+24V	+24 V
	8	RS-485 信号 A	RS-485 信号 A
	9	不适用	NC
	外壳	屏蔽	机壳接地

表 3 UN 200 SMART DB9 引脚定义

注意：RS-485 的 A\B 信号线，通俗叫法有 A\B;485+\485-。UN 200 SMART DB9 引脚中的 3 号引脚，即 RS-485 信号 B，为通俗叫法的 A 或 485+；8 号引脚，即 RS-485 信号 A，为通俗叫法的 B 或 485-。

1.2. 总线连接器

在复杂的工业现场或长距离通讯的情况下，建议选择优质的总线连接器和电缆。亿维自动化的总线连接器自带终端电阻和偏置电阻，在此情况下，可提高通讯的稳定和抗干扰能力。总线连接器和电缆，订货号如表 4。

序号	品名	订货号
1	PROFIBUS 总线连接器 90 度出线无编程口	UN 972-0BA12-0XA0
2	PROFIBUS 总线连接器 90 度出线有编程口	UN 972-0BB12-0XA0

3	PROFIBUS 总线连接器 35 度出线无编程口	UN 972-0BA41-0XA0
4	PROFIBUS 总线连接器 35 度出线有编程口	UN 972-0BB41-0XA0
5	PROFIBUS 总线电缆 紫色两芯屏蔽双绞线	UN 830-0EH10

表 4 总线链接器&电缆

1.3. 为什么选择总线连接器和总线电缆

众所周知，网线有超五类和超六类之分，超五类传输带宽可高达 1000Mb/s，但一般只应用在 100Mb/s 的网络中；超六类主要应用在千兆网络中，在传输性能上远远高于超五类网线标准。超五类，超六类的电缆直观区别就是电缆铜芯线径不同，超六类铜芯明显粗于超五类。同理推测，亿维自动化的总线电缆，回路阻抗：<150R/KM，优于一般通讯电缆。线阻小，通讯距离长，抗干扰能力强。

亿维自动化的总线连接器，自带终端电阻和偏置电阻，同样可以提高通讯的质量。

建议组网方式如图 5:

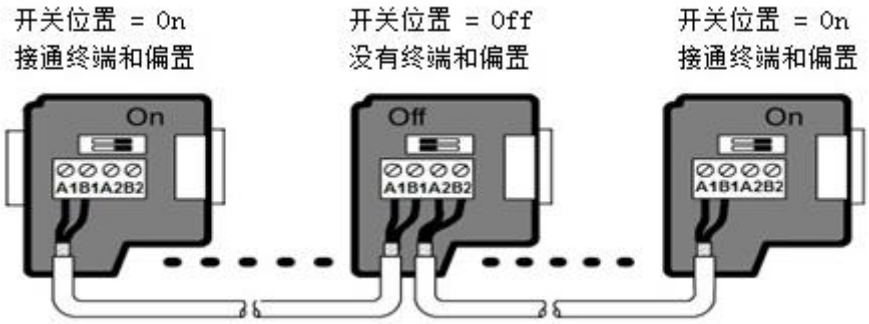


图 5 总线接头

终端和偏置电阻如图 6:

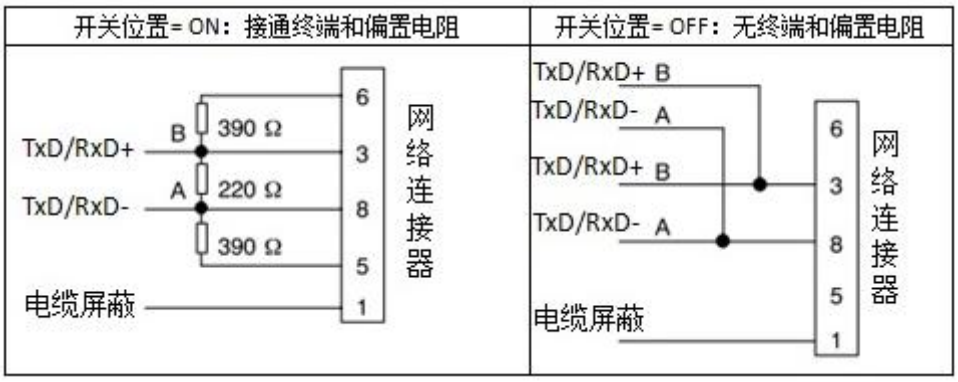


图 6 终端和偏置电阻

1.4. 通讯距离

通讯波特率越高，通讯距离越短。在长距离通讯下，适当降低通讯速率。9600 波特率的最长距离建议在 1200 米。

2. Modbus 地址

通讯的目的是对寄存器进行读写操作，因此需要了解 Modbus 地址的表示方式。
Modbus 地址表示有多种方式，如 40001，4x0001，0000H,此三个地址实为同一个地址。地址中有 4 标识的，为十进制表示方式，起始地址为 1，即实际起始地址为 40001；地址标识中有 H 的，为十六进制表示方式，起始地址为 0。在 SMART PLC 中，地址表示为 40001；亿维 HMI 或常见组态软件中，地址表示为 4x1；在变频器或仪表中，地址常表示为 0000H。
UN 200 SMART 做从站，地址对应如下：
Modbus 地址通常被写为包含数据类型和偏移量的 5 个字符的数值。第一个字符决定数据类型，最后四个字符在数据类型中选择适当的数值。然后，Modbus 主设备将地址映射至正确的功能。Modbus 从站指令支持下列地址：
00001 至 00128 是映射至 Q0.0 - Q15.7 的离散输出
10001 至 10128 是映射至 I0.0 - I15.7 的离散输入
30001 至 30032 是映射至 AIW0 至 AIW62 的模拟输入寄存器
40001 至 4xxxx 是映射至 V 存储器的保持寄存器。
所有 Modbus 地址均以 1 为基位。下表显示映射至 S7-200 地址的 Modbus 地址。
Modbus 地址 S7-200 地址
00001 Q0.0
00002 Q0.1
00003 Q0.2
... ...
00127 Q15.6
00128 Q15.7
10001 I0.0
10002 I0.1
10003 I0.2
... ...
10127 I15.6
10128 I15.7
30001 AIW0
30002 AIW2
30003 AIW4
... ...
30032 AIW62
40001 Hold Start
40002 HoldStart+2
40003 HoldStart+4
... ...
4xxxx HoldStart+2 x (xxxx-1)
对于亿维 HMI，地址对应如表 7:

Modbus 地址	HMI 内部地址	读/写	功能码
0x00001 - 0x60000	LB0 - LB59999	读	功能 1

数字量输出		写	功能 5：写单输出点 功能 15：写多输出点
1x00001 - 1x60000 数字量输入	LB0 - LB59999	读	功能 2
		写	-
3x00001 - 3x60000 输入寄存器	LW0 - LW59999	读	功能 4
		写	-
4x00001 - 4x60000 保持寄存器	LW0 - LW59999	读	功能 3
		写	功能 6：写单寄存器单元 功能 16：写多寄存器单元

表 7 HMI modbus 地址及功能码

3. 报文

对不同的 Modbus 地址进行读或写操作，需要不同的功能码，如上表 7。
常见用的功能码有 FC03、FC06，在此以功能码 03 对报文进行说明。
功能码 03,对寄存器 006BH 开始的三个寄存器进行读操作，主站报文示例如下：

从机地址	功能码	起始地址高位	起始地址低位	寄存器数量高位	寄存器数量低位	CRC 高位	CRC 低位
01	03	00	6B	00	03	74	17

表 8 主站 03 报文

从站报文响应报文如下：

从机地址	功能码	字节数	006BH 高字节	006BH 低字节	006CH 高字节	006CH 低字节	006DH 高字节	006DH 低字节	CRC 高位	CRC 低位
01	03	06	00	6B	00	13	00	00	F5	79

表 9 从站 03 报文

其他报文格式不再说明，有兴趣的可以到官网查询 https://modbus.org/

4. UN 200 SMART Modbus RTU 从站编程

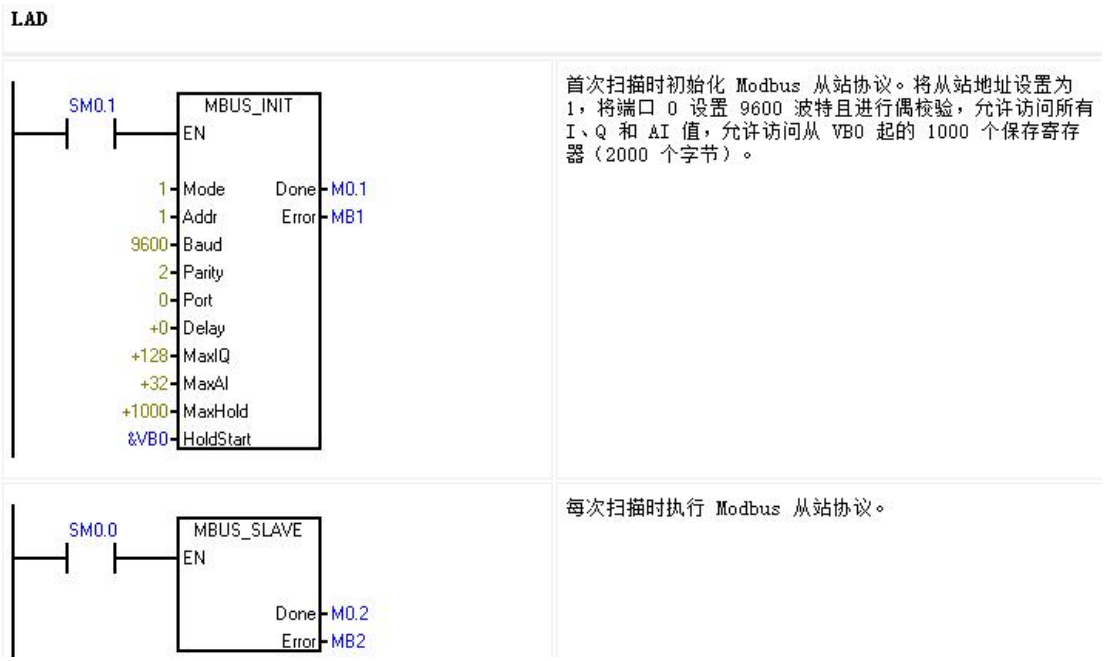


图 10 从站程序

上面程序实现的功能：将 CPU 的 0 口设置为从站地址为 1，波特率 9600，偶校验的 Modbus 从站。

允许主站操作的 IO 数量为 128 个，模拟量 32 个，以 VW0 开始的 1000 个寄存器。CPU 的 VW0 为 Modbus 地址 40001，VW2 为 40002，依次类推。

参数说明：

“模式”(Mode) 输入的值用于选择通信协议：输入值为 1 时，分配 Modbus 协议并启用该协议；输入值为 0 时，分配 PPI 协议并禁用 Modbus 协议。

参数“地址”(Addr) 将地址设置为 1 至 247 之间（包括边界）的值。

参数“波特”(Baud) 将波特率设置为 1200、2400、4800、9600、19200、38400、57600 或 115200。

参数“奇偶校验”(Parity) 应设置为与 Modbus 主站的奇偶验校相匹配。所有设置使用一个停止位。接受的值如下：0（无奇偶校验）、1（奇校验）和 2（偶校验）。

参数“端口”(Port) 设置物理通信端口（0 = CPU 中集成的 RS-485，1 = 可选信号板上的 RS-485 或 RS-232）。

参数“延时”(Delay) 通过使标准 Modbus 信息超时时间增加分配的毫秒数来延迟标准 Modbus 信息结束超时条件。在有线网络上运行时，该参数的典型值应为 0。如果使用具有纠错功能的调制解调器，则将延时设置为 50 至 100 ms 之间的值。如果使用扩频无线通信，则将延时设置为 10 至 100 ms 之间的值。“延时”(Delay) 值可以是 0 至 32767 ms。

参数 MaxIQ 用于设置 Modbus 地址 0xxxx 和 1xxxx 可用的 I 和 Q 点数，取值范围是 0 至 256。值为 0 时，将禁用所有对输入和输出的读写操作。建议将 MaxIQ 值设置为 256。

参数 MaxAI 用于设置 Modbus 地址 3xxxx 可用的字输入 (AI) 寄存器数，取值范围是 0 至 56。值为 0 时，将禁止读取模拟量输入。

参数 MaxHold 用于设置 Modbus 地址 4xxxx 或 4yyyyy 可访问的 V 存储器中的字保持寄存器数。例如，如果要允许 Modbus 主站访问 2000 个字节的 V 存储器，请将 MaxHold 的值设置为 1000 个字（保持寄存器）。

参数 HoldStart 是 V 存储器中保持寄存器的起始地址。该值通常设置为 VB0，因此参数 HoldStart 设置为 &VB0（地址 VB0）。也可将其它 V 存储器地址指定为保持寄存器的起始地址，以便在项目中的其它位置使用 VB0。Modbus 主站可访问起始地址为 HoldStart，字数为 MaxHold 的 V 存储器。

MBUS_INIT 指令完成时，“完成”(Done) 输出接通。

Error 输出字节包含指令的执行结果。仅当“完成”(Done) 接通时，该输出才有效。如果“完成”(Done) 关闭，则错误参数不会改变。

5. UN 200 SMART Modbus RTU 主站编程

上文讲到 Modbus 通讯机制，主站设备同一时间或当前时间只允许发送或接受，对于多个从站，或多次对寄存器进行操作，建议采用轮询机制，即同一时间只允许触发一次 MSG 指令。按照此编程思路，推荐两种轮询操作。

5.1. 主站初始化

将 Modbus 通讯波特率设为 9600，偶校验，超时时间 1000ms，使用本体 DB9 通讯。

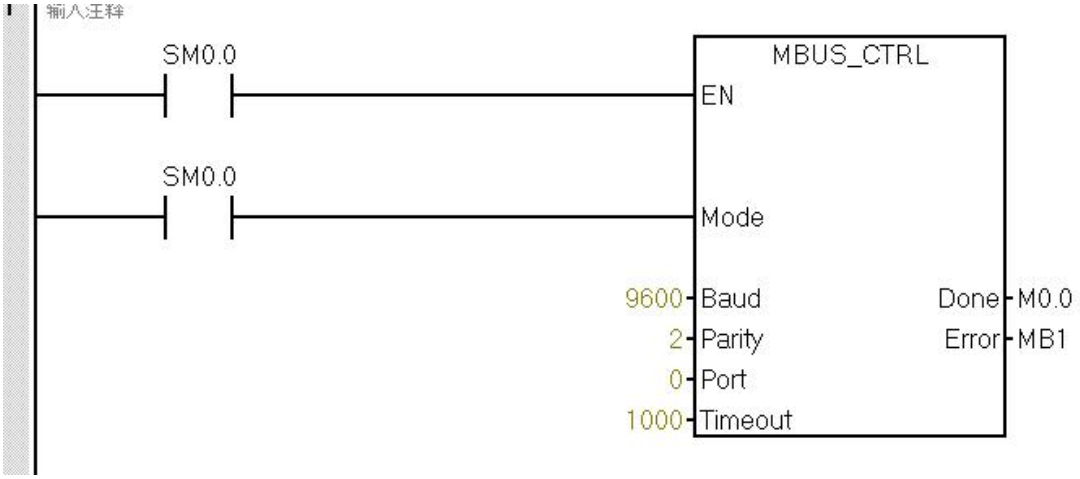


图 11 主站初始化

5.2. 轮询模式一

思路：用 C0 寄存器的数值变化，触发 MSG 指令，确保同一时间只有一个 MSG 在执行。

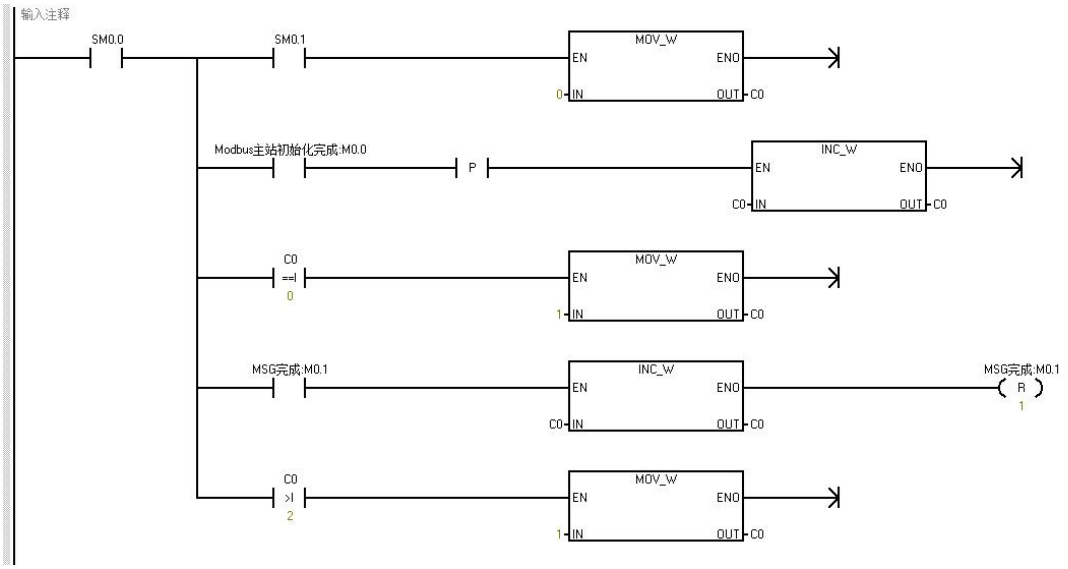


图 12 轮询 1-1

程序功能：上电 C0 清零；主站初始完成后，C0 为 1；每 MSG 指令完成后，C0 自加 1；第三次完成后，再执行第一个 MSG 指令

轮询：

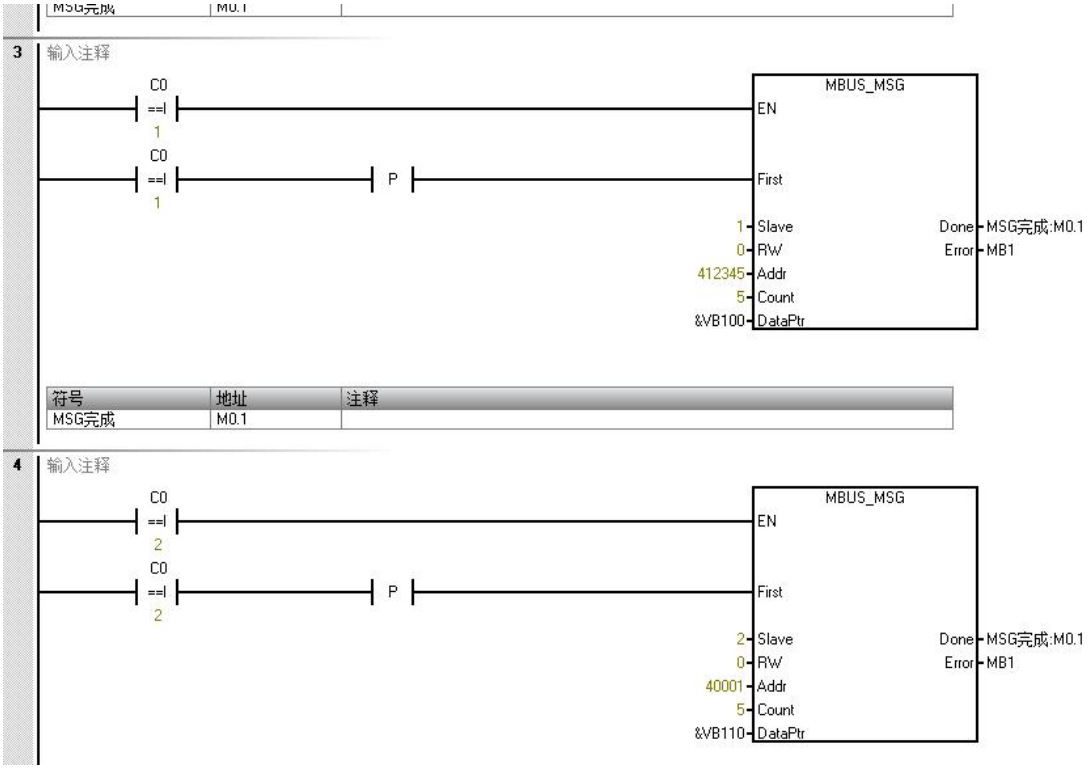


图 13 轮询 1-2

网络 3 程序功能：读取从站地址为 1 的 412345 开始的 5 个寄存器，存放在主站 CPU VW100 开始的 5 个字。

网络 4 程序功能：读取从站地址为 2 的 40001 开始的 5 个寄存器，存放在主站 CPU VW110 开始的 5 个字。

5.3. 轮询模式二

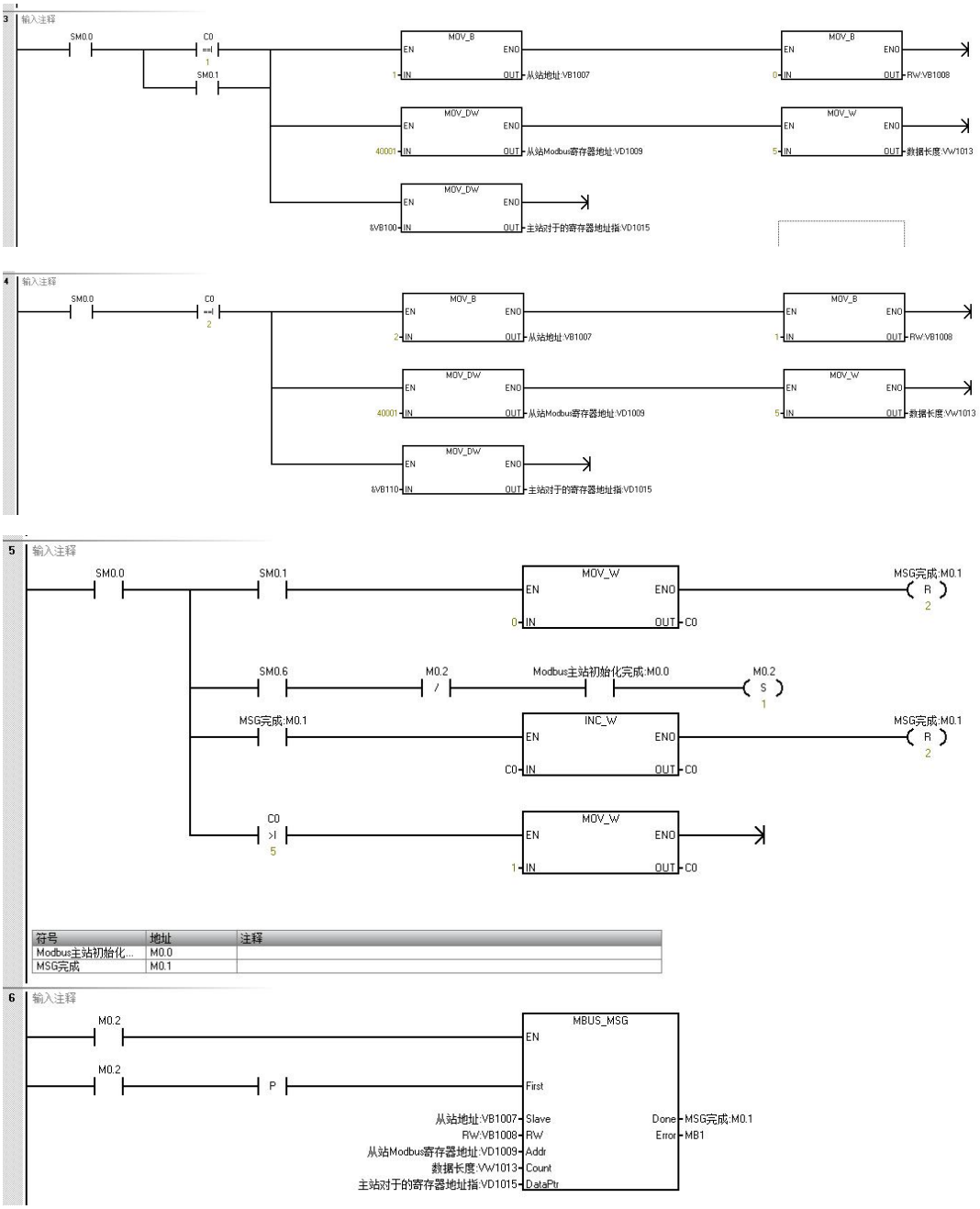


图 14 轮询 2

程序功能：读取从站地址为 1 的 40001 开始的 5 个寄存器，存放在主站 CPU VW100 开始的 5 个字。

将 CPU VW110 开始的 5 个字写入从站地址为 2 的 40001 开始的 5 个寄存器。

也有习惯使用 MSG 指令的完成位置位一个内部继电器 Mx.x，Mx.x 触发下一条 MSG 指令，如此循环的；或固定时间的触发方式，等不同编程思路。不论哪种编程思路，都要确保同一时间只有一条 MSG 指令被触发。

6. 注意事项

A. Modbus 主站或从站初始化指令初始化后，PPI 协议不可用。
B. 同一个串口，只能用作 Modbus 主站、从站、PPI 等其中的一种（程序控制初始化外）。
C. CPU 做主站时，同一时间只能有一条 MSG 指令被触发（重要的事说 N 遍）。
D. UN 200 SMART 的 DB9 RS485 的 A、B 有别于通俗说法的 A、B。
E. 认清从站寄存器地址表示方式，是十进制还是十六进制。
F. 通讯顺利的情况下，可用跳过前四个章节。

7. 问题排查

通讯异常时，建议从以下几个方面排查：

A. 确保通讯电缆连接正确。参考第一章节，重点关注 1.1 章节。
B. 确保主从通讯参数一致。
C. 确认从站的寄存器能被主站进行读写操作。某些变频器或仪表的寄存器只读或只写，或可读可写。某些变频器一次可读或可写的数据长度有限。
D. 以上正常，监控 PLC 程序，检测某一个 MSG 指令是否一直触发，而没有跳转动作。
E. 用电脑串口助手软件，监控通讯报文，定位是主站没有发出数据，还是从站没有响应数据，还是从站响应的报文有误。参考第三章节。
监控通讯报文：将电脑 485 的 A、B 并联在通讯链路上。

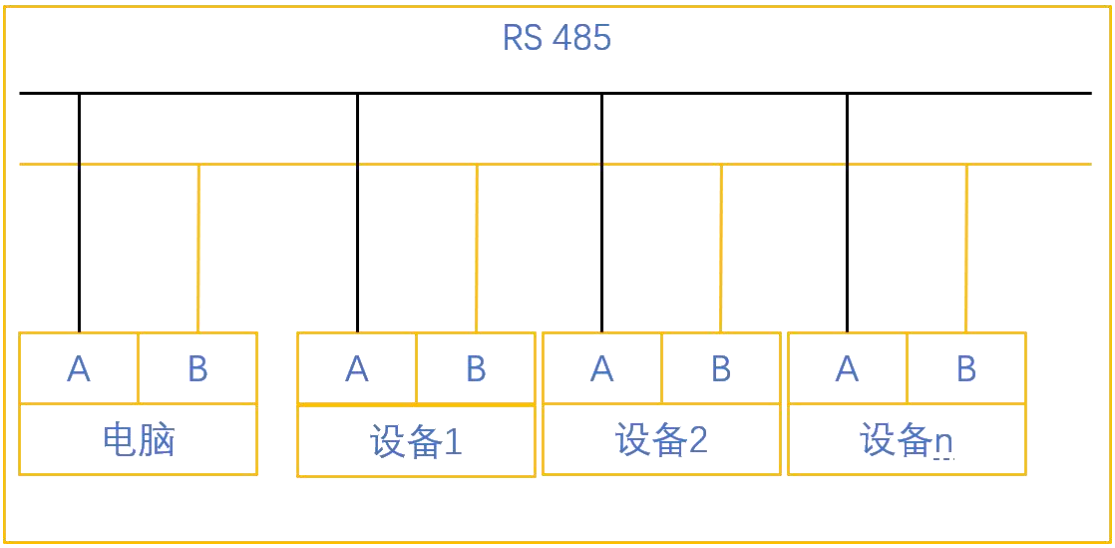


图 15 电脑监听

F. 以上皆正常，通讯仍有问题，拨打电话：4000300890，时刻准备为您服务。

8. 通讯时效

从站数量越多，操作寄存器的次数越多，通讯周期越长。为快速通讯，批量读取或写入寄存器、或提高通讯波特率。若有从站不在线或异常，通讯周期不可控。

以远程会议为例，说明 Modbus 通讯机制：

5 个人远程会议，5 个人同时说话，大家都听不清，实现不了信息交流。

引入主持人机制，主持人即主站，主持人把另外 4 个人都排上序号，1、2、3、4，即 4 个从站。

主持人说话，即主站发送报文，该报文有固定格式，第一个字节为从站地址，即人员编号。

主持人不说话，其他四人不准说话，即便是说话也会被主持人屏蔽。即从站任意发送报文，主站接受的也认为是无效信息。

只有主持人点到谁，谁才能说话，且按照主持人规定的格式发言，即报文格式固定。

主持人说：1 号 xxxx。4 个人都能听到，但只有 1 号可以响应，且要以正确的方式响应。响应错误，主持人也会将信息视为无效信息。

主持人在叫 1 号的时候，1 号开小差，没有及时响应，超过预定的超时时间，主持人再叫一次，如此三次。

三次以后，1 号仍没有响应，主持人放弃 1 号，继续叫 2 号、3 号、4 号，如此即为轮询机制。

正常情况下，一问一答，响应很快。如有一人开小差，通讯周期延长 3 倍的超时时间。

所以，在全员在线的情况下，通讯周期和语速，即波特率有关，人数，即从站数量有关；不在线，通讯周期不可控。

如此，要确保有优质的通讯链路和正常在线的从站，才能保证通讯周期的稳定。