

SIEMENS

S7-200 做主站 S7-300 CP341 做从站的 Modbus RTU 通讯

Modbus RTU Communication – S7-200 as Master and S7-300 CP341 as Slave

Getting-Started

Edition (2010 年 6 月)

摘要 本文档讨论使用 S7-200 做主站，S7-300 CP341 做从站的 Modbus RTU 通讯。

关键词 CP341，Modbus RTU，功能码，S7-200

Key Words CP341，Modbus RTU，Function Code，S7-200

目 录

1. 概述	4
2. 软件环境	4
2.1 STEP7 V5.4 SP4	4
2.2 CP PTP Param V5.1 SP11	4
2.3 CP PTP Modbus Slave V3.1 SP7	4
2.4 STEP7 Micro/WIN V4.0 SP6	4
2.5 Toolbox_V32-STEP 7-Micro WIN 32 Instruction Library	4
3. 硬件列表和接线	5
3.1 硬件列表	5
3.2 硬件接线	5
3.2.1 接口定义	5
3.2.2 接线示意图	6
4. 组态设置和编程	6
4.1 S7-200 做Modbus主站的设置	6
4.1.1 Modbus RTU主站库	7
4.1.2 S7-200 Modbus主站编程	8
4.2 CP341 做Modbus从站的硬件组态	9
4.2.1 硬件组态	9
4.2.2 设置Modbus参数	10
4.2.3 Modbus驱动的下栽	11
4.2.4 CP341 做Modbus从站的编程	12
5. 通讯测试	13
5.1 FC01/05/15 功能码	13
5.2 FC02 功能码	15
5.3 FC03/06/16 功能码	16
5.4 FC04 功能码	18
5.5 Limits 栏	20
6. 总结	20
7. 相关参考资料	20
附录一推荐网址	21

1. 概述

在现场应用中，很多仪表和设备仅支持 Modbus RTU 的通讯协议，第三方仪表可以做 Modbus 主站或从站，西门子的通讯模块 CP341 / CP441-2 通过 Dongle（硬件狗）可以扩展该协议，S7-200 集成的口可以支持自由口通讯，通过指令库也可以方便的实现 Modbus RTU 通讯。本文以 S7-200 作为 Modbus 主站，CP341 作为 Modbus 从站，实现 Modbus RTU 通讯，阐述两者在通讯方面的设置和注意事项。

2. 软件环境

2.1 STEP7 V5.4 SP4

用于编写 S7-300/400 程序，此软件需要从西门子购买，本文档中的 300 的程序是使用 Step7 V5.4 SP4 的软件编写。

2.2 CP PTP Param V5.1 SP11

串行通讯模板的驱动程序，安装此驱动后才能对 PtP 模板进行参数配置，并在 Step7 中集成通讯编程需要使用的功能块。此驱动随购买模板一起提供，也可以从以下的链接下载。

<http://support.automation.siemens.com/CN/view/zh/27013524>

2.3 CP PTP Modbus Slave V3.1 SP7

CP341 或CP441-2 用于Modbus从站时，需要安装此驱动协议，但安装之前必须先安装 PtP Driver，此驱动可以在购买Modbus Dongle时选择购买，也可以从以下的链接下载。

<http://support.automation.siemens.com/CN/view/zh/27774276>

2.4 STEP7 Micro/WIN V4.0 SP6

用于 S7-200 编程的软件，本文档中的 200 的程序是使用 Step7 Micro/win 的软件编写。此软件可以从西门子下载中心免费下载，也可以从以下的链接下载。

<http://www.ad.siemens.com.cn/download> 网站 自动化系统>>S7-200>>软件，文档编号 S0002。

2.5 Toolbox_V32-STEP 7-Micro WIN 32 Instruction Library

S7-200 实现Modbus RTU功能，可以使用Modbus的指令库，要使用西门子的标准指令库，必须先安装指令库的软件包 Instruction Library，安装后，可以在Step 7-Micro/WIN软件的库中找到Modbus相关的指令，该软件包可以从以下的链接下载。

<http://www.ad.siemens.com.cn/download> 网站 自动化系统>>S7-200>>软件，文档编号

S0010。

3. 硬件列表和接线

3.1 硬件列表

S7-300 从站	CPU315-2DP	6ES7 315-2AG10-0AB0
	CP341 RS422/485	6ES7 341-1CH01-0AE0
	Dongle	6ES7 870-1AB01-0YA0
	PC 适配器 (USB)	6ES7 972-0CB20-0XA0
S7-200 主站	CPU 224XP	6ES7 214-2BD23-0XB0

表 1 硬件设备

3.2 硬件接线

3.2.1 接口定义

S7-200 的通讯口为 RS485 物理口 (9 针口)，CP341 是 RS422/485 的接口类型 (15 针口)，两种设备的接口引脚的示意图如下所示，更详细的信息可以参考 CP341 及 S7-200 通信接口的手册。

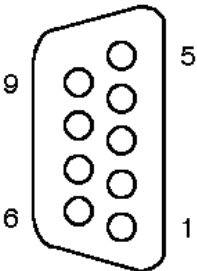
CPU插座(9针母头)	引脚号	Port0/Port1 (端口0/端口1) 引脚定义
	1	机壳接地 (与端子PE相同) /屏蔽
	2	逻辑地 (24V公共端)
	3	RS-485信号 B 或 TxD/RxD +
	4	RTS (TTL)
	5	逻辑地 (5V公共端)
	6	+5V, 通过100 Ohm电阻
	7	+24V
	8	RS-485信号 A 或 TxD/RxD -
	9	10位协议选择 (输入)
金属壳		机壳接地 (与端子PE相同) /与电缆屏蔽层连通

图 1 S7-200 CPU 通信口引脚定义

针	标识	输入/输出	含义
1	-	-	-
2	T (A) -	输出	发送数据 (四线制模式)
3	-	-	-
4	R (A)/T (A) -	输入 输入/输出	接收数据 (四线制模式) 接收/发送数据 (两线制模式)
5	-	-	-
6	-	-	-
7	-	-	-
8	GND	-	功能性接地 (隔离)
9	T (B) +	输出	发送数据 (四线制模式)
10	-	-	-
11	R (B)/T (B) +	输入 输入/输出	接收数据 (四线制模式) 接收/发送数据 (两线制模式)
12	-	-	-
13	-	-	-
14	-	-	-
15	-	-	-

图 2 S7-300 CP341 RS422/485 通讯口引脚定义

3.2.2 接线示意图

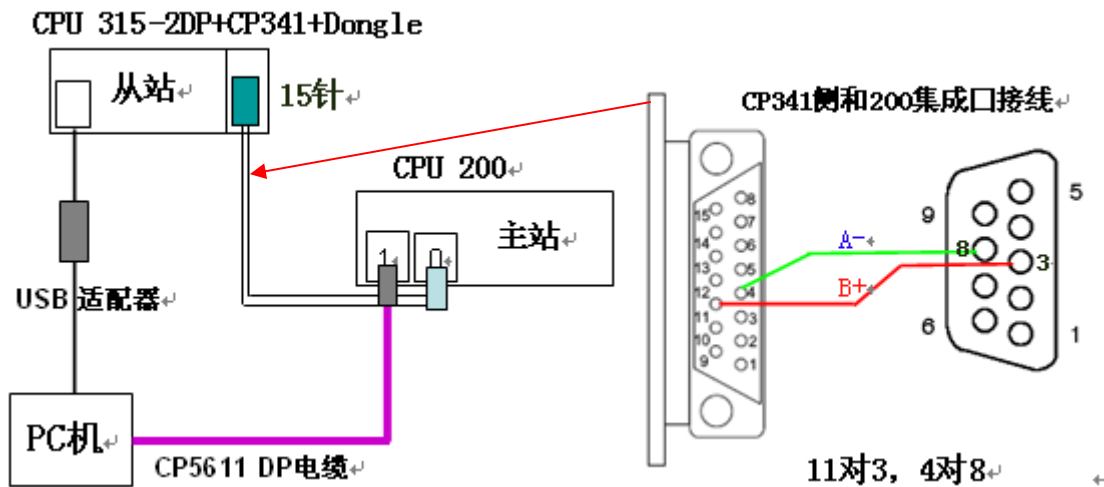


图 3 硬件结构和接线示意图

4. 组态设置和编程

4.1 S7-200 做 Modbus 主站的设置

S7-200 CPU上的通信口在电气上是标准的RS-485半双工串行通信口，此串行字符通信的格式：1个起始位；7/8位数据位；1位奇/偶/无校验；1停止位。通信波特率可以设置为1200、2400、4800、9600、19200、38400、57600或112500，符合这些格式的串行通讯设备可以和S7-200进行自由口通讯，Modbus RTU指令库就是使用自由口编程实现的。

4.1.1 Modbus RTU 主站库

使用 Modbus 主站指令库时需要注意的几点：

- 需要 S7-200 的编程软件是 Micro/WIN V4.0 SP5 及以上版本；
- Modbus RTU 主站库对 CPU 的版本有要求，CPU 的版本必须为 2.00 或者 2.01（即订货号为 6ES721*—***23-0BA*）；
- Modbus 主站可读/写的最大数据量为 120 个字（指每一个 MBUS_MSG 指令）；
- Modbus 主站库支持 Port0 和 Port1（从站库只支持 Port0 口），本例中用 Port0；
- 使用 Modbus 库时必须对库存储区进行分配，见下图设置，而且分配的空间不能和程序中其它空间冲突，否则编译调用会报错。

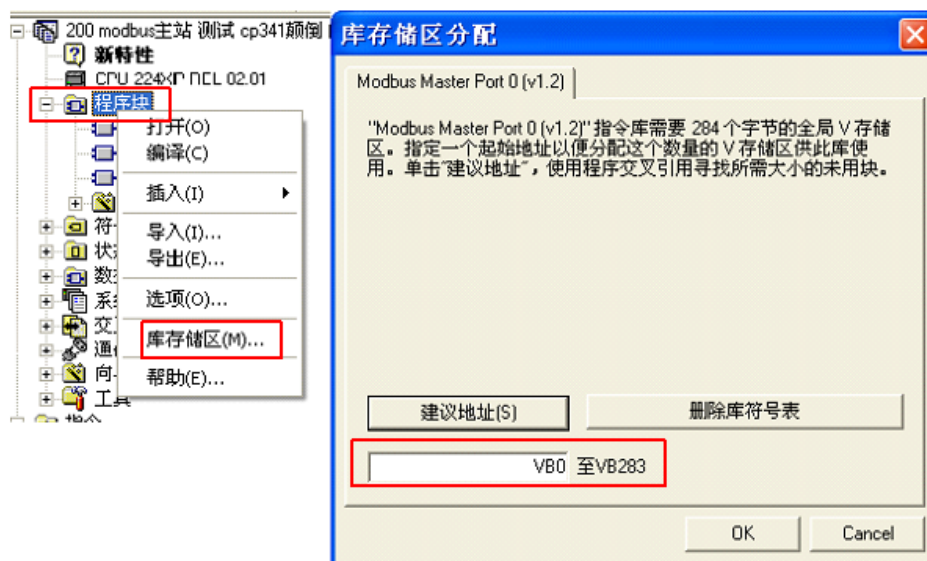


图 4 库存储区设置

- Modbus 主站库支持的功能码和地址对应关系：

Modbus 地址	读 / 写	Modbus 从站须支持的功能
00001~09999 数字量输出	读	功能 1: 读输出点
	写	功能 5: 写单个输出点 功能 15: 写多个输出点
10001~19999 数字量输入	读	功能 2: 读输入点
30001~39999 输入寄存器	读	功能 4: 读输入寄存器
40001~49999 保持寄存器	读	功能 3: 读保持寄存器
	写	功能 6: 写单个寄存器 功能 16: 写多个寄存器

表 2 需要从站支持的功能

4.1.2 S7-200 Modbus 主站编程

编程时，使用 SM0.0 调用 MBUS_CTRL 完成主站的参数初始化，详细见下表，参数的说明也可以从子程序的局部变量表中找到。

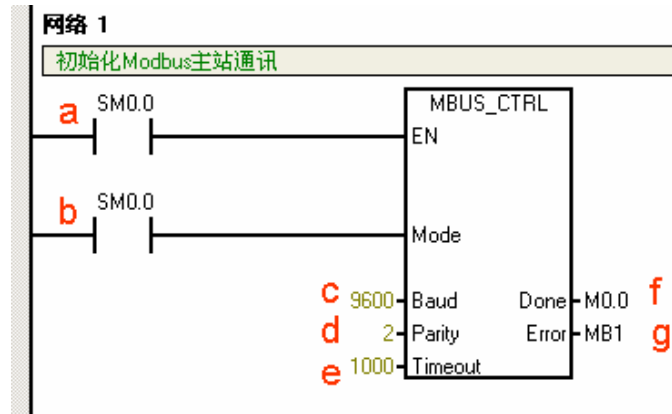


图 5 Modbus RTU 主站初始化

图中各参数含义如下

编号	符号/含义	说 明
a	EN / 使能	必须保证每一扫描周期都被使能（使用 SM0.0）。
b	Mode / 模式	为 1 时使能为 Modbus 协议；为 0 时恢复为 PPI 协议。
c	Baud / 波特率	支持的通讯波特率为 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200。
d	Parity / 校验	校验方式选择：0=无校验；1=奇校验，2=偶校验。
e	Timeout / 超时	主站等待从站响应的的时间，以毫秒为单位，典型的设置值为 1000 毫秒，允许设置的范围为 1-32767。这个值必须设置足够大以保证从站有时间响应。
f	Done / 完成位	初始化完成，此位会自动置 1。
g	Error / 错误位	初始化错误代码。

表 3

调用 Modbus RTU 主站读写子程序 MBUS_MSG，发送一个 Modbus 请求。

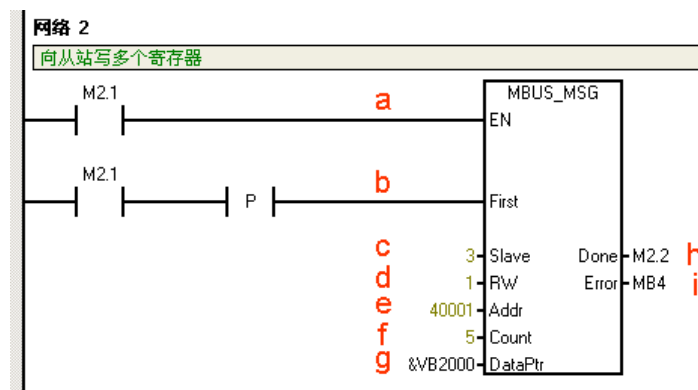


图 6 调用 Modbus RTU 主站读写子程序

图中各参数含义如下

编号	符号/含义	说 明
a	EN / 使能	同一时刻只能有一个读写功能使能。
b	First / 读写请求位	每一个新的读写请求必须使用脉冲触发。
c	Slave / 从站地址	可选择的范围 1-247。
d	RW / 读写操作位	0=读, 1=写。
e	Addr / 读写从站的数据地址	选择读写的数据类型: 00001 至 0xxxx - 开关量输出 10001 至 1xxxx - 开关量输入 30001 至 3xxxx - 模拟量输入 40001 至 4xxxx - 保持寄存器。
f	Count / 数据的个数	通讯的数据个数 (位或字的个数)。
g	DaptPtr / 数据指针	如果是读指令, 读回的数据放到这个数据区中; 如果是写指令, 要写出的数据放到这个数据区中。
h	Done / 完成位	读写功能完成位。
i	Error / 错误代码	只有在 Done 位为 1 时, 错误代码才有效。

表 4

从上图中可见, S7-200 作为 Modbus RTU 主站, 波特率 9.6Kb/s, 偶校验, 连接从站的站地址是 3, 数据存储区为 VB2000 开始的区域。

4.2 CP341 做 Modbus 从站的硬件组态

4.2.1 硬件组态

The screenshot displays the HW Config interface for a Siemens S7-300 PLC. The hardware rack configuration is as follows:

Slot	Module	Order number	FI...	M...	I...	Q...	Con...
1							
2	CPU 315-2 DP	6ES7 315-2AG10-0ABV2.6 2			2047		
X2	DP						
3							
4	CP 341-RS422/485	6ES7 341-1CH01-0AE0			256... 256...		

A red box highlights the CP 341 module in slot 4, and a red arrow points to its logical address '256...' in the 'I...' column.

图 7 S7-300 侧硬件组态

4.2.2 设置 Modbus 参数

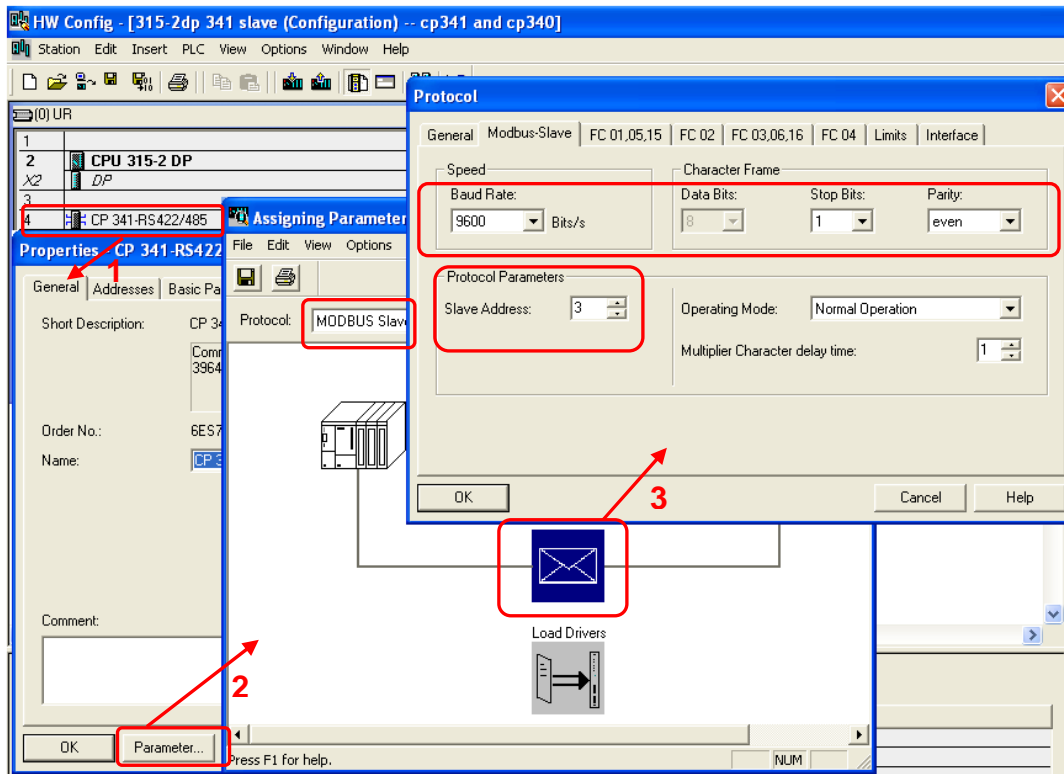


图 8 消息帧字符结构

按照上述操作设置参数，从上图可以看出，本例中的传输波特率 9.6Kb/s，1 位起始位，8 位数据位，偶校验位，1 位停止位，从站地址是 3，主从通讯设备的字符帧格式和波特率等参数设置需要一致。

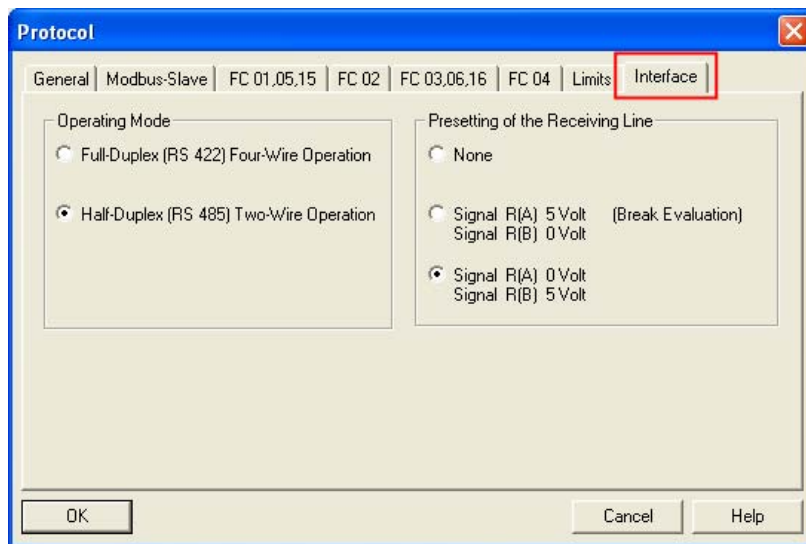


图 9 RS422/485 接口组态

RS422/485 接口只能一个有效，接口的选择只需要组态而不需要在硬件上短接。

4.2.3 Modbus 驱动在下载

当配置好 Modbus 通信的参数后，保存前需要向 CP341 下载 Modbus Slave 的驱动，一旦下载完成后无需再次下载。

需要注意的是，在下载驱动时（可以在无 Dongle 情况下下载），需要将 CPU 停机，然后下载，操作过程如下所示。

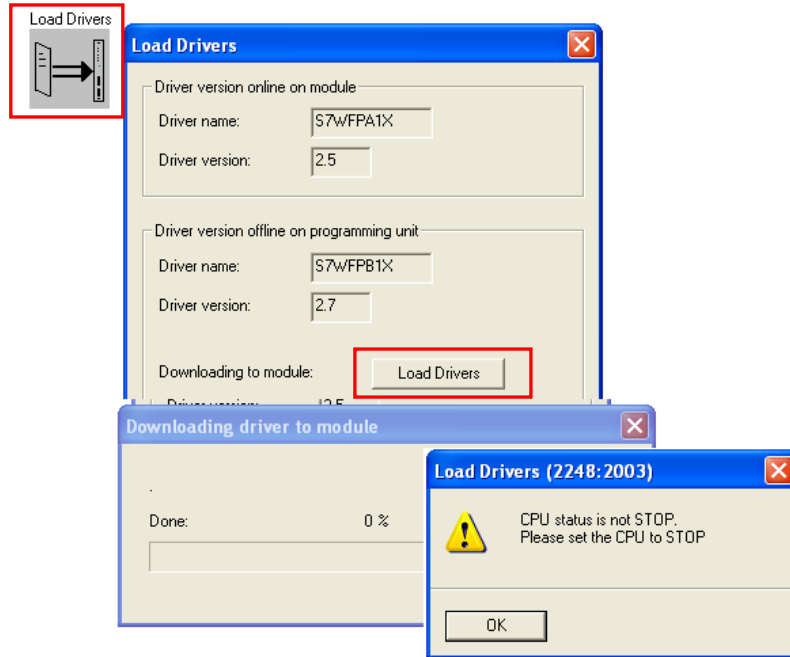


图 10 下载 Dongle 时，需要 CPU 停机



图 11 从站驱动下载后结果

4.2.4 CP341 做 Modbus 从站的编程

从 Step7 软件下的 EXAMPLE 目录中，找到项目名“zXX21_05_PtP_Com_MODSL”的项目，打开，然后将 Modbus 通讯模块 FB80 传递到用户项目中，打开路径如下所示。

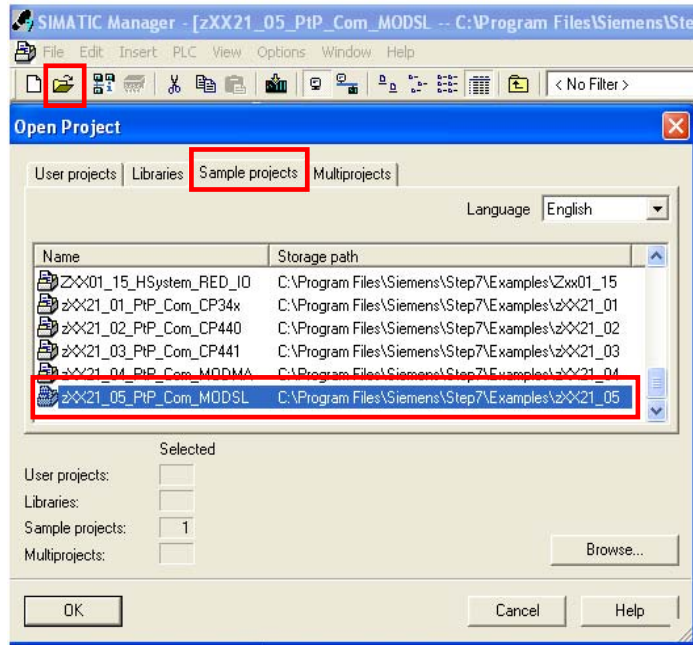


图 12 Modbus Slave 例程打开路径

OB1 中调用 FB80 编程如下：

Network 1: Example of a call-up of the communication

Comment:

```

CALL "MODB_341", "IDB_MODB_341"    FB80 / DB80
LADDR      :=256
START_TIMER :=T120
START_TIME :=S5T#5S
OB_MASK    :=TRUE
CP_START   :=MO.0
CP_START_FM :=MO.1
CP_NDR     :=MO.2
CP_START_OK :=MO.3
CP_START_ERROR:=MO.4
ERROR_NR   :=MW2
ERROR_INFO :=MW4
    
```

	IN	OUT
CP_START	1	1
CP_START_FM	1	1
CP_NDR	0	0
CP_START_OK	1	1
CP_START_ERROR	0	0
ERROR_NR	16#0	16#0
ERROR_INFO	16#0	16#0

图 13 FB80 程序块调用

CP 卡初始化正常后，CP_START，CP_START_FM 和 CP_START_OK 为 1 信号，否则 CP_START_ERROR 为 1，同时可以从 ERROR_NR 察看错误信息，也可以在硬件组态中在线后的 CP341 的诊断缓冲区察看详细的错误信息，错误信息对照和处理方式可以参考 [《S7-300 以用于PtP CP Modbus 协议RTU格式S7 的可装载驱动程序为从站》](#) 的手册。

FB80 的各参数含义如下

LADDR	硬件组态中 CP341 的起始逻辑地址，本例中为 256
START_TIMER	初始化超时定时器，本例中为 T120
START_TIME	初始化定时器时间，本例中为 5S
OB_MASK	I/O 访问错误屏蔽位，本例中为 True (I/O 访问错误已屏蔽)
CP_START	FB 初始化使能位，本例中为 M0.0
CP_START_FM	CP_START 初始化的上升沿位，本例中为 M0.1
CP_NDR	从 CP 卡写操作位，本例中为 m0.2
CP_START_OK	初始化完成且无错误，本例中为 M0.3
CP_START_ERROR	初始化完成，但有错误，本例中为 M0.4
ERROR_NR	错误号，本例中为 MW2
ERROR_INFO	错误信息，本例中为 MW4

表 5

5. 通讯测试

Modbus RTU 格式通信协议是以主从的方式进行数据传输的，在传输的过程中主站是主动方，即主站发送数据请求报文到从站，从站返回响应报文。Modbus 系统间的数据交换是通过功能码来控制的，以下对现场常用的功能码进行分类测试，关于功能码的详细信息请参考手册。

5.1 FC01/05/15 功能码

CP341 从站的通讯区域配置

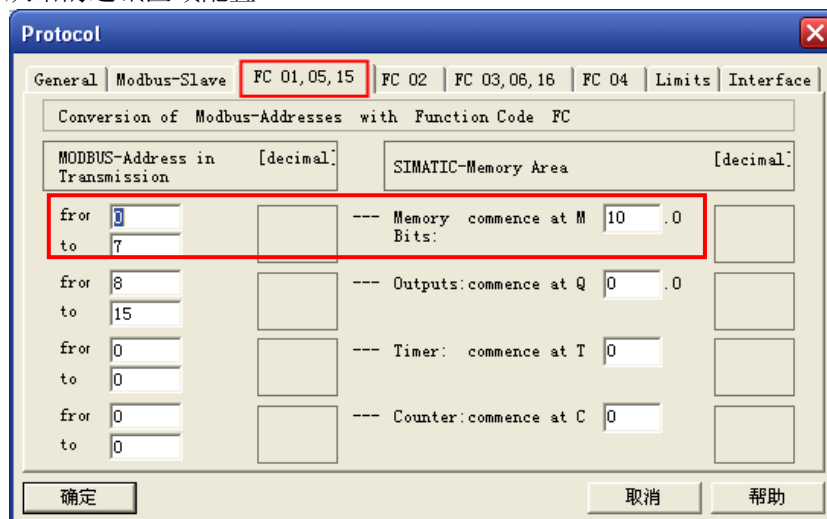


图 14 FC01/05/15 参数组态界面

FC01、FC05、FC15 对应的数据区为位输出，数据的传递以位为单位，可以读写操作，用户地址区为 0xxxx，Modbus 地址在信息传递中从 0 开始。如上图，左边为信息传递地址（地址区不能冲突），右边对应的是 S7-300 的数据区。例如左边信息传递地址从 0 ~ 7 对应用户地址区为 00001 ~ 00008，对应 S7-300 的 M10.0 ~ M10.7，并且以此为例说明 FC01 功能码的通讯。

S7-200 主站程序调用

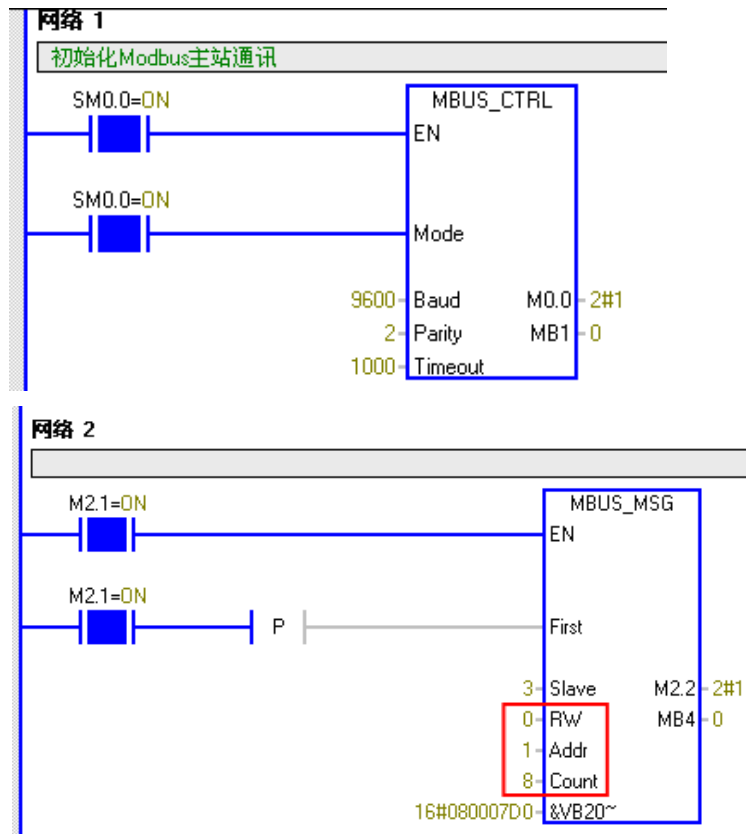


图 15 功能码 FC01 使用

S7-200 主站，用功能码 FC01 读取从站 8 点数字量输出，接收的数据存放在 VB2000 开始的区域，测试截图结果如下。

S7-300侧

10	//FC01读数字量输出状态 8个 00001~00008 对应 m10.0~m10.7		
11	MB 10	BIN	2#1110_0011

S7-200侧

状态表																
	· 3 ·	· 4 ·	· 5 ·	· 6 ·	· 7 ·	· 8 ·	· 9 ·	· 10 ·	· 11 ·	· 12 ·	· 13 ·	· 14 ·	· 15 ·	· 16 ·	· 17 ·	· 18 ·
	地址	格式	当前值	新值												
1	VB2000	二进制	2#1110_0011													

图 16 FC01 功能码数据交换

5.2 FC02 功能码

CP341 从站的通讯区域配置

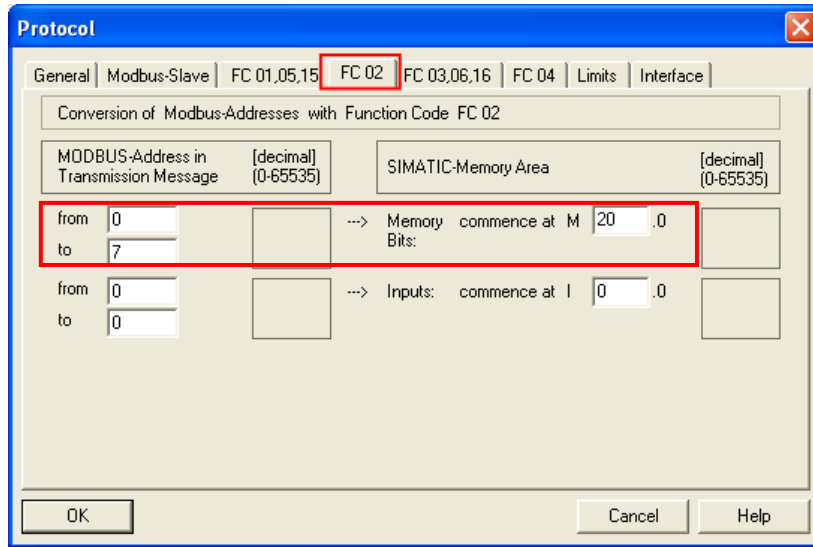


图 17 FC02 参数组态界面

FC02 对应的数据区为位输出，数据的传递以位为单位，只读操作，用户地址区为 1xxxx，Modbus 地址在信息传递中从 0 开始，如上图，左边为信息传递地址（地址区不能冲突），右边对应的是 S7-300 的数据区。例如左边信息传递地址从 0 ~ 7 对应用户地址区为 10001 ~ 10008，对应 S7-300 的 M20.0 ~ M20.7，并且以此为例说明 FC02 功能码的通讯。

S7-200 主站程序调用

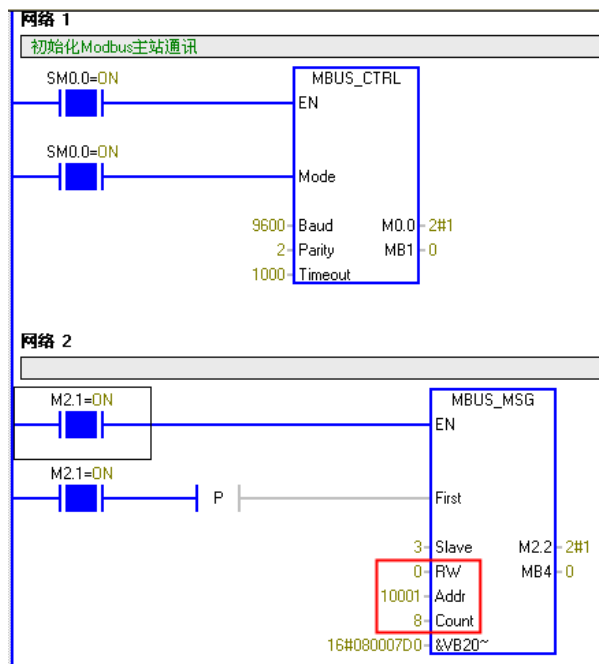


图 18 功能码 FC02 使用

S7-200 主站，用功能码 FC02 读取从站 8 点数字量输入，接收的数据存放在 VB2000 开始的区域，测试截图结果如下。

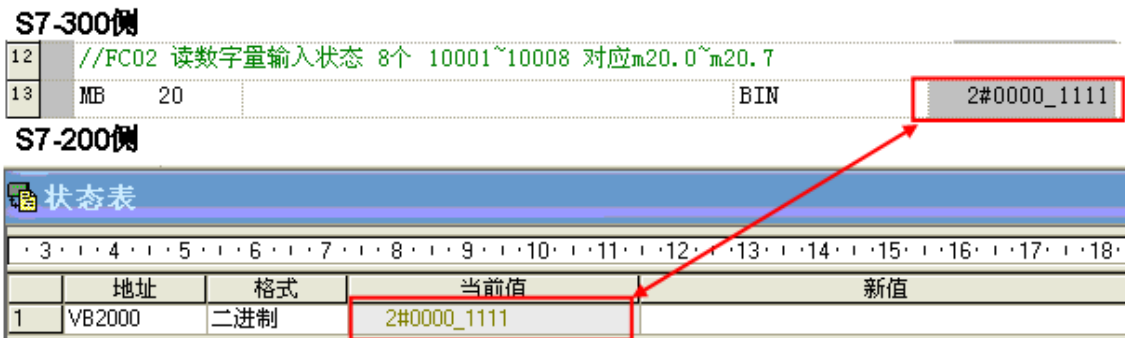


图 19 FC02 功能码数据交换

5.3 FC03/06/16 功能码

CP341 从站的通讯区域配置

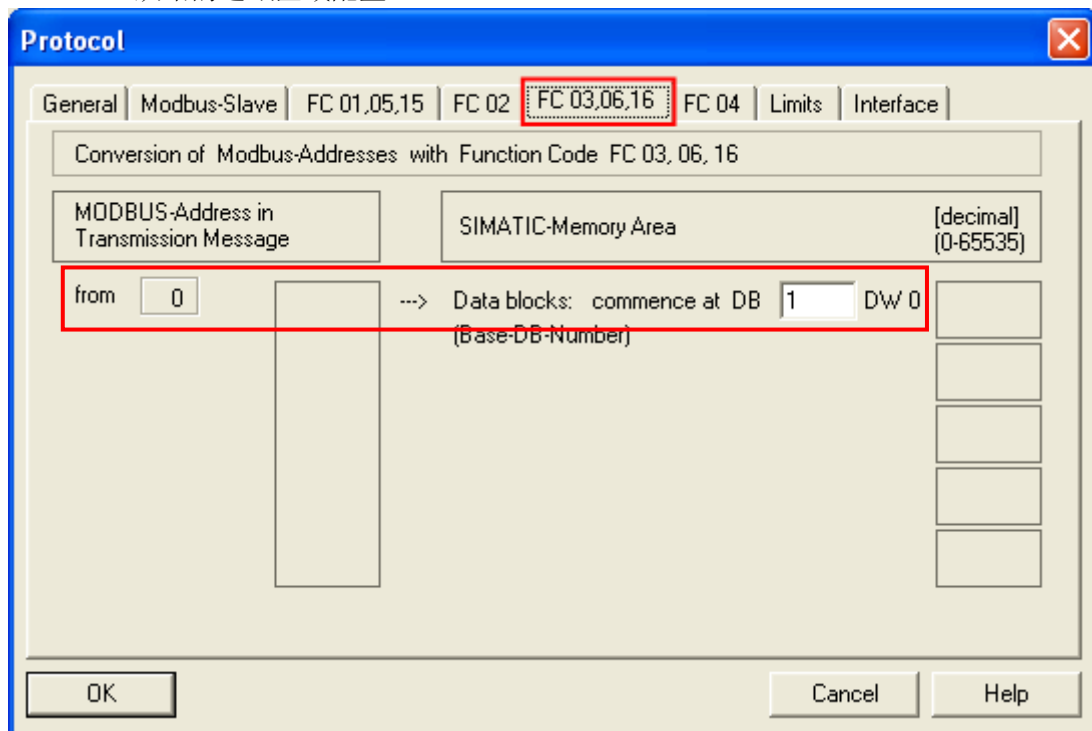


图 20 FC03/06/16 参数组态界面

FC03/06/16 对应的数据区为寄存器，数据的传递以字为单位，可以读写操作，用户地址区为 4xxxx，Modbus 地址在信息传递中从 0 开始。如上图，左边为信息传递地址，右边对应的是 S7-300 的数据区，左边传输地址不可改，右边只对应一个数据区。例如用户地址区为 40001 ~ 40004，对应 S7-300 数据区为 DB1.DBW0 ~ DB1.DBW6，并且以此为例说明 FC03 功能码的通讯。

S7-200 主站程序调用

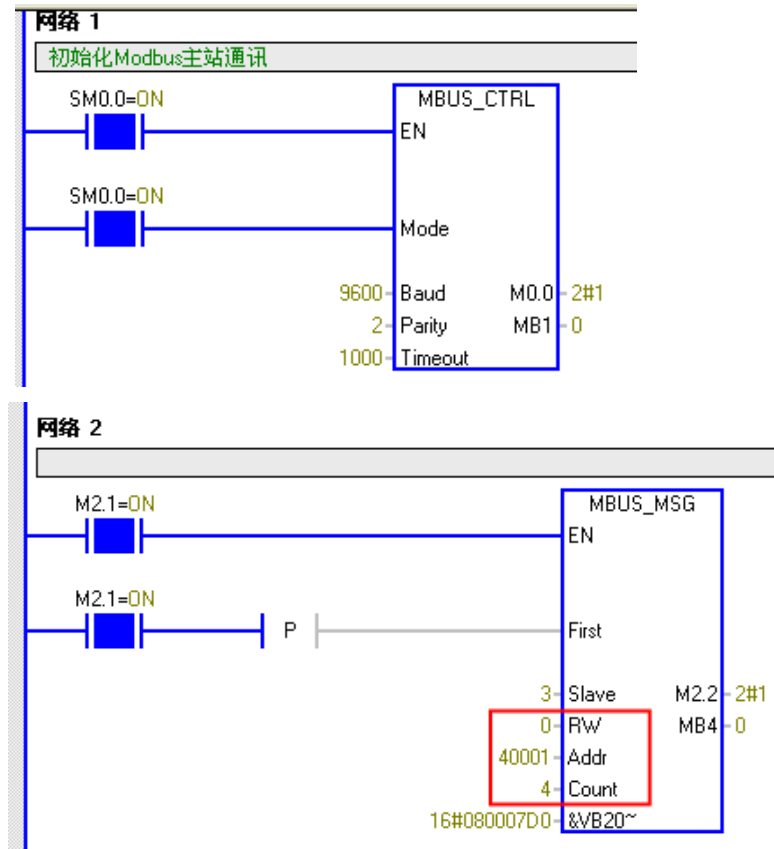


图 21 功能码 FC03 使用

S7-200 主站，用功能码 FC03 读取从站 4 个字寄存器，接收的数据存放在 VB2000 开始的区域，测试截图结果如下。

S7-300例

状态表

地址	格式	当前值	新值
1 VB2000	二进制	2#0001_0001	
2 Vw2000	十六进制	16#1122	
3 Vw2002	十六进制	16#3344	
4 Vw2004	十六进制	16#5566	
5 Vw2006	十六进制	16#7788	

S7-200例

14	//FC03读保持寄存器的状态 4个 40001~40004对应db1的dbw0~dbw3			
15	DB1.DBW	0	“主站读写保持寄存器”.read_holddata[1]	HEX W#16#1122
16	DB1.DBW	2	“主站读写保持寄存器”.read_holddata[2]	HEX W#16#3344
17	DB1.DBW	4	“主站读写保持寄存器”.read_holddata[3]	HEX W#16#5566
18	DB1.DBW	6	“主站读写保持寄存器”.read_holddata[4]	HEX W#16#7788

图 22 FC03 功能码数据交换

5.4 FC04 功能码

CP341 从站的通讯区域配置

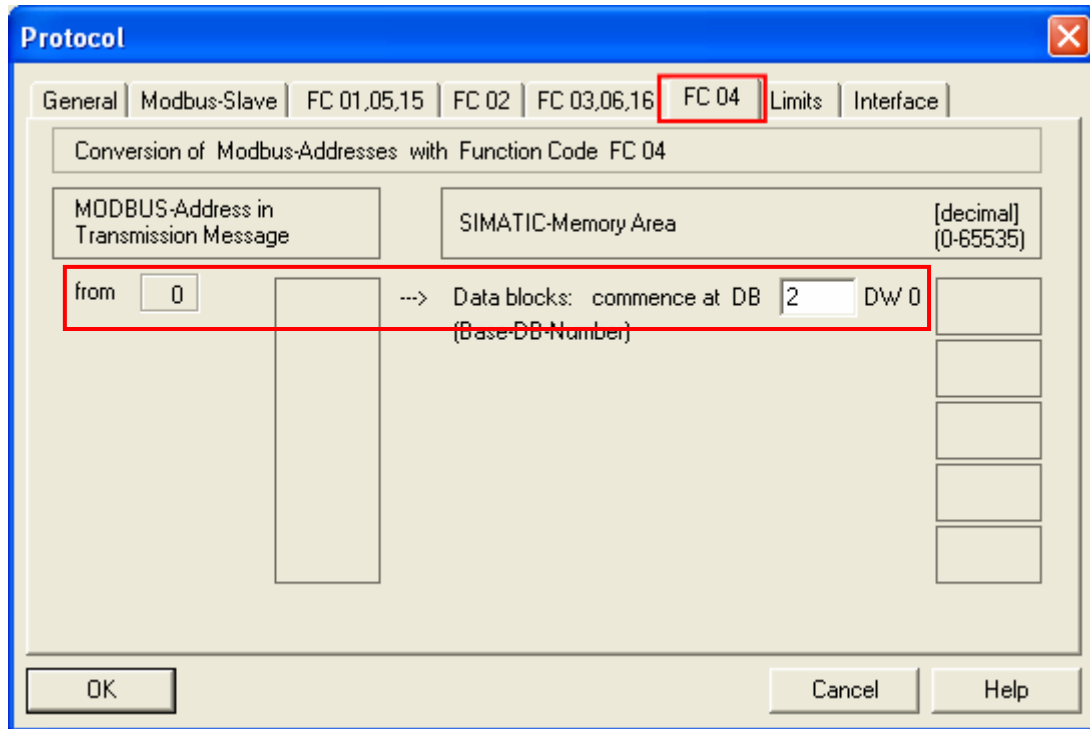
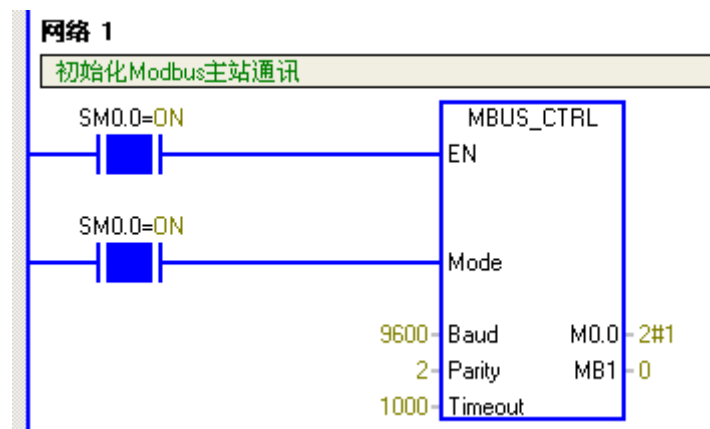


图 23 FC04 参数组态界面

FC04 对应的数据区为寄存器输入，数据的传递也以字为单位，只读操作，用户地址区 3xxxx，Modbus 地址在信息传送中从 0 开始。如上图，左边为信息传递地址，右边对应的是 S7-300 的数据区，左边传输地址不可改，右边只对应一个数据区。例如用户地址区为 30001 ~ 30004，对应 S7-300 数据区为 DB1.DBW0 ~ DB1.DBW6，并且以此为例说明 FC04 功能码的通讯。

S7-200 主站程序调用



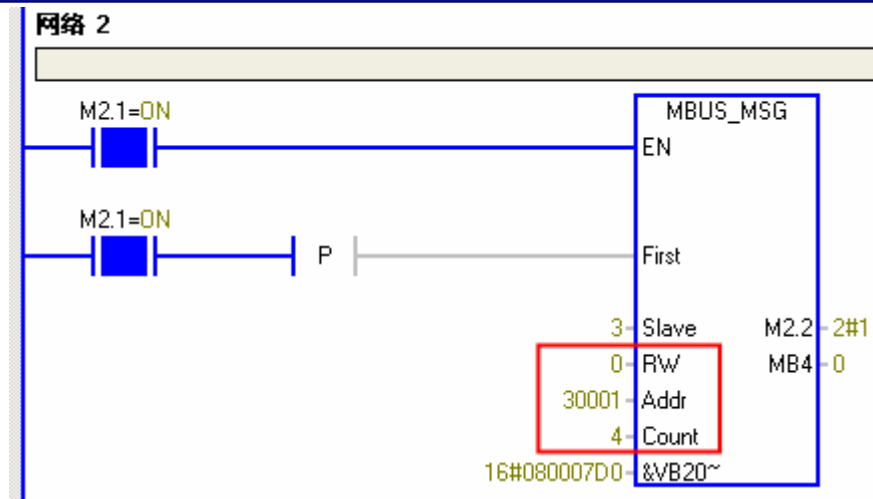


图 24 功能码 FC04 使用

S7-200 主站，用功能码 FC04 读取从站 4 个字输入寄存器，接收的数据存放在 VB2000 开始的区域，测试截图结果如下。

S7-300侧

//FC04读输入寄存器的状态 4个 30001~30004对应db2的dbw0~dbw6

DB2.DBW	0	"主站读输入寄存器".read_aiw[1]	HEX	W#16#0100
DB2.DBW	2	"主站读输入寄存器".read_aiw[2]	HEX	W#16#0200
DB2.DBW	4	"主站读输入寄存器".read_aiw[3]	HEX	W#16#0300
DB2.DBW	6	"主站读输入寄存器".read_aiw[4]	HEX	W#16#0400

S7-200侧

状态表

地址	格式	当前值	新值
1 VB2000	二进制	2#0000_0001	
2 Vw2000	十六进制	16#0100	
3 Vw2002	十六进制	16#0200	
4 Vw2004	十六进制	16#0300	
5 Vw2006	十六进制	16#0400	

图 25 FC04 功能码数据交换

5.5 Limits 栏

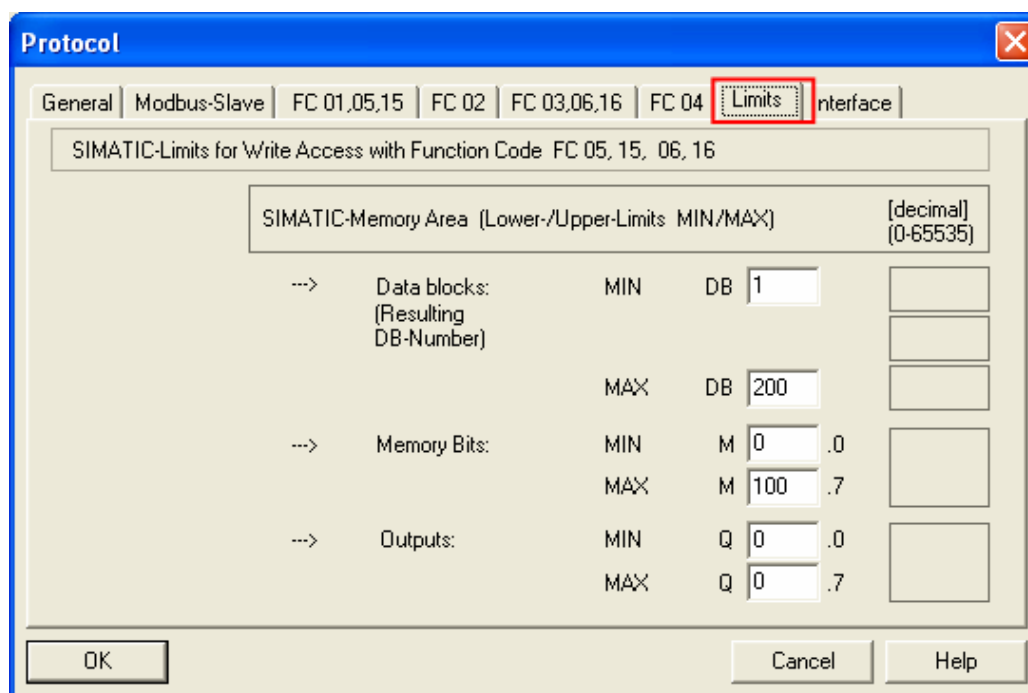


图 26 Limits 参数组态界面

对于写功能码 FC05、06、15、16，可以禁用或限制访问相关 S7-300 存储区，即使用这些功能码时，S7-300 存储区需要在设定的最小和最大的范围之间，如果访问的区域超出这个范围，则访问会被拒绝，同时输出报错误信息。

6. 总结

本文档以 S7-200 为主站和 CP341 为从站简单介绍了 Modbus RTU 通讯，关于通讯的组态设置，编程以及常用功能码的使用，其具体的使用可以作为西门子串行通讯模块与第三方的仪表、设备等进行串行通信的参考。

7. 相关参考资料

关于西门子串行通信应用的文档可以参考相关产品手册，或登录下载中心网站 <http://www.ad.siemens.com.cn/download/>，搜索下载如下文档：

A0006: 串口通讯模块的信息与使用

A0081: CP340/341/440/441 通讯及编程

A0336: CP341 Modbus RTU 多站点轮询

A0440: CP340/341 基于 ASCII 驱动协议的多站点轮询

A0384: S7-300 CP341 作主 S7-200 作从的 Modbus 通信

如果您对该文档有任何建议，请将您的宝贵建议提交至[下载中心留言板](#)。

该文档的文档编号：**A0451**

附录一 推荐网址

自动化系统

西门子（中国）有限公司

工业自动化与驱动技术集团 客户服务与支持中心

网站首页：www.4008104288.com.cn

自动化系统 下载中心：

<http://www.ad.siemens.com.cn/download/DocList.aspx?Typeld=0&CatFirst=1>

自动化系统 全球技术资源：

<http://support.automation.siemens.com/CN/view/zh/10805045/130000>

“找答案”自动化系统版区：

<http://www.ad.siemens.com.cn/service/answer/category.asp?cid=1027>

通信/网络

西门子（中国）有限公司

工业自动化与驱动技术集团 客户服务与支持中心

网站首页：www.4008104288.com.cn

通信/网络 下载中心：

<http://www.ad.siemens.com.cn/download/DocList.aspx?Typeld=0&CatFirst=12>

通信/网络 全球技术资源：

<http://support.automation.siemens.com/CN/view/zh/10805868/130000>

“找答案”Net版区：<http://www.ad.siemens.com.cn/service/answer/category.asp?cid=1031>

注意事项

应用示例与所示电路、设备及任何可能结果没有必然联系，并不完全相关。应用示例不表示客户的具体解决方案。它们仅对典型应用提供支持。用户负责确保所述产品的正确使用。这些应用示例不能免除用户在确保安全、专业使用、安装、操作和维护设备方面的责任。当使用这些应用示例时，应意识到西门子不对在所述责任条款范围之外的任何损坏/索赔承担责任。我们保留随时修改这些应用示例的权利，恕不另行通知。如果这些应用示例与其它西门子出版物(例如，目录)给出的建议不同，则以其它文档的内容为准。

声明

我们已核对过本手册的内容与所描述的硬件和软件相符。由于差错难以完全避免，我们不能保证完全一致。我们会经常对手册中的数据进行检查，并在后续的版本中进行必要的更正。欢迎您提出宝贵意见。

版权© 西门子（中国）有限公司 2001-2010 版权保留

复制、传播或者使用该文件或文件内容必须经过权利人书面明确同意。侵权者将承担权利人的全部损失。权利人保留一切权利，包括复制、发行，以及改编、汇编的权利。

西门子（中国）有限公司