

廊坊西门子PLC模块授权总代理商库存现货（已更新）

产品名称	廊坊西门子PLC模块授权总代理商库存现货（已更新）
公司名称	上海臣冠工业控制设备有限公司
价格	8.00/台
规格参数	品牌:SIEMENS 数量:4000 运输方式:快递物流
公司地址	上海市松江区乐都路358号503室（注册地址）
联系电话	13524157645

产品详情

廊坊西门子PLC模块授权总代理商库存现货（已更新）

廊坊西门子PLC模块授权总代理商库存现货（已更新）

S7-200做主站S7-300 CP341做从站的Modbus RTU通讯

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：[27013524](#)

2.3 CP PTP Modbus Sle 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：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中心免费下，也可以从以下的链接下。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。自动化系统>>S7-200>>软件，文档编号S0010。

图11 从站驱动后结果

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 Sle 例程打开路径

OB1中调用FB80编程如下：

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。

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。

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。

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3xxx x，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。

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和的范围之间，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。