西门子河北省（中国）授权 一级代理

产品名称	西门子河北省（中国）授权 一级代理
公司名称	广东湘恒智能科技有限公司
价格	.00/件
规格参数	西门子变频器:西门子触摸屏 西门子伺服电机:西门子PLC 西门子直流调速器:西门子电缆
公司地址	惠州大亚湾澳头石化大道中480号太东天地花园2栋二单元9层01号房
联系电话	18475208684 18475208684

产品详情

第一部分：S7-1200 Modbus RTU通讯（一）概述Modbus具有两种串行传输模式：分别为ASCII和RTU。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，每个从站必须有唯一的地址，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 RTU通信以主从的方式进行数据传输，在传输的过程中Modbus RTU主站是主动方，即主站发送数据请求报文到从站，Modbus RTU从站返回响应报文。S7-1200以下模块支持 Modbus RTU通信：通信模块/通信板订货号CM1241 RS2326ES7241-1AH32-0XB0CM1241 RS422/4856ES7241-1CH32-0XB0CB 1241 RS4856ES7241-1CH30-1XB0注意：（1）使用通信模块CM 1241 RS232作为Modbus RTU主站时，只能与一个从站通讯。（2）使用通信模块CM 1241 RS485作为Modbus RTU主站时，则允许建立最多与 32 个从站的通讯。（3）使用通信板CB 1241 RS485时，CPU 固件必须为 V2.0 或更高版本，且使用软件必须为STEP 7 Basic V11 或STEP 7 Professional V11 以上更高版本。（二）Modbus RTU指令版本与限制随着博途软件和 S7-1200 CPU 固件的不断更新，S7-1200 Modbus RTU 指令也出现了不同的版本。用户需要根据使用的软件和硬件，正确选择使用符合要求的 S7-1200 Modbus RTU 指令来实现 Modbus RTU 通信，其软件和硬件要求和指令版本说明如下。（1）博途中的 S7-1200 Modbus RTU 指令博途中提供了2个版本的 Modbus RTU指令。如下图 1 所示：早期版本的 Modbus RTU 指令（图1. 中 MODBUS (V2.2)）仅可通过 CM1241 通信模块或 CB1241 通信板进行 Modbus RTU 通信。新版本的 Modbus RTU 指令（图1. 中 MODBUS(RTU) V3.0）扩展了 Modbus RTU 的功能，该指令除了支持 CM1241 通信模块、CB1241 通信板，还支持 PROFINET 或 PROFIBUS 分布式 I/O 机架上的 PTP 通信模块实现 Modbus RTU 通信。（2）新版本 Modbus RTU 指令的使用限制条件新版本 Modbus RTU 指令通过CM1241通信模块或CB1241通信板进行Modbus RTU通信时，需要满足如下条件：a. S7-1200 CPU 的固件版本不能低于V4.1b. CM1241通信模块 V2.1 以上或 CB1241图1. 两个版本 Modbus RTU 指令（三）常见问题（1）S7-1200 是否支持 Modbus ASCII 通信模式？西门子不提供支持上述通信模式的的现成指令，需要用户自己用自由口模式编程。（2）Modbus RTU指令V1和V2两个版本有什么区别？Modbus RTU指令版本 V2 将参数“ REQ ”和“ DONE ”

添加到“ MB_COMM_LOAD ”指令。而且，“ MB_MASTER ”和“ MB_SLAVE ”指令的“ MB_ADDR ”参数现在允许一个 UInt
值以进行扩展寻址。（3）同一CPU程序中是否可以同时使用V1和V2两个不同版本的Modbus
RTU指令？不能在同一CPU 程序中同时使用V1（V1.x）和V2（V2.y）指令版本。用户程序的 Modbus
指令必须具有相同的主版本号；主版本组内的各个指令可具有不同的次版本号。（4）S7-1200
通信模块CM1241是否可作为Modbus RTU主站或作为Modbus RTU从站？对S7-1200
通信模块CM1241组态并编程调用“ MB_COMM_LOAD ”指令，可将其设置为Modbus
RTU通信模式。通过编程调用“ MB_MASTER ”指令，S7-1200 通信模块CM1241可作为Modbus
RTU主站，或调用“ MB_SLAVE ”指令，S7-1200 通信模块CM1241可作为Modbus
RTU从站。注意：无论S7-1200 通信模块CM1241作为Modbus
RTU主站还是从站，都需要调用“ MB_COMM_LOAD ”指令进行编程。（5）S7-1200 CM1241/CB1241
Modbus RTU 通信是否支持两位停止位？支持。注意：S7-1200 CM1241/CB1241属性里可以设置停止位，
但是该模块用于 Modbus 通信时，此设置的停止位无效， 需要在 Modbus_Commload 指令的背景 DB 里
Static 修改 STOP_BITS停止位数值为 2。如下图 2-3所示：图2. CM1241 配置停止位参数Modbus_Commload
指令的背景 DB 里 Static 修改 STOP_BITS停止位数值为 2（默认值=1）图3. 修改 Modbus RTU
通信停止位第二部分：V3版指令功能（一）Modbus RTU指令概述博途V13
SP1版本软件中提供了2个版本的Modbus RTU指令：图1. 两个版本Modbus
RTU指令（1）早期版本的Modbus RTU指令（图1. 中 MODBUS
(V2.2)）仅可通过CM1241通信模块或CB1241通信板进行Modbus RTU通信。（2）新版本的 Modbus
RTU指令（图1. 中 MODBUS(RTU) V3.0）扩展了Modbus
RTU的功能，该指令除了支持CM1241通信模块、CB1241通信板，还支持 PROFINET 或 PROFIBUS
分布式 I/O 机架上的PTP通信模块实现Modbus RTU通信。（3）新版本 Modbus
RTU指令所支持的PTP模块如下图2所示：图2. 新版本 Modbus RTU指令所支持的PTP模块（二）Modbus
RTU指令实例环境介绍新版本Modbus RTU指令中包含Modbus RTU 主站指令和从站指令。本文以
CPU1217C+CM1241 RS422/485+ET200SP CM PTP 模块为例，介绍新版本 Modbus RTU
指令主从通信的编程步骤。其中CPU 机架CM1241 RS422/485作为Modbus RTU从站，分布式机架ET200SP
中 CMPTP 模块作为Modbus RTU主站。1、网络结构图如下：图3. Modubus RTU
网络通信结构图2、本项目中使用到的硬件和软件如下:（1）硬件：① CPU1217C (订货号：6ES7
217-1AG40-0XB0)，固件版本V4.1.3② CM1241 RS422/485模块 (订货号：6ES7
241-1CH32-0XB0)，固件版本V2.1③ 24V 电源PS307（订货号：6ES7307-1KA02-0AA0）④ ET200 SP
IM155-6PN HF（订货号：6ES7155-6AU00-0CN0）⑤ CM
PTP模块（订货号：6ES7137-6AA00-0BA0）（2）软件：① 博途SP1 UP
9（三）实例之设备组态1、组态CM1241 RS422/485模块（1）打开设备视图，添加S7-1200CPU，并在硬件
目录里找到“ 通信模块 ”→“ 点到点 ”→“ CM1241(RS422/485) ”，拖拽此模块至CPU左侧即可，如下图
4所示：图4. 添加 CM 1241 RS422/485模块注意：固件版本>=V2.1 的CM 1241
RS422/485模块，才支持新版本Modbus RTU指令。（2）接下来，在“ 设备视图 ”中用鼠标选中CM1241(
RS422/485)模块，在“ 属性 ”→“ 端口组态 ”中配置此模块硬件接口参数，本例以传输率=9.6Kbps，奇偶
校验=无奇偶校验，数据位=8位字符，停止位=1为例。如CM 1241 端口组态设置如下图5所示：图5.
CM1241 RS422/485 模块端口组态（3）最后在“ 硬件标识符 ”里确认一下硬件标识符为269（该参数在程
序编程中会被使用），如下图6所示：图6 硬件标识符（4）另外，S7-1200
还提供了系统和时钟存储器功能，为了便于后续指令，建议使能该功能。在CPU
“ 属性 ”→“ 常规 ”→“ 系统和时钟存储器 ”使能系统和时钟存储器功能，如图7所示。图7.
系统和时钟存储器功能2、组态ET200 SP CM PtP
模块（1）插入一个ET200SP分布式站点，打开网络视图并拖入一个ET200SP站点，并将其分配给相应的I
O 控制器（本例CPU1217C 为 IO 控制器），如图8所示：图8. 插入ET200SP站点（2）组态ET200SP
站点，在ET200SP的"设备视图"环境下，为ET200SP
站点添加信号、通信模块和服务器模块，在本例中只添加了CM
PTP模块和服务器模块。在ET200SP"设备视图"中用鼠标选中CM PTP，在“ 属性 ”→“ 常规 ”→“ 接口 ”
→“ 操作模式 ”中配置此模块硬件接口参数，本例设定“ 指定工作模式"："半双工（RS485）2线制操作"
；"接收线路的初始状态"："无"。如下图9所示：图9. CM PTP 操作模式注意：ET200SP站点中，服务器模
块是必须组态的。服务器模块随接口模块一起采购，无需单独购买。ET200SP接口模块需要为其分配IP地

址和Device Name，有关ET200 SP 分布式IO 组态详细步骤，请参考《ET200 SP 使用快速入门》，本例不再描述Profinet IO通信的相关设置与步骤。《ET200 SP 使用快速入门》下载链接：https://support.industry.siemens.com/cs/cn/zh/view/78304711（3）接下来，在“ 属性 ”→“ 常规 ”→“ 接口 ”→“ 端口组态 ”中配置此模块端口组态参数，本例设定"协议"："Freeport/Modbus"；"端口参数"设置：传输率=9.6Kbps，奇偶校验=无奇偶校验，数据位=8位字符，停止位=1为例。端口组态设置如下图10所示：图10. CM PTP 端口组态（4）最后需要在“ 硬件标识符 ”里确认一下CM PTP 模块硬件标识符，该参数在程序编程中会被使用。（四）实例之软件编程1、Modbus RTU 主站编程Modbus RTU主站编程需要调用Modbus_Comm_Load 指令和Modbus_Master 指令，其中Modbus_Comm_Load 指令通过 Modbus RTU 协议对通信模块进行组态，Modbus_Master 指令可通过由 Modbus_Comm_Load 指令组态的端口作为 Modbus 主站进行通信， Modbus_Comm_Load 指令的 MB_DB 参数必须连接到 Modbus_Master 指令的（静态）MB_DB 参数。本例中分布式机架ET200SP 中 CM PTP 模块作为Modbus RTU主站，其相关编程步骤如下：（1）OB1 中插入一个FC函数，并在函数中拖入Modbus_Comm_Load 指令和Modbus_Master 指令。如图11所示：图11. 拖入Modbus RTU 主站指令Modbus_Comm_Load指令各参数意义如下表1所示：引脚说明REQ上升沿触发PORT通信端口的硬件标识符BAUD波特率选择：3600，6000，12000，2400，4800，9600，19200，38400，57600，76800，115200PARITY奇偶检验选择：0-无；1-奇校验；2-偶校验FLOW_CTRL流控制选择：0-（默认值）无流控制RTS_ON_DLYRTS延时选择：0-（默认值）RTS_OFF_DLYRTS关断延时选择：0-（默认值）RESP_TO响应超时：默认值 = 1000 ms。MB_MASTER 允许用于从站响应的时间（以毫秒为单位）。MB_DB对 Modbus_Master 或 Modbus_Slave 指令的背景数据块的引用。MB_DB 参数必须与 Modbus_Master 或 Modbus_Slave 指令中的静态变量MB_DB 参数相连。DONE如果上一个请求完成并且没有错误，DONE 位将变为 TRUE 并保持一个周期。ERROR如果上一个请求完成出错，则 ERROR 位将变为 TRUE 并保持一个周期。STATUS 参数中的错误代码仅在 ERROR = TRUE 的周期内有效。STATUS端口组态错误代码，请参考TIA 软件在线帮助或S7-1200 系统手册。表1 MB_COMM_LOAD指令参数意义Modbus_Master指令各参数意义如下表2所示：引脚说明EN使能端REQTRUE = 请求向 Modbus 从站发送数据，建议采用上升沿触发MB_ADDRModbus RTU从站地址。默认地址范围：0至247；扩展地址范围：0至65535。值0被保留用于将消息广播到所有Modbus从站。MODE模式选择：指定请求类型（读取或写入）。DATA_ADDR从站中的起始地址：指定Modbus从站中将供访问的数据的起始地址。DATA_LEN数据长度：指定要在该请求中访问的位数或字数。DATA_PTR数据指针：指向要进行数据写入或数据读取的标记或数据块地址。DONE完成位：上一请求已完成且没有出错后，DONE 位将保持为 TRUE 一个扫描周期时间。BUSYFALSE – Modbus_Master 无激活命令:TRUE – Modbus_Master 命令执行中ERRORSTATUS如果上一个请求完成并且没有错误，DONE 位将变为 TRUE 并保持一个周期。ERRORSTATUS错误代码表2 Modbus_Master指令参数意义注意：①Modbus_Comm_Load指令不建议在启动组织块OB100中调用，建议在OB1中调用。Modbus_Comm_Load指令在OB1中调用时，其输入位“ REQ ”需使用上升沿触发，本例中该输入位采用“ FirstScan ”系统存储器位。②Modbus_Comm_Load指令背景数据块中的静态变量“ MODE ”用于描述PTP模块的工作模式，有效的工作模式包括：0 = 全双工 (RS232)1 = 全双工 (RS422) 四线制模式（点对点）2 = 全全双工 (RS 422) 四线制模式（多点主站，CM PtP (ET 200SP)）3 = 全全双工 (RS 422) 四线制模式（多点从站，CM PtP (ET 200SP)）4 = 半双工 (RS485) 二线制模式该静态变量“ MODE ”默认数据为0（RS232 全双工模式），需要根据CM PTP模块实际组态修改该数值，本例中CM PTP模块工作在RS485半双工模式需要将该数值修改为4，如图12所示：图12. Modbus_Comm_Load背景数据块静态变量“ MODE ”修改为③Modbus_Master指令的“ DATA_PTR ”参数用于指向要进行数据写入或数据读取的数据区域地址，该数据区域支持优化访问的数据块或者非优化（标准的）数据块，建议采用非优化访问的数据块。本例中使用的数据区为非优化访问的数据块，在数据块的属性中取消“ 优化的块访问 ”即可将数据块修改为非优化访问的数据块（鼠标右键数据块，选择“ 属性 ”，取消“ 优化的块访问 ”），如图13所示：图13. 设置数据块为非优化访问当Modbus_Master指令的“ DATA_PTR ”指向非优化访问的数据块时，该输入参数需要使用指针方式填写如P#DB3.DBX0.0 WORD 5 方式填写。④当Modbus RTU网络中存在多个modbus RTU从站或一个modbus RTU从站同时需要读操作和写操作，则需要调用多个Modbus_Master指令，Modbus_Master指令之间需要采用轮询方式调用。下图14.用于描述两个Modbus_Master指令轮询调用的方式。图14.Modbus_Master轮询调用方式（2）插入"Pull or plug of modules" 中断OB83本例中Modbus

RTU主站模块安装在分布式IO站点上，因此程序中需要考虑分布式IO站点故障、CM PTP 模块插拔模块等故障。分布式IO站点中插出、拔入模块时，操作系统都会调用一次OB83。通过OB83接口区的输入变量“ 16#Event_Class ”判断故障的模块和类型：事件类型16#39表示模块被拔出，事件类型16#38表示模块被插入。CM PTP 模块被重新插入的时候，需要在中断OB83中调用Modbus_Comm_Load 指令对通信模块进行重新组态，如图15所示。图15. OB83中再次调用Modbus_Comm_Load 指令注意：①OB83 中调用Modbus_Comm_Load指令的背景数据块需要与OB1中调用的Modbus_Comm_Load指令的背景数据块相同。②CM PTP模块的硬件标识符也可以在"PLC变量"--->"系统常数"中查询，如图16所示：图16. 系统常量（3）插入"Rack or Station failure" 中断OB86分布式IO站点故障和恢复时，操作系统都会调用一次OB86。通过OB86接口区的输入变量“ 16#Event_Class ”判断故障的模块和类型：事件类型16#39表示站点故障，事件类型16#38表示站点恢复。CM PTP 模块所在的IO站点恢复时，需要在中断OB86中调用Modbus_Comm_Load 指令对通信模块进行重新组态，如图17所示：图17. OB86中调用Modbus_Comm_Load 指令注意：①OB86中调用Modbus_Comm_Load指令的背景数据块需要与OB1中调用的Modbus_Comm_Load指令的背景数据块相同。②分布式IO 站点的硬件标识符也可以在"PLC变量"--->"系统常数"中查询。2、Modbus RTU 从站编程Modbus RTU从站编程需要调用Modbus_Comm_Load 指令和Modbus_Slave 指令，其中Modbus_Comm_Load 指令通过 Modbus RTU 协议对通信模块进行组态，Modbus_Slave 指令可通过由 Modbus_Comm_Load 指令组态的端口作为 Modbus 从站进行通信， Modbus_Comm_Load 指令的 MB_DB 参数必须连接到 Modbus_Slaver 指令的（静态）MB_DB 参数。本例中CPU 机架CM1241 RS422/485作为Modbus RTU从站，其相关编程步骤如下：（1）OB1 中插入一个FC函数，并在函数中拖入Modbus_Comm_Load 指令和Modbus_Slave 指令。如图18所示：图18. 拖入Modbus RTU 从站指令Modbus_Slave指令各参数意义如下表3所示：引脚说明MB_ADDRModbus 从站的标准寻址：标准寻址范围（1 到 247）扩展寻址范围（0 到 65535）MB_HOLD_REG数据指针，指向Modbus 保持寄存器的地址， Modbus 保持寄存器可以为M存储区或DB数据区。如果Modbus 保持寄存器为DB数据区，则DB数据区支持优化访问的数据块或非优化访问的数据块，建议采用非优化访问的数据块。NDR可用的新数据：FALSE - 无新数据TRUE – 表示新数据已由 Modbus 主站写入如果上一个请求完成并且没有错误，NDR 位将变为 TRUE 并保持一个周期。DR读取数据：FALSE - 无新数据TRUE – 表示该指令已将 Modbus 主站接收到的数据存储在目标区域中。如果上一个请求完成并且没有错误，DR 位将变为 TRUE 并保持一个周期。ERROR如果上一个请求完成出错，则 ERROR 位将变为 TRUE 并保持一个周期。如果执行因错误而终止，则 STATUS 参数中的错误代码仅在 ERROR = TRUE 的周期内有效。STATUS错误代码表3 Modbus_Slave指令参数意义注意：①Modbus_Comm_Load指令不建议在启动组织块OB100中调用，建议在OB1中调用。Modbus_Comm_Load指令在OB1中调用时，其输入位“ REQ ”需使用上升沿触发，本例中该输入位采用“ FirstScan ”系统存储器位。②Modbus_Comm_Load 指令背景数据块中的静态变量“ MODE ”用于描述PTP模块的工作模式，有效的工作模式包括：0 = 全双工 (RS232)1 = 全双工 (RS422) 四线制模式（点对点）2 = 全全双工 (RS 422) 四线制模式（多点主站，CM PtP (ET 200SP)）3 = 全全双工 (RS 422) 四线制模式（多点从站，CM PtP (ET 200SP)）4 = 半双工 (RS485) 二线制模式该静态变量“ MODE ”默认数据为0（RS232 全双工模式），需要根据CM1241 RS422/485模块实际组态修改该数值，本例中CM1241 RS422/485模块工作在RS485半双工模式需要将该数值修改为4，如何修改“ MODE ”静态变量见图12所示。③Modbus_Slave指令的“ MB_HOLD_REG ”用于指向Modbus 保持寄存器的数据区域地址，该数据区域支持优化访问的数据块或者非优化（标准的）数据块，建议采用非优化访问的数据块。本例中使用的数据区为非优化访问的数据块，固该输入参数需要使用指针方式填写如P#DB6.DBX0.0 WORD 100 方式填写。如何在数据块的属性中取消“ 优化的块访问 ”，见图13所示。将程序下载到PLC中，并使用Profibus DP通信电缆将CM1241 RS422/485与CM PTP串口模块连接起来，即可测试Modbus RTU通信了。