佳木斯西门子模块PLC代理商-高压变频器，电机一级总代理

产品名称	佳木斯西门子模块PLC代理商- 高压变频器，电机一级总代理
公司名称	上海跃韦科技集团有限公司
价格	.00/件
规格参数	西门子:西门子PLC模块.电机代理 全系列:西门子变频器通讯电缆代理 德国:西门子触摸屏DP接头代理
公司地址	上海市金山区吕巷镇溪北路59号5幢（三新经济小区）（注册地址）
联系电话	15821196730 15821196730

产品详情

我司长期***供应产品：西门子授权代理商优点详尽详细如下：

1、 SIMATIC，PLC、S7-200、S7-300、S7-400、S7-1200,S7-1500,S7-200SMART,S7-200CN,ET200

2、 逻辑思维控制器 LOGO！230RC、230RCO、230RCL、24RC、24RCL等

3、 SITOP 系列产品可调稳压电源 24V DC 1.3A、3A、10A、20A、40A

4、HMI 触摸液晶屏TD200 TD400C TP177,MP277 MP377SIEMENS 交、可调稳压电源传动系统

5、 变频调速器MICROMASTER系列产品：MM、MM420、MM430、MM440、G110，G120,V20,V90,ECO MIDASTER系列产品：MDV 6SE70系列产品（FC、VC、SC）

6、全源数据直流调速装置 6RA23、6RA24、6RA28、6RA70 系列产品SIEMENS 加工中心 直流伺服电机

7、840D、802S/C、802SL、828D 801D：6FC5210,6FC6247,6FC5357,6FC5211,6FC5200,6FC5510,

8、伺服驱动 ：6SN1123,6SN1145,6SN1146,6SN1118,6SN1110,6SN1124,6SN1125,6SN1128

近西门子PLC价格大幅上调，在工控界引起了不小的风波，不仅涨价，甚至还缺货，导致很多人不得不更改方案。听说近已经完成了芯片替换，希望不久能够恢复供货，并把价格回调。

通过这件事，从侧面可以看出，西门子在工控领域的市场占有率很大，那么对于上位机开发人员来说，使用西门子PLC作为下位机，我们应该如何与之进行通信呢？

西门子PLC支持很多种通信协议，主要分为两种，一种是串口通信，一种是以太网通信，同时也可以通过OPC实现数据通信。

串口通信

西门子PLC支持串口通信，在S7-200和S7-200Smart中，都直接集成了串口，但是从S7-1200到S7-1500，慢慢都取消掉了，如果需要，可以通过扩展模块的方式来增加，出现这种现象的原因，其实也是工业发展的必然结果。串口通信的优势在于简单、成本低，但是劣势也非常明显，就是传输效率低。西门子早期的串口通信主要是Profibus DP通信，但是上位机是无法直接与西门子PLC走Profibus DP通信的，因此，西门子PLC常用的串口通信方案如下所示：

PPI通信：PPI通信只针对S7-200和S7-200 Smart系列PLC，其他型号不支持。

ModbusRTU主站：西门子PLC对Modbus协议支持还是比较不错的，这里是指PLC做Slave（即从站），上位机做Master（即主站）。

ModbusRTU从站：这里是指PLC做Master（即主站），上位机做Slave（即从站）。

以太网通信

西门子PLC通信还是以太网通信为主，我们常说的西门子通信协议分别是S7协议和Profinet协议，但是Profinet是一种总线协议，目前，C#是无法直接与西门子PLC走Profinet通信的。因此，西门子PLC常用的以太网通信方案如下所示：

S7通信：基本上从S7-200到S7-1500均可以实现，这里有很多可以选择的开源或商业库，包括

http://s7.net、pronodave、libnodave、sharp7，也可以自己封装通信库。

ModbusTCP Server：这里是指PLC做Server（即服务器），上位机做Client（即客户端）。

ModbusTCP Client：这里是指PLC做Client（即客户端），上位机做Server（即服务器）。

OpenProtocol Server：这里是指开放式TCP通信，PLC做TCPServer（即服务器），上位机做TCPClient（即客户端）。

OpenProtocol Client：这里是指PLC做TCPClient（即客户端），上位机做TCPServer（即服务器）。

OPC通信

OPC通信是工业控制中常用的一种通信方式，主要在于OPC软件的选择以及OPCDA、OPCUA的选择，因此，西门子PLC常用的OPC通信方案如下所示：

PC Access系列：西门子针对S7-200开发PC-Access软件，针对S7-200 Smart又提供了PC-Access Smart软件，可以直接通过这些软件实现OPCDA通信。

Simatic Net 系列OPCDA：Simatic Net是西门子主推的OPC软件，支持西门子全系列，这里主要是OPCDA通信方式。

Simatic Net 系列OPCUA：新版的Simatic Net也开始支持OPCUA，这里主要是OPCUA通信方式。

KepServer 系列OPCDA：KepServer同样作为一款商业OPC软件，在国内使用率非常高，同样也支持西门子全系列，这里主要是OPCDA通信方式。

Simatic Net 系列OPCUA：新版的KepServer也开始支持OPCUA，这里主要是OPCUA通信方式。

S7通信协议

在以上众多的通信方式和通信协议中，就目前而言，使用S7通信是***方便，也是应该***广泛的，那么S7协议相对于其他协议来说，有哪些优势呢？

使用S7通信协议***大的优势在于不需要编写PLC程序，而且S7协议在底层做了很强的封装，在上位机通信应用中相比其他通信协议来说，也有很大的优势。

虽然不需要编写PLC程序，但仍然需要做一些简单的配置：

开启Put/Get

PLC侧需要设置勾选允许来自远程对象的Put/Get通信访问
对于西门子1200/1500系列，必须要勾选允许Put/Get访问，对于200Smart/300/400，则不需要。

DB块去除优化访问

对于基于博图开发S7-1200/1500的项目，如果要与DB块数据通信，需要要去除DB的优化的块访问，对于200Smart/300/400，则不需要。如果希望通过标签通信，可以采用OPCUA。

务必保证通信地址是有效地址

因为PLC大多数是基于存储区的，每个地址肯定是隶属于某个存储区，大家都知道西门子PLC自带的存储区有I区、Q区、M区、T区、C区，但是对于常用的DB存储区是没有的，需要自己去创建，也就意味着，如果你要读取DB地址，必须要提前创建好DB存储区，除此以外，DB存储区创建之后，默认是没有字节的，需要自己一个个添加变量，才能形成有效存储区，因此一个DB存储区的范围是有限并且可见的（可以通过偏移量看出来）。

S7协议之布尔操作

对于布尔操作，很多协议都有，但是这里的布尔操作是指寄存器布尔，比如DB100.DBX0.0，很多时候，我们都是通过先读取DB100.DBB0的值，再通过位运算结果，写入到DB100.DBB0中，实现DB100.DBX0.0的操作，但是这种方式有弊端

***：每次操作一个布尔值都需要与PLC进行两次数据交互。

第二：安全性和稳定性无法保障，你不知道在你读取和写入之间，这个字节的值是否已经发生了改变。

这样的问题也存在于Modbus协议的寄存器位操作，如40001.05，三菱、欧姆龙的寄存器位操作，如D100.06、W12.04，给上位机开发者带来很多苦恼。

但是S7协议支持直接位操作，有专门的报文指令实现这样的功能。

S7协议之PDU读取

大部分人都知道S7协议一次性读取有限制，但是具体是多少？怎么计算出来的？

S7协议的一次性读取长度是根据PDU计算出来的，这个PDU的值是来自于PLC本身，不同型号的CPU，它的PDU是不一样的，可以参考下面两张图：

西门子PLC的PDU大小是和CPU息息相关的，一般会有240、480、960三个档次，知道PDU之后，那么一次性读取的字节长度，就是在PDU的基础上减去18，这个18是指包头包尾会有18个字节，这样我们就知道了一般的PLC，一次性能读取222个字节（240-18=222），但是对于S7-1516这样的PLC，我们一次性是可以读取942个字节的（960-18=942），这个一次性能读取的字节越长，越能提高上位机的通信效率。

刚刚的方式是通过KepServer测试的，实际开发过程中，该怎么获取CPU的PDU呢，实际上在建立连接的第二次握手时，返回的报文中就包含PDU的值。

第二次握手返回的报文长度是27个字节，***后两个字节就是PDU的值，上图展示的是S7-1200PLC返回的报文，0和240的组合即为240。

对于S7-1500，我这里也做了一下测试，结果如下，返回结果为3和192，3和192的组合恰好是960（960=3*256+192）。

虽然PDU是由硬件做了限制，但是我们可以通过软件的方式，实现大量数据的读取，只需要在底层做一些封装即可。做了一下测试，针对S7-1200和S7-1500同时读取M区的8000个字节的耗时比较，S7-1200耗时800多ms，S7-1500耗时仅需200ms，由此可见，硬件对通信的重要性。

S7协议之多组读取

对于很多其他的通信协议，当我们遇到数据变量比较零散，同时读取多个存储区或者一个存储区多个不同部分的时候，我们只能针对每个存储区或者每块区域做一个数据请求，但是西门子S7协议可以解决这样的问题。

西门子S7协议有一个非常强大的一个地方，可以同时读取很多个不同的存储区，***大支持19种，总共读取长度仍然受PDU的限制。

这里我们仍然以实验测试为例，体验多组读取带来的美妙体验。

假设我们的通信组配置如下：

通信组01：读取I区从0开始的1个字节

通信组02：读取Q区从0开始的1个字节

通信组03：读取M区从0开始的200个字节

通信组04：读取M区从500开始的50个字节

通信组05：读取M区从1000开始的60个字节

通信组06：读取DB100从0开始的20个字节

通信组07：读取DB100从20开始的20个字节

通信组08：读取DB100从40开始的20个字节

通信组09：读取DB100从60开始的20个字节

我们采用常用S7-1200PLC，通过配置软件实现配置以上9个通信组，开始通信测试，首先我们选择的是单组读取的方式，就是针对每个组，依次进行读取，结果如下，耗时大约200ms，这个时间应该相对来说还是比较正常的。

接着，将读取方式改成了多组读取，再进行测试发现结果如下：

通过结果发现，多组读取对于存储区较为零散的项目来说，有着非常重要的作用，可以大大提高通信效率。

总结

通过上面一系列的分享，相信大家对西门子PLC通信有了更加深入的了解，希望大家可以多多实践。

每种通信方式都有自己的优缺点，对各种通信方式和协议了解之后，你才能够在不同的场合选择适合的通信方式，给出***合理的解决方案。