

西门子一级总代理2024已更新

| | |
|------|--|
| 产品名称 | 西门子一级总代理2024已更新 |
| 公司名称 | 浔之漫智控技术（上海）有限公司 |
| 价格 | 888.00/台 |
| 规格参数 | 西门子:西门子代理商 西门子CPU:西门子plc 德国:全新原装 |
| 公司地址 | 上海市松江区石湖荡镇塔汇路755弄29号1幢一层A区213室 |
| 联系电话 | 195****8569 195****8569 |

产品详情

西门子一级总代理2024已更新

西门子一级总代理2024已更新

西门子一级总代理2024已更新

浔之漫智控技术（上海）有限公司 经营理念是：以质量求生存，以诚信谋发展。

我们公司能提供全套产品，我们有着zuihao的库存，最优惠的价格

，最优质的售后服务和最强大的技术力量

我公司大量现货供应，价格优势，品质保证，德国原装进口

西门子PLC通信全解析

前言

最近西门子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。听说最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TCP Server（即服务器），上位机做TCP Client（即客户端）。

OpenProtocol Client：这里是指PLC做TCP Client（即客户端），上位机做TCP Server（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通信是最方便，也是应该最广泛的，那么S7协议相对于其他协议来说，有哪些优势呢？

使用S7通信协议最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

第一：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。

PLC与变频器屏蔽线的接法

为防止plc和变频器之间的控制信号线受空间电磁场的干扰，可在这些控制信号线的外层接屏蔽线，以提高系统的抗干扰能力。此种接线一定要注意，对屏蔽的接地点只能选取一点。不管是在PLC一边，还是在变频器的一边。一般选在信号接收端，即变频器一边。这样，可提高系统的抗干扰能力。如果屏蔽线在两端都接地，会使屏蔽线上有电流流过，不但不能提高系统的抗干扰的能力，反而会加重外界对PLC的干扰。

PLC与变频器屏蔽线的接法遵守下面的原则

屏蔽线尽量靠尽电势低的一端，可以这么理解，一般我们认为地电势为“0”，而在事实情况下，如有两个接地端，某一时刻两个接地端会存在电势差，在两个接电线之间将会有电流经过，这也是一种干扰。

在实际应用中如果控制电缆经过的场所比较复杂需要多端接地的时候,我们一般采取割断屏蔽层,再不同的地方接地.较厂的控制设备通讯电缆屏蔽层接地也常采取这种方式。

以上就是PLC与变频器屏蔽线的接法的相关信息，希望可以帮到您。

| | |
|--------------------|---|
| 6ES7288-2DE08-0AA0 | S7-200 SMART，EM DE08，数字量输入模块，8 x 24 V DC 输入 |
| 6ES7288-2DE16-0AA0 | S7-200 SMART，EM DE16，数字量输入模块，16 x 24 V DC 输入 |
| 6ES7288-2DR08-0AA0 | S7-200 SMART，EM DR08，数字量输出模块，8 x 继电器输出 |
| 6ES7288-2DT08-0AA0 | S7-200 SMART，EM DT08，数字量输出模块，8 x 24 V DC 输出 |
| 6ES7288-2QR16-0AA0 | S7-200 SMART，EM QR16，数字量输出模块，16 x 继电器输出 |
| 6ES7288-2QT16-0AA0 | S7-200 SMART，EM QT16，数字量输出模块，16 x 24 V DC 输出 |
| 6ES7288-2DR16-0AA0 | S7-200 SMART，EM DR16，数字量输入/输出模块，8 x 24 V DC 输入/8 x 继电器输出 |
| 6ES7288-2DT16-0AA0 | S7-200 SMART，EM DT16，数字量输入/输出模块，8 x 24 V DC 输入/8 x 24 V DC 输出 |
| 6ES7288-2DR32-0AA0 | S7-200 SMART，EM DR32，数字量输入/输出模块，16 x 24 V DC 输入/16 x 继电器输出 |
| 6ES7288-2DT32-0AA0 | S7-200 SMART，EM DT32，数字量输入/输出模块，16 x 24 V DC 输入/16 x 24 V DC 输出 |
| 6ES7288-3AE04-0AA0 | S7-200 SMART，EM AE04，模拟量输入模块，4 输入 |
| 6ES7288-3AE08-0AA0 | S7-200 SMART，EM AE08，模拟量输入模块，8 输入 |
| 6ES7288-3AQ02-0AA0 | S7-200 SMART，EM AQ02，模拟量输出模块，2 |

| | |
|--------------------|--|
| 6ES7288-3AQ04-0AA0 | 输出 S7-200 SMART, EM AQ04, 模拟量输出模块, 4 输出 |
| 6ES7288-3AM03-0AA0 | S7-200 SMART, EM AM03, 模拟量输入/输出模块, 2 输入/ 1 输出 |
| 6ES7288-3AM06-0AA0 | S7-200 SMART, EM AM06, 模拟量输入/输出模块, 4 输入/ 2 输出 |
| 6ES7288-3AR02-0AA0 | S7-200 SMART, EM AR02, 热电阻输入模块, 2 通道 |
| 6ES7288-3AR04-0AA0 | S7-200 SMART, EM AR04, 热电阻输入模块, 4 通道 |
| 6ES7288-3AT04-0AA0 | S7-200 SMART, EM AT04, 热电偶输入模块, 4 通道 |

我公司是一家专业的自动化工控产品维修企业，公司有充足的备件和优良的维修工程师，可为客户提供各

种品牌变频器维修，伺服维修，直流调速器维修，数控系统维修，触摸屏维修及各种控制板，电路板类的

专业维修、现场抢修、技术支持等。维修企业化运作，为客户提供持续的保障，所有维修工程师均接受专

业的技术培训，除现场器件板类快速更换维修外，我们均采用器件级维修，只将故障电子元器件及不良电

子元器件进行更换，以此降低维修成本。 24小时接修服务，先检测，报价，经用户认可再进行维修。所有维修变频器经负载试验、质量保证，没有修不好的机器，只有不精通的技术，维修成功率99%。
维修一部：专业维修西门子变频器、伺服、直流调速器、触摸屏、PLC、电源等全系列自动化产品，维修工程师经西门子培训合格后持证上岗。