

# SIEMENS西门子吉林省吉林市（授权）电机一级代理商——西门子东北总代理

产品名称	SIEMENS西门子吉林省吉林市（授权）电机一级代理商——西门子东北总代理
公司名称	广东湘恒智能科技有限公司
价格	.00/件
规格参数	西门子总代理:PLC 西门子一级代理商:驱动 西门子代理商:伺服电机
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	15903418770 15915421161

## 产品详情

### Modbus TCP通信

通信方式Modbus设备可分为主站(master)和从站(slave)。主站只有一个，从站有多个，主站向各从站发送请求帧，从站给予响应。在使用TCP通信时，主站为client端，主动建立连接；从站为server端，等待连接。

主站请求：功能码+数据

从站正常响应：请求功能码+响应数据

从站异常响应：异常功能码+异常码，其中异常功能码即将请求功能码的最高有效位置1，异常码指示差错类型

注意：需要超时管理机制，避免无期限的等待可能不出现的应答

IANA ( Internet Assigned Numbers Authority , 互联网编号分配管理机构 ) 给Modbus协议赋予TCP端口号为502，这是目前在仪表与自动化行业中唯一分配到的端口号。通信过程

connect 建立TCP连接准备Modbus报文使用send命令发送报文在同一连接下等待应答使用recv命令读取报文，完成一次数据交换通信任务结束时，关闭TCP连接

## 仿真软件

Modbus poll 和Modbus slave是一组Modbus仿真软件，可以实现Modbus RTU、TCP、串口仿真等。

仿真软件网址：<https://modbustools.com/download.html>

在ModbusTCP中，Modbus poll 作为客户端请求数据，Modbus slave 作为服务器端处理请求。

使用c语言编写客户端连接Modbus slave时，注意数据格式，一条指令一次性发出，否则连接会出错。

使用软件时，需要指定功能码，在setup->slave definition或者poll definition中进行设置。- slave ID：从站编号（事务标识符）- function：功能码，0x01对应线圈操作，0x02对应离散量操作，0x03对应保持寄存器操作，0x04对应输入寄存器操作- address：开始地址- quantity：寄存器/线圈/离散量的数量

## 一些概念

在工业自动化控制中，经常会遇到开关量，数字量，模拟量，离散量，脉冲量等各种概念，而人们在实际应用中，对于这些概念又很容易混淆。现将各种概念罗列如下：1.开关量一般指的是触点的“开”与“关”的状态，一般在计算机设备中也会用“0”或“1”来表示开关量的状态。开关量分为有源开关量信号和无源开关量信号，有源开关量信号指的是“开”与“关”的状态是带电源的信号，专业叫法为跃阶信号，可以理解为脉冲量，一般的都有220VAC,110VAC,24VDC,12VDC等信号，无源开关量信号指的是“开”和“关”的状态时不带电源的信号，一般又称之为干接点。电阻测试法为电阻0或无穷大。2.数字量很多人会将数字量与开关量混淆，也将其与模拟量混淆。数字量在时间和数量上都是离散的物理量，其表示的信号则为数字信号。数字量是由0和1组成的信号，经过编码形成有规律的信号，量化后的模拟量就是数字量。3.模拟量模拟量的概念与数字量相对应，但是经过量化之后又可以转化为数字量。模拟量是在时间和数量上都是连续的物理量，其表示的信号则为模拟信号。模拟量在连续的变化过程中任何一个取值都是一个具体有意义的物理量，如温度，电压，电流等。4.离散量离散量是将模拟量离散化之后得到的物理量。即任何仪器设备对于模拟量都不可能有个完全jingque的表示，因为他们都有一个采样周期，在该采样周期内，其物理量的数值都是不变的，而实际上的模拟量则是变化的。这样就将模拟量离散化，成为了离散量。5.脉冲量脉冲量就是瞬间电压或电流由某一值跃变到另一值的信号量。在量化后，其变化持续有规律就是数字量，如果其由0变成某一固定值并保持不变，其就是开关量。综上所述，模拟量就是在某个过程中时间和数量连续变化的物理量，由于在实际的应用中，所有的仪器设备对于外界数据的采集都有一个采样周期，其采集的数据只有在下一个采样周期开始时才有变动，采样周期内其数值并不随模拟量的变化而变动。这样就将模拟量离散化了，例如：某设备的采样周期为1秒，其在第五秒的时间采集的温度为35度，而第六秒的温度为36度，该设备就只能标称第五秒时间温度35度，第六秒时间温度36度，而第五点五秒的时间其标称也只是35度，但是其实际的模拟量是35.5度。这样就将模拟信号离散化。其采集的数据就是离散化了，不再是连续的模拟量信号。由于计算机只识别0和1两个信号，即开关量信号，用其来表示数值都是使用数字串来表示，由于计算能力的问题，其数字串不能无限长，即其表达的精度也是有限的，同样的以温度为例，由于数字串限制，其表达温度的精度只能达到0.1度，小于该单位的数值则不能被标称，这样就必须将离散量进行量化，将其变为数字量。即35.68度的温度则表示为35.6度。