

SIEMENS江西省吉安市西门子中国授权代理商-西门子变频器- 西门子技术服务-西门子PLC模块

产品名称	SIEMENS江西省吉安市西门子中国授权代理商- 西门子变频器-西门子技术服务-西门子PLC模块
公司名称	广东湘恒智能科技有限公司
价格	.00/件
规格参数	变频器:西门子代理商 触摸屏:西门子一级代理 伺服电机:西门子一级总代理
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（仅限办公）（注册地址）
联系电话	18126392341 15267534595

产品详情

Modbus TCP数据帧

ModbusTCP的数据帧可分为两部分：MBAP+PDU。（一）报文头MBAP：MBAP为报文头，长度为7字节，组成如下：

（二）帧结构PDU：PDU由功能码+数据组成。功能码为1字节，数据长度不定，由具体功能决定。

（1）功能码：Modbus的操作对象有四种：线圈、离散输入、保持寄存器、输入寄存器。

BPDU详细结构

请求：MBAP 功能码 起始地址H 起始地址L 数量H 数量L（共12字节）响应：MBAP 功能码 数据长度
数据（一个地址的数据为1位）如：在从站0x01中，读取开始地址为0x0002的线圈数据，读0x0008位00 01
00 00 00 06 01 01 00 02 00 08回：数据长度为0x01个字节，数据为0x01，第一个线圈为ON，其余为OFF00 01
00 00 00 04 01 01 01 01

（2）0x05：写单个线圈：将从站中的一个输出写成ON或OFF，0xFF00请求输出为ON,0x000请求输出为O
FF。

请求：MBAP 功能码 输出地址H 输出地址L 输出值H 输出值L（共12字节）响应：MBAP 功能码
输出地址H 输出地址L 输出值H 输出值L（共12字节）如：将地址为0x0003的线圈设为ON00 01 00 00 00 06
01 05 00 03 FF 00回：写入成功00 01 00 00 00 06 01 05 00 03 FF 00

（3）0x0F：写多个线圈：将一个从站中的一个线圈序列的每个线圈都强制为ON或OFF，数据域中置1的
位请求相应输出位ON，置0的位请求响应输出为OFF。

请求：MBAP 功能码 起始地址H 起始地址L 输出数量H 输出数量L 字节长度 输出值H
输出值L响应：MBAP 功能码 起始地址H 起始地址L 输出数量H 输出数量L

（4）0x02：读离散量输入：从一个从站中读1~2000个连续的离散量输入状态。

请求：MBAP 功能码 起始地址H 起始地址L 数量H 数量L（共12字节）响应：MBAP 功能码 数据长度
数据（长度：9+ceil（数量/8））如：从地址0x0000开始读0x0012个离散量输入00 01 00 00 00 06 01 02 00 00
00 12回：数据长度为0x03个字节，数据为0x01 04
00，表示第一个离散量输入和第11个离散量输入为ON，其余为OFF00 01 00 00 00 06 01 02 03 01 04 00

（5）0x04：读输入寄存器：从一个远程设备中读1~2000个连续输入寄存器。

请求：MBAP 功能码 起始地址H 起始地址L 寄存器数量H 寄存器数量L（共12字节）响应：MBAP 功能码
数据长度 寄存器数据(长度：9+寄存器数量×2)如：读起始地址为0x0002，数量为0x0005的寄存器数据00
01 00 00 00 06 01 04 00 02 00 05回：数据长度为0x0A，第一个寄存器的数据为0x0c，其余为0x0000 01 00 00 00
0D 01 04 0A 00 0C 00 00 00 00 00 00 00 00

（6）0x03：读保持寄存器：从远程设备中读保持寄存器连续块的内容。

请求：MBAP 功能码 起始地址H 起始地址L 寄存器数量H 寄存器数量L（共12字节）响应：MBAP 功能码
数据长度 寄存器数据(长度：9+寄存器数量×2)如：起始地址是0x0000，寄存器数量是 0x000300 01 00 00
00 06 01 03 00 00 00 03回：数据长度为0x06，第一个寄存器的数据为0x21，其余为0x0000 01 00 00 00 09 01 03
06 00 21 00 00 00 00

(7) 0x06 : 写单个保持寄存器 : 在一个远程设备中写一个保持寄存器。

请求 : MBAP 功能码 寄存器地址H 寄存器地址L 寄存器值H 寄存器值L (共12字节) 响应 : MBAP 功能码
寄存器地址H 寄存器地址L 寄存器值H
寄存器值L (共12字节) 如 : 向地址是0x0000的寄存器写入数据0x000A00 01 00 00 00 06 01 06 00 00 00
0A回 : 写入成功00 01 00 00 00 06 01 06 00 00 00 0A

(8) 0x10 : 写多个保持寄存器 : 在一个远程设备中写连续寄存器块 (1~123个寄存器)。

请求 : MBAP 功能码 起始地址H 起始地址L 寄存器数量H 寄存器数量L 字节长度
寄存器值 (13+寄存器数量 × 2) 响应 : MBAP 功能码 起始地址H 起始地址L 寄存器数量H 寄存器数量L (共12字节) 如 : 向起始地址为0x0000, 数量为0x0001的寄存器写入数据, 数据长度为0x02, 数据为0x000F
00 01 写入成功00 01 00 00 00 06 01 02 00 00 00 01