# VIENA PLC\_modbus协议使用说明

VIENA系列PLC提供串口RS232，串口RS485 , 以太网等通讯端口；可兼容MODBUS RTU，MODBUS TCP协议。

### PLC寄存器对应Modbus地址（10进制）

|  |  |  |  |
| --- | --- | --- | --- |
| **Modbus地址** | | **PLC内部地址** | **说明** |
| 0x | 0000~0255 | Q0.0~Q31.7 | PLC输出线圈 |
| 1x | 0000~0255 | I0.0~I31.7 | PLC离散输入 |
| 3x | 0000~0031 | AIW0~AIW62 | PLC模拟量输入寄存器 |
| 4x | 0000~0031 | AQW0~AQW62 | PLC模拟量输出寄存器 |
| 4x | 0032~0047 | MW0~MW30 | PLC保持寄存器 |
| 4x | 1140~？ | VW0~？ | V区地址范围根据PLC型号而定 |

在对PLC寄存器数据进行位操作时，每个modbus地址中需将高低八位地址对换。

例： 4x1140.0 → V1.0

**⇣**

4x1140.7 → V1.7

4x1140.8 → V0.0

**⇣**

4x1140.15 → V0.7

**注：市面上现有部分设备MODBUS起始地址为1，则使用该类型设备与PLC通讯时，在本文档中MODBUS地址上+1即可。**

### MODBUS通讯格式

MODBUS RTU (读寄存器请求)

|  |  |  |  |
| --- | --- | --- | --- |
| 上位机请求 | | PLC应答 | |
| 从站地址(8bit) | 01H | 从站地址(8bit) | 01H |
| 功能码(8bit) | 03H | 功能码(8bit) | 03H |
| 起始寄存器地址(16bit) | 04H | 数据长度(8bit) | 04H |
| 74H | 回复数据 (读取数据长度\*16bit) | 00H |
| 读取数据长度(16bit) | 00H | 00H |
| 02H | 00H |
| CRC校验码(16bit) | 85H | 00H |
| 21H | CRC校验码(16bit) | FAH |
|  |  | 33H |

**CRC 校验码： (多项式：X16+X15+X2+1)**

CRC（Cyclical Redundancy Check）校验码是由以下方法计算得出

步骤一：加载一值为FFFFH 的16 位寄存器，称为CRC 寄存器。

步骤二：数据的第一字节和CRC 寄存器的低字节作异或门运算，并将运算结果放回CRC 寄存器。

步骤三：将CRC 寄存器位右移并将最高位填零，并检查移出之最低字节。

步骤四：如果移出的最低字节为0 重复步骤三，否则将CRC 寄存器与值A001H 作异或门运算，并将运算结果放回CRC 寄存器。

步骤五：重复步骤三及四，直到8 个位皆完成右移。如此一个字节便完成。

步骤六：重复步骤二及五，将数据内所有字节计算一次便可得出CRC 校验码。

请特别注意传收数据格式中CRC 寄存器的高、低字节传送顺序。

MODBUS TCP (读寄存器请求)

|  |  |  |  |
| --- | --- | --- | --- |
| 上位机请求 | | PLC应答 | |
| 事务处理标识(16bit) | 00H | 事务处理标识(16bit) | 00H |
| 00H | 00H |
| 协议标识(16bit)  0为modbus协议 | 00H | 协议标识(16bit) | 00H |
| 00H | 00H |
| 请求后缀数据长度(16bit) | 00H | 应答后缀数据长度(16bit) | 00H |
| 06H | 07H |
| 从站地址(8bit) | 01H | 从站地址(8bit) | 01H |
| 功能码(8bit) | 03H | 功能码(8bit) | 03H |
| 起始寄存器地址(16bit) | 04H | 应答数据长度(8bit) | 04H |
| 74H | 回复数据 (读取数据长度\*16bit) | 00H |
| 读取数据长度(16bit) | 00H | 00H |
| 02H | 00H |
|  |  | 00H |