**Modbus通信协议**

Modbus Communication protocol

**1.数据格式Data Format：**

**1.1串口参数 Serial port parameters**

1200-115200波特率，1位起始位，8位数据位，偶校验，1位停止位。

1200-115200 baud rate, 1 start bit, 8 data bits, even parity, 1 stop bit.

**1.2 帧描述Frame description：**

|  |  |  |  |
| --- | --- | --- | --- |
| 从机地址  Slave address | 功能码  Function code | 数据  Data | CRC16 |
| 1 字节  1 byte | 1 字节  1 byte | 0-252 字节  0-252 bytes | 2 字节  2 bytes |

Modbus帧最大长度为256字节，必须以连续的字符流发送整个报文帧，字符与字符之间的时间间隔不允许超过2毫秒。

The maximum length of the Modbus frame is 256 bytes, and the entire message frame must be sent as a continuous character stream. The time interval between characters is not allowed to exceed 2 milliseconds.

注：数据流发送时，除CRC16为低字节在前外，其余数据均为高字节在前。

Note: When the data stream is sent, except for CRC16, which is low byte first, the rest of the data is high byte first.

**2.通用读写命令 Read and write commands**

**2.1功能码03H/04H （读取寄存器）Function code 03H/04H (read register)**

主机发送命令：The host sends the command:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 内容  Content | 从机地址  Slave  address | 功能码  Function  code | 起始寄存器地址  Start register  address | 读取寄存器个数  Read the number of registers | CRC16 |
| 长度length | 1 | 1 | 2 | 2 | 2 |
| 举例Example | 0x01 | 0x03 | 0x00 0x02 | 0x00 0x09 | 0x24 0x0C |

从机正常应答命令The slave responds to the command normally：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 内容Content | 从机地址  Save address | 功能码  Function code | 数据字节数  Data bytes | 数据  Data | CRC16 |
| 长度Length | 1 | 1 | 1 | 寄存器个数\*2  Number of registers\*2 | 2 |
| 举例Example | 0x01 | 0x03 | 0x12 | 从寄存器0002开始  的9个地址的数据  Starting from register 0002  The data of 9 addresses |  |

每个寄存器地址对应数据为2字节。

The data corresponding to each register address is 2 bytes.

如果寄存器地址无效则发送异常应答（功能码最高位置1），格式如下：

If the register address is invalid, an exception response will be sent (the highest position of the function code is 1). The format is as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 内容  Content | 从机地址  Slave address | 功能码  Function code | 错误代码  Error code | CRC16 |
| 长度length | 1 | 1 | 1 | 2 |
| 举例example | 0x01 | 0x83 | 0x02 | 0xC0 0xF1 |

**2.2 功能码06H（****写单个寄存器） /Function Code 06H(write a single register)**

主机发送命令：Host sends demand

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 内容Content | 从机地址  Slave address | 功能码  Function  code | 寄存器地址  Register  address | 保存数据  Saved  data | CRC16 |
| 长度length | 1 | 1 | 2 | 2 | 2 |
| 举例example | 0x01 | 0x06 | 0x00 0x00 | 0x00 0x02 | 0x08 0x0B |

从机正常应答命令：the slave responds demands normally

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 内容  Content | 从机地址  Slave address | 功能码  Function code | 寄存器地址  Register address | 保存的数据  Saved date | CRC16 |
| 长度length | 1 | 1 | 2 | 2 | 2 |
| 举例example | 0x02 | 0x06 | 0x00 0x00 | 0x00 0x02 | 0x08 0x38 |

注：对于本设备，修改0x0000地址数据即修改从机地址。

Note: For this device, modifying the 0x0000 address data means modifying the slave address.

如果数据错误或者寄存器地址无效，从机返回异常应答，格式如下。

If the data is wrong or the register address is invalid, the slave returns an exception response with the following format.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 内容  Content | 从机地址  Slave address | 功能码  Function code | 错误代码  Error code | CRC16 |
| 长度length | 1 | 1 | 1 | 2 |
| 举例example | 0x01 | 0x86 | 0x03 | 0x02 0x61 |

**2.3功能码10H （写多个数据到连续寄存器）**

**Function code 10H (write multiple data to continuous registers)**

主机发送命令: the host sends demands

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 内容  content | 从机  地址  slave address | 功能码function code | 寄存器  起始地址  register  initial address | 寄存器  个数 the numbers of register | 数据  字节数 data bytes | 数据1  Data 1 | 数据2  Data 2 | 数据N  Data N | CRC16 |
| 长度length | 1 | 1 | 2 | N | 1 | 2 | 2 | … | 2 |
| 举例example | 0x01 | 0x10 | 0x00  0x00 | 0x00  0x01 | 0x02 | 0x00  0x02 |  |  | 0x27  0x91 |

从机正常应答命令：The slave responds demands normally

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 内容  content | 从机地址  The slave address | 功能码  Function code | 寄存器起始地  址register initial address | 保存的寄存器个数the numbers of register | CRC16 |
| 长度length | 1 | 1 | 2 | 2 | 2 |
| 举例example | 0x02 | 0x10 | 0x00 0x00 | 0x00 0x01 | 0x01 0xFA |

注：对于本设备，修改0x0000地址数据即修改从机地址。

Note: For this device, modifying the 0x0000 address data means modifying the slave address.

如果数据错误或者寄存器地址无效，从机返回异常应答，格式如下

If the data is wrong or the register address is invalid, the slave returns an exception response with the following format:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 内容content | 从机地址  the slave address | 功能码function code | 错误代码error code | CRC16 |
| 长度length | 1 | 1 | 1 | 2 |
| 举例example | 0x01 | 0x90 | 0x03 | 0x0C 0x01 |

**2.4 错误代码:**（本协议提供4种错误代码）

Error code: (this agreement provides 4 error codes) below

01：功能码不存在 Function code does not exist

02：寄存器地址无效 Register address is invalid

03：数据错误 data error

04: 设备故障（电量异常时）device failure (when the energy is abnormal)

**2.5 主动上报示例Proactive reporting examples**

**01 03 1C 00 00 00 09 00 00 00 00 00 00 05 69 03 9E 00 C6 56 0C 01 AC 03 D2 13 89 00 01 00 02 AC F6**

01 //Modbus ID = 1

03 //Read Ack

1C //Len = 28

00 00 00 09 //total energy 0.09kWh

00 00 00 00 00 00 05 69 //total amount consumed 0.1385

03 9e //active power 0.926kW

00 c6 //reactive power 0.198kW

56 0c //voltage 220.28V

01 ac //current 4.28A

03 d2 //power factor 0.978

13 89 //frequency 50.01Hz

00 01 //relay status = closed

00 02 //working mode = credit prepaid

AC F6 //CRC16

**3、寄存器地址Register Address**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 地址Address | 含义  Meaning | 长度Length | R/W/C | 描述Description |
| 100/0 | 软硬件版本号  Software and hardware version | 1 | R/W | 十进制，解析为X.X.XX，写0xA55A重启升级，寄存器0也可读  Decimal, parsed as X.X.XX, write 0xA55A to restart and upgrade, register 0 can also be read |
| 101 | 通讯地址 communication address | 1 | R/W | 1-247可设can be set |
| 102 | 序列号series number | 2 | R/W | 需一起设置，暂时8位BCD码解析  Need to be set together, temporary 8-digit BCD code analysis |
| 104 | 总电量 total energy | 2 | R/C | 6+2，十进制解析，按住按钮&写0x0000A5EC清零相关电量  使用AES加密清零无需按按钮  6+2, decimal analysis, press and hold the button & write 0x0000A5EC to clear the relevant energy.  use AES encryption to clear without pressing the button |
| 106 | 剩余电量  remaining energy | 2 | R/C |
| 108 | 总金额 Total amount | 4 | R/C | 10+4，十进制解析，按住按钮&写0x000000000000A5EC清零金额  使用AES加密清零无需按按钮  10+4, decimal analysis, press and hold the button & write 0x000000000000A5EC to clear the amount.  use AES encryption to clear without pressing the button |
| 112 | 剩余金额Remaining amount | 4 | R/C |
| 116 | 当月电量the energy of this month | 2 | R/C | 单位0.01，当月电量，仅金额预付费时有效，按按钮写0x0000A5EC清零  The unit is 0.01, the current month's energy is only valid when the amount is prepaid, press the button and write 0x0000A5EC to clear it. |
| 118 | 当月金额 the amount of this month | 4 | R/C | 单位0.0001，当月金额，仅金额预付费时有效，按按钮写0x0000A5EC清零  The unit is 0.0001, the current month's amount, only valid when the amount is prepaid, press the button to write 0x0000A5EC to clear |
| 122 | 有功功率 active power | 1 | R | W |
| 123 | 无功功率reactive power | 1 | R | Var |
| 124 | 电压voltage | 1 | R | 0.01V |
| 125 | 电流current | 1 | R | 0.01A |
| 126 | 功率因数power factor | 1 | R | 0.001（部分版本带符号，故以int16处理Some versions are signed, so they are processed as int16） |
| 127 | 频率frequency | 1 | R | 0.01Hz |
| 128 | 继电器状态relay status | 1 | R | Bit0=1,closed ; bit1=1, relay failure;  For opening and closing, see register 167 |
| 129 | 工作模式working mode | 1 | R/W | 0=后付费 1=电量预付费 2=金额预付费，改需按按钮  0=Postpaid 1=Prepaid for energy 2=Prepaid for amount, you need to press the button to change |
| 130 | 时间 time | 3 | R/W | 年月日时分秒，设置需3个一起设置Month, year, day, hour, minute, second,  3 setting requires to be set together |
| 133 | RTC校准 calibration | 1 | R/W | 写00归零，写其余校准，单位0.01秒/天，读/写的同时开秒脉冲输出180秒  校准需按按钮，仅限工厂操作  Write 00 to return to zero, write the rest of the calibration, the unit is 0.01 seconds/day, read/write while turning on second pulse output for 180 seconds  Calibration requires pressing a button, factory operation only |
| 134 | 过流阀值Overcurrent threshold | 1 | R/W | 单位  unit 0.01A |
| 135 | 过流断闸恢复时间  Overcurrent trip recovery time | 1 | R/W | 单位分钟  若当前处于过流断闸期间，设置值小于当前恢复计数值，当前恢复计数值=设置值  Unit: minute  If it is currently in the overcurrent trip period and the setting value is less than the current recovery count value, the current recovery count value = the setting value |
| 136 | 工作状态&最后一步操作Working status & last step operation | 1 | R | 高字节为上次最后一次运行步骤【供调试用】 低字节为运行状态，0=配置失败 1=配置阶段 2=入网阶段 3=通讯阶段  The high byte is the last running step [for debugging]  The low byte is running status, 0=configuration failure 1=configuration stage 2=network access stage 3=communication stage |
| 137 | 信号强度 | 1 | R | 单位Unit 1% |
| 138 | 上行频率 H  Uplink frequency H | 1 | R/W | 单位Unit 0.1MHz |
| 139 | 上行频率L Uplink frequency L | 1 | 高4bit=通道数，默认8；低12bit=信道带宽，默认200KHz  High 4bit = number of channels, default 8; low 12bit = channel bandwidth, default 200KHz |
| 140 | 上上行频率 H  Uplink frequency H | 1 |  | EU868标准下行同上行，下行不可设置，预留寄存器  EU868 standard downlink is the same as uplink, downlink cannot be set, reserved register |
| 141 | 下行频率L Downlink frequency L | 1 |  |
| 142 | DEVEUI | 4 | R | 模块地址【唯一】 Module address [unique] |
| 146 | APPEUI | 4 | R/W | 默认default：FCC23DFFFE0F2DBF |
| 150 | APPKEY | 8 | R/W | 默认default：7DF1A7469DF4B288F5C319E7FA7D8181 |
| 158 | ADR功能function | 1 | R/W | 0=关闭 close 1=开启自动速率调整 Turn on automatic rate adjustment |
| 159 | 速率（ADR关时）  Rate (when ADR is off) | 1 | R/W | 0=SF12,BW125 1=SF11,BW125 2=SF10,BW125 3=SF9,BW125  4=SF8,BW125 5=SF7,BW125 6=SF7,BW250 7=FSK50 |
| 160 | 端口port | 1 | R/W | 1-254 |
| 161 | 发射功率transmitting power | 1 | R/W | 0=20dbm 1=18dbm 2=16dbm 3=14dbm 4=12dbm 5=10dbm 6=8dbm 7=6dbm |
| 162 | 数据上报间隔  Data reporting interval | 1 | R/W | 1-1440 minutes ; default 2 minutes |
| 163 | 电量透支阀值  energy overdraft threshold | 2 | R/W | 单位0.01kWh， 不大于1000000.00，需按按钮，充值后清0，余额大于0后清0  The unit is 0.01kWh, not more than 1000000.00, you need to press the button, it will be cleared to 0 after recharging, and it will be cleared to 0 after the balance is greater than 0. |
| 165 | 金额透支阀值  Amount overdraft threshold | 2 | R/W | 单位0.01Rand，不大于10000000.00，需按按钮，充值后清0，余额大于0后清0  The unit is 0.01Rand, not greater than 10000000.00. You need to press the button. It will be cleared to 0 after recharging. It will be cleared to 0 after the balance is greater than 0. |
| 167 | 断闸时间 Breaking time | 2 | R/W | 单位秒，写0合闸，写非0断闸，断电时间不计入断闸时间内  若当前处于过流断闸期间，写0会清除过流断闸计时.最大2^32=4294967296秒  The unit is seconds, write 0 to close, write non-zero to break, the power outage time is not included in the break time.  If it is currently in the overcurrent trip period, writing 0 will clear the overcurrent trip timing. Max. 2^32=4294967296 seconds |
| 169 | 阶梯方案1  Ladder plan 1 | 25 | R/W | 月1B+日1B+[阶梯n电量2B+阶梯n电价4B]\*8，n=1~8  电量单位kWh，电价单位0.0001Rand，建议电量从0开始  阶梯和电价全F为无效电量最大65534，单价最大10000.0000  Month 1B+Day 1B+[Ladder n energy 2B+Ladder n energy price 4B]\*8, n=1~8  The unit of energy is kWh, the unit of energy price is 0.0001Rand, it is recommended that the energy starts from 0  The ladder and energy price are all F, the maximum invalid energy is 65534, and the maximum unit price is 10000.0000 |
| 194 | 阶梯方案2  Ladder plan 2 | 25 | R/W |
| 219 | 阶梯方案3  Ladder plan 3 | 25 | R/W |
| 244 | 阶梯方案4  Ladder plan 4 | 25 | R/W |
| 269 | AES128操作operation | 16 | W | 见下文 see below |
| 285 | 密钥恢复出厂值  Restore key to factory value | 1 | W | 写0x00A5密钥恢复默认值，无错误应答  Write 0x00A5 key to restore default value, no error response |
| 286 | 上一个电量充值记录  Last energy recharge record | 5 | R | 年月日时分秒+充值电量\*0.01kWh  Year, month, day, hour, minute and second + recharge power\*0.01kWh |
| 291 | 上一个金额充值记录  Recharge record of the previous amount | 5 | R | 年月日时分秒+充值金额\*0.01Rand  Year, month, day, hour, minute and second + recharge amount\*0.01Rand |
| 296 | 心跳包内容掩码  Mask of the heartbeat packet | 2 | R/W | Bit17~bit0指示寄存器132~100的18个参数（非寄存器地址），设置需2个寄存器一起设置。默认0x00001FE28，即心跳包内容由前到后为总电量、总金额、有功功率、无功功率、电压、  电流、功率因数、频率、继电器状态、工作模式。Bit17~bit0 indicate the 18 parameters (non register addresses) of registers 132~100, which require both registers to be set together. The default is 0x00001FE28, which means that the content of the heartbeat packet from top to bottom includes total energy, total amount, active power, reactive power, voltage , current, power factor, frequency, relay status, operating mode. |
| 65535 | Checksum | 1 | R | 十六进制显示 Hexadecimal display |
| 注：合闸会有2秒左右的延迟 Note: There will be a delay of about 2 seconds when closing. | | | | |

**4、AES128加密操作 AES128 encryption operation**

加密段结构：Encrypted segment structure:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 操作类型  operation type | 时间戳  timestamp | 长度length | 操作内容  Operation contents | 校验  calibration |
| 长度length（Byte） | 2 | 4 | 1 | 24（实际操作内容长度为0-24）/  24 (actual operation content length is 0-24) | 1 |
| 说明explain | 见下文  see below | 相对于1970-1-1 00:00:00的秒数  /Seconds relative to 1970-1-1 00:00:00 | 实际操作内容长度/The actual operation content length | 未用到部分默认补0/  The unused parts are padded with 0 by default. | SUM8 |

注：加密段总长固定为32字节，承载该加密段的寄存器起始于269

Note: The total length of the encrypted segment is fixed at 32 bytes, and the register carrying the encrypted segment starts at 269.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AES128加密操作内容说明AES128 encryption operation content description | | | | |
|  | | | | |
| 操作类型 Operation type | 含义meaning | 长度length | 类型type | 说明Explain |
| 0x0000 | 测试testing | 0 |  | 返回正确 Return correct |
| 0x0011 | 系统工作模式  System operating mode | 1 | uint8 | H4：A=开AES加密（固定） 5=关AES加密（预留） L4：0=后付费 1=电量预付费 2=金额预付费/H4: A=AES encryption on (fixed) 5=AES encryption off (reserved) L4: 0=post-paid 1=power pre-paid 2=amount pre-paid |
| 0x0012 | 改AES密钥 Change AES key | 16 |  |  |
| 0x0013 | 继电器控制 Relay control | 4 | uint32 | 断闸时间，单位秒，即0为合闸，非0为断闸/  Breaking time, unit second, that is, 0 means closing, non-0 means breaking. |
| 0x0014 | 过流阀值 Overcurrent threshold | 4 | uint32 | 单位0.001A，电表仅保存到0.01A，上位机输入建议做到0.01A，最大655.35A/The unit is 0.001A, the meter only saves to 0.01A, the upper computer input is recommended to be 0.01A, the maximum is 655.35A |
| 0x0015 | 选择性清零/复位Selective clear/reset | 4 | uint32 | 高4位需等于0xA,低28位指示需清内容 bit7=系统复位 bit6=月电量 bit5=月金额 bit4=时间戳 bit3=总电量 bit2=总金额 bit1=剩余电量 bit0=剩余金额/  The high 4 bits need to be equal to 0xA, and the low 28 bits indicate that the content needs to be cleared.  bit7=system reset bit6=monthly energy bit5=monthly amount bit4=time stamp bit3=total energy bit2=total amount bit1=remaining energy bit0=remaining amount |
| 0x0016 | 电量充值 energy recharge | 4 | int32 | 单位0.01kWh， 有符号数，单次变化量不大于2000000.00， 变化后结果需在±1000000.00之间/Unit: 0.01kWh, signed number, single change is not greater than 2000000.00, the result after change must be between ±1000000.00 |
| 0x0017 | 金额充值 Amount recharge | 4 | int32 | 单位0.01Rand，有符号数，单次变化量不大于10000000.00，变化后结果需在±10000000000.0000000之间  /The unit is 0.01Rand, signed number, the single change amount is not greater than 10000000.00, and the result after the change must be between ±10000000000.0000000 |
| 0x0018 | 电量透支阀值Energy overdraft threshold | 4 | uint32 | 单位0.01kWh，不大于1000000.00  /Unit: 0.01kWh, no more than 1000000.00 |
| 0x0019 | 金额透支阀值 Amount overdraft threshold | 4 | uint32 | 单位0.01Rand，不大于10000000.00  /The unit is 0.01Rand, not greater than 10000000.00 |

电表保留最近32次操作的时间戳，但不区分该时间戳是何功能，服务器操作时每条新命令的时间戳需唯一且递增

The energy meter retains the timestamps of the last 32 operations, but does not distinguish the function of the timestamp. The timestamp of each new command during server operation must be unique and incrementing.