

Modbus 协议寄存器定义文档

一、协议概览

项目	配置
协议类型	Modbus RTU
从机地址	1
波特率	115200
数据位	8
校验位	无
停止位	1

二、寄存器总览

2.1 读数据区

功能	功能码	寄存器类型	起始地址	长度/范围	说明
实时显示数据-线路1	0x04	输入寄存器	0x0000	0x0000 ~ 0x0032	单精度浮点数，32bit，2寄存器/点
实时显示数据-线路2	0x04	输入寄存器	0x0034	0x0034 ~ 0x0066	参数顺序同线路1
实时显示数据-线路3	0x04	输入寄存器	0x0068	0x0068 ~ 0x009A	参数顺序同线路1
实时显示数据-线路4	0x04	输入寄存器	0x009C	0x009C ~ 0x00CE	参数顺序同线路1
AI输入	0x04	输入寄存器	0x00D0	0x00D0 ~ 0x00DE	8路 AI，单精度浮点数
B码对时	0x04	输入寄存器	0x00E0	0x00E0 ~ 0x00E2	秒/分、时/日、月/年

功能	功能码	寄存器类型	起始地址	长度/范围	说明
开入状态	0x04	输入寄存器	0x00E3	1寄存器	16路，每 bit 一路
开出状态	0x04	输入寄存器	0x00E4	1寄存器	16路，每 bit 一路
事件总寄存器	0x04	输入寄存器	0x00E5	1寄存器	内容为 n 时表示有 n 个事件待读取
自检 / 串口 / 网口状态	0x04	输入寄存器	0x00E6	1寄存器	bit15 自检状态，bit11 ~ bit8 为网口1~4状态，bit3 ~ bit0 为串口1~4状态
遥信状态	0x04	输入寄存器	0x00E7	1寄存器	bit3 频率越限，bit2 CT断线，bit1 PT断线
读事件内容	0x04	输入寄存器	0x0100	5 * n	当 0x00E5 != 0 时读取

2.2 读/写参数区

功能	功能码	寄存器类型	起始地址	寄存器长度	说明
时间设置	0x03 / 0x10	保持寄存器	0x0000	2	时间戳，32bit
串口设置	0x03 / 0x10	保持寄存器	0x0004	16	4路 × 8字节
线路定值设置	0x03 / 0x10	保持寄存器	0x0014	64	4路 × (7类定值 + 2个变比参数)
AI通道设置	0x03 / 0x10	保持寄存器	0x0054	30	12路整体下发
AO通道设置	0x03 / 0x10	保持寄存器	0x0072	30	12路整体下发
AI报警设置	0x03 / 0x10	保持寄存器	0x0090	30	12路整体下发

功能	功能码	寄存器类型	起始地址	寄存器长度	说明
读事件成功回复	0x03	保持寄存器	0x0100	1	内容为本次成功读取的事件个数 n

2.3 线圈区

功能	功能码	寄存器类型	起始地址	长度	说明
写开出（批量）	0x0F	线圈	0x0000	12	写多个线圈，控制12路开出

三、实时数据寄存器表

3.1 线路1实时量

寄存器地址	参数名	寄存器地址	参数名	寄存器地址	参数名
0x0000	Ua	0x0012	Pt	0x0024	PFa
0x0002	Ub	0x0014	Qa	0x0026	PFb
0x0004	Uc	0x0016	Qb	0x0028	PFc
0x0006	Ia	0x0018	Qc	0x002A	PFt
0x0008	Ib	0x001A	Qt	0x002C	Uab
0x000A	Ic	0x001C	Sa	0x002E	Ubc
0x000C	Pa	0x001E	Sb	0x0030	Uca
0x000E	Pb	0x0020	Sc	0x0032	Frq
0x0010	Pc	0x0022	St	-	-

3.2 线路2~线路4地址范围

线路	地址范围	说明
线路2	0x0034 ~ 0x0066	参数顺序同线路1
线路3	0x0068 ~ 0x009A	参数顺序同线路1
线路4	0x009C ~ 0x00CE	参数顺序同线路1

3.3 AI输入寄存器表

寄存器地址	输入编号
0x00D0	Ai1
0x00D2	Ai2
0x00D4	Ai3
0x00D6	Ai4
0x00D8	Ai5
0x00DA	Ai6
0x00DC	Ai7
0x00DE	Ai8

3.4 B码对时寄存器表

寄存器地址	位分配	内容
0x00E0	[15:8] = 秒, [7:0] = 分	秒/分
0x00E1	[15:8] = 时, [7:0] = 日	时/日
0x00E2	[15:8] = 月, [7:0] = 年	月/年

3.5 状态寄存器表

寄存器地址	含义	说明
0x00E3	开入状态	16路输入, 每 bit 一路
0x00E4	开出状态	16路输出, 每 bit 一路
0x00E5	事件总寄存器	值为 n 表示有 n 个事件待读取
0x00E6	自检 / 串口 / 网口状态	bit15 表示自检状态, bit11 ~ bit8 表示网口1~4状态, bit3 ~ bit0 表示串口1~4状态
0x00E7	遥信状态	bit3 频率越限, bit2 CT断线, bit1 PT断线, 其余位保留

3.6 自检 / 串口 / 网口状态寄存器

3.6.1 寄存器 0x00E6

项目	定义
寄存器类型	输入寄存器
功能码	0x04
地址	0x00E6
说明	用于监控设备开机自检、4路串口、4路网口状态

位位置	功能	含义说明
Bit15	自检状态	1 = 自检异常 / 未完成，0 = 自检正常完成
Bit11	Net4 网口状态	1 = 网口4异常 / 断开，0 = 网口4正常连接
Bit10	Net3 网口状态	1 = 网口3异常 / 断开，0 = 网口3正常连接
Bit9	Net2 网口状态	1 = 网口2异常 / 断开，0 = 网口2正常连接
Bit8	Net1 网口状态	1 = 网口1异常 / 断开，0 = 网口1正常连接
Bit3	Com4 串口状态	1 = 串口4异常 / 无数据，0 = 串口4正常
Bit2	Com3 串口状态	1 = 串口3异常 / 无数据，0 = 串口3正常
Bit1	Com2 串口状态	1 = 串口2异常 / 无数据，0 = 串口2正常
Bit0	Com1 串口状态	1 = 串口1异常 / 无数据，0 = 串口1正常
其余位	保留	未使用，读为 0

3.6.2 寄存器 0x00E7

项目	定义
寄存器类型	输入寄存器
功能码	0x04
地址	0x00E7
说明	用于反馈开机自检及运行过程中的遥信类异常状态

位位置	功能	含义说明
Bit3	频率超限	1 = 频率超出阈值，0 = 频率正常
Bit2	CT 断线	1 = CT（电流互感器）回路断线，0 = CT 回路正常

位位置	功能	含义说明
Bit1	PT 断线	1 = PT（电压互感器）回路断线，0 = PT 回路正常
其余位	保留	未使用，读为 0

3.6.3 使用场景与解读示例

- 事件总寄存器 0x00E5 用于表示当前待处理事件个数，值非 0 时表示存在待读取事件，值为 0 表示无事件。
- 状态寄存器 0x00E6、0x00E7 用于快速反馈开机自检、通信链路和遥信告警状态，便于上位机快速诊断设备健康状况。

读取 0x00E6 时，若返回值为 0x800F（二进制 1000 0000 0000 1111），表示：

- Bit15 = 1，自检异常或未完成
- Bit3 ~ Bit0 = 1111，Com1 ~ Com4 全部异常

读取 0x00E7 时，若返回值为 0x0006（二进制 0000 0000 0000 0110），表示：

- Bit3 = 0，频率正常
- Bit2 = 1，CT 断线
- Bit1 = 1，PT 断线

读取 0x00E5 ~ 0x00E7 共 3 个寄存器的 Modbus RTU 报文示例：

- 主机请求：[从站地址] 04 00 E5 00 03 [CRC16]
- 从站响应：[从站地址] 04 06 [00E5值] [00E6值] [00E7值] [CRC16]

四、事件寄存器定义

4.1 读事件内容

项目	定义
触发条件	事件总寄存器 0x00E5 != 0
功能码	0x04
寄存器类型	输入寄存器
起始地址	0x0100
读取长度	5 * n

数据名	数据寄存器	格式	说明
时间戳	0x0100 ~ 0x0101	32位无符号	事件发生时间戳
毫秒计时	0x0102	16位无符号	事件发生毫秒值

数据名	数据寄存器	格式	说明
线路号 + 事件类型	0x0103	16位无符号	高4位为线路号，低4位为事件类型
事件代码	0x0103 低8位扩展语义	8位无符号	按事件类型解释具体代码
动作值	0x0104	16位无符号	监测值或动作状态值

4.2 字段取值说明

线路号

值	含义
0	装置
1	线路1
2	线路2
3	线路3
4	线路4

事件类型

值	含义
1	保护类
2	动作类
3	报警类
4	操作类
5	AI越限类

事件代码

类别	代码定义
保护类	1 = PT断线， 2 = CT断线， 其余依次编号
报警类	1 = 过压， 2 = 过流， 3 = 频率越限 等
动作类	开入序号，表示第 n 路发生状态变化
AI越限类	AI通道号，表示第 n 通道发生越限
操作类	由主站界面操作直接生成记录

动作值

类别	含义
保护类 / 报警类	越限时的监测值
动作类	开入/开出状态，0 -> 分，非 0 -> 合

4.3 读事件成功回复

项目	定义
功能码	0x03
寄存器类型	保持寄存器
起始地址	0x0100
数据长度	1
内容	本次成功读取的事件个数 n

五、参数区寄存器说明

5.1 参数页读写规则

- 参数页在开机及切换到参数类页面时，应先发送 03H 读取参数。
- 参数发生修改后，应发送 10H 下发更新。
- 主站应在参数修改成功后生成对应“参数修改”事件，并实时显示、存盘。
- 对时功能除可在系统设置页统一下发外，也可通过上位机独立“对时设置”接口单独触发，底层仍写时间设置寄存器 0x0000。

5.2 参数区表格

参数类别	功能码	寄存器类型	起始地址	长度	说明
时间设置	0x03 / 0x10	保持寄存器	0x0000	2	时间戳，32bit
串口设置	0x03 / 0x10	保持寄存器	0x0004	16	4路 × 8字节
线路定值设置	0x03 / 0x10	保持寄存器	0x0014	64	含7类定值与2个变比参数
AI通道设置	0x03 / 0x10	保持寄存器	0x0054	30	12路整体下发
AO通道设置	0x03 / 0x10	保持寄存器	0x0072	30	12路整体下发
AI报警设置	0x03 / 0x10	保持寄存器	0x0090	30	12路整体下发
开出状态字写入	0x10	保持寄存器	0x00A6	1	16位状态字，每 bit 一路开出

参数类别	功能码	寄存器类型	起始地址	长度	说明
网口设置	0x03 / 0x10	保持寄存器	0x00AE	28	4路 × 14字节 / 2 = 28

5.2.1 时间设置 / 独立对时说明

项目	定义
寄存器类型	保持寄存器
功能码	0x03 / 0x10
起始地址	0x0000
寄存器长度	2
数据格式	32 位时间戳，低 16 位在前，高 16 位在后

说明：

- 主站可在系统设置页统一读取/下发该寄存器。
- 主站也可通过独立“对时设置”功能，单独向该寄存器写入目标时间。
- 上位机后端可额外开放独立对时接口，例如：
 - GET /api/config/time-sync
 - POST /api/config/time-sync
- 以上接口属于上位机软件封装，底层协议仍然只对应本节 0x0000 时间设置寄存器。

5.3 通讯设置

5.3.1 基本定义

项目	定义
寄存器类型	保持寄存器
功能码	0x03 / 0x10
起始地址	0x0004
寄存器长度	16
长度说明	4(路) × 4(8byte数据/2) = 16

说明：

- 对应界面中的“串口设置”区域。
- 共支持 4 路串口参数读写。
- 每一路串口参数占用 8 字节，即 4 个保持寄存器。
- 主站进入参数页面时应先使用 03H 回读当前串口参数，界面修改后再使用 10H 整组下发。

5.3.2 单路串口参数组成

单路串口参数结构对应 `com_param_t`，总长度 8 字节：

字段	类型	字节数	说明
<code>baud_rate</code>	<code>uint32_t</code>	4	波特率
<code>parity</code>	<code>uint8_t</code>	1	校验位
<code>data</code>	<code>uint8_t</code>	1	数据位
<code>stop</code>	<code>uint8_t</code>	1	停止位
<code>protocol</code>	<code>uint8_t</code>	1	通讯协议

5.3.3 寄存器分配

串口	寄存器范围	长度	说明
串口1	<code>0x0004 ~ 0x0007</code>	4	对应界面中的一组串口参数
串口2	<code>0x0008 ~ 0x000B</code>	4	对应界面中的一组串口参数
串口3	<code>0x000C ~ 0x000F</code>	4	预留/扩展串口参数
串口4	<code>0x0010 ~ 0x0013</code>	4	预留/扩展串口参数

5.3.4 界面字段对应关系

对应界面中的典型字段如下：

界面字段	协议字段
串口号	由寄存器块位置区分，不单独占用字段
波特率	<code>baud_rate</code>
校验位	<code>parity</code>
数据位	<code>data</code>
停止位	<code>stop</code>
通讯协议	<code>protocol</code>

5.4 常规配置 / 网口设置

5.4.1 基本定义

项目	定义
寄存器类型	保持寄存器
功能码	0x03 / 0x10
起始地址	0x00AE
寄存器长度	28
长度说明	(4(路) × 14byte数据) / 2 = 28

说明：

- 对应界面中的“常规配置 / 网口设置”区域。
- 共支持 4 路网口参数读写。
- 每一路网口参数占用 14 字节，即 7 个保持寄存器。
- 主站进入参数页面时应先使用 03H 回读当前网口参数，界面修改后再使用 10H 整组下发。

5.4.2 单路网口参数组成

单路网口参数结构对应 net_t，总长度 14 字节：

```
typedef struct
{
    uint8_t id[4];
    uint8_t mask[4];
    uint8_t gateway[4];
    uint8_t protocol;
    uint8_t rev;
} net_t;
```

字段	类型	字节数	说明
id	uint8_t[4]	4	IP 地址，4 个字节
mask	uint8_t[4]	4	子网掩码，4 个字节
gateway	uint8_t[4]	4	默认网关，4 个字节
protocol	uint8_t	1	通讯协议
rev	uint8_t	1	保留

5.4.3 寄存器分配

网口	寄存器范围	长度	说明
网口1	0x00AE ~ 0x00B4	7	对应界面中的一组网口参数
网口2	0x00B5 ~ 0x00BB	7	对应界面中的一组网口参数
网口3	0x00BC ~ 0x00C2	7	预留/扩展网口参数
网口4	0x00C3 ~ 0x00C9	7	预留/扩展网口参数

5.4.4 界面字段对应关系

对应界面中的典型字段如下：

界面字段	协议字段
网卡号	由寄存器块位置区分，不单独占用字段
IP地址	id[4]
子网掩码	mask[4]
默认网关	gateway[4]
通讯协议	protocol

六、开出控制说明

6.1 写保持寄存器方式

项目	定义
功能码	0x10
寄存器类型	保持寄存器
起始地址	0x00A6
长度	1
说明	16位状态字，每 bit 表示一路开出

6.2 写线圈方式

项目	定义
功能码	0x0F
寄存器类型	线圈

项目	定义
起始地址	0x0000
长度	12
说明	写多个线圈，控制12路开出

七、通讯时序说明

7.1 开机初始化时序

- 主站开机后，先通过 03H 读取参数区。
- 参数读取成功后，主站应通过 04H 读取状态寄存器 0x00E6、0x00E7，确认开机自检、串口、网口及遥信异常状态。
- 若 0x00E6.Bit15 = 1，表示设备自检异常或尚未完成；若对应串口 / 网口状态位为 1，表示对应通信接口异常。
- 若 0x00E7 中 Bit3 / Bit2 / Bit1 置位，则表示频率越限、CT断线、PT断线等遥信异常已出现。
- 若参数读取失败，或开机自检状态异常，主站生成报警事件，可归类为“开机自检（通讯链路）”异常。
- 开机自检结束后，进入周期轮询阶段。

7.2 周期轮询时序

- 主站周期发送 04H，读取实时输入寄存器。
- 收到从站 04H 应答后，更新实时数据、状态数据。
- 状态数据至少应覆盖 0x00E3 ~ 0x00E7，其中：
 - 0x00E3 表示开入状态
 - 0x00E4 表示开出状态
 - 0x00E5 表示事件总数
 - 0x00E6 表示自检 / 串口 / 网口状态
 - 0x00E7 表示遥信异常状态
- 若 0x00E5 = 0，继续下一轮周期轮询。
- 若 0x00E5 = n 且 n > 0，立即进入读事件流程。

补充说明：

- 若上位机需要在页面上动态显示设备当前时间，可额外按固定周期读取时间设置寄存器 0x0000。
- 推荐上位机软件每 1 秒轮询一次，并通过独立时间推送通道发送给前端页面。
- 推荐的软件推送通道示例：`/ws/time-sync`
- 若需快速巡检设备状态，主站可直接读取 0x00E5 ~ 0x00E7 共 3 个寄存器，以同时获得事件数量、自检 / 通信链路状态及遥信告警状态。

7.3 读事件时序

- 主站发送“读事件”指令：
 - 功能码：04H
 - 输入寄存器地址：0x0100
 - 读取长度：5 * n
- 主站收到正确应答后，解析本批事件内容。
- 主站发送“读事件成功回复”：
 - 功能码：03H
 - 保持寄存器地址：0x0100
 - 长度：1
 - 内容：本次成功读取的事件个数 n
- 从站收到回复后，应将事件总寄存器 0x00E5 中的事件个数扣减 n。
- 若扣减后 0x00E5 仍非 0，主站应继续重复读事件流程，直到 0x00E5 = 0。

7.4 事件生成与保存

- 从站负责生成并暂存：
 - 报警类事件
 - 保护类事件
 - 动作类事件
- 主站负责生成：
 - 操作类事件

主站侧操作类事件至少包括：

代码	含义
1	控制分/合
2	读定值失败
3	线路定值修改
4	AI报警参数修改
5	AI通道参数修改
6	AO通道参数修改
7	通讯参数修改
8	密码修改

统一要求：

- 从站生成的事件与主站生成的事件，均保存在主站端。
- 主站应形成历史事件记录文件。
- 历史事件应支持按分类、时间段、线路号等条件检索。

7.5 时间推送建议

为便于上位机页面显示设备当前时间，建议增加独立时间推送链路：

1. 后台服务每 1 秒读取一次时间设置寄存器 0x0000。
2. 将回读结果转换为标准时间字符串。
3. 通过独立 WebSocket 通道推送给页面。

推荐推送报文格式：

```
{
  "type": "time_sync",
  "data": {
    "time_sync": "2026-05-25 14:30:01"
  }
}
```

说明：

- 该推送属于上位机软件实现建议，不新增下位机寄存器。
- 底层时间真值仍以 0x0000 时间设置寄存器为准。