

---

**SmartGen**

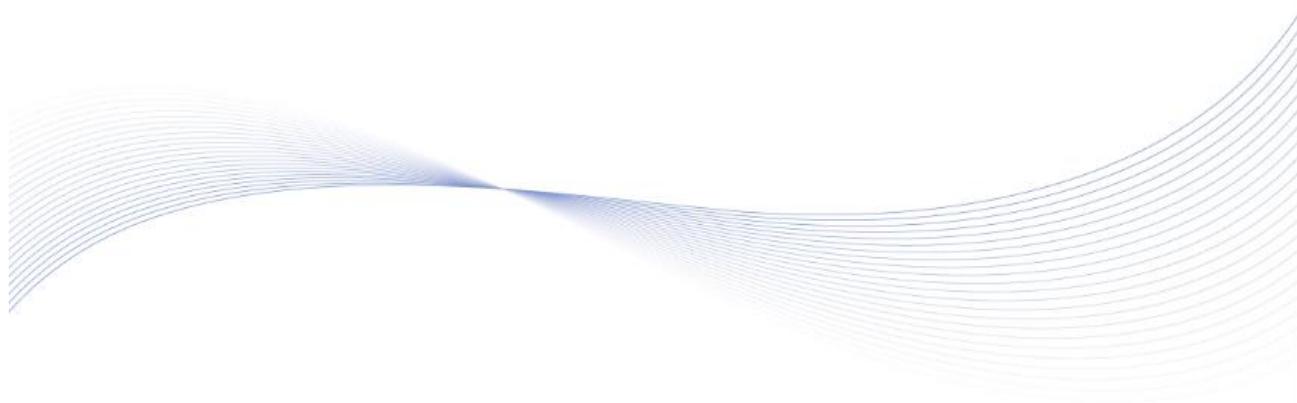
MAKING CONTROL SMARTER

**HAT360 系列**

**(HAT361/HAT361C/HAT363/HAT363C)**

**双电源自动切换控制器**

**通信协议**



郑州众智科技股份有限公司  
SMARTGEN(ZHENGZHOU)TECHNOLOGY CO.,LTD.

---

## 目 次

前 言 .....	3
1 描述 .....	4
2 接线图.....	4
3 控制器内部寄存器地址和数据 .....	5
3.1 功能码 03H 所对应的报警、状态开关量数据区.....	5
3.2 功能码 03H 所对应的数值数据区 .....	10
3.3 功能码 05H 所对应的遥控开关量区.....	12
3.4 S1 电源状态描述.....	13
3.5 S2 电源状态描述.....	13
3.6 发电机组状态描述.....	14
3.7 开关状态描述 .....	14
4 常见问题.....	15
4.1 通信线屏蔽层接地.....	15
4.2 终端电阻.....	15
4.3 RS485 转 USB 通信适配器 .....	15
4.4 通信距离延长 .....	15
4.5 通信失败常见解决办法.....	15

## 前 言

**SmartGen**是众智的注册商标

不经过本公司的允许，本文档的任何部分不能被复制（包括图片及图标）。  
本公司保留更改本文档内容的权利，而不通知用户。

公司地址：中国·河南省郑州市高新区雪梅街 28 号

电话：+86-371-67988888/67981888/67992951

+86-371-67981000（外贸）

传真：+86-371-67992952

网址：[www.smartgen.com.cn/](http://www.smartgen.com.cn/)

[www.smartgen.cn/](http://www.smartgen.cn/)

邮箱：[sales@smartgen.cn](mailto:sales@smartgen.cn)

表1 版本发展历史

日期	版本	内容
2023-11-3	V1.0	开始发布。

## 1 描述

本通信协议详细描述了本机RS485半双工串行口通信的读写命令格式及内部信息数据的定义，以便第三方开发使用。

HAT360双电源控制器有1个RS485接口。

控制器作为从机使用，采用Modbus-RTU协议，不支持Modbus-ASCII等其它协议。

通信地址：1~254（出厂默认：1）

波特率：2400/4800/9600/19200bps（出厂默认：9600bps）

起始位：1位

数据位：8位

校验位：无、奇校验、偶校验（出厂默认：无）

停止位：1或2位（出厂默认：1位）

支持的功能码：03H，05H。功能码03H用于读取控制器的报警、状态信息以及各种电量数据；功能码05H用于发送遥控命令。

数据校验方式：CRC16。

控制器内部寄存器均以“字（双字节）”为单位。

通信超时时间：大于200ms。

通信距离：9600波特率，使用带屏蔽的120欧姆双绞线的条件下最远通信距离可达1000米。

单次最大可以读取120个字寄存器的数据。

最多可以有32台控制器一起组网通信。

RS485连接时必须要求用带屏蔽层的120欧姆双绞线，要求屏蔽层单端接地。

## 2 接线图

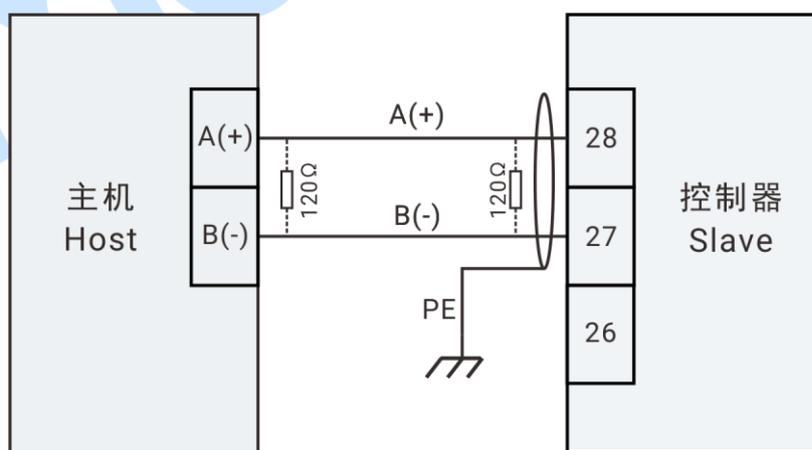


图1 单机通信接线图

注1：1个120欧姆阻抗匹配电阻可根据现场情况通过短接26/27端子接入，参见后面说明。

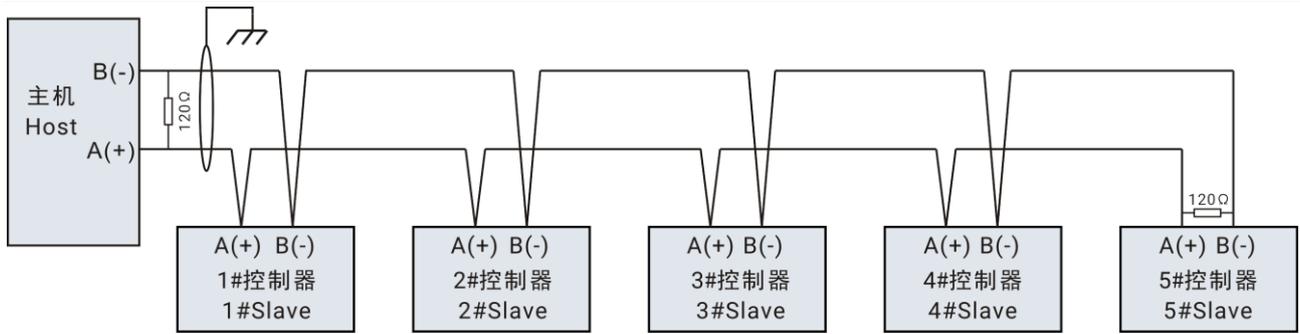


图2 多机通信接线图

注1：在组网之前请将各个控制器的通信模块地址设置好，同一个网络内禁止有相同的模块地址。

注2：通信线的屏蔽层在主机侧单端接地。

### 3 控制器内部寄存器地址和数据

在后面的表格中，S1指一路电源，S2指二路电源，表格中“/”表示此项保留。

#### 3.1 功能码 03H 所对应的报警、状态开关量数据区

表2 报警、状态开关量数据区

Modbus 地址	PLC 地址	名称	说明
500.0	40501.0	公共报警	为 0 时表示无公共报警 为 1 时表示有公共报警发生 (500.0 表示地址为 500 的第 0 位的布尔值) 以下内容依次类推
500.1	40501.1	公共警告报警	
500.2	40501.2	公共故障报警	
500.3	40501.3	LONO 输出	
500.4	40501.4	保留	
500.5	40501.5	保留	
500.6	40501.6	保留	
500.7	40501.7	保留	
500.8	40501.8	自动模式	0: 手动模式 1: 自动模式
500.9	40501.9	保留	
500.10	40501.10	S1 主用	S1 表示一路电源 为 1 表示一路电源作为常用电源 为 0 表示一路电源作为备用电源
500.11	40501.11	S2 主用	S2 表示二路电源 为 1 表示二路电源作为常用电源 为 0 表示二路电源作为备用电源
500.12	40501.12	OFF 模式	控制器退出控制
500.13	40501.13	保留	
500.14	40501.14	保留	
500.15	40501.15	发电机组开机输出	为 0 表示未输出发电机开机信号

Modbus 地址	PLC 地址	名称	说明
			为 1 表示发电机开机信号已经输出
501.0	40502.0	S1 电压正常	
501.1	40502.1	S1 电压异常	
501.2	40502.2	S1 电压瞬时异常	
501.3	40502.3	S1 电压瞬时正常	
501.4	40502.4	/	
501.5	40502.5	/	
501.6	40502.6	/	
501.7	40502.7	/	
501.8	40502.8	S1 电压无	
501.9	40502.9	S1 电压过高	
501.10	40502.10	S1 电压过低	
501.11	40502.11	S1 频率过高	
501.12	40502.12	S1 频率过低	
501.13	40502.13	S1 缺相	
501.14	40502.14	S1 逆相序	
501.15	40502.15	/	
502.0	40503.0	S2 电压正常	
502.1	40503.1	S2 电压异常	
502.2	40503.2	S2 电压瞬时异常	
502.3	40503.3	S2 电压瞬时正常	
502.4	40503.4	/	
502.5	40503.5	/	
502.6	40503.6	/	
502.7	40503.7	/	
502.8	40503.8	S2 电压无	
502.9	40503.9	S2 电压过高	
502.10	40503.1	S2 电压过低	
502.11	40503.11	S2 频率过高	
502.12	40503.12	S2 频率过低	
502.13	40503.13	S2 缺相	
502.14	40503.14	S2 逆相序	
502.15	40503.15	/	
503.0	40504.0	开关转换失败	
503.1	40504.1	S1 合闸失败	
503.2	40504.2	S1 分闸失败	
503.3	40504.3	/	
503.4	40504.4	S2 合闸失败	
503.5	40504.5	S2 分闸失败	
503.6	40504.6	/	
503.7	40504.7	/	
503.8	40504.8	/	
503.9	40504.9	/	
503.10	40504.10	强制分断故障报警	

Modbus 地址	PLC 地址	名称	说明
503.11	40504.11	/	
503.12	40504.12	/	
503.13	40504.13	开关脱扣故障报警	
503.14	40504.14	/	
503.15	40504.15	两路同时合闸故障	
504.0	40505.0	/	
504.1	40505.1	/	
504.2	40505.2	强制分断警告	
504.3	40505.3	/	
504.4	40505.4	/	
504.5	40505.5	/	
504.6	40505.6	/	
504.7	40505.7	/	
504.8	40505.8	/	
504.9	40505.9	/	
504.10	40505.10	/	
504.11	40505.11	/	
504.12	40505.12	/	
504.13	40505.13	/	
504.14	40505.14	/	
504.15	40505.15	/	
505.0	40506.0	可编程输入口 1 状态	为 0 表示输入口无输入 为 1 表示输入口有输入
505.1	40506.1	/	
505.2	40506.2	/	
505.3	40506.3	/	
505.4	40506.4	/	
505.5	40506.5	/	
505.6	40506.6	/	
505.7	40506.7	/	
505.8	40506.8	/	
505.9	40506.9	/	
505.10	40506.10	/	
505.11	40506.11	/	
505.12	40506.12	/	
505.13	40506.13	/	
505.14	40506.14	/	
505.15	40506.15	/	
506.0	40507.0	可编程输出口 1 状态	为 1 表示输出口有输出 为 0 表示输出口无输出
506.1	40507.1	/	
506.2	40507.2	/	
506.3	40507.3	/	
506.4	40507.4	/	

Modbus 地址	PLC 地址	名称	说明
506.5	40507.5	/	
506.6	40507.6	/	
506.7	40507.7	/	
506.8	40507.8	/	
506.9	40507.9	/	
506.10	40507.10	/	
506.11	40507.11	/	
506.12	40507.12	/	
506.13	40507.13	/	
506.14	40507.14	/	
506.15	40507.15	/	
507.0	40508.0	S1 合闸控制输出	
507.1	40508.1	S1 分闸控制输出	
507.2	40508.2	S2 合闸控制输出	
507.3	40508.3	S2 分闸控制输出	
507.4	40508.4	S1 开关合闸状态	
507.5	40508.5	S2 开关合闸状态	
507.6	40508.6	强制分断状态	
507.7	40508.7	/	
507.8	40508.8	/	
507.9	40508.9	/	
507.10	40508.10	/	
507.11	40508.11	/	
507.12	40508.12	远端开机带载	
507.13	40508.13	远端开机不带载	
507.14	40508.14	市电异常开机	
507.15	40508.15	/	
508.0	40509.0	/	
508.1	40509.1	/	
508.2	40509.2	/	
508.3	40509.3	/	
508.4	40509.4	/	
508.5	40509.5	/	
508.6	40509.6	/	
508.7	40509.7	/	
508.8	40509.8	/	
508.9	40509.9	/	
508.10	40509.10	开机禁止	
508.11	40509.11	/	
508.12	40509.12	S1 合闸禁止	
508.13	40509.13	S2 合闸禁止	
508.14	40509.14	/	
508.15	40509.15	/	
509.0	40510.0	/	

Modbus 地址	PLC 地址	名称	说明
509.1	40510.1	/	
509.2	40510.2	/	
509.3	40510.3	/	
509.4	40510.4	/	
509.5	40510.5	/	
509.6	40510.6	消防联动输出	
509.7	40510.7	/	
509.8	40510.8	/	
509.9	40510.9	/	
509.10	40510.10	/	
509.11	40510.11	自投自复开关量输入	
509.12	40510.12	遥控禁止开关量输入	
509.13	40510.13	/	
509.14	40510.14	/	
509.15	40510.15	/	

示例：

如果需要读取“手/自动状态及主用状态”，首先查上表得到两个开关量对应的地址为 500.8 与 500.10、500.11，可知需要读取 1 个地址的数据。

假设从机（控制器）地址为 01，主机（可以是计算机）发送指令如下表：

表3 主机（计算机）发送指令

从机地址	功能码	起始地址(500)		请求数据个数(2)		CRC 16 校验	
		高字节	低字节	高字节	低字节	低字节	高字节
01	03	01	F4	00	01	C4	04

从机应答信息如下表：

表4 从机（控制器）应答指令

从机地址	功能码	数据个数 (字节数)	数据		CRC 16 校验	
			地址 500 的数据 高字节	地址 500 的数据 低字节	低字节	高字节
01	03	02	05	00	BB	14

表5 数据分析

地址	接收的数据(十六进制)	转换为二进制数	数据含义
500	0500H	0000 0101 0000 0000 ( 分别 对应 500.15 , 500.14.....500.1, 500.0)	第 10 位数据为 1, 表示 S1 主用, 第 8 位数据为 1, 表示自动模式

## 3.2 功能码 03H 所对应的数值数据区

表6 数值数据区

Modbus 地址	PLC 地址	名称	测量范围 (十进制)	倍率	单位	说明	备注
1000	41001	UAB1 (一路 AB 线电压)	0~65000	1	V	16 位无符号数	
1001	41002	UBC1 (一路 BC 线电压)	0~65000	1	V	16 位无符号数	
1002	41003	UCA1 (一路 CA 线电压)	0~65000	1	V	16 位无符号数	
1003	41004	UA1 (一路 A 相电压)	0~65000	1	V	16 位无符号数	
1004	41005	UB1 (一路 B 相电压)	0~65000	1	V	16 位无符号数	
1005	41006	UC1 (一路 C 相电压)	0~65000	1	V	16 位无符号数	
1006	41007	UA1 相位 (一路 A 相相位)	0~360	1	°	16 位无符号数	注 3
1007	41008	UB1 相位 (一路 B 相相位)	0~360	1	°	16 位无符号数	
1008	41009	UC1 相位 (一路 C 相相位)	0~360	1	°	16 位无符号数	
1009	41010	频率 1 (一路电源频率)	0~100.0	0.1	Hz	16 位无符号数	
1010	41011	/					
1011	41012	/					
1012	41013	/					
1013	41014	/					
1014	41015	/					
1015	41016	/					
1016	41017	/					
1017	41018	/					
1018	41019	/					
1019	41020	/					
1020	41021	UAB2 (二路 AB 线电压)	0~65000	1	V	16 位无符号数	
1021	41022	UBC2 (二路 BC 线电压)	0~65000	1	V	16 位无符号数	
1022	41023	UCA2 (二路 CA 线电压)	0~65000	1	V	16 位无符号数	
1023	41024	UA2 (二路 A 相电压)	0~65000	1	V	16 位无符号数	
1024	41025	UB2 (二路 B 相电压)	0~65000	1	V	16 位无符号数	

Modbus 地址	PLC 地址	名称	测量范围 (十进制)	倍率	单位	说明	备注
1025	41026	UC2 (二路 C 相电压)	0~65000	1	V	16 位无符号数	
1026	41027	UA2 相位 (二路 A 相相位)	0~360	1	°	16 位无符号数	
1027	41028	UB2 相位 (二路 B 相相位)	0~360	1	°	16 位无符号数	
1028	41029	UC2 相位 (二路 C 相相位)	0~360	1	°	16 位无符号数	
1029	41030	频率 2 (二路电源频率)	0~100.0	0.1	Hz	16 位无符号数	
1030	41031	/					
1031	41032	/					
1032	41033	/					
1033	41034	/					
1034	41035	/					
1035	41036	/					
1036	41037	/					
1037	41038	/					
1038	41039	/					
1039	41040	/					
1040	41041	/					
1041	41042	/					
1042	41043	S1 电压状态	0~65535	序号		16 位无符号数	见 <a href="#">S1 电源状态描述</a>
1043	41044	S1 电压状态延时	0~65535	1	s	16 位无符号数	
1044	41045	S2 电压状态	0~65535	序号		16 位无符号数	见 <a href="#">S2 电源状态描述</a>
1045	41046	S2 电压状态延时	0~65535	1	s	16 位无符号数	
1046	41047	发电机组状态	0~65535	序号		16 位无符号数	见 <a href="#">发电机组电源状态描述</a>
1047	41048	发电机组状态延时	0~65535	1	s	16 位无符号数	
1048	41049	ATS 状态	0~65535	序号		16 位无符号数	见 <a href="#">开关状态描述</a>
1049	41050	ATS 状态延时	0~65535	1	s	16 位无符号数	
1050	41051	保留					
1051	41052	互为备用有效状态					
1052	41053	保留					
1053	41054	自投自复设置					

注1: 实际数值 = 接收的数据 \* 倍率。以频率举例: 接收到数据为 500(1F4H), 倍率为 0.1Hz, 则实际频率值为 50.0Hz(500\*0.1Hz);

注2: 对于 4 字节的数据, 实际的数值 = 接收数据高位 \* 65536 + 接收数据低位。

注3: 当接收的数据为 32766 时, 表示无正常数据, 可显示“###”。

注4: 有符号数定义。以接收的数据为 8000H 为例, 将其转换为二进制数为 1000 0000 0000 0000b, 最高位为 1, 是负数, 将其减 1 得到反码, 对反码取反, 得到的数即为负数的绝对值, 转换为十进制数为-32768。

示例:

读取“UAB1,UBC1”, 首先查表得到其地址为 1000, 1001, 可知需要读取 1 个字的数据。

假设从机地址为 01，主机发送指令如下表：

表7 主机发送指令

从机地址	功能码	起始地址(1000)		请求数据个数(2)		CRC 16 校验	
		高字节	低字节	高字节	低字节	低字节	高字节
01	03	03	E8	00	02	44	7B

从机应答指令如下表：

表8 从机应答指令

从机地址	功能码	数据个数(字节数)	数据				CRC 16 校验	
			地址 1000 的数据高字节	地址 1000 的数据低字节	地址 1001 的数据高字节	地址 1001 的数据低字节	低字节	高字节
01	03	04	01	7C	01	7C	3A	66

将接收到的数据填充到对应地址中，如下表。

表9 数据分析

地址	接收的数据（十六进制）
1000	017CH
1001	017CH

### 3.3 功能码 05H 所对应的遥控开关量区

表10 遥控开关量区

Modbus 地址	PLC 地址	名称	说明
15000	15001	遥控 S1 路合闸	仅发送 FF00H 有效
15001	15002	遥控 S1 路分闸	仅发送 FF00H 有效
15002	15003	遥控 S2 路合闸	仅发送 FF00H 有效
15003	15004	遥控 S2 路分闸	仅发送 FF00H 有效
15004	15005	自动/手动	手动模式：仅发送 0000H 有效 自动模式：仅发送 FF00H 有效
15005	15006	S1 主用状态设置	仅发送 FF00H 有效
15006	15007	S2 主用状态设置	仅发送 FF00H 有效
15007	15008	报警复位	仅发送 FF00H 有效
15008	15009	遥控发电机组开机	仅发送 FF00H 有效
15009	15010	遥控发电机组停机	仅发送 FF00H 有效
15010	15011	OFF	仅发送 FF00H 有效
15011	15012	/	仅发送 FF00H 有效
15012	15013	远端控制	仅发送 FF00H 有效

注：上表中遥控命令仅发送一次即可。

示例：

遥控控制器工作在自动模式，首先查表得到其遥控地址为 15004。

假设从机地址为 01，主机发送指令如下表：

表11 主机发送指令

从机地址	功能码	遥控地址(15004)		遥控数据		CRC 16 校验	
		高字节	低字节	高字节	低字节	低字节	高字节
01	05	3A	9C	FF	00	40	CC

从机应答指令如下表：

表12 从机应答指令

从机地址	功能码	遥控地址(404)		遥控数据		CRC 16 校验	
		高字节	低字节	高字节	低字节	低字节	高字节
01	05	3A	9C	FF	00	40	CC

可以通过功能码 03H 读取地址 500.8 的自动模式状态来验证遥控指令是否成功执行。

### 3.4 S1 电源状态描述

表13 S1 电源状态描述

数值 (序号)	名称	延时
0	S1 正常鉴别	有延时，单位：秒
1	S1 异常鉴别	有延时，单位：秒
2	S1 电压正常	无延时
3	S1 电压无	无延时
4	S1 电压过高	无延时
5	S1 电压过低	无延时
6	S1 频率过高	无延时
7	S1 频率过低	无延时
8	S1 缺相	无延时
9	S1 逆相序	无延时

示例：

若地址1042的内容是1，1043的内容是5，则表示目前正在进行一路电源电压异常鉴别延时，倒计时5s。

若地址1042的内容是4，则表示目前一路电源出现电压过高。

### 3.5 S2 电源状态描述

表14 S2 电源状态描述

数值 (序号)	状态	延时
0	S2 正常鉴别	有延时，单位：秒
1	S2 异常鉴别	有延时，单位：秒
2	S2 电压正常	无延时
3	S2 电压无	无延时
4	S2 电压过高	无延时
5	S2 电压过低	无延时
6	S2 频率过高	无延时
7	S2 频率过低	无延时
8	S2 缺相	无延时
9	S2 逆相序	无延时

## 3.6 发电机组状态描述

表15 发电机组状态描述

数值（序号）	状态	延时
0	开机延时	有延时，单位：秒
1	停机延时	有延时，单位：秒
2	发电机组开机	无延时
3	发电机组待机	无延时

示例：

若地址1046的内容是1，1047的内容是50，则表示发电机组正在准备停机，倒计时为50s。

若地址1046的内容是2，则表示发电机组已经开机。

## 3.7 开关状态描述

表16 开关状态描述

数值（序号）	状态	延时
0	准备转换	无延时
1	S1 正在合闸	有延时，单位：秒 s
2	S1 正在分闸	有延时，单位：秒 s
3	S2 正在合闸	有延时，单位：秒 s
4	S2 正在分闸	有延时，单位：秒 s
5	转换间隔	有延时，单位：秒 s
6	S1 再扣合闸	有延时，单位：秒 s
7	S1 再扣分闸	有延时，单位：秒 s
8	S2 再扣合闸	有延时，单位：秒 s
9	S2 再扣分闸	有延时，单位：秒 s
10	S1 带载供电	无延时
11	S2 带载供电	无延时
12	负载断开	无延时

## 4 常见问题

### 4.1 通信线屏蔽层接地

为了防止通信线上产生耦合干扰信号，需要将通信线屏蔽层单端接地。

### 4.2 终端电阻

在线型网络两端（相距最远的两个通信端口上），需要在一对通信线上并联终端120欧姆电阻。根据传输线理论，终端电阻可以吸收网络上的反射波，有效地增强信号强度。两个终端电阻并联后的值应当基本等于传输线在通信频率上的特性阻抗。

一个正规的RS-485网络通常使用终端电阻。在网络连接线非常短、临时或实验室测试时也可以不使用终端。

### 4.3 RS485 转 USB 通信适配器

可通过本公司生产的SG72A模块与PC机通信。

### 4.4 通信距离延长

通过一对本公司生产的SGCAN300光纤中继模块，实现远距离通信，最远可达10公里。



图3 SGCAN300 应用图

### 4.5 通信失败常见解决办法

- 1) 检查 RS485 正负极或网线是否正确接入，检查 RS485 转换器（若有）是否正常；
- 2) 检查终端匹配电阻是否正确接入；
- 3) 检查参数设置中的通信参数是否正确，如波特率、数据位、校验位和停止位需与控制器要求一致；
- 4) 选择 COM 的端口是否与 RS485 转换器连接到电脑的 USB 接口对应；
- 5) 控制器的通讯地址是否正确，出厂默认为：01；
- 6) 使用 03 功能码需注意每次读取数据长度最大为 120 个地址，并且读取的末尾地址不能超过最大 Modbus 通讯地址，注意 06 功能码映射的数值数据区写入功能一次只能写入一个地址的数据；
- 7) 如果 Modbus 通讯地址中有偏移地址，需要将原来基地址再加上偏移地址才是该项目的正确 Modbus 通讯地址；
- 8) 05 功能码使用 Modbus 地址通讯：虽然为 1 有效，0 无效，但是需发送 FF00H 才能使对应位为 1，发送 0000H 使对应位为 0；使用 PLC 地址通讯：发送 1 对应位置 1，发送 0 对应位置 0；
- 9) CRC-16 低字节在前，高字节在后校验是否正确；
- 10) 多次读取控制器数据频率不能过快，建议每次间隔 500ms 以上；
- 11) 在组网之前请将各个控制器的通信模块地址设置好，同一个网络内禁止有相同的模块地址；
- 12) 因为 Modbus 串口协议不支持多主站，所以不能多个软件同时与控制器通信；
- 13) 断开控制器 RS485 的连接线，测量控制器 RS485 的 A、B 端子间的电压差，如果电压差在+200mV 之间，则说明通信口有异常；
- 14) 如果通讯距离过长导致信号衰减，可以更换质量更好的电缆，或者在通讯电缆中间加中继器；
- 15) 串口通讯建议下载第三方通信软件如 modscan32，modbus poll 等验证是否能够通信正常。