

# **ATSE 控制器（Demo 板）通信协议**

## **Modbus-RTU 版**

**(Version 0.1.0)**



天津众智创新科技有限公司

## 目录

<b>1</b>	<b>协议概述 .....</b>	<b>1</b>
1.1	物理层 .....	1
1.2	数据链路层 .....	1
1.2.1	帧结构 .....	1
1.2.2	传输模式 .....	1
1.3	功能码描述 .....	2
1.3.1	功能码 0x03 .....	2
1.3.2	功能码 0x06 .....	2
1.3.3	功能码 0x10 .....	3
1.3.4	异常码 .....	3
1.3.5	功能码应用实例 .....	4
<b>2</b>	<b>应用数据定义 .....</b>	<b>5</b>
2.1	测量参数 .....	5
2.2	状态参数 .....	5
2.3	设定参数 .....	6
2.4	维护参数 .....	9
2.5	产品信息参数 .....	10

# 1 协议概述

## 1.1 物理层

物理层定义概述如下：

- (1) 通信传输方式：RS485。
- (2) 通信设备地址：1~247，默认地址为 1。
- (3) 通信波特率：2400、4800、9600 或 19200bps，默认波特率为 9600 bps。
- (4) 字节校验方式：偶校验或无校验，默认校验方式为偶校验。
- (5) 通信距离：最大 1000 米（传输介质：屏蔽双绞线）。

## 1.2 数据链路层

### 1.2.1 帧结构

本协议中，通信帧中包括四大部分：地址、功能码、数据域、差错校验（CRC）。如下表 1.2.1 所示。

表 1.2.1 帧结构

地址	功能码	数据域	差错校验
----	-----	-----	------

同时，规定帧的最大长度为 256 个字节，如下表 1.2.2 所示：

表 1.2.2 帧长度

地址	功能码	数据	CRC
1 字节	1 字节	0~252 字节	2 字节 CRC 低位 CRC 高位

在本协议中，地址域的内容为设备地址，功能码用于通知从机执行何种操作，功能码的后面是含有请求和响应参数的数据域。

从机检测到帧结束之后，执行 CRC 计算和校验。然后分析地址域来确定帧是否发往这个设备。如果不是发往这个设备，那么丢弃这个帧。

CRC 域校验整个报文的内容，不管报文有无奇偶校验，均应使用这种 CRC 校验。

CRC 域包含两个 8 位字节组成的一个 16 位值。

CRC 域作为报文的最后域附加到报文上。当进行这种附加时，首先附加域的低位字节，然后附加域的高位字节。CRC 高位字节是报文中发送的最后字节。

### 1.2.2 传输模式

- (1) 传输方式：半双工。
- (2) 校验方式：偶校验或无校验。
- (3) 传输格式：每个字节帧中包含 11 位：1 个起始位，8 个数据位（低位先发），有校验时 1 个停止位，无校验时 2 个停止位。

## 1.3 功能码描述

### 1.3.1 功能码0x03

使用该功能码从远程设备中读保持寄存器连续块的内容。请求协议帧说明了起始寄存器地址和寄存器数量。在协议帧中，从零开始寻址寄存器，因此编号为1的寄存器地址为0。将响应报文中的寄存器数据打包，每个寄存器由两个字节，第一个字节为高位字节，第二个字节为低位字节。

请求和响应的格式如下表 1.3.1.1~表 1.3.1.3 所示：

表 1.3.1.1 请求

功能码	1 字节	0x03
起始地址	2 字节	0x0000~0xFFFF
寄存器数量	2 字节	1~125 (0x007D)

表 1.3.1.2 正常响应

功能码	1 字节	0x03
字节数	1 字节	2×N <sup>*</sup>
寄存器值	N <sup>*</sup> ×2 字节	...

\* N=寄存器的数量。

表 1.3.1.3 异常响应

差错码	1 字节	0x83
异常码	1 字节	01 或 02 或 03 或 04

### 1.3.2 功能码0x06

使用该功能码在一个远程设备中写单个保持寄存器，请求协议帧指定了被写入寄存器的地址。在协议帧中，从零开始寻址寄存器，因此编号为1的寄存器地址为0。

请求和响应的格式如下表 1.3.2.1~表 1.3.2.3 所示：

表 1.3.2.1 请求

功能码	1 字节	0x06
寄存器地址	2 字节	0x0000~0xFFFF
寄存器值	2 字节	0x0000~0xFFFF

表 1.3.2.2 正常响应

功能码	1 字节	0x06
寄存器地址	2 字节	0x0000~0xFFFF
寄存器值	2 字节	0x0000~0xFFFF

表 1.3.2.3 异常响应

差错码	1 字节	0x86
异常码	1 字节	01 或 02 或 03 或 04

### 1.3.3 功能码0x10

使用该功能码在一个远程设备中写连续寄存器块（1~123 个寄存器）。在请求数据域中指定了请求写入的值。将数据按每个寄存器两个字节打包。

正常的响应应该返回功能码、起始地址和被写入的寄存器的数量。

请求和响应的格式如下表 1.3.3.1~表 1.3.3.3 所示：

表 1.3.3.1 请求

功能码	1 字节	0x10
起始地址	2 字节	0x0000~0xFFFF
寄存器数量	2 字节	0x0001~0x0078
字节计数	1 字节	2×N <sup>*</sup>
寄存器值	N <sup>*</sup> ×2 字节	值

\* N= 寄存器的数量。

表 1.3.3.2 正常响应

功能码	1 字节	0x10
起始地址	2 字节	0x0000~0xFFFF
寄存器数量	2 字节	1~123 (0x007B)

表 1.3.3.3 异常响应

差错码	1 字节	0x90
异常码	1 字节	01 或 02 或 03 或 04

### 1.3.4 异常码

本协议中的异常码定义如下表 1.3.4.1 所示：

表 1.3.4.1 Modbus 通信中的异常码

代码	名称	含义
01	非法功能	对于服务器（或从站）来说，询问中接收到的功能码是不允许的操作，这也许是因为功能码仅仅适用于新设备，而在被选单元中没有实现；同时，还可能表示服务器（或从站）在错误状态中处理这种请求，例如：因为它是未配置的，并且正在被要求返回寄存器值
02	非法数据地址	对于服务器（或从站）来说，询问中接收到的数据地址是不允许的地址；特别是，寄存器编号和传输长度的组合是无效的；对于带有 100 个寄存器的控制器来说，带有偏移量 96 和长度 4 的请求，会被成功地处理，带有偏移量 96 和长度 5 的请求将产生异常码 02
03	非法数据值	对于服务器（或从站）来说，询问数据域中包含的是不允许的值，这个值指示了组合请求中剩余结构方面的错误，例如：隐含长度是不正确的；它决不意味着寄存器中被提交存储的数据项有一个应用程序期望之外的值，因为 Modbus 协议并不知道任何特殊寄存器的任何特殊值的具体含义
04	从站设备故障或操作失败	当服务器（或从站）正在试图执行请求的操作时，产生不可恢复的差错

### 1.3.5 功能码应用实例

本节以最常见的读保持寄存器（0x03）和写单个寄存器（0x06）指令为例，描述该类指令的操作方法（本章所使用的数据均为 16 进制数，下列实例中假定设备的通信地址为 1）。

#### 1. 读保持寄存器（0x03）

假设某个参数的地址为 1000（寄存器名为 1001），要通过通信方式读取该参数，则应从上位机发送下述指令：010303E80001047A，该指令说明如表 1.3.5.1 所示：

表 1.3.5.1 读取指令

设备地址 (1 字节)	功能码 (1 字节)	起始地址 (2 字节)	寄存器数量 (2 字节)	CRC 校验值 (2 字节)
01	03	03E8	0001	047A

如果该参数为零，则返回的数据帧为：0103020000B844，该数据帧说明如下表 1.3.5.2 所示（若无返回，则表明发生了通信故障；若返回的数据帧为异常帧（5 个字节），则表明发送的指令为非法指令或指令未得到正确执行）：

表 1.3.5.2 读取指令的返回数据帧

设备地址 (1 字节)	功能码 (1 字节)	返回字节数 (1 字节)	返回值 (2 字节)	CRC 校验值 (2 字节)
01	03	02	0000	B844

#### 2. 写单个寄存器（0x06）

假设某个可修改参数的地址为 10000（寄存器名为 10001），要通过通信方式修改该参数的值（假设该参数已处于可修改的状态），要将其值修改为 100，则应从上位机发送下述指令：0106271000648350，该指令说明如表 1.3.5.3 所示：

表 1.3.5.3 参数修改指令

设备地址 (1 字节)	功能码 (1 字节)	寄存器地址 (2 字节)	寄存器值 (2 字节)	CRC 校验值 (2 字节)
01	06	2710	0064	8350

如果修改成功，则返回的数据帧为：0106271000648350，该数据帧说明如下表 1.3.5.4 所示（若无返回，则表明发生了通信故障；若返回的数据帧为异常帧（5 个字节），则表明发送的指令为非法指令或指令未得到正确执行）：

表 1.3.5.4 修改指令的返回数据帧

设备地址 (1 字节)	功能码 (1 字节)	寄存器地址 (2 字节)	寄存器值 (2 字节)	CRC 校验值 (2 字节)
01	06	2710	0064	8350

## 2 应用数据定义

### 2.1 测量参数

表 2.1.1 测量参数定义

寄存器	地址	属性	类型	系数	单位	取值范围	说明
电压测量参数							
1200	1199	R	UINT16	1	V	0~690	常用电源线电压 Uab
1201	1200	R	UINT16	1	V	0~690	常用电源线电压 Ubc
1202	1201	R	UINT16	1	V	0~690	常用电源线电压 Uca
1203	1202	R	UINT16	1	V	0~690	备用电源线电压 Uan
1204	1203	R	UINT16	1	V	0~690	备用电源线电压 Ubn
1205	1204	R	UINT16	1	V	0~690	备用电源线电压 Ucn
1206	1205	R	UINT16	1	V	0~690	常用电源线电压 Uab
1207	1206	R	UINT16	1	V	0~690	常用电源线电压 Ubc
1208	1207	R	UINT16	1	V	0~690	常用电源线电压 Uca
1209	1208	R	UINT16	1	V	0~690	备用电源线电压 Uan
1210	1209	R	UINT16	1	V	0~690	备用电源线电压 Ubn
1211	1210	R	UINT16	1	V	0~690	备用电源线电压 Ucn
1212	1211	R	UINT16	1	%	0~200	常用电源电压不平衡率
1213	1212	R	UINT16	1	%	0~200	备用电源电压不平衡率
1214	1213	R	UINT16	1	-	A,B,C 或 A,C,B	常用电源相序
1215	1214	R	UINT16	1	-	A,B,C 或 A,C,B	备用电源相序
频率测量参数							
1300	1299	R	UINT16	0.01	Hz	1500~6500	常用电源频率
1301	1300	R	UINT16	0.01	Hz	1500~6500	备用电源频率

### 2.2 状态参数

表 2.2.1 运行状态参数定义

寄存器	地址	属性	类型	系数	单位	取值范围	说明
系统运行状态							
7000	6999	R	UINT16	—	—	见表 2.2.2。	系统运行状态
7001	7000	R	UINT16	—	—	见表 2.2.3。	设备诊断状态

表 2.2.2 系统运行状态

位域	取值范围	取值定义	含义
0	0~1	0 = 主电源正常 1 = 主电源故障	主电源状态
1	0~1	0 = 备电源正常 1 = 备电源故障	备电源状态

2	0~1	0 = 主电源未接通 1 = 主电源接通	主电源合闸位置
3	0~1	0 = 备电源未接通 1 = 备电源接通	备电源合闸位置
4	0~1	0 = 不在分闸位置 1 = 在分闸位置	分闸位置
5	0~1	0 = 无消防信号 1 = 有消防信号	消防信号
6	0~1	0 = 主电源断路器未脱扣 1 = 主电源断路器已脱扣	主电源断路器脱扣信号
7	0~1	0 = 备电源断路器未脱扣 1 = 备电源断路器已脱扣	备电源断路器脱扣信号
8	0~1	0 = 主电源断路器未合闸 1 = 主电源断路器已合闸	主电源断路器合闸信号
9	0~1	0 = 备电源断路器未合闸 1 = 备电源断路器已合闸	备电源断路器合闸信号
10~15	保留	保留	保留

表 2.2.3 设备诊断状态

位域	取值范围	取值定义	含义
0	0~1	0: 存储器正常 1: 存储器发生故障	存储器状态
1	0~1	0: 动作正常 1: 系统拒动	系统拒动状态
2	0~1	0: 通信正常 1: 通信超时	通信状态
3~15	保留	保留	保留

## 2.3 设定参数

表 2.3.1 设定参数定义

寄存器	地址	属性	类型	系数	单位	取值范围	说明
锁定参数（注 1）							
9000	8999	R/W	UINT16	—	—	0: 锁定 21317: 解锁	修改锁定参数， 缺省值: 0（注 1）。
通信参数							
10000	9999	R/W	UINT16	—	—	1~247	通信地址，缺省值: 1
10001	10000	R/W	UINT16	—	—	0: 无校验 1: 偶校验 2: 奇校验	奇偶校验， 缺省值: 1
10002	10001	R/W	UINT16	—	bps	2400、4800、 9600、19200	波特率， 缺省值: 9600
10003	10002	R/W	UINT16	—	bps	1、2	停止位个数，



							缺省值: 1
通信链接超时设定参数							
10100	10099	R/W	UINT16	1	s	20~100, 步长 1s	超时设定时间
11002	11001	R/W	UINT16	—	—	0: 开启 1: 关闭	超时报警模式
过压保护参数							
11600	11599	R/W	UINT16	1	V	-5%~-30%Ue, 步长为 1V	常用电源欠压动作动作值
11601	11600	R/W	UINT16	1	V	-5%~-30%Ue, 步长为 1V	常用电源欠压动作返回值
11602	11601	R/W	UINT16	1	V	+5%~+30%Ue, 步长为 1V	常用电源过压动作动作值
11603	11602	R/W	UINT16	1	V	+5%~+30%Ue, 步长为 1V	常用电源过压动作返回值
11604	11603	R/W	UINT16	1	V	-5%~-30%Ue, 步长为 1V	备用电源欠压动作动作值
11605	11604	R/W	UINT16	1	V	-5%~-30%Ue, 步长为 1V	备用电源欠压动作返回值
11606	11605	R/W	UINT16	1	V	+5%~+30%Ue, 步长为 1V	备用电源过压动作动作值
11607	11606	R/W	UINT16	1	V	+5%~+30%Ue, 步长为 1V	备用电源过压动作返回值
11608	11607	R/W	UINT16	1	%	5%~30%, 步长为 1%	电压不平衡动作动作值
11609	11608	R/W	UINT16	1	%	5%~30%, 步长为 1%	电压不平衡动作返回值
11610	11609	R/W	UINT16	1	-	A,B,C 或 A,C,B	相序动作设定值
11611	11610	R/W	UINT16	0.01	Hz	-1%~-10%Fe, 步长为 1%	欠频动作值
11612	11611	R/W	UINT16	0.01	Hz	-1%~-10%Fe, 步长为 1%	欠频返回值
11613	11612	R/W	UINT16	0.01	Hz	+1%~+10%Fe, 步长为 1%	过频动作值
11614	11613	R/W	UINT16	0.01	Hz	+1%~+10%Fe, 步长为 1%	过频返回值
11615	11614	R/W	UINT16	0.02	s	0~30s, 步长为 0.5s	常用电源断开延时 TS
11616	11615	R/W	UINT16	0.02	s	0~60s, 步长为 0.5s	常用电源闭合延时 TCE
11617	11616	R/W	UINT16	0.02	s	0~30s, 步长为 0.5s	备用电源恢复延时 TBS
11618	11617	R/W	UINT16	0.02	s	0~60s, 步长为	备用电源闭合延时

						0.5s	TCN
11619	11618	R/W	UINT16	0.02	s	0~300s, 步长为1s	发电机停止延时 TG
11620	11619	R/W	UINT16	1	—	见表 2.3.2。	系统保护模式
<b>系统设置参数</b>							
12000	11999	R/W	UINT16	—	—	见表 2.3.3	系统接线类型
12001	12000	R/W	UINT16	—	—	见表 2.3.4	系统工作模式
<b>控制参数（注 3）</b>							
18000	17999	R/W	UINT16	—	—	见表 2.3.5。	用户控制指令

注 1:

- 1) 要通过通信方式修改任意设定参数和控制参数，必须先执行解锁设置（锁定参数本身不受此限制，本地按键操作修改参数也不受此限制）；
- 2) 解锁后，若设定参数修改完成，可通过通信设定恢复锁定设置；若未恢复，则系统会在 30 分钟后自动恢复锁定设置；
- 3) 锁定参数不保存，上电后自动恢复锁定状态；
- 4) 当保护参数具备相关的调整旋钮时，通信设定值不能大于当前旋钮对应的设定值。

注 2：当旋钮调整到关闭位置时，不能使用通信功能将其修改为报警或跳闸模式；当旋钮在打开位置时，不能使用通信功能将其修改为关闭模式（除非使用工厂命令）。

注 3：控制参数不保存，控制操作执行完成后自动回复初始状态。

表 2.3.2 系统保护模式

位域	取值范围	取值定义	含义
0	0~1	0 = 开启 1 = 关闭	欠压动作模式
1	0~1	0 = 开启 1 = 关闭	过压动作模式
2	0~1	0 = 开启 1 = 关闭	电压不平衡动作模式
3	0~1	0 = 开启 1 = 关闭	相序错误动作模式
4	0~1	0 = 开启 1 = 关闭	欠频动作模式
5	0~1	0 = 开启 1 = 关闭	过频动作模式
6	0~1	0 = 开启 1 = 关闭	缺相动作模式
7	0~1	0 = 开启 1 = 关闭	失压动作模式
8	0~1	0 = 开启 1 = 关闭	N 线接错动作模式
9~15	保留	—	—

表 2.3.3 系统接线类型

位域	取值范围	取值定义	含义
0~15	0~2	0 = 两极 1 = 三极 2 = 四极 其它值保留。	系统接线类型

表 2.3.4 系统工作模式定义

位域	取值范围	取值定义	含义
----	------	------	----

0~1	0~2	0 = 自投自复 1 = 互为备用 2 = 自投不自复（定制） 其它值保留。	返回模式
2	0~1	0 = 自动     1 = 手动	操作模式
3	0~1	0 = 电网—电网 1 = 电网—发电机	电源模式
4	0~1	0 = 两位置     1 = 三位置	位置类型
5	0~1	0 = 左主右备     1 = 右主左备	主电选择
6~15	保留	—	—

表 2.3.5 用户控制指令定义

位域	取值范围	取值定义	含义
0~15	—	0: 初始值; 17491: 恢复出厂设置; 21075: 系统状态复位; 21588: 试验脱扣。	用户控制指令

## 2.4 维护参数

表 2.4.1 产品信息参数定义

寄存器	地址	属性	类型	系数	单位	取值范围	说明
已转换次数							
20100	20099	R	UINT16	—	—	—	已发生的转换次数
故障记录参数							
21000	20999	R	UINT16	—	—	—	已发生故障总次数
21001	21000	R	UINT16	—	—	见表 2.4.2。	最后一次故障类型
21002	21001	R	UINT16	—	—	—	最后一次故障动作值
21003	21002	R	UINT16	—	—	—	最后一次故障动作时间低位
21004	21003	R	UINT16	—	—	—	最后一次故障动作时间高位
21005	21004	R	UINT16	—	—	—	最后一次故障对应的设定值

表 2.4.2 故障类型定义

位域	取值范围	取值定义	含义
0~15	0~22	0 = 无故障 1 = 主缺相 2 = 主失压 3 = 主欠压 4 = 主过压 5 = 主电压不平衡	系统故障类型

		6 = 主相序故障 7 = 主欠频 8 = 主过频 9 = 主 N 线接错 10 = 备缺相 11 = 备失压 12 = 备欠压 13 = 备过压 14 = 备电压不平衡 15 = 备相序故障 16 = 备欠频 17 = 备过频 18 = 备 N 线接错 19 = 拒动故障 20 = 存储器接错 21 = RTC 故障 22 = 通信链接超时 其它值保留。	
--	--	--	--

## 2.5 产品信息参数

表 2.5.1 产品信息参数定义

寄存器	地址	属性	类型	系数	单位	取值范围	说明
产品参数							
40000	39999	R	UINT16	—	—	见表 2.5.2。	控制器型号
40001	40000	R	UINT16	—	—	0: 2P 1: 3P 2: 4P	断路器极数
40002	40001	R	UINT16	—	—	0 = CB 级 1 = PC 级	产品类别
40003	40002	R	UINT16	V	—	—	额定电压
40004	40003	R	UINT16	—	—	0: 50Hz 1: 60Hz	频率类型
40005	40004	R	UINT16	—	—	0: OFF, 其它值为 设定次数。	故障记录次数
制造信息							
40200	40199	R	UINT16	—	—	见表 2.5.3。	软件版本号
厂商信息							
40300	40299	R	UINT16	—	—	—	厂商编号, 保留。

表 2.5.2 控制器型号

位域	取值范围	取值定义	含义
0~15	离散值	100 = CB100	—

		200 =PC100 其它值保留。	
--	--	----------------------	--

表 2.5.3 软件版本号定义

位域	取值范围	取值定义	含义
0~7	0~255	—	修改次数。
8~11	0~15	—	副版本号。
12~15	0~15	—	主版本号。

**联系方式:**

网址: <http://www.freesoar.net/>

总部地址: 天津市宝坻区霍各庄镇产业功能区东区 3 排 21 号

**联系方式:**

手机: +86-185-1188-0516

邮箱: [sales001@freesoar.net](mailto:sales001@freesoar.net)

研发中心: 北京市大兴区黄村东大街 38 号院火神庙商业中心 D 座 4 层

**联系方式 (商务):**

电话: +86-010-6926 8077

手机: +86-136-9109-9969

邮箱: [sales002@freesoar.net](mailto:sales002@freesoar.net)

**联系方式 (技术):**

手机: +86-156-0138-0811

邮箱: [fae001@freesoar.net](mailto:fae001@freesoar.net)

