

S7-TCP-IO8R-A 模块产品手册

--V1.2



东莞市艾莫迅自动化科技有限公司

Dongguan Amsamotion Automation Technology Co.,Ltd.

目录

一、产品概述.....	1
1.1、产品简介.....	1
1.2、特点功能.....	1
1.3、应用场景.....	2
二、产品规格.....	2
2.1、产品参数.....	2
2.2、端子接线.....	4
2.2.1、端子接线.....	4
2.2.2、端子功能说明：.....	5
2.2.3、COM2 口（DB9 母头）引脚定义.....	6
2.2.3、输入信号说明：.....	6
三、S7-TCP 模块使用说明.....	7
3.1、设置模块参数.....	7
3.1.1、设置网段.....	7
3.1.2、进入网页.....	7
3.1.3、模块 I/O 点地址设置.....	8
3.1.4、扩展功能.....	9
3.2、PLC 访问模块.....	10
四、端口与寄存器地址说明.....	11
4.1、S7-TCP-IO8R-A 的 TCP 链接端口功能对应表.....	11
4.2、S7-TCP-IO8R-A 的串口功能对应表.....	12
4.3、端口数据缓冲区长度说明.....	13
4.4、数字输入、输出地址.....	13
4.5、输入寄存器地址.....	13
4.6、保持寄存器地址.....	14
4.7、系统参数(上位机修改).....	14
五、产品功能.....	15
5.1、MODBUS TCP 功能.....	15
5.2、MODBUS TCP 转 MODBUS RTU 功能.....	15
5.3、MODBUS RTU 转 MODBUS TCP 功能.....	16
5.4、MODBUS RTU 功能.....	16
5.5、MODBUS TCP 控制多从站功能.....	17
5.5.1、功能说明.....	17
5.5.2、功能配置.....	17
5.5.3、功能测试.....	18
5.6、TCP 转 RS485 透传功能.....	19

5.7、按键恢复出厂设置功能..... 19

六、参数配置.....20

6.1、配置前准备..... 20

6.2、使用“艾莫迅 MODBUS 调试工具”配置..... 21

6.2.1、调试工具的连接..... 21

6.2.2、修改本机 IP..... 22

6.2.3、修改本机地址..... 23

6.2.4、修改 COM 口参数..... 24

6.2.5、修改串口模式..... 26

6.2.6、修改总线错误模式..... 26

6.3、网页配置..... 28

6.3.1、登陆模块 IP 网页..... 28

6.3.2、模块 IP 设置..... 29

6.3.3、远端服务器 IP 设置..... 30

6.3.4、COM2 口参数设置..... 31

七、MODBUS TCP 报文格式说明.....34

7.1、数字量输入信号采集命令..... 34

7.2、数字量输出信号采集命令..... 35

7.3、数字量输出信号单个控制命令..... 36

7.4、数字量输出信号多个控制命令..... 38

7.5、输入寄存器读出命令..... 39

7.6、保持寄存器读出命令..... 41

7.7、写单个保持寄存器命令..... 42

7.8、写多个保持寄存器命令..... 43

修订历史..... 1

关于我们..... 1

一、产品概述

1.1、产品简介

S7-TCP-IO8R-A 模块是一款扩展式远程分布式 IO 模块,支持通过西门子以太网的 S7TCP 协议连接 PLC;PLC (无需任何编程)可以通过对应的寄存器地址直接访问模块,支持的 PLC 有 SMART200/300/1200 等;还同时支持 MODBUS RTU 与 S7TCP 的转换,能将本模块通过 MODBUS RTU 接入的从站模块的 IO 点转为 S7TCP,PLC 可通过寄存器地址直接访问这些 IO。

本模块还支持 MODBUS TCP 服务器、MODBUS TCP 客户端、MODBUS RTU 从站、MODBUS RTU 主站、MODBUS TCP 转 MODBUS RTU、MODBUS RTU 转 MODBUS TCP 以及 TCP 转 RS485 透传等实用功能,是一款经济稳定、功能强大的产品。

1.2、特点功能

- 8 路光电隔离数字量输入,8 路继电器数字量输出(对应数量状态指示灯)
- 6 路 12 位模拟量输入,1 路 12 位模拟量输出
- 2 路 485 接口,1 路 DB9 母头,1 路端子,独立使用
- 1 路 RJ45 型网口,10/100Mbps 以太网通讯
- 带波特率、站号拨码开关,方便设置模块参数
- 支持 S7TCP 客户端协议,可直接作为西门子以太网型 PLC 的扩展模块。
- 支持 MODBUS TCP,MODBUS RTU 及 TCP 协议,同时支持 4 路 MODBUS TCP 连接
- 系统内置 MODBUS TCP 转 MODBUS RTU、MODBUS RTU 转 MODBUS TCP;可作为 MODBUS TCP 网络服务器或客户端
- 支持将最多 6 个 MODBUS RTU 从站与本模块转换为对应配置点数的 1 个 MODBUS TCP 服务器控制

- 专用上位机可设置模块参数永久保存
- 电源电路采用防反接设计
- 广泛用于工业现场设备的信号采集和控制

1.3、应用场景

S7-TCP-IO8R-A 模块的可应用范围很广，如：PLC 控制、工业自动化、楼宇自控、POS 系统、电力监控、门禁医疗、考勤系统、自助银行系统、电信机房监控、信息家电、LED 信息显示设备、测量仪表及环境动力监控系统、售饭系统等含 RS485 串口的设备或系统。

二、产品规格

2.1、产品参数

主要参数	
输入接口 (DI)	
输入点数	8 路
输入信号类型	开关触点信号或电平信号
输入信号有效范围	DC 20~28V
绝缘回路	光耦隔离
输出接口 (DO)	
输出点数	8 路
输出类型	继电器输出，常开触点
触点容量	30VDC/5A 250VAC/5A
绝缘回路	机械绝缘
模拟量输入 (AI)	
输入点数	6 路
输入类型	3 路 0~10V; 3 路 0~20ma
转换精度	12 位
模拟量输出 (AO)	
输出点数	1 路
输出类型	0~10V 或 0~20ma 可选一种，独立端子
转换精度	12 位
COM1 (RS485 通讯参数)	
接口类型	RS485，接线端子

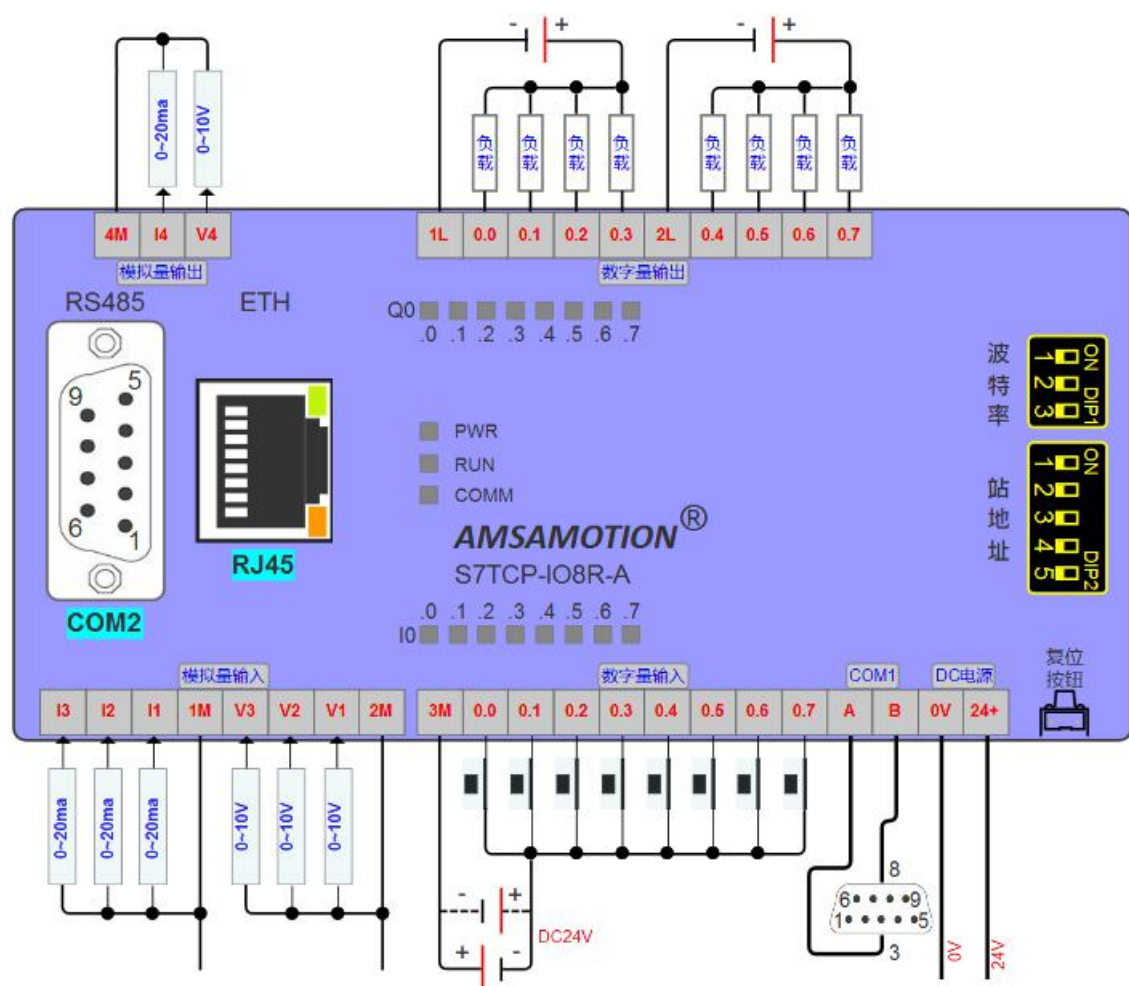
波特率	4800~115200（可配置）
通信格式	默认 8 位数据，1 位停止，无校验（可配置）

续表：

通信模式	1) MODBUS TCP 转 MODBUS RTUMODBUS RTU 2) MODBUS RTU: 针对本模块站号，功能为本模块被 MODBUS RTU 主站访问 针对其余站号，功能为 MODBUS RTU（主站）转 MODBUS TCP（服务端） 3) TCP 透传
地址范围	1~254
传输距离	1200 米
COM2（RS485 通讯参数）	
接口类型	RS485，DB9 母头：3 线（A+），8 线（B-）；5 线（地）
波特率	4800~115200（出厂时 9600，波特率拨码开关配置）
通信格式	默认 8 位数据，1 位停止，无校验（可配置）
通信模式	1) MODBUS TCP 转 MODBUS RTUMODBUS RTU 2) MODBUS RTU：仅对本模块站号，功能为本模块被 MODBUS RTU 主站访问 3) TCP 透传 4) MODBUS RTU 主站
地址范围	1~254
传输距离	1200 米
网络通讯参数	
接口形式	RJ45
网络类型	局域网
IP 地址	192.168.1.12（可配置）
通讯协议	MODBUS TCP、TCP/IP
速率	10/100Mbps；全双工；自适应
电源参数	
工作电压	DC 24V；带防反接保护
功耗	2W~4W
工作环境	
工作温度	-20℃~+70℃
存储温度	-40℃~+85℃
其他	
安装方式	导轨
尺寸	125MM(长)*80MM(宽)*50MM(高)，以实物为准

2.2、端子接线

2.2.1、端子接线

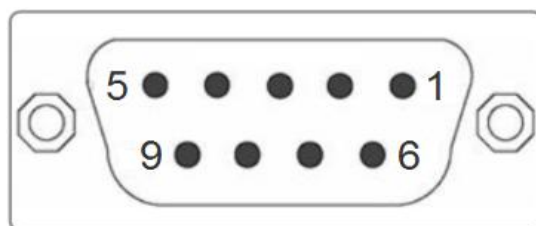


2.2.2、端子功能说明：

端子标号	功能说明
24+	DC 24V 电源正极
0V	DC 24V 电源负极
A	485 A
B	485 B
3M	第 1~8 路数字量输入通道公共端
0.0	第 1 路数字量输入
0.1	第 2 路数字量输入
0.2	第 3 路数字量输入
0.3	第 4 路数字量输入
0.4	第 5 路数字量输入
0.5	第 6 路数字量输入
0.6	第 7 路数字量输入
0.7	第 8 路数字量输入
2M	模拟量电压输入的地
V1	第 1 路模拟量电压 0~10V 输入
V2	第 2 路模拟量电压 0~10V 输入
V3	第 3 路模拟量电压 0~20ma 输入
1M	模拟量电流输入的地
I1	第 1 路模拟量电流 0~20ma 输入
I2	第 2 路模拟量电流 0~20ma 输入
I3	第 3 路模拟量电流 0~20ma 输入
4M	模拟量电压输出的地
I4	模拟量电流 0~20ma 输出
V4	模拟量电压 0~10V 输出

端子标号	功能说明
1L	第 1~4 路数字量输出通道公共端
0.0	第 1 路数字量输出
0.1	第 2 路数字量输出
0.2	第 3 路数字量输出
0.3	第 4 路数字量输出
2L	第 5~8 路数字量输出通道公共端
0.4	第 5 路数字量输出
0.5	第 6 路数字量输出
0.6	第 7 路数字量输出
0.7	第 8 路数字量输出
PWR	电源指示灯，上电常亮
RUN	系统运行指示灯，正常时慢闪
COMM	COM 口通讯指示灯，COM1 通讯时闪烁黄灯，COM2 通讯时闪烁红灯，COM 口都通讯时两种颜色交叉闪烁
COM2	DB9 母头，485 接口
ETH	10/100Mbps 网口
波特率	COM2 口波特率拨码开关
站地址	COM2 口模块站号拨码开关
复位按钮	复位模块 IP、站号、COM 口参数等

2.2.3、COM2 口（DB9 母头）引脚定义



引脚顺序	引脚作用	引脚名称
1	空	NC
2	地	GND
3	485A	A
4	空	NC
5	地	GND
6	空	NC
7	空	NC
8	485B	B
9	空	NC

2.2.3、输入信号说明：

- 输入信号支持正电/高电或负电/低电接入。
- 当输入为正电/高电有效时，公共端接电源负极，输入端子接对应的输入信号。
- 当输入为负电/低电有效时，公共端接电源正极，输入端子接对应的输入信号。

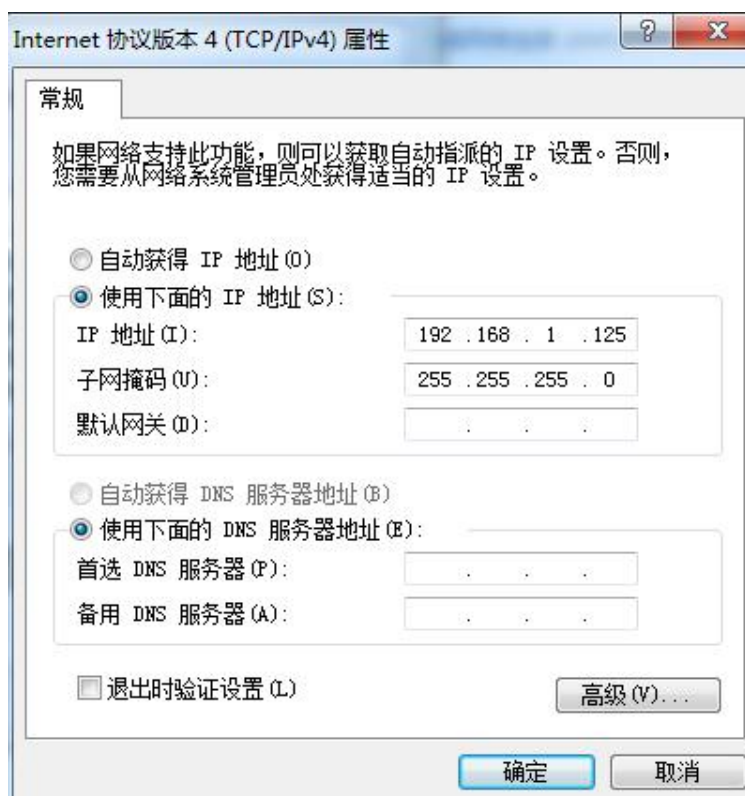
三、S7-TCP 模块使用说明

3.1、设置模块参数

3.1.1、设置网段

把电脑网卡网段改为跟模块网段一样（模块默认 IP 192.168.1.12），如何修改网段可以

百度电脑网卡如何修改网段



3.1.2、进入网页

通过网页进入 192.168.1.12,用默认帐号和密码登录



3.1.3、模块 IO 点地址设置

找到 S7 专用参数选择对应参数

- PLC 的 IP：填写 PLC 端的 IP 地址
- 西门子 PLC 类型：可以选择 S7-1200、S7-300、SMART200 (注意：S7-1500 的也选择 S7-1200 连接即可)

S7专用参数

PLC的IP:

192.168.1.128

西门子PLC类型:

S7 200 SMART

寄存器类别	寄存器地址	寄存器个数
数字输入	10	8
数字输出	11	8
模拟输入	12	6
模拟输出	14	1
连接状态	50	

保存并重启

例如：本模块有 8 开关量输入输出、6 模拟量输入、1 模拟量输出，参数填写好后点击保存并重启，重新上电

如上图填写，本模块的输入输出的映射地址分别是：

S7-1200/S7-300

- 输入:I10.0-I10.7 输出：Q11.0-Q11.7
- 模拟量输入：IW12-IW24 模拟量输出：QW14
- 与 PLC 的连接状态：IB50 (注意：如果与 PLC 通讯成功该状态字节的数据会不断跳动变化，若与 PLC 通讯失败则该字节始终为 0 ，在配置该字节时请勿与其他地址冲突。)

SMART200

- 输入:I10.0-I10.7 输出 : Q11.0-Q11.7
- 模拟量输入 : VW12-VW24 模拟量输出 : AQW14
- 与 PLC 的连接状态 : IB50 (注意 : 如果与 PLC 通讯成功该状态字节的数据会不断跳动变化 , 若与 PLC 通讯失败则该字节始终为 0 , 在配置该字节时请勿与其他地址冲突。)
-

使用注意 : PLC 写程序时直接使用对应地址即可 , PLC 端不需要写通信程序

3.1.4、扩展功能

模块自带一个 485 通信口 , 可以作为本模块的输入输出扩展用 ; 扩展的模块的 IO 点 , PLC 可以通过地址直接访问。

例如 : 在本模块 485 上接上了一个开关量 16 入 16 出的 MODBUS 模块 , 把此模块站号设置为 2 , 设置如下 , 即可扩展本模块的输入输出个数。

从 8 输入输出扩展到 24 输入输出 , 如此类推 , 最多扩展 6 个模块。

MODBUS元件参数

串口参数	115.2	8	None	1
站号	线圈元件个数	离散元件个数	只读寄存器个数	读写寄存器个数
2号站	16	16	0	0
3号站	0	0	0	0
4号站	0	0	0	0
5号站	0	0	0	0
6号站	0	0	0	0
7号站	0	0	0	0
开启主站功能	RTU主站			

S7专用参数

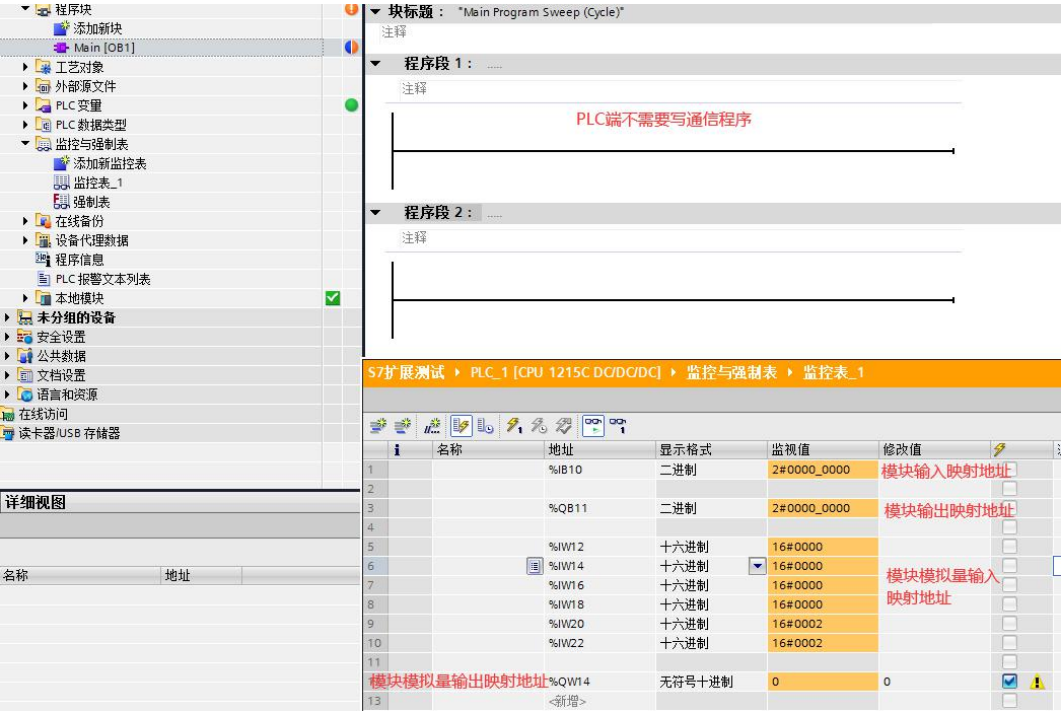
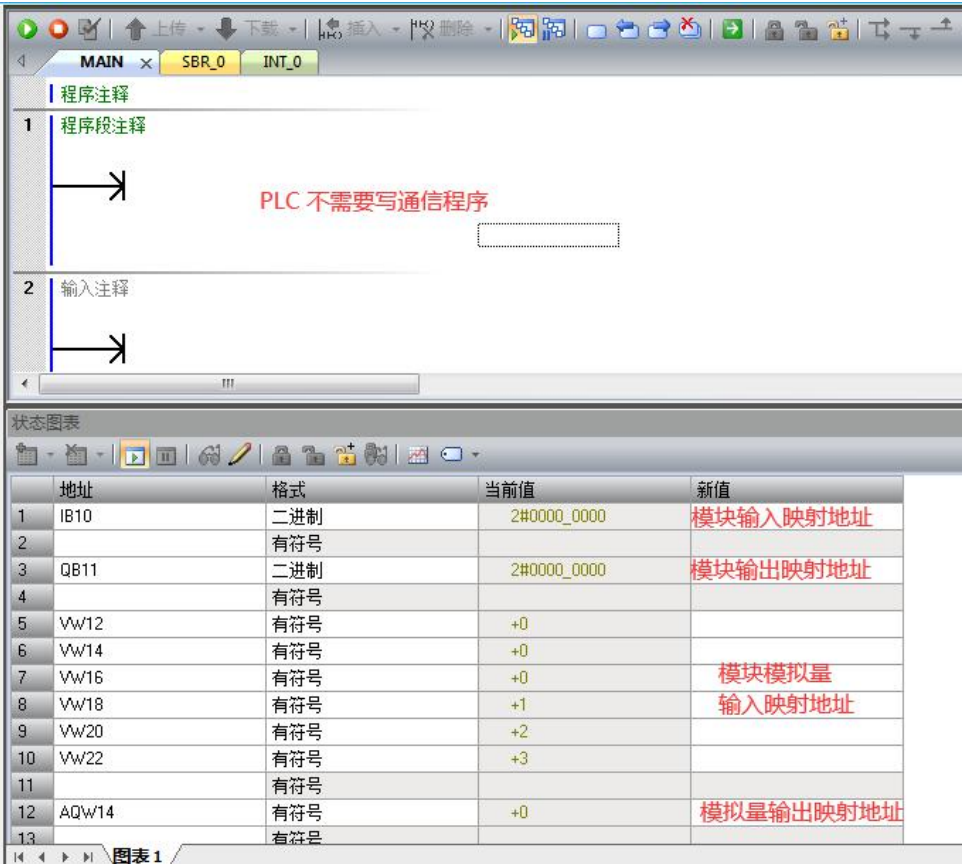
S7服务器IP: 192.168.1.222

西门子PLC类型: S7 200 SMART

寄存器类别	寄存器地址	寄存器个数
数字输入	10	24
数字输出	11	24
模拟输入	12	6
模拟输出	14	1

保存并重启

3.2、PLC 访问模块



四、端口与寄存器地址说明

4.1、S7-TCP-IO8R-A 的 TCP 链接端口功能对应表

IP 端口号	支持 功能	最大 连接 数量	详情描述
502	1、MODBUS TCP 功能 2、MODBUS TCP 转 MODBUS RTU 功能(此时对应 COM1)	1	1) 当 MODBUS TCP 报文地址=模块地址时, 对应 MODBUS TCP 功能。 2) 当 MODBUS TCP 报文地址=(2~254) 且与模块地址不冲突时, 对应 MODBUS TCP 转 MODBUS RTU 功能。 3) 该端口两路连接时支持三类连接方式: A. 两路同时对应 MODBUS TCP 功能或 MODBUS TCP 转 MODBUS RTU 功能 B. 1 路链接对应 MODBUS TCP、1 路链接对 MODBUS TCP 转 MODBUS RTU 功能 (具体由报文中从站的站号决定)。
9502	1、MODBUS TCP 功能 2、MODBUS TCP 转 MODBUS RTU 功能(此时对应 COM2) 3、TCP 透传功能(此时对应 COM2)	1	1) 当 MODBUS TCP 报文地址=模块地址时, 对应 MODBUS TCP 功能。 2) 当 MODBUS TCP 报文地址=(2~254) 且与模块地址不冲突时, 对应 COM2 口 MODBUS TCP 转 MODBUS RTU 功能。 3) 配置串口 2 为透传功能时候, 该端口的 TCP 连接实现将 TCP 数据透传给 COM2。
9503	1、MODBUS TCP 功能 2、MODBUS TCP 转 MODBUS RTU 功能(此时对应 COM2) 3、TCP 透传功能(此时对应 COM1)	1	1) 当 MODBUS TCP 报文地址=模块地址时, 对应 MODBUS TCP 功能。 2) 当 MODBUS TCP 报文地址=(2~254) 且与模块地址不冲突时, 对应 COM2 口 MODBUS TCP 转 MODBUS RTU 功能。 3) 配置串口 1 为透传功能时候, 该端口的 TCP 连接实现将 TCP 数据透传给 COM1。
5502	1、MODBUS TCP 控制多从站	1	1) 当 COM2 口模式为“MODBUS 主站”时, 可将最多 6 个 MODBUS RTU 从站与本模块, 转换为与它们网页配置的 IO、保持/输入寄存器点数对应的 1 个 MODBUS TCP 服务端控制。

4.2、S7-TCP-IO8R-A 的串口功能对应表

● 串口功能描述

端口	支持功能	最大连接数量	详情描述
COM1	1、MODBUS TCP 转 MODBUS RTU 功能 2、 1) MODBUS RTU 功能 2) MODBUS RTU 转 MODBUS TCP 功能 3、TCP 透传	2	1、上位机配置 COM1 为 TCP 转 RTU 功能时, COM1 可以连接其他 MODBUS RTU 从站; 实现以太网控制其他 MODBUS RTU 从站模块功能 (对应 TCP 连接的 502 端口)。 2、上位机配置 COM1 为 RTU 功能时: 1) 当收到站号与本模块一致, 其他 MODBUS RTU 主站可以通过 MODBUS RTU 协议访问本设备。 2) 当收到站号与本模块不一致, 其他 MODBUS RTU 主站可以通过本模块访问 MODBUS TCP 服务器设备。 3、配置 COM1 为透传功能时, COM1 与 9503 端口的 TCP 连接实现数据透传 (对应 TCP 连接的 9503 端口)。
COM2	1、MODBUS TCP 转 MODBUS RTU 功能 2、MODBUS RTU 功能 3、TCP 透传 4、MODBUS TCP 控制多从站	1	1、上位机配置 COM2 为 TCP 转 RTU 功能时, COM2 可以连接其他 MODBUS RTU 从站; 实现以太网控制其他 MODBUS RTU 从站模块功能 (对应 TCP 连接的 9502/9503 端口)。 2、上位机配置 COM2 为 RTU 功能时, 其他 MODBUS RTU 主站可以通过 MODBUS RTU 协议访问本设备。 3、配置 COM2 为透传功能时, COM2 与 9502 端口的 TCP 连接实现数据透传 (对应 TCP 连接的 9502 端口)。 4、配置 MODBUS 主站功能时, COM2 通过 5502 端口, 可将最多 6 个 MODBUS RTU 从站与本模块, 转换为与它们网页配置的 IO、保持/输入寄存器点数对应的 1 个 MODBUS TCP 服务端控制。(对应 TCP 连接 5502 端口)。

● 串口与端口号功能对应关系

端口	COM 口与 TCP 关系表				
	MODBUS RTU 从站	MODBUS 主站转 MODBUS TCP	MODBUS TCP 转 MODBUS RTU	MODBUS RTU 转 MODBUS TCP	TCP 转串口透传
COM1	支持	不支持	502	支持 (网页设置)	9503
COM2	支持	5502 端口	9502、9503	不支持	9502

4.3、端口数据缓冲区长度说明

端口	TCP 透传		MODBUS 协议下		主站功能
	接收数据 最大允许长度	接收数据 最大允许长度	接收数据 最大允许长度	接收数据 最大允许长度	从站数量
COM1	512	512	240	240	
COM2	512	512	240	240	6 路从站
TCP 连接	512	512	512	512	

4.4、数字输入、输出地址

名称	PLC 对应地址	MODBUS 对应地址	支持 功能码
输入通道 1	10001	0x00	0x02
输入通道 2	10002	0x01	0x02
输入通道 3	10003	0x02	0x02
输入通道 4	10004	0x03	0x02
输入通道 5	10005	0x04	0x02
输入通道 6	10006	0x05	0x02
输入通道 7	10007	0x06	0x02
输入通道 8	10008	0x07	0x02
输出通道 1	00001	0x00	0x01 0x05 0x0F
输出通道 2	00002	0x01	0x01 0x05 0x0F
输出通道 3	00003	0x02	0x01 0x05 0x0F
输出通道 4	00004	0x03	0x01 0x05 0x0F
输出通道 5	00005	0x04	0x01 0x05 0x0F
输出通道 6	00006	0x05	0x01 0x05 0x0F
输出通道 7	00007	0x06	0x01 0x05 0x0F
输出通道 8	00008	0x07	0x01 0x05 0x0F

4.5、输入寄存器地址

名称	PLC 对应地址	MODBUS 对应地址	支持 功能码
模拟量输入通道 1 (V1)	30001	0x00	0x04
模拟量输入通道 2 (V2)	30002	0x01	0x04
模拟量输入通道 3 (V3)	30003	0x02	0x04
模拟量输入通道 4 (I1)	30004	0x03	0x04
模拟量输入通道 5 (I2)	30005	0x04	0x04
模拟量输入通道 6 (I3)	30006	0x05	0x04

4.6、保持寄存器地址

名称	PLC 对应地址	MODBUS 对应地址(字)	默认值(十进制)	支持功能码
预留	40001~40006	0x00~0x05		0x03
模拟量输出	40007	0x06	0	0x03 0x06
预留	40008	0x07		0x03

4.7、系统参数(上位机修改)

名称	MODBUS 对应地址 (字)	默认值 (十进制)
预留	0x00	100
预留	0x01	1
本机地址配置	0x02	1
COM1 通信参数配置	0x03	9600, 1, 8, NONE
帧结束时间	0x04	0
离散输入显示模式切换	0x05	0
预留	0x06	0
预留	0x07	0
总线模式	0x08	401
本机 IP 段 1	0x09	192. 168
本机 IP 段 2	0x0A	1. 12
本机 MAC1	0x0B	255. 255
本机 MAC2	0x0C	255. 255
本机 MAC3	0x0D	255. 255
COM2 通信参数	0x0E	9600, 1, 8, NONE
各串口模式配置	0x10	0

 注意：修改保持寄存器参数后应将模块断电重启

五、产品功能

5.1、MODBUS TCP 功能

MODBUS TCP 报文地址为模块地址时，将对本模块进行访问，即 MODBUS TCP 功能。

MODBUS TCP 功能参数		
类别	参数详情	说明
TCP 服务器 IP	192.168.1.12	该 IP 为默认值，参考章节 5.2.2 或 5.3.2 设置其他 IP
TCP 服务器端口	502、9502、9503	固定端口
模块地址	1~126	出厂模块站号 1，可设置范围 1~126，参考章节 5.2.3

5.2、MODBUS TCP 转 MODBUS RTU 功能

直接将 MODBUS TCP 的请求转换为 MODBUS RTU 请求，并通过 RS485 口发送给从站；

然后将对应的从站应答数据转换为 MODBUS TCP 报文发送给上位机，相关参数见下表。

MODBUS TCP 转 MODBUS RTU 功能参数			
类别	参数详情		说明
	COM1	COM2	
TCP 服务器 IP	192.168.1.12		该 IP 为默认值，参考章节 5.2.2 或 5.3.2 设置其他 IP
TCP 服务器端口	502	9502、9503	固定端口，其中 502 端口可最多支持 2 路上位机链接
串口模式	TCP 转 RTU		出厂默认模式，可通过章节 4.7 或章节 5.2.5 设置
MODBUS RTU 从站地址	2~254		连接到本机的 RS485 口的 MODBUS 从机地址必须在 2~254 范围内，且不与本模块地址冲突
RS485 串口参数	默认参数： 波特率：9600，8 位数据， 无校验，1 位停止位		参考章节 5.2.4 或 5.3.4 设置其他串口参数

5.3、MODBUS RTU 转 MODBUS TCP 功能

本模块 COM1 口支持将 MODBUS RTU 报文转换为 MODBUS TCP 报文，实现 MODBUS RTU 主站与 MODBUS TCP 服务器间的数据转换。当 COM1 口为“RTU”模式时，模块自动启动 MODBUS TCP 客户端功能，自动连接通过网页设置的远程 MODBUS TCP 服务器。相关参数说明见下表：

MODBUS RTU 转 MODBUS TCP 功能参数		
类别	参数详情	说明
	COM1	
远端服务器 IP	192.168.1.124	该 IP 与端口为出厂默认参数，参考章节 5.3.3 设置其他远程服务器 IP 与端口
远端服务器端口	8080	
串口模式	RTU	参考章节 5.2.5 设置串口模式为 RTU
RS485 串口参数	默认参数： 波特率：9600，8 位数据， 无校验，1 位停止位	参考章节 5.2.4 设置其他串口参数

5.4、MODBUS RTU 功能

本模块 COM1 口和 COM2 口都支持 MODBUS RTU 功能。当 COM1 或 COM2 口为“RTU”模式时，本模块可作为 MODBUS RTU 从站设备使用。相关参数说明见下表：

MODBUS RTU 功能参数		
类别	参数详情	说明
MODBUS RTU 从站地址	1~126	1) 本模块站号可参考章节 5.2.3 设置 2) 当 COM1 口收到站号与本模块一致时，则当作 MODBUS RTU 报文处理；反之，则将 MODBUS RTU 报文转为 MODBUS TCP 处理，即章节 4.3 所述功能。
串口模式	RTU	参考章节 5.2.5 设置串口模式为 RTU
RS485 串口参数	默认参数： 波特率：9600，8 位数据， 无校验，1 位停止位	参考章节 5.2.4 设置其他串口参数

5.5、MODBUS TCP 控制多从站功能

5.5.1、功能说明

本模块的 COM2 口支持 MODBUS RTU 主站功能，本功能用于将连接在 COM2 口的至多 6 个 MODBUS RTU 从站及本模块的 IO 点数转换为 1 个 MODBUS TCP 服务端，通过 1 个 MODBUS TCP 连接即可实现全部从站的读写处理。

按原站号大小关系，自动映射为 MODBUS TCP 对应的寄存器区域，模块寄存器地址最前（模块地址为 2~7 与 RTU 站号“冲突”时，仍保持在前），其余低站号寄存器地址在前。

MODBUS RTU 主站功能参数		
类别	参数详情	说明
串口编号	COM2	
TCP 服务器 IP	192.168.1.12	该 IP 为默认值，参考章节 5.2.2 或 5.3.2 设置其他 IP
TCP 服务器端口	5502	固定端口
模块地址	1~126	出厂模块站号 1，可设置范围 1~126，参考章节 5.2.3
其余 MODBUS RTU 从站地址	2~7	MODBUS RTU 从站站号必须为 2~7 号
MODBUS RTU 从站最大数量	6	本模块为 MODBUS TCP 服务端
串口模式	MODBUS 主站	参考章节“5.3.4-开启主站模式”设置
COM2 串口参数	默认参数： 波特率：9600，8 位数据， 无校验，1 位停止位	COM2 串口参数修改参考章节 5.2.4， 所有从站串口参数应一致

5.5.2、功能配置

将 COM2 模式设为 MODBUS RTU 主站（参考章节“5.3.4-开启主站模式”），并在网页配置对应从站的点数后（参考章节 5.3.4-MODBUS TCP 控制多从站通讯配置），模块的 COM2 就自动启动 MODBUS RTU 主站定时扫描。

5.5.3、功能测试

将各串口参数一致的 MODBUS RTU 从站以手拉手总线正确连接至模块的 COM2 口后，可使用艾莫迅针对该功能提供的专用测试工具“AMX_ModbusTCP 测试工具”（版本 V1.0），按下列步骤进行测试：

- 填写模块地址，本模块出厂默认 IP 为 192.168.1.12
- 填写端口号 5502（默认，其他功能连接时可更改）
- 填写数字输出个数、数字输入个数、只读寄存器个数、保持寄存器个数（根据模块 IP 网页配置的 6 个 RTU 从站总点数，参考章节 5.3.4-MODBUS TCP 控制多从站通讯配置）
- 填写模块地址（1~126），出厂时本模块地址为 1
- 点击设置按钮
- 点击启动第 2 路 MODBUS TCP 按钮（连接后按钮颜色变为红色）
- 检查数字输入、线圈、输入寄存器、保持寄存器 4 个区域状态数值，是否与从站对应



注意：

- ☞ 选择第一路 MODBUS TCP 连接测试也可，但注意端口号需修改为 5502
- ☞ 两路 MODBUS TCP 连接均设置时，个数将相加，第 2 路连接的地址在前
- ☞ 本模块的保持寄存器不支持 5502 端口读取或写入

5.6、TCP 转 RS485 透传功能

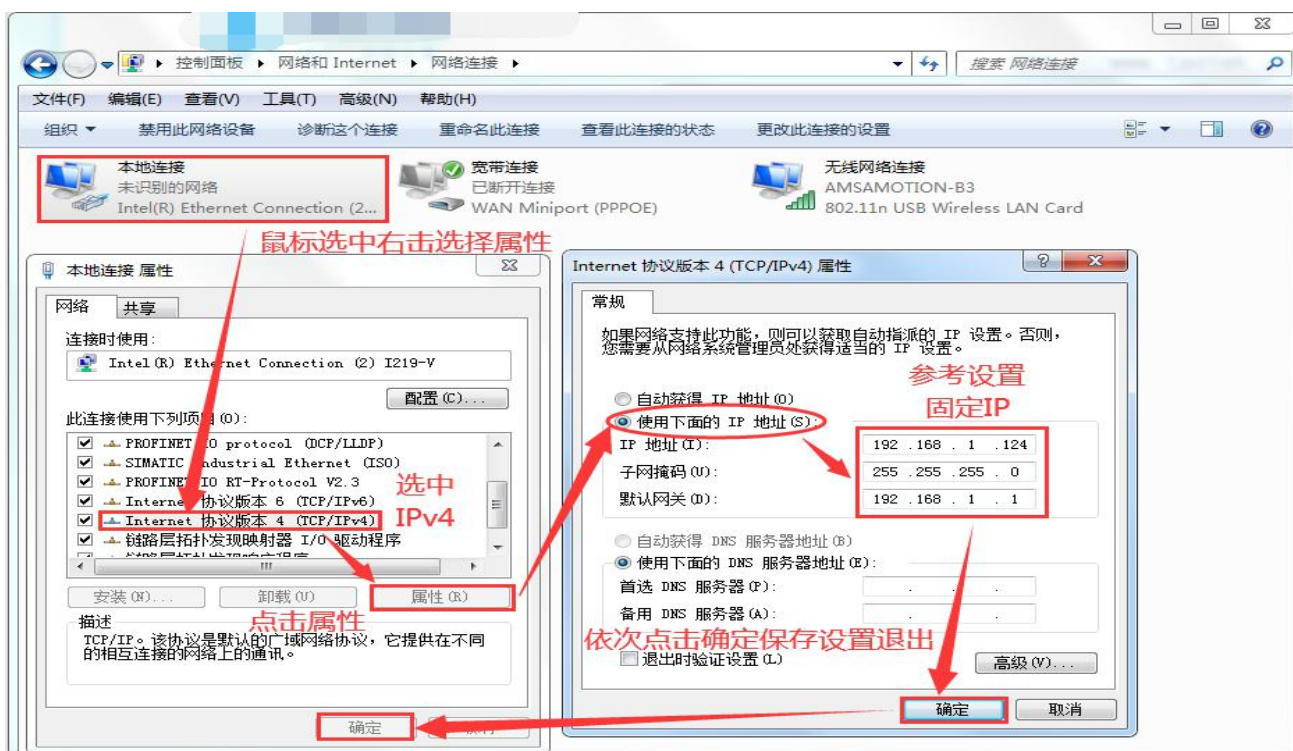
本模块 COM1 口和 COM2 口都支持 TCP 透传功能。当 COM1 或 COM2 口为“TCP 透传”模式时，TCP 客户端数据将原样发送给连接模块的 RS485 设备。相关参数说明见下表：

TCP 转 RS485 功能参数			
类别	参数详情		说明
	COM1	COM2	
TCP 服务器 IP	192.168.1.12		该 IP 为默认值，参考章节 5.2.2 或 5.3.2 设置其他 IP
TCP 服务器端口	9503	9502	固定
串口模式	TCP 透传		参考章节 5.2.5 设置串口模式为 TCP 透传
RS485 串口参数	默认参数： 波特率：9600，8 位数据， 无校验，1 位停止位		参考章节 5.2.4 设置其他串口参数

5.7、按键恢复出厂设置功能

在模块上电且 RUN 灯闪烁时，按住复位按钮（大约 5S）直到 RUN 灯变常亮后松开按钮，RUN 灯常亮 5S 后恢复闪烁，再将模块断电至少 3S 后上电，模块即恢复出厂参数，如下表。

参数名称	参数默认值
模块 IP 地址	192.168.1.12
模块地址	出厂时为 1，使用后为 DIP2 拨码开关对应 1~32 站号，参考章节 5.2.3
串口通讯参数	波特率 9600，8 位数据位，1 位停止位，无校验； 其中 COM2 口波特率出厂时为 9600，使用后为 DIP1 拨码开关对应波特率，参考“章节 6.2.4-COM2 波特率设置”
串口模式	COM1、COM2 串口模式均为 MODBUS TCP 转 MODBUS RTU
总线错误模式	模式为总线错误复位，判定总线错误时间阈值为 2s
远程服务器 IP	地址：192.168.1.124，端口：8080
MODBUS TCP 控制 多从站通讯配置	模块 IP 网页上“1 号站~6 号站”的线圈元件、离散元件、只读寄存器、读写寄存器的个数均为 0



情况 2：已更改过模块 IP：

A. 用户记得模块 IP 时，请参考情况 1 中 B 操作内容，设置电脑 IP 与模块同一网段；

B. 用户忘记模块 IP 时，按章节 4.7 内容复位模块 IP，然后参考情况 1 内容处理。

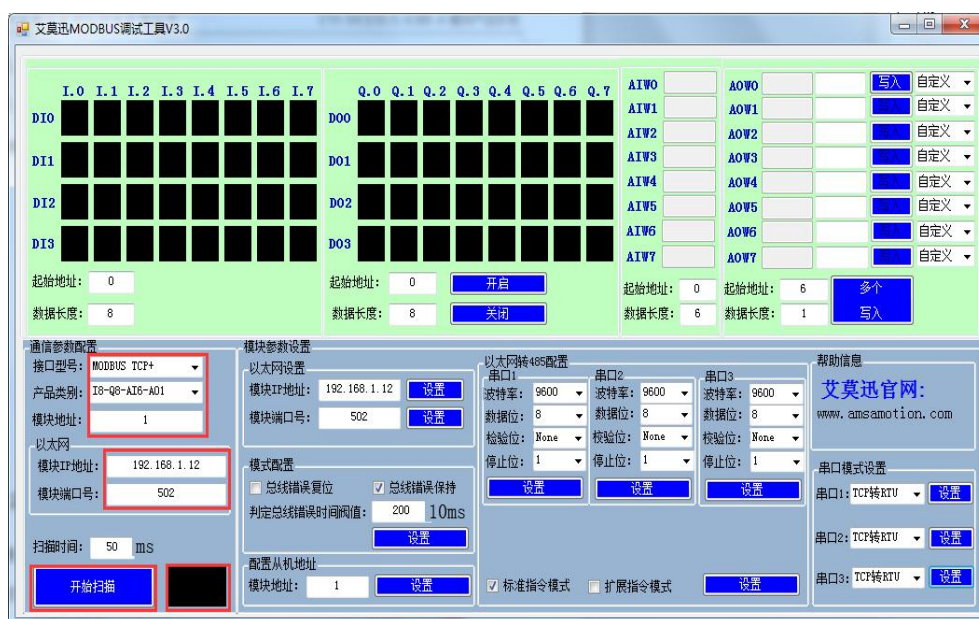
6.2、使用“艾莫迅 MODBUS 调试工具”配置

6.2.1、调试工具的连接

艾莫迅 MODBUS 调试工具（版本 V3.0）的使用（配置或调试功能）与其他上位机一样，需要建立上位机与模块的通讯，请按照以下步骤进行配置工具的连接：

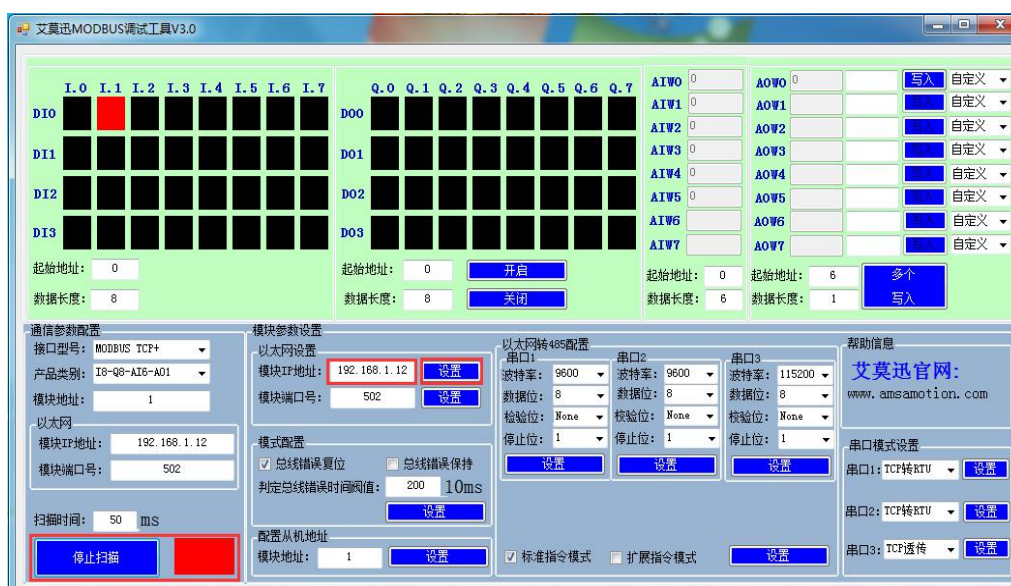
- 打开配置工具，在“接口型号”栏选择“MODBUS TCP+”
- 选择对应的产品类别（主机型号），本主机为 I8-Q8-AI6-AO1
- 填写模块地址（1~126），出厂时本模块地址为 1
- 填写模块 IP 地址，本模块出厂默认 IP 为 192.168.1.12
- 填写端口号 502（**连接 9502、9503 端口不可用于配置模块参数**）

F. 点击开始扫描按钮，成功连接后按钮文字变为停止扫描，其右边通讯状态图标颜色将由黑色变为红色



6.2.2、修改本机 IP

在“以太网设置”区域填写所需模块 IP 地址后，点击同一水平线位置的“设置”按钮，RUN 灯常亮 5S 后恢复闪烁，再将模块断电至少 3S 后上电，新设置 IP 即生效。



⚠注意：不支持修改模块端口号

6.2.3、修改本机地址

➤ 设置 1~32 站号

修改站号的范围在 1~32，必须通过调整模块上“站地址”拨码开关的状态设置，注意当模块上电时调整拨码状态时，需将模块断电至少 3S，再上电方可生效。具体对应关系如下表中所示（出厂时所有拨码为 OFF）。

站地址拨码对应ETH-MODBUS模块站号表

1、拨码开关打到数字一边为关
2、拨码开关打到ON一边为开

关

开

站地址

1

2

3

4

5

ON

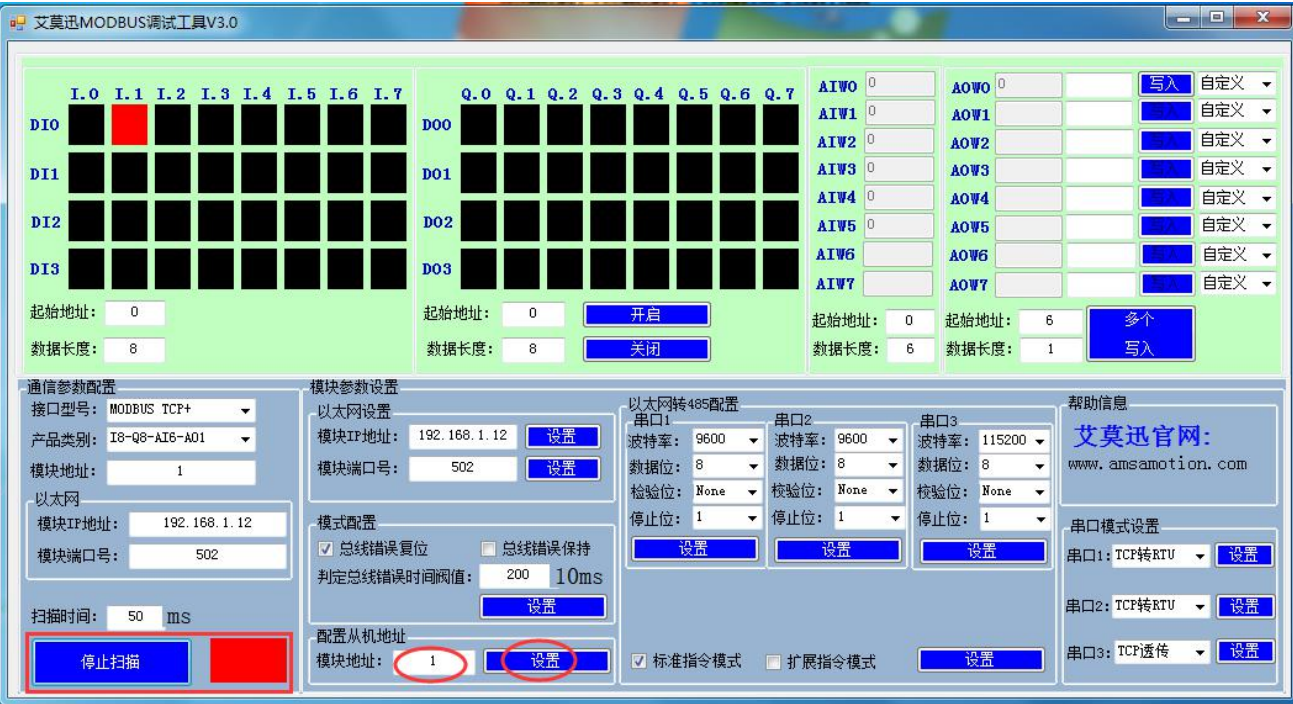
DIP2

1号开关状态	2号开关状态	3号开关状态	4号开关状态	5号开关状态	站号
OFF	OFF	OFF	OFF	OFF	1
ON	OFF	OFF	OFF	OFF	2
OFF	ON	OFF	OFF	OFF	3
ON	ON	OFF	OFF	OFF	4
OFF	OFF	ON	OFF	OFF	5
ON	OFF	ON	OFF	OFF	6
OFF	ON	ON	OFF	OFF	7
ON	ON	ON	OFF	OFF	8
OFF	OFF	OFF	ON	OFF	9
ON	OFF	OFF	ON	OFF	10
OFF	ON	OFF	ON	OFF	11
ON	ON	OFF	ON	OFF	12
OFF	OFF	ON	ON	OFF	13
ON	OFF	ON	ON	OFF	14
OFF	ON	ON	ON	OFF	15
ON	ON	ON	ON	OFF	16
OFF	OFF	OFF	OFF	ON	17
ON	OFF	OFF	OFF	ON	18
OFF	ON	OFF	OFF	ON	19
ON	ON	OFF	OFF	ON	20
OFF	OFF	ON	OFF	ON	21
ON	OFF	ON	OFF	ON	22
OFF	ON	ON	OFF	ON	23
ON	ON	ON	OFF	ON	24
OFF	OFF	OFF	ON	ON	25
ON	OFF	OFF	ON	ON	26
OFF	ON	OFF	ON	ON	27
ON	ON	OFF	ON	ON	28
OFF	OFF	ON	ON	ON	29
ON	OFF	ON	ON	ON	30
OFF	ON	ON	ON	ON	31
ON	ON	ON	ON	ON	32

➤ 设置 33~126 站号

本模块可设置的最高站号为 126，当“站地址”拨码开关的所有状态为 ON 时（即设置前模块站号为 32），方可通过调试工具给模块设置 33~126 之间的站号。

如下图所示，在“配置从机地址”区域填写所需设置的模块地址后，点击右方同一水平线位置的“设置”按钮，再将模块断电至少 3S 后上电，新设置模块地址即生效。



6.2.4、修改 COM 口参数

➤ COM 口的通讯参数说明

串口编号	COM 口通讯参数类型			
	波特率	数据位	停止位	校验位
COM1	4800~115200 仅支持上位机设置	8 或 7 位 (仅 TCP 透传可设置 7 位)	1/1.5/2	None/Odd/Even (7 位数据位时，不支持 None)
COM2	4800~115200 仅支持拨码开关设置	8 或 7 位 (仅 TCP 透传可设置 7 位)	1/1.5/2	None/Odd/Even (7 位数据位时，不支持 None)

➤ COM2 的波特率设置

COM2 的波特率由模块上的“波特率” 拨码开关状态决定，注意当模块上电时调整拨码状态时，需将模块断电至少 3S，再上电方可生效。具体关系可见下表（出厂时所有拨码为 OFF）。

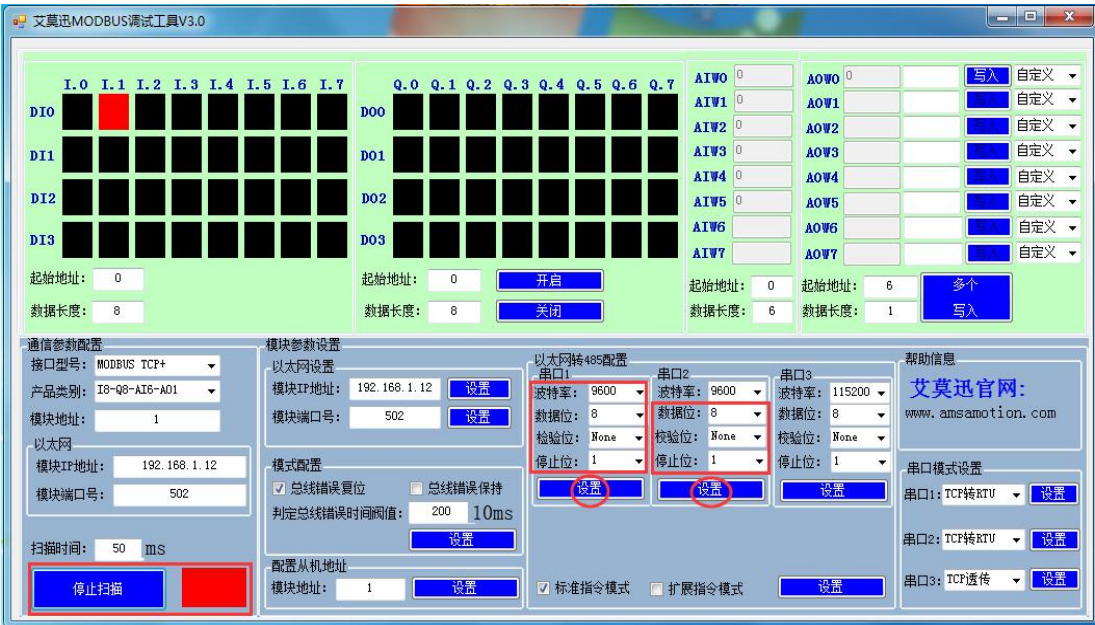
波特率拨码对应COM2波特率对应表



1号开关状态	2号开关状态	3号开关状态	波特率
OFF	OFF	OFF	9600
ON	OFF	OFF	19200
OFF	ON	OFF	38400
ON	ON	OFF	57600
OFF	OFF	ON	115200
ON	OFF	ON	9600
OFF	ON	ON	9600
ON	ON	ON	4800

➤ COM 口参数设置说明（除 COM2 波特率外）

如下图所示，在“以太网转 485 配置” 区域，从下拉清单中选择对应串口的通讯参数后（串口 1 即 COM1 口、串口 2 即 COM2 口），点击右方同一垂直线位置的“设置” 按钮，RUN 灯常亮 5S 后恢复闪烁，再将模块断电至少 3S 后上电，新设置串口参数即生效。



⚠注意：

- ☞设置数据位 7 需要串口模式为 TCP 透传时（串口模式设置见章节 5.2.5）
- ☞设置数据位 7 时，校验位不支持无校验（None）

6.2.5、修改串口模式

如下图所示，在“串口模式设置”区域，从下拉清单中选择对应串口的模式后（串口 1 即 COM1 口、串口 2 即 COM2 口），点击下方同一水平线位置的“设置”按钮，RUN 灯常亮 5S 后恢复闪烁，再将模块断电至少 3S 后上电，新设置串口模式即生效。



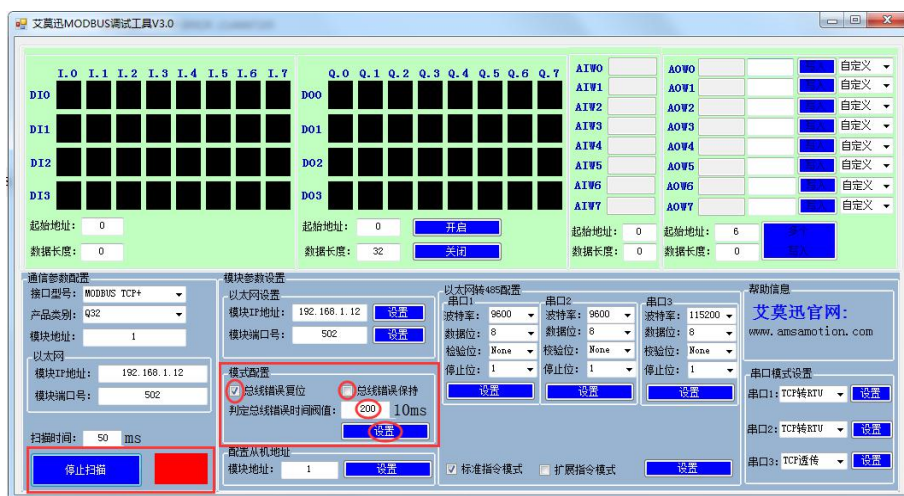
注意：对于 MODBUS 主站模式，串口 1 暂不支持，串口 2 需在网页设置。

6.2.6、修改总线错误模式

总线错误的判断功能主要用于在连接本模块的通讯出现总线错误后，决定本模块的所有输出线圈状态是继续保持，或是复位为线圈关断状态。

模块支持 MODBUS TCP 客户端 502、9502、9503、5502 四路端口，以及 COM1 与 COM2 接口的两路 MODBUS RTU 主站连接本模块，当以上六路连接中**至少一路连接**本模块的通讯正常时，**总线**通讯即**正常**，当 MODBUS TCP 客户端或者 MODBUS RTU 主站与本模块之间通讯**无一路连接**并超过一定时间时，**总线**通讯即判断**错误**。

用户可通过“艾莫迅 MODBUS 调试工具”设置总线错误模式（复位或保持）、总线错误判定时间（阈值）。如下图所示，在“模式配置”区域，根据需求进行总线错误复位或者总线错误保持的勾选，以及在判定总线错误时间阈值（单位 10ms）处填入数值（即 MODBUS TCP 客户端或者 MODBUS RTU 主站与本模块间无连接的时间超过这一设置数值后，判定为总线错误），点击“设置”按钮，RUN 灯常亮 5S 后恢复闪烁，再将模块断电至少 3S 后上电，新设置的总线错误模式和判定时间即生效。



注意：

- ❖ 出厂或者按键复位时，模式为总线错误复位，总线错误判断时间阈值为 2s
- ❖ 总线错误判断时间阈值设置范围为：2s~327.67s，设置值超出范围时默认 2ms
- ❖ 总线错误判定时间为持续时间，即当无连接时间未超过总线错误时间内再次连接本模块后，判定时间待下次无连接开始从零秒计时。

注意

- ❖ 由于艾莫迅 MODBUS 配置工具刚开始扫描 6 秒钟内，处于较快频率获取模块当前参数状态，若此时用户在选择需设置参数，未尽快点击相应设置按钮，容易恢复设置前参数导致需要重复操作。
- ❖ 需要在模块断电前设置多个参数时，应在 RUN 灯恢复闪烁后，再设置下一个参数。
- ❖ 以上操作(除对输入\出口的操作)均支持掉电保存，切勿频繁操作，避免损坏模块，造成工作异常。

6.3、网页配置

6.3.1、登陆模块 IP 网页

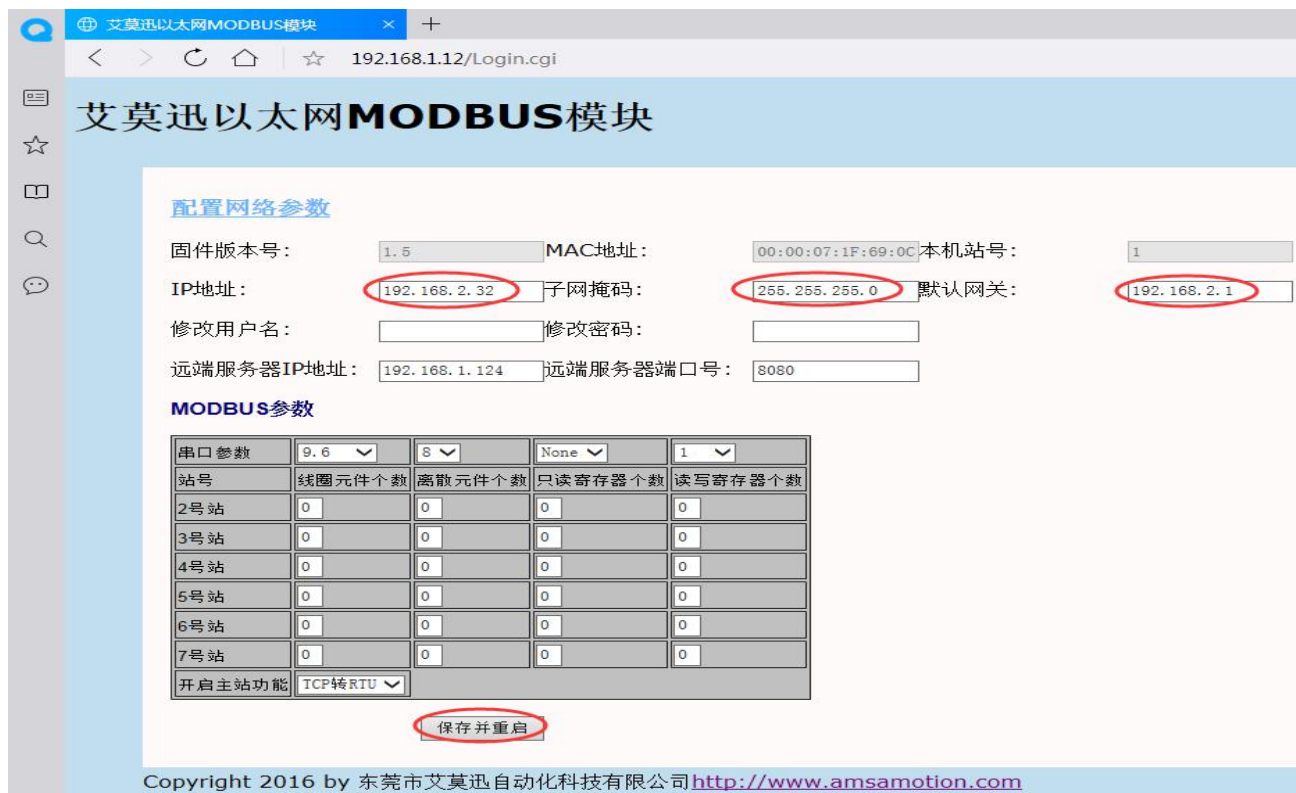
打开浏览器输入模块的 IP (默认 IP 为 192.168.1.12) 后进入登录页面，在登录账号与登录密码处均填写 “amx666” 后，点击登录按钮，即可进入模块的参数页面，如下图所示。



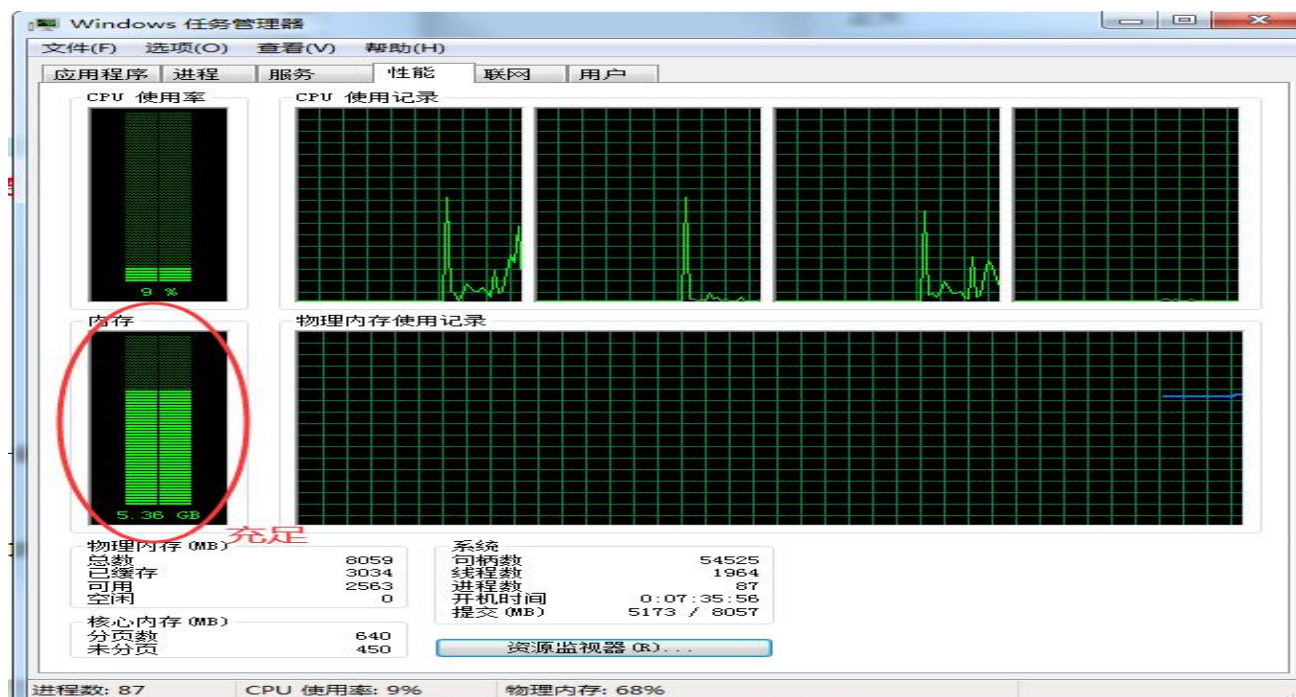
注意：仅在点击登录按钮后，读取模块当前参数。

6.3.2、模块 IP 设置

如下图所示，在参数页面“IP 地址”区域，将所需 IP 地址填入，然后点击保存并重启按钮，至网页无法显示后，将模块断电至少 3S 后上电，新设置模块 IP 地址即生效。



注意：多次点击保存并重启设置 IP 无效时，请检查电脑物理内存是否够用。



6.3.3、远端服务器 IP 设置

COM1 口串口功能为 MODBUS RTU 转 MODBUS TCP 时，相关远端服务器参数，需由模块 IP 网页设置。

如下图所示，在参数页面”远端服务器 IP 地址“区域，将所需远端服务器 IP 地址、端口号填入，然后点击保存并重启按钮，至网页无法显示后，将模块断电至少 3S 后上电，新设置远端服务器 IP 地址、端口号即生效。



注意：远端服务器 IP 地址应注意与模块 IP 在同一网段。

6.3.4、COM2 口参数设置

➤ COM 口串口参数（除波特率外）

如下图所示，在参数页面“串口参数”区域，从下拉清单中选择对应 COM2 口的通讯参数后，然后点击同一水平线位置的“确定”按钮，或点击保存并重启按钮，至网页无法显示后，将模块断电至少 3S 后上电，新设置 COM2 串口参数即生效。



⚠注意:

- ☞设置数据位 7 需要串口模式为 TCP 透传时（串口模式设置见章节 5.2.5 或下一小节“开启主站功能”内容）
- ☞设置数据位 7 时，校验位不支持无校验（None）

➤ 开启主站功能

如下图所示，在参数页面“开启主站功能”区域，从下拉清单中可选择对应 COM2 口的串口模式，然后点击保存并重启按钮，至网页无法显示后，将模块断电至少 3S 后上电，新设置 COM2 串口模式即生效。



⚠注意：COM2 口的其他串口模式，也可通过此处下拉清单中选择设置

➤ MODBUS TCP 控制多从站通讯配置

如下图所示，在参数页面“2号站~7号站”区域，填写**对应站号**“线圈元件、离散元件、只读寄存器、读写寄存器”的个数，然后点击右下角确定，或点击保存并重启按钮，至网页无法显示后，将模块断电至少 3S 后上电，新设置 MODBUS TCP 控制多从站通讯配置即生效。

艾莫迅以太网MODBUS模块

192.168.1.12/Login.cgi

艾莫迅以太网MODBUS模块

配置网络参数

固件版本号: 1.5MAC地址: 00:00:07:1F:69:0C本机站号: 1

IP地址: 192.168.1.12子网掩码: 255.255.255.0默认网关: 192.168.1.1

修改用户名: 修改密码:

远端服务器IP地址: 192.168.1.124远端服务器端口号: 8080

MODBUS参数

串口参数	9.6	8	None	1
站号	线圈元件个数	离散元件个数	只读寄存器个数	读写寄存器个数
2号站	8	8	6	1
3号站	8	0	0	0
4号站	0	16	0	0
5号站	16	0	0	0
6号站	16	0	0	0
7号站	16	16	0	0
开启主站功能	RTU主站			

保存并重启

Copyright 2016 by 东莞市艾莫迅自动化科技有限公司<http://www.amsamotion.com>

⚠注意：要 MODBUS TCP 控制多从站可用，还需将 COM2 口模式设置为 RTU 主站。

📖 注意

✧ 以上操作(除对输出\入口的操作)均支持掉电保存，切勿频繁操作，避免损坏模块，造成工作异常。

七、MODBUS TCP 报文格式说明

7.1、数字量输入信号采集命令

➤ 协议说明

功能码：0x02

该命令用于读出当前离散输入寄存器状态；本机离散输入寄存器 0x00-0x07 对应输入通道 1-8，当输入口状态为无效时，指示灯灭，返回 0；有效时，指示灯亮，返回 1。

➤ 读离散输入请求报文格式说明

读离散输入请求 (MODBUS TCP 报文格式)

序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE；出厂本机为 1，其余用于 RS485 口的从机站号
5	功能码	1	0x02	MODBUS 通讯协议的相关功能码
6	起始地址	2	高字节在前	从该寄存器地址开始读输入离散量
7	寄存器个数	2	高字节在前	

➤ 读离散输入应答报文格式说明

读离散输入应答 (MODBUS TCP 报文格式)

序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号，同请求报文
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE；出厂本机为 1，其余用于 RS485 口的从机站号
5	功能码	1	0x02	MODBUS 通讯协议的相关功能码
6	数据长度	1		假设数据长度值为 N，单位：字节
7	数据	N	低字节在前	本站号时对应 8 位离散输入，数据从低位到高位对应离散输入 1~8 通道，每个字节高位在前

➤ 示例报文说明

读取本机的 1~8 输入通道状态，示例中输入通道 2、8 有效

请求报文:

00 06 00 00 00 06 01 02 00 00 00 08

应答报文

00 06 00 00 00 04 01 02 01 82

读取 2 号从站的 1~16 输入通道状态，示例中 2 号从站的输入通道 4、6、9、15 有效

请求报文:

00 06 00 00 00 06 02 02 00 00 00 10

应答报文

00 06 00 00 00 05 02 02 02 28 41

7.2、数字量输出信号采集命令

➤ 协议说明

功能码：0x01

该命令用于读出当前线圈寄存器状态；本机线圈寄存器 0x00-0x07 对应数字量输出通道 1-8，当输出口状态为无效时，指示灯灭，返回 0；有效时，指示灯亮，返回 1。

➤ 读线圈输出状态的请求报文格式说明

读线圈状态请求(MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE; 出厂本机为 1，其余用于 RS485 口的从机站号
5	功能码	1	0x01	MODBUS 通讯协议的相关功能码
6	起始地址	2	高字节在前	
7	寄存器个数	2	高字节在前	

➤ 读线圈输出应答报文格式说明

读线圈状态应答 (MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号，同请求报文
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE; 出厂本机为 1，其余用于 RS485 口的从机站号
5	功能码	1	0x01	MODBUS 通讯协议的相关功能码
6	数据长度	1		数据长 N 字节，则数据长度值为 N
7	数据	1	低字节在前	本站站号时对应 8 位线圈输出，数据从低位到高位对应离散输入 1~8 通道，每个字节高位在前

➤ 示例报文说明

读取本机的 1~8 通道的线圈状态,示例中线圈通道 2、8 有效

请求报文:

00 01 00 00 00 06 01 01 00 00 00 08

应答报文

00 01 00 00 00 04 01 01 01 82

读取 2 号从站的 1~16 通道输出线圈状态，示例中 2 号从站的输出通道 1、7、10、16 有效

请求报文:

00 01 00 00 00 06 02 01 00 00 00 10

应答报文

00 01 00 00 00 05 02 01 02 41 82

7.3、数字量输出信号单个控制命令

➤ 协议说明

功能码：0x05

该命令用于控制单个线圈寄存器状态；本机线圈寄存器 0x00-0x07 对应数字量输出通道 1-8，当输出口状态为无效时，指示灯灭，返回 0；有效时，指示灯亮，返回 1。

➤ 写单个离散输出的请求报文格式说明

写单个线圈请求 (MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE; 出厂本机为 1, 其余用于 RS485 口的从机站号
5	功能码	1	0x05	MODBUS 通讯协议的相关功能码
6	写入地址	2	高字节在前	
7	写入值	2	高字节在前	写入 0xFF00 表示使能输出; 写入 0x0000 表示停止输出;

➤ 写单个离散输出的应答报文格式说明

写单个线圈应答 (MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号, 同请求报文
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE; 出厂本机为 1, 其余用于 RS485 口的从机站号
5	功能码	1	0x05	MODBUS 通讯协议的相关功能码
6	写入地址	2	高字节在前	
7	写入值	2	高字节在前	写入 0xFF00 表示使能输出; 写入 0x0000 表示停止输出;

➤ 示例报文说明

使能本机通道 1 的输出

请求报文:

31 A6 00 00 00 06 01 05 00 00 FF 00

应答报文

31 A6 00 00 00 06 01 05 00 00 FF 00

停止本机通道 1 的输出

请求报文:

31 A6 00 00 00 06 01 05 00 00 00 00

应答报文

31 A6 00 00 00 06 01 05 00 00 00 00

7.4、数字量输出信号多个控制命令

➤ 协议说明

功能码：0x0F

该命令用于控制多个线圈寄存器状态；本机线圈寄存器 0x00-0x07 对应数字量输出通道 1-8，当输出口状态为无效时，指示灯灭，返回 0；有效时，指示灯亮，返回 1。

➤ 写多个离散输出的请求报文格式说明

写多个线圈请求 (MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE；出厂本机为 1，其余用于 RS485 口的从机站号
5	功能码	1	0x0F	MODBUS 通讯协议的相关功能码
6	起始地址	2	高字节在前	
7	写入长度	2	高字节在前	
8	写入数据 字节数	1		假设写入数据字节数的值为 N
9	写入数据	N	低字节在前	每个字节高位在前

➤ 写多个离散输出的应答报文格式说明

写多个线圈应答 (MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE; 出厂本机为 1, 其余用于 RS485 口的从机站号
5	功能码	1	0x0F	MODBUS 通讯协议的相关功能码
6	起始地址	2	高字节在前	
7	写入长度	2	高字节在前	

➤ 示例报文说明

控制本机 1~8 通道的输出线圈状态，示例中使输出通道 1、3、6、8 有效

请求报文:

31 A6 00 00 00 08 01 0F 00 00 00 08 01 A5

应答报文

31 A6 00 00 00 06 01 0F 00 00 00 08

控制 254 号从站的 3~15 通道的 13 个输出线圈状态，示例中使输出通道 3、9、13、15 有效

请求报文:

31 A6 00 00 00 09 FE 0F 00 02 00 0D 02 41 14

应答报文

31 A6 00 00 00 06 FE 0F 00 02 00 0D

7.5、输入寄存器读出命令

➤ 协议说明

功能码：0x04

该命令用于读取当前输入寄存器数值；本机输入寄存器 0x00-0x05 对应模拟量输入通道 1-6，数值范围为 0-4095，电压输入通道范围为 0-10V，电流输入通道范围为 0-20mA，即电压输入 10V 或电流输入 20mA 时，对应模拟量接入通道读入 0x0FFF。

➤ 读输入寄存器请求报文格式说明

读离散输入请求 (MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE; 出厂本机为 1, 其余用于 RS485 口的从机站号
5	功能码	1	0x04	MODBUS 通讯协议的相关功能码
6	起始地址	2	高字节在前	
7	寄存器个数	2	高字节在前	

➤ 读输入寄存器应答报文格式说明

读离散输入应答 (MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号, 同请求报文
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE; 出厂本机为 1, 其余用于 RS485 口的从机站号
5	功能码	1	0x04	MODBUS 通讯协议的相关功能码
6	数据长度	1		假设数据长度值为 N
7	数据	N	低字在前	本站号时即模拟量输入低通道在前; 每个寄存器数据占一个字的长度

➤ 示例报文说明

读取本机输入寄存器 1-6 通道数值, 示例中 1、4 通道分别输入电压 10V、电流 20ma

请求报文:

00 04 00 00 00 06 01 04 00 00 00 06

应答报文

00 04 00 00 00 0F 01 04 0C FF FF 00 00 00 00 FF FF 00 00 00 00

读取 2 号从站的输入寄存器 30001~30006 地址数值，示例中 30001、30006 地址的数值为 0x7531、0x7536。

请求报文:

00 04 00 00 00 06 02 04 00 00 00 06

应答报文

00 04 00 00 00 0F 02 04 0C 75 31 00 00 00 00 00 00 00 00 75 36

7.6、保持寄存器读出命令

➤ 协议说明

功能码：0x03

该命令用于读取当前保持寄存器数值；本机用户有效保持寄存器 0x06 对应模拟量输出通道，数值范围为 0-4095，电压输出通道范围为 0-10V，电流输出通道范围为 0-20mA。即保持寄存器 0x06 读取数值 4095 时，电压输出通道输出 10V，电流输出通道输出 20ma。

➤ 读保持寄存器的请求报文格式说明

读保持寄存器请求(MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE; 出厂本机为 1，其余用于 RS485 口的从机站号
5	功能码	1	0x03	MODBUS 通讯协议的相关功能码
6	起始地址	2	高字节在前	
7	寄存器个数	2	高字节在前	本站号时寄存器个数为 7，可读取模拟量输出通道当前数值

➤ 读保持寄存器的应答报文格式说明

读保持寄存器应答 (MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号，同请求报文
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE; 出厂本机为 1，其余用于 RS485 口的从机站号
5	功能码	1	0x03	MODBUS 通讯协议的相关功能码
6	数据长度	1		假设数据长度值为 N，单位：字节
7	数据	N	低字节在前	每个寄存器数据占 1 个字的长度

➤ 示例报文说明

读取 127 号从站的保持寄存器 40001~40006 通道数值，示例中 40001、40006 通道的数值为 0x9C41、0x9C46。请求报文:

00 17 00 00 00 06 7F 03 00 00 00 06

应答报文

00 17 00 00 00 0F 7F 03 0C 9C 41 00 00 00 00 00 00 00 00 9C 46

7.7、写单个保持寄存器命令

➤ 协议说明

功能码：0x06

该命令用于写单个保持寄存器数值；本机用户可用保持寄存器 0x06 对应模拟量输出通道，数值范围为 0-4095，电压输出通道范围为 0-10V，电流输出通道范围为 0-20mA，当保持寄存器 0x06 写入数值 4095 时，电压输出通道输出 10V，电流输出通道输出 20ma。

➤ 写单个保持寄存器的请求报文格式说明

写单个保持寄存器请求 (MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号

2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数字字节长度
4	单元标识	1		范围 0x01~0xFE; 出厂本机为 1，其余用于 RS485 口的从机站号
5	功能码	1	0x06	MODBUS 通讯协议的相关功能码
6	起始地址	2	高字节在前	
7	寄存器值	2	高字节在前	

➤ 写单个保持寄存器应答报文格式说明

写单个保持寄存器应答 (MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号，同请求报文
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围 0x01~0xFE; 出厂本机为 1，其余用于 RS485 口的从机站号
5	功能码	1	0x06	MODBUS 通讯协议的相关功能码
6	起始地址	2	高字节在前	
7	寄存器值	2	高字节在前	

➤ 示例报文说明

设置 127 号从站的保持寄存器 40005 通道数值为 0x9C45。

请求报文:

00 00 00 00 00 06 7F 06 00 04 9C 45

应答报文

00 00 00 00 00 06 7F 06 00 04 9C 45

7.8、写多个保持寄存器命令

➤ 协议说明

功能码：0x10

该指令仅用于连续写多个数值给连接本机 RS485 接口的从站保持寄存器。

➤ 写多个保持寄存器请求报文格式说明

写多个保持寄存器请求(MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围从 0x02~0xFE; 用于连接 RS485 口的从机地址
5	功能码	1	0x10	MODBUS 通讯协议的相关功能码
6	起始地址	2	高字节在前	
7	寄存器个数	2	高字节在前	
8	数据个数	1		假设寄存器个数为 N, 则数据个数的值为 2N, 单位: 字节
9	数据	2N	低字节在前	假设寄存器个数为 N, 则数据的长度 (字节) 值为 2N

➤ 写多个保持寄存器应答报文格式说明

写多个保持寄存器应答(MODBUS TCP 报文格式)				
序号	报文字段	长度 (字节)	字节 存放方式	说明
1	事务处理标识	2	高字节在前	一般是报文序号, 同请求报文
2	协议标识	2	高字节在前	一般默认为 00 00
3	报文长度	2	高字节在前	除去事务处理标识、协议标识、以及报文长度的数据字节长度
4	单元标识	1		范围从 0x02~0xFE; 用于连接 RS485 口的从机地址
5	功能码	1	0x10	MODBUS 通讯协议的相关功能码
6	起始地址	2	高字节在前	
7	寄存器个数	2	高字节在前	

➤ 示例报文说明

设置 127 号从站的保持寄存器 40001~40004 通道数值分别为 0x9C41、0x9C42、0x9C43、0x9C44。

请求报文:

00 00 00 00 00 0F 7F 10 00 00 00 04 08 9C 41 9C 42 9C 43 9C 44

应答报文

00 00 00 00 00 06 7F 10 00 00 00 04

修订历史

版本	修订日期	修订说明	维护人
1.0	2020.07.09	初始版本（不带拨码）	ZHU
1.1	2020.08.15	带拨码、总线错误模式	ZHU
1.2	2021.12.28	统一型号、增加 S7 通讯状态说明	ZHU



关于我们

官方网站: <http://amsamotion.com>

邮箱: amx@amsamotion.com

技术热线: 4001-522-518 拨 1

销售热线: 4001-522-518 拨 2

公司地址: 广东省东莞市南城区袁屋边艺展路 9 号兆炫制造园 B 栋 1 楼