

瑞捷物联Modbus TCP-CAN

转换模块说明书

型号: RJ268CAN

文件版本: V24.10.



目 录

1. 功能简介	2
1.1 功能概述	2
1.2 性能特点	2
1.2.1 硬件特点	2
1.2.2 CAN 属性	2
1.2.3 以太网属性	2
1.3 典型应用	3
2. 设备安装	4
2.1 设备尺寸	4
2.2 设备固定	4
2.3 接口定义及功能	5
3. 设备使用	6
3.1 与 PC 连接	6
3.1.1 恢复出厂设置	6
3.1.2 更改 PC 端 IP 地址	7
3.2 与以太网连接	8
3.3 与 CAN 总线连接	8
3.4 CAN 总线终端电阻	9
3.5 系统状态指示灯	9
4. CT01BNEW.exe 软件使用	10
4.1 恢复出厂设置	10
4.2 基本参数配置	10
4.2.1 用电脑连接 RJ268CAN 模块	10
4.2.2 滤波设置发送	12
4.2.3 滤波设置接收	13
4.3 下载到 RJ268CAN 模块的 Flash	13
5. 应用实例	14
5.1 读取接收到的 CAN 帧	14
5.2 写入要发送的 CAN 帧	14
6. 技术规格	15
7. 常见问题	16
8. 免责声明	17
附录 A: Modbus TCP 协议简介	18
A.1 Modbus TCP 协议数据格式	18
A.2 Modbus 常用功能码	20

1. 功能简介

1.1 功能概述

RJ268CAN 模块是集成1路标准以太网接口和1路标准CAN接口的 ModbusTCP 从站转CAN 的协议转换模块。采用RJ268CAN 模块,用户可以轻松完成CAN总线网络和以太网网络的互连互通,进一步拓展CAN 总线网络的范围。

RJ268CAN 可以将以太网网络与CAN总线网络桥接,用户可以将此智能协议转换模块集成到自己的系统中,从而使本不具备相互通信能力的以太网网络与CAN总线快速具备通信能力,从而节省开发时间、降低开发成本、快速抢占市场先机。

RJ268CAN 模块现已被广泛应用于构建现场总线实验室、工业控制网络、智能小区监控等网络环境中。同时该设备具有体积小、即插即用等特点,且模块使用DIN 导轨的安装方式,使其特别适用于工业现场或机柜中与其他设备配套使用。

RJ268CAN 模块上已集成CAN接口电气隔离保护模块,使其避免由于瞬间过流/过压而对设备造成损坏,增强系统在恶劣环境中使用的可靠性。

用户可以通过附带的“CT01BNEW.exe”软件对RJ268CAN 模块进行配置。目前该配置软件仅支持 Modbus TCP-CAN 协议之间转换的配置,对于以太网端或CAN端的其他标准或自定义协议,暂时不支持用户自己对其配置,如需要,我公司可为用户提供任意协议之间的配置服务。

1.2 性能特点

1.2.1 硬件特点

- 高速的32位工业级控制器;
- 内嵌硬件看门狗定时器;
- 使用外接电源供电 (9~28V DC, 75mA);
- 工作温度范围: $-40^{\circ}\text{C} \sim 85^{\circ}\text{C}$;
- 静电放电抗扰度等级: 接触放电 $\pm 4\text{KV}$, 空气放电 $\pm 8\text{KV}$;
- 电快速瞬变脉冲群抗扰度等级: $\pm 2\text{KV}$;
- 浪涌抗扰度等级: 电源接口 $\pm 1\text{KV}$. CAN 总线接口 $\pm 4\text{KV}$;
- 标准DIN导轨安装方式,专为工业设计。

1.2.2 CAN 属性

- 集成1路CAN 总线接口,使用端子接线方式;
- CAN总线号包括: CAN H、CAN L、CAN GND;
- CAN总线支持CAN2.0A 和 CAN2.0B 帧格式,符合 ISO/DIS 11898规范;
- CAN总线通讯波特率在 5kbps~1Mbps之间;
- CAN总线接口采用电气隔离,隔离模块绝缘电压: 1500V DC;

1.2.3 以太网属性

- RJ45, 支持10/100M自适应;
- Modbus从站支持功能码: 03H、04H、06H、16H;

- 支持静态或动态 IP 获取；
- 网络断开后自动恢复连接资源，可靠地建立 TCP 连接；
- 兼容SOCKET 工作方式，上位机通讯软件编写遵从标准的SOCKET规则。

1.3典型应用

- 工业以太网设备与CAN网络设备互联
- 电力通讯网络
- 工业控制设备
- 高速、大数据量通讯
- CAN总线与串行总线之间的网关网桥；
- 工业现场网络数据监控；
- CAN教学应用远程通讯；
- CAN工业自动化控制系统；
- 低速CAN网络数据采集数据分析；
- 智能楼宇控制数据广播系统等CAN总线应用系统。
- PLC设备连接CAN总线网络通讯；

2. 设备安装

2.1 设备尺寸

设备外形尺寸: (长, 含接线端子)115mm*(宽)100mm* (厚)22mm, 其示意图下图所示。



尺寸:长115*宽100*厚22mm 重量:155克

图 2.1 RJ268CAN模块外形尺寸

2.2 设备固定

RJ268CAN模块安装方法如下图2.2所示, 可使用一字螺丝刀辅助将模块安装到DIN 导轨上。

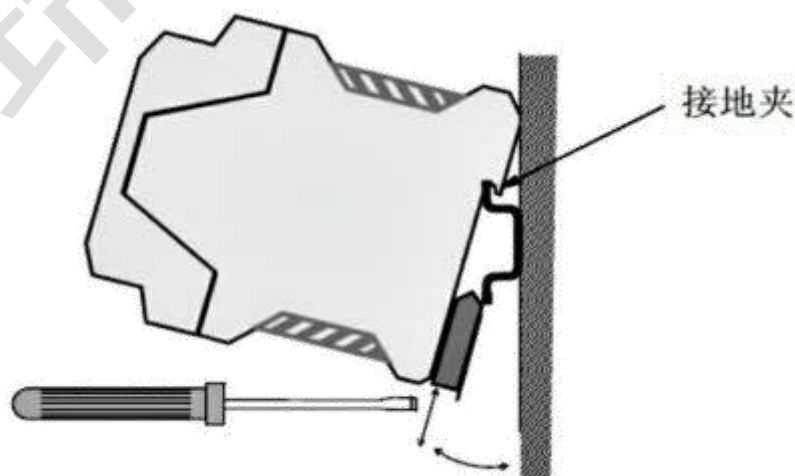


图 2.2 RJ268CAN模块安装

请保证设备的良好接地，否则会有电击危险。接地宜采用单独接地或单点接地，不可采用公共接地。RJ268CAN模块地需要外部接地线，即端子的PE引脚。

2.3接口定义及功能

RJ268CAN 模块集成1路9-28V DC 电源接口、1路标准CAN 总线接口、1路标准以太网接口。RJ268CAN 模块接线端子排如图2.3所示。



图2.3 RJ268CAN模块接线端子排

RJ268CAN 模块的电源接口由一个 4Pin插拔式接线端子引出，其接口定义如表2.1 所示。

引脚	端口	名称	功能
13	9-28V DC	+	9-28V 直流电源输入正
14		—	9-28V 直流电源输入负
15		NC	未使用
16		PE	屏蔽

表2.1 RJ268CAN 电源接口定义

RJ268CAN 模块CAN 总线接口由1个4 Pin接线端子引出,可以用于连接1个 CAN 总线接口的设备，其接口定义如表2.2所示。

引脚	端口	名称	功能
9	CAN-BUS	CAN-G	CAN_GND
10		CAN-L	CAN_L 信号线 (CAN 低)
11		CAN-H	CAN_H 信号线 (CAN高)
12		PE	屏蔽
1-8	NC	NC	未使用

表2.2 RJ268CAN 模块的CAN 总线信号分配

3. 设备使用

RJ268CAN 模块工作原理如图3.1所示。

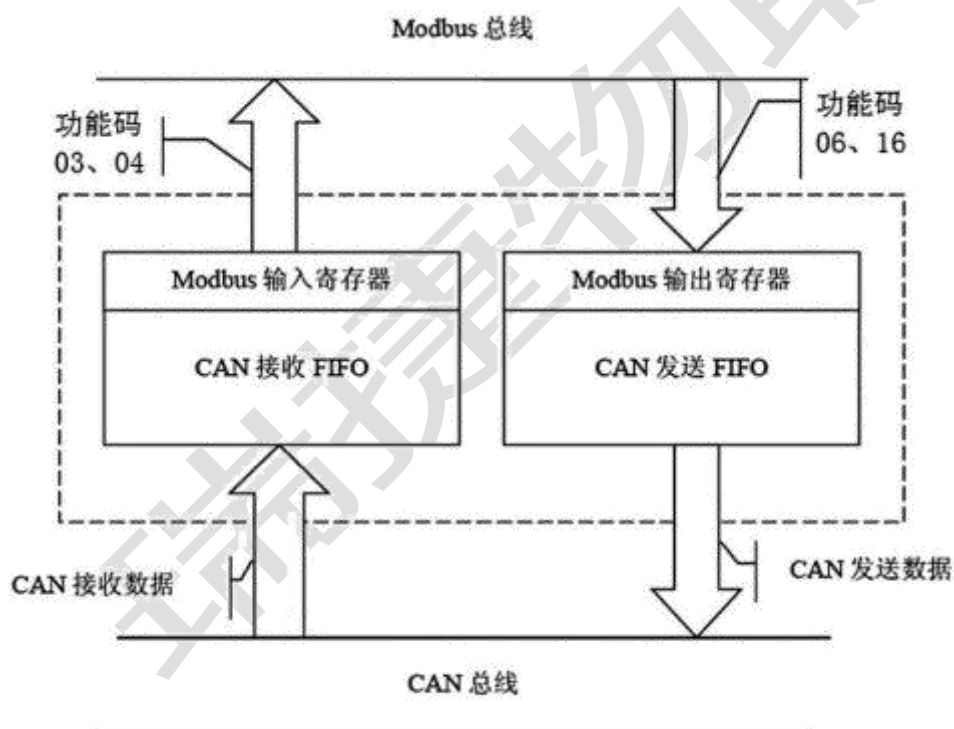


图3.1 J268CAN 模块工作原理

3.1 与 PC 连接

RJ268CAN模块使用9-28VDC供电，当设备获得正常供电后，可使用PC端的“CT01BNEW.exe”配置软件对其工作模式及基本运行参数进行配置(CT01BNEW.exe软件使用方法详见第4章)，RJ268CAN模块目前仅支持用户对 Modbus TCP转CAN之间的通信进行配置，其他协议暂不支持用户自行配置。

3.1.1 恢复出厂设置

RJ268CAN模块硬件出厂默认IP: 192.168.10.30, 如果用户已经修改过IP地址并且忘记, 可进行参数复位, 具体操作请参照 4.1恢复出厂设置。

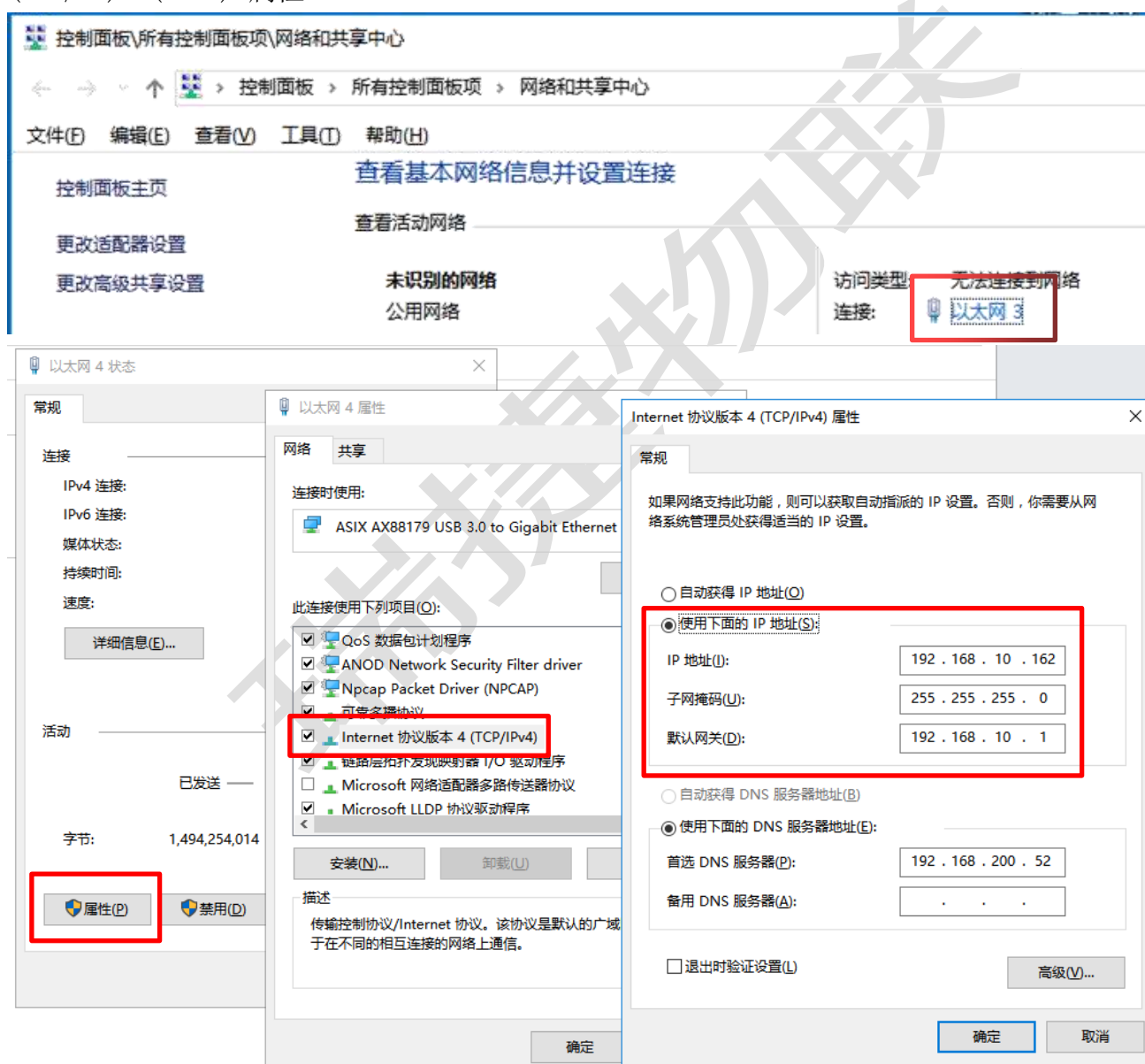
3.1.2 更改 PC 端IP 地址

用户在使用PC机与RJ268CAN 模块进行通信前, 需要保证用户的PC机内有以太网卡, 并且PC机与RJ268CAN模块必须在同一个网段内。只有在同一网段, 您才能使用PC机对 RJ268CAN模块进行配置。如果网段不同, 则需对 PC机进行以下设置

用户使用的操作系统是 Windows XP/7、8、10, 用户可以修改本机IP 地址的方式设置本机IP 及网段。Windows8、windows 10操作参照 Windows7 系统。

修改本机 IP 地址

进入操作系统后, 进入本机的控制面板→进入“网络连接”(WinXP)或“网络和共享中心”(Win 7、8、10)→进入“本地连接”属性→“Internet协议(TCP/IP)”(winXP)或“Internet协议版本4(TCP/IP)”(Win7) 属性。



在“IP 地址”栏中点击修改, 输入与RJ268CAN 同一网段的IP 地址, 如上图即可完成添修改PC 机 IP 地址操作。

3.2与以太网连接

RJ268CAN模块的以太网接口集成10/100M自适应以太网芯片，符合以太网标准协议规范，支持即插即用。用户可以使用五类以上网线进行工业以太网与RJ268CAN模块连接。

3.3 与CAN总线连接

RJ268CAN模块接入CAN总线的连接方式：将CAN H连CAN H，CAN L连CAN L即可建立通信。

CAN总线网络采用直线拓扑结构，总线最远的2个终端需要安装120 Ω 的终端电阻； 如果节点数目大于2，则中间节点不需要安装120 Ω 的终端电阻。对于分支连接，其长度不应超过3米。CAN总线的连接见图3. 4所示。

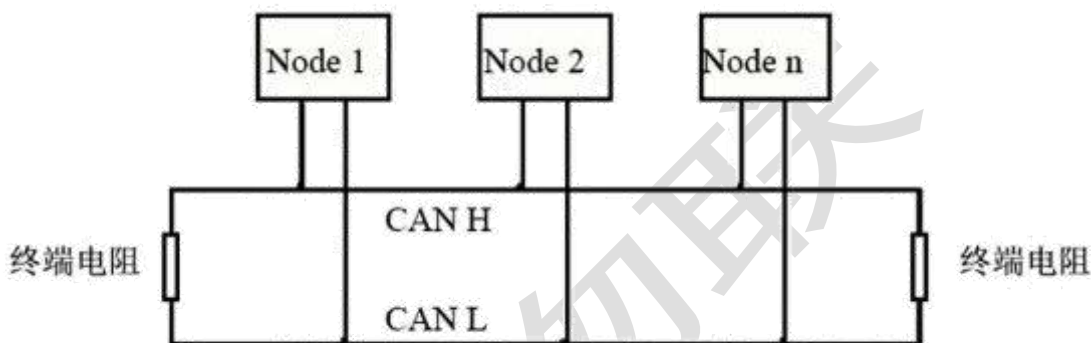


图 3.4 CAN 总线网络的拓扑结构

注意：CAN总线电缆可以使用普通双绞线、屏蔽双绞线。理论最大通信距离主要取决于总线波特率，最大总线长度和波特率关系详见表3. 1。若通讯距离超过1Km，应保证线的截面积大于 $\phi 1.0\text{mm}^2$ ，具体规格应根据距离而定，常规是随距离的加长而适当加大。

波特率	总线长度
1 Mbit/s	25m
500 kbit/s	100m
250 kbit/s	250m
125 kbit/s	500m
50 kbit/s	1km
20 kbit/s	2.5km
10 kbit/s	5km
5 kbit/s	13km

表3. 1波特率与最大总线长度参照表

3.4 CAN总线终端电阻

为了增强CAN通讯的可靠性，消除CAN总线终端信号反射干扰，CAN总线网络最远的两个端点通常要加入终端匹配电阻，如图3.5所示。终端匹配电阻的值由传输电缆的特性阻抗所决定。例如双绞线的特性阻抗为120Ω，则总线上的两个端点也应集成120Ω终端电阻。

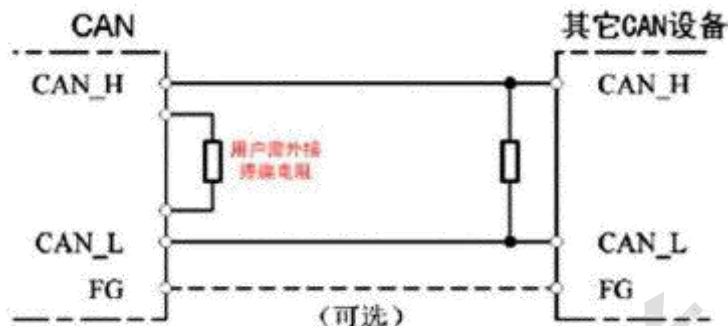


图3.5 RJ268CAN模块与其他CAN节点设备连接

请注意：RJ268CAN模块内部未集成120Ω终端电阻，模块外部提供电阻接线端子。需要接入终端电阻时，将电阻两端分别接入CAN_L、CAN_H即可。

3.5 系统状态指示灯

RJ268CAN模块具有1个SYS指示灯，用来指示设备的运行状态，1个DAT指示灯，用来指示数据传输。这2个指示灯的具体指示功能见表3.2，这2个指示灯处于各种状态下时，CAN总线的状态如表3.3所示。

指示灯	颜色	指示状态
SYS	绿	系统运行指示
DAT	绿	数据转换传输指示

表3.2 RJ268CAN模块指示灯

RJ268CAN模块上电后，系统初始化状态指示灯SYS点亮，表明设备已经供电，系统正在初始化；否则，表示系统存在电源故障或发生有严重的错误。

以太网端与CAN端均连接正常后，当总线间有数据在传输时，数据信号指示灯DAT会闪烁。

指示灯	状态	指示状态
SYS	常亮	设备初始化通过，待机状态
	不亮	设备初始化未通过
DAT	不亮或常亮	总线间无数据传输
	闪烁	总线间有数据传输

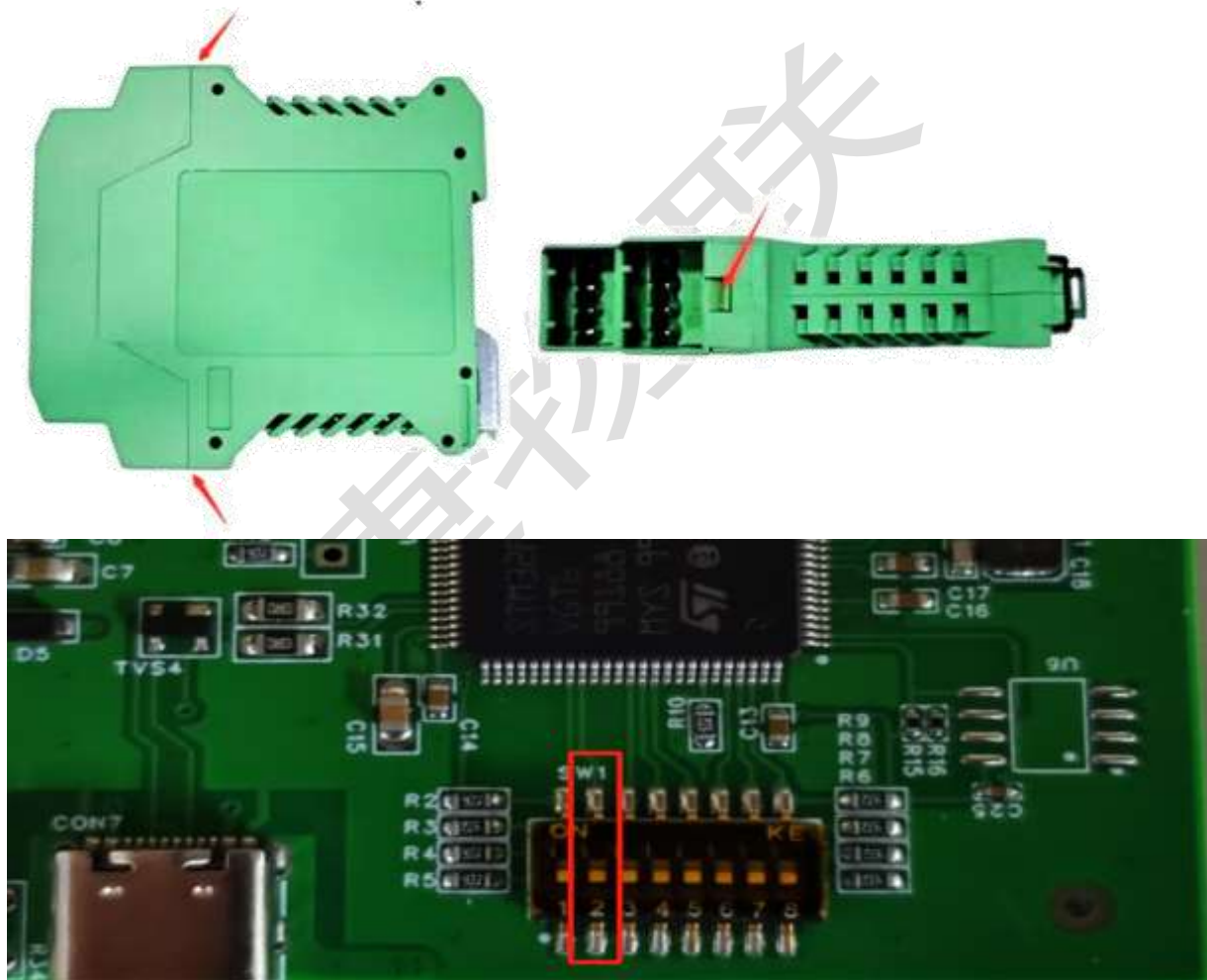
表3.3 RJ268CAN模块指示灯状态

4. CT01BNEW.exe软件使用

4.1 恢复出厂设置

RJ268CAN 模块硬件出厂默认IP: 192.168.10.30, 如果用户已经修改过IP 地址并且忘记, 通过设备中的拨码开关, 对其进行参数复位。默认的CAN 总线波特率是 1M, 默认 Modbus映射表都为0。

具体操作为: 先不要对模块上电, 用一字螺丝刀撬动模块顶端和尾端的卡扣, 打开设备外壳, 找到设备中如图3.2所示的拨码开关, 将2号开关拨到ON位置, 然后将系统上电, 等待大约3秒钟, 看到前面板上面的SYS指示灯闪烁, 此时关闭电源, 然后将2号开关拨回到OFF状态。至此, 设备设置已经恢复到出厂默认状态, 系统默认的IP: 192.168.10.30。



请注意: 设备恢复出厂设置后, 所有的参数设置及映射表设置会被全部清除, 请谨慎操作。

4.2 基本参数配置

RJ268CAN 模块可以使用“CT01BNEW.exe”软件对其进行参数配置, 包括: 工作模式、工作端口、目标端口、目标IP、CAN 工作模式、CAN波特率等基本参数。

4.2.1 用电脑连接RJ268CAN模块

1. 首先将RJ268CAN模块上电，用网线将RJ268CAN模块与电脑连接好，待设备的SYS指示灯闪烁时，表示RJ268CAN模块初始化完毕，处于待连接状态。

2. 打开“CT01BNEW.exe”软件,输入RJ268CAN 模块的IP 地址，点击“ Connect”进行连接。如下图4.2 所示。

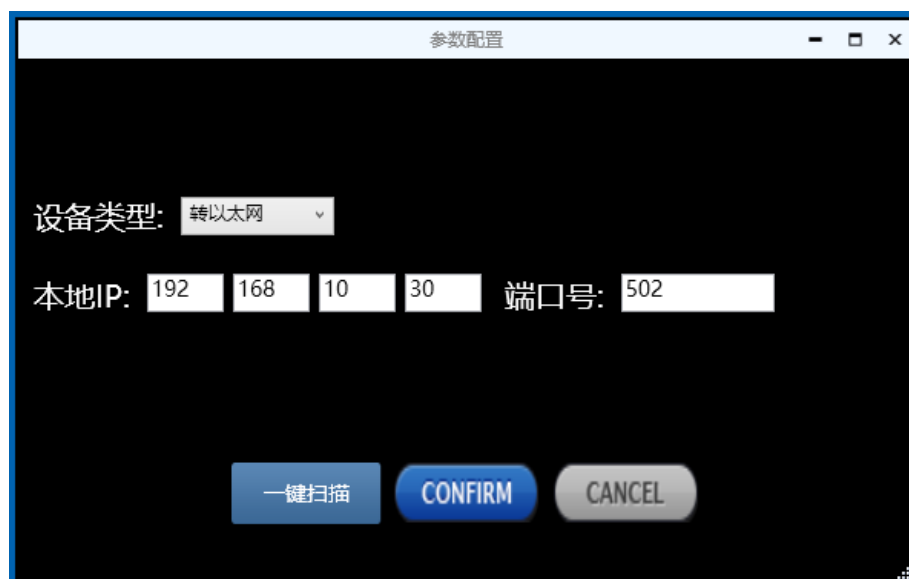


图4.2配置软件初始界面

点击“ Confirm”出现如下图4.3 软件主界面：



图4.3配置软件主界面

- 软件重新连接按键：点击后跳转回通讯配置界面。
- 界面下方显示当前设备类型，软件版本，硬件版本
- 刷新按键：点击后，重新读取当前设备信息

- 写入按键：点击后，写入当前设置的CAN波特率，RS485波特率，RS485地址，及发送接收报文
- CAN波特率：打开界面显示当前设备CAN波特率，可切换其他波特率写入
- IP地址：打开界面显示当前设备IP地址，编制输入性地址

4.2.2 滤波设置发送

- 连接成功后切换至滤波设置发送界面



- 读取按键：点击后读取当前设备设置的发送报文信息。
- 写入按键：点击后，写入当前设置发送报文信息。
- ID：可写入发送的报文ID
- EXT：帧格式（标准帧：0/扩展帧：4）
- RTR：帧类型（数据帧：0/远程帧：1）
- Address(100-17F)：Modbus首地址，范围（0x100-0x17F）
- Len：数据长度，范围（1-8）（注：Modbus首地址和数据长度组合，切勿重复占用）
- SendMode：发送模式（数据触发模式：0/循环发送模式：1）
 - 数据触发模式：当有 Modbus 主机用 06 指令写 Modbus 相应地址数据时，如果数据发生改变，那么触发相应的 CAN 帧数据发送；
 - 循环发送模式：设置每间隔一定时间，循环发送相应的 CAN 帧数据，间隔时间在 Send Timer 中设置，输入 10 进制数，单位是毫秒，比如输入 1000，那么就是间隔 1000ms 发送一次
- Time(ms)：发送时间间隔（单位：ms，最大0xFFFF）
- 注：最大可设置32条

4.2.3 滤波设置接收

连接成功后切换至滤波设置接收界面



- 读取按键：点击后读取当前设备设置的接收报文信息。
- 写入按键：点击后，写入当前设置接收报文信息。
 - ID：可写入接收的报文ID
 - EXT：帧格式（标准帧：0/扩展帧：4）
 - RTR：帧类型（数据帧：0/远程帧：1）
 - Address(00-7F)：Modbus首地址，范围（0x00-0x7F）
 - Len：数据长度，范围（1-8）（注：Modbus首地址和数据长度组合，切勿重复占用）
 - 注：最大可设置32条

4.3 下载到RJ268CAN模块的 Flash

当配置完成后，可以点击工具栏中的“写入”将配置数据写入到设备的FLASH中，数据写入成功后，**需要重新上电**，来启用新的设置。

5. 应用实例

用户可通过随机附赠的网络调试助手发送 Modbus指令来进行调试。使用时请选择TCP Client, 远程主机地址为 192.168.10.30:502 (IP 地址为出厂预设值,可修改; 端口号不可修改)。

请注意：使用网络调试助手时请使用“十六进制显示”和“十六进制发送”。

5.1 读取接收到的 CAN 帧

例如：配置 Modbus从站地址为1, Modbus寄存器首地址为0x01, 功能码为03, CAN 为标准帧, 帧ID为0x181, CAN 帧数据为0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00。

用户 Modbus主站发送请求帧：

00 00 00 00 00 06 01 03 00 01 00 04

主机发送	字节数	例 (Hex)
传输标识	2字节	00 00
协议标识	2字节	00 00
数据长度	2字节	00 06
设备地址	1字节	01
功能码	1字节	03
起始地址	2字节	00 01
寄存器数量	2字节	00 04

RJ268CAN 的响应帧：

00 00 00 00 00 0B 01 03 08 00 00 00 00 00 00 00

从机回送	字节数	例 (Hex)
传输标识	2字节	00 00
协议标识	2字节	00 00
数据长度	2字节	00 0B
设备地址	1字节	01
功能码	1字节	03
响应字节数	1字节	08
寄存器值	8字节	00 00 00 00 00 00 00 00

此时，RJ268CAN 模块 Modbus端已收到了来自其他设备的CAN 端发出的帧ID为0x181的数据帧。

5.2 写入要发送的CAN帧

例如：Modbus寄存器首地址为0x100, 功能码为16(10H), CAN 为标准帧, 帧ID为0x201, CAN帧数据为0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08。

用户 Modbus 主站发送请求帧：

00 00 00 00 00 0F 01 10 01 01 00 04 08 02 01 04 03 06 05 08 07

主机发送	字节数	例 (Hex)
传输标识	2字节	00 00
协议标识	2字节	00 00
数据长度	2字节	00 0F
设备地址	1字节	01
功能码	1字节	10
起始地址	2字节	01 01
寄存器数量	2 字节	00 04
响应字节数	1字节	08
寄存器值	8字节	02 01 04 03 06 05 08 07

RJ268CAN的响应帧：

00 00 00 00 00 06 01 10 01 01 00 04

从机回送	字节数	例 (Hex)
传输标识	2字节	00 00
协议标识	2字节	00 00
数据长度	2字节	00 06
设备地址	1字节	01
功能码	1字节	10
起始地址	2字节	01 01
寄存器数量	2 字节	00 04

此时，其他设备的CAN端已收到了来自RJ268CAN 模块的 Modbus端发出的帧ID为0x201 的数据帧。

6. 技术规格

连接方式	
以太网	RJ45
CAN	OPEN4接线端子
接口特点	
以太网接口	10/100M自适应
CAN接口	遵循ISO 11898标准，支持CAN2.0A/B
CAN波特率	5kbit/s~1Mbit/s
电气隔离	1500V DC
CAN终端电阻	未集成
供电电源	
供电电压	9-28V DC
供电电流	75mA MAX (28V DC)
环境试验	
工作温度	-40℃~+85℃
工作湿度	15%~90%RH，无凝露

EMC测试	EN 55024:2011-09 EN 55022:2011-12
防护等级	IP 20
基本信息	
外形尺寸	115mm*100mm*22mm
重量	155g

7. 常见问题

1. 是否一定需要使用 120 Ω 终端匹配电阻？

建议120 Ω 终端匹配电阻用于吸收端点反射，提供稳定的物理链路。一条完整的CAN总线上需要有且只需有2个120 Ω 终端电阻，分别接在总线最远的两个节点处。

2. 能否在一条CAN总线上安装多块RJ268CAN模块？

由于CAN总线结构特点，一条总线上可以连接多个CAN节点，所以在不影响总线的前提下，一条CAN总线允许安装多块RJ268CAN网关，实际数量与CAN总线最大节点数有关。

3. RJ268CAN模块最高的数据转换率是多少？

RJ268CAN模块的单一CAN通道最高支持8000 fps的CAN总线数据转换，这里提到的帧是指标准帧8个数据的数据帧，如果是小于8字节数据或者远程帧可能会更快。

4. 为何DAT状态指示灯不亮？

只有当CAN或以太网端有数据传输且模块正处于数据转换中，DAT指示灯才会亮起。

5. 为何调用接口函数时系统非法操作？

首先在使用接口函数时请认真阅读函数说明，保证输入参数合法，特别注意指针（地址）的传递，或参照提供的例子程序，倘若问题还是未能解决，可联系我公司技术支持。

6. RJ268CAN模块的通讯波特率如何设置？

CT01BNEW.exe软件提供一组常用的波特率的设置值，若要使用其他的波特率，请与瑞捷物联有限公司相关人员联系。

7. 系统进入待机或睡眠状态是否影响接收？

会有影响。这时所有处理将停止，最大可能导致硬件接收缓冲溢出错误。若有程序打开设备将尝试阻止系统进入待机或睡眠状态，从而保证系统正常工作。使用RJ268CAN模块时，请禁止系统的待机和睡眠功能。

8. 免责声明

感谢您购买瑞捷物联的CAN系列软硬件产品。CAN系列是温州瑞捷物联科技有限公司的注册商标。本产品及手册为瑞捷物联版权所有。未经许可，不得以任何形式复制翻印。在使用之前，请仔细阅读本声明，一旦使用，即被视为对本声明全部内容的认可和接受。请严格遵守手册、产品说明和相关的法律法规、政策、准则安装和使用该产品。在使用产品过程中，用户承诺对自己的行为及因此而产生的所有后果负责。因用户不当使用、安装、改装造成的任何损失，瑞捷物联将不承担法律责任。

关于免责声明的最终解释权归瑞捷物联所有。

瑞捷物联

附录A: Modbus TCP 协议简介

Modbus通信协议是由 Modicon公司开发的应用在PLC或其他工业控制器上的一种通用语言。通过此协议,各控制器之间可以实现串行通信,Modbus通信协议定义了一个控制器能识别使用的消息结构,描述了主控制器访问从站设备的过程,例如规定从站怎样做出应答响应,检查和报告传输错误等。Modbus协议的通信方式为主从方式。主站首先向从站设备发送通信请求指令,从节点根据请求指令中的功能码向主站发回回答数据。网络中的每个从站设备都必须分配给一个唯一的地址,最多可达31个从站设备。通过多达24种总线命令实现主控制器与从站设备之间的信息交换。从站设备只执行发给自己的指令,对于其它从站地址开头的报文不作应答。这种一问一答的通信模式,大大提高了通信的正确率。因其具有操作简单、高效、通信可靠等优点,Modbus协议已成为一个国际通信标准,得到了国际上大多数工控产品生产厂家的支持。该通信协议已广泛应用于机械、水利、电力、环保等行业设备中。

ModbusTCP通信协议可供自动化设备的监控使用。常见的应用是开发基于该协议的网关,通过网关可以将PLC、I/O模块和其它总线连到以太网上。ModbusTCP是在不改变原有的 Modbus协议基础上,只是将其作为应用层协议简单的移植到TCP/IP协议上。Modbus TCP协议每一个呼叫都要求一个应答。利用TCP/IP协议,通过网页的形式可以使用户界面更加友好。利用网络浏览器就可以查看企业网内部的设备运行情况。Schneider公司已经为 Modbus注册了502端口,这样就可以将实时数据嵌入到网页中,通过在设备中嵌入 Web服务器,就可以将 Web浏览器作为设备的操作终端。但是 Modbus协议本身存在一些缺陷,它不支持诸如基于对象的通信模型等一些正在被广泛采用的网络新技术,用户在使用的时候,不得不手工配置一些参数,比如信息数据类型、寄存器号等等。

A.1 Modbus TCP 协议数据格式

TCP/IP 协议和以太网的链路层校验机制已可保证数据包传递的正确性,因此 Modbus TCP 报文中不再存在CRC-16或LRC 校验域,但需要添加一个 Modbus应用帧头(MBAP)。它可对 Modbus的参数及功能进行解释。每个 TCP/IP 报文仅可含有一个 Modbus帧。

在 Modbus TCP ADU中,MBAP头部占7个字节(含4个子域),及交易标识符TI(Transaction Identifier)、协议标识符 PI(Protocol Identifier),长度标识符L(Length)(占用2字节,指明 Protocol Identifier 和 Data 域的总长度)和单元标识符UI(Unit Identifier)组成。TI 占用2字节,用来标识 Modbus帧的次序,PI 占用2字节,用于确认应用层协议。UI占1字节,用于标识 Modbus设备单元。功能码占1字节,可分为位操作和16位字操作两类。功能码指出要进行的操作,如功能码15代表写多个位寄存器,功能码06表示对独立的16位字寄存器进行写操作。数据域最多可达248字节,其具体格式与功能码相关。当客户机发送请求数据时,数据域给出要操作的寄存器的起始地址(2字节)和个数(1字节);当服务器发送应答数据时,数据域给出被操作的寄存器个数(1字节)及各寄存器状态值。图A.1 给出了 Modbus 与 Modbus TCP 数据帧格式比较。

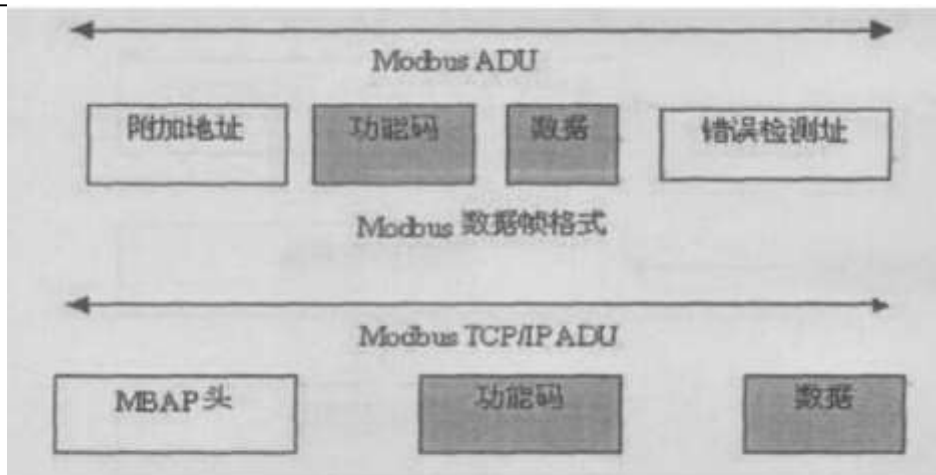


图 A.1 Modbus 与 Modbus TCP/IP 帧格式

Modbus TCP 的ADU数据单元规范如表A.1所示。

	描述	所占字节
MBAP头	传输标识码高位 Hi	1
	传输标识码低位 Lo	1
	协议标识符	2
	长度标识符	2
	单元标识符	1
Modbus请求	功能码	1
	开始地址	2
	寄存器数目	2

表 A.1 Modbus TCP 的ADU数据单元规范

在通过 ModbusTCP 传送数据之前，需要在客户机和服务器之间建立一个TCP/IP 连接。服务器使用端口502作为 Modbus TCP 的连接端口。Modbus TCP连接的建立通常由TCP/IP Socket接口的软件协议自动实现，因此对应用完全透明。一旦客户端和服务端之间的TCP/IP 连接建立，同样的连接可以根据要求的方向用来传输任意数量的用户数据。客户端和服务端还可以同时建立多个TCP/IP连接，最大的连接数量取决于 TCP/IP 接口的规范。

当某一设备发出请求，则其相应的设备要做出响应。响应的数据格式如表B.2 所示。

字节	响应数据
Byte0、 Byte1	传输标识码=0(响应时拷贝该数据)
Byte2、 Byte3	协议标识符
Byte4	长度标识符高字节=0
Byte5	长度标识符低字节 (标识其后有多少个字节)
Byte6	单元标识符(从设备地址)
Byte7	Modbus功能码
Byte8	数据

表 A.2 Modbus TCP 响应数据格式

A.2 Modbus 常用功能码

在 Modbus消息帧的功能码中较常使用的是01、02、03、04、06和 16功能码，使用它们即可实现对从机的数字量和模拟量的读写操作。下面以在RTU 传输模式下通讯为例，对这些功能码进行详细介绍。

功能码	名称	功能说明
01	读取线圈状态	取得一组线圈的当前状态 (ON/OFF)
02	读取输入状态	取得一组开关输入的当前状态 (ON/OFF)
03	读取保持寄存器	在一个或多个保持寄存器中取得当前的二进制值
04	读取输入寄存器	在一个或多个输入寄存器中取得当前的二进制值
05	强置单线圈	强置一个逻辑线圈的通断状态
06	预置单寄存器	把具体二进制值装入一个保持寄存器
07	读取异常状态	取得8个内部线圈的通断状态
08	回送诊断校验	把诊断校验报文送从机，通信诊断
16	预置多寄存器	把具体二进制值装入一串连续的保持寄存器
128~255	保留	用于异常应答

下面是2个 Modbus命令的主从机收发的数据包格式，其余的命令可参照其格式。

(1) 功能码：03H

代码功能：读保持寄存器

说明：读从机保持寄存器的二进制数据，不支持广播。

查询：查询信息规定了要读的寄存器起始地址及寄存器的数量，寄存器寻址起始地址为0000，寄存器1-16所对应的地址分别为0-15。

响应：响应信息中的寄存器数据为二进制数据，每个寄存器分别对应2个字节，第一个字节为高位值数据，第二个字节为低位数据。

(2) 功能码：10H（十进制为16）

代码功能：预置多个寄存器

说明：把数据按顺序预置到各(4x类型)寄存器中，广播时该功能代码可把数据预置到全部从机中的相同类型的寄存器中。需要注意的是该功能代码可越过控制器的内存保护，在寄存器中的预置值一直保持有效，只能由控制器的下一个逻辑来处理寄存器的内容，控制逻辑中无该寄存器程序时，则寄存器中的值保持不变。

查询：信息中规定了要预置的寄存器类型，寄存器寻址的起始地址为0。查询数据区中指定了寄存器的预置值，M84和484型控制器使用10位二进制数据，2个字节，剩余的高6位置0。而其他类型的控制器使用一个16位二进制数据，每个寄存器2个字节。

响应：正常响应返回从机地址、功能代码、起始地址和预置寄存器数。