



# 使用说明书

## RFID 总线控制器

**BAE8M**



## 1. 手册简介

本手册适用于必感电子（苏州）有限公司所生产的 BAE8 系列 RFID 总线控制器（总线模块）。




本手册包含了正确使用本设备所需的全部信息，包括必要功能、性能、使用方法等信息。它既适用于自己调试系统并将其与其他单元（自动化系统、控制器）连接的编程人员和测试/调试人员，也适用于安装扩展或执行故障/错误分析的服务和维护人员。

在安装本设备并投入运行之前，请仔细阅读本手册。本手册包含说明和注释，可帮助您逐步完成安装和调试。这样可以确保本产品无故障使用。熟悉本手册您将可以获得以下好处：

- 确保设备的操作安全
- 帮助您利用设备的全部功能
- 避免错误和相关故障
- 减少维修，避免成本浪费

### 1.1. 相关约定

本手册采用了如下几种醒目标志来表示操作过程中应该注意的地方，这些标志的意义如下：

	该图标表示需引起重视的警告或危险事项。
	该图标表示提醒操作中应注意的事项，如果操作错误可能导致设备损坏等不良后果。
	该图标表示对操作内容的描述进行必要的补充和说明。

### 1.2. 通用安全说明

本设备只能由合格人员进行安装，操作，维修和维护。合格人员是指，具有与电气设备的构造和操作，及其安装有关的技能和知识，并已接受安全培训以识别和避免所涉及危险的人员。

- 用户修改和/或修理是危险的，将使保修失效并使制造商免于承担任何责任。
- 产品维修只能由我司人员进行。未经授权的打开和不适当的维修产品可能导致大量的设备损坏或可能对用户造成人身伤害。

如果发生严重故障，请停止使用该设备，防止设备意外操作。如果需要维修，请将设备退回本公司在当地的代表或销售办事处。

运营公司有责任遵守当地适用的安全规定。将未使用过的设备存放在原始包装中。这为设备提供了最佳的防撞击和防潮保护。请确保环境条件符合本相关规定。

根据欧洲安全标准 EN 60950，本设备只能配合受限功率的电流源来操作设备，即电源必须具备过压过流保护功能。以防止本设备发生电源故障时，影响到其它设备的安全；或者外部设备发生故障，影响到本设备的安全。

### 1.3. 版权声明

必感电子（苏州）有限公司版权所有，并保留对本手册及本声明的最终解释权和修改权

### 1.4. 免责声明

本手册依据现有信息制作，其内容如有更改，恕不另行通知。

## 2. 产品介绍

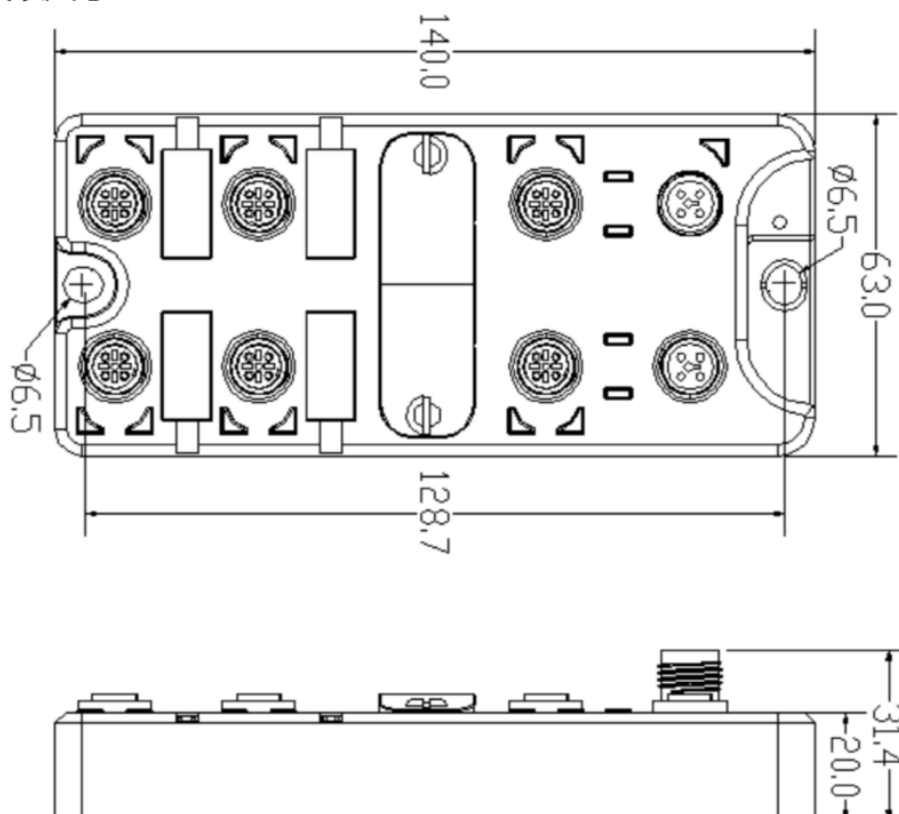
### 2.1. 产品简介

BAE8M 系列 RFID 总线控制器（总线模块）支持 Modbus TCP 协议。包含两个 M12 T-CODE 电源供电接口，两个 M12 D-CODE 5-PIN 总线接口，4 个 M12 A-CODE RFID 读写头接口。

工业以太网传输速率最高支持 100Mbps，可级联多套总线模块到 PLC 中，提供强大的现场采集数据能力。外壳采用轻便坚固的工程塑料，具有连接范围广、通信能力强、环境适应好、防护等级高等特点：

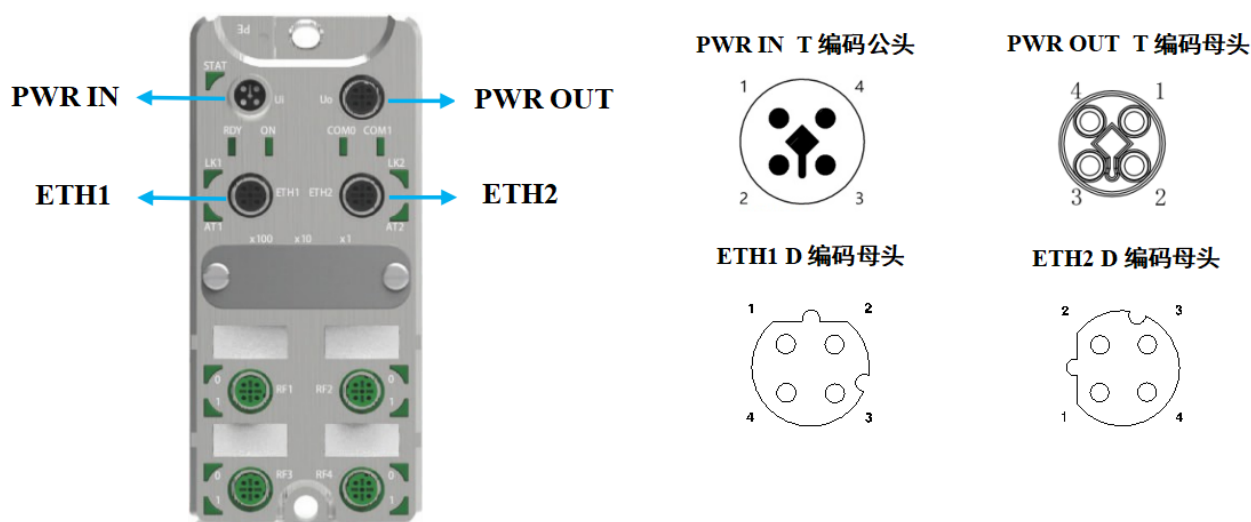
- 可同时连接 4 个 RFID 读写头进行独立操作；
- 支持 Modbus TCP 协议；
- IP67 的防护等级，能够适应油污、粉尘、潮湿等恶劣工况；
- 双网口，集成交换机功能，可组星型网络和树型网络；
- 电源输入带反接保护和 3000W 浪涌保护，RFID 端口带防反接和过压过流保护；

### 2.2. 外观及安装尺寸



## 2.3. 端口介绍

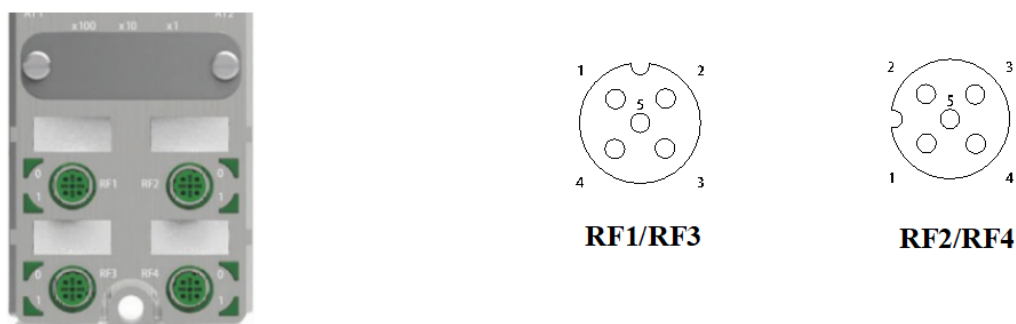
### 2.3.1. 网络及电源端口




### 针脚定义

针脚	ETH (以太网)	PWR(电源)
1	TD+ (黄, 与RJ45 1脚连接)	24V( US+ )
2	RD+ (白, 与RJ45 3脚连接)	GND( UA- )
3	TD- (橙, 与RJ45 2脚连接)	GND( US- )
4	RD- (蓝, 与RJ45 6脚连接)	24V( UA+ )

### 2.3.2. RFID 端口: M12 A-Code 母头, 4 路

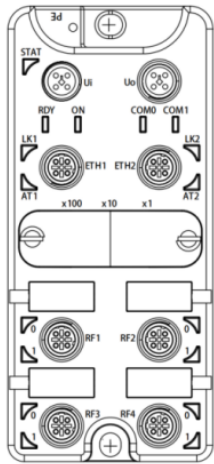


### 针脚定义

针脚	说明	描述
1	24 V	电源+
2	RS485-A	RS485 D+
3	GND	电源-
4	RS485-B	RS485 D-
5	FE	安全接地
	通信线建议使用屏蔽双绞线; 通讯线缆长度: Max<=50m; 通讯线缆线芯使用 24AWG 及以上	

2.4. 指示灯说明


BAE8 系列 RFID 总线控制器总共包含 17 个 LED 状态指示灯，  
分别为系统状态，网络状态，模块状态，总线状态和 RFID 端  
口指示灯。




2.4.1. 系统状态及网络状态 LED 指示灯

指示灯	颜色	含义	状态	描述
STAT	红绿双色 	系统状态	灯灭 ●	未上电或总线模块故障
			绿色常亮 ●	上电正常
			红色长闪 2 次 	网络模块异常 单次闪烁时红灯亮 1000ms
			红色短闪 2 次 	MAC 地址未初始化 单次闪烁时红灯亮 100ms
			红色常亮 ●	模块工作异常/RFID 端口异常
LK1	绿色 	网络状态	灯灭 ●	网络连接不正常
LK2			绿色常亮 ●	网络连接正常
AT1	绿色 	网络状态	灯灭 ●	当前无数据传输
AT2			绿色闪烁 ●●●●	当前数据传输中

2.4.2. 模块状态 LED 指示灯

模块指示灯		描述
RDY	ON	
灯灭 ●	绿色常亮 ●	总线模式或初始状态
灯灭 ●	绿色闪烁 	闪烁频率 1Hz，网关模式
绿色常亮 ●	灯灭 ●	正在进行网络参数设置
灯灭 ●	灯灭 ●	电源供电异常或硬件损坏

### 2.4.3. 总线状态 LED 指示灯

名称	颜色	状态	描述
COM0	绿色 ●	熄灭 ●	未上电或设备故障
		绿色闪烁 	闪烁频率 1Hz, 等待连接
		绿色常亮 ●	已建立 TCP 连接
		绿色闪烁 ●●●	闪烁频率 10Hz, 当前有数据通信
COM1	红色 ●	熄灭 ●	无故障
		红色常亮 ●	检测到 IP 地址冲突

### 2.4.4. RFID 端口 LED 指示灯



工作模式	名称	颜色	状态	描述
总线模式	ON	绿色 ●	绿色常亮 ●	总线模式或初始状态
			灯灭 ●	未上电或端口未使能
	0	绿色 ●	绿色闪烁 ●	与 RFID 通讯正常
			绿色常亮 ●●●	RFID 都区范围内存在标签
			灯灭 ●	RFID 端口正常
	1	红色 ●	红色常亮 ●	RFID 端口电压/电流异常等
			红色闪烁 ●●●●●	与 RFID 通讯异常;
网关模式	ON	绿色 ●	绿色闪烁 	闪烁频率 1Hz, 网关模式
	0	绿色 ●	灯灭 ●	从上电起, 未收到 RFID 的响应数据
			绿色闪烁 ●●●	上一次指令 RFID 响应失败
			绿色常亮 ●	上一次指令 RFID 响应成功
	1	红色 ●	灯灭 ●	无故障
			红色常亮 ●	RFID 端口电压/电流异常等
			红色闪烁 ●●●●●	上次指令未收到与 RFID 响应, 该端口收到 RFID 响应后, 红色 LED 熄灭

注: 关于工作模式的介绍, 请参见第 6 章节。



### 3. 安装说明




#### 3.1. 相关配件订购

	I/O接口 M12 A 编码公头螺钉接线圆形连接器	BKA4H00
	PWR OUT M12 T 编码公头螺钉接线圆形连接器	BKT4H00
	PWR IN M12 T 编码母头螺钉接线圆形连接器	BKT4B00
	ETH 接口 M12 D 编码公头螺钉接线圆形连接器	BKD4H00





#### 3.2. 安装注意事项

为防止产品动作不良、误动作或对性能、设备带来负面影响，请遵守以下事项。

##### 3.2.1. 关于安装场所

	请避免安装在散热量高的设备（加热器、变压器、大容量电阻等）附近
	请避免安装在电磁干扰严重的设备（大型电机、变压器、收发器、变频器、开关电源等）附近。 本产品使用 13.56MHz 的频带与 RFID 读写头（RF）通信。收发器、电机、变频器、开关电源等产生的电波噪音可能会影响产品与 RF 标签之间的通信。周围有这些设备时可能会影响产品与 RF 标签之间的通信或损坏 RF 标签。 在这些设备附近使用本产品时，请先确认其影响后再使用。
	靠近安装多个读写器时，可能会因相互干扰而导致通信性能降低，读写器之间请保持 50cm 以上间距

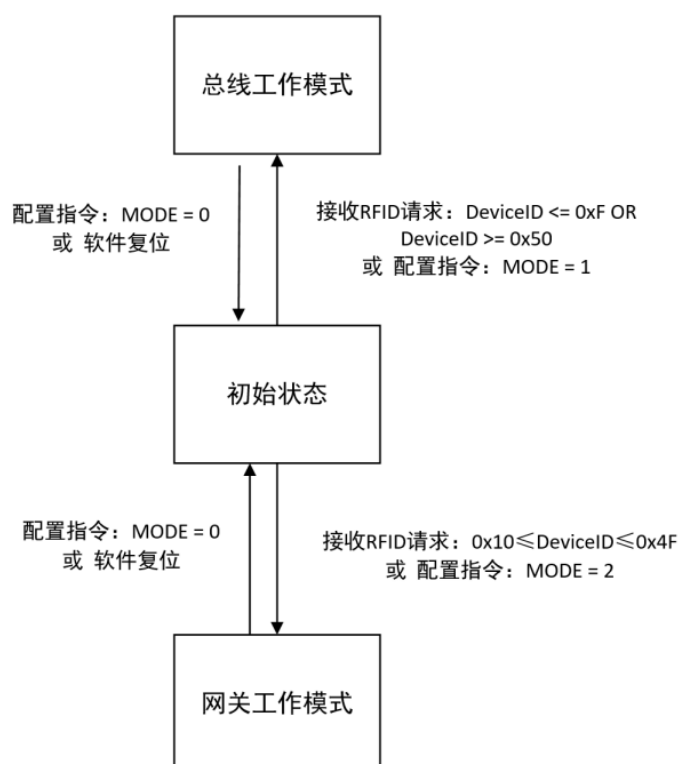
##### 3.2.2. 关于应用事项

	严禁使用 AC 电源。否则有破裂的危险，严重影响到人身及设备的安全
	请使用受限功率的电流源来操作设备，即电源必须具备过压过流保护功能。以防止本设备发生电源故障时，影响到其它设备的安全；或者外部设备发生故障，影响到本设备的安全。
	请避免错误接线。否则有破裂、烧坏的危险。有可能会影响人身及设备的安全。
	读写器天线面与标签面平行时，识别距离最远。标签倾斜安装时通信距离会缩短。标签的安装，请考虑倾斜影响后再安装。

## 4. 软件接口说明

### 4.1. 两种工作模式

BAE8M04 总线控制器支持两种不同的工作模式：网关工作模式和总线工作模式。可通过对指令进行识别自动进入对应的工作模式，也可以通过接收控制器的配置进入相应的工作模式。两种工作模式不可直接切换，若需要切换需要先将模式配置为初始状态或软件复位恢复初始状态。



#### 4.1.1. 网关工作模式

BAE8M04 总线模块作为 MODBUS 网关，将接收到 MODBUS TCP 转换为 MODBUS RTU 协议发送给对应的端口。在进行协议转换时，将 MODBUS TCP 请求的单元标识符作为 RFID 端口编号（如 1 代表 RFID 端口 1），转换后的 MODBUS RTU 报文采用 0 作为设备地址(广播地址)。

MODBUS TCP 请求报文格式					
MBAP 报文头				功能码	数据
事务元标识符	协议标识符	长度	单元标识符		
Hi Lo	Hi Lo	Hi Lo	(ID_TCP)		
2 bytes	2bytes	2bytes	1byte	1byte	N bytes
			0x1*:RF1 端口		
			0x2*:RF2 端口		
			0x3*:RF3 端口		
			0x4*:RF4 端口		



MODBUS RTU 请求报文格式			
设备地址 (ID_RTU)	功能码	数据	CRC 校验 Lo Hi
1byte (ID_TCP 低 4 位)	1byte	N bytes	2 bytes MODBUS RTU

注：具体的寄存器定义，请参见 RFID 技术手册。

#### 4.1.2. 总线工作模式

总线工作模式是指模拟总线的 IO 传输的方式进行工作，对 RFID 的访问都通过 IO 采用命令流来进行，控制器采用 MODBUS TCP 协议来完成对 IO 内存的同步。

#### 4.2. 寄存器地址定义

BAE8M04 总线模块的基本配置主要包括设备信息和连接相关的参数配置，此部分的寄存器掉电可保存，配置后断电重启生效。设备参数如下表所示：

字段	起始地址	结束地址	寄存器数量	操作类型	说明
输入输出内存	0000 H	0040 H	65	RW	网关模式下，作为输入输出内存用于对 RFID 命令的传输
厂商名字	F100 H	F109 H	10	R	
产品代码	F10A H	F113 H	10	R	
版本号	F114 H	F115 H	2	R	软件版本号
产品序列号	F116 H	F11B H	6	R	
MAC 地址	F11C H	F11E H	3	R	
端口号	F11F H	F11F H	1	R	固定值 502
IP 地址	F120 H	F121 H	2	RW	默认：192.168.0.10
子网掩码	F122 H	F123 H	2	RW	默认：255.255.255.0
网关	F124 H	F125 H	2	RW	默认：192.168.0.1
工作模式	F400 H	F400 H	1	RW	掉电不保存 0：初始状态 1：总线模式 2：网关模式
其他					网关模式下，用于直接访问 RFID，具体定义参见 RFID 技术手册

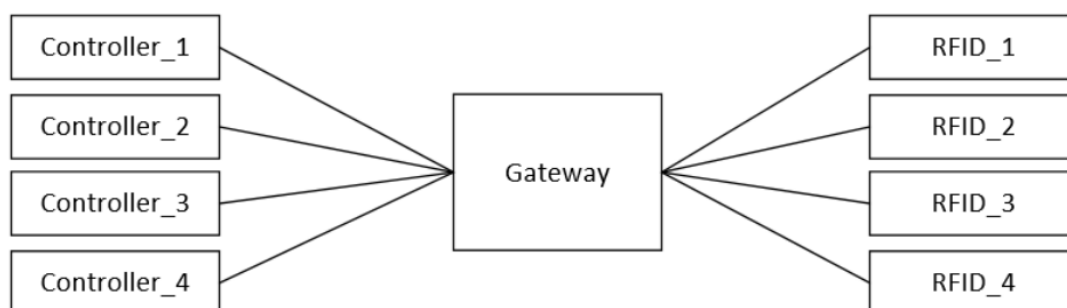
注：可通过拨码盘进行地址的设置，IP 地址采用默认的网段“192.168.0.\*”，拨码可设置最后一段 IP 地址的值，3 个拨码从左到右依次为配置地址的百位、十位、个位。若使用软件配置，配置方法参见 RFID Controller DEMO 使用手册。

### 4.3. 网关工作模式

在网关工作模式下，有两种方式，方式一是与总线模块同时建立 4 个不同的 TCP 连接，这 4 个 TCP 连接的 IP 地址以及端口号（502）都相同，只是通过不同的连接通道（连接 ID）或不同的控制器来建立不同的连接。用户可以分别通过不同的 TCP 连接来访问不同的 RFID 读头；方式二是与总线模块建议一个 TCP 连接，通过同一个 TCP 连接来访问不同的 RFID 读头（通过 MODBUS TCP 请求的单元标识符（ID\_TCP）来区分）。

#### 方式一：

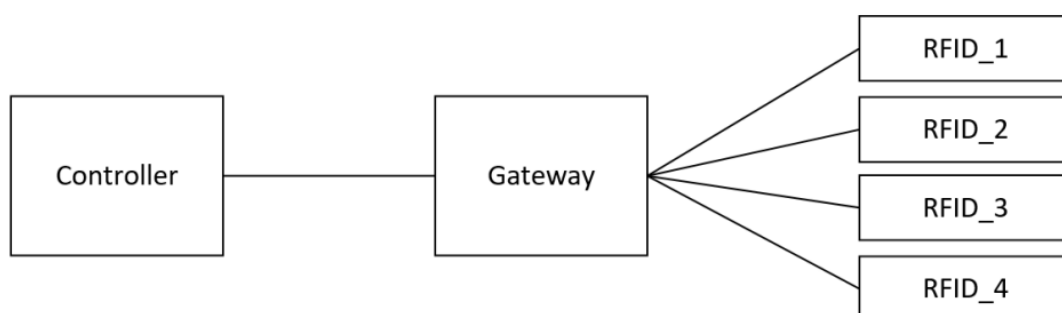
使用不同的 TCP 连接通过网关对 RFID 进行控制时，可以是一个控制器同时与网关建立 4 个连接，也可以是 4 个不同的控制前分别与网关建立连接。



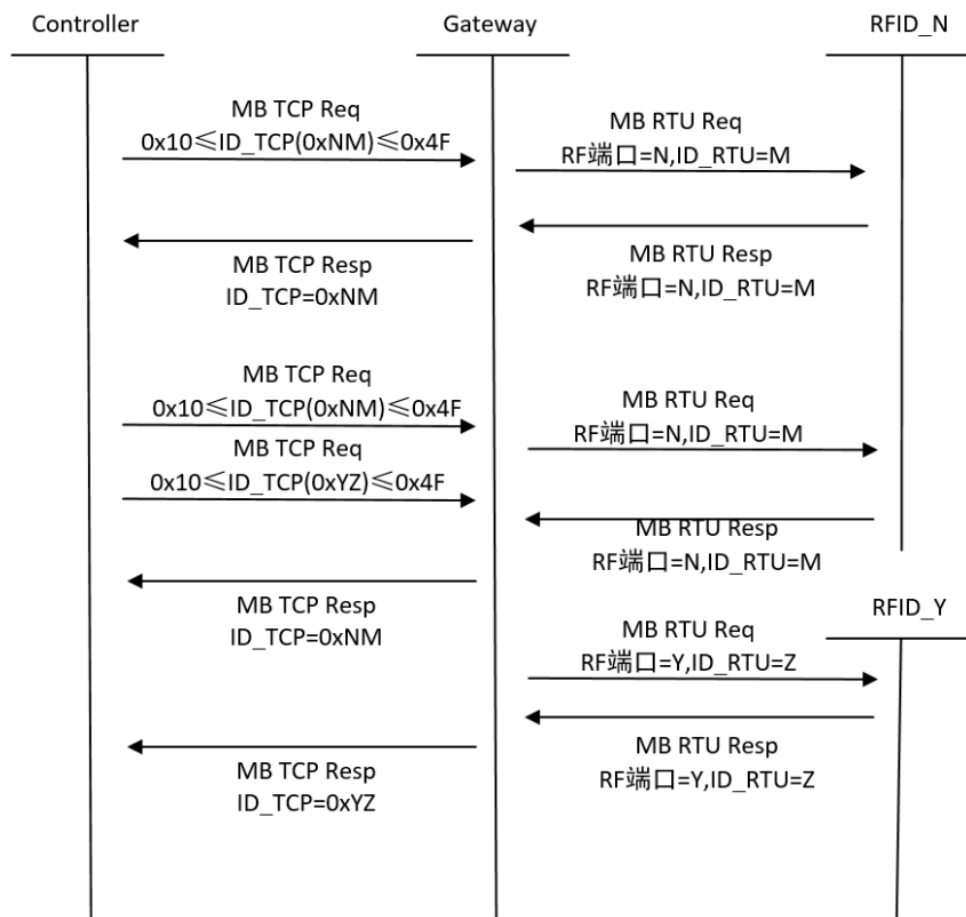
注：不支持使用不同的 TCP 连接控制同一个 RFID 读头。

#### 方式二：

使用同一个 TCP 连接通过网关对不同的 RFID 进行控制时，用户需要通过改变 MODBUS TCP 协议的单元标识符(ID\_TCP)来指定数据发送给哪个 RFID 端口。



在对多读头进行控制时，控制器可先发送 MODBUS 请求给读头 N，等待收到响应后再发送请求给另一个读头。亦可分别先给不同的读头发送请求，再等待其响应。



注：不建议在不等待响应的情况下，连续给同一个读头发送请求。

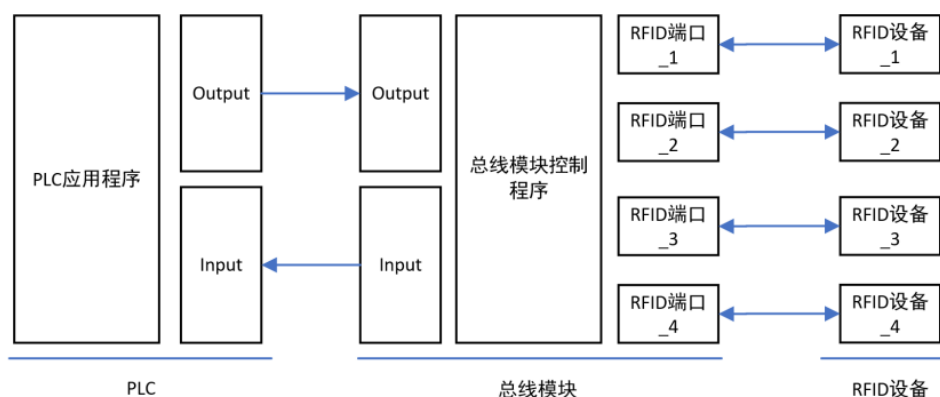
网关通过接收的 MODBUS TCP 请求的单元标识符(ID\_TCP)来判断将数据转发给哪一路 RFID 端口，单元标识符和 RFID 端口的对应关系如下：

单元标识符(ID_TCP)	RFID 端口	MB RTU 设备地址
0x1*	RF1	*, ID_TCP 低 4 位
0x2*	RF2	
0x3*	RF3	
0x4*	RF4	

注：如单元标识符为 0x12，表示给 RF1 端口的 RFID 发送请求，RF1 端口转发请求时使用设备地址为 2。

#### 4.4. 总线工作模式

BAE8M04 总线模块与 PLC 使用 MODBUS TCP 协议进行通信，总线模块内含一片内存用于 IO 数据的同步，PLC 需主动发送 MODBUS 指令进行 IO 数据的同步。以下为 PLC、总线模块、RFID 之间通讯的架构图。



MODBUS 寄存器地址与 IO 数据地址对应关系如下：

字节偏移地址	MB 寄存器地址	Input	Output
0	0_H	1	1
1	0_L	0	0
2	1_H	3	3
3	1_L	2	2
4	2_H	5	5
5	2_L	4	4
6	3_H	7	7
7	3_L	6	6
8	4_H	9	9
9	4_L	8	8
10	5_H	11	11
11	5_L	10	10
.....	.....	.....	.....
118	60_H	119	119
119	60_L	118	118
120	61_H	121	121
121	61_L	120	120
122	62_H	123	123
123	62_L	122	122
124	63_H	125	125
125	63_L	124	124
126	64_H	127	127
127	64_L	126	126
128	65_H	129	129
129	65_L	128	128

#### 4.4.1. Output

PLC 发送给总线模块的数据将通过输出来传输，每个 RFID 都是独立工作的，都有独立的内存来接收命令，输出内存的定义如下：

地址					定义				
预留	RFID-1	RFID-2	RFID-3	RFID-4	Bit4-7	Bit3	Bit2	Bit1	Bit0
0	1	33	65	97	RFU	Mode	Trigger	oToggleBit	Enable
129	2	34	66	98	RFU				
	3	35	67	99	Command/ Write datas				
	4	36	68	100	Start Address(High) / Write datas				
	5	37	69	101	Start Address(Low) / Write datas				
	6	38	70	102	Number of bytes/ Write datas				
	7-32	39-64	71-96	103-128	Write datas				

其中各个字段的功能说明如下：

Enable	使能 RFID 1: 启用 0: 禁用
oToggleBit	翻转位，用于长数据分包传输的握手。在分包传输过程中，若此位翻转，表示已准备好下一帧数据（已接收完上一帧数据）
Trigger	命令触发位： 上升沿：触发当前命令。 下降沿：若当前命令仍在执行则结束当前的命令。否则无效。
Mode	读写器的工作模式： 0: 主动工作模式（在主动工作模式的状态下，有标签在可读区域，将自动上传标签在位信号和标签 UID）； 1: 被动工作模式（根据命令执行读卡操作，不主动监测标签状态）；
RFU	预留
Command	需要执行的命令
Start Address	读取/写入的起始地址
Number of Bytes	读取/写入的字节数
Write Datas	写入的数据

#### 4.4.2. Input

总线模块发送给 PLC 的数据通过输入来传输，每个 RFID 都是独立工作的，都有独立的内存来发送命令响应，输入内存的定义如下：

地址					定义						
预留	RFID-1	RFID-2	RFID-3	RFID-4	Bit6-7	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
0	0	32	64	96	RFU	iToggleBit	Err	Done	Busy	TP	Ready
129	1	33	65	97	RFU				RSSI		IsPassiveMode
	2	34	66	98	Errcode/Read datas						
	3	35	67	99	DataLen/Read datas						
	4-31	36-63	68-95	100-127	Read datas						

其中各个字段的功能说明如下：

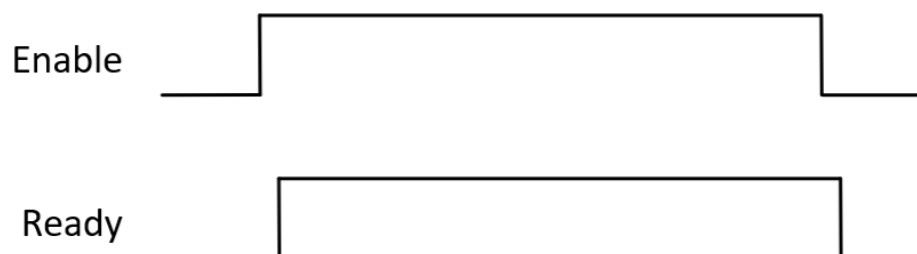
Ready	读写器状态信号，指示读写器是否准备好工作： 1：正常； 0：异常；
TP	标签信号，指示当前标签是否在可读区域： 1：在可读区域； 0：不在可读区域；
Busy	指示网关当前的状态： 1：已接收到命令，正在执行； 0：空闲；
Done	指示当前命令是否执行完毕： 1：执行完毕； 0：正在执行/无有效命令；
Err	指示当前命令是否正确执行： 1：异常；(具体见 ErrCode) 0：正确执行；
iToggleBit	翻转位，用于长数据分包传输的握手。在分包传输过程中，若此位翻转，表示已准备好下一帧数据（已接收完上一帧数据）
IsPassiveMode	指示读头当前的工作模式，工作模式可通过输出区的 Mode 进行修改： 0：自动读卡模式； 1：非自动读卡（触发一次读取一次）；
RSSI	读写器的 RSSI 信号强度等级： 0：当前无标签在可读取区域 1：标签处于临界区域 2：标签处于可工作区域 3：标签处于推荐工作区域
RFU	预留
Errcode	错误码：（由读写器传递过来优先） 0x00:无错误 其他：发生错误，具体错误定义见后文
DataLen	返回的数据长度
Read Datas	读取的数据



### 4.4.3. 时序

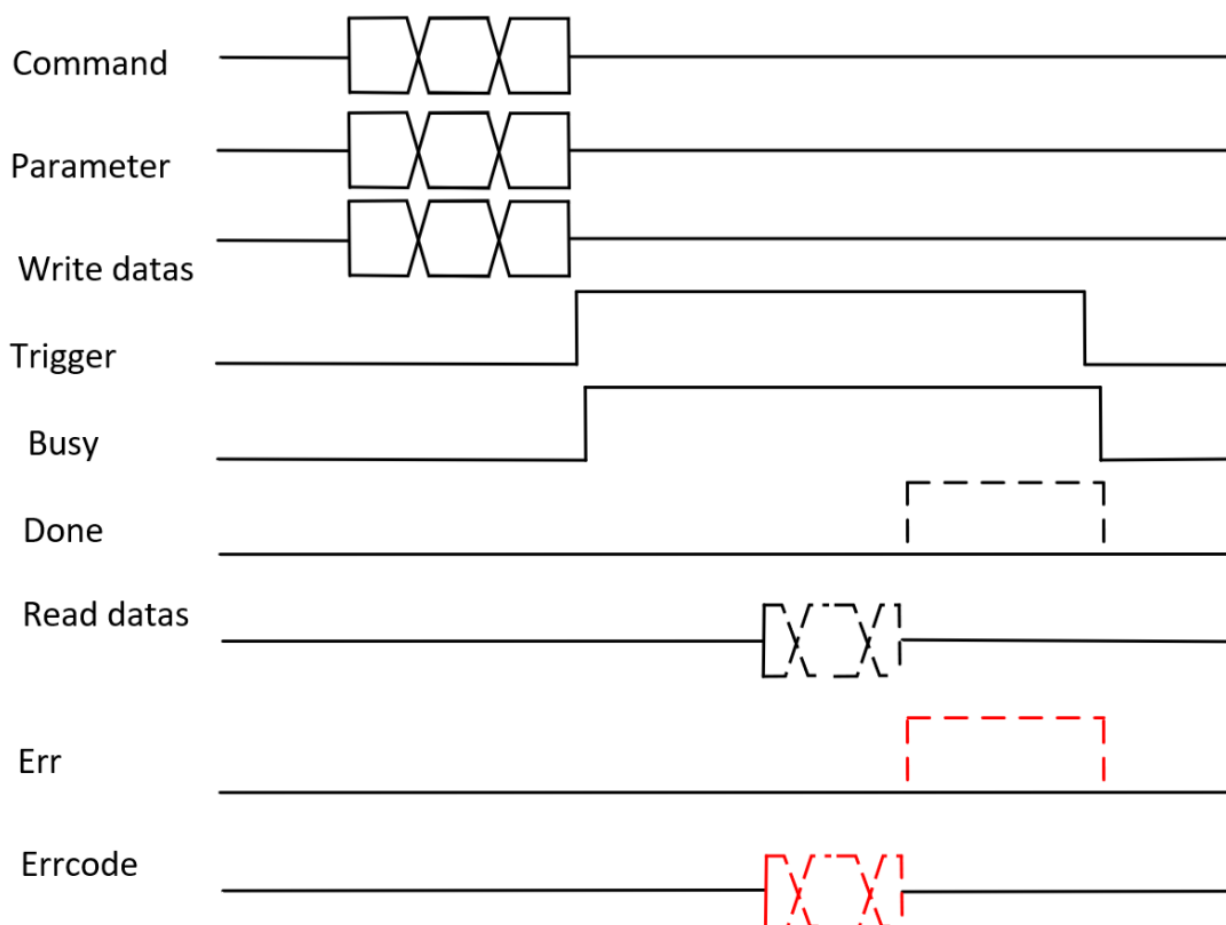
#### 4.4.3.1. 使能 RFID

使能是使 RFID 工作的必要条件，在整个工作期间需要保持 RFID 使能。使能 RFID 涉及到 Enable 和 Ready 两个信号，具体的时序如下所示。若 Enable 置位后，Ready 未置位，则可能总线模块与 RFID 通讯异常。



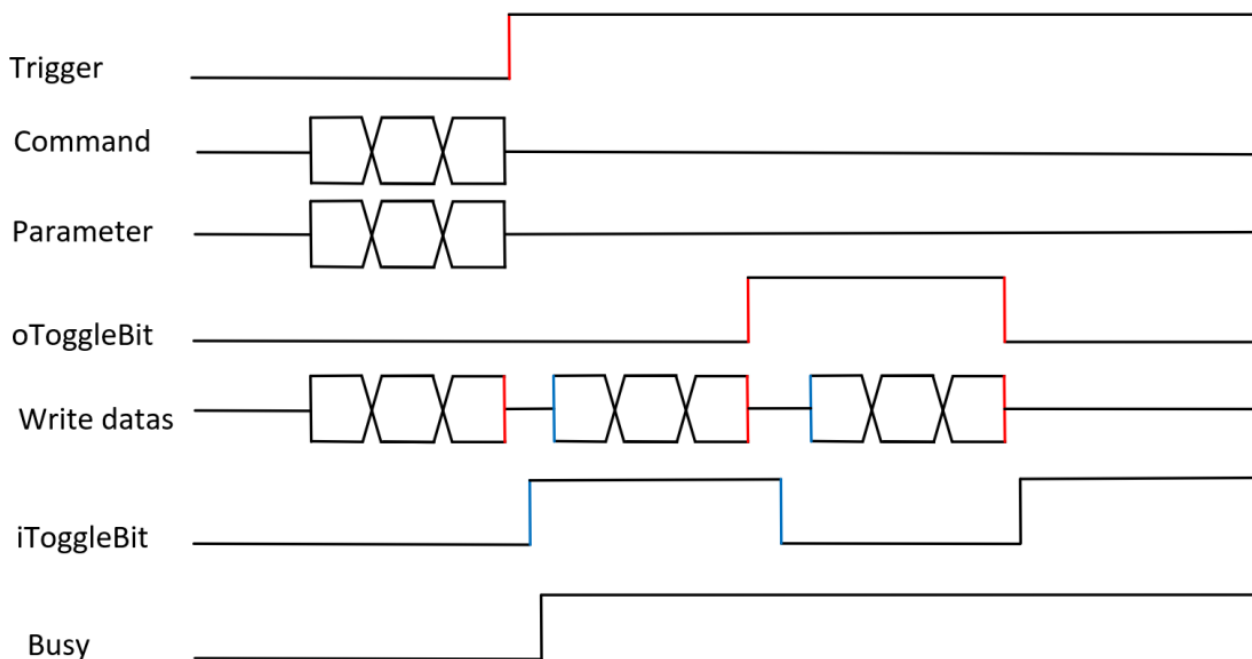
#### 4.4.3.2. 命令执行

命令的执行以 Trigger 上升沿信号开始，在给 Trigger 信号置位之前，先将命令/参数/数据填充好。在命令执行期间保持 Trigger 信号置位，若取消当前命令的执行，将 Trigger 复位即可，Trigger 后输入数据取的状态信息将复位。命令执行完后可从 Read datas/Errcode 取命令执行的结果。



#### 4.4.3.3. 长数据分包传输

在实际应用的过程中，可能存在一次无法传输完数据的情况，此时需要分包进行传输。以 PLC 启动长数据传输为例，时序图如下：



#### 4.5. 总线控制器支持的命令

总线模块支持支持读取标签和写标签命令，读取标签命令的通讯格式如下：

读标签	命令值	参数			备注
请求	0x11	Start Address (2 Bytes)	Number of Bytes (1 Byte)	—	Output
正确响应	—	Errcode (1 Byte, 0x00)	Datalen (1 Byte)	Read Datas (N Bytes)	Input
错误响应	—	Errcode (1 Byte, 非 0x00)	Datalen (1 Byte, 0x00)	—	Input

读取标签命令的通讯格式如下：

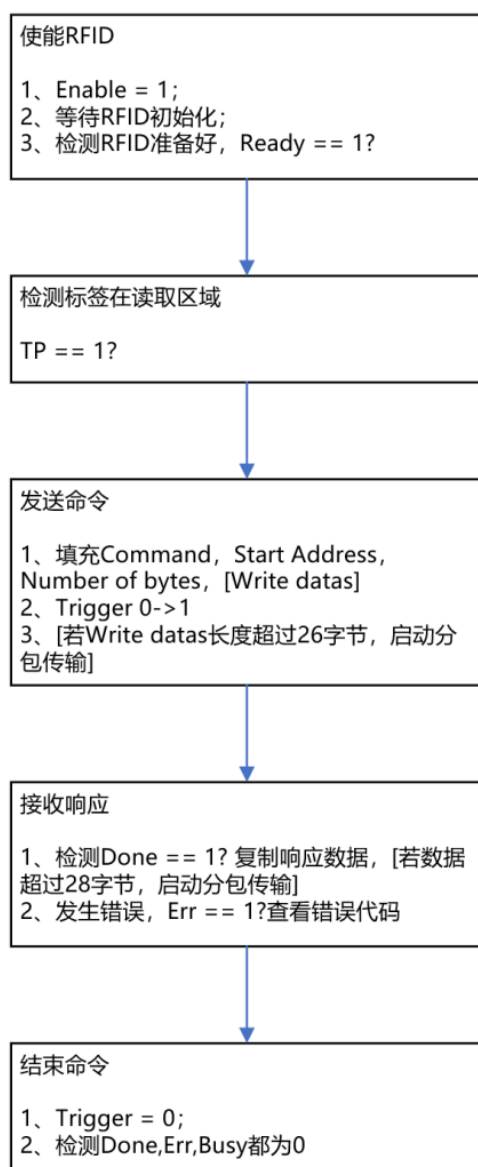
写标签	命令值	参数			备注
请求	0x12	Start Address (2 Bytes)	Number of Bytes (1 Byte)	Write Datas (N Bytes)	Output
正确响应	—	Errcode (1 Byte, 0x00)	Datalen (1 Byte, 0x00)	—	Input
错误响应	—	Errcode (1 Byte, 非 0x00)	Datalen (1 Byte, 0x00)	—	Input

## 4.6. 错误代码

错误码		定义	说明
十进制	十六进制		
0	0x00	无错误	
144	0x90	无标签响应	此时标签可能不在读取范围
145	0x91	射频数据错误	此时可能有强电磁干扰导致数据传输出错，或者数据传输一半标签离开读取区域
147	0x93	标签内存锁定	标签内存已经锁定，禁止写入
149	0x95	标签离开	读取到一半数据，标签离开
150	0x96	标签离开	写一半数据，标签离开
161	0xA1	射频数据发射异常	射频数据无法发送出去
176	0xB0	参数错误	

## 4.7. 应用举例

在实际应用时，建议按照如下的流程进行操作：



### 4.7.1. RFID 监控

- RFID 工作状态控制

Output	Input
Enable: 1/0	Ready: 1/0

- 将 RFID 设置为主动工作模式，并对 RFID 进行监控

Output	Input
使能读写器并设置为主动工作模式 Enable:1 Mode:0	Ready: 1
	检测到有 RFID 标签 Datalen: UID LEN Read datas: UID RSSI: 1-3 TP: 1
检测到 TP 置 1，获取标签 UID	

### 4.7.2. RFID 标签内存读取

- 从 RFID 标签的地址 0x0004 开始，读取 16 个字节

Output	Input	
Enable:1	Ready: 1	
	检测到标签在读取区域，TP：1	
发送读取命令 Command:0x11 Start Address:0x0004 Number of bytes:0x10 Trigger:1	置 Busy:1	
	读取正确 Errcode:0x00 Datalen: 0x10 Read datas:读取的数据 Err:0 Done:1	读取出错 Errcode:非 0x00 Datalen: 0x00 Err:1 Done:1
拷贝数据，结束任务 Trigger:0	Done:0 Busy:0 Err:0	

- 从 RFID 标签的地址 0 开始，读取 64 字节

Output	Input
Enable:1	Ready: 1
	检测到标签在读取区域，TP： 1
发送读取命令 Command:0x11 Start Address:0x0000 Number of bytes:0x40 Trigger:1	置 Busy:1
	读取正确 Errcode:0x00 Datalen: 0x40 Read datas(4-31):28 字节读取数据 Err:0 Done:1
拷贝数据，oToggleBit 翻转通过 总线模块可进行下一帧传输	Read datas(2-31):30 字节读取数据 iToggleBit 翻转通知 PLC 可进行数据接收（若读取的数据更多增加此步骤，直到所有的数据传输完）
拷贝数据，oToggleBit 翻转通过 总线模块可进行下一帧传输	Read datas(4-9):6 字节读取数据 iToggleBit 翻转通知 PLC 可进行数据接收
拷贝数据，结束任务 Trigger:0	Done:0 Busy:0 Err:0

#### 4.7.3. RFID 标签内存写入

- 从 RFID 标签的地址 0x0004 开始，写入 16 个字节

Output	Input	
Enable:1	Ready: 1	
	检测到标签在读取区域，TP： 1	
发送写入命令 Command:0x12 Start Address:0x0004 Number of bytes:0x10 Write Datas(6-21):16 字节数据 Trigger:1	置 Busy:1	
	写入成功 Errcode:0x00 Datalen: 0x00 Err:0 Done:1	写入失败 Errcode:非 0x00 Datalen: 0x00 Err:1 Done:1

结束任务 Trigger:0	Done:0 Busy:0 Err:0
-------------------	---------------------------

● 从 RFID 标签的地址 0 开始, 写入 64 字节

Output	Input	
Enable:1	Ready: 1	
	检测到标签在读取区域, TP: 1	
发送写入命令 Command:0x12 Start Address:0x0000 Number of bytes:0x40 Write Datas(6-31):26 字节数据 Trigger:1	置 Busy:1 拷贝数据, iToggleBit 翻转通知 PLC 可进行下一帧传输	
Write datas(2-31): 30 字节数据 oToggleBit 翻转通过总线模块可进行数据接收	拷贝数据, iToggleBit 翻转通知 PLC 可进行下一帧传输	
Write datas(2-9): 8 字节数据 oToggleBit 翻转通过总线模块可进行数据接收	拷贝数据	
	写入成功 Errcode:0x00 Datalen: 0x00 Err:0 Done:1	写入失败 Errcode:非 0x00 Datalen: 0x00 Err:1 Done:1
结束任务 Trigger:0	Done:0 Busy:0 Err:0	

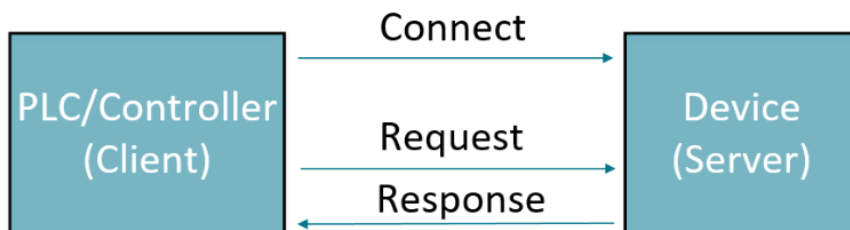


## 5. 技术参数

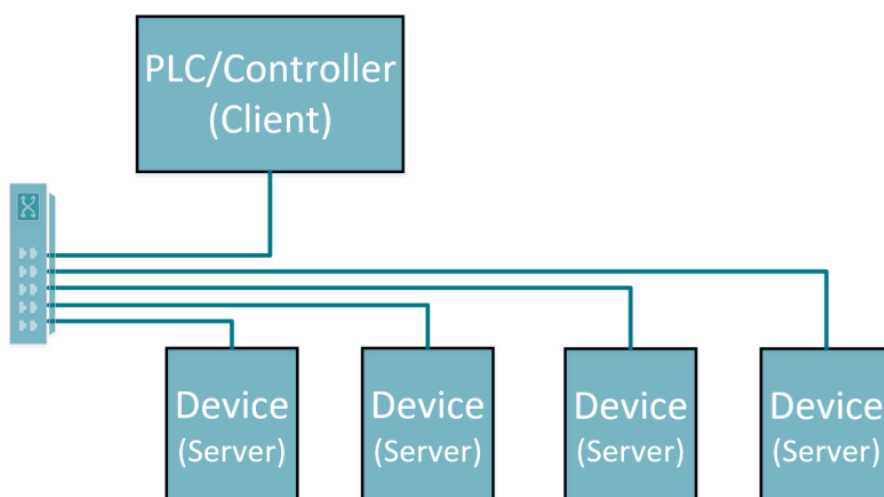
型号		BAE8M04
物理参数	产品尺寸	140.0 * 63.0 * 31.4mm
	壳体材质	锌合金
电源	额定电压	18-30V DC
	额定电流	IMAX≤0.3A@24V (不含 RFID)
	电源接口	T-CODE 公头/母头 4 针
	电源保护	反接保护、3000W 浪涌保护
通讯	通讯协议	Modbus TCP
	网络接口	双网口, 符合 IEE802.3 标准
	系统拓扑结构	星型结构, 树型结构
	通讯线缆长度	Max=100m
	通讯接口	D-CODE M12 母头, 4 针
RFID 端口	RFID 数量	4 个独立通道(RS485)
	RFID 接口	A-CODE M12 母头
	负载能力	VOUT=24V±20%, IOUT≤0.7A
	电路保护	电源防反接、过压过流保护
环境适应性	工作温度	-25°C~+70°C
	存储温度	-40°C~+85°C
	湿度	5%~95%RH (无凝露)
	防护等级	IP67, EN 60529
	抗振动	2 mm (f= 5...29.5 Hz) , EN 60068-2-6 7 g (f= 29.5...150 Hz) , EN 60068-2-6
	静电放电抗扰度 ESD	接触放电, 8KV, 过 A 级 空气放电, 15KV, 过 A 级 IEC 61000-4-2
认证及声明	CE	EN 61000-6-4 EN 61000-6-2
	RoHs 指令	2011/65/EU 2015/863/EU

## 6. ModBus TCP 协议

在一个以太网的通讯网络里面，设备作为服务器，PLC(控制器)作为客户端。在通讯之前需要先建立连接，连接由客户端发起。通讯采用问答的方式，由 PLC 发起。



建立通讯需要确认好 IP 地址和端口号，MODBUS TCP 固定的端口号为 502。在建立连接前，需要确认 PLC 与 RFID 在同一个网段。当有多个设备接入到网络时，需要将每个 RFID 都配置不同的 IP 地址，多个设备可以通过交换机连接到一起。

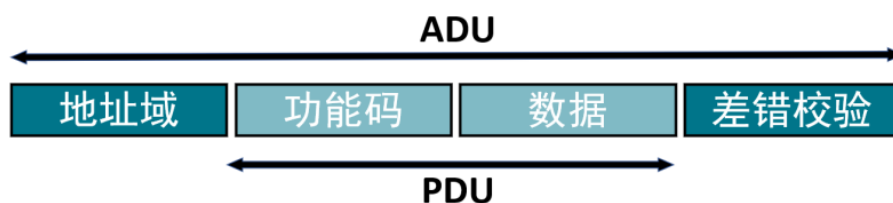


### 6.1. 设备支持的命令

此设备支持的 MODBUS 指令如下：

命令码		说明
十六进制	十进制	
03	3	读多个寄存器
06	6	写单个寄存器
10	16	写多个寄存器

MODBUS 协议定义了一个与基础通信层无关的简单协议数据单元（PDU）。特定总线或网络上的 MODBUS 协议映射能够在应用数据单元（ADU）上引入一些附加域。



## MODBUS RTU ADU

MODBUS RTU 的 ADU 包含地址域、PDU 和差错校验，其中地址域为设备地址，差错校验位 CRC 校验。

设备地址	功能码	数据	CRC 校验 Lo Hi
1byte	1byte	N bytes	2 bytes MODBUS RTU

- 设备地址：从站设备地址，组网应用 1-16，点对点通讯 0
- CRC 校验：CRC16-MODBUS，对前面的所有数据进行校验

## MODBUS TCP ADU

MODBUS RTU 的 ADU 包含地址域、PDU，其中地址域为 MBAP 报文头

MBAP 报文头				功能码	数据
事务元标识符 Hi Lo	协议标识符 Hi Lo	长度 Hi Lo	单元标识符		
2 bytes	2bytes	2bytes	1byte	1byte	N bytes

- 事务元标识符：事务处理的识别码
- 协议标识符：MODBUS = 0
- 长度：以下字节的数量
- 单元标识符：默认 FFH

## 6.2. 读多个寄存器

读取多个寄存器的请求 ADU 如下：

协议	地址域					功能码	数据		差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 03H	地址 Hi Lo	数量 Hi Lo	CRC Lo Hi
RTU	——	——	——	——	1byte	1byte	2 bytes	2 bytes	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	——				——

- 事务元标识符：事务处理的识别码
- 协议标识符：MODBUS = 0
- 长度：以下字节的数量，此处为 6
- 单元标识符：默认 FFH
- 地址：从站设备地址，组网应用 1-16，点对点通讯 0
- 命令码：读取多个寄存器的命令码固定为 3
- 首寄存器地址：需要读取的第一个寄存器的地址
- 寄存器数量：需要读取的寄存器的数量，当读取的区域为标签内存区域时，取值范围为  $1 \leq N \leq 120$ ，其他情况下，取值范围为  $1 \leq N \leq 123$

读取多个寄存器的正常响应 ADU 如下：

协议	地址域					功能码	数据		差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 03H	字节数	寄存器值 Hi Lo	CRC Lo Hi
RTU	——	——	——	——	1byte	1byte	1 bytes	2bytes (寄存器 1)	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	——			..... 2bytes (寄存器 N)	——

- 命令码：与请求一致
- 读取的字节数：寄存器数量的 2 倍
- 寄存器值：需要读取的寄存器的值

读取多个寄存器的异常响应 ADU 如下：

协议	地址域					功能码	数据	差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 83H	错误码	CRC Lo Hi
RTU	——	——	——	——	1byte	1byte		2 bytes
TCP	2bytes	2bytes	2bytes	1byte	——		1byte	——

### 6.3. 写单个寄存器

写单个寄存器的请求 ADU 如下：

协议	地址域					功能码	数据		差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 6H	地址 Hi Lo	寄存器值 Hi Lo	CRC Lo Hi
RTU	——	——	——	——	1byte	1byte			2 bytes
TCP	2bytes	2bytes	2bytes	1byte	——		2 bytes	2 bytes	——

- 命令码：读取多个寄存器的命令码固定为 6
- 寄存器地址：需要操作的寄存器地址
- 寄存器值：需要操作的寄存器的值

写单个寄存器的正常响应 ADU 如下：

协议	地址域					功能码	数据		差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 6H	地址 Hi Lo	寄存器值 Hi Lo	CRC Lo Hi
RTU	——	——	——	——	1byte	1byte			2 bytes
TCP	2bytes	2bytes	2bytes	1byte	——		2 bytes	2 bytes	——

- 地址：与请求一致
- 命令码：与请求一致
- 寄存器地址：与请求一致
- 寄存器值：与请求一致

写单个寄存器的异常响应 ADU 如下：

协议	地址域					功能码	数据	差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 86H	错误码	CRC Lo Hi
RTU	——	——	——	——	1byte	1byte	1byte	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	——			——

## 6.4. 写多个寄存器

写多个寄存器的请求 ADU 如下：

协议	地址域					功能码	数据				差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 10H	寄存器地址 Hi Lo	寄存器数量 Hi Lo	字节数	寄存器值 Hi Lo	CRC Lo Hi
RTU	——	——	——	——	1byte	1byte	2 bytes	2 bytes	1byte	2bytes (第 1 个寄存器)	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	——					..... 2bytes (第 1 个寄存器)	——

- 命令码：读取多个寄存器的命令码固定为 10H
- 寄存器地址：需要操作的首个寄存器地址
- 寄存器数量：需要操作的寄存器的数量，当操作的区域为标签内存区域时，取值范围为  $1 \leq N \leq 120$ ，其他情况下，取值范围为  $1 \leq N \leq 121$
- 字节数：寄存器值总共占用的字节数， $2 * \text{寄存器数量}$
- 寄存器值：需要操作的寄存器的值

写多个寄存器的正常响应 ADU 如下：

协议	地址域					功能码	数据		差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 10H	寄存器地址 Hi Lo	寄存器数量 Hi Lo	CRC Lo Hi
RTU	——	——	——	——	1byte	1byte	2 bytes	2 bytes	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	——				——

- 命令码：与请求一致
- 寄存器地址：与请求一致
- 寄存器数量：与请求一致

写多个寄存器的异常响应 ADU 如下：

协议	地址域					功能码	数据	差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 90H	错误码	CRC Lo Hi
RTU	——	——	——	——	1byte	1byte	1byte	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	——			——

必感电子（苏州）有限公司  
地址：苏州工业园区唯西路96号  
网址：[www.bitsense.cn](http://www.bitsense.cn)  
邮箱：[info@bitsense.cn](mailto:info@bitsense.cn)