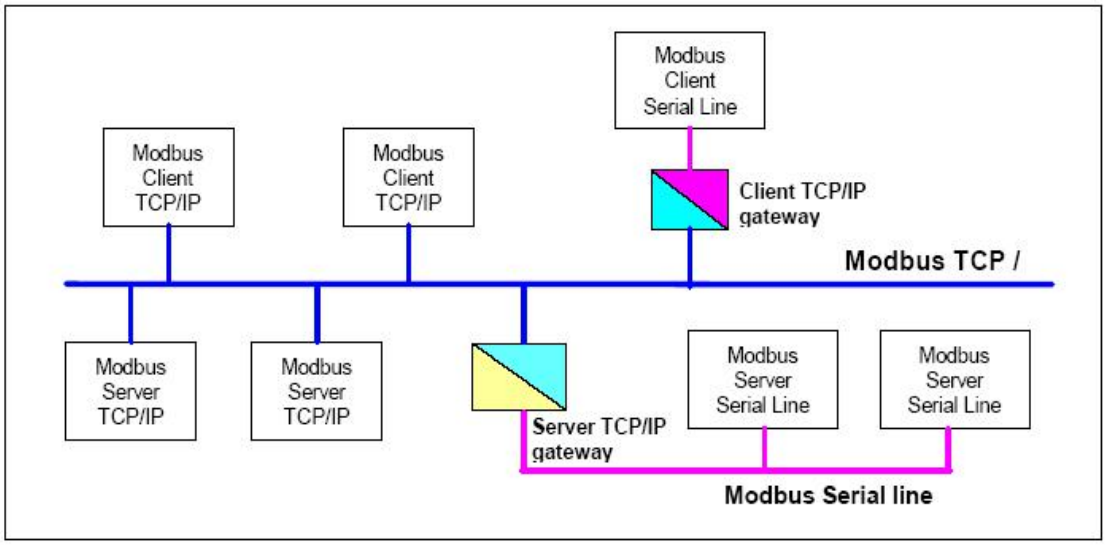
DAM-E3021A Modbus TCP 地址分配表

1 MODBUS 简介

工业控制已从单机控制走向集中监控、集散控制，如今已进入网络时代，工业控制器连网也为网络管理提供了方便。MODBUS 就是工业控制器的网络协议中的一种。

MODBUS 规约作为一个通讯协议是由 MODICON 公司在 1979 年首次提出的，它是一个标准的、真正开放的、在工业自动化领域应用最广泛的网络通讯协议。通过此协议，控制器相互之间、控制器经由网络（例如以太网）和其它设备之间可以通信。它已经成为一通用工业标准。通过这一协议，不同厂商生产的控制设备可以连成工业网络，进行集中监控。

Modbus TCP 协议是 MODBUS 协议另一版本，它于 1999 年被开发出来以允许 Internet 用户访问以太网设备。由于没有任何商业利益驱使，Modbus TCP 协议的开放性及用户对它的熟悉程度再加上其应用的简单易学，现在 Modbus TCP 已经成为世界领先的工业以太网协议。



此协议定义了一个控制器能认识使用的消息结构,而不管它们是经过何种网络进行通信的。它描述了控制器请求访问其它设备的过程，如果回应来自其它设备的请求，以及怎样侦测错误并记录。它制定了消息域格局和内容的公共格式。

当在 Modbus 网络上通信时，此协议决定了每个控制器须要知道它们的设备地址，识别按地址发来的消息，决定要产生何种行动。如果需要回应，控制器将生成反馈信息并用 Modbus 协议发出。在其它网络上，包含了 Modbus 协议的消息转换为在此网络上使用的帧

或包结构。这种转换也扩展了根据具体的网络解决节地址、路由路径及错误检测的方法。

标准的 Modbus 口是使用 RS-232C 兼容串行接口，它定义了连接口的针脚、电缆、信号位、传输波特率、奇偶校验。控制器能直接或经由 Modem 组网。

控制器通信使用主—从技术，即仅设备（**主设备**）能初始化传输（查询）。其它设备（**从设备**）根据**主设备**查询提供的数据做出相应反应。典型的**主设备**：主机和可编程仪表。典型的**从设备**：可编程控制器。

主设备可单独和**从设备**通信，也能以广播方式和所有**从设备**通信。如果单独通信，**从设备**返回消息作为回应，如果是以广播方式查询的，则不作任何回应。Modbus 协议建立了**主设备**查询的格式：设备（或广播）地址、功能代码、所有要发送的数据、错误检测域。

从设备回应消息也由 Modbus 协议构成，包括确认要行动的域、任何要返回的数据、和错误检测域。如果在消息接收过程中发生错误，或**从设备**不能执行其命令，**从设备**将建立错误消息并把它作为回应发送出去。

在其它网络上，控制器使用对等技术通信，故任何控制都能初始和其它控制器的通信。这样在单独的通信过程中，控制器既可作为**主设备**也可作为**从设备**。提供的多个内部通道可允许同时发生的传输进程。

在消息位，Modbus 协议仍提供了主—从原则，尽管网络通信方法是“对等”。如果控制器发送消息，它只是作为**主设备**，并期望从**从设备**得到回应。同样，当控制器接收到消息，它将建立一**从设备**回应格式并返回给发送的控制器。

主设备查询

查询消息中的功能代码告之被选中的**从设备**要执行何种功能。数据段包含了**从设备**要执行功能的任何附加信息。例如功能代码 03 是要求**从设备**读保持寄存器并返回它们的内容。数据段必须包含要告之**从设备**的信息：从何寄存器开始读及要读的寄存器数量。错误检测域为**从设备**提供了一种验证消息内容是否正确的方法。

从设备回应

如果从设备产生正常的回应，在回应消息中的功能代码是在查询消息中的功能代码的回应。数据段包括了从设备收集的数据：像寄存器值或状态。如果有错误发生，功能代码将被修改以用于指出回应消息是错误的，同时数据段包含了描述此错误信息的代码。错误检测域允许主设备确认消息内容是否可用。

每个 MODBUS 帧都包括地址域　功能域　数据域 **错误检测域**

2 工作方式

2.1 MODBUS RTU 方式

地址	功能代码	数据数量	数据 1	...	数据 n	CRC 高字节	CRC 低字节

地址域　功能域　　数据域　　错误检测域

帧定界：在 MODBUS RTU 方式下，每两个字符之间发送或者接收的时间间隔不能超过 1.5 倍字符传输时间。如果两个字符时间间隔超过了 3.5 倍字符传输时间，就认为一帧数据已经接收完成，新的一帧数据传输开始。

MODBUS message

Start	Address	Function	Data	CRC Check	End
≥ 3.5 char	8 bits	8 bits	N x 8 bits	16 bits	≥ 3.5 char

2.2 MODBUS ASCII 方式

:	地址	功能代码	数据数量	数据 1	...	数据 n	LRC 高字节	LRC 低字节	回车	换行

地址域　功能域　数据域　　错误检测域

帧定界：在 MODBUS ASCII 方式下，一个 8 位的数据使用两个 ASCII 字符来表示。比如 16 进制的 0x3A 用字符“3”和字符“A”表示。其中“:”表示帧的起始，“CR LF”表示帧的结束。

Start	Address	Function	Data	LRC	End
1 char :	2 chars	2 chars	0 up to 2x252 char(s)	2 chars	2 chars CR,LF

2.3 MODBUS TCP 方式

MBAP Header	功能代码	数据数量	数据 1	...	数据 n

协议头　　功能域　　数据域

帧定界：在 MODBUS TCP 方式下，由于模块的地址由 IP 地址确定，所以不再有地址

域内容，考虑到 TCP 网络是可靠的数据传输网络，故不再有校验数据。但是考虑到在 IP 网上数据到达的顺序可能与我们预期的数据不一致，故增加了一个数据序号，考虑到在 MODBUS TCP 协议上承载 MODBUS 协议，还在头部数据中增加了一个地址域。

Fields	Length	Description -	Client	Server
Transaction Identifier	2 Bytes	Identification of a MODBUS Request / Response transaction.	Initialized by the client	Recopied by the server from the received request
Protocol Identifier	2 Bytes	0 = MODBUS protocol	Initialized by the client	Recopied by the server from the received request
Length	2 Bytes	Number of following bytes	Initialized by the client (request)	Initialized by the server (Response)
Unit Identifier	1 Byte	Identification of a remote slave connected on a serial line or on other buses.	Initialized by the client	Recopied by the server from the received request

MBAP Header

3 支持命令

目前，本公司所生产的以太网分布式采集模块均采用该协议，MODBUS TCP 方式。支持的功能码主要包括如下几种：

01 READ COIL STATUS

02 READ INPUT STATUS

03 READ HOLDING REGISTERS

04 READ INPUT REGISTERS

05 FORCE SINGLE COIL

06 PRESET SINGLE REGISTER

15 FORCE MULTIPLE COILS

16 FORCE MULTIPLE REGISTERS

20 READ FILE RECORD

21 WRITE FILE RECORD

4 地址映射表

4.1 读继电器状态

功能码：01

说明：读取输出继电器的状态

数据说明：

地址	描述	说明
00001	第 01 路开关量输出当前状态	＝1 导通 ＝0 未导通
00002	第 02 路开关量输出当前状态	＝1 导通 ＝0 未导通
00003	第 03 路开关量输出当前状态	＝1 导通 ＝0 未导通
00004	第 04 路开关量输出当前状态	＝1 导通 ＝0 未导通
00005	第 05 路开关量输出当前状态	＝1 导通 ＝0 未导通
00006	第 06 路开关量输出当前状态	＝1 导通 ＝0 未导通
00007	第 07 路开关量输出当前状态	＝1 导通 ＝0 未导通
00008	第 08 路开关量输出当前状态	＝1 导通 ＝0 未导通
保留		
00065	第 01 路开关量输出安全状态	＝1 导通 ＝0 未导通
00066	第 02 路开关量输出安全状态	＝1 导通 ＝0 未导通
00067	第 03 路开关量输出安全状态	＝1 导通 ＝0 未导通
00068	第 04 路开关量输出安全状态	＝1 导通 ＝0 未导通
00069	第 05 路开关量输出安全状态	＝1 导通 ＝0 未导通
00070	第 06 路开关量输出安全状态	＝1 导通 ＝0 未导通
00071	第 07 路开关量输出安全状态	＝1 导通 ＝0 未导通
00072	第 08 路开关量输出安全状态	＝1 导通 ＝0 未导通
保留		
00097	通道 0 脉冲输出启动停止	=1 启动；=0 停止
00098	通道 1 脉冲输出启动停止	=1 启动；=0 停止
00099	通道 2 脉冲输出启动停止	=1 启动；=0 停止
00100	通道 3 脉冲输出启动停止	=1 启动；=0 停止
00101	通道 4 脉冲输出启动停止	=1 启动；=0 停止
00102	通道 5 脉冲输出启动停止	=1 启动；=0 停止
00103	通道 6 脉冲输出启动停止	=1 启动；=0 停止
00104	通道 7 脉冲输出启动停止	=1 启动；=0 停止
保留		
00649	DI0 锁存状态	=1 锁存；=0 未锁存
00650	DI1 锁存状态	=1 锁存；=0 未锁存
00651	DI2 锁存状态	=1 锁存；=0 未锁存
00652	DI3 锁存状态	=1 锁存；=0 未锁存
00653	DI4 锁存状态	=1 锁存；=0 未锁存
00654	DI5 锁存状态	=1 锁存；=0 未锁存
00655	DI6 锁存状态	=1 锁存；=0 未锁存
00656	DI7 锁存状态	=1 锁存；=0 未锁存
保留		

00665	DI0 过滤使能	=1 使能；=0 除能
00666	DI1 过滤使能	=1 使能；=0 除能
00667	DI2 过滤使能	=1 使能；=0 除能
00668	DI3 过滤使能	=1 使能；=0 除能
00669	DI4 过滤使能	=1 使能；=0 除能
00670	DI5 过滤使能	=1 使能；=0 除能
00671	DI6 过滤使能	=1 使能；=0 除能
00672	DI7 过滤使能	=1 使能；=0 除能
保留		
00681	DI0 反向	=1 反向；=0 非反向
00682	DI1 反向	=1 反向；=0 非反向
00683	DI2 反向	=1 反向；=0 非反向
00684	DI3 反向	=1 反向；=0 非反向
00685	DI4 反向	=1 反向；=0 非反向
00686	DI5 反向	=1 反向；=0 非反向
00687	DI6 反向	=1 反向；=0 非反向
00688	DI7 反向	=1 反向；=0 非反向
保留		
00697	通道 DI0 计数器启动、停止	=1 启动；=0 停止
00698	通道 DI1 计数器启动、停止	=1 启动；=0 停止
00699	通道 DI2 计数器启动、停止	=1 启动；=0 停止
00700	通道 DI3 计数器启动、停止	=1 启动；=0 停止
00701	通道 DI4 计数器启动、停止	=1 启动；=0 停止
00702	通道 DI5 计数器启动、停止	=1 启动；=0 停止
00703	通道 DI6 计数器启动、停止	=1 启动；=0 停止
00704	通道 DI7 计数器启动、停止	=1 启动；=0 停止
保留		
00713	通道 DI0 清除计数值	1= 清除；=0 不清除
00714	通道 DI1 清除计数值	1= 清除；=0 不清除
00715	通道 DI2 清除计数值	1= 清除；=0 不清除
00716	通道 DI3 清除计数值	1= 清除；=0 不清除
00717	通道 DI4 清除计数值	1= 清除；=0 不清除
00718	通道 DI5 清除计数值	1= 清除；=0 不清除
00719	通道 DI6 清除计数值	1= 清除；=0 不清除
00720	通道 DI7 清除计数值	1= 清除；=0 不清除
保留		
00729	通道 DI0 计数器溢出标志位	1= 溢出；=0 未溢出
00730	通道 DI1 计数器溢出标志位	1= 溢出；=0 未溢出
00731	通道 DI2 计数器溢出标志位	1= 溢出；=0 未溢出
00732	通道 DI3 计数器溢出标志位	1= 溢出；=0 未溢出
00733	通道 DI4 计数器溢出标志位	1= 溢出；=0 未溢出
00734	通道 DI5 计数器溢出标志位	1= 溢出；=0 未溢出
00735	通道 DI6 计数器溢出标志位	1= 溢出；=0 未溢出

00736	通道 DI7 计数器溢出标志位	1= 溢出；=0 未溢出
保留		
00745	通道 DI0 计数值保存使能	1= 保存；=0 不保存
00746	通道 DI1 计数值保存使能	1= 保存；=0 不保存
00747	通道 DI2 计数值保存使能	1= 保存；=0 不保存
00748	通道 DI3 计数值保存使能	1= 保存；=0 不保存
00749	通道 DI4 计数值保存使能	1= 保存；=0 不保存
00750	通道 DI5 计数值保存使能	1= 保存；=0 不保存
00751	通道 DI6 计数值保存使能	1= 保存；=0 不保存
00752	通道 DI7 计数值保存使能	1= 保存；=0 不保存
保留		

MODBUS 请求

域名称	字节数	取值
功能码	1byte	0x01
起始地址	2byte	0x0000 to 0xFFFF
读取数量	2byte	1 to 2000(0x7D0)

MODBUS 响应

域名称	字节数	取值
功能码	1byte	0x01
字节计数	1byte	n =（读取数量+7）/ 8
线圈状态	nbyte	

错误响应

域名称	字节数	取值
功能码	1byte	0x01+0x80
错误代码	1byte	0x1 or 0x2

举例说明

请求		响应	
域名称	数据（hex）	域名称	数据（hex）
功能码	01	功能码	01
起始地址高(字节)	00	字节计数	03
起始地址低(字节)	13	27（h）～05 状态	CD
读取数量高(字节)	00	35（h）～28 状态	6B
读取数量低(字节)	13	38（h）～36 状态	05

4.2 读开关量输入

功能码：02

说明：读取输入开关量的状态

数据说明：

地址	描述	说明
10001	第 01 路开关量输入状态	＝0 断开，＝1 吸合
10002	第 02 路开关量输入状态	＝0 断开，＝1 吸合
10003	第 03 路开关量输入状态	＝0 断开，＝1 吸合
10004	第 04 路开关量输入状态	＝0 断开，＝1 吸合
10005	第 05 路开关量输入状态	＝0 断开，＝1 吸合
10006	第 06 路开关量输入状态	＝0 断开，＝1 吸合
10007	第 07 路开关量输入状态	＝0 断开，＝1 吸合
10008	第 08 路开关量输入状态	＝0 断开，＝1 吸合
保 留		

MODBUS 请求

域名称	字节数	取值
功能码	1byte	0x02
起始地址	2byte	0x0000 to 0xFFFF
读取数量	2byte	1 to 2000(0x7D0)

MODBUS 响应

域名称	字节数	取值
功能码	1byte	0x02
字节计数	1byte	n＝（读取数量+7）/ 8
输入状态	nbyte	

错误响应

域名称	字节数	取值
功能码	1byte	0x02+0x80
错误代码	1byte	0x1 or 0x2

举例说明

请求		响应	
域名称	数据（hex）	域名称	数据（hex）
功能码	02	功能码	02
起始地址高(字节)	00	字节计数	03
起始地址低(字节)	C4	204(h)～197 状态	AC
读取数量高(字节)	00	212(h)～205 状态	DB
读取数量低(字节)	16	218(h)～213 状态	35

4.3 读保持寄存器

功能码：03

说明：读取保持寄存器的值

数据说明：读取的是十六位整数或无符号整数

地址	描述	说明
40001	通道 DO0 工作模式	0x01 直接输出模式； 0x02 低到高延时输出； 0x03 高到低延时输出； 0x04 脉冲连续输出； 0x05 脉冲固定输出；
40002	通道 DO1 工作模式	
40003	通道 DO2 工作模式	
40004	通道 DO3 工作模式	
40005	通道 DO4 工作模式	
40006	通道 DO5 工作模式	
40007	通道 DO6 工作模式	
40008	通道 DO7 工作模式	
保留		
40033	通道 0 输出高电平时间	
40034	通道 0 输出低电平时间	
40035	通道 1 输出高电平时间	
40036	通道 1 输出低电平时间	
40037	通道 2 输出高电平时间	
40038	通道 2 输出低电平时间	
40039	通道 3 输出高电平时间	
40040	通道 3 输出低电平时间	
40041	通道 4 输出高电平时间	
40042	通道 4 输出低电平时间	
40043	通道 5 输出高电平时间	
40044	通道 5 输出低电平时间	
40045	通道 6 输出高电平时间	
40046	通道 6 输出低电平时间	
40047	通道 7 输出高电平时间	
40048	通道 7 输出低电平时间	
保留		
40097	通道 0 增加脉冲输出数量	
40098	通道 1 增加脉冲输出数量	
40099	通道 2 增加脉冲输出数量	
40100	通道 3 增加脉冲输出数量	
40101	通道 4 增加脉冲输出数量	
40102	通道 5 增加脉冲输出数量	
40103	通道 6 增加脉冲输出数量	

40104	通道 7 增加脉冲输出数量	
保留		
40129	DO0 固定脉冲输出数量	
40130	DO1 固定脉冲输出数量	
40131	DO2 固定脉冲输出数量	
40132	DO3 固定脉冲输出数量	
40133	DO4 固定脉冲输出数量	
40134	DO5 固定脉冲输出数量	
40135	DO6 固定脉冲输出数量	
40136	DO7 固定脉冲输出数量	
保留		
40161	通道 0 上升沿/下降沿延时输出时间	
40162	通道 1 上升沿/下降沿延时输出时间	
40163	通道 2 上升沿/下降沿延时输出时间	
40164	通道 3 上升沿/下降沿延时输出时间	
40165	通道 4 上升沿/下降沿延时输出时间	
40166	通道 5 上升沿/下降沿延时输出时间	
40167	通道 6 上升沿/下降沿延时输出时间	
40168	通道 7 上升沿/下降沿延时输出时间	
保留		
40649	通道 DI0 工作模式	0x01 DI 量输入模式; 0x02 低到高锁存模式; 0x03 高到低锁存模式； 0x04 计数工作模式； 0x05 频率工作模式;
40650	通道 DI1 工作模式	
40651	通道 DI2 工作模式	
40652	通道 DI3 工作模式	
40653	通道 DI4 工作模式	
40654	通道 DI5 工作模式	
40655	通道 DI6 工作模式	
40656	通道 DI7 工作模式	
保留		
40665	通道 DI0 计数值高位	
40666	通道 DI0 计数值低位	
40667	通道 DI1 计数值高位	
40668	通道 DI1 计数值低位	
40669	通道 DI2 计数值高位	
40670	通道 DI2 计数值低位	
40671	通道 DI3 计数值高位	
40672	通道 DI3 计数值低位	
40673	通道 DI4 计数值高位	
40674	通道 DI4 计数值低位	

40675	通道 DI5 计数值高位	
40676	通道 DI5 计数值低位	
40677	通道 DI6 计数值高位	
40678	通道 DI6 计数值低位	
40679	通道 DI7 计数值高位	
40680	通道 DI7 计数值低位	
保留		
40697	DI0 高电平宽度	
40698	DI1 高电平宽度	
40699	DI2 高电平宽度	
40700	DI3 高电平宽度	
40701	DI4 高电平宽度	
40702	DI5 高电平宽度	
40703	DI6 高电平宽度	
40704	DI7 高电平宽度	
保留		
40713	DI0 低电平宽度	
40714	DI1 低电平宽度	
40715	DI2 低电平宽度	
40716	DI3 低电平宽度	
40717	DI4 低电平宽度	
40718	DI5 低电平宽度	
40719	DI6 低电平宽度	
40720	DI7 低电平宽度	
保留		
40513	看门狗控制寄存器	Bit0：使能； Bit1：溢出； Bit2：复位。
40514	看门狗溢出时间寄存器	超时时间,单位 s
40515	看门狗复位寄存器	0xaa 0x55
40516	UDP 搜索端口号	5000~60000（出厂设置 5001）
40517	TCP 连接空闲超时控制寄存器	0：除能；1：使能
40518	TCP 连接空闲超时寄存器	0~65535 单位 s
40519	重新启动寄存器	0x00：不启动； 0x01：重新启动
40520	恢复出厂设置	0x00：不恢复 0x01: 恢复

MODBUS 请求

域名称	字节数	取值

功能码	1byte	0x03
起始地址	2byte	0x0000 to 0xFFFF
读取数量	2byte	1 to 125(0x7D)

MODBUS 响应

域名称	字节数	取值
功能码	1byte	0x03
字节计数	1byte	2n
输入状态	2nbyte	

错误响应

域名称	字节数	取值
功能码	1byte	0x03+0x80
错误代码	1byte	0x1 or 0x2

举例说明

请求		响应	
域名称	数据（hex）	域名称	数据（hex）
功能码	03	功能码	03
起始地址高(字节)	00	字节计数	02
起始地址低(字节)	08	输入寄存器高	00
读取数量高(字节)	00	输入寄存器低	0A
读取数量低(字节)	01		

注 1：脉冲输出电平宽度单位是：毫秒；看门狗定时长度单位是：毫秒

注 2：看门狗控制寄存器的最高位上电为 1，可以做模块复位判断。

4.4 设置单个继电器

功能码：05

MODBUS 请求

域名称	字节数	取值
功能码	1byte	0x05
设置地址	2byte	0x0000 to 0xFFFF
设置内容	2byte	0x0000 or 0xFF00 0x0000 释放继电器 0xFF00 吸合继电器

MODBUS 响应

域名称	字节数	取值
功能码	1byte	0x05

设置地址	2byte	0x0000 to 0xFFFF
设置内容	2byte	0x0000 or 0xFF00

错误响应

域名称	字节数	取值
功能码	1byte	0x05+0x80
错误代码	1byte	0x1 or 0x2

举例说明

请求		响应	
域名称	数据（hex）	域名称	数据（hex）
功能码	05	功能码	05
设置地址高(字节)	00	设置地址高(字节)	00
设置地址低(字节)	05	设置地址低(字节)	05
设置内容高(字节)	FF	设置内容高(字节)	FF
设置内容低(字节)	00	设置内容低(字节)	00

4.5 设置单个保持寄存器

功能码：06

MODBUS 请求

域名称	字节数	取值
功能码	1byte	0x06
设置地址	2byte	0x0000 to 0xFFFF
设置内容	2byte	0x0000 to 0xFFFF

MODBUS 响应

域名称	字节数	取值
功能码	1byte	0x06
设置地址	2byte	0x0000 to 0xFFFF
设置内容	2byte	0x0000 to 0xFFFF

错误响应

域名称	字节数	取值
功能码	1byte	0x06+0x80
错误代码	1byte	0x1 or 0x2

举例说明

请求		响应	
域名称	数据（hex）	域名称	数据（hex）
功能码	06	功能码	06

设置地址高(字节)	00	设置地址高(字节)	00
设置地址低(字节)	08	设置地址低(字节)	08
设置内容高(字节)	00	设置内容高(字节)	00
设置内容低(字节)	19	设置内容低(字节)	19

4.6 设置多个继电器

功能码：0F

MODBUS 请求

域名称	字节数	取值
功能码	1byte	0x0F
设置起始地址	2byte	0x0000 to 0xFFFF
设置长度	2byte	0x0000 to 0x07B0
字节计数	1byte	n
设置内容	nbyte	

MODBUS 响应

域名称	字节数	取值
功能码	1byte	0x0F
设置起始地址	2byte	0x0000 to 0xFFFF
设置长度	2byte	0x0000 to 0x07B0

错误响应

域名称	字节数	取值
功能码	1byte	0x0F+0x80
错误代码	1byte	0x1 or 0x2

举例说明

请求		响应	
域名称	数据（hex）	域名称	数据（hex）
功能码	0F	功能码	0F
设置地址高(字节)	00	设置地址高(字节)	00
设置地址低(字节)	13	设置地址低(字节)	13
设置数量高(字节)	00	设置数量高(字节)	00
设置数量低(字节)	0A	设置数量低(字节)	0A
字节计数	02		
设置内容高(字节)	CD		
设置内容低(字节)	01		

4.7 设置多个保持寄存器

功能码：10

MODBUS 请求

域名称	字节数	取值
功能码	1byte	0x10
设置起始地址	2byte	0x0000 to 0xFFFF
设置长度	2byte	0x0000 to 0x07B0
字节计数	1byte	2n
设置内容	2nbyte	

MODBUS 响应

域名称	字节数	取值
功能码	1byte	0x10
设置起始地址	2byte	0x0000 to 0xFFFF
设置长度	2byte	0x0000 to 0x07B0

错误响应

域名称	字节数	取值
功能码	1byte	0x10+0x80
错误代码	1byte	0x1 or 0x2

举例说明

请求		响应	
域名称	数据（hex）	域名称	数据（hex）
功能码	10	功能码	10
设置地址高(字节)	00	设置地址高(字节)	00
设置地址低(字节)	01	设置地址低(字节)	01
设置数量高(字节)	00	设置数量高(字节)	00
设置数量低(字节)	02	设置数量低(字节)	02
字节计数	04		
设置内容高(字节)	00		
设置内容低(字节)	0A		
设置内容高(字节)	01		
设置内容低(字节)	02		

4.8 读文件记录

功能码：14/06

读取文件记录，在 MODBUS 中，认为文件是一个由 16BIT 位串构成的数组，其寻址是

按照地址进行的。文件读取，规定读取的起始地址和读取长度，改变读取地址和长度就可以遍历整个文件。文件没有名字，只有编号。本系统仅支持一次读写一个文件。

MODBUS 请求

域名称	字节数	取值
功能码	1byte	0x14
字节计数	1byte	0x07 to 0xF5
子功能码	1byte	0x06
文件号	2byte	0x0000 to 0xFFFF
记录号	2byte	0x0000 to 0x270F
读取长度	2byte	n
子功能码	1byte	0x06
……	……	

MODBUS 响应

域名称	字节数	取值
功能码	1byte	0x14
字节计数	1byte	0x07 to 0xF5
子功能字节计数	1byte	0x07 to 0xF5
子功能码	1byte	0x06
数据	2nbyte	

错误响应

域名称	字节数	取值
功能码	1byte	0x14+0x80
错误代码	1byte	0x1 or 0x2

举例说明

请求		响应	
域名称	数据（hex）	域名称	数据（hex）
功能码	14	功能码	14
字节计数	07	字节计数	06
子功能码	06	响应计数	05
文件号高(字节)	00	子功能码	06
文件号低(字节)	04	记录数据高(字节)	0D
记录号高(字节)	00	记录数据低(字节)	FE
记录号低(字节)	01	记录数据高(字节)	00
读取长度高(字节)	00	记录数据低(字节)	20
读取长度低(字节)	02		

4.9 写文件记录

功能码：15/06

MODBUS 请求

域名称	字节数	取值
功能码	1byte	0x15
字节计数	1byte	0x07 to 0xF5
子功能码	1byte	0x06
文件号	2byte	0x0000 to 0xFFFF
记录号	2byte	0x0000 to 0x270F
写长度	2byte	n
数据	2nbyte	
……	……	

MODBUS 响应

域名称	字节数	取值
功能码	1byte	0x15
字节计数	1byte	0x07 to 0xF5
子功能码	1byte	0x06
文件号	2byte	0x0000 to 0xFFFF
记录号	2byte	0x0000 to 0x270F
写长度	2byte	n
数据	2nbyte	

错误响应

域名称	字节数	取值
功能码	1byte	0x15+0x80
错误代码	1byte	0x1 or 0x2

举例说明

请求		响应	
域名称	数据（hex）	域名称	数据（hex）
功能码	15	功能码	15
字节计数	0B	字节计数	0B
子功能码	06	子功能码	06
文件号高(字节)	00	文件号高(字节)	00
文件号低(字节)	04	文件号低(字节)	04
记录号高(字节)	00	记录号高(字节)	00
记录号低(字节)	01	记录号低(字节)	01
写长度高(字节)	00	写长度高(字节)	00
写长度低(字节)	02	写长度低(字节)	02
写数据	4byte	写数据	4byte

4.10 EEPROM 分配

```
//file 0
#define MODULE_NET_ADDR                 0x0000
#define MODULE_VER_ADDR                 0x0020
//file 1
#define NET_CONFIG_ADDR                 0x0000
#define MODULE _NAME _ADDR              0x0020
//file 2 to file 7
……
```

说明：

EEPROM 为 8kbyte 容量，分为 8 个文件块，每个大小为 1kbyte。

1、NET_CONFIG_ADDR

恢复出厂设置的网络配置参数。结构如下表：

字节数	4	4	4	6	2	2	2	2
内容	IP 地址	子网 掩码	默认 网关	MAC 地址	TCP 端口号	Http 端口号	UDP 端口号	获取 IP 方式

2、MODULE_VER_ADDR

模块版本信息。结构如下表：

字节	42byte
内容	DAM-E3016　V6.20 2006.09.01 ID:DAME123456