MODBUS 规约中文说明书

北京阿尔泰科技

ART Technology Development Co.,Ltd.

MODBUS 规约

MODBUS 规约是 MODICOM 公司开发的一个为很多厂商支持的开放规约

Modbus 协议是应用于电子控制器上的一种通用语言。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。有了它，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。

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。

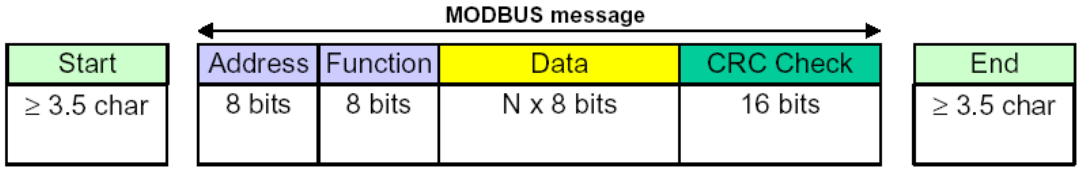
每个 MODBUS 帧都包括**地址域　功能域　数据域 错误检测域**

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 :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 倍的字符传输时间，规约就认为一帧数据已经接收，新的一帧数据传输开始。



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：

“:”帧起始　　**“CR LF”**帧结束

ASCII 方式用两个 ASCII 字符表示一个 8 位数据，比如 16 进制的 3A 用字符“3”和字符“A”表示。

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

支持的命令

我们目前所支持的功能码非常有限，主要包括：

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

1. 读开关量输出状态

功能码：01
说明：读取开关量输出的状态

数据说明：

地址(16 进制)	描述	说明
1000	第 01 路开关量输出状态	
1001	第 02 路开关量输出状态	
1002	第 03 路开关量输出状态	
1003	第 04 路开关量输出状态	
1004	第 05 路开关量输出状态	
1005	第 06 路开关量输出状态	
1006	第 07 路开关量输出状态	
1007	第 08 路开关量输出状态	
1008	第 09 路开关量输出状态	
1009	第 10 路开关量输出状态	
100a	第 11 路开关量输出状态	
100b	第 12 路开关量输出状态	
100c	第 13 路开关量输出状态	
100d	第 14 路开关量输出状态	
100e	第 15 路开关量输出状态	
100f	第 16 路开关量输出状态	
保留		

MODBUS 请求

功能码	1 BYTE	0x01
起始地址	2 BYTE	0x0000 TO 0xFFFF
读取数量	2 BYTE	1 TO 2000(0x7D0)

MODBUS 响应

功能码	1 BYTE	0x01
字节计数	1 BYTE	N
线圈状态	**n** BYTE	**n** =N or N+1

N =读取数量/8　　如果余数不为 0 则 N=N+1

错误 响应

功能码	1 BYTE	0x01+ 0x80
错误代码	1 BYTE	0x1 or 0x2

举例

请求		响应	
模块地址	数据（hex）	模块地址	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）～20 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

2. 读开关量输入状态

功能码：02

说明：读取开关量输入的状态

数据说明：

地址(十六进制)	描述	说明
1000	第 01 路开关量输入状态	
1001	第 02 路开关量输入状态	
1002	第 03 路开关量输入状态	
1003	第 04 路开关量输入状态	
1004	第 05 路开关量输入状态	
1005	第 06 路开关量输入状态	
1006	第 07 路开关量输入状态	
1007	第 08 路开关量输入状态	
1008	第 09 路开关量输入状态	
1009	第 10 路开关量输入状态	
100a	第 11 路开关量输入状态	
100b	第 12 路开关量输入状态	
100c	第 13 路开关量输入状态	
100d	第 14 路开关量输入状态	
100e	第 15 路开关量输入状态	
100f	第 16 路开关量输入状态	
保 留		

MODBUS 请求

功能码	1 BYTE	0x02
起始地址	2 BYTE	0x0000 TO 0xFFFF
读取数量	2 BYTE	1 TO 2000(0x7D0)

MODBUS 响应

功能码	1 BYTE	0x02
字节计数	1 BYTE	N
输入状态	**n** BYTE	**n** =N or N+1

N =读取数量/8　　如果余数不为 0 则 N=N+1

错误 响应

功能码	1 BYTE	0x02+ 0x80
错误代码	1 BYTE	0x1 or 0x2

举例

请求		响应	
模块地址	数据（hex）	模块地址	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

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合整数

地址	描述	说明
1000	第 01 路模拟量输入量程	单端电压输入： 00：±5V 01：±10V 02：0~5V 03：0~10V 差分电压输入： 04：±5V 05：±10V 06：0~5V 07：0~10V 单端电流输入： 0A：4~20mA
1001	第 02 路模拟量输入量程	同上
1002	第 03 路模拟量输入量程	同上
1003	第 04 路模拟量输入量程	同上
1004	第 05 路模拟量输入量程	同上
1005	第 06 路模拟量输入量程	同上
1006	第 07 路模拟量输入量程	同上
1007	第 08 路模拟量输入量程	同上
1008	第 01 路模拟量输出量程	00：±5V 01：±10V 02：0~5V 03：0~10V
1009	第 02 路模拟量输出量程	同上
100a	第 03 路模拟量输出量程	同上
100b	第 04 路模拟量输出量程	同上
保 留		

1010	第 01 路模拟量输出值	输出值浮点表示的低 16 位
1011	第 01 路模拟量输出值	输出值浮点表示的高 16 位
1012	第 02 路模拟量输出值	输出值浮点表示的低 16 位
1013	第 02 路模拟量输出值	输出值浮点表示的高 16 位
1014	第 03 路模拟量输出值	输出值浮点表示的低 16 位
1015	第 03 路模拟量输出值	输出值浮点表示的高 16 位
1016	第 04 路模拟量输出值	输出值浮点表示的低 16 位
1017	第 04 路模拟量输出值	输出值浮点表示的高 16 位
保 留		
1020	系统时钟：时	采用 BCD 码表示
1021	系统时钟：分	同上
1022	系统时钟：秒	同上
1023	系统时钟：年	同上
1024	系统时钟：月	同上
1025	系统时钟：日	同上
1026	系统时钟：周	同上
保 留		

MODBUS 请求

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

MODBUS 响应

功能码	1 BYTE	0x03
字节计数	1 BYTE	N*2
输入状态	N*2 BYTE	

错误 响应

功能码	1 BYTE	0x03+ 0x80
错误代码	1 BYTE	0x1 or 0x2

举例

请求		响应	
模块地址	数据（hex）	模块地址	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	保持寄存器高	00
读取数量高(字节)	00	保持寄存器低	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. 读输入寄存器

功能码：04

说明：读取输入数据

数据说明：读取的是十六位整数或无符合整数

地址(十六进制)	描述	说明
1000	第 01 路模拟量输入值	输入值浮点表示的低 16 位
1001	第 01 路模拟量输入值	输入值浮点表示的高 16 位
1002	第 02 路模拟量输入值	输入值浮点表示的低 16 位
1003	第 02 路模拟量输入值	输入值浮点表示的高 16 位
1004	第 03 路模拟量输入值	输入值浮点表示的低 16 位
1005	第 03 路模拟量输入值	输入值浮点表示的高 16 位
1006	第 04 路模拟量输入值	输入值浮点表示的低 16 位
1007	第 04 路模拟量输入值	输入值浮点表示的高 16 位
1008	第 05 路模拟量输入值	输入值浮点表示的低 16 位
1009	第 05 路模拟量输入值	输入值浮点表示的高 16 位
100a	第 06 路模拟量输入值	输入值浮点表示的低 16 位
100b	第 06 路模拟量输入值	输入值浮点表示的高 16 位
100c	第 07 路模拟量输入值	输入值浮点表示的低 16 位
100d	第 07 路模拟量输入值	输入值浮点表示的高 16 位
100e	第 08 路模拟量输入值	输入值浮点表示的低 16 位
100f	第 08 路模拟量输入值	输入值浮点表示的高 16 位
保留		
8000	硬件标识 ID	
保留		
8010	设备性能	高八位是 n 路 DI，低八位 n 路 DO
8011	设备性能	高八位是 n 路 AI，低八位 n 路 AO

MODBUS 请求

功能码	1 BYTE	0x04
起始地址	2 BYTE	0x0000 TO 0xFFFF
读取数量	2 BYTE	1 TO 125(0x7D)

MODBUS 响应

功能码	1 BYTE	0x04
字节计数	1 BYTE	N*2
输入状态	N*2 BYTE	

错误 响应

功能码	1 BYTE	0x04+ 0x80
错误代码	1 BYTE	0x1 or 0x2

举例

请求		响应	
模块地址	数据（hex）	模块地址	数据（hex）
功能码	04	功能码	04
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（9）	00
读取数量高(字节)	00	输入寄存器低（9）	0A
读取数量低(字节)	01		

5. 设置单个继电器

功能码：05

MODBUS 请求

功能码	1 BYTE	0x05
设置地址	2 BYTE	0x0000 TO 0xFFFF
设置内容	2 BYTE	0x0000 OR 0xFF00 0x0000 释放继电器 0xff00 吸合继电器

MODBUS 响应

功能码	1 BYTE	0x05
设置地址	2 BYTE	0x0000 TO 0xFFFF
设置内容	2 BYTE	0x0000 OR 0xFF00

错误 响应

功能码	1 BYTE	0x05+ 0x80
错误代码	1 BYTE	0x1 or 0x2

举例

请求		响应	
模块地址	数据（hex）	模块地址	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

6. 设置单个保持寄存器

功能码：06

MODBUS 请求

功能码	1 BYTE	0x06
设置地址	2 BYTE	0x0000 TO 0xFFFF
设置内容	2 BYTE	0x0000 to 0xFFFF

MODBUS 响应

功能码	1 BYTE	0x06
设置地址	2 BYTE	0x0000 TO 0xFFFF
设置内容	2 BYTE	0x0000 to 0xFFFF

错误 响应

功能码	1 BYTE	0x06+ 0x80
错误代码	1 BYTE	0x1 or 0x2

举例

请求		响应	
模块地址	数据（hex）	模块地址	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

7. 设置多个继电器

功能码：0F

MODBUS 请求

功能码	1 BYTE	0x0F
设置起始地址	2 BYTE	0x0000 TO 0xFFFF
设置长度	2 BYTE	0x0000 TO 0x7B0
字节计数	1 BYTE	N
设置内容	N BYTE	

MODBUS 响应

功能码	1 BYTE	0x0F
设置起始地址	2 BYTE	0x0000 TO 0xFFFF
设置长度	2 BYTE	0x0000 TO 0x7B0

错误 响应

功能码	1 BYTE	0x0F+ 0x80
错误代码	1 BYTE	0x1 or 0x2

举例

请求		响应	
模块地址	数据（hex）	模块地址	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		

8. 设置多个保持寄存器

功能码：10

MODBUS 请求

功能码	1 BYTE	0x10
设置起始地址	2 BYTE	0x0000 TO 0xFFFF
设置长度	2 BYTE	0x0000 TO 0x7B0
字节计数	1 BYTE	N*2
设置内容	N*2 BYTE	

MODBUS 响应

功能码	1 BYTE	0x10
设置起始地址	2 BYTE	0x0000 TO 0xFFFF
设置长度	2 BYTE	0x0000 TO 0x7B0

错误 响应

功能码	1 BYTE	0x10+ 0x80
错误代码	1 BYTE	0x1 or 0x2

举例

请求		响应	
模块地址	数据（hex）	模块地址	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		

9. 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

功能码	1 BYTE	0x14
字节计数	1 BYTE	0x07 TO 0xF5
子功能码	1 BYTE	0x06
文件号	2 BYTE	0x0000 TO 0xFFFF
记录号	2 BYTE	0x0000 TO 0x270F
读取长度	2 BYTE	N
子功能码	1 BYTE	0x06

……	……	

MODBUS 响应

功能码	1 BYTE	0x14
字节计数	1 BYTE	0x07 TO 0xF5
子功能字节计数	1 BYTE	0x07 TO 0xF5
子功能码	1 BYTE	0x06
数据	2N BYTE	

错误 响应

功能码	1 BYTE	0x14+ 0x80
错误代码	1 BYTE	0x1 or 0x2

举例

请求		响应	
模块地址	数据（hex）	模块地址	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	记录号高(字节)	0D
记录号高(字节)	00	记录号低(字节)	FE
记录号低(字节)	01	读取长度高(字节)	00
读取长度高(字节)	00	读取长度低(字节)	20
读取长度低(字节)	02		

10．写文件记录

功能码：15/06

MODBUS 请求

功能码	1 BYTE	0x15
字节计数	1 BYTE	0x07 TO 0xF5
子功能码	1 BYTE	0x06
文件号	2 BYTE	0x0000 TO 0xFFFF
记录号	2 BYTE	0x0000 TO 0x270F
写长度	2 BYTE	N
数据	2N BYTE	
……	……	

MODBUS 响应

功能码	1 BYTE	0x15
字节计数	1 BYTE	0x07 TO 0xF5
子功能码	1 BYTE	0x06
文件号	2 BYTE	0x0000 TO 0xFFFF
记录号	2 BYTE	0x0000 TO 0x270F
写长度	2 BYTE	N

数据		

错误 响应

功能码	1 BYTE	0x15+ 0x80
错误代码	1 BYTE	0x1 or 0x2

举例

请求		响应	
模块地址	数据（hex）	模块地址	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

附：配置文件分配：

网络配置：访问文件号 00，记录号 4097，记录长度 24 字节，结构如下：

字节数	4byte	4byte	4byte	6byte	2byte	2byte	2byte
内容	IP 地址	子网 掩码	默认 网关	MAC 地址	TCP 端口	UDP 端口	自动 获取 IP

串口配置：访问文件号 00，记录号 4113，记录长度 6 字节，结构如下：

字节数	4byte	1byte	1byte
内容	波特率	从站号	校验方式