MODBUS 集成指南

Version 0.1

Honeywell

ECC AP TAC

2008.10

商标信息

版本信息

2008 年 10 月 Version 0.1

联系方式

如果有任何问题以及建议可联系我们：
ECC.AP.TAC@Honyewell.com
此文档将可能持续更新，恕不预先通知。
获知更多技术信息可浏览网站
http://customer.honeywell.cn 服务与支持栏目

目录

引言

MODBUS 是目前楼宇自控中应用较为普遍的一种通信协议，通常可见于 PLC ，电表，冷水机组/热泵控制器，变频器等设备。

本文的目的在于介绍 MODBUS 的通信介质，通信协议(如数据寻址，数据类型等)基础知识，并且附录有 SymmetrE, WEBs 等系统集成 MODBUS 实验。

术语

ASCII	American Standard Code for Information Interchange
Bit	二进制数中的单个位
Byte	二进制数中八个位
CLIENT	计算机网络中的客户机,可远程享用服务器上的服务数据等
CRC	Cyclic redundancy check, 用于校验错误的校验码方法
Coils	PLC 中可读写的位寄存器数据
Discrete Input	PLC 的数字性输入数据(只读),位寄存器数据
Drive	本文档中特指 Modbus Plus 网络中的硬件接口
GATEWAY	网关,指不同网络或总线之间的转换软硬件接口
HMI	Human-Machine Interface, 人机接口
Holding Registers	PLC 中可读写的 16 位寄存器数据
IEEE	Institute of Electrical and Electronics Engineers
Input Registers	PLC 的模拟性输入数据(只读),16 位寄存器数据
Integer	整型,有符号或无符号整数类型
I/O	Input/Output 本文档特指输入输出模块
LRC	Longitudinal redundancy check, 用于校验错误的校验码方法
MBAP header	MODBUS Application Protocol header
Peer to Peer	网络中各节点可直接进行端对端通信
PLC	Programmable Logical Controller
RS232	Recommended Standard 232, 串行通信标准
RS485	Recommended Standard 485, 串行通信标准
RTU	Remote Terminal Unit, 远程终端设备
SERVER	计算机网络中的服务器, 提供各种服务与数据等
TCP/IP	Transmission Control Protocol over Internet Protocol
Word	二进制数,两个 Byte 或 16 个 bit.

MODBUS 简介

1. 历史背景

MODBUS 于 1979 产生于 Modicon 公司(现被 Schneider 公司收购)，卜一面世因其简单开放的通信方式逐渐成为工业系统中流行的标准。最早这一通信方式主要依赖于 RS232,RS485 等串行通信总线，随着 Ethernet 普及，基于 TCP/IP 的通信方式以及标准出现并流行。2008 年，MODBUS 协议正式成为中国国家标准《基于 MODBUS 协议的工业自动化网络规范》(GB/T 19582-2008)。
MODBUS 的国际组织主要有 MODBUS-IDA, 负责推广 MODBUS 标准以及对 MODBUS 产品的认证。其网站包括要厂商，产品列表，以及协议文档等内容。
网站：www.MODBUS.org

2. 典型通信方式

典型 MODBUS 通信的方式是主从方式(TCP/IP 及 MODBUS Plus 网络有所不同在后面章节有所描述)。
以 MODBUS 在的串行通信总线中的通信方式为例：
只有主机(Master)可以发送包括从机(Slave)地址, 任务代码(Function code)的请求信息，同时启动等待超时计时器(Time out)。而从机在获得请求信息后，确认地址一致，并且同时校验请求信息，当正确无误，则返回对应于任务代码的应答信息，否则将不予回应。如果主机没有收到从机的应答信息，只有在等待超时计时器超时后才可发送下一个请求信息。

3. 优缺点

MODBUS 的通信方式非常简单，其中信息格式也简单易懂，无论是工程调试，软件开发等方面都较为快捷简单。依赖于 RS232/485, Ethernet TCP/IP 的通信网络也较为普遍，采用 MODBUS 标准的厂家设备也很普遍，在系统集成和设备互连方面技术障碍少。同时有大量免费的协议文档，调试软件工具可以使用。
但需要注意的是典型的 MODBUS 的串行通信方式依赖的主从结构通信，使得从机无法主动与其他从机进行通信(Peer to Peer)，所有的通信必须依赖于主机。

通信网络

目前使用较多的 MODBUS 通信网络主要有 TCP/IP (Ethernet), 串行通信 (EIA/TIA-232-E, EIA-422, EIA/TIA-485-A,红外,无线电等), MODBUS Plus 令牌总线(MB+)。

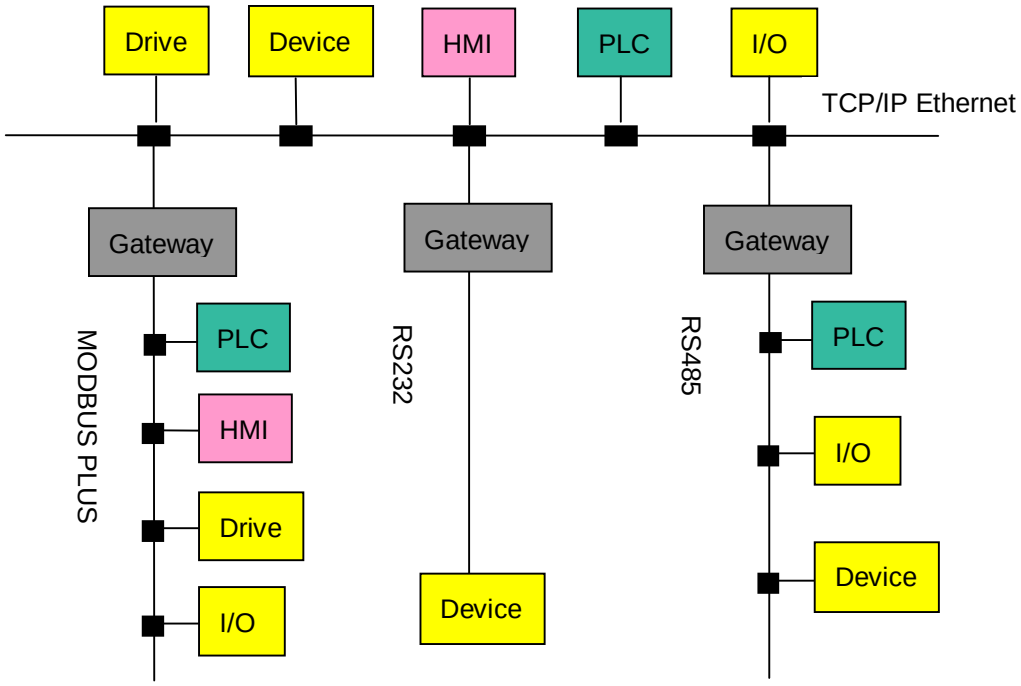

图-1. MODBUS的网络架构

因为 RS232 及 RS485 的应用最早和最广泛，大多数厂家对 MODBUS 基于 RS232, RS485 的软硬件接口支持最多。同时随着 TCP/IP 的广泛使用，对 MODBUS TCP 的支持也越来越多，目前 MODBUS TCP 的设备既包括直接提供数据的设备也包括 RS232/485 转换到 TCP/IP(Ethernet)的网关设备。MODBUS Plus 是高速的令牌总线，支持多主机制，但是由于通信硬件复杂，以及设备厂家不多的原因使用并不广泛。需要注意的是 MODBUS /RS485 尽管和 MODBUS Plus 总线在电气上类似，但是不能兼容和通用。如果需要集成 MODBUS Plus 设备可使用 MODBUS Plus 到 TCP/IP(Ethernet)网关来实现。

MODBUS 基于 RS232/485

1. 总线通信介质

1.1. RS232 的信号规定

信号代号	对于 DCE	DCE 需要	DTE 需要	描述
Common	--	X	X	信号公共端
CTS	In			清除发送
DCD	--			数据载体检测(从 DCE 到 DTE)
DSR	In			数据集预备
DTR	Out			数据终端预备
RTS	Out			请求发送
RXD	In	X	X	接收数据
TXD	Out	X	X	发送数据

X 代表需要
信号电气标准遵照 EIA/TIA-232
RXD 必须接另一个设备的 TXD.

1.2. RS232 电缆,接口及限制

推荐使用屏蔽 3 芯(或 5 芯) Category 5 电缆。
RS232 通常采用 RJ45, D-Shell 9 Pin 电气接口，具体接法参照厂家说明。
通常 RS232 最大通信距离<18 米。

1.3. RS485 总线结构

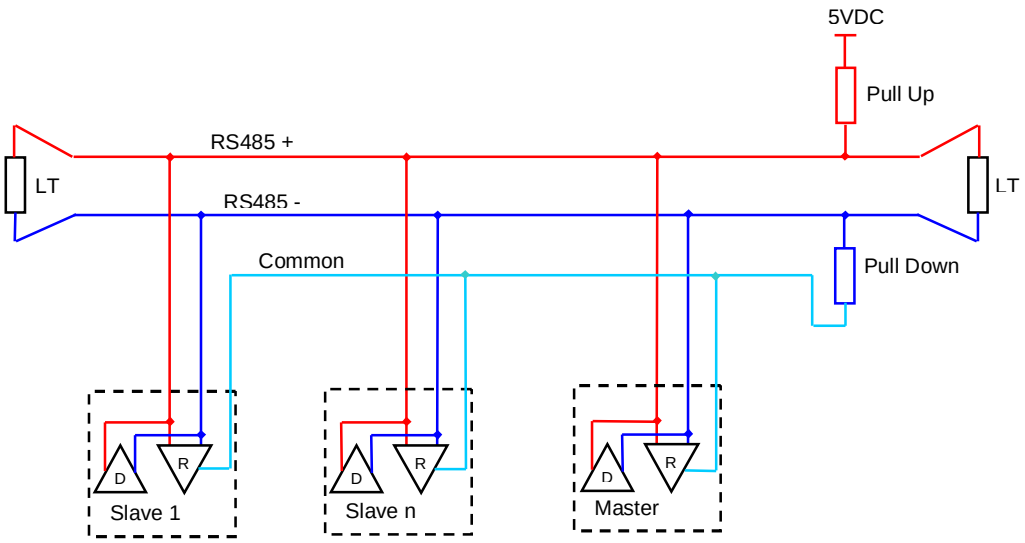

图-2 MODBUS/RS485总线结构

信号电气标准遵照 EIA/TIA-485
LT (Line Termination): 150 Ω (0.5 W) 电阻,
或 120 Ω (0.25W) 电阻串联 1nF 电容(最小耐压 10V)

Pull Up: 450 Ω ~650 Ω
Pull Down: 450 Ω ~650 Ω
总线极性: 总线接线(D1,D0)必须保证极性一致，
具体极性(+/-)必须参照厂商设备说明。
**Pull Up, Pull Down 电阻以及 Common 公共线并不是强制的，但其设置会增强 RS485 总线的通信性能。*

1.4. RS485 总线电缆及容量限制

推荐使用 AWG24(0.511mm,0.20mm^2)规格的屏蔽双绞线,
推荐电缆 Belden 9841 或相同规格电缆。
总线最大长度 1000 米(无中继器)
总线支持最大设备数量为 32 (Full load, 设备全负载)
** 如设备的 RS485 收发器为 1/2, 1/4 或更小的负载，请参照厂家说明的总线设备数量*

2. 总线通信速率

MODBUS 标准规定 MODBUS 串行通信设备必须支持 19,200bps(默认), 9600bps 两种速率。其他通信速率可选 1200, 2400, 4800, 38400 bps, 57,600bps, 115,200Kbps

3. MODBUS 传输模式

MODBUS 标准规定 MODBUS 串行通信设备必须支持 RTU 模式，ASCII 模式可选。

3.1. RTU 传输模式

3.1.1. 字节(byte)编码方式

译码系统: 每个字节为1个8位二进制数值
数据位数: 8位 低位先发送
起始位: 1位
奇偶校验位: 1位 (默认为奇,可选偶和无, 如选无,则仍占1位)
停止位: 1位

例如, 传送数值为5(B00000101)的有奇校验位的RTU码:

0	1	0	1	0	0	0	0	0	1	1
起始	D0	D1	D2	D3	D4	D5	D6	D7	校验	停止
	数据位(低位先发送)									

3.1.2. 主机 ADU (Application Data Unit) 格式

ADU 是主机和从机通信的数据块，规定了它的格式，则从机可以按照标准解析主机的请求信息，主机也可以准确解析从机数据。

部分名称		**Protocol Data Unit**		
数据意义	Slave Address	Function Code	DATA	CRC
解释	从机地址	功能代码	数据正文	循环冗余校验码
字节 数 (byte,11bits)	1	1	0~252	2
举例(0x)	11	03	00 6B 00 03	76 87
举例说明	主机向17号从机读取保持寄存器0x006B起3个Byte的数值请求			

其中Function Code和Data部分为PDU(Protocol Data Unit),为MODBUS协议核心部分，即各种传输方式中PDU都保持相同的格式。

其中Slave Address, Function Code, DATA在后面的章节均有阐述。
采用循环冗余校验(CRC)方式来检查数据是否完整和正确。具体的CRC算法，本指南不做阐述，可参照MODBUS over Serial Line Specification and implementation Guide里的介绍了例程。

3.2. ASCII 传输模式

3.2.1. 字节(byte)编码方式

译码系统: 每个字节包含4位可表示成ASCII字符(0~9,A~F), 此ASCII字符可表示 1位16进制。
数据位数: 7位 低位先发送
起始位: 1位
奇偶校验位: 1位 (默认为奇,可选偶和无, 如选无,则仍占1位)
停止位: 1位

例如, 传送ASCII表示字符为5(B00110101)的有奇校验位的ASCII码:

0	1	0	1	0	1	1	0	1	1
起始	D0	D1	D2	D3	D4	D5	D6	校验	停止
	数据位(低位先发送)								

3.2.2. 主机 ADU (Application Data Unit) 格式

部分名称			**Protocol Data Unit**			
数据意义	Start	Slave Address	Function Code	DATA	LRC	End
解释	起始字符	从机地址	功能代码	数据正文	纵向冗余校验码	停止字符
字符数 (char,10bits)	1	2	2	0~2x252	2	2
举例(ASCII)	:	11	03	00 6B 00 03	7 E	CR,LF
举例(0x)	3A	3131	3033	3030 3642 3030 3033	3745	0D0A
举例说明	主机向17号从机读取保持寄存器0x006B起3个Byte的数值请求					

从例子中可以看出:
ASCII码在传输相同的数据位数时，由于编码的特性其使用的bits数几乎是RTU方式的2倍。
其中Slave address, Function Code后面篇章有所介绍。LRC的计算本文档不作介绍，请参考参考文献。

4. 从机地址 (Slave Address)

尽管 RS485 总线最多支持 32 个全负载设备，但是从机的地址可选择 1~247, 0 为广播地址, 248~255 为预留号码。总线当中的从机地址不得重复或冲突。

5. 从机数据地址及类别 (Data address and Category)

MODBUS 从机设备将数据按照标准进行归类并且放置在特定的内存区域。如下表所示:

类别	类型	读写	类比	地址范围
Discrete Input	Bits	Read only	Digital Input	1~65536
Coils	Bits	Read/Write	Digital Output	1~65536
Input Registers	16-bit, Word	Ready only	Analog Input	1~65536
Holding Registers	16-bit, Word	Read/Write	Analog Output	1~65536

6. 从机数据地址的表示方法

由于 MODBUS 协议修改和完善的原因，目前各个厂家的设备在表示数据地址方法并不统一，可大概分为 984 经典(十进制), 包含数据类别码的新标法(十进制), 十六进制。
需要注意十进制代表数据序号，不一定等同于 PDU 里的地址。十六进制一般直接等同于 PDU 地址的表示。下表举例说明:

类别	十进制表示			十六进制表示
	984经典	新标法	标准标法	
Discrete Input	10001~19999	100001~165536	1~65536	1x0000~1xFFFF
Coils	1~9999	1~65536	1~65536	0x0000~0xFFFF
Input Registers	30001~39999	300001~365536	1~65536	3x0000~3xFFFF
Holding Registers	40001~49999	400001~465536	1~65536	4x0000~4xFFFF

十六进制另一种标法为 0000H~FFFFH

PDU 里的十六进制地址偏移(offset)为 0, 而十进制地址或序号偏移为 1。
举例：
第 1 个 Holding Register 数据的十进制序号为 1， 或 40001，而在 PDU 地址十六进制表示 则为 0x00。在 MODBUS 集成中经常出现地址偏移的问题而无法读取正确数值。

7. 模拟数据类型

Input Registers 及 Holding Registers 均放置为 16 bits 二进制数值。
根据设备厂家的定义常见有以下几种模拟数据类型, 可能会占用 1 个或者 2 个以上数据。

数据类型	十进制范围	数据个数	总位数	无效位	数值位	指数位	符号位
Integer	0~65536	1	16	0	16	0	0
Signed Integer	-32768~32767	1	16	0	15	0	1
Long	-2,147,483,648 2,147,483,647	2	32	0	31	0	1
Float (IEEE754)	$\pm 3.4*10^{38}$	2	32	0	23	8	1
8bits integer	0~255	1	16	8	8	0	0
8bits Signed integer	-128~127	1	16	8	7	0	1

8. 功能码 (Function Code)

在 PDU 中，功能码用来指示从机执行相应的任务。MODBUS 标准中规定的常用的功能码如下表:

功能码	16进制表示	目标数据	任务	功能类型
01	0x01	Multiple Coils	Read	Bits
02	0x02	Multiple Discrete Inputs	Read	Bits
03	0x03	Multiple Holding Registers	Read	Bits
04	0x04	Multiple Input Registers	Read	Bits
05	0x05	Single Coil	Write	Bits
06	0x06	Single Holding Register	Write	Bits
07	0x07	Exception Status	Read	Diagnostic
08	0x08		Diagnostic	Diagnostic
11	0x0B	Communication event counter	Read	Diagnostic
12	0x0C	Communication event log	Read	Diagnostic
15	0x0F	Multiple Coils	Write	Bits
16	0x10	Multiple Holding Registers	Write	Bits
17	0x11	Slave ID	Read	Diagnostic
20	0x14	File record	Read	File
21	0x15	File record	Write	File
22	0x16	Holding Registers	Mask Write	Bits
23	0x17	Multiple Holding Registers	Read/Write	Bits
24	0x18	FIFO queue	Read	Bits
43	0x2B	Device identification	Read	Diagnostic

其中标色的是常用的功能代码。

下面是一个主机请求读取从机地址 108~110 (0x006B~006D) Holding Register 数值的 PDU.以及从机回应的数值。

数据名称	Function	Starting Address Hi	Starting Address Lo	No.of Registers Hi	No. of Registers Lo
解释说明	功能代码	起始地址高位	起始地址地位	读取数量高位	读取数量低位
举例(0x)	03	00	6B	00	03

从机返回 6 个 byte(3 个 16bit)值， 分别为 0x022B, 0000, 0064, 假设为整型分别为:555, 0, 96.

数据名称	Function	Byte Count	Register1 Value Hi	Register1 Value Lo	Register2 Value Hi	Register2 Value Lo	Register3 Value Hi	Register3 Value Lo
解释说明	功能代码	字节位数	寄存器 1 高位	寄存器 1 低位	寄存器 2 高位	寄存器 2 低位	寄存器 3 高位	寄存器 3 低位
举例(0x)	03	06	02	2B	00	00	00	60

MODBUS 基于 TCP/IP

1. 网络架构

MODBUS 基于 TCP/IP 的通信方式依赖于 Ethernet 网络。

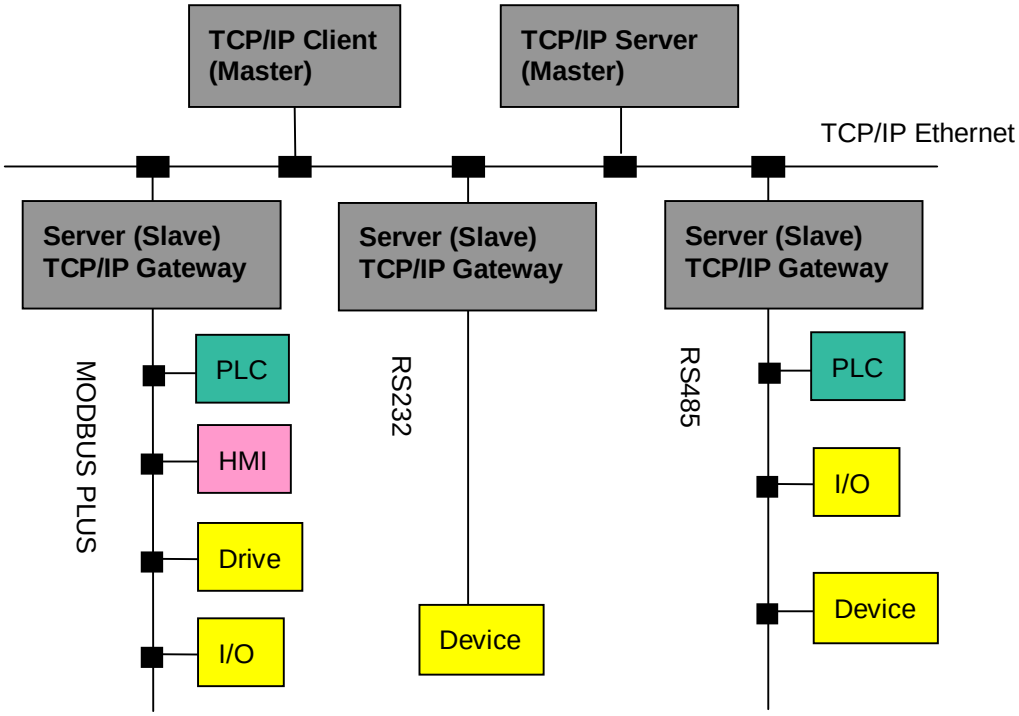

图 3 MODBUS 基于 TCP/IP 的网络架构

Ethernet 网络遵照 IEEE802.3 标准

MODBUS/TCP 提供数据服务的设备主要有 2 种类型：一种是直接提供数据访问服务的设备成为 SERVER(Slave), 一种是提供数据转发功能的 MODBUS 网关叫做 SERVER GATEWAY(Slave).
而访问数据的设备称为 CLIENT(Master).

2. 通信模式

TCP/IP 是面向连接(Connection oriented)的通信协议，在 MODBUS CLIENT 与 SERVER 建立连接后则直接利用 TCP 格式封装 MODBUS 的 PDU 进行收发。基于 TCP/IP 协议的特性，MODBUS CLIENT 及 SERVER 的通信有以下一些与串行通信比较而突出的特征：

- 1个MODBUS/TCP设备可以设计成CLIENT请求数据也可以作为SERVER提供数据。
- 1个MODBUS/TCP设备支持多个TCP/IP连接，所以支持多个设备之间的数据共享和Peer to Peer通信。
- MODBUS/TCP CLIENT设备可以在未得到SERVER应答信息前发送多个请求信息，可以更高效利用TCP/IP带宽。
- 标准规定了MODBUS SERVER的专用TCP/IP端口为502。

3. ADU 格式

相比 MODBUS 串行通信中的 RTU 方式，MODBUS/TCP 使用 MBAP Header 替代了 Slave address, 去除了 CRC 校验，而使用 TCP/IP 本身的校验方式。
MBAP (MODBUS Application Protocol header).

部分名称		**Protocol Data Unit**	
数据意义	MBAP	Function Code	DATA
解释	MODBUS报文头	功能代码	数据正文
字节 数 (byte, 8bits)	7	1	0~252
举例(0x)	01 00 00 00 00 06 11	03	00 6B 00 03
举例说明	主机向17号TCP从机读取保持寄存器0x006B起3个Byte的数值请求		

PDU 格式同 MODBUS 串行通信中一致。

4. MBAP Header 结构

部分名称	**MBAP**				**Protocol Data Unit**
数据意义	Transaction Identifier	Protocol Identifier	Length	Unit Identifier	Function Code & Data
解释	处理编号	协议编号	字节长度	设备号	功能码和数据正文
字节数 (byte, 8bits)	2	2	2	1	0~252
举例(0x)	01 00	00 00	00 06	11	03 00 6B 00 03
举例说明	主机向17号TCP从机读取保持寄存器0x006B起3个Byte的数值请求				

- Transaction Identifier: 由MODBUS CLIENT在发送请求信息时生成的一个事务处理编号，一个事物处理指发送了请求信息，并得到回复的一个完整过程。一个CLIENT可以同时处理多个事务，则事务处理必须有唯一的编号以区分处理。
- Protocol Identifier: 对于MODBUS TCP通信为固定值 0x00.
- Length: 指从Unit Identifier开始后包括PDU的字节(Byte)数.
- Unit Identifier: 类似于Slave Address, 如果MODBUS SEVER为直接数据提供者则值为0xFF; 如果MODBUS SERVER 作为 GATEWAY转发信息到串行通信总线或者MODBUS PLUS，则值为总线上的设备地址 1~247, 0x01~F7, 0代表广播。

下面是一个主机请求读取 TCP 从机地址 108~110 (0x006B~006D) Holding Register 数值的完整 TCP 报文.以及从机回应的完整 TCP 报文,分别返回数值 555,0,96。

主机: 01 00 00 00 00 06 11 03 00 6B 00 03
从机: 01 00 00 00 00 09 11 03 06 02 2B 00 00 00 60

Honeywell 系统支持的 MODBUS 接口

1. SymmetrE

SymmetrE R310.1 目前支持服务器作为:
MODBUS/TCP CLIENT,
MODBUS/RS232 MASTER;
MODBUS/RS485 MASTER.
具体接口 License 及订购联系市场与销售部门

2. WEBs

WEBs 3.22 服务器 及 WEBs 403, 545, 600 控制器目前支持作为:
MODBUS/TCP CLIENT, SEVER
MODBUS/RS232 MASTER, SLAVE;
MODBUS/RS485 MASTER, SLAVE.
并支持集成:
MODBUS/TCP SERVER GATEWAY
具体接口 License 及订购联系市场与销售部门

3. TREND

TREND IQ3 Integration Controller 可通过编程支持作为:
MODBUS/TCP CLIENT, SEVER, SERVER GATEWAY；
MODBUS/RS232 MASTER, SLAVE;
MODBUS/RS485 MASTER, SLAVE.
具体硬件及工具定购联系市场与销售部门

4. Alerton

BCM-MDBS 可作为
MODBUS RS232 MASTER
MODBUS RS485 MASTER
FLG-MODBUS 可作为:
MODBUS RS232 MASTER
MODBUS RS485 MASTER
具体硬件及接口定购联系市场与销售部门

参考文献

- MODBUS APPLICATION PROTOCOL SPCIFICATION V1.1b, 2008
- MODBUS Over Serial Line Specification and Implementation Guide V1.02,2008
- MODBUS MESSAGEING ON TCP/IP IMPLEMENTATION GUIDE V1.0b,2008
- Modicon Modbus Protocol Reference Guide, 1996
- WEBs 3.22 MODBUS User Guide. 2008
- SymmetrE R310.1 MODBUS Interface Reference , 2005
- IQ3 Integration controller Manual, 2003
- Trend Custom Language Manual, 2003
- Alerton BCM-MDBS Manual, 2003
- Alerton FLG-MODBUS Manual, 2003

资源与工具

免费文档与测试模拟工具

- MODBUS-IDA, www.modbus.org
- MODBUS Tester(Serial),TCP Parser, RTU Parser, www.Chipkin.com
- MODBUS TCP/IP,RTU Slave Simulator, www.hmisys.com
- Modpoll Modbus Master Simulator (TCP and Serial), www.modbusdriver.com

优秀收费工具

- Modbus Poll (TCP and Serial), www.modbustools.com
- Modbus Scan (TCP and Serial), www.win-tech.com

附录

附录 **1. SymmetrE** 集成 **Modbus TCP/RS485** 设备实验

附录 **2. WEBs** 集成 **Modbus TCP/RS485** 设备实验