第 3 章

Modbus 控制网络

Modbus 是一种广泛使用的工业通信协议，自 1979 年由 Modicon 公司（现为施耐德电气的一部分）推出以来，它已经成为工业通信领域的事实标准。Modbus 协议简洁，易于理解和实施，支持多种通信方式，包括串行通信（如 RS-232 和 RS-485）和 TCP/IP 网络通信，因此在自动化和控制系统中得到了广泛应用。

本章讲述了 Modbus 的基本特性、通信模型、物理层标准、串行链路层标准以及基于 TCP/IP 的 Modbus TCP。具体内容如下：

（1）Modbus 概述。Modbus 协议以其简单性、开放性和灵活性而著称，它采用客户机/服务器（主站/从站）模型，通过定义统一的帧结构实现设备间的高效数据通信。这种通信协议能够适应包括传统串行通信和现代 TCP/IP 网络通信在内的多种应用场景，使其成为工业通信领域的一个重要标准。

（2）Modbus 物理层。Modbus 协议支持包括 RS-232 和 RS-485 在内的多种接口标准。RS-232 主要用于短距离的点对点通信，而 RS-485 则因其支持更长距离通信和多设备连接，在工业应用中更为常见。

（3）Modbus 串行链路层标准。在串行链路层面，Modbus 定义了 ASCII 和 RTU 两种传输模式，分别优化了可读性和通信效率。此外，通过 CRC 或 LRC 方法进行的差错检验确保了数据传输的准确性和完整性。Modbus 还定义了一系列功能码，用于指定主站请求的操作类型，如读写寄存器或线圈。编程方法部分则详细介绍了如何构建请求/响应帧及处理通信过程中的错误和异常。

（4）Modbus TCP。Modbus TCP 扩展了 Modbus 协议，使其能够在 TCP/IP 网络上运行，从而允许设备在更广泛的网络环境中通信。这一部分还介绍了 Modbus TCP 消息的结构，包括事务标识符、协议标识符、长度和单元标识符，以及 Modbus-RTPS，这是一种用于实现实时数据交换和控制的实时发布订阅机制。

通过本章的学习，读者不仅能够理解 Modbus 协议的基本原理和关键特性，还能够掌握其在实际工业通信场景中的应用。这为深入学习和实践 Modbus 通信提供了坚实的基础，有助于在自动化和控制系统设计中有效利用 Modbus 技术。

3.1　概述

Modbus 是全球第一个真正用于工业现场的总线协议。为更好地普及和推动 Modbus 基于以太网的分布式应用，目前施耐德电气已将 Modbus 协议的所有权移交给分布式自动化接口(Interface for Distributed Automation，IDA)组织，并成立了 Modbus-IDA 组织，为 Modbus 今后的发展奠定了基础。在我国，Modbus 已经成为国家标准 GB/T 19582—2008。据不完全统计，Modbus 的节点安装数量目前已经超过了 1000 万个。

3.1.1　Modbus 的特点

Modbus 具有如下特点：

(1) 标准、开放。用户可以免费、放心地使用 Modbus 协议，不需要缴纳许可费用，也不会侵犯知识产权。目前，支持 Modbus 的厂家超过 400 家，支持 Modbus 的产品超过 600 种。

(2) Modbus 支持多种电气接口，如 RS-232、RS-485 和以太网等；还可以用各种介质传输 Modbus 信号，如双绞线、光纤和无线介质等。

(3) Modbus 的帧格式简单、紧凑，通俗易懂，用户使用容易，厂商开发简单。

3.1.2　Modbus 的通信模型

Modbus 是 OSI 参考模型第 7 层上的应用层报文传输协议，它在连接至不同类型总线时或网络的设备之间提供客户机/服务器通信。Modbus 的通信模型如图 3-1 所示。

<table>
<tr><td colspan="3">Modbus应用层</td></tr>
<tr><td colspan="2" rowspan="3"></td><td>基于TCP的Modbus</td></tr>
<tr><td>TCP</td></tr>
<tr><td>IP</td></tr>
<tr><td>HDLC</td><td>Modbus串行链路协议</td><td>Ethernet/IEEE 802.3</td></tr>
<tr><td>令牌传递网络</td><td>RS-232/RS-485</td><td>以太网</td></tr>
</table>

图 3-1　Modbus 的通信模型

目前，Modbus 包括标准 Modbus、Modbus＋和 Modbus TCP 共 3 种形式。标准 Modbus 指的就是在异步串行通信中传输 Modbus 信息。Modbus＋指的就是在一种高速令牌传递网络中传输 Modbus 信息，采用全频通信，具有更高的通信传输速率。Modbus TCP 就是采用 TCP/IP 和以太网协议来传输 Modbus 信息，属于工业控制网络范畴。本章主要介绍基于异步串行通信的标准 Modbus。

3.1.3　通用 Modbus 帧

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)上引入一些附加字段。通用

Modbus 帧的格式如图 3-2 所示。

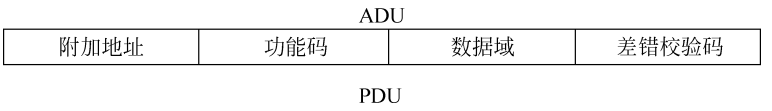


图 3-2　通用 Modbus 帧的格式

Modbus PDU 中功能码的主要作用是表明将执行哪种操作，功能码后面是含有请求和响应参数的数据域。Modbus ADU 中的附加地址用于告知站地址，差错码是根据报文内容执行冗余校验计算的结果。

3.1.4　Modbus 通信原理

Modbus 是一种简单的客户机/服务器型应用协议，其通信过程如图 3-3 所示。

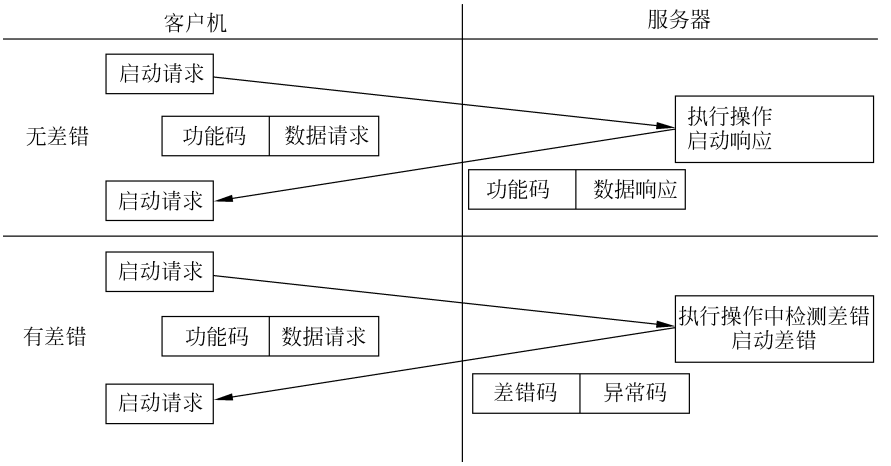


图 3-3　Modbus 协议的通信过程

首先，客户机准备请求并向服务器发送请求，即发送功能码和数据请求，此过程称为启动请求；然后服务器分析并处理客户机的请求，此过程称为执行操作；最后向客户机发送处理结果，即返回功能码和数据响应，此过程称为启动响应。如果在执行操作过程中出现任何差错，服务器将启动差错响应，即返回一个差错码或异常码。

Modbus 串行链路协议是一个主-从协议，串行总线的主站作为客户机，从站作为服务器。在同一时刻只有一个主站连接总线，一个或多个(最多为 247 个)从站连接于同一个串行总线。Modbus 通信总是由主站发起，从站根据主站功能码进行响应。从站在没有收到来自主站的请求时，不会发送数据，所以从站之间不能互相通信。主站在同一时刻只会发起一个 Modbus 事务处理。主站以如下两种模式对从站发出 Modbus 请求。

1. 单播模式

在单播模式下，主站寻址单个从站，从站接收并处理完请求后，向主站返回一个响应。在这种模式下，一个 Modbus 事务处理包含两个报文：一个是来自主站的请求；另一个是来自

从站的应答。每个从站必须有唯一的地址(1～247),这样才能区别于其他节点而被独立寻址。

2. 广播模式

在广播模式下,主站向所有从站发送请求,对于主站广播的请求,从站不返回响应。广播请求必须是写命令。所有的设备必须接收广播模式的写功能,地址 0 被保留用来识别广播通信。

3.2　Modbus 物理层

在物理层,串行链路上的 Modbus 系统可以使用不同的物理接口,最常用的是 RS-485 两线制接口。作为附加选项,该物理接口也可以使用 RS-485 四线制接口。当只需要短距离的点对点通信时,也可以使用 RS-232 串行接口作为 Modbus 系统的物理接口。

3.2.1　RS-232 接口标准

RS-232C 标准(协议)的全称是 EIA-RS-232C 标准,定义为"数据终端设备(Data Terminal Equipment,DTE)和数通信设备(Digital Communication Equipment,DCE)之间串行二进制数据交换接口技术标准"。它是在 1970 年由美国电子工业协会(EIA)联合贝尔系统、调制解调器厂家及计算机终端生产厂家共同制定的用于串行通信的标准。其中 EIA(Electronic Industry Association)代表美国电子工业协会,RS(Recommended standard)代表推荐标准,232 是标识号,C 代表 RS-232 的最新一次修改。

图 3-4　DB9 插头座

1. RS-232C 端子

RS-232C 的连接插头用 9 针的 EIA 连接插头座,如图 3-4 所示,其主要端子分配如表 3-1 所示。

表 3-1　RS-232C 的主要端子

端　脚	方　向	符　号	功　能
3	输出	TXD	发送数据
2	输入	RXD	接收数据
7	输出	RTS	请求发送
8	输入	CTS	为发送清零
6	输入	DSR	数据设备准备好
5		GND	信号地
1	输入	DCD	数据信号检测
4	输出	DTR	
9	输入	RI	

(1) 信号含义。

① 从计算机到 MODEM 的信号。

DTR——数据终端(DTE)准备好：告诉调制解调器计算机已接通电源，并准备好了。

RTS——请求发送：告诉 MODEM 现在要发送数据。

② 从 MODEM 到计算机的信号。

DSR——数据设备(DCE)准备好：告诉计算机 MODEM 已接通电源，并准备好了。

CTS——为发送清零：告诉计算机 MODEM 已做好了接收数据的准备。

DCD——数据信号检测：告诉计算机 MODEM 已与对端的 MODEM 建立了连接。

RI——振铃指示器：告诉计算机对端电话已在振铃。

③ 数据信号。

TXD——发送数据。

RXD——接收数据。

(2) 电气特性。

RS-232C 的电气线路连接方式如图 3-5 所示。

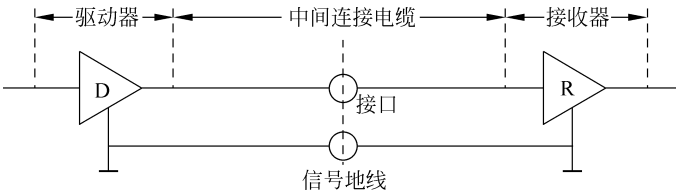


图 3-5 RS-232C 的电气线路连接

接口为非平衡型，每个信号用一根导线，所有信号回路共用一根地线。信号速率低于 20kb/s，电缆长度少于 15m。由于是单线，线间干扰较大。其电性能用±12V 标准脉冲。值得注意的是，RS-232C 采用负逻辑。

在数据线上：传号 Mark＝－5～－15V，为逻辑 1 电平。

空号 Space＝＋5～＋15V，为逻辑 0 电平。

在控制线上：通 On＝＋5～＋15V，为逻辑 0 电平。

断 Off＝－5～－15V，为逻辑 1 电平。

RS-232C 的逻辑电平与 TTL 电平不兼容，为了与 TTL 器件相连，必须进行电平转换。

由于 RS-232C 采用电平传输，在数据传输速率为 19.2kb/s 时，其通信距离只有 15m。若要延长通信距离，必须以降低数据传输速率为代价。

2. 通信接口的连接

当两台计算机经 RS-232C 口直接通信时，两台计算机之间的联络线如图 3-6 所示。虽然不接 MODEM，图中仍连接着有关的 MODEM 信号线，这是由于 INT 14H

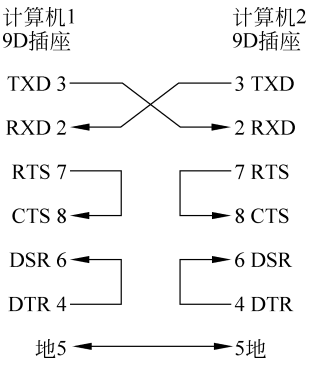


图 3-6 不使用调制解调器信号的 RS-232C 接口

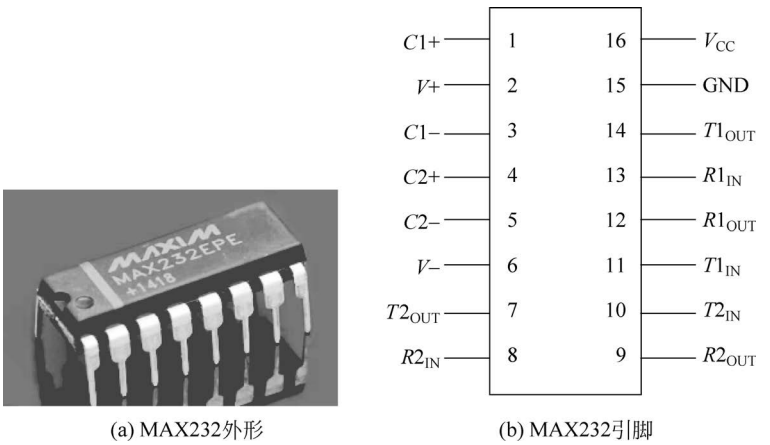
中断需要使用这些信号。如果程序中没有调用 INT 14H，在自编程序中也没有用到调制解调器的有关信号，那么两台计算机直接通信时，只连接 2、3、7（25 针 EIA）或 3、2、5（9 针 EIA）就可以了。

3. RS-232C 电平转换器

为了使采用＋5V 供电的 TTL 和 CMOS 通信接口电路能与 RS-232C 标准接口连接，必须进行串行口的输入/输出信号的电平转换。

目前常用的电平转换器有 Motorola 公司生产的 MC1488 驱动器、MC1489 接收器，TI 公司的 SN75188 驱动器、SN75189 接收器及美国 MAXIM 公司生产的单一＋5V 电源供电、多路 RS-232 驱动器/接收器，如 MAX232A 等。

MAX232A 内部具有双充电泵电压变换器，把＋5V 变换成±10V，作为驱动器的电源，具有两路发送器及两路接收器，使用相当方便。MAX232A 外形和引脚如图 3-7 所示，典型应用如图 3-8 所示。



(a) MAX232外形　　(b) MAX232引脚

图 3-7　MAX232A 外形和引脚图

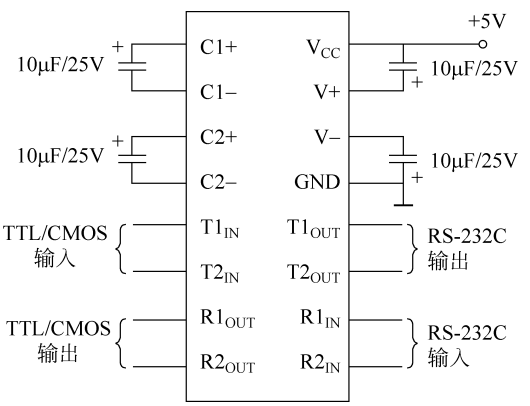


图 3-8　MAX232A 典型应用

单一+5V 电源供电的 RS-232C 电平转换器还有 TL232、ICL232 等。

3.2.2 RS-485 接口标准

由于 RS-232C 通信距离较近，当传输距离较远时，可采用 RS-485 串行通信接口。

1. RS-485 接口标准

RS-485 接口采用二线差分平衡传输，其信号定义如下。

当采用+5V 电源供电时，

- 若差分电压信号为−2500～−200mV 时，则为逻辑 0；
- 若差分电压信号为+2500～+200mV 时，则为逻辑 1；
- 若差分电压信号为−200～+200mV 时，则为高阻状态。

RS-485 的差分平衡电路如图 3-9 所示。其一根导线上的电压是另一根导线上的电压值取反。接收器的输入电压为这两根导线电压的差值 $V_A - V_B$。

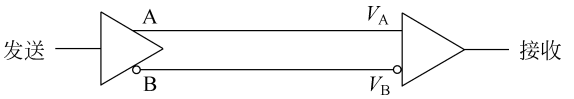
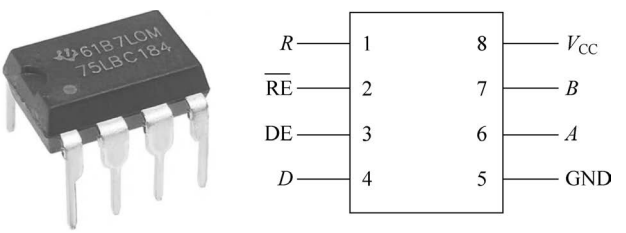


图 3-9 差分平衡电路

2. RS-485 收发器

RS-485 收发器种类较多，如 MAXIM 公司的 MAX485，TI 公司的 SN75LBC184、SN65LBC184 以及高速型 SN65ALS1176 等。它们的引脚是完全兼容的，其中，SN65ALS1176 主要用于高速应用场合，如 PROFIBUS-DP 现场总线等。下面仅介绍 SN75LBC184。

SN75LBC184 为具有瞬变电压抑制的差分收发器，SN75LBC184 为商业级产品，其工业级产品为 SN65LBC184，引脚如图 3-10 所示。



(a) SN 75LBC184外形　　(b) SN 75LBC184引脚

图 3-10 SN75LBC184 外形和引脚图

SN75LBC184 引脚介绍如下：

R——接收端。

$\overline{RE}$——接收使能，低电平有效。

DE——发送使能，高电平有效。

D——发送端。

A——差分正输入端。

B——差分负输入端。

V_{CC}——+5V 电源。

GND——地。

SN75LBC184 和 SN65LBC184 具有如下特点。

(1) 具有瞬变电压抑制能力,能防雷电和抗静电放电冲击。

(2) 限斜率驱动器,使电磁干扰减到最小,并能减少传输线终端不匹配引起的反射。

(3) 总线上可挂接 64 个收发器。

(4) 接收器输入端开路故障保护。

(5) 具有热关断保护。

(6) 低禁止电源电流,最大 300μA。

(7) 引脚与 SN75176 兼容。

3. 应用电路

RS-485 应用电路如图 3-11 所示。

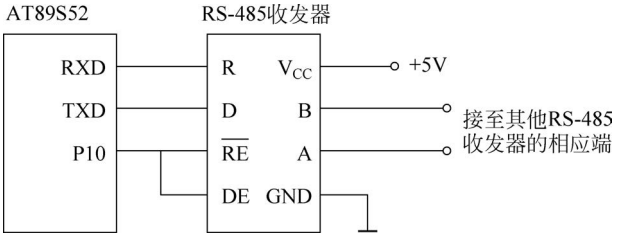


图 3-11　RS-485 应用电路

在图 3-11 中,RS-485 收发器可为 SN75LBC184、SN65LBC184、MAX485 等。当 P10 为低电平时,接收数据;当 P10 为高电平时,发送数据。

如果采用 RS-485 组成总线拓扑结构的分布式测控系统,那么在双绞线终端应接 120Ω 的终端电阻。

3.3　Modbus 串行链路层标准

Modbus 串行链路层标准就是通常所说的标准 Modbus 协议,它是 Modbus 协议在串行链路上的实现。Modbus 串行链路层协议是一个主-从协议,该协议位于 OSI 参考模型的第 2 层。

Modbus 串行链路层标准定义了一个控制器能够识别和使用的消息结构,而不管它们是经过何种网络进行通信的,也不需要考虑通信网络的拓扑结构。它定义了各种数据帧格式,用来描述控制器请求访问其他设备的过程、如何响应来自其他设备的请求及怎样侦测错误并记录。

3.3.1 Modbus 的传输模式

Modbus 定义了美国信息交换标准代码(ASCII)模式和远程终端单元(RTU)模式两种串行传输模式。在 Modbus 串行链路上,所有设备的传输模式(及串行口参数)必须相同,默认设置必须为 RTU 模式,所有设备必须实现 RTU 模式。若要使用 ASCII 模式,需要按照使用指南进行设置。在 Modbus 串行链路设备实现等级的基本等级中只要求实现 RTU 模式,常规等级要求实现 RTU 模式和 ASCII 模式。

1. ASCII 模式

使用 ASCII 模式,消息以冒号(:)字符(ASCII 为 3AH)开始,以回车换行符结束(ASCII 为 0DH、OAH)。

其他域可以使用的传输字符是十六进制的 0～9、A～F 的 ASCII。网络上的设备不断侦测“:”字符,当接收到一个“:”时,每个设备都解码下个域(地址域)来判断消息是否是发给自己的。

消息中字符间发送的时间间隔最长不能超过 1s,否则接收的设备将认为传输错误。典型 ASCII 消息帧结构如图 3-12 所示。

起始符	设备地址	功能代码	数据	LRC校验	结束符
1个字符	2个字符	2个字符	*n*个字符	2个字符	2个字符

图 3-12 典型 ASCII 消息帧结构

2. RTU 模式

使用 RTU 模式,消息发送至少要以 3.5 个字符时间的停顿间隔开始。传输的第一个域是设备地址,可以使用的传输字符是十六进制的 0～9、A～F。网络设备不断侦测网络总线,包括停顿间隔时间,当第一个域(地址域)接收到消息时,每个设备都进行解码以判断消息是否是发给自己的。在最后一个传输字符之后,一个至少 3.5 个字符时间的停顿标志了消息的结束,一个新的消息可在此停顿后开始传输。

整个消息帧必须作为一个连续的流传输。如果在帧完成之前有超过 1.5 个字符时间的停顿时间,接收设备将刷新不完整的消息,并假定下一字节是一个新消息的地址域。同样地,如果一个新消息在小于 3.5 个字符时间内接着前一消息开始传输,那么接收设备将认为它是前一消息的延续。这将导致一个错误,因为在最后 CRC 域的值不可能是正确的。典型 RTU 消息帧结构如图 3-13 所示。

停顿时间	设备地址	功能代码	数据	CRC校验	停顿时间
大于3.5个字符时间	8b	8b	*n*个8b	16b	大于3.5个字符时间

图 3-13 典型 RTU 消息帧结构

例如,向 1 号从站的 2000H 寄存器写入 12H 数据的 RTU 消息帧格式如表 3-2 所示。

表 3-2 Modbus RTU 消息帧格式

段 名	例子(HEX 格式)	说 明
设备地址	01	1 号从站
功能代码	06	写单个寄存器
寄存器地址	20	寄存器地址(高字节)
	00	寄存器地址(低字节)
写入数据	00	数据(高字节)
	12	数据(低字节)
CRC 校验	02	CRC 校验码(高字节)
	01	CRC 校验码(低字节)

这里完整的 RTU 消息帧为 01H 06H 20H 00H 00H 12H 02H 01H。

3. 地址域

消息帧的地址域包含两个字符(ASCII)或位(RTU),可能的从站地址是 0～247(十进制)。单个设备的地址范围是 1～247。主站通过将要联络的从站的地址放入消息中的地址域来选通从站,当从站发送回应消息时,它把自己的地址放入回应的地址域中,以便主站能够知道是哪一个设备做出回应。

地址 0 是用于广播的地址,所有的从站都能识别。当 Modbus 协议用于更高水准的网络时,广播可能不被允许或以其他方式代替。

4. 功能代码域

消息帧中的功能代码域包含两个字符(ASCII)或 8b(RTU),可能的代码范围是十进制的 1～255。其中,有些代码适用于所有控制器,有些适用于某种控制器,还有些保留以备后用。

当消息从主站发往从站时,功能代码域将告知从站需要执行哪些行为,例如,去读取输入的开关状态、读一组寄存器的数据内容、读从站的诊断状态及允许调入、记录、校验从站中的程序等。

当从站回应时,它使用功能代码域来指示是正常响应(无误)还是差错响应(有某种错误发生)。对于正常响应,从站仅回应相应的功能代码。对于差错响应,从站返回一个差错码,具体方法为:将功能代码的最高位置 1。

例如,一从站发往从站的消息要求读一组保持寄存器,产生的功能代码为 00000011(十六进制为 03H),对正常响应,从站仅回应同样的功能代码;对差错响应,它返回 10000011(十六进制为 83H)。

除功能代码因异议错误做了修改外,从站会将一异常码放到回应消息的数据域中,这能告诉主站发生了什么错误。

主站应用程序得到差错响应后,典型的处理过程是重发消息,或者诊断发给从站的消息并报告给操作人员。

5. 数据域

数据域是由两个十六进制数集合构成的，范围为 00～FFH。根据网络传输模式，这可以是由一对 ASCII 字符组成或一个 RTU 字符组成的。

从主站发给从站的消息的数据域包含附加的信息，指示从站必须用于执行由功能代码所定义的行为。例如，主站需要从站读取一组保持寄存器(功能代码为 03H)，数据域则指定了起始寄存器及要读的寄存器数量。如果主站写一组从站的寄存器(功能代码为 10H)，数据域则指明了要写的起始寄存器、要写的寄存器数量、数据域的数据字节数及要写入寄存器的数据。如果没有错误发生，由从站返回的数据域包含请求的数据；如果有错误发生，此域包含异常码，主站应用程序可以用来判断下一步要采取什么行动。

在某种消息中，数据域可以是不存在的(0 长度)。例如，主站要求从站回应通信事件记录(功能代码为 OBH)时，从站不需要附加任何信息。

3.3.2 Modbus 的差错检验

标准的 Modbus 串行网络采用两种错误检测方法。奇偶校验对每个字符都可用，帧检测(LRC 或 CRC)应用于整个消息。它们都是在消息发送前由主设备产生的，从设备在接收过程中检测每个字符和整个消息帧。

退出传输前用户要给主设备配置一预先定义的超时时间间隔，这个时间间隔要足够长，以使任何从设备都能作为正常响应。如果从设备检测到一传输错误，那么消息将不会接收，也不会对主设备作出响应。这样超时事件将触发主设备来处理错误。发往不存在的从设备的消息也会产生超时。

1. 奇偶校验

用户可以配置控制器是奇校验还是偶校验，或无校验。这将决定每个字符中的奇偶校验位是如何设置的。

如果指定了奇校验或偶校验，那么 1 的位数将算到每个字符的位数中(ASCII 模式为 7 个数据位，RTU 模式为 8 个数据位)。例如，RTU 字符帧中包含以下 8 个数据位：1 1 0 0 0 1 0 1。

帧中 1 的总数是 4 个。如果使用了偶校验，那么帧的奇偶校验位将是 0，使 1 的个数仍是偶数(4 个)；如果使用了奇校验，那么帧的奇偶校验位将是 1，使 1 的个数是奇数(5 个)。

如果没有指定奇偶校验，那么传输时没有校验位，也不进行校验检测，而是将一个附加的停止位填充至要传输的字符帧中。

2. LRC 检测

使用 ASCII 模式时，消息包括了一基于 LRC 方法的错误检测域。LRC 域检测消息域中除开始的冒号及结束的回车换行符以外的内容。

LRC 域包含一个 8 位二进制数的字节。LRC 值由传输设备来计算并放到消息帧中，接收设备在接收消息的过程中计算 LRC，并将它和接收到消息中 LRC 域中的值比较，如果两值不相等，则说明有错误。

LRC 方法是将消息中的 8b 的字节连续累加，不考虑进位。

3. CRC 检测

使用 RTU 模式时，消息包括了一基于 CRC 方法的错误检测域。CRC 域检测整个消息的内容。

CRC 域是两个字节，包含一个 16 位的二进制数。它由传输设备计算后加入到消息中。接收设备重新计算收到消息的 CRC，并与接收到的 CRC 域中的值比较，如果两值不同，则有错误。

3.3.3 Modbus 的功能码

Modbus 协议定义了公共功能码、用户定义功能码和保留功能码 3 种功能码。

公共功能码是指被确切定义的、唯一的功能码，由 Modbus-IDA 组织确认，可进行一致性测试，且已归档为公开。

用户定义功能码是指用户无须得到 Modbus-IDA 组织的任何批准就可以选择和实现的功能码，但是不能保证用户定义功能码的使用是唯一的。

保留功能码是某些公司在传统产品上现行使用的功能码，不作为公共功能码使用。Modbus 功能码如表 3-3 所示。

表 3-3 Modbus 功能码

功能码	名　　称	作　　用
01	读线圈状态	取得一组逻辑线圈的当前状态(ON/OFF)
02	读输入状态	取得一组开关输入的当前状态(ON/OFF)
03	读保持寄存器	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	写单个线圈	强制设置一个逻辑线圈的通断状态
06	写单个寄存器	把具体的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，这 8 个线圈的地址由控制器决定，用户逻辑可以定义这些线圈，以说明从机状态，短报文适用于迅速读取状态
08	回送诊断校验	把诊断校验报文送从机，以对通信处理进行评鉴
09	编程(只用于 484)	使主机模拟编程功能，修改从机逻辑
10	探询(只用于 484)	可使主机与一台正在执行长程序任务的从机通信，探询该从机是否已完成其操作任务，仅在含有功能码 09 的报文发送后，本功能码才发送
11	读取事件计数	可使主机发出单询问，并随即判定操作是否成功，尤其是该命令或其他应答产生通信错误时

续表

功能码	名　　称	作　　用
12	读取通信事件记录	可使主机检索每台从机的 Modbus 事务处理通信事件记录。如果某项事务处理完成，记录会给出有关错误
13	编程(184/384 484 584)	可使主机模拟编程功能，修改从机逻辑
14	探询(184/384 484 584)	可使主机与正在执行任务的从机通信，定期探询该从机是否已完成其程序操作，仅在含有功能码 13 的报文发送后，本功能码才发送
15	写多个线圈	强制设置一串连续逻辑线圈的通断
16	写多个寄存器	把具体的二进制值装入一串连续的保持寄存器
17	报告从机标识	可使主机判断编址从机的类型及该从机运行指示灯的状态
18	884 和 MICRO 84	可使主机模拟编程功能，修改 PC 状态逻辑
19	重置通信链路	发生非可修改错误后，使从机复位于已知状态，可重置顺序字节
20	读取通用参数(584L)	显示扩展存储器文件中的数据信息
21	写入通用参数(584L)	把通用参数写入扩展存储文件，或修改之
22～64	保留作扩展功能备用	—
65～72	留作用户功能	留作用户功能的扩展编码
73～119	非法功能	—
120～127	保留	留作内部作用
128～255	保留	用于异常应答

Modbus 协议是为了读写 PLC 数据而产生的，主要支持输入离散量、输出线圈、输入寄存器和保持寄存器涉及的数据类型。Modbus 功能码与对应的数据类型如表 3-4 所示。

表 3-4　Modbus 功能码与数据类型对应表

代　　码	功　　能	数 据 类 型
01	读取线圈状态	位
02	读取输入状态	位
03	读取保持寄存器	整型、字符型、状态字、浮点型
04	读取输入寄存器	整型、状态字、浮点型
05	写单个线圈	位
06	写单个寄存器	整型、字符型、状态字、浮点型
15	写多个线圈	位
16	写多个寄存器	整型、字符型、状态字、浮点型

Modbus 协议相当复杂，但常用的功能码主要是 01、02、03、04、05、06、15 和 16。

3.3.4 Modbus的编程方法

由RTU模式消息帧格式可以看出，在完整的一帧消息开始传输时，必须和上一帧消息之间至少有3.5个字符时间的间隔，这样接收方在接收时才能将该帧作为一个新的数据帧接收。另外，在本数据帧进行传输时，帧中传输的每个字符之间必须不能超过1.5个字符时间的间隔，否则，本帧将被视为无效帧，但接收方将继续等待和判断下一次3.5个字符的时间间隔之后出现的新一帧并进行相应的处理。

因此，在编程时首先要考虑1.5个字符时间和3.5个字符时间的设定和判断。

1. 字符时间的设定

在RTU模式中，1个字符时间是指按照用户设定的波特率传输一个字节所需要的时间。

例如，当传输波特率为2400b/s时，1个字符时间为

$$11\times 1/2400\approx 4583(\mu s)$$

同样，可得出1.5个字符时间和3.5个字符时间分别为

$$11\times 1.5/2400=6875(\mu s)$$

$$11\times 3.5/2400\approx 16\,041(\mu s)$$

为了节省定时器，在设定这两个时间段时可以使用同一个定时器，定时时间取0.5个字符时间，同时设定两个计数器变量为 m 和 n，用户可以在需要开始启动时间判断时将 m 和 n 清零。而在定时器的中断服务程序中，只需要对 m 和 n 分别做加1运算，并判断是否累加到3和7。当 $m=3$ 时，说明1.5个字符时间已到，此时可以将1.5个字符时间已到标志T15FLG置成01H，并将 m 重新清零；当 $n=7$ 时，说明3.5个字符时间已到，此时将3.5个字符时间已到标志T35FLG置成01H，并将 n 重新清零。

当波特率为1200～19 200b/s时，定时器定时时间均采用此方法计算而得。

当波特率为38 400b/s时，Modbus通信协议推荐此时1个字符时间为500μs，即定时器定时时间为250μs。

2. 数据帧接收的编程方法

在实现Modbus通信时，设每个字节的一帧信息需要11位，其中1位起始位、8位数据位、2位停止位、无校验位。通过串行口的中断接收数据，中断服务程序每次只接收并处理一字节数据，并启动定时器实现时序判断。

当接收新一帧数据时，在接收完第一个字节之后，置一帧标志FLAG为0AAH，表明当前存在一有效帧正在接收，在接收该帧的过程中，一旦出现时序错误，就将帧标志FLAG置成55H，表明当前存在的帧为无效帧。其后，接收到本帧的剩余字节仍然放入接收缓冲区，但标志FLAG不再改变，直至接收到3.5字符时间间隔后的新一帧数据的第一个字节，主程序即可根据FLAG标志判断当前是否有有效帧需要处理。

Modbus数据串行口接收中断服务程序结构如图3-14所示。

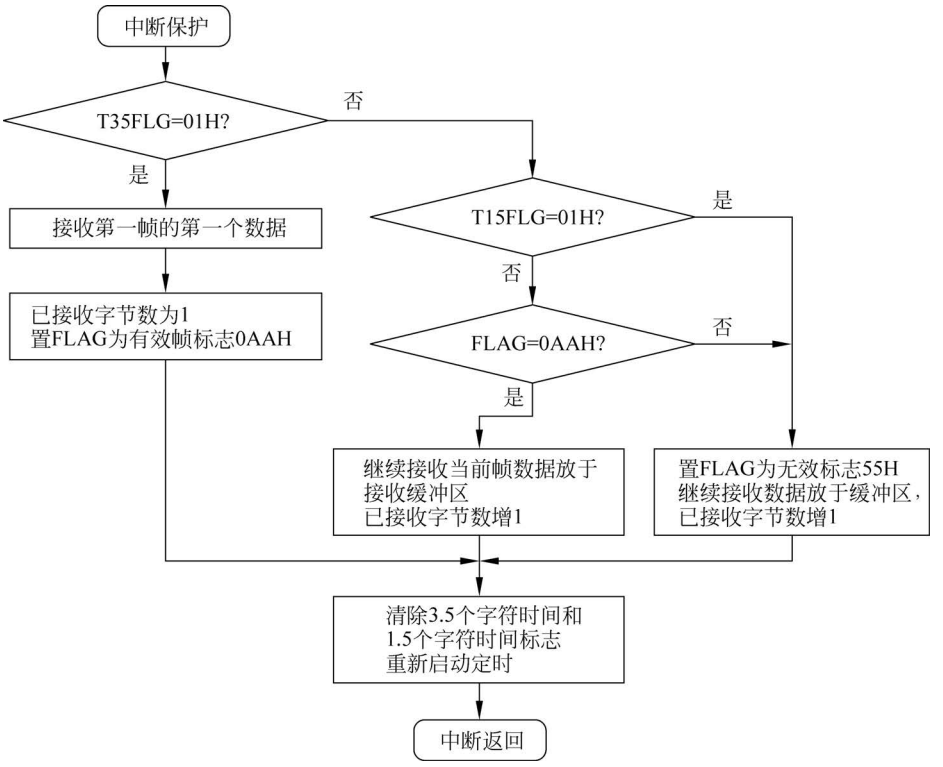


图 3-14　Modbus 数据串行口接收中断服务程序结构

3.4　Modbus TCP

Modbus 是目前应用最广泛的现场总线协议之一。1999 年推出了在以太网中运行的工业以太网协议(Modbus TCP)。Modbus TCP 以一种比较简单的方式将 Modbus 帧嵌入 TCP 帧中。互联网编号分配管理机构(Internet Assigned Numbers Authority,IANA)给 Modbus 协议赋予 TCP 端口 502,这是其他工业以太网协议所没有的。Modbus 标准协议已被提交给互联网工程任务部(Internet Engineering Task Force,IETF)并成为以太网标准。Modbus 也是使用广泛的事实标准,其普及得益于使用门槛低,无论用串口还是用以太网,硬件成本低廉,Modbus 和 Modbus TCP 都可以免费获取,且在网上有很多免费资源,如 C/C++、Java 样板程序,ActiveX 控件及各种测试工具等,所以用户使用起来很方便。另外,几乎可找到任何现场总线到 Modbus TCP 的网点,方便用户实现各种网络之间的互联。

3.4.1　Modbus TCP 概述

Modbus TCP 的通信参考模型如图 3-15 所示。从图 3-15 中可以看到,Modbus 是 OSI

参考模型第 7 层上的应用层报文传输协议，它在连接至不同类型总线或网络的设备之间提供客户机/服务器通信。

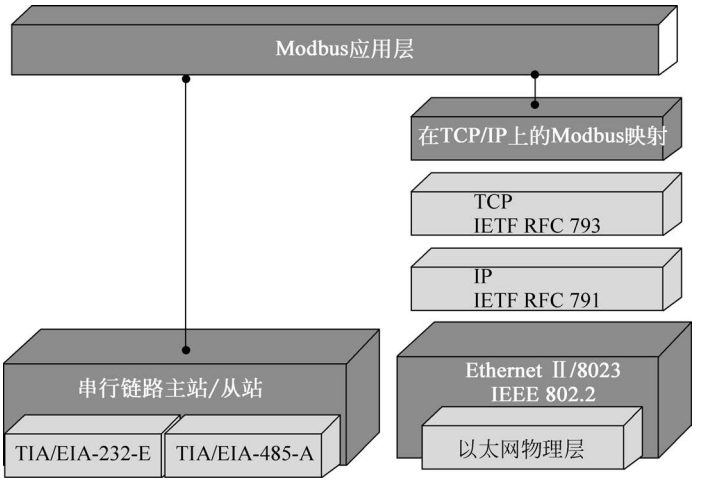


图 3-15　Modbus TCP 的通信参考模型

Modbus 是一个请求、应答协议，并且提供功能码规定的服务。目前，Modbus 网络支持有线、无线类的多传输介质。有线介质包括 EIA/TIA-232、EIA-422、EIA/TIA-485，以太网和光纤等。如图 3-16 所示为 Modbus TCP 的通信体系结构，每种设备(PLC、HMI、控制面板、驱动设备和 I/O 设备等)都能使用 Modbus 协议来启动远程操作。在基于串行链路和以太网 TCP/IP 的 Modbus 上可以进行相同的通信，一些网关允许在几种使用 Modbus 协议的总线或网络之间进行通信。

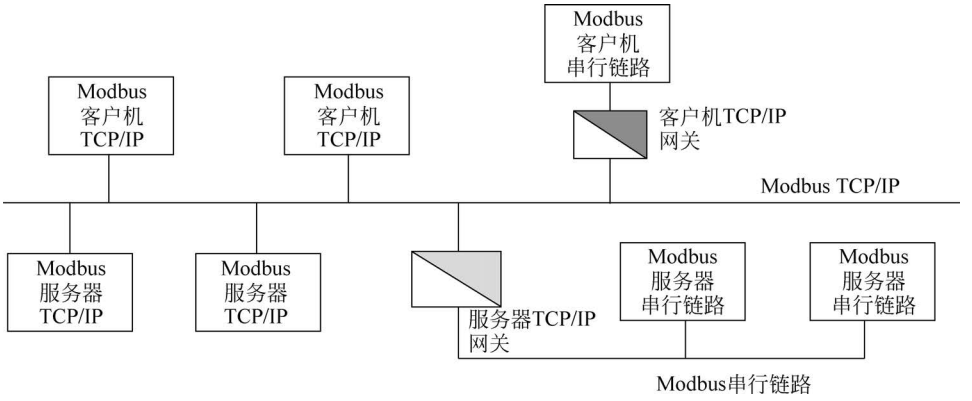


图 3-16　Modbus TCP 的通信体系结构

Modbus TCP 具有以下特点。

(1) TCP/IP 已成为信息行业的事实标准。

世界上超过 90%的网络都使用 TCP/IP，只要在应用层使用 Modbus TCP，就可实现工

业以太网数据交换。

(2) 易于与各种系统互联。

采用 Modbus TCP 的系统可灵活应用于管理网络、实时监控及现场设备通信,强化了与不同应用系统互联的能力。

(3) 网络实施价格低廉。

由于 Modbus TCP 在原有以太网的基础上添加了 Modbus 应用层,所以 Modbus TCP 设备可全部使用通用网络部件,大大降低了设备成本。

(4) 满足用户要求。

目前,我国已把 Modbus TCP 作为工业网络标准之一,用户可免费获得协议及样板程序,可在 UNIX、Linux、Windows 系统环境下运行,不需要专门的驱动程序。在国外,Modbus TCP 被国际半导体产业协会(SEMI)定为网络标准,国际水处理、电力系统也把它作为应用的事实标准,还有越来越多行业将其作为标准来用。

(5) 高速的网络传输能力。

用户最关心的是所使用网络的传输能力,100Mb/s 以太网的传输结果为每秒 4000 个 Modbus TCP 报文,而每个报文可传输 125 个字(16bit),故相当于 4000×125=500 000 个模拟量数据(8 000 000 开关量)。

(6) 厂家能提供完整的解决方案。

工业以太网的接线元件包括工业集成器、工业交换机、工业收发器、工业连接电缆。工业以太网服务器支持远程和分布式 I/O 扫描功能、设备地址 IP 的设置功能、故障设备在线更换功能、分组的信息发布与订阅功能及网络动态监视功能,还包含支持瘦客户机的 Web 服务。Modbus TCP 还拥有其他工控设备的支持,如工业用人机接口、变频器、软启动器、电动机控制中心、以太网 I/O、各种现场总线的网桥,甚至带 Modbus TCP 的传感器,这些都为用户使用提供了方便。

3.4.2 Modbus TCP 应用数据单元

Modbus TCP 采用 TCP/IP 和以太网协议来传输 Modbus 信息,因此与 Modbus 串行链路数据单元类似,Modbus TCP 的应用数据单元就是将 Modbus 简单协议数据单元(PDU)按照 TCP/IP 标准进行封装而形成的。一个 TCP 帧只能传送一个 Modbus ADU,建议不要在同一个 TCP PDU 中发送多个 Modbus 请求或响应。Modbus TCP 采用客户机与服务器之间的请求响应式通信服务模式。在 TCP/IP 网络和串行链路子网之间需要通过网关互联。如图 3-17 所示为 Modbus TCP 应用数据单元的结构,可以看到,在 Modbus TCP 应用数据单元中有一个被称为 MBAP 的报文头,即 Modbus 应用协议报文

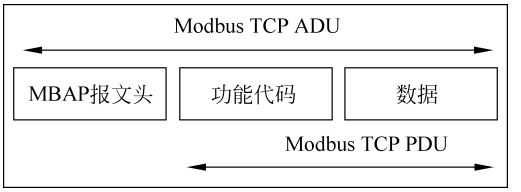


图 3-17 Modbus TCP 应用数据单元的结构

头，这种专用报文头的长度为7字节，该报文头所包含的字段如表3-5所示。

表3-5 MBAP报文头的字段

字 段	长度/B	描 述	客 户 机	服 务 器
事务处理标识符	2	识别Modbus请求/响应事务处理	由客户机设置	服务器从接收的请求中重新复制
协议标识符	2	0＝Modbus协议	由客户机设置	服务器从接收的请求中重新复制
长度	2	随后的字节数量	由客户机设置(请求)	由服务器设置(响应)
单元标识符	1	识别串行链路或其他总线上连接的远程从站	由客户机设置	服务器从接收的请求中重新复制

事务处理标识符用于事务处理配对；长度字段是后续字段的字节数，包括单元标识符和数据字段的字节数；单元标识符用于系统内的路由选择。通过TCP将所有Modbus TCP ADU发送至注册的502端口。

3.4.3 Modbus-RTPS

2008年10月，ISA展会期间，Modbus组织与IDA宣布合并，致力于基于以太网的控制方案的推广，合并后的Modbus-IDA组织横跨欧美，成为能够与PROFINET和Ethernet/IP抗衡的阵营。

Modbus-RTPS是Modbus-IDA组织开发的基于以太网TCP/IP和Web互联网技术的实时以太网，其中的RTPS(Real-Time Publish/Subscribe)是基于以太网TCP/IP的实时扩展通信协议。RTPS协议及其应用程序接口由一个兼容各种设备的中间件来实现，它采用美国RTI(Real-Time Innovations)公司的NDDS(Network Data Delivery Service)3.0实时通信系统。

RTPS协议基于发布者/预订者建立，进行扩展后增加了设置数据发送截止时间、控制数据流速率和使用多址广播等功能。它可以简化为一个数据发送者和多个数据接收者通信的工作，进而极大地减轻了网络的负荷。

习题

1. 简述Modbus的特点。
2. 简述Modbus通信模型和工作原理。
3. 简述通用Modbus帧的组成和各部分功能。
4. 简述RS-485接口标准与RS-232接口标准的区别。
5. 简述Modbus串行链路协议规定的差错检验方式。
6. 简述Modbus常用的功能码。