PROFIBUS 和 MODBUS 协议互连方法的研究

李　娜,方彦军

(南京师范大学 控制科学与工程系,江苏 南京 210042)

[摘要]　在介绍了 PROFIBUS 和 MODBUS 两种现场总线协议模型的基础上,探讨了 PROFIBUS 和 MODBUS 两种现场总线的协议下协议下的网络互连技术与协议转换模型. 在不改变原有的网络体系结构的条件下,采用网关进行协议转换,构建了自低层向高层逐层进行的协议转换模型. 同时也给出了网关实现的具体软、硬件设计方法,解决了异构网络互连问题.

[关键词]　现场总线,协议转换,互连方法

[中图分类号]TP14,　[文献标识码]B,　[文章编号]1672-1292-(2004)03-0023-04

0　引言

现场总线控制系统由于它的开放性、分散性和完全可互操作性等特点,正成为未来新型工业控制系统的发展方向. 但现场总线协议标准众多且通讯协议差异很大,互不兼容. 这一方面给现场总线控制系统的集成带来了很大困难,导致出现"自动化孤岛";另一方面也给现场总线技术的推广以及现场总线控制系统的应用带来了不利影响. 本文运用数据链路层的网络互连技术,对 PROFIBUS-DP 和 MODBUS 总线之间的协议转换进行了研究.

1　PROFIBUS-DP 与 MODBUS 协议

1.1　PROFIBUS-DP 协议

PROFIBUS 是应用于制造业和过程自动化领域中的现场总线标准[1]. 它包括 3 个兼容的版本: PROFIBUS-DP、PROFIBUS-PA 和 PROFIBUS-FMS. PROFIBUS-DP 主要应用于自动控制系统与和分散外围设备 I/O 及智能现场仪表之间的高速数据通信. PROFIBUS 协议同样采用 ISO/OSI 简化模型,它使用了 1、2 层外加用户接口,3 至 7 层未加描述. 这种精简的结构确保高速数据传输.

PROFIBUS-DP 的物理层是根据 EIA 标准的 RS-485 制定的[1]. 数据链路层描述了用于数据传输中报文的一般格式、安全机制和可用的传输服务. PROFIBUS-DP 协议的任务只是定义用户数据怎样通过总线从一个站传送到另一个站. 在这里,传输协议并没有对(DDLM)提供对第 2 层的访问. 在用户接口中规定了 PROFIBUS-DP 设备的应用功能,以及各种类型的系统和设备的行为特性.

根据 OSI 参考模型,第 2 层规定总线存取控制、数据安全性以及传输协议和报文的处理. 在 PROFIBUS 中,第 2 层称为 FDL 层(现场总线数据链路层). 第 2 层的数据服务如表 1 所示. 这些服务由上层协议通过第 2 层的服务存取点(Service Access Point,SAP)调用. PROFIBUS-DP 使用了这些服务的子集,即 SRD 和 SDN 服务. 在 PROFIBUS-DP 中,每个 SAP 都赋有一个定义明确的功能,其中 Default SAP 用于数据交换.

表 1　PROFIBUS 传输服务

服务	功能	DP	PA	FMS
SDA	发送数据需应答			×
SRD	发送和请求数据需应答	×	×	×
SDN	发送数据不需应答	×	×	×
CSRD	循环地发送和请求数据需应答			×

每个 PROFIBUS-DP 系统可包含 3 种不同类型的设备: 一类主站(master)、二类主站和从站(slave). 主从站之间采取主从方式的总线存取协议. 从图 1 数据传输原理图中可以得到主从站之间报文通信的基本顺序.

1.2　MODBUS 协议

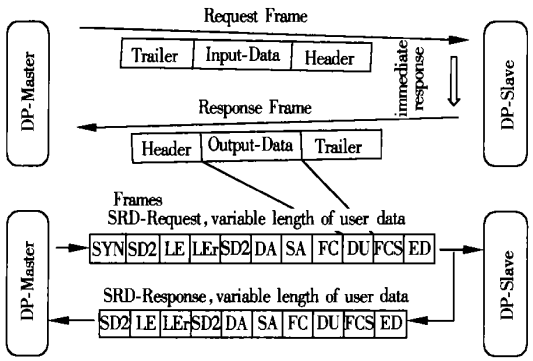
自 1979 年以来 MODBUS 协议是工业串行通讯事实上的标准[2]. MODBUS 标准定义了应用层的通信协议,位于 OSI 模型的第 7 层. 连接在同一总线或网络中的设备以"client/server"模式进行通信. 它目前可应用于:基于以太网的 TCP/IP 协议;不同媒介的异步串行通信(EIA/TIA-232-E,EIA-422,EIA/TIA-485A,光纤,无线电等);MODBUS PLUS,一种高速令牌网络.

当它应用于串行总线上时,数据交换在一个主站和几个从站之间进行. 主站执行了 client 的功

收稿日期: 2003-12-24.

作者简介: 李娜(1977 -),女,硕士,助教,主要从事现场总线控制系统方面的教学与研究. E-mail:linananjing@163.com

能,从站执行了 server 的功能. MODBUS 通信协议栈,参见文献[1].

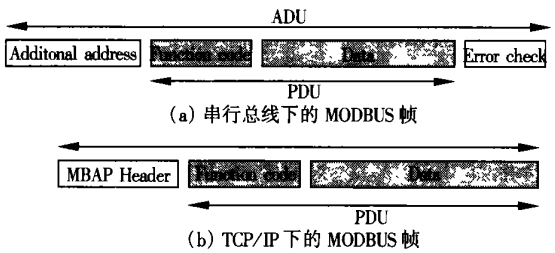


Syn = Synchronisation Time　　SA = Source Address
SD2 = Start Delimitter 2　　FC = Function Code
LE = Length　　DU = Data Unit
LEr = Repeated Length　　FCS = Frame Check Sequence
DA = Destination Address　　ED = End Delimitter

图 1　数据传输原理

MODBUS 协议定义了一个协议数据单元 PDU (protocol data unit),它与下层的通信层次无关. MODBUS 协议定义了 3 种 PDU,分别为:MODBUS 请求 PDU,mb. req. pdu;MODBUS 应答 PDU,mb. rsp. pdu;MODBUS 异常响应 PDU,mb. excep. rsp. pdu.

MODBUS 协议映射到特定的总线或网络上时,要在 PDU 的前后附加特定的域组成应用数据单元 ADU (application data unit). MODBUS 协议运行在串行总线和以太网总线上时的 ADU 格式分别如图 2(a)、图 2(b)所示.



(a) 串行总线下的 MODBUS 帧

(b) TCP/IP 下的 MODBUS 帧

图 2　MODBUS 帧

ADU 由 client/master 建立,并由它启动一次 MODBUS 通信. 功能代码(function code)指明了 server 要执行什么操作. 一些功能代码后面还附加了子功能码(sub-function)以定义多项操作. Client 向 server 发送的消息中的 Data 域是 client 请求 server 要执行某项功能所需的附加信息. 在某些特定的请求中,server 不需要附加信息,功能代码本身已指明了请求的操作. 在这种情况下数据字段长度为 0.

如果对于一个正常接收的 ADU,如果它的 MOD-BUS 功能代码没有错误,server 对 client 响应的 Data 域包含了 client 请求的数据. 如果功能代码有错误,则 Data 域中包含一个异常代码. Client 可以根据这个异常代码来决定下一步的行动.

2　网络互连与协议转换

由于 TCP/IP 协议复杂,本文只讨论运行在串行总线上的 MODBUS 协议与 PROFIBUS-DP 的协议转换.

为了在不改变原有网络的体系结构的情况下,实现网络间的互连,需要在互连的网络中间增加一个协议转换设备. 按照 OSI 模型,协议转换可以在物理层实现,也可以在数据链路层上、网络层上实现. 物理层上的互连设备通常可以采用中继器,它仅是对比特流的拷贝转发,数据在中继器内不进行任何形式的转换. 这样形成的互连系统从数据链路层的角度看基本上可视作一个单一网络. 网络在物理层的互连要求所连接的子网必须具有相同的数据传输速率和链路协议;数据链路层的互连设备可采用网桥[3]. 它是按帧接收或传送信息的. 当从一条链路上收到一帧信息后,网桥先检查链路层协议的包头,如果可能的话,再将该信息传送到另一条链路;网络层的互连采用路由器,但对高层协议不同的网络之间的互连爱莫能助;对于高层的网络互连要用网关来实现. 网关相当于一个协议转换器,可以是双向的,也可以是单向的,主要用来连接不同协议的网络.

PROBUS-DP 与 MODBUS 虽然在物理层都可采用 RS-485 总线,但它们的数据链路层和用户接口/应用层完全不同,因此是两个异构的网络. 要实现这两种网络的互连就必须采用网关进行协议转换. 协议转换一般采用分层的方法,自低层向高层逐层进行. 低层支持高层,高层调用低层. 低层断开后,高层连接也随之断开,但是高层的断开却不会影响低层. 图 3 给出了 PROFIBUS-DP 到 MODBUS 协议转换的通信模型的一个模型.

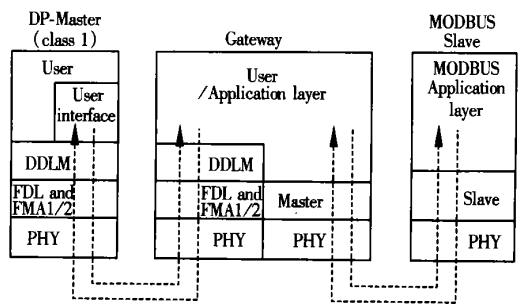


图 3　PROFIBUS-DP 到 MODBUS 协议转换通信模型

在图 3 所示的模型中,一次通信由 PROFIBUS-DP 主站启动. 首先,DP-Master 将在请求 PDU 的前后加上地址域和 CRC 校验组成一个 ADU,然后调用数据链路层 Default SAP 服务. 数据链路层将 ADU 作为它的报文的 DU 域,组成一个 SRD 服务报文再交付给物理层发送到网关. 网关的数据链路层接收到有效的 SRD 报文后,通知 DP 用户接口,DP 用户接口调用 Default SAP 服务将其 DU 中的数据(ADU)取走. 网关可不对 ADU 做任何处理,直接向 MODBUS 的数据链路层发送出去. 被寻址的 MODBUS 从站的数据链路层接收到网关发过来的有效的 ADU 后,应用层将 PDU 取走. MODBUS 从站依据 PDU 的要求执行相应的操作,并将结果组成一个应答 PDU 或者异常响应 PDU,按前述的逆向过程发送到 DP-Master. 这样,由 DP-Master 启动的对 MODBUS 从站的访问就完成了.

在实际应用中,DP-Master 往往是 PLC,在 PLC 中进行 CRC 校验比较困难. 因此开发网关时,可在网关的用户接口/MODBUS 应用层完成实现 CRC 校验. 这样可以将 DU 中的数据进行简化,由 address + PDU 组成. 由网关也可对 PDU 的合法性进行初步检验,如检验功能代码是否合法(这项工作本应由 MODBUS 从站完成),如不合法,则由网关直接产生 mb_excep_rsp_pdu 发送到 DP-Master,从而提高网络的响应速度.

MODBUS 协议规定,在串行总线上,MODBUS ADU 的最大长度为 256 字节. PROFIBUS 调用 SRD 传送服务时,DU 中数据长度为 1～224 个字节. 因此,网关与 MODBUS 从站之间的数据帧最大长度不能超过 226 个字节(224 字节 + 2 字节 CRC).

3 网关的实现

网关的实现包括软件设计和硬件设计两部分.

3.1 硬件设计

PROFIBUS 是开放的、与制造商无关、无知识产权保护的标准. 原则上,PROFIBUS 协议在任何微处理器上都可以实现[3]. 通信的速度超过 500kbps 时,推荐使用协议专用芯片(ASIC). 由于 PROFIBUS 协议复杂,专用芯片的使用也可以使 PROFIBUS-DP 总线设备的开发周期大大缩短. DP 从站功能最常用的 ASIC 是 SIEMENS 公司的 SPC3[4]. SPC3 将完整的 PROFIBUS-DP 协议集成在芯片中,可独立完成全部 PROFIBUS-DP 通信功能,加速了通讯协议的执行. SPC3 还提供格式化的用户数据接口,源码提供的固态程序使用户易于访问这些接口. MODBUS 协议也是完全开放的协议,与 PROFIBUS 协议相比,MODBUS 协议要简单得多,不须用协议芯片实现. 图 4 给出一个基于 89C52 单片机和 SPC3 的网关的结构框图. PROFIBUS-DP 所需要的串行口由 SPC3 提供,MODBUS 需要的串行口则由单片机提供.

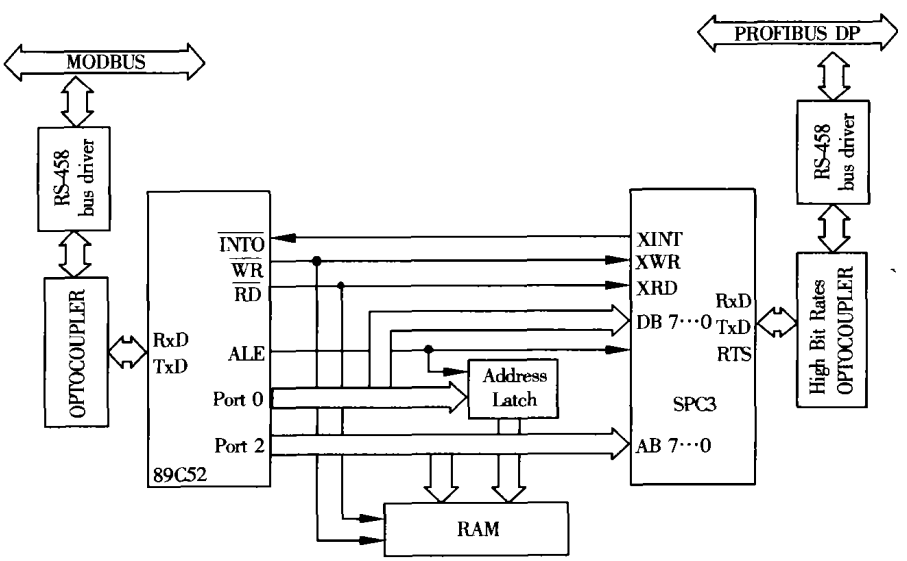


图 4 网关硬件原理框图

3.2 软件设计

软件主要包括来自 MODBUS 从站的数据处理和 PROFIBUS-DP 接口程序. 数据处理程序主要对数据处理、分析,然后上传,同时接受来自主站的命令和数据,然后进行相应的操作. 这通过在 89C52 单片机上编程实现. PROFIBUS-DP 接口程序主要负责配置、诊断和数据交换. 这通过对 SPC3 进行设置完成,主程序流程图如图 5. 其中 SPC3 启动的初始

化包括设置 SPC3 允许的中断、写入从站识别号和地址、设置 SPC3 方式寄存器、设置诊断缓冲区、参数缓冲区、配置缓冲区、地址缓冲区、初始长度,并根据以上初始值求出各个缓冲区的指针及辅助缓冲区的指针,根据传输的数据长度,确定输入缓冲区、输出缓冲区及指针等.

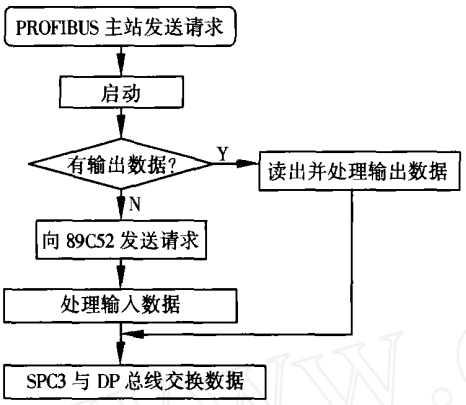


图 5　主程序流程图

4　结束语

使用本文研究设计的关于 PROFIBUS-DP 与 MODBUS 两种总线的网关,DP-Master 可以对 MODBUS 网络上的站点进行透明的访问,解决了这两种异构网络的互连问题.按照图 3 所示的通信模型设计的网关,PROFIBUS-DP 主站调用了 MODBUS 从站的服务,而逆向却不能实现,从这个意义讲该网关是个单向的网关,这是由于这两种总线的主从站式的机制所决定的.当然,也可以设计另外一个通信模型,由 MODBUS 主站调用的一个 PROFIBUS-DP 从站的服务.由于 PROFIBUS-DP 是 IEC 的标准之一[5],显然前一种模型实用价值更大一些.

[参考文献]

[1] 阳宪惠. 现场总线技术及应用[M]. 北京:清华大学出版社,1999. 20-25.

[2] Grahan Loose. Fieldbus the user's perspective: measument control, feature on fieldbus-part2 [J]. Measument Control 1994(27):47-51.

[3] Whetel J. K. Integrating the world wide web and Database technology[J], AT&T Technical journal 1996 21(2):16-21.

[4] 王福来,吴世红,蔡树梅等. 采用 SPC3 的职能型 PROFIBUS-DP 现场总线接口的开发[J]. 电气传动 2000(2):51-54.

[5] Manfred Popp. PROFIBUS-DP 快速入门[M]. 北京:机械工业出版社,1997. 101-120.

Research on Interlinking Method between PROFIBUS and MODBUS Protocol

LI Na, FANG Yanjun

(Department of Control Science and Engineering, Nanjing Normal University, Nanjing 210042, China)

Abstract: In this paper, the protocol conversion mode between Profibus and Modbus protocol is discussed based on the research in the two kinds of fieldbus. The interlinking technology and conversion model are studied. Without changing the net structure and with the gateway applied to perform the conversion, the interlinking model is constructed from bottom to top level. The outline of gateway implementation is discussed with the design of software and hardware given in the paper.

Key words: fieldbus, protocol conversion, interlinking method

[责任编辑:刘健]