基于 PROFIBUS 和以太网的嵌入式监测系统

王志秦

(唐山学院 信息工程系,河北 唐山 063000)

摘要:基于 PROFIBUS 和以太网的嵌入式监测系统,利用嵌入式技术和以太网技术为 PROFIBUS 总线监测和诊断提供了解决方案。该系统采用 ARM 嵌入式微处理器作为控制系统核心,利用嵌入式 TCP/IP 协议与 PROFIBUS 总线协议实现对现场设备的远程监测和诊断。

关键词:以太网;嵌入式监测系统;ARM;PROFIBUS

中图分类号:TP273.5 **文献标志码**:A **文章编号**:1672-349X(2015)03-0036-03

DOI:10.16160/j.cnki.tsxyxb.2015.03.013

A PROFIBUS and Ethernet Based Embedded Monitoring System

WANG Zhi-qin

(Department of Information Engineering, Tangshan College, Tangshan 063000, China)

Abstract: The embedded monitoring system based on PROFIBUS and Ethernet combines embedded technology, Ethernet technology and field bus diagnostic technology. It uses the ARM embedded microprocessor as the core of the system. The embedded TCP/IP protocol and PROFIBUS protocol are used for monitoring and diagnostics.

Key Words: Ethernet; embedded monitoring system; ARM; PROFIBUS

0 引言

PROFIBUS 总线广泛应用于现场工业控制设备中,是工业现场总线标准规范之一。现有小型工业企业控制系统升级改造和信息化集成过程中,迫切需求一种低成本的、基于以太网网络的、对 PROFIBUS 总线控制系统进行监测和诊断的系统。现有的基于 PC 机和 OPC 技术的监测和诊断系统,技术复杂,不适应恶劣的工业现场应用场合,成本高,阻碍了监测诊断系统的应用发展[1]。

针对小型工业企业信息化集成度低,自动控制系统远程监测诊断技术复杂,设备成本高等特点,研究以太网信息融合环境下 PROFIBUS 总线设备的远程监测与诊断问题,将嵌入式技术、以太网技术和现场总线诊断技术相结合,设计基于 PROFIBUS 总线和以太网的嵌入式监测系统。系统采用 ARM 嵌入式微处理器作为控制系统核心,利用嵌入式 TCP/IP 协议与 PROFIBUS 总线协议实现对现场设备的远程监控和诊断。本系统能够有效地对 PROFIBUS 总线控制系统进行监测和诊断,将控制系统的状态和诊断信息传输给以太网的终端,具有成本低、智能化、信息集成化等特点,可以较低成本方便地实现工业控制网络与办公网络的信息化集成。

1 系统硬件设计

1.1 总体设计

基于 PROFIBUS 和以太网的嵌入式监测系统处于工业控制系统与局域以太网网络之间,通过解析 PROFIBUS 网络上传输的协议数据获得与监测和诊断有关的有效信息,通过以太网网络将数据传送至特定的终端设备。系统原理如图 1 所示。

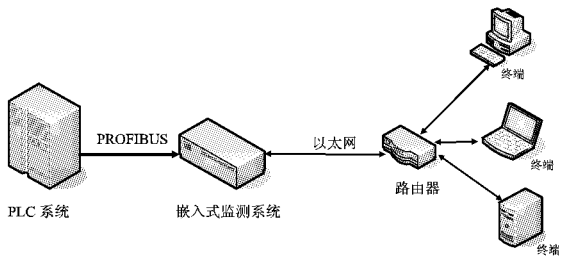

图 1 系统原理图

系统采用 ARM 处理器构建嵌入式系统硬件设备,包含 PROFIBUS 总线协议接口芯片和以太网控制器接口芯片。

收稿日期:2015-03-18

基金项目:唐山市科技支撑项目(12110235b)

作者简介:王志秦(1979—),女,河北唐山人,讲师,硕士,主要从事数字图像处理、无线传感器网络研究。

ARM 处理器具有处理速度快、成本低、片上资源丰富、功能强、编程方便、抗干扰能力强等优点，适合作为嵌入式系统设备的处理器核心。PROFIBUS 总线协议的物理层协议符合 RS485 总线协议，可采用该类器件构成接口电路，监听总线上的报文信息。以太网控制器接口器件集成了 IEEE802.3 协议标准的介质访问控制子层（MAC）和物理层的性能，支持以太网全双工通信方式，支持 UTP，AUI 和 BNC 自动检测，可以方便地与微处理器进行接口。由以上器件构成的系统再配以外部存储器和必要功能模块，作为系统的硬件基础。系统硬件总体结构如图 2 所示。

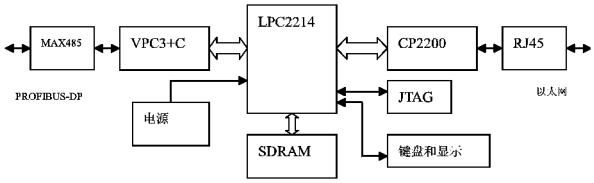

图 2　系统硬件总体结构图

1.2　主控制器模块

主控制器模块的主要功能就是通过控制 PROFIBUS-DP 协议芯片及以太网接口芯片来实现对 PROFIBUS 总线进行监控，分析有效数据并转换通信，主要包括 CPU，复位电路等。

CPU 采用具有 ARM7 内核的嵌入式处理器 LPC2214 作为控制核心。它是由 NXP 半导体公司推出的一款基于 ARM7TDMI-S 的微控制器，具有外部 RAM 存储器扩展总线，可用于代码或数据存储。LPC2214 微处理器是一款功能比较丰富，性能比较优异，性价比较高的芯片[2]。

1.3　PROFIBUS-DP 模块

PROFIBUS-DP 通信模块主要负责微控制器和现场总线的数据通信，包括参数配置和数据交换。它的硬件电路主要由协议芯片 VPC3＋C 和 RS485 接口组成。

VPC3＋C 是 SIMENS 公司提供的一种用于 PROFIBUS-DP 开放式工业现场总线智能化接口的芯片。它集成了全部的 PROFIBUS-DP 协议，其中包括方式寄存器、状态寄存器、中断寄存器、各种缓冲器指针和缓冲区等，从而减轻了智能从站的压力，可用于 12M 波特率总线。VPC3＋C 支持所有 8 位处理机和微处理器。内部的 DART 接口中，可完成并行数据流和串行数据流的互换[3]。

PROFIBUS-DP 接口通过 RS-485 传输，VPC3＋C 通过 RTS，TXD，RXD 引脚与 MAX3485 的引脚相连。

1.4　以太网模块

以太网控制器由 CP2200 以太网控制器与带有隔离变压器的 RJ45 接口构成。CP2200 以太网控制器是 SILABS 公司最新生产的单芯片以太网控制器。CP2200 可以提供目前应用最广泛的局域网技术，是体积较小和效能较高的以太网控制器。

1.5　其他功能模块

该系统的 SDRAM 部分是系统运行的主要区域，系统及用户数据、堆栈均位于此。这里选用 1 片 512K 字节的 IS61LV5128，数据总线宽度也是 16 位，占用的地址空间为 Ox0c000000h－Ox0c080000h。系统电源管理模块为系统不同模块提供稳定的电源供应。JTAG 接口提供系统调试功能。指示灯和按键提供系统运行状态和参数设定功能。

2　系统软件设计

在系统硬件平台的基础上，移植嵌入式操作系统 μC/OS-II 以及嵌入式 TCP/IP 协议栈，通过软件对 PROFIBUS 报文进行解析，将提取出的有效信息发送给上位机终端。

2.1　嵌入式操作系统

本系统采用嵌入式操作系统实现系统任务的调度和管理。μC/OS-II 是著名的、源码公开的实时内核，可用于各类 8 位、16 位和 32 位单片机或 DSP。它具有一个完整的、可移植、可固化、可剪裁的占先式实时多任务内核，已有 10 多年应用史，在诸多领域得到广泛应用。μC/OS-II 的可移植性较强，所以移植起来只需要在 OS_CPU.H 包含几个类型的定义和几个常数的定义；在 OS_CPU_C.C 和 OS_CPU_A.ASM 中包含几个函数的定义和时钟节拍中断服务程序的代码。

2.2　嵌入式 TCP/IP 协议

TCP/IP 通常被认为是一个四层协议系统，分别为：链路层、网络层、传输层、应用层，每一层都有相应的协议集合来实现不同的功能，其层次结构和主要的网络协议如图 3 所示。

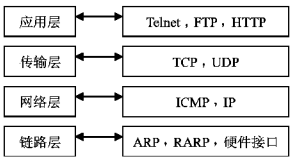

图 3　TCP/IP 层次结构图

为了既实现相应的功能又节省系统资源，需要对协议进行有针对性的模块化裁剪，使其变为 TCP/IP 协议簇的一个子集。经过裁剪后，只保留 IP 协议、TCP 协议和 UDP 协议。基于 PROFIBUS 和以太网的嵌入式监测系统，为解决传输速率差别和冗余信息阻塞，连续一致型的系统状态信息和诊断信息采用 UDP 协议进行发送，变化型系统状态信息和诊断信息采用 TCP 协议发送，终端控制信息采用 TCP 协议发送[4]。

2.3　PROFIBUS-DP 报文解析

基于 PROFIBUS 和以太网的嵌入式监测系统利用软件解析 PROFIBUS 总线报文，将诊断信息和控制信息发送给终端设备。PROFIBUS-DP 通过数据链路层协议，在不可靠的物理链路上实现可靠的数据传输。主站与从站之间的周期性数据传输采用主从方式，主站向从站发送或索取信息。系统针对 PROFIBUS-DP 不同的帧格式和 SAP，通过软件解析报文含义，将诊断信息发送给处理器。

2.3.1 PROFIBUS-DP 数据交换

VPC3 包括如下的服务访问点(服务):缺省 SAP(读写数据交换),SAP55(改变站地址),SAP56(读输入),SAP57(读输出),SAP58(向 DP 从站发控制命令),SAP59(读组态数据),SAP60(读从站诊断信息),SAP61(发送参数设置数据),SAP62(校验组态数据)。VPC3 中集成的 PROFIBUS-DP 状态机,用来描述 PROFIBUS-DP 站在每种情况下的行为。

在 VPC3+C 正常工作之前,需要进行初始化以配置需要的寄存器。主站和 VPC3+C 通过默认的服务访问点交换数据。主站和 VPC3+C 通过服务访问点 SAP60 处理诊断数据,VPC3+C 需要完成的任务主要包括以下 5 点。

①2 个缓冲区可用,VPC3+C 诊断数据发送缓冲区和用户诊断缓冲区。

②用户将外部诊断数据保存在 Diag buffer 中。

③有 NEW DIAG CMD 启动诊断数据的爆发。

④用"Diag buffer changed"确认诊断数据已传达。

⑤设置 Diag_Flag,下一个读写周期将有高优先权响应新的诊断请求。

2.3.2 报文解析与封装

PROFIBUS 报文的一般结构为:

SD	LE	LEr	SDr	DA	SA	FC	DU	FCS	ED

第一个字节 SD 指明报文帧结构。第二个字节 LE 为包括 DA,SA,FC,DSAP,SSAP 在内的所有数据的长度。第三个字节是 LEr,通过判断 LE 与 LEr 是否一致来判断报文是否有误。第四个字节 SDr 作用同 LEr,判断接收的报文是否有误。FCS 是校验码。最后一个字节 ED 固定为 0x16,用来标志报文的结束。

解析过程的主要部分是完成 DA,SA,FC,DSAP,SSAP,DU 的解析。DA 为报文的目的地址,SA 为源地址。如果 DA 的最高位为 0,则表示无 DSAP;如果 SA 的最高位为 0,则表示无 SSAP。FC 为功能码,它标识了报文帧的类型,同时包含了传输过程和相应控制过程中的信息,如是否数据丢失或需要重复传输、站点的种类以及 FDL 的状态等。DU 为数据单元,如果有 DSAP 和 SSAP,则除去 SAP 值剩余的 DU 值为具体数据。

数据封装,在简单报文模块完成数据的设置之后,即报文的 DA,SA,FC 及 DU 值已经由用户或操作员输入,此时报文解析模块完成对数据报文类型的选择,进行 DSAP,SSAP 的值的确定,计算 LE(LEr),FCS 的值,加入报头 SD 和结束符 ED,将整个报文进行完整封装,然后交由以太网转换模块进行发送[6]。

对 PROFIBUS 总线的各种 SAP 报文进行解析,将无用信息丢弃,将系统控制状态和错误诊断信息存储于数据缓冲池,并逐一发送。

3 系统实验

将基于 PROFIBUS 和以太网的嵌入式监测系统接入实验设备,PLC 控制系统采用西门子 S-300 系列 PLC,通过 PROFIBUS-DP 总线连接嵌入式监测系统,嵌入式监测系统软件预先设定 IP 地址和监控变量,并连接实验用计算机,计算机端通过网络测试软件接收监测数据。实验系统针对具有 80 个数字量 I/O 和 10 个模拟量 I/O 的控制系统运行状态和诊断信息进行处理和传输,当改变系统环境和参数时,需要重新设定系统软件参数。PROFIBUS-DP 总线传输速率为 187.5 kbit/s,以太网传输速率为 2 Mbit/s,数据包长度为 80 至 200 字节,以工作 20 min 采集的系统传输数据为例,系统传输信息的丢包率如表 1 所示。实验表明,UDP 数据包丢包率虽然较高,但其发送的是重复性数据,不影响关键数据接收。系统关键数据采用 TCP 协议发送,TCP 数据包丢包率较低,系统的状态数据和诊断数据能够进行有效传输。

表 1 系统丢包率

总包数	UDP 状态信息包	TCP 诊断信息包	收到 UDP 包数	收到 TCP 包数	UDP 丢包率	TCP 丢包率
53 477	48 531	4 946	35 427	4 847	27%	2%

4 结论

基于 PROFIBUS 和以太网的嵌入式监测系统利用嵌入式技术和以太网技术为 PROFIBUS 总线监测诊断提供了解决方案。该系统能够有效地对 PROFIBUS 总线控制系统进行监测和诊断,并将控制系统的状态和错误诊断信息传输给以太网网络的终端,具有低成本、智能化、信息集成化等特点,可以方便地实现工业控制网络与办公网络的信息化集成。

参考文献:

[1] 周悦,于海斌. Profibus 和 FF 现场总线的性能分析与评价[J]. 吉林大学学报:信息科学版,2004,22(4):434-437.

[2] 何一鸣,鲍玉军. 基于 LPC2214 的传感器网关设计[J]. 南京航空航天大学学报,2012,44(6):911-915.

[3] 肖红翼,高建民. 基于 dsPIC 的 Modbus-Profibus-DP 总线适配器的设计[J]. 自动化与仪表,2012(3):29-32.

[4] 韩光洁,赵海. Embedded Internet 环境下 TCP/IP 协议簇的约简[J]. 小型微型计算机系统,2004,25(9):1602-1606.

[5] Lu Sheng, Liu Tan. Research on the communication and network organization of SIMATIC S7-300 based on PROFIBUS-DP [J]. Machine tool&Hydraulics, 2007,35(9):15-19.

(责任编校:白丽娟)