

文章编号: 1671-7848(2006)03-0274-04

## Socket 套接字在工业数据通信中的应用

孙钦龙, 邵惠鹤

(上海交通大学 自动化系, 上海 200030)



**摘 要:** 针对工业数据采集领域的现状, 提出一种新的基于工业以太网的数据采集方案, 在工业过程控制中实现基于 Socket 套接字的实时数据通信。介绍了 Socket 套接字的基本概念和工业以太网技术的最新发展, 采用基于 Rabbit2000 高性能单片机扩展的带有以太网通信接口的核心模块 BL2100 及其所对应的 Dynamic C 开发环境, 实现了基于 Socket 套接字的工业以太网数据通信, 并且给出了比较详细的流程。系统已经有数十套成功地应用于实际生产中, 满足了工业数据通信要求的实时性和准确性。

**关 键 词:** 工业数据通信; Socket; 工业以太网

**中图分类号:** TP 393; TP 274 **文献标识码:** A

## Application of Socket in Industrial Data Communication

SUN Qin-long, SHAO Hui-he

(Department of Automation, Shanghai Jiaotong University, Shanghai 200030, China)

**Abstract:** To the status of data acquisition field, a new communication scheme based on the Industrial Ethernet and Socket are introduced. The scheme uses the BL2100 network module cored by Rabbit2000 MCU and the development kit Dynamic C. A new data acquisition system is designed and detailed flow chart of the socket communication is narrated. The system is applied to manufacture field successfully, and high appraisalment is obtained.

**Key words:** industrial data communication; Socket; industrial ethernet

### 1 引 言

工业过程控制中需要测量和控制的变量很多, 以往基于 PC 机外接的数据采集卡, 采集的点数有限, 而且要直接和 PC 机的串口或者并口相连, 极大限制了 PC 机资源的充分利用。工业以太网的出现为构成开放式的模块化的数据采集奠定了基础。本项目开发一个基于工业以太网的嵌入式智能模块的开放式数据采集系统。

以太网是目前应用最广泛的网络, 它不但应用于商用网络, 同时在近年来大举进军工业控制领域, 取得了巨大的经济效益。以太网最初得到应用时, 它采用带有冲突检测的多路载波侦听协议(CS-MA/CD)和二进制指数回退算法。在这种协议和算法下, 当网络繁忙时, 它的非实时性和不确定性大大增加。因此, 以太网在很长的一段时间只能用于对实时性和确定性要求不是很高的办公网络, 它在工业数据通信领域的应用受到很大限制。随着交换

技术和全双工数据通信技术的发展, 工业以太网已经大大提高了在数据通信中的实时性和确定性, 而且在许多工业领域得到成功应用。

### 2 以太网用于工业数据通信的技术基础

1) 以太网的交换技术和全双工通信技术 以太网的交换技术由原先的端对端的网桥连接发展到了现在的以太网交换机。以太网交换机的原理很简单, 它检测从以太端口来的数据包的目的地的 MAC(介质访问层)地址, 然后与系统内部的动态查找表进行比较, 若数据包的 MAC 层地址不在查找表中, 则将该地址加入查找表中, 并将数据包发送给相应的目的端口。在数据发送的过程中, 目前广泛应用存储转发技术, 先把输入端口的数据包存储起来, 然后进行 CRC 检查, 在对错误包处理后才取出数据包的目的地址, 通过查找表转换成输出端口送出包。正因如此, 存储/转发方式在数据处理时延时大, 这是它的不足, 但它可以对进入交换

收稿日期: 2005-05-31; 收修定稿日期: 2005-06-16

作者简介: 孙钦龙(1978-)男, 山东临沂人, 研究生, 主要研究方向为工业以太网应用, 工业过程控制等; 邵惠鹤(1936-)男, 上海人, 教授, 博士生导师。

机的数据包进行错误检测，尤其重要的是它可以支持不同速度的输入输出端口间的转换，保持高速端口与低速端口间的协同工作。

全双工(Full-Duplex)技术也是随着以太网技术的发展而被广泛地用于以太网交换机的。现在各大厂家都有基于 IEEE802.3X 全双工通信协议的机型。IEEE802.3X 标准规范中确定了全双工以太网(Full-Duplex Ethernet)的工作模式，它在站点之间提供可以独立发送与接收的点对点的链路(物理介质必须支持全双工通信)，可以同时接收和发送数据，因而不存在共享介质竞争和发送数据帧碰撞的问题，而且网络的吞吐量也增加了一倍。本系统所用的阿尔法交换机符合 IEEE802.3/802.3X 以太网标准，带有多个 10/100 Mbps 自适应端口，支持全双工通信和 IEEE802.3X 流量控制，内置 MAC 地址存储空间，每个端口对应一个 LED 用于设备状态和故障显示，这种交换机集成了目前以太网技术的最新成果。

有了交换技术和全双工技术的支持，以太网的不确定性和实时性差的确定得到很大的改观，在工业数据通信领域得到了众多厂商的认可。

2) 网络单片机的发展和相对应的软件开发环境 随着以太网通信技术的进步，各大厂商纷纷推出基于嵌入式以太网的处理器，本系统所用的 Rabbit2000 就是其中的一种。Z-Word 公司推出的 BL2100 核心模块使用了 Rabbit2000 处理器，它是专门应用于嵌入式领域的以太网通信智能模块，支持各种网络协议(如 TCP,HTTP,FTP,SMTP,PPP 等)，开发过程中使用的是基于 TCP/IP 协议的 Socket 编程系统。对应于硬件配置，Z-Word 公司提供了相应的软件开发环境，即 Dynamic C 语言，它去掉了普通 C 语言中不符合实时性要求的部分，加入了适用于实时控制的功能，提供了众多功能丰富的函数库，包括数学函数库、I/O 函数库、串口通信函数库、数据采集和数据输出函数库，还有基于各种网络协议的网络通信所需要的函数库。BL2100 在系统编程(ISP)程序开发调试方面非常方便。

### 3 系统的总体设计

系统设计为三层的网络结构，最上层为 PC 监控机，中间层为网络通信模块 BL2100，现场层为 MSP430 智能控制节点。

PC 机和 BL2100 之间的通信是基于工业以太网，BL2100 和 MSP430 之间的通信是用 RS-485 总线来实现的。

监控 PC 机采用组态软件开发出相应的监控界面，可以实现多种多样的数据处理功能，包括历史

数据存储、实时数据动态显示、报警信息输出等。同时操作人员根据不同的控制要求可以发出不同的控制命令。BL2100 网络模块带有工业以太网接口和 RS-485 接口，多个网络模块可以通过以太网交换机来连接 PC 监控机，在局域网内可以充分利用丰富的 IP 地址资源而不受外网的限制，适合于工厂内部环境。MSP430 智能节点主要作用是接收采集命令，进行现场数据采集，通过 RS-485 总线传给 BL2100。根据不同的硬件配置，可以在每条总线上挂接多达 128 个 MSP430 智能节点。BL2100 一方面通过 RS-485 和 MSP430 进行数据通信获得各个节点的采样数据，另一方面把数据处理打包以 Socket 套接字通信的方式发送给 PC 监控机。

系统结构示意图如图 1 所示。

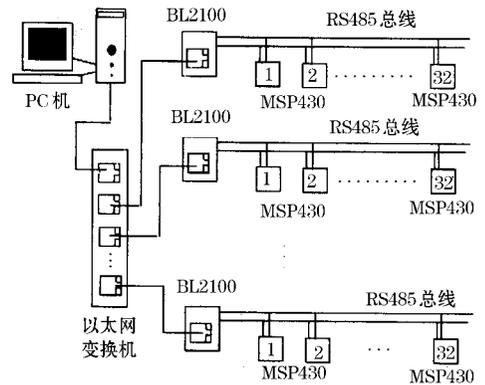


图 1 系统示意图

### 4 系统软件开发

1) 网络模块总体程序框图 如图 2 所示。

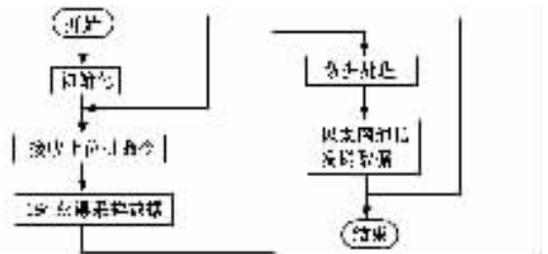


图 2 网络模块总体程序框图

网络模块 BL2100 运行过程中，程序首先进行必要的硬件初始化，然后接收 PC 监控机发送的命令，确定系统各个采样通道的配置，包括采样周期、滤波参数设置等，然后通过 RS-485 总线发出命令，MSP430 接到命令进行数据采集，采集完毕发送给 BL2100，再通过工业以太网发送给 PC 机。

2) 基于 TCP/IP 协议的 Socket 编程 Socket(套接字)是通过标准的 UNIX 文件描述符和其他程序通信的一个方法，它最早由加州大学伯克利分校研发，每一个套接字都用一个半相关描述：{协议,本

地地址、本地端口)来表示;一个完整的套接字则用一个相关描述:{协议、本地地址、本地端口、远程地址、远程端口},每一个套接字都有一个本地的由操作系统分配的惟一的套接字号。1983年,TCP/IP协议和 Socket 套接字融合,从而实现了在 TCP 协议基础上的 Socket 通信方式。

在本系统使用的 Dynamic C 语言开发环境中,提供了基于 TCP/IP 协议的 Socket 网络通信编程所需的全部库函数。

Socket 通信首先要创建套接字,其次给套接字赋予地址信息,再建立 Socket 连接,最后进行数据通信。通讯过程中还要有网络状况侦听功能和网络错误处理子程序。本系统的通信有实时数据和非实时数据两部分信息流,实时数据包括采样得到的数据流,非实时数据主要是各种各样的采样控制参数流。数据通信以实时数据流为主兼之以非实时数据流,程序设计按照 Server/Client 的形式,网络模块 BL2100 为服务器,PC 机为客户机。下面以运行在网络模块上的数据发送程序来说明 Socket 通信设计的主要流程,通信程序框图如图 3 所示。

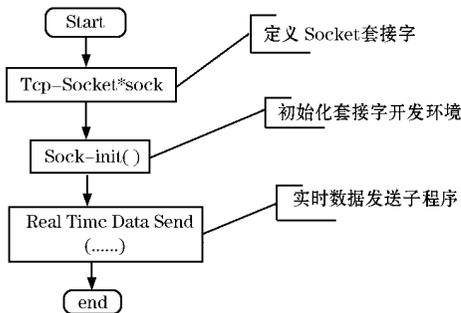


图 3 Socket 通信程序框图

①定义 Socket 套接字 它是基于 TCP 协议的,必须包含一个完整的 TCP 连接所需要的全部信息。但是它还不是一个具体的针对某一连接的,只是一个定义。②初始化 Socket 套接字开发环境 主要是在 Dynamic C 语言的编译环境中声明,获得开发环境的支持。该函数载入 Rabbit2000 关于 TCP, Socket 的相关的驱动程序,它必须在所有的 TCP, Socket 相关函数调用之前调用。③调用发送实时数据的子程序,在这里面要具体的创建套接字,建立、连接、发送数据。

子程序的部分源码如下:

```

void RealTimeDataSend( tcp_Socket * sock ,
long * buff , int * state , word my_port )
{switch( * state )
{case 0 :
    if( tcp_oper( ... ) != 0 ) //侦听网络建立连接
    print( " Connect success ! " );

```

```

else
    sock_tick( ... ) //套接字管理 完毕后转
    往 sock_err( ) 函数
timer_2 = MS_TIMER //定时器
( * state ) + + ;
break ;
case 1 :
    if( sock_established( sock ) ) //建立本连接
    的套接字
    { //建立套接字成功
        * state = 2 ;
        sock_mode( ... ) //数据类型
        timer_3 = MS_TIMER ;
        print( " Socket success establish !!! \n " );
    }
    else if( MS_TIMER - timer_2 > OUT_TIME )
    { //超时处理
        * state = 3 ;
        print( " Time out " );
    }
    break ;
case 2 : //发送数据
    if( send_start = 0 ) //是第一次发送数据
    //发送全部的实时和非实时参变量
    { sock_fastwrite( buff ) //往发送缓冲区
    写入数据
        send_start = 1 ;
    }
    else if( send_start = 1 )
    { sock_fastwrite( buff );
    //只发送实时变量
    }
    sock_tick( ... );
    * state = 2 ;
    break ;
case 3 :
    sock_abor( sock ) //close the socket
    * state = 0 ;
    break ;
}
sock_err( ... ) //套接字错误处理
}

```

以上是对实时发送子程序的大体介绍,\*sock 是具体的套接字,\*buff 是发送缓冲区,\*state 是运行状态 my\_port 是 TCP 端口号。具体的思路是先侦听网络的状况,网络状况允许则建立本次通讯连接的 Socket 套接字,设定 Socket 通讯的数据格式。如果网络状况不好,则转入相应的错误或超时处理函数。在程序中,存在一个上电第一次运行的问题,此时所有的实时和非实时数据都要进行通信来进行系统数

据同步,此后只发送实时数据。程序中设置了 \* state 多状态开关变量来标志各种不同的运行情况,该状态初始化为 0。

以上介绍的是网络模块向 PC 机发送数据的流程。但是这只是单方向的数据流动,如上所述,现在的工业以太网技术支持全双工的通信,即数据的双向流动可以完美地实现,基于此,现场的智能节点在不断向 PC 机发送采集数据的同时也可以随时接受来自 PC 机的控制信息及其对应的数据流。本文设计了相应的数据接受子程序。函数的定义如下:

```
unRealTimeDataReceive( tcp-socket * sock ,
long * buff , int * state , word my-port )
{...
    case 2 :
        sock _fastread( buff ) //从接收缓冲区读取数据
        ..... }
```

参数的定义和接收子程序相比,只有在 \* state 等于 2 的时候不同,此时网络模块接收数据,它根据缓冲区第一个数据获得所要接收的参数的索引号,将缓冲区第二个数据赋给具体的参数变量。还有一点要说明的是,工作人员进行监控操作,这个过程不是实时进行的,带有很强的随机性。因此控制信息流不是实时存在的,而是随机的,各个网络模块会不断地侦听网络来查看有没有对应本模块的数据包,如果有则进入接收子程序。

(上接第 201 页)

- [19] 傅丰礼. 用三维有限元法计算直线电机的起动推力[J]. 中小型电机, 1998, 25(4):1-3.
- [20] 谢经明, 程立, 艾武, 等. 高响应直线电机控制系统的研究[J]. 机械与电子, 2004, 25(5):29-31.
- [21] Nam K, Sung J H. A new approach to vector control for linear induction motor considering end effects[C]. Phoenix, USA: IEEE IAS Annual Meeting, 1999.
- [22] 徐小品, 等. 基于 SVPWM 的电机变频调速系统的研究与实现[J]. 机电工程, 2004, 21(1):34-38.
- [23] Caldara S, Nuccio S, Galluzzo G R, et al. A fuzzy diagnostic system: application to linear induction motor drives[C]. Ottawa, Canada: IEEE Instrumentation and Measurement Technology Conference, 1997.
- [24] 钟扬, 叶云岳, 赵光宙. 直线感应电机的新型 PID 控制研究综述[J]. 微特电机, 2002, 30(2):27-30.
- [25] 孙武贞. 感应式直线电动机瞬时电流跟踪控制变频技术[J]. 电气传动, 1991, 21(6):21-26.
- [26] 邓中亮. 高频响精密位移直线电机及其控制的研究[J]. 中国电机工程学报, 1999, 19(2):41-46.
- [27] 刘金凌, 王先逵, 吴丹, 等. 直线电机伺服系统的模糊推理自校正 PID 控制[J]. 清华大学学报, 1998, 38(2):44-46, 50.
- [28] 叶云岳, 陈凯元. 直线电机的 PID 控制与模糊控制[J]. 电工技术学报, 2001, 16(3):11-15.

## 5 结 语

本文结合数据采集系统讨论了工业以太网在工业数据通信中的应用,简要介绍了在 Dynamic C 环境下基于 TCP 协议的 Socket 网络编程,给出了相关子程序部分源码。本系统开发以后,用于一套生物发酵控制系统中,已经在上海数家生物制药研发中心得到了成功的应用。实践证明,基于工业以太网的通信运行很稳定,延迟很小,在一台 PC 监控机同时和多台发酵系统连接工作的情况下,运行同样稳定,实时性和确定性都得到了有效的保证。可以预见,工业以太网在工业数据通信中的应用必将日益广泛,基于 TCP/IP 协议的 Socket 套接字通信方式作为实现的方法简单实用稳定,已经获得了大多数工业监控开发软件的支持。目前集管理和控制于一体的工业生产过程计算机集成控制系统(CIPS)正在快速地发展,工业以太网技术使 CIPS 进入工厂企业的步伐大大加快,这极大地促进制造业的信息化进程。

参考文献:

- [1] 邵惠鹤. 工业过程高级控制[M]. 上海:上海交通大学出版社, 1998.
- [2] Tareerbaum A S. 潘爱民译. Computer networks( fourth edition) [M]. 北京:清华大学出版社, 2004.
- [3] Z-World Inc. Dynamic C premier for emiconductor microprocessors integrated C development system user's manual [Z]. California: Z-world Corporation, 1999.
- [4] Z-World Inc. Dynamic C TCP/IP user's manual [Z]. California: Z-world Corporation, 2001.
- [29] 刘泉, 张建民, 王先逵. 直线电机在机床工业中的最新应用及技术分析[J]. 机床与液压, 2004, 32(6):1-3.
- [30] 叶云岳, 等. 直线电机驱动的新型冲压机[J]. 电工技术杂志, 2000, 15(2):35-36.
- [31] 何志龙, 等. 冰箱用直线压缩机研究[J]. 西安交通大学学报, 2003, 37(11):20-24.
- [32] 宋凯, 等. 磁悬浮列车用直线电机推进系统发展综述[J]. 微电机, 1999, 32(1):32-35.
- [33] 郭秀欣, 等. 直线电机在煤矿中的应用前景[J]. 煤矿机械, 2002, 19(10):5-7.
- [34] 杨正新, 等. 直接驱动的发展和未来[J]. 中国机械工程, 2000, 11(10):1180-1182.
- [35] 叶云岳. 现代先进驱动技术及其应用[J]. 机电工程, 2004, 21(1):1-4.
- [36] 王爱乐, 等. 国外直线电机驱动新产品的发展[J]. 科技情报开发与经济, 2003, 13(8):76-77.
- [37] 张春良, 等. 直线电机驱动技术的研究与现状[J]. 农业机械学报, 2002, 33(5):119-123.
- [38] Mendrela E A. Comparison of the performance of a linear reluctance oscillating motor operating under AC supply with one under DC supply[J]. IEEE Trans on Energy Conversion, 1999, 14(3):328-332.
- [39] 崔广渊, 宋书中, 等. 共振式直线电机及其变频器的总体功率因数研究[J]. 电工技术学报, 2003, 18(1):15-20.