Computer Science and Application 计算机科学与应用, 2015, 5, 186-193
Published Online May 2015 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2015.55024

Hans汉斯

Design and Realization of Embedded Termination of PLC Equipments' Remote Monitoring Based on 3G Technology

Hongjun Chen[1], Duo Li[1], Hua Ye[1,2]

[1]School of Automation, Southeast University, Nanjing Jiangsu
[2]Key Laboratory of Measurement and Control of CSE of Ministry of Education, Southeast University, Nanjing Jiangsu
Email: zhineng@seu.edu.cn

Received: May 7th, 2015; accepted: May 23rd, 2015; published: May 28th, 2015

Abstract

Against application background of the CP1H PLC of Omron Company, the design of remote monitoring system about PLC devices base on 3G network on the embedded Linux platform is realized. The paper puts forward the 3G communication solution according to the shortcomings of the GPRS and the Ethernet's in practical application. The system uses S3C6410/ARM11 as controller and ZET MF210 wireless module, which is taking in the WCDMA system. The system implements 3G function through the configuration in the embedded Linux system related to drive, transplant the PPP suite, write configuration script and so on. This paper introduces the hardware design, driver transplant, and the realization of the function of network communication process. This solution has the advantages like fast, stable and reliable.

Keywords

Embedded Linux, 3G, PLC, Monitor

基于3G通信的PLC嵌入式监控终端设计与实现

陈洪骏[1]，李　多[1]，叶　桦[1,2]

[1]东南大学自动化学院，江苏　南京

[2]东南大学复杂工程系统测量与控制教育部重点实验室，江苏 南京
Email: zhineng@seu.edu.cn

收稿日期：2015年5月7日；录用日期：2015年5月23日；发布日期：2015年5月28日

摘 要

本文以欧姆龙CP1H型号的PLC为应用背景，设计了基于嵌入式linux下3G无线通信的PLC设备远程监控终端。论文针对GPRS与以太网的不足在实际应用的缺陷，提出了基于3G通信技术的数据传输方案，采用S3C6410/ARM11作为控制器和中兴MF210无线模块，采用WCDMA制式，通过在嵌入式linux系统中配置相关驱动，移植PPP套件，编写配置脚本来实现3G通信数据监控功能。介绍硬件设计，驱动移植，网络通信功能的实现过程。本方案具有快速稳定可靠等优点。

关键词

嵌入式linux，3G，PLC，监控

1. 引言

能否对售出设备进行远程通信和监控对于设备制造厂家意义重大。远程通信和监控有利于减少去现场修改 PLC 程序的人员费用，缩短设备故障诊断时间，提高设备维护效率；有助于企业了解设备运行状况，改进设备的制造质量。本文中使用的欧姆龙 CP1H 型号 PLC 可拓展 CP1J 网络模块实现网络通信[1] [2]，实现远程的程序下载上传功能，但是每个拓展模块的不菲价格将增加每台 PLC 设备的配置成本。选用 GPRS 无线通信方式方便，但传输速度与稳定性达不到实时监控的要求；有线通信模式满足速度要求，但是考虑现场环境复杂性，会增加布网的难度。综合两种方式的优点，选用 3G 无线传输方式[3]，有较高传输速度，降低组网复杂度，系统运行稳定可靠。结构图如图 1 所示，是整个监控系统的结构图，本文设计的监控终端就是图 1 中的 3G 终端部分。

2. 终端硬件结构

3G 监控终端硬件结构如图 2 所示。

硬件上采用“ARM + 3G”系统架构，选用 Tiny6410/arm11 核心板作为主处理器，该处理器基于 ARM1176JZF-S 核设计，运行频率为 533 MHz，最高可以达到 667 MHz。核心板集成了 128M DDR RAM，256M SLC Nand Flash 存储器，采用 5 V 供电，在板实现 CPU 必需的各种核心电压转换，方便二次开发。3G 模块选用的是中兴的 MF210，支持 UMTS850 (900)/1900/2100、GSM/GPRS/EDGE 850/900/1800/1900 多频段 HSUPA 的 PCI Express Mini Card 无线网卡，可以提供移动环境下的 WCDMA、GSM/GPRS、EDGE (EGPRS)和 HSUPA 高速数据接入服务。并在 HSUPA 下最大的上下行速率为 7.2 Mbit/s。

3. 3G 模块驱动设计

本系统中使用的 MF210 3G 模块与 Tiny6410 以 USB 接口相连接，3G 模块使用的虽然是一个 USB 接口，但实质上是一个虚拟串口，在 Linux 设备中是一个 USB 串口设备，系统中需要加载 USB serial 的驱动。串口设备属于 TTY 设备，对应的驱动程序包含设备驱动的成员函数以及设备对应的结构体成员。本系统中使用的是 linux3.3 版本，自带串口 USB 设备驱动，所以只需要添加对 3G 模块的设备支持即可[4] [5]。

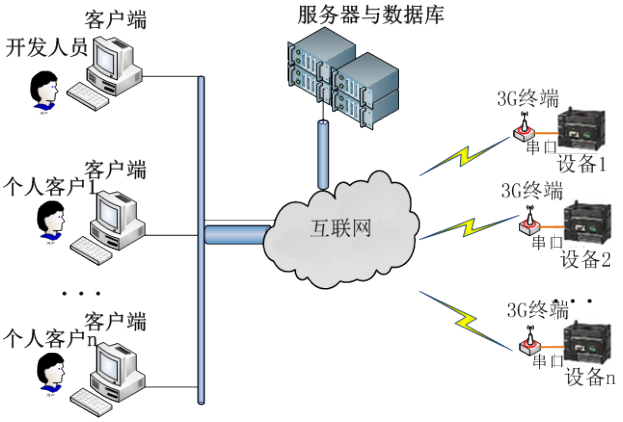

Figure 1. Monitoring system structure
图 1. 监控系统结构图

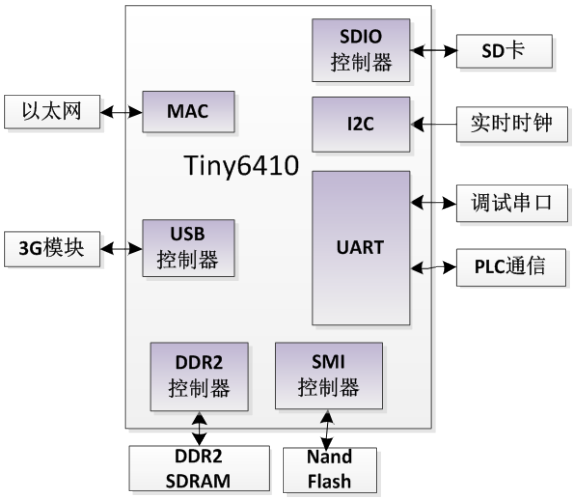

Figure 2. System hardware structure
图 2. 系统硬件结构图

3.1. 内核配置

首先需要在 Linux 系统内核添加 usb 转 serial modem 的支持。通过修改 pl2303.c 和 pl2303.h 文件，添加对 MF210 模块的支持。由数据手册可知，MF210 的 VID 为 0x19d2，PID 为 0x0117，内核文件修改如下所示：

```
/*pl2303.h*/
#define  ZET_VENDOR_ID     0x19d2
#define  ZET_PRODUCT_ID       0x0117
/*pl2303.c*/
staticstructusb_device_idid_table[]=
{
……
{USB_DEVICE(ZET_VENDOR_ID, ZET_PRODUCT_ID)},
}
```

接下来在 menuconfig 界面下，配置内核驱动时，选中 USB Support，USB Serial Converter Support 和 USB Generic Serial Driver 选项。配置完成后，使用 make modules 命令，生成 pl2303.ko 和 usbserial.ko 两个驱动模块，加载到系统中即可。

3.2. 移植拨号工具

在嵌入式系统中加载 3G 模块驱动以后，接下来使用 PPP 套件进行拨号[6]。首先在内核中添加对 ppp 的支持，输入 make modules 命令，生成模块文件使用 insmod 命令按一定的顺序加载这些 ppp 驱动。

pppd 驱动加载成功后，还需要把 pppd 拨号工具移植到目标板中，交叉编译 pppd 源码，生成 chat、pppd 两个可执行程序，将其拷贝到/usr/sbin 目录下。

3.3. 编写 pppd 配置文件 wcdma 和拨号脚本

pppd 移植成功后，只要编写好 pppd 脚本，即可运行 pppd 程序进行拨号。pppd 脚本如下所示

```
/dev/ttyUSB0
460800
usepeerdns
noipdefault
ipcp-accept-local
ipcp-accept-remote
connect  '/usr/sbin/chat –s –v –f chat-wcdma-connect'
```

其中，/dev/ttyUSB0 为指定连接的设备，460800 为连接使用的控制字符传输速率，usepeerdns 表示使用服务器端协商的 DNS，noipdefault 表示不使用默认 IP，ipcp-accept-local 表示接受服务器分配的本机 IP 地址，ipcp-accept-remote 表示接受服务器指定的服务器 IP 地址。

在 wcdma 配置文件中，会调用 chat-wcdma-connect 拨号脚本[7]。拨号脚本如下：

```
TIMEOUT 10
ABORT 'NO CARRIER'
ABORT 'ERROR'
ABORT 'NO DIALTONE'
ABORT 'BUSY'
ABORT 'NO ANSWER'
'' \rAT
OK \rATZ
OK \rAT+CGDCONT=1,"IP","3gnet',,0,0
OK-AT-OK ATDT*99#
CONNECT \d\c
```

五个 ABORT 语句表示当拨号中出现这些问题时，退出执行。3gnet 是中国联通 3G 网络接入点。ATDT*99#是中国联通的 Modem 拨号字符。

最后使用命令 pppd call wcdma&就可以拨号，拨号成功后可以在程序中使用 socket 进行网络通信。

4. 网络通信设计

当 3G 模块驱动编写完成并且拨号成功后，在应用层可以基于 socket 编写应用程序。本嵌入式终端负责将 PLC 的串口数据进行转发，转换成网络数据包后从 3G 网络发送到 PC 服务器，并且从 PC 端接收

相关数据转换成串口数据发送至 PLC。在整个 PLC 数据通信中，传送的是 PLC 指令以及 PLC 返回的实时数据，为了保证数据的可靠传送，采用面向连接的 TCP 传送协议。

4.1. TCP 的工作原理

TCP 传送协议是面向连接的通信协议，是一种可靠传输协议，工作原理是两个进程在进行 TCP 通信协议进行通信之前，必须要先建立 TCP 协议连接，该过程通常被称为“三次握手”。只有当连接建立成功后，才可以进行通信，TCP 协议有重传机制，TCP 协议中有多种方式保证数据传输的可靠性[8]。

4.2. Socket 通信原理

在嵌入式终端的应用程序中，网络通信都是基于套接字进行通信的，socket 套接字将复杂的 TCP/IP 协议族隐藏在接口后面，应用进程只要操作 socket 套接字即可完成网络通信的所有步骤。在 linux C 语言中，套接字编程分为客户端跟服务器端两种模式。图 3 表示 socket 通信流程。

4.3. 基于生产者-消费者模式的数据处理

在网络通信中，并发操作使得通信的效率得到提高，这就需要用到多线程技术。在本文涉及的终端系统中，需要将网络数据跟串口数据的相互转发，生产者消费者模型是解决这个问题比较好的设计模式。

生产者和消费者在同一时间段内对同一个存储空间进行操作，如图 4 所示，生产者向空间里存放数据，而消费者取用数据。

如果不加以协调可能会出现以下问题：存储空间已满，而生产者占用使用权，而消费者则一直等待着生产者让出使用权，生产者则又等待着消费者消耗产品，这样就会造成生产者和消费者互相等待，从而发生死锁。

在监控终端程序中，接收网络数据线程从网络接收数据，存放在循环队列中，相当于生产者，PLC 指令写线程从循环队列中取出数据，经过处理得到 PLC 指令经串口发送至 PLC，相当于消费者。只有当缓存区里面有数据时，PLC 指令写线程才能取数据，当缓存区满时，接收网络数据线程不能继续存放数据，这时如果有网络数据到来，要舍弃。如图 5 所示。

在实际运行中，还有从 PLC 读取数据往队列中存放，往网络写数据线程从队列中读取。由于读写操作不是原子操作，所以读线程和写线程之间可能会同时改写头指针跟尾指针，所以读写线程需要同步，当写线程在写数据的时候，不允许读数据，在读线程读数据时，也不允许写操作。生产者与消费者之间需要同步，同时又能通知对方的操作完成状态，所以我们结合使用互斥锁与条件变量。

当写线程准备开始写数据时，那么就加锁，其他读线程想读数据由于没有获得锁，所以只能阻塞，当写线程数据写完后，需要通知读线程可以来读取数据，那么就发送一个条件信号，并且释放锁，读线程收到可以读的信号后，并且获得锁，就进行加锁，让自己进行读数据，等到读完数据，再发送信号通知写线程可以进行写了。具体方法如图 6 所示。

5. 3G 通信功能测试

为了测试远程监控终端的网络通信功能，在 PC 上用 JAVA 编写简易客户端[9]，服务器模块，用来测试网络通信功能。整个网络数据通信流程是，客户端跟嵌入式终端充当网络通信中的客户端，跟服务器建立网络连接，PC 客户端跟服务器发送 PLC 指令，服务器转发指令给终端，终端收到网络指令后，转换成 PLC 串口指令发送至 PLC，PLC 返回指令，最终传达给 PC 客户端。流程如图 7 所示。

在通信之前，需要先开启服务器，再开启客户端，然后客户端发送指令，得到远端 PLC 的响应，现为了获取实时监控数据，向 PLC 定时发送指令，获取 PLC 相关数据。如图 8 所示。

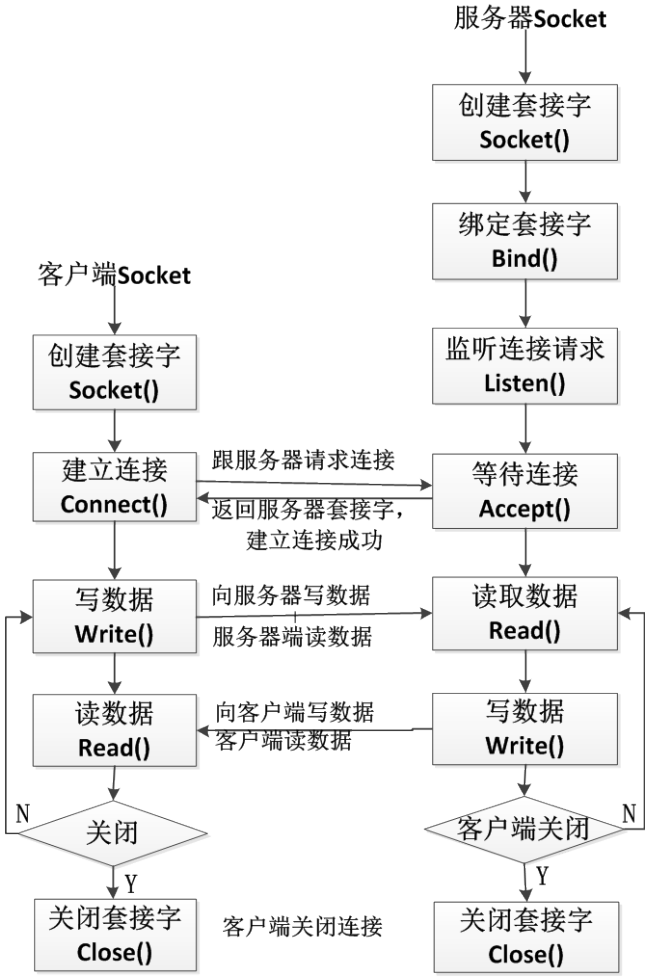

Figure 3. Socket programming flow chart
图 3. 套接字编程流程图

Figure 4. Producers-consumer model
图 4. 生产者－消费者模型

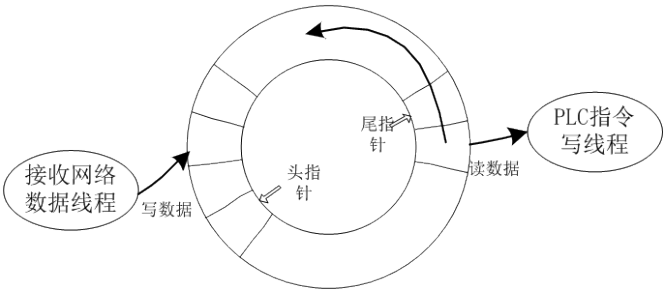

Figure 5. Thread synchronization Schematic diagram
图 5. 线程同步问题示意图

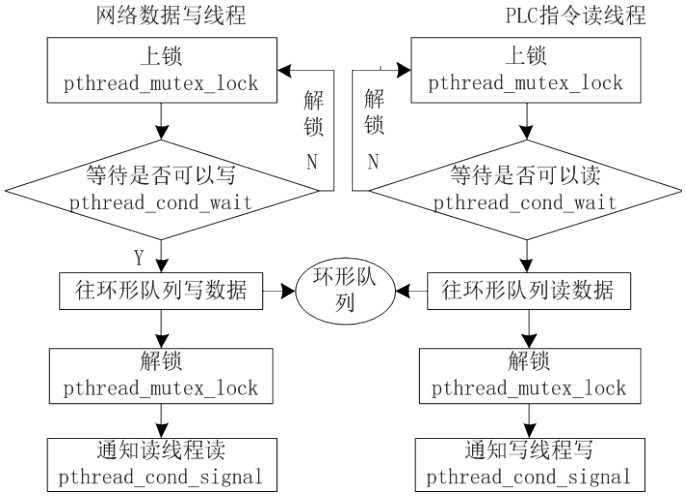

Figure 6. Multithreaded synchronization flow chart
图 6. 多线程同步流程图

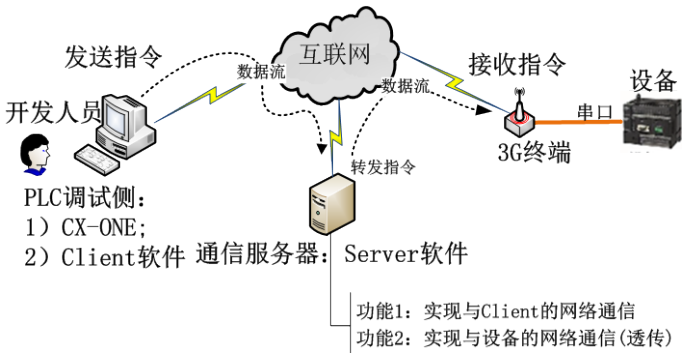

Figure 7. Network data translate schematic diagram
图 7. 网络数据收发示意图

Figure 8. Network communication test
图 8. 网络通信测试

6. 结束语

本终端系统是基于 Tiny6410 核心板与 linux3.3 版本上，选用 ZET 的 MF210 3G 模块，由于 3G 模块与系统板之间以 USB 接口连接，简化了硬件与驱动的设计；在 3G 模块的使用上，只要进行相关的脚本编写与编译拨号软件，即可使用 3G 功能；在网络通信程序设计上，采用基于套接字 socket 的网络编程技术，编程步骤清晰明确，为了实现并发通信，采用基于生产者－消费者设计模式的多线程编程技术，使得数据传输的实时性高，保证了系统的可靠稳定运行。

参考文献 (References)

[1] 欧姆龙公司 (2009) CP1H 操作手册(中文)W450-CN5-02. http://www.fa.omron.com.cn/index.php?cat_code=%2Fproducts%2Fdownload&type=0&lan=&jixing=&fenlei=&keywords=CP1H&x=9&y=11&p=2

[2] 欧姆龙公司 (2009) CP1H/CP1L CPU 单元编程手册(中文)W451-CN5-01. http://www.fa.omron.com.cn/index.php?cat_code=%2Fproducts%2Fdownload&type=0&lan=&jixing=&fenlei=&keywords=CP1H&x=9&y=11&p=1

[3] 曾桂根, 吴霜 (2010) 基于嵌入式 Linux 的 3G 接入方案的设计与实现. *计算机技术与发展*, **9**, 193-197.

[4] 程琼, 孙敏 (2012) 基于 3G 和嵌入式技术的数据传输系统设计. *工业控制计算机*, **12**, 93-96.

[5] 胡柯, 颉潭成, 刘陆群 (2003) 基于 TCP/IP 和 Socket 实现网络通信. *组合机床与自动化加工技术*, **9**, 50-52.

[6] 何苏勤, 张俊 (2011) 基于嵌入式 Linux 的 3G 无线视频终端的设计与实现. *电子设计工程*, **7**, 57-61.

[7] 郭敏, 曹广 (2007) 嵌入式 Linux 下使用 MC39 实现 GPRS 拨号上网. *广东通信技术*, **12**, 63-66.

[8] 罗亚非 (2009) 基于 TCP 的 socket 多线程通信. *电脑知识与技术*, **3**, 563-565.

[9] 李芝兴 (2006) Java 程序设计之网络编程. 清华大学出版社, 北京.