Profibus 总线的无线网关设计

Design of the Wireless Gateway Based on Profibus

张建奇[1]　李墨翰[1]　张建锋[1]　王安民[2]

(西安航天自动化股份有限公司[1],陕西 西安　710065;中国市政工程西北设计研究院有限公司[2],陕西 西安　730000)

摘　要：为使无线技术能够方便地应用到工业环境中,设计了一种基于 Profibus 工业现场总线的无线网关。网关将 ZigBee 无线技术融入开放的 Profibus 现场总线当中,把通过无线采集模块采集到的数据进行汇总和格式转换后送至 Profibus 总线中,同时把 Profibus 总线发来的数据通过无线发送到指定的无线采集模块。实际测试结果表明,无线模块的发射功率、接收灵敏度、通信距离、误包率和速度满足工业应用的实时性和安全性要求,并且可以方便地实现 PLC 对无线路由 I/O 的配置和编程,从而能够方便地替代传统的传输方式。

关键词：Profibus　ZigBee　单片机　工业现场总线　无线网关　CC2530

中图分类号：TP273+.5　　**文献标志码**：A

Abstract: In order to make wireless technology be easily applied in industrial environment, the wireless gateway based on Profibus industrial fieldbus has been designed. In this gateway, ZigBee wireless technology is integrated into the open Profibus fieldbus, the data collected through wireless acquisition module are summarized and sent to Profibus after format being converted. The data sent from Profibus are transmitted to wireless acquisition module via wireless technology. The result of practical test indicates that the transmitting power, receiving sensitivity, communication distance, packet error rate, and speed of the wireless module all meet the real time security requirement in industrial applications, and the gateway can implement wireless routing I/O configuration and programming from PLC, thus to replace traditional transmission pattern.

Keywords: Profibus　ZigBee　Single chip machine　Industrial fieldbus　Wireless gateway　CC2530

0　引言

随着物联网技术的兴起,无线技术开始越来越受到人们的重视。ZigBee 是一种新兴的近距离、低复杂度、低功耗、低数据速率、低成本的无线网络技术,主要用于近距离无线连接。它依据 IEEE 802.15.4 标准,能够在数千个微小的传感器之间相互协调实现通信。这些传感器只需要很少的能量,以接力的方式通过无线电波将数据从一个网络节点传到另一个节点,具有非常高的通信效率,应用前景广泛。Profibus 是现在应用最广泛的开放工业现场总线之一。将 ZigBee 无线通信技术接入 Profibus 现场总线,可以方便地将无线技术融入到工业控制当中,如电力系统自动化等行业[1],从而实现无线生产过程控制以及监控等功能[2-3]。

1　网关的总体设计

Profibus 总线的无线网网关能够将 Profibus 总线及带路由功能的无线采集模块(即路由 I/O 模块)透明连接到一起,通过 PLC 可以实现对每一个路由 I/O 的配置以及数据的采集、指令的下发和报警的处理。整个无线采集系统如图 1 所示。

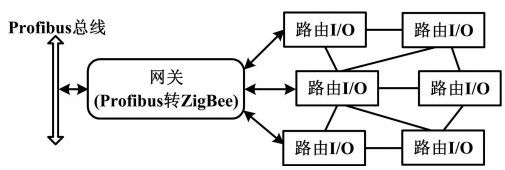

图 1　系统结构图

Fig. 1　Structure of the system

Profibus 总线无线网网关可以划分为 ZigBee 模块、协议转换模块、Profibus 总线协议模块和供电模块 4 个部分。ZigBee 模块核心采用 TI 公司的 CC2530 芯片,主要完成无线网络的组网管理以及数据采集的工作。协议转换模块使用 ATMEL 公司的 8 位单片机 Atmega128A。Profibus 总线协议及接口模块通过使用 PROFICHIP 公司的 VPC3+C 和 ADI 公司的 ADM2486 来实现。电源模块采用 NI 的 LM25575 芯片,其将24 V 的输入电压转换成 5 V 电压供系统使用。

2　网关硬件设计

系统协议转换单元 Atmega128A 起到承上启下的作用,它既可以对 VPC3+C 进行配置管理,与 Profibus

修改稿收到日期:2012-05-27。

第一作者张建奇(1975-),男,1999 年毕业于南京理工大学动力工程系,获硕士学位,高级工程师;主要从事物联网与自动控制的技术研究。

总线进行数据交换,又可以通过串口和网络协调器 CC2530 通信,采集终端数据,并将 PLC 发送的数据传送给 CC2530,最终传送到指定的路由 I/O。其中,CC2530 使用了 TI 的 Z-STACK 协议栈[4]。

系统协议转换单元 Atmega128A 在传输数据的同时对数据进行校检,从而保证数据的可靠性,实现 Profibus 总线到无线网络数据的无缝交换[5]。

2.1　无线网络协调器部分

系统无线网络协调器采用 TI 的 CC2530 实现。CC2530 是用于 2.4 GHz IEEE 802.15.4 的片上系统解决方案,它结合了领先的 RF 收发器的优良性能,是业界标准的增强型 8051 CPU。系统内具有 8 kB RAM 和最大 256 kB 闪存,以及许多其他强大的功能,最高通信速度可达 250 kbit/s。CC2530 具有不同的运行模式,使得它尤其适用于超低功耗要求的系统。

网关中的 CC2530 作为无线网络的网络协调器,是整个无线网络的中心,它负责自组网管理以及 I/O 数据的采集、传输、路由、汇聚、下发等多种工作。给 CC2530 加入射频前端 CC2591,可以大幅提高无线网络覆盖范围。

无线网络协调器电路如图 2 所示。

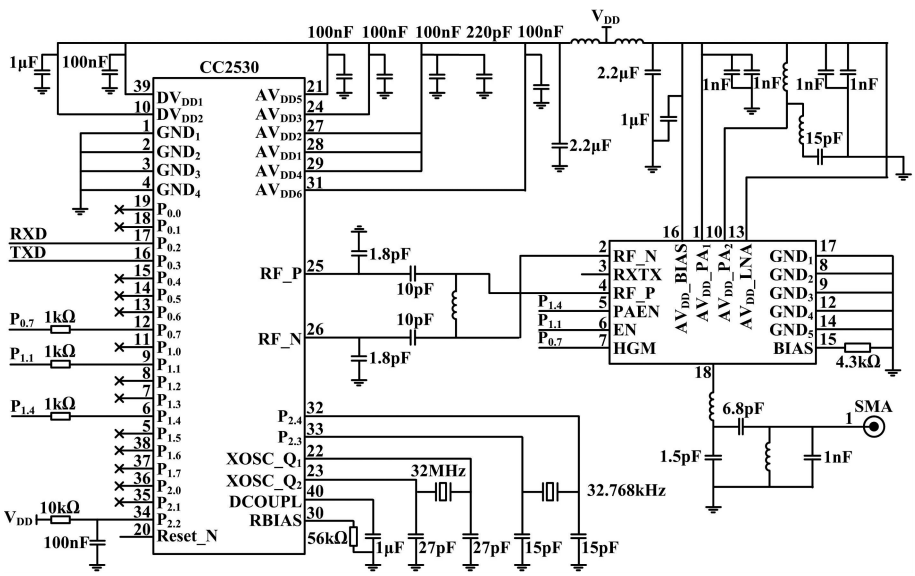

图 2　无线网络协调器电路

Fig. 2　Circuit of wireless network coordinator

2.2　Profibus 部分

系统采用 VPC3+C 实现 Profibus-DP 的从站功能,与 Profibus 总线的接口芯片使用 Profibus 兼容芯片 ADM2486。Profibus 接口电路原理图如图 3 所示。

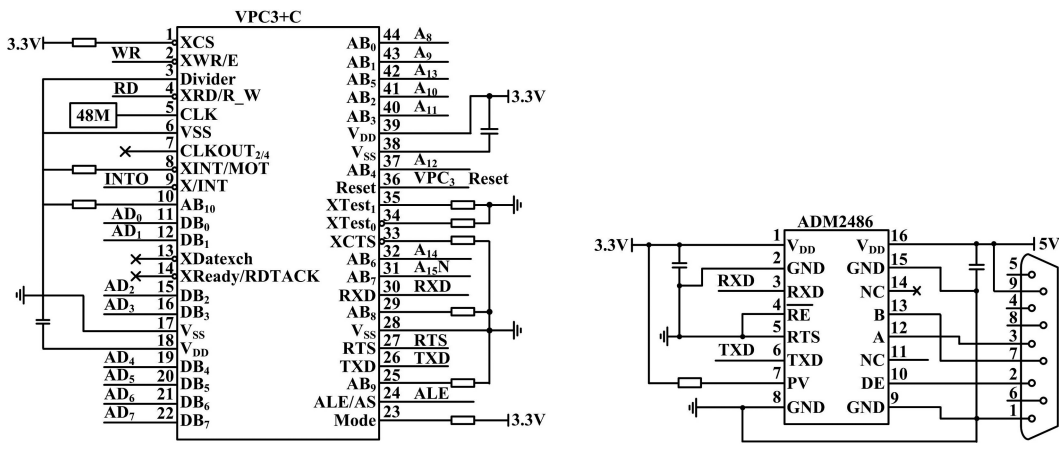

图 3　Profibus 接口电路

Fig. 3　Interface circuit of Profibus

VPC3+C 集成了全部的 Profibus 协议,可以方便地实现各种 Profibus 总线功能[6],最高速度可达 12 Mbit/s。VPC3+C 支持 4 种通信模式,这里 Atmega128A 采用同步 Intel 模式与 VPC3+C 通信。ADM2486 为半双工隔离式的 RS-485 收发器,具有 25 kV/μs 的高共模瞬变抗扰度及热关断保护功能[7]。

3　系统软件设计

系统软件分为网关协议转换和 ZigBee 无线网络两个部分。

3.1　网关协议转换部分

在本方案的设计中,网关软件的协议转换子程序为主程序模块/中断处理模块的形式。Atmega128A 单片机使用同步 Intel 模式与 VPC3+C 芯片通信。主程序模块主要负责系统初始化和寄存器状态查询,并根据寄存器状态进行相应操作[8]。

① 初始化

在 VPC3+C 芯片正常工作之前,首先需要对其进行初始化,对寄存器进行配置。这包括设置协议芯片的中断允许,写入从站识别号和地址,设置 VPC3+C 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、初始化长度等;并根据以上初始值得出各个缓冲区的指针和辅助缓冲区的指针;根据传输的数据长度,确定输出缓冲区以及输入缓冲区和指针。

VPC3+C 初始化流程图如图 4 所示。

图 4　VPC3+C 初始化流程图

Fig. 4　Flowchart of VPC3+C initialization

② 外部存储器映射

VPC3+C 芯片的内部 RAM 作为 Atmega128A 单片机的外部扩展存储器,因此,Atmega128A 可以直接以访存的形式访问 VPC3+C 芯片上的存储器。按照硬件设计,Atmega128A 单片机的 PA_0 ~ PA_7 引脚作为外部 8 位数据总线,PC_0 ~ PC_7 引脚作为外部 8 位地址总线,且地址最高位通过取反后接到 VPC3+C 芯片上,形成片选信号。当地址最高位为 1 时,表示访问外部存储器,即 VPC3+C 芯片内部的存储器;反之访问 Atmega128A 内部存储器。

③ 产品识别 ID 号及从站地址的设置

产品识别 ID 号在从站设备描述文件(general station device, GSD)中加以设置。程序在初始化 VPC3+C芯片时,同样要设置产品识别 ID 号,且必须与 GSD 文件里描述的一致。从站地址在 PLC 配置程序里设定。考虑到一个 Profibus 总线上可以同时挂接多个网关,因此,网关的从站地址必须方便用户修改。

```
DPS2_SET_IDENT_NUMBER_HIGH(ident_numb_high);
                                    //产品 ID 号高位
DPS2_SET_IDENT_NUMBER_LOW(ident_numb_low);
                                    //产品 ID 号低位
VPC3_SETSTATION_ADDRESS(get_stationID());
                                    //读取并设置从站地址
```

④ 设置 VPC3+C 芯片输入输出缓冲区大小

VPC3+C 芯片内部设有专门的用户 I/O 数据缓冲区,在使用前需要对其进行配置。在配置 VPC3+C 芯片前,需要先对 GSD 文件输入输出大小的定义作修改,如:Module="100 Byte In,40 Byte Out" 0x6f,0x63,0x5f,0x5f,0x5f,0x51。

该设置表示从站输入缓冲区为 100 B、输出缓冲区为 40 B。接下来配置 VPC3+C 芯片。配置前,首先需取得其配置缓冲区指针,并依次把配置数据写入配置缓冲区(需与 GSD 文件中的一致)。

```
*(real_config_data_ptr+i)= config_data[i];
```

然后根据缓冲区大小便可计算出输入输出缓冲区指针。对于该指针的读写操作,其会被 VPC3+C 芯片转换成 Profibus 协议上传到 PLC 中,实现数据的传输。

⑤ ZigBee 协议数据与 Profibus 协议数据映射转换

当 Atmega128A 接收到无线网络协调器发送的数据时,需要根据数据中的帧类型、站号、站类型字段计算出 VPC3+C 中输入缓冲区指针,并将数据按格式写入输入缓冲区中对应的位置。

同样当接收到 PLC 从 Profibus 总线发送的数据时,需要根据开关量所在地址计算出实际对应的站号与站类型,并且封装成规定的帧结构,通过网络协调器发送给对应的路由 I/O 设备[9]。

3.2　ZigBee 无线网络

ZigBee 无线网络协议通过 TI 的 Z-STACK 协议栈

来实现。Z-STACK 采用操作系统的思想来构建,采用事件轮询的方式来对事件进行处理。当各层完成初始化后,系统进入低功耗模式,当事件发生时,唤醒系统,开始进入中断处理事件,结束后继续进入低功耗模式。如果同时有几个事件发生,则判断优先级,逐次处理事件。这种软件构架可以极大地降低系统功耗[10]。此外,只需要编写应用层程序就可以实现 ZigBee 无线网络的应用开发,不需要将过多的精力投入到网络协议的具体细节当中。

协调器与路由 I/O 通过以下数据结构组织通信数据。

```
union RfRx_t{
uint8 RxBuf[RF_MAX_PAYLOAD_SIZE];
                    //802.15.4 标准最大有效数据长度
struct RFRXBUF{
uint8 frameType;
  //帧类型:0 表示命令帧;1 表示数据帧;2 表示应答帧
uint8 stationNum;
                          //站号,路由 I/O 拨码开关值
uint8 stationType;
                          //站类型:0 表示 DO 模块;
                        1 表示 DI 模块;2 表示 AI 模块
uint8 stationStatus;
                                          //站状态
uint8 dataType;
                          //数据类型,如实现 I/O 扩展,
                      该字节可指定数据为某一种 I/O 数据
uint8 dataLength;
                  //有效数据总长度,应答帧数据长度为 0
uint8 data[RF_MAX_PAYLOAD_SIZE-6];
                          //有效数据缓冲区,低位对齐,
                           最后一字节存储 SUM 校验码
}RXDATA;
}RfRx;
```

系统上电后,根据程序配置数据,在指定的信道中建立网络号为 PANID 的网络。部分源代码如下。

```
-DDEFAULT_CHANLIST=0X04000000     //channel 26
-DZDAPP_CONFIG_PAN_ID=0X0022 //PANID:0x0022
```

此时,只要网络中有路由 I/O 设备上电,由于有相同的信道号与网络标志号,路由 I/O 设备会自动加入到该网络。若加入网络成功,则会触发协议栈中的 ZDO_STATE_CHANGE 消息,应用程序在应用层接收到该消息并确认后,便可以正式开始路由 I/O 的工作流程。

当路由 I/O 设备加入网络后,需要先与协调器实施绑定。绑定过程在协议栈应用层实现,路由 I/O 设备读取自身的拨码值与短地址,并按照上述协议数据结构,封装成命令帧发送给协调器。部分源代码如下。

```
ScrSaddr=NLME_GetShortAddr();          //取得短地址
Station_id=get_stationID();              //取得站号
BuildMsg(ScrSaddr,Station_id);          //封装命令帧
SendData(0x0000,RfTx.TxBuf,2+PACKET_WITHOUT_
DATA+1);                                  //向协调器报告
DeviceStatus=WAIT_CMD_CONFIRM;
          //进入状态机的 WAIT_CMD_CONFIRM 状态
osal_start_timerEx(App_TaskID,WAIT_CONFIRM_MS_
EVT,WAIT_CONFIRM_TIMEOUT);
                        //开启命令帧应答超时定时器
```

协调器接收到命令帧,经确认无误后,在本地 RAM 中记录站号与短地址的对应关系,并回复命令应答帧给相应的路由 I/O 设备。至此,路由 I/O 设备的绑定过程结束。如当协调器有控制数据需要下发时,只需要先查表,根据站号查出对应的短地址,便可发送至目的路由 I/O 设备。

4　结束语

对西门子 S7-300 PLC 进行编程。实际运行测试结果表明,无线模块的发射功率、接收灵敏度、通信距离、误包率和速度均满足工业应用的实时性和安全性要求。网关可以通过工业现场总线 Profibus 加入到工业应用当中,具有功耗低、布置方便、编程使用简单可靠等优点,可以替代原来有线传输的方式。随着工业物联网技术的兴起和发展,此无线模块具有良好的应用前景。

参考文献

[1] 张高群. 电力系统应用 ZigBee 技术初步研究[J]. 电子测量技术,2008(11):20-22.

[2] 梁湖辉,张峰,常冲,等. 基于 ZigBee 的变电站监测报警系统[J]. 电力系统保护与控制,2010(12):33-34.

[3] 何杏宇,张浩,彭道刚. ZigBee 技术在工业环境监测系统中的应用研究[J]. 机电一体化,2008(7):111-112.

[4] 杜焕军,张维勇,刘国田. ZigBee 网络的路由协议研究[J]. 合肥工业大学学报:自然科学版,2008(10):79-80.

[5] 杨顺,章毅,陶康. 基于 ZigBee 和以太网的无线网关设计[J]. 计算机系统应用,2010(1):43-45.

[6] 王保永,汪鹏,卢宏军. 基于 PROFIBUS 的智能接口芯片 SPC3 及其应用[J]. 国外电子元器件,2005(3):23-25.

[7] 张婕,王征,郭天乐. SPC3 在现场总线智能从站设计中的应用[J]. 现代电子技术,2008(3):5-7.

[8] 李孝辉,张慧慧,孙树文. 基于 C8051 和 SPC3 的 PROFIBUS 智能从站设计[J]. 微计算机信息,2007(26):120-123.

[9] 王学伟. PROFIBUS-DP 现场总线智能节点的设计[D]. 哈尔滨:哈尔滨理工大学,2008.

[10] 胡鸿豪,林程,宋丽平. 基于 S3C2410 的 ZIGBEE 无线传感器网络网关的设计[J]. 大众科技,2008(12):43-45.