基于 ModBus 协议的负载模拟系统设计

单 星 林晓焕 郭丹蕊 汪 通
(西安工程大学电子信息学院 西安 710048)

摘 要：为了对实际的外部设备进行有效的控制，设计了一种基于 ModBus 协议的负载物理模拟平台控制系统。上位机采用 C++ Builder XE2 进行主站的通信程序设计，下位机采用西门子 S7-200 SMART，使用 ModBus RTU 协议库设计通信程序，将计算机与 PLC 连接起来，组成高性价比的负载物理模拟平台自动控制系统。通过上位机的数据的发送和接收实验，验证了设计的负载物理模拟平台控制系统的有效性和可行性。

关键词：ModBus 协议；C++ Builder XE2；负载物理模拟平台
中图分类号：TP29 **文献标识码**：A **国家标准学科分类代码**：520.4030

Design of load simulation system based on ModBus protocol

Shan Xing Lin Xiaohuan Guo Danrui Wang Tong
(School of Electronic Information, Xi'an Polytechnic University, Xi'an 710048, China)

Abstract: In order to the effective control of external devices, the design of load physical simulation platform of control system based on ModBus protocol comes out. The upper computer uses C++ Builder XE2 master communication program design, the Hypogynous Machine uses Siemens S7-200 SMART, using the ModBus RTU protocol library design program, the computer connected to the PLC together to form a cost-effective load physical simulation platform automatic control system. Through the PC send and receive experimental data verify the effectiveness and feasibility of the design of the physical simulation platform load control system.

Keywords: ModBus protocol; C++ Builder XE2; physical simulation platform load

1 引 言

在实际工业控制系统中，有些设备不便于现场调试，需要进行有效的远程控制，远程控制是现代工业比较青睐的技术，国内外对此都做了深入的研究[1]，比如法国的“A-LARM”研究组对生产过程的智能报警和监控系统的研究，哈尔滨工业大学的“微计算机化机组状态监视与故障诊断专家系统 MMMDES”等，这一系列的研究都表明远程监控正在被现代工业所认可并大规模的使用。与传统的远程监控不同的是，在负载物理模拟平台自动控制系统中，各个设备都放在不同的负载箱内，相互独立，抗干扰能力比较强；使用多串口，便于增加新设备，可扩展性有很大的提高。

综合以上分析，本文设计了一种基于 ModBus RTU 协议[2]的模拟物理平台的自动控制系统，该系统上位机用 C++ Builder XE2 开发环境，与 PLC 的通信通过 RS485 接口的 ModBus 协议。通过上位机数据的发送和接收，验证了设计的负载物理模拟平台控制系统的有效性和可行性。

2 研究主要内容及原理

负载自动控制为开环方式，在工控机屏幕界面设置负载加载的模拟开关，手动进行负载加载，设计负载物理模拟平台系统，主要任务是实现负载开关柜的远程控制。当上位机的负载开关动作后通过 ModBus 协议能把对应下位机设备对应变化进行实时采集，以此来验证系统的可靠性。要使实时的信息成为可能，就要进行上位机和下位机的通信，本文着重对上位机和下位机之间通信的实现及可靠性进行分析验证。整个通信过程采用主从应答式，上位机为主站，所有 PLC 均为从站，应答时间不超过 1 s。主站采用先读后写方式，上位机读取 PLC 状态后会通过串口监控界面显示出来，通过 PLC 指示灯显示和上位机读取到的数据对比，验证通信是否成功。

整个通信流程[3]由上位机出发，上位机通过串口发送

收稿日期：2015-04

命令，PLC 接收到命令后，按照标准的 ModBus RTU 协议，对指令做出相应的处理，具体流程如图 1 所示。

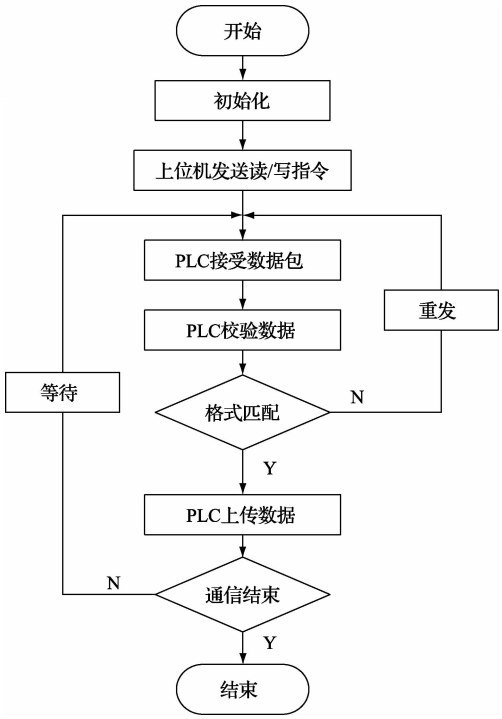

图 1　通信流程

ModBus 是一个工业网络通信系统，通过终端设备和计算机通过一定的线路或者网络连接而成，可用于各种过程监视和数据采集。ModBus RTU 协议[4]传输采用主从应答方式。具体的主从设备查询的响应周期流程如图 2 所示[5]。

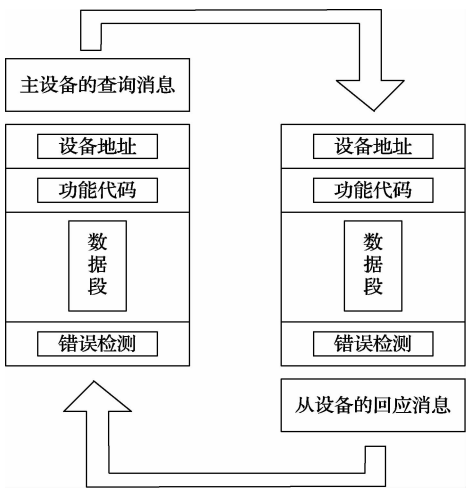

图 2　主从设备查询响应周期流程

3　上位机的通信编程

采用 C++ Builder XE2 编写上位机软件，C++ Builder 含有优秀的可视化控件，可以对控件直接编程，代码使用 C++这种具有面向对象特性的语言作为开发语言。在 C++ Builder XE2 下开发上位机数据的方法主要有：利用通信控件 TMSComm[6]；利用 Windows API 函数[7]；设计开发串口通信。本设计主要是在 Windows API 函数的基础上开发设计串口通信。

使用串口之前首先要进行串口初始化[8]，设置波特率为 19 200 bit/s，8 位数据位，1 个停止位，无奇偶校验。

```
bool OpenAndInitAllComPort() {
  AnsiString strCOM;
  DCB dcb;
  dcb.BaudRate = 19200;
  dcb.ByteSize = 8;
  dcb.StopBits = 0;
  dcb.Parity = PARITY_NONE;
  for (int i = 0; i < 16; i++) {
  g_hCOM[i] = 0;
  strCOM.printf("oWriteComCtrl%i", i + 1);
  g_oWriteComCtrl[i].hEvent =
  CreateEvent(NULL, true, false, strCOM.c_str
());
  }
// 打开 端口
OpenAndInitOneComPort("COM3", g_hCOM[3],
dcb);
OpenAndInitOneComPort("COM4", g_hCOM[4],
dcb);
OpenAndInitOneComPort("COM5", g_hCOM[5],
dcb);
OpenAndInitOneComPort("COM6", g_hCOM[6],
dcb);
OpenAndInitOneComPort("COM7", g_hCOM[7],
dcb);
OpenAndInitOneComPort("COM8", g_hCOM[8],
dcb);
OpenAndInitOneComPort("COM9", g_hCOM[9],
dcb);
return true;
}
```

参数设置是根据实际情况设定，串口初始化要使上下位机参数相同，才能进行通信。

4　PLC 从站程序设计

在工控机与西门子 S7-200 SMART 中，所有的 PLC 是作为从站与上位机进行信息交换的，采用 STEP7MicroWIN SMART[9]进行 PLC 程序的编写，其中 STEP 7 MicroWIN SMART 库中包含 ModBus RTU Slave 指令，ModBus RTU Slave 指令包括 MBUS_INIT 和两条指令。MBUS_SLAVE 首先进行串口初始化，编程时

首先要使用SM0.1(上电时运行一次)调用子程序MBUS_INIT进行初始化,使用SM0.0调用子程序MBUS_SLAVE进行初始化,并且进行参数设置[10]。对于本次设计,参数设置如下:模式选择Mode设置为1,即为启动Modbus,从站地址Addr设置;波特率Baud设置为192 00 bit/s;奇偶校验Parity设置为0无校验;端口Port设置为0,表示使用CPU中集成的RS485;延时Delay设置为缺省值0;保持寄存器区起始地址设置,以&VBx指定,采用间接寻址方式,初始化完成标志Done,若为1,则表示初始化完成,初始化错误代码Error,若为0表示没有错误。程序流程如图3所示。

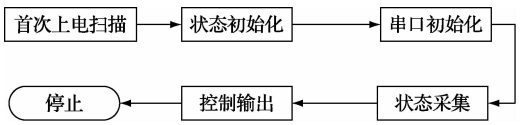

图3 PLC程序设计流程

5 系统可行性验证及结果分析

串口发送和接收都会显示有数据,表示通信成功,表示通信板卡安装成功,上位机下位机的物理连接已经完成。

在模拟物理平台的自动控制系统中,只要上电风机先开,风机不动作负载不能加载。对于交流负载来说,规定按照先阻性后感性或容性的加载顺序。

PLC的输入包括有本控/远控I0.0,电机的过载I0.1、A相欠载I0.2、B相欠载I0.3、C相欠载I0.4、PLC电源I0.6和紧急急停I0.5,对于模拟系统来说只有是远控时才能通过PLC对实际开关进行控制,所以验证时即设定为远控,输出为各个负载对应的电流值大小,由于对应负载比较多,需要对PLC进行模块扩展。下面以交流为例进行验证和分析:系统使用ModBus的03和10功能码进行读写操作,由于系统执行先读后写的规则,也就是上位机对下位机先发送03读操作命令,打开观察PLC输入指示灯的变化,有2个灯亮,分别是PLC电源和远控,打开串口显示界面,上位机发送的数据:01表示PLC的地址,功能码是03起始地址为0004,读取一个字节,后两位是CRC[11]校验。PLC接收到上位机发送的这串指令后首先验证格式以及地址和功能是否匹配,如果匹配将PLC中的信息传给上位机,上位机根据接收到的一串指令判断通信是否正常,如表1所示,接收到的寄存器值为41(十六进制),转换为二进制为0100 0001,验证了上电后PLC的电源接通且系统处于远控状态。

表1 上位机读命令执行

发送	03	00	04	02			
接收	00	01	C5	CB			
	01	03	02	00	41	78	74

读操作完成后再验证写操作,使用10功能码,在功率因数允许范围内,电阻加0.5A、10A和40A,电容加2A和4A,串口显示界面如表2所示,由于负载比较多,需要设置4个字,每个字节的高字节设为00,所以发送指令为00 03 00 50 00 00 00 06 十六进制03转换二进制为0000 0011分别表示风机启动和电阻0.5A,同理50表示二进制为0101 0000,表示电阻10A和40A接通,同理06表示加载的电容负载,同时PLC及其扩展模块也会输出相应的输出指示灯。

表2 上位机写命令执行

发送	01	10	00	00	00	04	08	00	03	00	50
	00	00	00	06	45	76					
接收	01	10	00	00	00						
	02	04	C1	CA							

根据上述方法就可以验证通信是否正确,此外,一个完整的系统中交流负载还有功率因数门限设置,温度门限设置,过载报警等部分。

6 结 论

该文设计了一种基于ModBus RTU协议的模拟物理平台的自动控制系统,由于ModBus协议的简单性和开放性,使得该协议得到广泛的应用。上位机使用C++Builder XE2开发环境实现上位机对下层设备的监控,程序设计主要使用C++编写,不但操作简便,而且充分利用了C++Builder XE2中的可视控件,使界面更加美观,减少高级语言复杂的开发流程。试验测试表明,系统稳定可靠,可以广泛地应用于其他设备。

参 考 文 献

[1] 尹崧宇,赵大军,房欣.关于远程监控与控制钻机的研究的探讨[J].西部探矿工程,2013,25(6):67-68.

[2] 王军霞,赵金龙,程秀竹,等.ModBus RTU通讯协议在S7-200 PLC中的应用[J].自动化信息,2013(4):53-55.

[3] 赵晓明,徐立,邵威,等.基于VC++的上位机与西门子系列PLC通信的研究[J].机电工程,2007,24(7):42-44.

[4] 唐建东.基于ModbusRTU的变压器油微水变送器设计[J].电子测量技术,2013,36(5):111-113.

[5] 汪正果.Modbus协议在S7—200 PLC与PC机通信中的应用[J].煤矿机械,2010,31(2):192-194.

[6] 李小亭,张深,方立德,等.基于PLC的小型高精度多相流实验装置测控系统设计[J].电子测量与仪器学报,2014,28(6):670-673.

[7] 张捍卫,韦鹏宽.C++ Builder中串口通信的实现[J].电脑知识与技术:学术交流,2007,3(14):432-433.

(下转第79页)

参考文献

[1] 张大伟,陈佳品,冯洁,等. 面向准危重病人的区域化无线监护系统研制[J]. 仪器仪表学报,2014,35(1):74-81.

[2] 夏立方,蔡娇,赵升,等. 基于ZigBee技术的智能无线调光系统设计[J]. 电子测量技术,2013,36(10):109-114.

[3] 裴永召,朱蕴璞. 基于ZigBee的智能扬声器系统设计[J]. 国外电子测量技术,2014,33(2):45-48.

[4] 焦尚彬,宋丹,张青,等. 基于ZigBee无线传感器网络的煤矿检测系统[J]. 电子测量与仪器学报,2013,27(5):436-442.

[5] 汪燕. ZigBee组网的温度数据采集器的设计[J]. 计算机与现代化,2012(8):101-104.

[6] 陈章进,姚真平,张建峰. 基于ZigBee技术的城市智能公交系统设计[J]. 电子测量技术,2014,37(4):38-42.

[7] 王春香,纪松波. 采用ZigBee技术的温室环境监控系统设计[J]. 电子测量技术,2014,37(12):120-122.

[8] 奇华,李铮,刘 军. 基于ZigBee的污水监测系统节点软件设计[J]. 国外电子测量技术,2014,33(12):26-27.

[9] 汪玉凤,尹靖康,刘翘楚,等. 新型煤矿安全检测系统的设计[J]. 计算机测量与控制,2013,21(4):939-941.

[10] 曲丽蓉,胡荣,范寿康. LabVIEW、MATLAB及其混合编程技术[M]. 北京:机械工业出版社,2011.

作者简介

周海鸿,1962年出生,1984年7月毕业于。参与设计过广播系统、楼宇智能对讲系统、数字电视分支分配器等,并发表过多篇论文。

周嘉奉(通讯作者),1991年出生,在读研究生。主要研究方向为集成电路测试理论。

E-mail:309162822@qq.com

(上接第54页)

[4] 何璇. LED室内照明关键技术的研究[D]. 广州:暨南大学, 2013.

[5] 刘娜. 红外通讯技术与蓝牙区别解析[J]. 信息系统工程, 2012(1):26.

[6] 何惠森. 基于AC-DC开关电源系统的电磁兼容设计及稳定性研究[D]. 西安:西安电子科技大学, 2012.

[7] 赵慧荣. LED驱动电路的电磁噪声研究及其改进[D]. 西安:陕西科技大学, 2012.

[8] 胡力元, 闫斌, 刘廷章. 大功率LED灯具的单级PFC恒流驱动及模拟调光技术的研究[J]. 电力电子技术, 2014(13):93-97.

[9] 刘秉安. 照相手机的LED闪光灯驱动电路设计的改进[J]. 电子测量技术,2013,36(4):24-27.

[10] 耿富平,谈恩民. 基于S3C6410的Android系统移植[J]. 国外电子测量技术,2014,33(4):76-80.

作者简介

邓术,1990年出生,硕士研究生。主要研究方向为智能调光系统与控制信号传输和开关电源技术。

E-mail:15578398562@163.com

何志毅(通讯作者),1965年出生,教授,博士。主要研究方向为LED无线光通信、光电显示与图像技术研究。

E-mail:hezhiyi@guet.edu.cn

(上接第74页)

[8] 安宪军,黄尔烈,贾少锐,等. 基于Delphi7.0的上位机与PLC的通信[J]. 现场总线技术应用,2007,23(3):47-48.

[9] 廖常初. S7-200 SMART与S7-200的比较[J]. 电工技术,2013(11):52-53.

[10] 刘明,郑敏. 基于ModBus RTU通讯协议在西门子PLC S7-200的应用[J]. 科技传播,2014(13):224-225.

[11] 蔡淼. ModbusRTU协议中字节型CRC-16算法分析与实现[J]. 物联网技术,2015(3):35-36.

作者简介

单星,1989年出生,硕士研究生。主要研究方向为数据通信与计算机网络。

E-mail : 1053363656@qq.com