文章编号：1005-5630(2013)01-0070-05

Modbus/TCP协议的通信处理器模块设计*

李慧燕[1]，费 鹏[2]，沈昱明[1]
（1. 上海理工大学 光电信息与计算机工程学院，上海 200093；
2. 上海自动化仪表股份有限公司，上海 200233）

摘要：为了实现通信处理器模块通信的功能，在实时操作系统uC/OS-II和ARM7内核的软硬件平台上，通过移植LwIP到ARM开发平台提出了一种支持多线程实时应用的嵌入式TCP/IP协议栈的方案。在通讯应用层上，将Modbus帧嵌入到TCP帧中，分析研究Modbus/TCP协议通信结构模型，最终简单可靠地实现了嵌入式Modbus/TCP通信协议。结果表明，结合Modbus/TCP通信协议，可通过创建多个线程函数，稳定有效地实现Modbus/TCP客户端/服务器端之间数据的传送。

关键词：实时操作系统；LwIP；Modbus/TCP；客户端/服务器
中图分类号：TP 273 **文献标识码**：A **doi**：10.3969/j.issn.1005-5630.2013.01.014

A design of communication processor module based on Modbus/TCP protocol

LI Huiyan[1], *FEI Peng*[2], *SHEN Yuming*[1]
(1. School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China;
2. Shanghai Automation Instrumentation Co., Ltd., Shanghai 200233, China)

Abstract: To realize the functions of communications processor module, an embedded TCP/IP protocol stack was proposed based on the uC/OS-II real-time operating system and the hardware platform of ARM7 kernel, which can support multi-threaded real time application by transplanting the LwIP to ARM development platform. On the communication application layer, the Modbus frames was embedded to the TCP frames, and the Modbus/TCP protocol communication structure model was analyzed, in order to ultimately achieve the embedded Modbus/TCP communication protocol simply and reliably. The results indicated that the Modbus/TCP data transfer between client and server was realized stably and effectively by combining with Modbus/TCP protocol and establishing several thread functions.

Key words: real-time operating system; LwIP; Modbus/TCP; client/server

引 言

所谓工业以太网，是根据国际标准IEEE802.3，设计应用于工业控制系统现场的需要，它的特点主要有系统安全性高和数据实时性强等。近年来，工业以太网控制技术和网络协议设计技术快速发展，协议

* **收稿日期**：2012-06-14
作者简介：李慧燕(1988-)，女，甘肃民乐人，硕士研究生，主要从事通信协议方面的研究。

设计也有了突破性的进展，工业以太网技术得以迅速发展。

Modbus-IDA 组织是由施耐德公司成立的，就是为了专门对 Modbus 协议进行研究和开发的。在国内，Modbus TCP/IP 协议已经处于比较成熟的阶段，并对其广泛应用。为了让 Modbus 广泛有效地使用，提出了一种支持多线程实时应用的方案，即基于 AT91R40008 的微处理器，在实时操作系统 uC/OS-II 和 ARM7 内核的软硬件平台上，通过移植 TCP/IP 协议栈[1] LwIP 到 ARM 开发平台并结合 Modbus/TCP 协议实现通信处理器模块通信的功能。

1　Modbus/TCP 协议模型

Modbus/TCP 协议[2-3]是在 TCP/IP 标准中，应用层采用工业领域事实标准 Modbus 实现的。经过国际公认，502 端口被专门用于 Modbus TCP/IP 应用层，且其串行总线方式支持各种介质的 rs-232、rs-422、rs-485 接口，网络通信模式如图 1 所示。

在一个客户端与服务器的以太网 TCP/IP 协议为基础的网络上，Modbus 报文传输服务提供商的设备之间可以进行相互的通信，且支持 Modbus 请求、响应、指示和证实这 4 种类型的客户端/服务器模式报文。Modbus/TCP 客户端首先要通过启动事务报文处理，并在网络上发送一个 Modbus 请求，服务器端接收到该报文请求，产生 Modbus 指示信号，当服务器收到该请求时，会自动产生一个 Modbus 响应，并向客户端发送此响应，当客户端接收到信息时，也会做出响应的反应，即产生 Modbus 证实来确认已经将 Modbus 请求发送完毕。

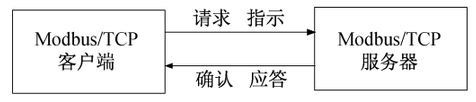

图 1　Modbus/TCP 的网络通信模式

Fig. 1　The network communication mode of Modbus/TCP

Modbus TCP/IP 的通信系统可以包括不同类型的嵌入式设备，例如 TCP/IP 网络可以通过网桥或交换机与串行链路子网相连，且客户端串行链路和服务器端串行链路通过 TCP/IP 网关连接到 MODBUS TCP/IP 上，最终可以相互之间进行通信，其通信结构如图 2 所示。

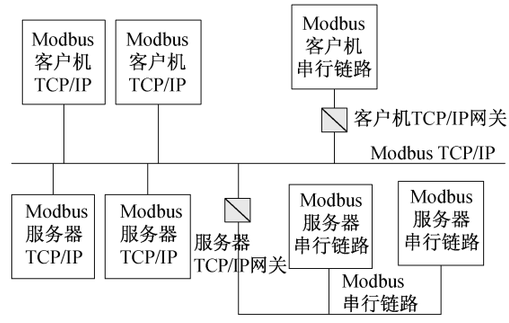

图 2　Modbus/TCP 通信结构

Fig. 2　Modbus/TCP communication structure

Modbus/TCP 功能组件结构模型[4]主要由四个层次组成，由下到上是 TCP/IP 栈、TCP 管理层、通信应用层和用户应用程序。其中，在 Modbus/ TCP 通信的应用层中包含了 Modbus 客户端、Modbus 服务器、Modbus 客户端接口和 Modbus 服务器接口四个部分，是系统的核心所在。Modbus 设备可以提供客户端/服务器 Modbus 接口和 Modbus 后台接口，而后台接口包括四种数据类型：离散输入 Discrete Input、离散输出 Coil、寄存器输入 Input Register 和寄存器输出 Holding Register。

Modbus 客户端完成对用户的远程控制和设备间的交换信息，用户发送一个 Modbus 请求到客户端接口，然后调用一个 Modbus 等待，最后再确认该事务处理。Modbus 客户端接口允许用户应用程序生成，并通过提供的 Modbus 服务请求接口访问 Modbus 应用对象。Modbus 服务器的主要功能是等待接收一个 Modbus 请求来读取和写入，然后生成 Modbus 响应。Modbus 的后台接口仅仅是一个 Modbus 服务器的应用程序对象之间的接口。

2 硬件开发平台设计

考虑到网络协议软件和实时操作系统与嵌入式工控产品的应用发展需求，硬件平台采用了美国 Atmel 公司提供的 AT91R40008 微控制器和台湾 Asix 公司推出的一款基于 AX88796 网卡的以太网接口芯片。硬件开发平台框图如图 3 所示。

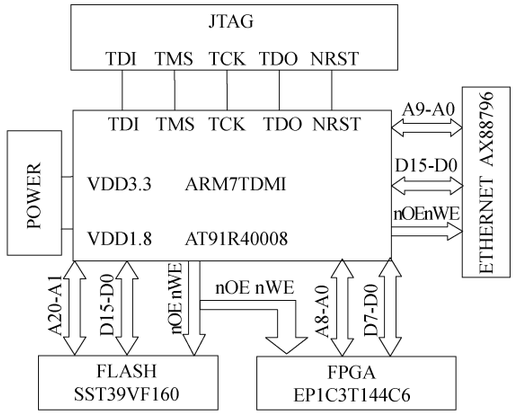

图 3 系统硬件开发平台框图

Fig. 3 The block diagram of system hardware development platform

AT91R40008 是一款主要面向嵌入式应用的高性能 32 位微处理器，目前在很多嵌入式设备上已经被大量的使用，工作频率为 66 MHz，且集成 256 kB 的片内 ARM，支持嵌入式 ICE 内电路仿真以及调试通信接口，不需要外扩 RAM 就可以满足一般的嵌入式系统的开发。

AX88796 是一款内部集成有 10/100 Mbps 自适应的介质访问控制层（MAC）[5] 和物理层收发器（PHY）的以太网控制器，与 NE2000 快速兼容。AX88796 与 AT91R40008 的接口电路如图 4 所示。

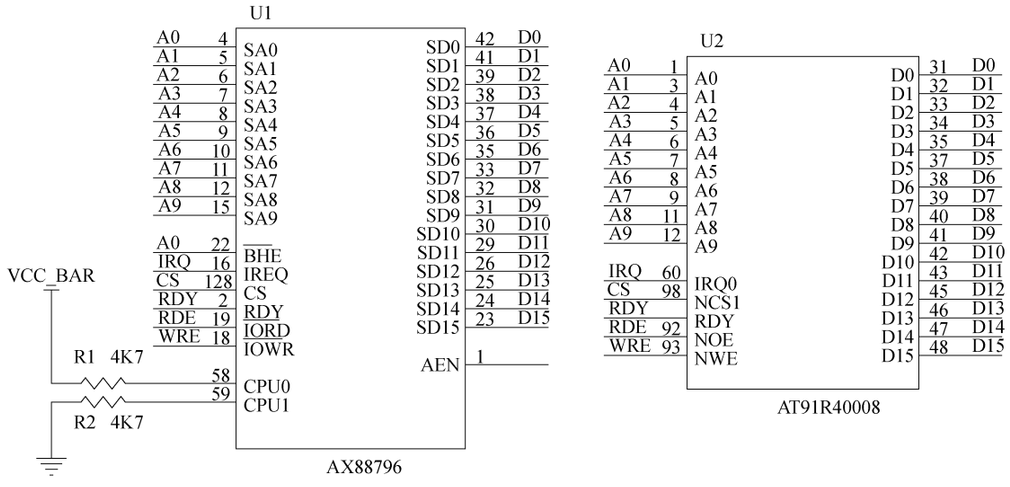

图 4 AX88796 与 AT91R40008 的接口电路

Fig. 4 The interface circuit of AX88796 and AT91R40008

片外 Flash 扩展选用 SST39VF160，是一个 1 MB 16 位的 CMOS 多功能 Flash（MPF）器件，由 SST 特有的高性能 SuperFlash 技术制造而成。调试工具 JTAG 是一种国际标准测试协议，主要用于芯片内部测试及对系统进行仿真、调试，AT91R40008 的 JTAG 接口共有 5 条信号线：NRST、TMS、TCK、TDI、TDO 分别为测试复位输入信号、模式选择、时钟、数据输入和数据输出线。为了拓展本通信模块的适用范围，还应该具有能够下载配置文件的串口，故本通信模块除了以太网和 RS485 接口外，另外还增加了 RS232 接口。

3 嵌入式 TCP/IP 协议栈的实现

考虑到系统的实时可靠性和代码公开的问题，采用代码开放的低成本的实时嵌入式操作系统 uC/OS-II和 TCP/IP 协议栈 LwIP，并结合采用 Modbus 协议的应用层来设计该系统的软件结构，其软件架构如图 5 所示。

3.1　uC/OS-II 的移植[5]

为了使实时操作系统 uC/OS-II 能够在 ARM7 的硬件开发平台 AT91R40008 上正确地运行，因此就要先将操作系统移植到该 ARM 处理器上。须知的是，在编写与处理器硬件相关的代码时要用汇编语言来完成，而操作系统 uC/OS-II 的大部分代码还是要用 C 语言来编写的。在进行操作系统的移植过程中，最主要的是实现与处理器息息相关的代码部分，具体的有使用 C 语言编写的头文件 OS_CPU. H、使用汇编程序语言编写的源文件 OS_CPU_A. S 和需要 C 程序语言编写的源文件 OS_CPU_C. C。

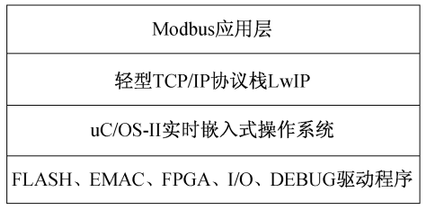

图 5　嵌入式 TCP/IP 协议栈软件架构
Fig. 5　The software architecture of embedded TCP/IP protocol stack

3.2　LwIP 的移植[6-8]

LwIP 的含义是轻型(Light weight)TCP/IP 协议栈，既可以移植到操作系统上，又可以在无操作系统的情况下独立运行。它是一种源代码开放的协议栈，可方便的用于嵌入式系统，它的成本较低，是用户使用的理想选择。它尽可能少的减少内存的使用率和缩小代码容量，这样就可以让 LwIP 适用于资源有限的小型平台，典型的如嵌入式系统。为了简化处理过程和内存要求，LwIP 对 API 进行了裁减，可以不复制一些数据。

在/include/arch 文件下的 cc. h 等头文件中存放这一些与处理器相关的数据长度和位顺序，它们的定义都与移植操作系统 uC/OS-II 时定义的数据参数是相符合的。通常在 C 语言的结构体中，struct 遵循四字节对齐结构。

操作系统模拟层的存在主要是为 LwIP 协议栈的移植提供便利条件，具体的移植涉及到的函数主要包括信号量操作函数、邮箱操作函数、实现 sys_arch_timeouts()函数和实现 sys_thread_new()函数这四个部分。

4　通信应用层软件设计

根据 Modbus/TCP 规范提供的参考组件模型，采用分层式软件设计方法。其中，在通信应用层软件设计过程中，通过创建多个线程函数来实现客户端/服务器之间数据的传送。

通信控制器模块发送定值信号到定值模块 SP 卡上的线程函数 sndto_sp_card_thread()；通过调用 sp_copy_modreg_to_485buf()函数，将 Modbus 协议对应地址中(Coils，Holding Reg)的数据拷贝到要发送的数据缓冲 485buf 中，然后通过 38 译码器选择通道，最后调用 sndto_sp_card()函数，通过 485 发送数据到 SP 卡上。

通信控制器模块接收来自定值模块 SP 卡的定值状态信号的线程函数 recvfrom_sp_card_thread()；通过调用 sp_recvfrom_fpga_to_485buf()函数，从相应 fpga(该芯片通过 RS485 接口进行 m 序列的发送和接收)内存中读取数据数据放入 485buf 中，然后调用 sp_copy_485buf_to_modreg()函数，将接收到定值卡 SP 卡数据拷贝到 Modbus 协议对应的地址中。

通信控制器模块接收来自调理模块 AD 卡的调理信号的线程函数 recvfrom_ad_card_thread()；通过调用 ad_recvfrom_fpga_to_485buf()函数，从相应 fpga 内存中读取数据放入缓冲 485buf 中，然后调用 ad_copy_485buf_to_modreg()函数，将接收到调理卡 AD 卡数据拷贝到 Modbus 协议对应的地址中。

Modbus/TCP 客户端线程函数 client_thread()；通过调用 conn_netconn()和服务器建立连接。连接一旦建立，客户和服务器之间就可以通过调用函数 netconn_write()来进行 Modbus/TCP 事务报文的传输，然后调用 netconn_recv()读应答报文，并根据事务响应情况给用户应用发送证实信息。最后待数据传输结束以后，双方调用函数 mbserver_close()关闭 TCP 连接。

Modbus/TCP 服务器主线程函数 mbserver_thread()；通过调用函数 netconn_new()创建一个套接字，然后调用函数 netconn_bind()将该套接字和本地网络地址绑定在一起，再调用函数 netconn_listen()

监听 TCP 502 端口的连接请求，最后调用函数 mbserver_accept()接收并产生一个新的线程处理连接，然后分析 netconn_recv()读取的报头并处理请求，等待请求成功或关闭连接。

5 结 论

介绍了在实时嵌入式操作系统 uC/OS-II 和 ARM7 内核的软硬件平台上，结合 Modbus/TCP 协议实现通信处理器模块信号传输的方法。将 uC/OS-II 实时操作系统移植到 ARM7 AT91R40008 系列的处理器内核上，再将嵌入式 TCP/IP 协议栈 LwIP 移植到该操作系统，实现了一种多线程的实时应用协议栈。在通讯应用层上，则在将 Modbus 信息帧嵌入到 TCP 帧中，分析研究 Modbus/TCP 协议通信结构模型，最终简单可靠地实现了嵌入式 Modbus/TCP 客户端/服务器端之间的通信。

参考文献：

[1] 王海，张娟，朱晓阳，等. TCP/IP 协议族[M]. 4 版. 北京：清华大学出版社，2011：300－319.
[2] 王可鹏. 基于 Modbus TCP/IP 通信的实现[J]. 电脑知识与技术，2008，4(3)：553－555.
[3] 司马莉萍，贺贵明，陈明榜. 基于 Modbus/TCP 协议的工业控制通信[J]. 计算机应用，2005，25(S1)：29－31.
[4] 金青，戴胜华，欧阳劲松. 基于 Modbus/TCP 的工业以太网通信[J]. 仪器仪表标准化与计量，2006(1)：22－24.
[5] 宋玉贵，康婷颋. 基于 ZigBee 的天幕靶信号处理装置的设计与研究[J]. 光学仪器，2012，34(1)：55－58.
[6] 王晓鸣，王树新，张宏伟. 实时操作系统 uC_OS_II 在 ARM 上的移植[J]. 机电一体化，2007，13(1)：56－58.
[7] 阙大顺，王近涛. LwIP 协议在 uC/OS-II 系统上的移植与实现[J]. 舰船电子工程，2006，26(4)：89－91.
[8] DUNKELS A. TCP/IP 协议栈 LwIP 的设计与实现[M]. 焦海波，译. 北京：北京航空航天大学出版社，2006：1－12.

(上接第 69 页)

PV 值可以估算出三个干涉图的局部光圈 ΔN 分别为：1.3、0.4、0.8，这个数值与直接用肉眼判定的局部光圈值基本上吻合，这就说明干涉图像的处理结果基本上达到了样机预期的目标。接下来要做的就是将本样机测量的数据与市场上的干涉仪测得的数据进行对比，经行全面的误差分析，做适当的改进，进一步提高精度。

4 结 论

本系统应用数字图像处理技术，通过 MATLAB 图像处理软件编程，实现了对本实验室研制的球面干涉仪检测信号(干涉图)的自动化处理，可以绘出三维波面图以及计算出被检镜片的面型数据 PV 值和 RMS 值。该算法相比空域相位测量法中的傅里叶变化(FFT)算法和空间载波相移法(SCPS)算法虽然在精度上略低一筹，但 SCPS 算法需要复杂的修正处理，而 FFT 算法需要大量复杂的计算，所以文中干涉图像处理算法相对简单。对目前大多数光学企业来讲，市面上现有的干涉仪由于价格昂贵、操作繁琐、体积庞大等原因仅仅使用在镜片的终检环节上，且不适合大批量的在线检测。而文中算法需要的设备简单，操作方便，可以更好地满足镜片加工企业大批量生产时非接触在线面形的检测要求。

参考文献：

[1] 韩振华，林 健，卓金寨，等. 一种球面在线检测系统及其结构设计[J]. 光学仪器，2012，32(1)：76－80.
[2] 李全臣. 干涉图数据处理的一种方法[J]. 计量技术，1999，3(6)：3－6.
[3] 鄢静舟，雷 凡，周必方，等. 用 Zernike 多项式进行波面拟合的几种算法[J]. 光学 精密工程，1999，7(5)：119－128.
[4] 龚 纯，王正林. MATLAB 语言常用算法程序集[M]. 北京：电子工业出版社，2008：115－141.
[5] WILLIAM K P. 数字图像处理[M]. 邓鲁华，张延恒，译. 北京：机械工业出版社，2005：158－433.
[6] 朱 昊，解 波，黄振宇，等. 泰曼－格林干涉仪干涉条纹计算机图像处理试验系统[J]. 大学物理，2007，26(2)：42－44.
[7] 鄢静舟，雷 凡，周必方，等. 干涉图特征信息自动采集方法[J]. 光学技术，2000，26(1)：70－75.
[8] 张 伟，刘剑峰，龙夫年，等. 基于 Zernike 多项式进行波面拟合研究[J]. 光学技术，2005，3(5)：674－677.