[文章编号] 1003－4684(2020)04-0055-05

基于 Modbus TCP 高速网络数据通讯系统

郑 振，赵大兴

（湖北工业大学机械工程学院，湖北 武汉 430068）

[摘 要] 针对传统工业自动化控制领域数据传输短距离、实时性低、维护成本高的问题，设计出基于 Modbus TCP 高速网络数据通讯系统。该系统终端硬件平台采用 STM32F407 作为采集系统的处理器，DP83848 芯片作为网络收发芯片，设计从站的硬件电路；软件上实现 Modbus TCP 协议和 uIP 协议栈在 ARM cortex-M4 平台上的移植；最后通过主站上位机软件，构建基于 ARM 的网络化高速实时数据采集系统，进行主从通信和数据采集。实验结果表明，该系统达到预期的设计目标，能够实现稳定、实时的数据采集。

[关键词] Modbus TCP 协议；工业以太网；uIP 协议栈；嵌入式系统

[中图分类号] TP273 [文献标识码] A

许多学者对工业自动化控制领域数据传输进行了研究。文献[1]设计了一种与底层链路无关的 ModBus 协议的协议栈，较好实现了数据的可靠通信，但其控制算法协议复杂，移植困难，对硬件的要求比较高。文献[2]一种基于 Modbus-RTU 协议设计的库房环境实时监控系统，在可靠性与稳定性上取得了一定的效果，但其传输距离存在明显的局限性。文献[3]基于 ARM 处理器和 MODBUS-RTU 通讯协议的温控系统，通过 RS232/485 总线组成二级通信网络，采用 MODBUS 协议“主－从”方式通信，但其通讯响应慢，时效性不高。文献[4]基于 PROFIBUS 现场总线实现了，PLC 控制系统稳定、高效的数据通讯，但其硬件成本比较高、研究投入大。文献[5]提出了基于 FreeModbus 协议栈的 Modbus/TCP 数据通讯控制系统，较好实现了数据的远程通讯与传输，但其模块高度集成化，无法根据需求进行定制更改。为了解决工业自动化中的传输距离短、时效性低、成本过高的问题，本文设计了一种基于 uIP 协议栈和 Modbus TCP 协议采集数据，并把数据传输至服务器端的一种数据通讯系统。

1 系统总体设计

基于 Modbus TCP 高速网络数据通讯系统可以看做是在以太网上运行的 Modbus，但其仅仅采用 TCP/IP 标准，简单地把 Modbus 所传输的信息包进行处理，再通过以太网发送给目标设备。这种方式使得任何 Modbus TCP 设备可以通过以太网进行连接和通信。而 Modbus TCP 网络的从站设备数量仅仅局限于网络物理层的承载能力，因此一个 Modbus TCP 主站可以控制更多的从站设备，极大提高了设备的利用率。基于 ModbusTCP 高速网络数据通讯系统采用 STM32F407VET6，网络协议采用 uIP 协议栈，通信协议采用 Modbus TCP 协议，最终通过 uIP 和 Modbus TCP 实现对数据高速、实时采集。系统硬件结构如图 1 所示。

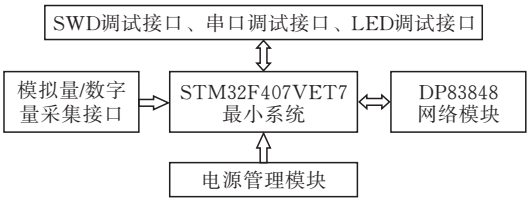


图 1 系统硬件结构

2 系统硬件设计

2.1 ARM 最小系统

主控采用 ST(意法半导体)最新的 ARM 内核 STM32 系统处理器（ARM Cortex-M4 内核）STM32F407VET6(LQFP100)。此款微控制器拥有丰富的硬件资源，极大的 flash 和 RAM，主频可达 168 MHz。主控板主要负责数字量或者模拟量的信号采集、控制网络的链接、数据的解析和传输，实现了数据的高速通讯。最小系统原理如图 2 所示。

[收稿日期] 2020－02－13

[第一作者] 郑 振(1995－)，男，河南驻马店人，湖北工业大学硕士研究生，研究方向为嵌入式系统，工业以太网

[通信作者] 赵大兴(1962－)，男，湖北崇阳人，湖北工业大学教授，研究方向为机器视觉，智能装备

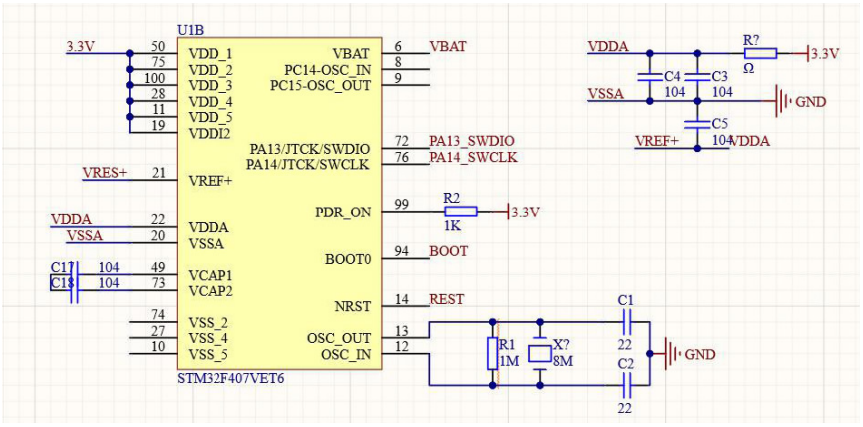


图 2 最小系统原理

2.2 以太网模块

作为一款以太网控制器，DP83848 设计用于在最严苛的环境中实现以太网连接，可在－55～125℃的军用级温度范围内满足 IEEE 802.3u 标准。其功耗低，有标准的 3.3 V MAC 接口，最大数据传输速率理论可达 100 Mb/s。DP83848 提供两个灵活的 LED 指示灯，一个用于链路， 另一个用于速度。此外，MII 和 RMII 都得到了支持，以确保设计的简便性和灵活性。其典型应用电路如图 3 所示，该模块在电路板上电路如图 4 所示。

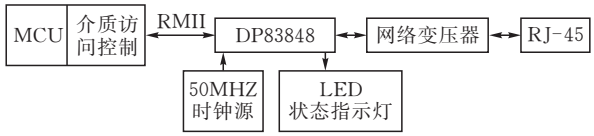


图 3 DP83848 典型应用电路

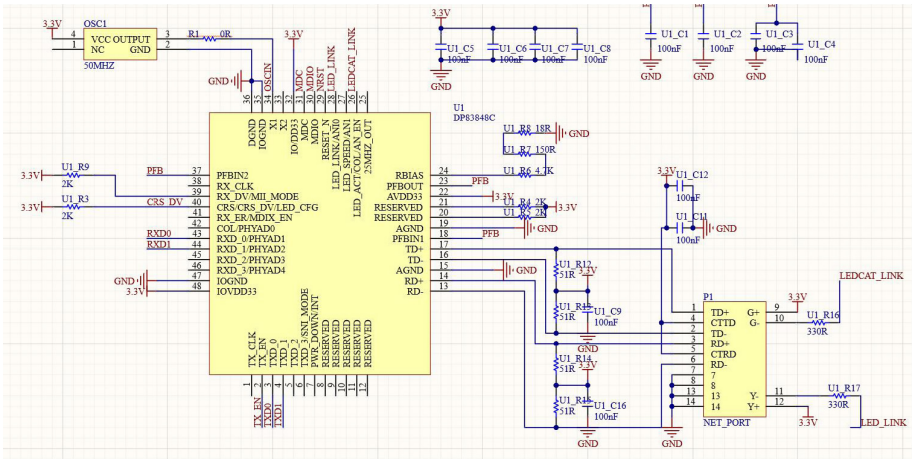


图 4 DP83848 网络模块电路

2.3 系统调试接口

STM32 不仅支持 JTAG 接口，还支持 SWD 接口进行编程调试。SWD 模式需要的引脚少，只需要通过简单的 4 根线与 JLINK 仿真器连接，即可完成开发过程中程序的下载和跟踪调试。SWD 接口的引脚为 SWDIO，GND，3.3 V，SWCLK。系统调试接口电路如图 5 所示。

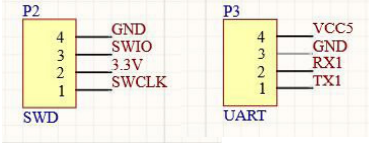


图 5 调试接口

2.4 电源管理电路

本系统用于高速网络传输，对电源功耗以及电源稳定性有较高要求，电源模块的设计是否合理关系到整个系统能否正常运行，因此选择良好的电源芯片变得十分重要。

在设计系统输入电源时，为了整个系统的演示方便，本系统使用电脑 USB 提供所需的电能，选择 ASM1117-3.3 电源芯片作为 5 V 转 3.3 V 电压转换芯片，在电源芯片前后加上合适电容，其作用是滤除相应高频低频信号干扰。在电路板上留出了多个 5 V以及 3.3 V 接口用于给外设供电，同时在电源与地之间接一个防反接二极管 M7，可承受瞬间反向电压，达到保护电路的目的。电源电路图如图 6 所示。

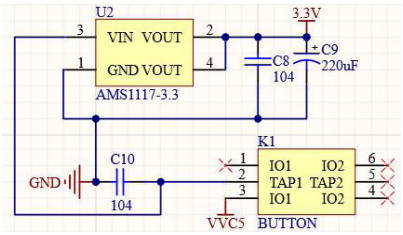


图 6　电源电路

3　系统软件设计

该控制系统的架构功能示意图如图 7 所示。TCP/IP 协议是数据传输可靠性的保证，而数据传输速度取决于该网络的带宽。通讯双方接收信息事先约定好数据报文的格式，是处理器对数据有效信息进行提取的关键。

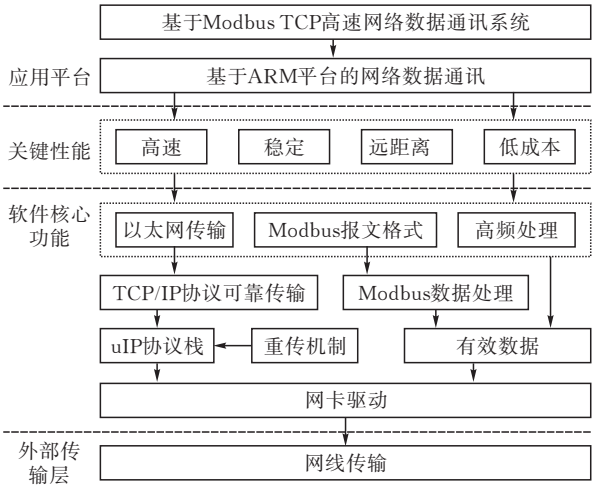


图 7　软件功能示意图

3.1　以太网传输模块

对于嵌入式系统而言，若能够运行本地 TCP/IP，则系统可以是公司局域网甚至是全球互联网。嵌入式设备有了 TCP/IP 的支持，设备将可以与网络中的其他主机进行通信，但是要使嵌入式设备进行网络通信，该设备必须要能运行可实现的 TCP/IP 协议栈[6]。uIP 协议栈就属于这样的网络协议栈，其重点是在应用层方面，即 TCP/IP 协议，对于底层协议（比如链路层协议），则一般由硬件实现。TCP/IP 数据流如图 8 所示。

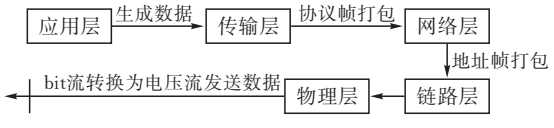


图 8　TCP/IP 数据流

上述就是发送数据的过程，接收则执行相反的操作。为了减小代码体积，实现基本 TCP/IP 功能，uIP 移除了许多并不必需的应用程序和协议栈之间接口，比如软件错误报告机制和动态的 TCP 连接相关的服务类型配置，以减轻单片机 RAM 的压力，降低单片机的购置成本。同时，uIP 采用事件驱动方式，当有事件发生时，会触发相应的应用程序，该程序可以指定宏定义，这样就可实现 uIP 调用用户应用程序。与其他 TCP/IP 协议栈不同的是，uIP 协议栈可以通过应用程序来实现重传机制，正是由于 uIP 所面对的目标对象架构 RAM 并不大，网络设备将数据包发送出去之后，uIP 并没有跟踪数据包内容，因此当数据包丢失时，uIP 则需要进行重传。当 uIP 要重传某个数据包的片段时，会设置重传标记，然后通知应用程序，重传该片段[7]。应用程序通过协议栈的调度来实现数据重传，使数据传输可靠性相比于其他协议栈更有效。

3.2　Modbus TCP 通讯协议

Modbus TCP 通信协议遵循基本的主从通信模式：主站设备采取主动查询的方式，发出启动请求给从站设备，然后由从站设备根据接收到的启动请求内容，准备数据响应发送给主站设备。Modbus TCP 通信系统包括能够连接至以太网的 Modbus TCP 从机，以及能够连接至以太网的 Modbus TCP 主机或网络服务器。

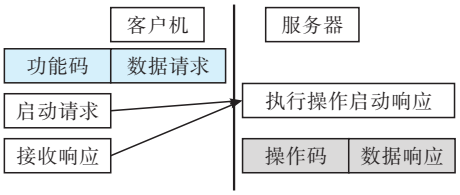
与普通 Modbus 不同的是，Modbus TCP 协议使用了一种专用的报文头识别单元 MBAP 报文头，可以使持多个独立的 Modbus 终端设备在使用同一个 IP 地址时不会发生冲突。在 Modbus TCP 中，如果将报文分成多个信息包依次发送，并在 MBAP 报文头上携带附加数据的长度信息，以此来使接收端识别报文的边界，接收端也可以接收到数据。TCP/IP 上的 MODBUS 请求/响应图如图 9 所示。

图 9　TCP/IP 上的 MODBUS 请求/响应

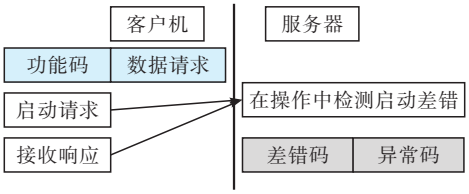
Modbus TCP 协议通过功能码来反映传输正常响应或传输错误响应（即异常响应）[8]。正常通讯过程响应如图 10a 所示。当产生错误或者异常响应时，服务器依旧会返回与客户机相同的功能码，并在该异常码后增加一个错误码，以此来告知客户机产生异常的原因，从而实现错误信息反馈。异常响应如图 10b 所示。

3.3　上位机

QT 可以同时开发 GUI 和非 GUI 程序。该软件提供了大量的应用接口程序及范例，并提供对 CAN 和 Modbus 的支持，极大缩短了开发时间。而 Qt Creator 是用于开发 QT 应用程序的软件，可通过直接调用控件，对控件进行编程，类似于 C++的



(a)正常响应



(b)异常响应

图 10 响应过程

编程方式完成上位机的制作。

在本设计中用到了文本框、下拉式菜单、按钮、定时器等组件。利用这些具有图形化接口的控件，可方便编写用户程序。其界面效果如图 11 所示。

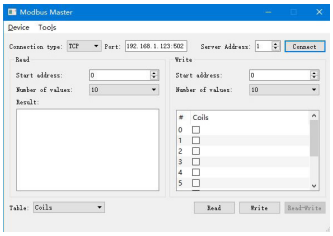


图 11 上位机界面

4 试验结果

系统测试主要以电脑作为客户端，单片机作为服务器，通过网络调试助手发送请求给单片机。程序初始化采集系统的 IP 地址为 192.168.1.128。单片机程序里源地址为 1000，输入寄存器个数为 4，使用 8 路 AD 采集端口 A0～A7 作为模拟量输入，8 路 IO 采集端口 C0～C7 作为数字开关量输入，AD 采样的值直接赋值给输入寄存器，数字量通过处理后赋值给线圈寄存器，然后通过协议发送至上位机端。硬件实物如图 12 所示。单片机的处理流程如图 13 所示。

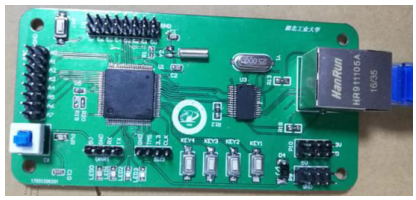


图 12 硬件实物

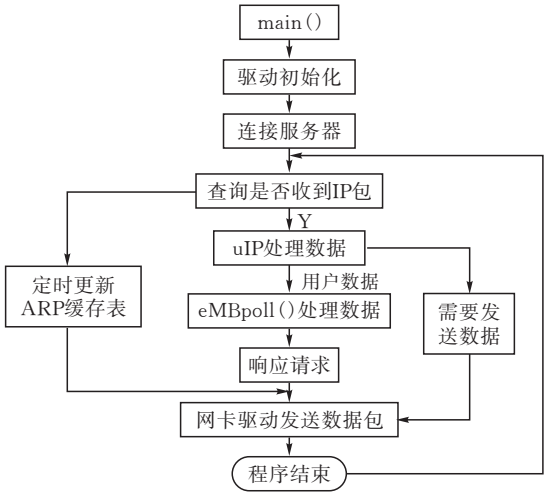


图 13 单片机处理流程

为了验证基于 Modbus TCP 高速通信系统的正确性，需要对该系统的功能进行分析，在上位机分别下发了 4 组指令，得到其发回的数据，并进行解析。

表 1 测试报文数据

次数	发送请求	接收反馈
1	00 00 00 00 00 06 01 03 00 00 00 03	00 00 00 00 00 03 01 0×83 0×02
2	00 00 00 00 00 06 01 03 03 E7 00 0A	00 00 00 00 00 03 01 0×83 0×02
3	00 00 00 00 00 06 01 03 03 E7 00 04	00 00 00 00 00 0B 01 03 08 00 FF 00 64 11 22 43 21
4	00 00 00 00 00 06 01 04 03 E7 00 04	00 00 00 00 00 0B 01 04 08 00 FF 00 64 11 22 12 34

从表 1 可以看出，在发送请求的 12 位 16 进制数据中，前 5 位为固定数据。在后 7 位数据中，以第 3 组数据为例，其中：06 表示在该数据后面的字节总数，01 表示从机地址；03 表示功能码；03 E7 为启动请求，换算成十进制为 999；00 04 表示为偏移地址，对应十进制为 4 。接收反馈的数据中，前 5 位数据为固定数据，第 6 位表示后面字节的总数，第 7 位表示地址，第 8 位表示请求的功能码，剩余数据表示各个寄存器数据。第 1 组由于单片机设置源地址为 1000，而单片机发送源地址为 0000，此时系统返回错误响应 0x83 0x02，表示非法数据地址；第 2 组由于单片机保持寄存器个数只有四个，而单片机请求读取 10 个，此时系统返回错误响应 0x83 0x02，表示非法数据地址；第 3 次和第 4 次为正常响应。

通过对发送数据和接收数据进行分析，验证了该系统基于 Modbus TCP 高速通信系统的正确性，同时为了验证通信速度的稳定性和快速性，利用 Wireshark 抓包工具对数据进行抓包截取，抓包取到的网络数据如图 14 所示。

从图 14 可以看出，通过 10 ms 周期的不断轮

A	B	C	D	E	F
Time	Source	Destination	protocal	lang	Info
10.000	192.168.1.123	192.168.1.128	Modbus/TCP	76	Query:
20.001	192.168.1.128	192.168.1.123	Modbus/TCP	71	Response:
30.011	192.168.1.123	192.168.1.128	Modbus/TCP	76	Query:
40.013	192.168.1.128	192.168.1.123	Modbus/TCP	71	Response:
50.022	192.168.1.123	192.168.1.128	Modbus/TCP	76	Query:
60.024	192.168.1.128	192.168.1.123	Modbus/TCP	71	Response:

图 14　网络数据包

询，向单片机发送数据，单片机能够在 1～3 ms 内高速响应并发回数据，其中通信速度、数据传输非常稳定。

5　结论

本文设计的以 STM32F407VET6 为核心的系统，通过 uIP 协议栈和 Modbus TCP 通讯协议实现了对数据实时采集。该系统以以太网通讯为原型，在设备联网的情况下数据就能够高速、稳定地传输到达目的地，较好解决了工业自动化领域数据传输的非实时性和距离短的问题，同时系统硬件结构简单，成本较低，比较容易运用到实际生产生活中。通过对该系统进行性能测试与通讯实验，结果表明该系统数据传输具有稳定性与快速性。

[参　考　文　献]

[1] 王佩. 面向物联网的 Modbus 协议栈设计与应用[D]. 成都：成都理工大学，2018.

[2] 朱毅. 基于 Modbus-RTU 的库房环境实时监控系统的设计与实现[D].武汉：华中师范大学，2019.

[3] 赖建军. 基于 ARM 处理器和 MODBUS-RTU 协议的温控系统设计[D].杭州：浙江工业大学，2016.

[4] 李千振. 基于 PROFIBUS 的污水处理 PLC 控制系统设计[D].大连：大连交通大学，2018.

[5] 朱阿曼. 基于 Modbus/TCP 通信的库房环境监控系统的设计[D].武汉：华中师范大学，2019.

[6] 祁树胜. SPI 接口以太网控制器 ENC28J60 及其应用[J]. 微计算机信息，2006，22(23)：266-268.

[7] 仇俊杰. 以太网络控制系统的研究及其协议分析[D]. 杭州：浙江大学，2006.

[8] 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.

High Speed Network Data Communication System based on Modbus TCP

ZHENG Zhen，ZHAO Daxing

(*School of Mechanical Engineering*，*Hubei Univ. of Tech.*，*Wuhan* 430068，*China*)

Abstract：Aiming at the problems of short distance of data transmission，low real-time performance and high maintenance cost in the field of traditional industrial automation control，a high-speed real-time data communication system based on ARM network is designed. The terminal hardware platform of the system adopts STM32F407 of ST company as the processor of the acquisition system，and DP83848 as the network transceiver chip，and designs the hardware circuit of the slave station. Modbus TCP protocol and uIP protocol stack are transplanted on ARM cortex-m4 platform. Finally，through the host computer software of the master station，a high-speed real-time data acquisition system based on ARM is built for master-slave communication and data acquisition. The experimental results show that the system achieves the desired design goal and can achieve stable and real-time data collection.

Keywords：Modbus TCP protocol；Industrial Ethernet；uIP stack；Embedded system

[责任编校：张　众]