Libnodave 库的 TCP 协议剖析

夏正龙[1],耿 浩[2]

(1. 江苏师范大学 电气工程及其自动化学院,江苏 徐州 221116;
2. 徐州上若科技有限公司 自动化事业部,江苏 徐州 221116)

摘 要:西门子系列 PLC 凭借出色的性能在工业应用场合得到了越来越广泛的应用,而工控领域不仅仅拘泥于就地集控方式,基于工业以太网络的远方集中监控应用也越来越广泛。目前上位机系统与西门子系列 PLC 进行以太网通讯普遍采用基于微软 COM/DCOM 技术达成的自动控制协定 OPC 协议,即工控组态软件方法,由于工控组态软件成本与工控数据点数多少相关,因此大型 PLC 自动控制系统软件成本高,性价比低。通过研究西门子 PLC 设备第三方开源驱动库 Libnodave,分别从应用的角度和库开发的角度对 Libnodave 源代码进行解析,给出了更简单清晰的数据包格式。通过 Ethernet 转 RS-485 设备连接 PLC 的驱动增强方法,详细介绍了测试代码的实现,该方法基于跨平台移植考虑,便于软件功能上的扩展。

关键词:ISO-on-TCP;Libnodave;以太网协议;可编程逻辑控制器
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2018)03-0160-05
doi:10.3969/j.issn.1673-629X.2018.03.034

TCP Analysis Based on Libnodave Library

XIA Zheng-long[1],GENG Hao[2]

(1. School of Electrical Engineering & Automation,Jiangsu Normal University,Xuzhou 221116,China;
2. Department of Automation,Xuzhou Shang Ruo Technology Co.,Ltd.,Xuzhou 221116,China)

Abstract:S7 series PLC of Siemens is playing an increasingly important role in industrial applications owing to its remarkable performance. Except for local control mode,the remote centralized monitoring based on industrial Ethernet is also widely applied. At present,the automatic control agreement OPC based on Microsoft COM/DCOM,namely industrial control software approach,is utilized commonly in communication between upper computer system and Siemens series PLC. Because the cost of industrial control group software is related to the number of industrial data points,the large PLC automatic control system is in high cost and low cost performance. In this paper,we analyze the Libnodave source code from the perspective of application and library development through the research on Libnodave,a third-party open source drive library,of Siemens PLC equipment and give a simpler and clearer packet format. The implementation of test code is described in detail with a driver enhancement method of Ethernet connecting to PLC via RS-485. In consideration of cross-platform transplantation,this method facilitates the expansion of software functions.

Key words:ISO-on-TCP;Libnodave;Ethernet protocol;PLC

1 概 述

现代工控领域多采用数字化智能装置代替传统的模拟仪表作为前端控制器,而数字智能装置一般都具备独自监测监控功能,能实时向上位集控后台实时上传工作状态。当前工控领域的集控方式由集中控制向分散控制,由分散管理向集中管理转变。西门子公司的 PLC(programmable logic controller)设备在工控领域应用广泛,其产品系列的丰富与可靠已经得到了广大用户的信赖。目前工控领域控制的实时性要求越来越高,自然需要一个高速的通讯网络。

随着以太网通讯在工业控制领域的普及,其通讯速率高、可靠性高,在实际应用中越来越广泛。西门子系列 PLC 以太网通讯模块有 cp243,cp343,cp443。200SMART 和 1200 自带以太网口。西门子以太网协议众多,有 ISO,ISO-on-TCP,TCP,UDP 等。ISO 协议是西门子早期的以太网通讯协议,通讯使用的是 MAC 地址。TCP、UDP 协议,属于用户自定义协议,PLC 端和上位机都需要用户写程序。ISO-on-TCP 协

收稿日期:2017-03-14 **修回日期**:2017-07-13 **网络出版时间**:2017-11-15
基金项目:江苏省自然科学基金青年基金项目(BK20160219)
作者简介:夏正龙(1983-),男,博士,讲师,研究方向为电力电子与电力传动、智能仪表开发。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20171115.1438.064.html

议是在 TCP/IP 协议层,按照 ISO 协议重新定义,通讯使用的是 IP 地址。因为 PLC 本身就支持 ISO-on-TCP 协议,所以 PLC 不用添加任何程序,只需要上位机按照规定的协议格式写程序就可以和 PLC 进行数据交换。

西门子公司开源驱动库 Libnodave 是一个开源驱动库,但该库的使用需要硬件匹配,它支持的通讯方式主要由 daveProtoMPI(针对西门子 300/400 系列 PLC 的 MPI 协议)、daveProtoMPI2(针对不带 STX 的 Andrew 版本西门子 300/400 系列 PLC 的 MPI 协议)、daveProtoMPI3(针对 step7 版本 300/400 系列 PLC 的 MPI 协议)、daveProtoMPI4(针对带 STX 的 Andrew 版本西门子 300/400 系列 PLC 的 MPI 协议)、daveProtoPPI(针对西门子 200 系列 PLC 的 PPI 协议)、daveProtoAS511(针对 S5 编程口协议)、daveProtoS7online(针对 s70nlinx. dll 动态链接库通信)、daveProtoISOTCP(针对带路由功能的 ISO on TCP 协议)、daveProtoISOTCP243(针对西门子 200 系列 PLC 设备中以太网模块 CP243 的 ISO on TCP 协议)、daveProtoISOTCPR(针对具有路由功能的 ISO on TCP 协议)、daveProtoMPI_IBH(针对通过网关联结的 MPI 协议)、daveProtoPPI_IBH(针对通过网关联结的 PPI 协议)、daveProtoNLpro、daveProtoUserTransport 组成。上述协议主要是 PPI 协议和 ISO on TCP 协议。

上位机软件连接西门子 PLC 可以通过四种方法。一是 opc server 连接 PLC,opc server 可以选用 Simatic Net、Kepserver 等[1]。二是组态软件连接 PLC。例如组态王驱动库,Intouch 的 DAServer 等。三是用自由口实现通讯[2]。四是编程方式连接 PLC,如开源的 Libnodave 和西门子的 prodave 库[3-4],而 PRODAVE 是用于上位机与 S7 系列 PLC 之间数据连接通信的商业软件包,它提供了一个接口函数库,DLL 和 LIB 库,以此完成 PLC 与上位机之间的数据通信。使用 PRODAVE 进行控制系统开发,需要调用开发包提供的动态链接库中的函数即可实现通信,而最新发布的 6.2 版新增加了对 Window 7 操作系统的支持。

以上四种方法,除了 Libnodave 是开源免费的,其他都需要授权。Libnodave 是跨平台的库,其支持 MPI 协议和以太网协议。以太网具有传输速率高、传输距离远、可靠性以及开放性较好等优点[5-12]。西门子公司 S7 系列 PLC 的通信可以通过开源驱动库 Libnodave 实现[13-14]。

文中参考 Libnodave 库,去掉 MPI 等协议,只保留需要的以太网协议,直接给出发包和收包的数据格式,代码结构清晰明了。Libnodave 库只提供了 cp243,cp343 的连接方式,文中在其基础上增加了 S7-200smart、西门子 1200 系列 PLC 的连接方式。

2　研究环境

设计的 Libnodave 库的 TCP 协议解析工作,都是在微软 Windows 7 环境下完成。后台 PC 机的 IP 地址为 192.168.1.18,子网掩码为 255.255.255.0。

操作系统:Windows 7;

编程软件:Visual Studio 2012;

西门子 S7-200smart 编程软件:S7-200 PC Access;

西门子 S7-300 编程软件:Step7 v5.5;

西门子 S7 系列 PLC:S7-300PLC + cp343,200SMART。

测试的 PLC 的 IP 地址是 192.168.0.25,子网掩码为 255.255.255.0。

由于西门子以太网中的 ISO on TCP 协议所采用的数据传输端口为 102,所以 port 设置为 102。

3　Libnodave 程序流程

在软件编写方面,鉴于通过工控组态软件或者 OPC 服务器/客户端的 PLC 远程连接上位机监测监控具有实时性较低、实施成本高等缺点,根据西门子 S7-300 与 S7-200SMART 的实际对象,采用西门子 Libnodave 开源免费函数库结合高级语言可以开发基于以太网通讯的监控软件,一定程度上优化远程监控计算机与 PLC 之间的通信。该方法对数据的采集与存储、故障分析与处理非常便利,具有实施难度低、数据交换方式灵活多变、实时性高等优点,具有极高的程序独立性,独立于西门子其他任何软件。

图 1 给出了 Libnodave 测试程序流程。

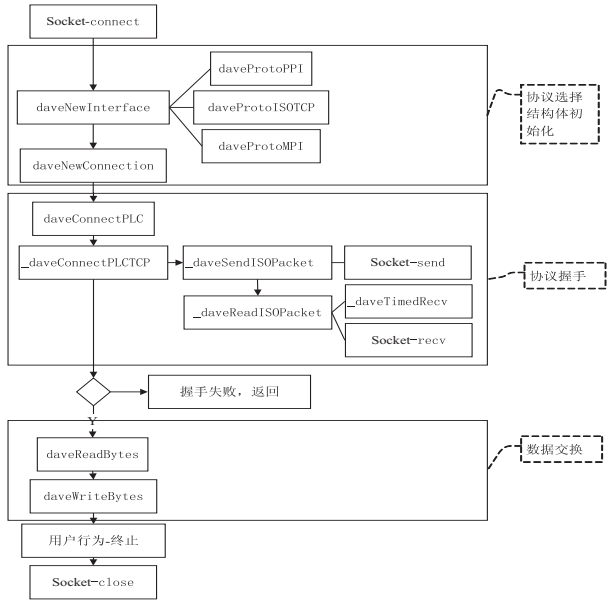

图 1　Libnodave 库测试程序流程

该程序用 socket 同步通讯,Libnodave 库协议握手需要调用 7 个函数。函数首先打开通信接口句柄后保存到相应变量中,该变量在电泳 daveNewInterface 时传递给新生成的 daveNewInterface 结构体。调用 daveNewConnection 时需要把已经生成的 daveInterface 结构体指针传送到新生成的 daveConnection 结构中保存。在调用其他功能函数时,硬件连接方面的信息通过 daveConnection 来传递,实现功能函数调用的协议不相关性。由上可见,发送的数据包分布在多个结构体中初始化,牵扯到多个函数的调用,代码结构纷繁复杂。

4 改进后的库函数

文中参考 Libnodave 库,改进后的库只有握手、读包、写包三个函数。数据包以 unsigned char 数组的形式给出,并标识出每一位的含义,代码清晰明了,方便移植。

由于所有的数据都是从 PLC 的内部存储空间获取,主要包括数据库 DB、位存储区 M、输入映像区 Inputs 和输出映像区 Outputs。针对上述四个区域,开发读取功能,并通过位逻辑 BOOL、字节 BYTE、整形 INT、双字节 WORD、长整型 DINT、双字 DWORD 以及实数 REAL7 中形式读取。

下面是封装的函数列表:

BOOL ConnectPLC();

BOOL ReadBytes(int area, int db, int start, int len, unsigned char * buffer);

BOOL WriteBytes(int area, int db, int start, int len, unsigned char * buffer);

area:读取的数据区,m 区是 0x83,DB 区 0x84。

db:m 区,值为 0;db 区,值为 db 区号。

start:读取的数据地址开始位置。

len:读取几个字节。

buffer:读取到的数值保存的缓冲区。

如:读取“DB1,W10”的数据,(W 表示一个字,所以是 2 个字节),函数应该写为:ReadBytes(0x84,1,10,2,buffer)。

4.1 握手数据包

每种以太网通讯模块的握手数据包都不相同。发送接收串都是 unsigned char 类型的数据。客户端向 PLC 发送握手数据包,如果数据包是不匹配的,PLC 是不会回数据的。所以接收到数据包并且数据包的长度是 22,就说明握手成功。握手通过后,就可以和 PLC 进行数据交换了。表 1 给出 cp243,cp343,1200,200smart 的握手数据包。所有发送的数据包前 2 个字节都是 0x03、0x00,第 3 和第 4 字节表示数据包的长度,计算公式为:串[2] * 256+串[3]。

表 1 cp243,cp343,1200,200smart 的握手数据包

PLC 型号	数据包
cp343	0x03, 0x00, 0x00, 0x16, 0x11, 0xE0, 0x00, 0x00, 0x00, 0x01, 0x00, 0xC1, 0x02, 0x01, 0x00, 0xC2, 0x02, 0x02 ,0x02 ,0xC0,0x01,0x09
cp243	0x03, 0x00, 0x00, 0x16, 0x11, 0xE0, 0x00, 0x00, 0x00, 0x01, 0x00, 0xC1, 0x02, 0x4d, 0x57, 0xC2, 0x02,0x4d,0x57,0xC0,0x01,0x09
1200	0x03, 0x00, 0x00, 0x16, 0x11, 0xE0, 0x00, 0x00, 0x00, 0x93, 0x00, 0xC1, 0x02, 0x10, 0x11, 0xC2, 0x02,0x03,0x01,0xC0,0x01,0x0a
200smart	0x03, 0x00, 0x00, 0x16, 0x11, 0xE0, 0x00, 0x00, 0x00,0x01,0x00,0xC1,0x02,0x00,0x00,0xc2,0x02, 0x02,0x00,0xc0,0x01,0xa

cp343:0x02 位置的值为 0x01,表示 PG 连接,0x02 表示 OP 连接,0x03 表示 Step7Basic 连接。

4.2 读数据包

表 2 为读数据包(“口”占一个字节);表 3 为读数据返回包。

表 2 读数据包

	偏移地址	数据	说明
数据头	0,1	0x03, 0x00,	值不变
	2,3	口, 口,	表示串的长度
	4-22	0x02, 0xf0, 0x80, 0x32, 0x01, 0x00, 0x00, 0xff, 0xff, 0x00, 0x0e, 0x00, 0x00, 0x04, 0x01, 0x12, 0x0a,0x10,	值不变
数据	22	口,	0x01 表示按位读,0x02 表示按字节读
	23,24	口, 口,	len/256,len%256
	25,26	口, 口,	db/256,db%256
	27	口,	0x83 表示 m 区,0x84 表示 db 区
	28	0x00,	值不变
	29,30	口, 口	(start * 8)/256,(start * 8)%256

如果读取 PLC 的数据包是不正确的,PLC 是不会回数据的。所以接收到数据包,说明读取成功。返回的数据包中包含了要读取的数据。

4.3 写数据包

文中设计数据可以向数据库 DB、位存储区 M、输入映像区 Inputs 和输出映像区 Outputs 中写入的功能,并可通过 BOOL、BYTE、INT、WORD、DINT、DWORD 以及 REAL 七种形式写数据。以 BYTE 为基本单元,以一帧数据为写入数据包为例,如表 4 所示。

表 3　读数据返回包

	偏移地址	数据	说明
数据头	0,1	0x03, 0x00,	固定值
	2,3	口, 口,	表示串的长度
	4-22	0x02, 0xf0, 0x80, 0x32, 0x03, 0x00, 0x00, 0xff, 0xff, 0x00, 0x02, 0x00, 0x06, 0x00, 0x00, 0x04, 0x01, 0xff, 0x04, 0x00, 0x10,	
数据	23,24	口, 口,	表示的是数据位长度,计算成字节公式:(串[23]*256+串[33])/8,其值应该和 len 一样
	25……	口, ……	返回的数据,比如返回 2 个字节数据,就占用串[25]和串[26]两个字节

表 4　写数据包

	偏移地址	数据	说明
数据头	0,1	0x03, 0x00,	值不变
	2,3	口, 口,	(35+len)/256, (35+len)%256
	4-14	0x02, 0xf0, 0x80, 0x32, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x0e	值不变
	15,16	口, 口,	(4+len)/256, (4+len)%256
	17-22	0x05, 0x01, 0x12, 0x0a, 0x10, 0x02	值不变
	23,24	口, 口,	len/256, len%256
	25,26	口, 口,	db/256, db%256
数据	27	口,	0x83 表示 m 区, 0x84 表示 db 区
	28	0x00,	值不变
	29,30	口, 口,	(start*8)/256, (start*8)%256
	31,32	0x00, 0x04	值不变
	33,34	口, 口,	(8*len)/256, (8*len)%256
	35……	口, ……	写入的数据,比如写入"db1,w10",就占用串[35]和串[36]两个字节

如果写入 PLC 的数据包是不正确的,PLC 是不会回数据的。所以接收到数据包并且数据包的长度是 22,就说明写入成功。

写数据包返回包
0x03, 0x00, 0x00, 0x16, 0x02, 0xf0, 0x80, 0x32, 0x03, 0x00, 0x00, 0x00, 0x00, 0x00, 0x02, 0x00, 0x01, 0x00, 0x00, 0x05, 0x01, 0xff

5　测试程序

测试程序主要有 4 个部分,分别为建立端口连接、设备联络握手、读写数据以及句柄释放,详细流程如图 2 所示。

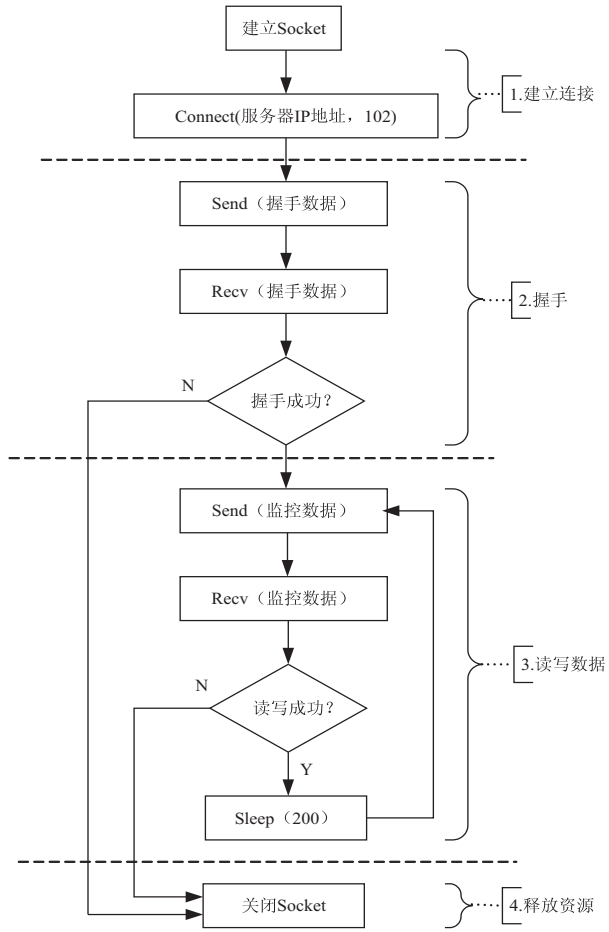

图 2　测试程序流程

(1)建立连接。

```
connect(sockClient,(SOCKADDR *)&addrSrv,sizeof(SOCKADDR));
//tcp 连接与初始化连接与端口号
```

(2)协议握手。

```
ConnectPLC();
//通过协议握手数据的发送与接收情况启动相关校验程序,从而判断是否握手成功
```

(3)数据交换。

```
unsigned char v2[2]={0};
daveReadBytes(AREA_DB,1,10,2,(void *)v2);
unsigned char v4[2]={0};
Put16(v4,2);
WriteBytes(AREA_M,0,20,2,(void *)v4);
//通过读写数据部分,启动数据帧的发送与接收工作,主要完成上位机与 PLC 的数据交换与处理。
```

(4)断开连接

```
closesocket(sockClient);
//关闭套接字
```

测试程序截图如图 3 所示。

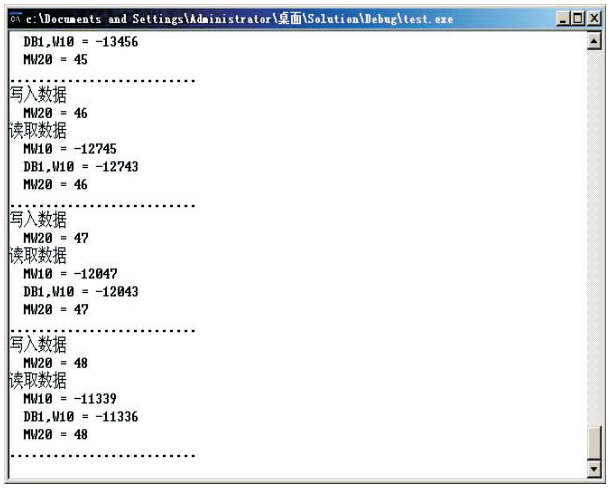

图 3 测试程序截图

6 结束语

通过研究西门子开源设备 Libnodave 驱动库,解析西门子系列 PLC 通信原理以及该开源库的编程结构,使得根据不同硬件或者平台需求借用源代码实现同西门子系列 PLC 通信成为可能。鉴于 Libnodave 驱动库的免费、开源、稳定、灵活等特点,取代 PRODAVE 来开发基于西门子 S7-300 与 S7-200SMART 的监控系统软件,从而降低成本,提高西门子相关产品的局限性。Libnodave 库是 C 语言编写的开源跨平台的库,但是仍然不方便在跨语言方面的移植,比如在 VB、C#等中调用它,需要把 Libnodave 封装成二进制文件,并提供接口函数。文中通过研究西门子开源设备 Libnodave 库,直接给出 send,recv 的字节码,非常方便跨语言、跨平台的移植,对于嵌入式应用环境中有限的运算资源是一个有利的支撑,其研究成果可以为工控行业各生产企业现场设备的升级改造与建设提供一定的借鉴,具有一定的参考价值。

参考文献:

[1] 任思成,王书鹤,亓克贵. 新一代工业过程控制软件接口标准-OPC 技术[J]. 仪器仪表学报,2002,23:265-267.

[2] 沈世斌. 基于 PLC 自由口通信的应用[J]. 仪表技术与传感器,2004(12):26-28.

[3] 周广颖,张金金,闫 隆. 基于 LIBNODAVE 的上位机与西门子 PLC 的通信[J]. 微计算机信息,2010,26(11-1):28-30.

[4] 赵 军,时良平,黄春阳. 基于 Prodave 技术的西门子 PLC 监控调试软件开发[J]. 自动化应用,2011(10):26-28.

[5] 张晓丽,马 俊,刘轶斐. 炼钢厂实时数据通信系统的研究与开发[J]. 仪器仪表学报,2005,26:553-556.

[6] 魏立新,冯 曦,王洪庆,等. LIBNODAVE 在 PLC 上位机监控软件中的运用[J]. 仪表技术与传感器,2014(7):82-84.

[7] DILIP P S,JAGTAP S R. Remote monitoring & controlling of real time industrial parameters with GSM & Ethernet[J]. International Journal of Electronics Communication & Instrumentation Engineering Research & Development,2013,3(2):1-10.

[8] SCHNEIER B. Cryptanalysis of Microsoft's point-to-point tunneling protocol (PPTP)[C]//Proceedings of the 5th ACM conference on computer and communications security. [s. l.]:ACM,1998:132-141.

[9] HU M,ZHAO Q,KURAMOTO M,et al. Research and implementation of layer two tunneling protocol (L2TP) on carrier network[C]//4th IEEE international conference on broadband network and multimedia technology. [s. l.]:IEEE,2011:80-83.

[10] 桂 芳,全书海. 网络控制系统传输时延分析与测试[J]. 计算机应用,2005,25(10):2264-2266.

[11] 张晓倩,宋晓茹,曹建建. 基于 CAN 总线的网络控制系统的仿真研究[J]. 计算机技术与发展,2016,26(7):192-195.

[12] 党安喜,裴少婧,尚耀东,等. 以太网时延仿真与性能分析[J]. 计算机工程与应用,2009,45(2):119-121.

[13] IANNONE F,BERTOCCHI A,BONCAGNI L,et al. Open source solutions in control and data acquisition systems:FTU case studies[J]. Fusion Engineering and Design,2010,85(3-4):321-324.

[14] 孙书欢,孔祥成,吴雪婷. 西门子 PLC 设备开源驱动库 Libnodave 的研究与改进[J]. 核电子学与探测技术,2013,33(7):847-851.