

OMRONCS1D 系列模块在船闸自动化系统中的应用

张超 江奎龙

徐州市伟思水务科技有限公司, 江苏 徐州 221006

[摘要] 文章论述了一种 VB.NET 实现和 OMRON CS1D 系列 PLC 之间的通讯实现。并成功的运用到安徽阜阳颖上船闸自动化控制系统中。主要实现上位机和 OMRON CS1D 系列 PLC 单元进行通讯以实现远程对闸阀门的开、关、停、急停、急停复位等的控制, 同时对该通讯协议进行了描述。以实例出发, 极具参考价值。该系统经实际运用, 效果良好。

[关键词] 工业以太网; FINS 协议; 闸阀门控制; VB.NET

DOI: 10.33142/hst.v3i5.2655

中图分类号: U641.335

文献标识码: A

Application of OMRONCS1D Series Modules in Shiplock Automation System

ZHANG Chao, JIANG Kuilong

Xuzhou Weiser Water Affair Science & Technology Co., Ltd., Xuzhou, Jiangsu, 221006, China

Abstract: This article discusses a communication between a VB.NET implementation and OMRON CS1D series PLC. And it was successfully applied to the automatic control system of Yingshang Shiplock in Fuyang, Anhui. It mainly realizes the communication between the upper computer and the OMRON CS1D series PLC unit to realize the remote control of opening, closing, stopping, emergency stop, emergency stop reset, etc. of the gate valve. At the same time, the communication protocol is described. Starting from examples, it is of great reference value. The system has been used in practice and the effect is good.

Keywords: Industrial Ethernet; FINS protocol; gate valve control; VB.NET

当前工业控制中, 由于现场条件复杂, 环境恶劣, 经常发生受控对象和上位机之间通讯延迟和不可靠, 造成控制紊乱, 极易造成事故。这就需要两者之间保证受控对象一方面要求传输速率的及时性和实时性, 另一方面需要传输性能的准确性和可靠性。工业以太网是基于 IEEE 802.3 (Ethernet) 的强大的区域和单元网络。利用工业以太网, SIMATIC NET 提供了一个无缝集成到新的多媒体世界的途径。

并涉及到众多开放性通讯标准协议, 特别是在工业控制中, 如现场总线 CAN-bus、DeviceNet、工业以太网 Ethernet 等, 并获了巨大发展。而 TCP/IP 网络通讯协议标准以其灵活性、可靠性、经济性和强大网络互连能力赢众多设备供应商青睐。而工业以太网从快速生成树冗余 (RSTP)、环网冗余 (RapidRingTM) 到主干冗余 (TrunkingTM), 优势和特点各自不同, 工作者可以根据不同的需求进行自主选择, 同时利用光纤作为载体, 可以避免以往通过以电缆为载体的 RS232 / RS485 通讯的诸多弊端。

船闸自动化是船闸实现完全数字化、现代化的主要部分, 其中运用了大量的计算机信息通讯技术、网络控制技术、数字化信息技术等, 笔者讨论了以 OMRON PLC 的 SC1D 系列的以太网模块 ENT11 为实例与上位机的通讯。上位机利用 VB.NET 的 winsock 规范下的 TCP / IP 协议实现了和 PLC 单元之间的 FINS TCP 通讯, 并提供了核心通信代码。

1 PLC 网络系统的结构体系与 FINS 协议

1.1 FINS 协议与 winsock 规范下的 TCP / IP 协议

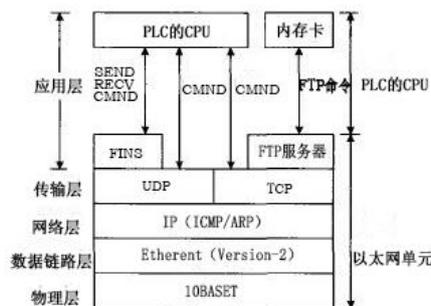


图1 FINS 协议与 winsock 规范下的 TCP / IP 协议关系图

FINS 通信协议是欧姆龙公司开发的用于工厂自动化控制网络的指令 / 响应系统, 使用 FINS 指令, 可实现网络间的无缝通信。网络对于用于信息层的 Ethernet, 用于控制器层的 Controller Link 网络和用于器件层的 DeviceNet 都是有效的。通过 FINS 指令, 上位机程序或 PLC 用户程序可以完成对另一个 PLC 数据区读或写操作, 程序得到极大的简化。同时以太网和 Link 网之间, 通过 FINS 指令使用的节点号, 为其提供了一致的寻址方式, 使得以太网单元通过自动转换、IP 地址表和复合地址表这三种转换方式中的任意一种, 能灵活的在 IP 地址和节点号之间转换。关系如图 1。

为了更可靠的通信, 将 FINS 信息封装在 UDP 数据区中利用 TCP / IP 协议进行传输。再进一步实现以太网和 Link 网之间的数据转发过程, 需要在 PLC 上安装以太网单元和 Link 通信单元。原理过程如下图所示。

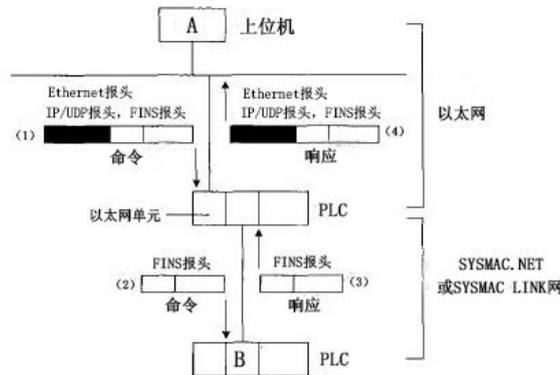


图 2 FINS 信息封装原理图

在上图中, 中继 PLC 的以太网单元接收到上位机程序发出带有 FINS 信息的网络帧包后, 进行数据帧包分解, 当抽取含有 FINS 信息后, 利用 Link 通信模块将 FINS 信息转发出去, 目的 PLC 获取数据并即时反馈响应数据, 该数据也采用 FINS 格式。以太网单元接收到中继 PLC 转发的数据帧包并进行封装后与上位机通信。作为以太网网段中一个节点的上位机程序, 需要遵循相同的地址转换规则并具有相应的节点号。

1.2 FINS 帧报文格式

在 PLC 之间采用 FINS 协议进行数据通信时, SEND、RECV 或 CMND 命令数据在通信模块内部自动实现封装和分解过程; 对于上位机程序添加 FINS 的报头和命令, Socket 控件自动完成 UDP 的报头生产的情况, 只发生在上位机和以太网模块之间的通信过程中。FINS 帧报文报头的格式见下图。

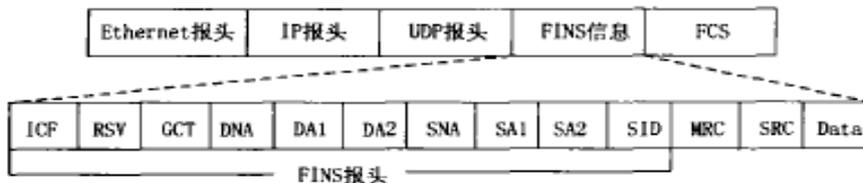


图 3 FINS 帧报文报头格式

图中名称详解如下:

表 1 FINS 帧报文说明表

序号	名称	作用
1	ICF	信息控制域, 主要用于标明命令和响应
2	RSV	系统保留
3	GCT	网关允许数目
4	DNA	目的网络号
5	DA1	目的节点号
6	DA2	目的节点单元, 用于标明 CPU 还是 CPU 总线单元
7	SNA	源网络号

(续表)

序号	名称	作用
8	SA1	源网络节点号, 对应上位机 IP 地址的主机部分
9	SA2	源节点单元, 对上位机而言应为 00
10	SID	服务和响应的标识, 可任意设置, 命令和响应有相同的数值
11	MRC	FINS 命令的主命令
12	SRC	FINS 命令的从命令
13	Data	数据区, 用于标明读数据时的地址范围或写数据时的地址和数据

1.3 通信过程中的以太网单元的设置

通信测试前先登记 I/O 表, 然后进行网络地址的设置 (含 IP 地址和子网掩码)、CPU 总线单元、地址转换方法、FINS 的 TCP 端口号。以太网通过旋转开关设定, 单元号为十六进制数, 数字范围不超过 15。同理, 节点号也是通过两个旋转开关设定, 节点号为两位十六进制数, 数字范围不超过 126。再使用编程设备对以太网单元进行设置。如果进行跨网通信, 为所有节点建立网络表是必须的, 而且每个网络表必须包含本地和中继两部分。本地网络表包含安装在 PLC 单元上的通信单元的单元号和网络号; 用于 FINS 通信时数据封装转发的中继网络表包括: 终点网络、中继网络和中继节点。

2 上位机软件通信程序的设计与实现

在系统通信的实现过程中, 笔者采用微软的 Socket 技术编程。为提高通信效率, 采用了异步 WinSock 即 VB.NET 中的 WinSock 控件的 TCP/IP 方式, 便于数据帧包的实时跟踪和准确性校对。上位软件和 PLC 模块交换数据放于 PLC 的内存区, FINS 报头的封装是编程的关键所在, 这决定了 PLC 数据读取的成败。下面结合项目案例进行详细阐述。

本例中 PLC IP 地址为内部网络地址 192. 168. 0. 51, 上位机计算机 IP 地址为 192. 168. 0. 10, 属于局域网内部通信模式。

上位机读取 PLC 的 D10001-D100026 共 26 个区的 I/O 状态字以及对 W142 区进行写命令字。加入并定义 Winsock 控件, 然后上位机软件对 PLC 进行通讯。

具体过程解释如下:

(1) 建立 PLC 和上位机之间的连接 Winsock.Connect。

(2) 上位机计算机对 PLC 进行通讯。首先进行“握手”确认。本过程也是 OMRON 公司的 FINS 协议和其他公司的协议的最大不同。目的是先将计算机的 IP 地址发送给 PLC, 等待 PLC 确认后并将 PLC 的地址返回给计算机, 返回数据正确即表明真正建立连接完毕。

命令:

```
4649 4E53 (FINS)
0000 000C (命令字节数)
0000 0000 (握手功能码)
0000 0000 (错误码)
0000 000A (计算机的 IP 地址或者叫节点号)
```

反馈信息, 包括被确认的计算机的 IP 地址或者叫节点号以及 PLC 的 IP 地址或节点号关键部分代码如下:

```
Private Sub ShakeToPLC()
```

```
Dim ab() As Byte 定义发送的字节函数
```

```
Dim address As Byte 定义 IP 地址的字节函数
```

```
'下面定义的是 PLC 的 IP 地址的最后一位数据比如 192.168.0.51 中的“51”。
```

```
address = &H33 ' PLC 的 IP 地址
```

```
ab(0) = &H46
```

```
ab(1) = &H49
```

```
ab(2) = &H4E
```

```
ab(3) = &H53  
ab(4) = &H0  
ab(5) = &H0  
ab(6) = &H0  
ab(7) = &HC  
ab(8) = &H0  
ab(9) = &H0  
ab(10) = &H0  
ab(11) = &H0  
ab(12) = &H0  
ab(13) = &H0  
ab(14) = &H0  
ab(15) = &H0  
ab(16) = &H0  
ab(17) = &H0  
ab(18) = &H0  
ab(19) = address '要连接的 PLC 的 IP 地址的最后一位  
Winsock.SendData ab
```

End Sub

连接建立后,开始读取 PLC 的 D10001-D100026 共 26 个区的 I/O 状态字。当发送命令且需要 PLC 响应时 ICF 域为 80H, RSV 域为 00H。GCT 因本例中 PLC 和上位机直接组成以太网, 故为 0。GCT 在本例中设置为 2。对于局域网 DNA 应为 0。本例中 PLC IP 地址为 192. 168. 0. 51, 对应的 DAI 为 33H。DA2 对于本地 PLC 为 0。SNA、SA1、SA2 与 PLC 地址相似, 本例中上位机 IP 地址为 192. 168. 0. 10, 上述 3 个字节均为 000A00H。SID 可任意设置, 本例设置为 EFH。内存单元的读取主命令 MRC 和从命令 SRC 分别为 01H 和 01H。

具体代码如下:

```
Private Sub ReadDataFromPLC()  
    Dim ab() As Byte  
    Dim address As Byte  
    Dim addressIPC As Byte  
    '下面定义的是本计算机的 IP 地址的最后一位数据比如 192.168.0.51 中的“51”。  
    address = &HA '表示计算机的 IP 地址  
    addressIPC = &H33 ' PLC 的 IP 地址  
    ab(0) = &H46  
    ab(1) = &H49  
    ab(2) = &H4E  
    ab(3) = &H53  
    ab(4) = &H0  
    ab(5) = &H0  
    ab(6) = &H0  
    ab(7) = &H1A  
    ab(8) = &H0  
    ab(9) = &H0  
    ab(10) = &H0  
    ab(11) = &H2  
    ab(12) = &H0  
    ab(13) = &H0
```

```

ab(14) = &H0
ab(15) = &H0
ab(16) = &H80
ab(17) = &H0
ab(18) = &H2
ab(19) = &H0
ab(20) = addressIPC '要连接的 PLC 的 IP 地址的最后一位
ab(21) = &H0
ab(22) = &H0
ab(23) = address(1) '本计算机的 IP 地址的最后一位
ab(24) = &H0
ab(25) = &HFF
ab(26) = &H1
ab(27) = &H1
ab(28) = &H82
'从 10001 开始到 10026 结束 共 26 个
ab(29) = &H27
ab(30) = &H11 'g_starADDRESS '开始要读取的第一位的 DM 区的数值数
ab(31) = &H0
ab(32) = &H0
ab(33) = &H1A 'g_length '需要读取的 DM 区的个数
Winsock.SendData ab

```

End Sub

写 PLC 的 W142 区的状态字。当发送命令且需要 PLC 响应时 ICF 域为 80H, RSV 域为 00H。GCT 因本例中 PLC 和上位机直接组成以太网, 故为 0。GCT 在本例中设置为 2。对于局域网 DNA 应为 0。本例中 PLC IP 地址为 192. 168. 0. 51, 对应的 DAI 为 33H。DA2 对于本地 PLC 为 0。SNA、SA1、SA2 与 PLC 地址相似, 本例中上位机 IP 地址为 192. 168. 0. 10, 上述 3 个字节均为 000A00H。SID 可任意设置, 本例设置为 EFH。具体代码如下:

```

Public Sub SendDateToPLC()
Dim ab() As Byte
Dim address As Byte
Dim addressIPC As Byte
'下面定义的是本计算机的 IP 地址的最后一位数据比如 192. 168. 0. 10 中的“10”。
address = &HA '表示中控室的 IP 地址的最后一位数字
'下面定义的是 PLC 的 IP 地址的最后一位数据比如 192. 168. 0. 51 中的“51”。
addressIPC = &H33 '表示被连接的 PLC 的 IP 地址的最后一位数字
ab(0) = &H46
ab(1) = &H49
ab(2) = &H4E
ab(3) = &H53
ab(4) = &H0
ab(5) = &H0
ab(6) = &H0
ab(7) = &H1C
ab(8) = &H0
ab(9) = &H0
ab(10) = &H0

```

```
ab(11) = &H2  
ab(12) = &H0  
ab(13) = &H0  
ab(14) = &H0  
ab(15) = &H0  
ab(16) = &H80  
ab(17) = &H0  
ab(18) = &H2  
ab(19) = &H0  
ab(20) = addressIPC '要连接的 PLC 的 IP 地址的最后一位  
ab(21) = &H0  
ab(22) = &H0  
ab(23) = address '本计算机的 IP 地址的最后一位  
ab(24) = &HB1  
ab(25) = &H0  
ab(26) = &H1  
ab(27) = &H2  
ab(28) = &HB1  
ab(29) = &H0  
ab(30) = &H8E '开始要写的第一位的 M 区的地址数值  
ab(31) = &H0  
ab(32) = &H0  
ab(33) = &H1 '需要写的 M 区的个数的数据值  
ab(34) = &H40 '需要写的数值的高位  
ab(35) = &H0 '需要写的数值的低位
```

```
Winsock.SendData ab  
End sub
```

3 结论

经过现场运行及测试,通信效果显著,确保了数据的实时性和准确性。本文论述的方法投资少、安全可靠,非常适合在工控领域进行推广。

运用 VB.NET 的 WinSock 与 OMRON PLC 进行以太网通信,由于 TCP/IP 协议被广泛运用于以太网单元,设计变得简单了,对 FINS 报头封装和协议确认是根本也是难点,其他过程与上位机程序之间的 TCP/IP 程序设计完全一致。用 VB.NET 设计的程序具有实时性好、速度快、开发周期短、上手快、可靠性高、运行稳定、安全可靠等优点,非常适合在工控领域进行推广运用。自动化控制系统采用了以太网通信技术后,与信息化、数字化等进行有机地结合,充分的体现了工业自动化优点,简化了系统设计,提高了系统的安全性和准确性。

此方法已成功应用于安徽阜阳颍上船闸的自动化控制工程的项目中,运行 2 年以来,稳定可靠的,客户评价很高。

[参考文献]

- [1]钱炜.施耐德 PLC 在九曲河枢纽船闸自动化控制中的应用[J].黑龙江科学,2020,11(02):52-53.
 - [2]严励.二堡船闸自动化控制系统的设计与应用[J].江苏水利,2020(01):62-65.
 - [3]蔡振华.大型水电厂保护整定计算及其软件的研究[D].武汉:华中科技大学,2008.
 - [4]陈正宏.邦朗水电站微机继电保护系统的调试及运行[J].云南水力发电,2006(03):80-82.
- 作者简介:张超(1978.5-),男,江苏邳州人,兰州理工大学,计算机通信,徐州市伟思水务科技有限公司,工程部主任,从事水文、水利、水电自动化测控相关领域研究,高级工程师。