

# 和利时系列 PLC 与西门子 S7- 300PLC 的以太网通信研究

方彦军

(南京师范大学控制科学与工程系, 210042, 南京)

[摘要] 通过对和利时公司 CPU24x PLC 系统和西门子公司 S7- 300/400 PLC 系统内部通讯处理器及通讯协议的研究, 介绍了一种采用以太网实现现场总线控制系统通信的方法, 并成功地实现了和利时公司 CPU24x PLC 系统和西门子公司 S7- 300/400 PLC 系统的相互通信。

[关键词] 现场总线系统(FCS), 以太网通信, 过程控制

[中图分类号]TN915, [文献标识码]B, [文章编号]1672- 1292- (2003)01- 0001- 04

当今国际上有影响的现场总线标准很多, 单是 2000 年 IEC 组织制定的国际现场总线标准就八九种之多. 众多的现场总线标准, 给控制系统的集成带来不便, 使得各厂商生产的现场总线产品难以集成在一起, 实现互可操作. 在现场总线标准难以统一的情况下, 以太网在工业自动化和过程控制领域获得了迅速增长, 现在不少厂商都为其生产的 PLC 及其远程 I/O 提供与以太网相连的接口和功能, 提供用以太网与其基于 PC 机的控制系统相连接. 本文对采用以太网来实现西门子公司 S7 系列的 PLC 系统和北京和利时公司的 CPU24x 系列 PLC 系统的相互通信进行了探讨.

## 1 系统结构

系统结构如图 1 所示. 西门子 S7300- PLC 系统与和利时 CPU24x PLC 系统的相互通信采用通信处理器 CP 来实现, S7- 300 PLC 为其系统的以太网通信提供有 CP343- 1 以太网通信处理器, 而和利时公司的 CPU24x PLC 系统的通信处理器 CP 内置于 CPU 中, 采用双端口 RAM 直接连接到 CPU24x, 双端口 RAM 被分成 4 个相等的称为页面帧的段. 这 4 个页面帧作为 CP 与 CPU

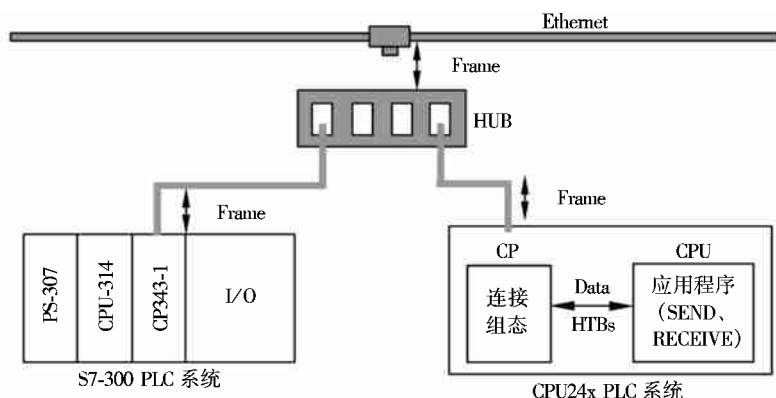


图 1 系统结构图

的应用程序连接的接口, 每个使用的接口都必须在启动及再启动程序中初始化. 作业请求由接口号和作业号来定义的, 并经数据管理功能被寄送至通信处理器. 每个通信处理器一次可以管理多达 64 个作业, 包括多达 32 个连接点, 数据的交换采用处理功能块( SEND 和 RECEIVE 等) 实现.

## 2 通信原理与实现方法

当前在工业应用领域采用以太网通信较普遍的协议格式有 IEEE802. 3 和 TCP/ IP 协议, 西门子 S7-

收稿日期: 2003- 02- 20.

作者简介: 方彦军, 1957- , 南京师范大学控制科学与工程系教授, 主要从事检测技术与过程控制方面的教学与研究工作.

300PLC 和和利时 CPU24x PLC 都提供了 H1 工业以太网和 TCP/IP 两种实现 PLC 间通信的解决方案, 这为我们实现它们间的通信提供方便。

Ethernet IEEE802.3 支持自由的总线访问原理, 在网络上的每个站当它要与其它站通信时, 可独立地访问网络, 这些访问采用 CSMA/CD(多路载波冲突/访问监测) 方案来协调。TCP/IP 应用于开放式的网络连接, 实现不同厂商间的数据通信。

## 2.1 H1- 工业以太网通信

H1- 工业以太网, 是一种基于以太网标准 IEEE 802.3 的协议, 用于可编程控制器间的高速、大量数据交换。其站间的数据交换采用“H1- 帧”, 传输连接为逻辑连接, 在不同的站间使用传输服务访问点(TSAP)来完成传输服务, 如图2所示。传输连接基于寻址信息, 寻址信息提供了两个服务访问点间的一个确切的路径说明。传输连接使用了下列两个参数: MAC 地址和 TSAP(传输服务访问点)。MAC 地址, 即以太网节点地址, 定义了一个站的访问应用。TSAP 标识了传输服务的访问通道。

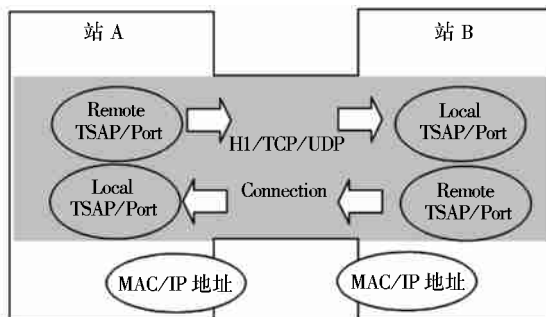


图2 发送或接收连接示意图

通信时, CPU 24x 系统的 CP 准备了一个数据缓冲区, 并使用背景通信功能 SEND- ALL 把数据传输到数据缓冲区, 然后 CP 创建一个 H1 帧, 并传输这个帧到对方站。当对方站接收到这个 H1 帧后发回一个确认报文给 CP, 然后对方站使用背景通信功能 RECEIVE- ALL 传输发送作业状态到各自的指示状态字中, 这样保证了总线的正常通讯。如图3所示。

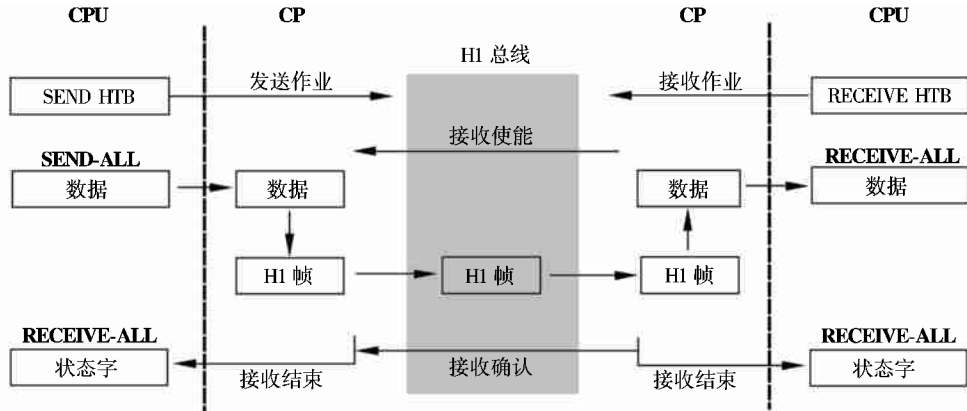


图3 H1 通信原理图

S7 PLC 以太网通信数据通信的触发由用户程序来实现, S7 提供有到用户接口的实现功能 SEND 和 RECEIVE, 其原理与和利时的类似。通信连接的组态在网络连接的组态中完成, CP 的任务是: (1) 从 Ethernet 接收数据, 并传输到 CPU 的用户数据区; (2) 从 CPU 的用户数据接收数据, 并发送到 Ethernet 上。

## 2.2 TCP/IP 通信

用于 PLC 间通信的 CP 应用层由应用程序使用标准的处理块来定义, 这些应用程序使用传输层的 TCP 或 UDP 协议交换数据。TCP 在网络上为数据提供安全的传输, 传输服务使用需确认的连接服务, 数据的传输需应答, 检测和更正通信错误, 因此 TCP 连接是安全的连接。UDP 提供快速的通信连接, 数据的传输不需要应答, 它既不关心数据包的丢失, 也不检查分组序列, 是一种相对不太安全的连接。

TCP 和 UDP 通信使用其下一层(互连网层)的 IP 协议实现通信。IP 协议的主要目的是提供到数据分

组的寻址, 并把分组数据传送到网络的目的地. 根据不同的网络用户定义的数据分组的大小不一致, IP 协议把数据分成小的数据分组, 以协调不同的网络间的通信. IP 对分组排序, 给每一个分组分配一个分组号, 便于接收方对数据分组的收集.

在和利时的 PLC 系统和 S7- 300/ 400PLC 系统中, 其 TCP/ IP 通信连接也使用了两个参数: IP 地址和 Port( 端口), 其使用及连接方法与 H1 以太网类似, 本地站和远程站的本地 Port 和远程 Port 交叉对应, 见图 2. PLC 应用要求定义数据传输的大小, 不允许使用缺省值, 并可指定通信作业优先级, 带优先级 1 的最大接收和发送数据量在初始化中定义. 通信使用接收和发送缓冲区, 它们位于 TCP/ IP 协议栈的全局缓冲区里.

### 3 通信实现与编程

无论是 S7- 300PLC 还是和利时 PLC, 通信编程包括两部分: (1) CP 连接组态; (2) PLC 通信编程. S7- 300PLC 的 CP 组态及 PLC 通信编程均使用软件 STEP7, 而和利时的 PLC 系统 CP 连接组态使用 WinNCS 配置软件, PLC 编程使用 S5. 下面以和利时的 CPU 24x PLC 与西门子公司 S7- 300PLC 通讯为例介绍其编程方法和有关问题.

#### 3.1 用于和利时 CPU 24x 的程序编程

和利时 PLC 的以太网通信实现, 首先应建立 CP 的以太网通信连接. CP 的通信连接有 H1- 工业以太网和 TCP/ IP 连接两种, 通信的实现靠相应的通信作业来启动和完成. 因此, 在建立 CP 的各个相应通信连接时, 可以为每个连接指定作业号. 系统在运行时, 指定了作业号的通信使用指定的通信作业完成指定的数据传输, 没指定作业号的将使用 Direct- All 通信作业来完成. 本地站和远程站的服务访问点 TSAP 应交叉, 本地站的发送服务访问点在远程站中对应的是接收作业的远程服务访问点, 其它的类推. 系统运行时, CP 根据 MAC 地址、TSAP 和组态建立的连接关系建立通信连接, 通信连接建立后, 才启动数据交换.

为了使 PLC 能够处理连接请求, 需在 PLC 中启动一个通信应用程序, 应用程序中使用了通信处理块. CP 在投入使用之前, 必须初始化. 初始化的内容包括与每个连接有关的局部和整体信息以及一般参数. 功能块 FB249 初始化页面编制模块上的接口. 直到 SYNCHRON 执行之后, 通信处理功能块才能正确地处理, 数据的传输和接收使用 SEND 和 RECEIVE 功能实现. SEND 和 RECEIVE 有两种作业模式: Direct 和 All 模式, Direct 模式为指定的作业传送数据, All 模式能为任何作业传送数据.

当 PLC 上电或重新启动时, CPU 和 CP 执行各自的引导程序, CPU 检测安装的模块并启动应用程序, 然后调用初始化程序初始化 CP. 程序中设计了一个初始化检查程序, 若出现初始化错误, 重置相应的初始化出错代码, 并停止 PLC 的运行, 指示系统启动失败. PLC 启动需要大约 15 s, 大约 15 s 后, CP 等待从 CPU 来的初始化请求直到初始化完成. CPU 的引导时间( 包括 CP 的引导时间) 大约需要 18 s, 在此定义了一个 20 s 的启动延时定时器. 为了保证系统的正确引导和初始化, 以及在 CPU 由 STOP 切换到 RUN 模式或由 RUN 切换到 STOP 后的重新执行冷/ 热启动时, 防止通信故障, 须在引导组织块、冷启动和热启动组织块 OB20、OB21 和 OB22 里重新调用 CP 初始化程序, 重新建立连接. 循环运行的程序在 OB1 中调用, 在此数据的发送作业定为每隔 100 ms 发送一次. 限于篇幅, 在此仅列出 PLC 中的通信程序结构图( 如图 4 所示). 图中用户程序 FB1 为接收程序, FB2 为发送程序, FB122 为初始化程序, 阴影部分调用了系统提供的标准功能块.

#### 3.2 用于西门子 S7- 300 PLC 的应用程序编程

S7- 300PLC 以太网通信数据接口功能的实现使用 SEND、RECEIVE 接口功能. 在 S7 用户程序里, CPU 和 CP 间的数据交换使用功能 FC5( AG\_ SEND) 和 FC6( AG\_ RECE) 来完成, 对于传输的数据每帧大于 240 字节的使用 FC50( AG\_ LSEND) 和 FC60( AG\_ LRECE) 来完成. S7- 300PLC 与和利时 PLC 以太

网通信用户程序的 CPU 循环顺序如图4所示。

#### 4 结束语

利用以太网来实现西门子 S7 与和利时 PLC 系统的相互通信,其通信方法较多,既可使用工业以太网 H1 连接,也可以使用 TCP 连接,对通信安全性较低、数据量大的应用场合还可以使用 UDP 连接。每个 H1 或 TCP 连接的数据传输量可以从 16 字节直到 8192 字节,而 UDP 最大可以达到 2048 字节,因此相当灵活,可以满足各种控制系统的需要。同时编程的工作量也不大,大量的通信实现功能都已集成在功能块和 CP 中,用户只需完成简单的组态和编制简单的通信程序即可实现相互间的通信。

在现场总线难以统一的情况,利用以太网来实现现场总线控制系统的通信互连,也是一种有效解决的方案,尤其是在车间级的通信中,与现场总线相比,采用以太网的解决方案,具有很大的优越性。

#### [参考文献]

- [1] 西门子公司. SIMATIC NET MANNAL: NCM S7 FOR Industrial Ethernet[Z]. 1999.
- [2] 西门子公司. 自动化技术与 SIMATIC S5- 115U 之 STEP 5 语言和功能块编程手册[Z]. 1992.
- [3] 北京和利时系统工程股份有限公司. FOPLCTM 硬件手册[Z]. 2000.

## Research on Communication Between Hollysys' PLC and Siemens S7- 300 PLC Based on Ethernet

Fang Yanjun

(Department of Control Science and Engineering, Nanjing Normal University, 210042, Nanjing, PRC)

**Abstract:** In this paper a kind of method that has implemented the communication of fieldbus control system with Ethernet is introduced. And it has formed the interconnected communication successfully between Hollysys' PLC and SIEMENS' S7- 300PLC.

**Key words:** fieldbus control system, Ethernet communication, process control

[责任编辑:刘健]

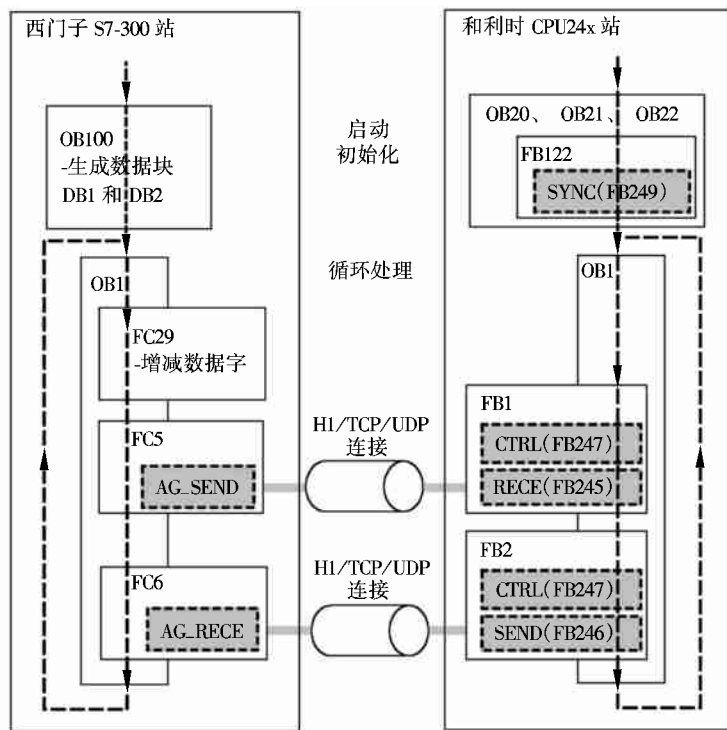


图4 程序结构及 CPU 的循环顺序