

以太网技术在 SSRF 设备控制中的应用

周大勇 刘德康 刘亚娟 沈立人

(中国科学院上海应用物理研究所 嘉定园区 上海 201800)

摘要 随着工控技术和以太网技术的发展,可编程逻辑控制器(Programmable Logic Controller, PLC)基本都具备了以太网连接功能。上海光源(Shanghai Synchrotron Radiation Facility, SSRF)大量采用了 PLC 作为设备控制器。应用以太网技术在上海光源设备控制中,通过以太网技术可以使设备控制器直接连接至控制网络。采用以太网技术简化了控制系统结构,同时也便于系统维护和升级。

关键词 以太网, EPICS, 可编程逻辑控制器, 设备控制

中图分类号 TL503.6

DOI: 10.11889/j.0253-3219.2014.hjs.37.120101

上海光源 (Shanghai Synchrotron Radiation Facility, SSRF) 控制系统软件基础平台使用 EPICS^[1-2] 系统, EPICS 即“实验物理及工业控制系统”(Experimental Physics and Industrial Control System), 是 20 世纪 90 年代初由美国洛斯阿拉莫斯国家实验室(LANL)和阿贡国家实验室(ANL)等联合开发的大型控制软件系统。发展至今, 已被全世界数十个大型科学研究工程项目所采用, 涉及粒子加速器和探测器系统、同步辐射装置、大型天文望远镜以及飞机工业等领域。EPICS 经过多年准备和实践, 源码现已公开, 已被选作开发 SSRF 控制系统的基本软件平台。在此基础软件平台上加以扩展, 开发一组 EPICS 增强软件系统, 用以组合整个 SSRF 控制系统软件以及与其它系统的互连。EPICS 控制系统结构如图 1 所示。

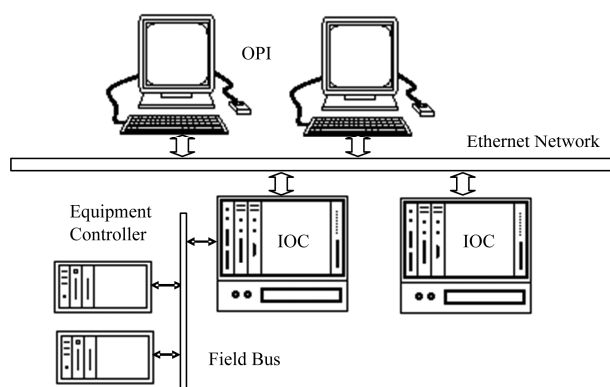


图 1 EPICS 控制系统结构
Fig.1 EPICS control system architecture.

1 控制系统的组成

EPICS 基本由三部分组成: (1) 操作员接口层 (Operator Interface, OPI), 位于控制系统的顶层, 具有访问整个控制系统的能力, 同时兼具与外部系统的通信联结。通过人机交互界面监控内部系统的运行, 实现控制参数设置/回读、报警处理、数据存档等功能。(2) 输入输出控制器 (Input/Output Controller, IOC), 通过现场总线或直接 I/O 方式控制前端设备控制器, 实现数据的实时采集、控制量的设置、响应监控层或其他 IOC 的请求、处理来自设备控制层的外部事件等; 局域网(Local Area Network, LAN), 即以太网, EPICS 通过 Channel Access 协议实现 IOC 和 OPI 的通讯。(3) 设备控制器(Device Controller), 主要进行现场设备的控制, 设备控制器一般通过现场总线或以太网与 IOC 连接。

上海光源控制系统采用 EPICS 结构, 控制系统底层设备控制器大部分为可编程逻辑控制器 (Programmable Logic Controller, PLC)。随着以太网技术^[3]的发展, 一些 PLC 厂商也开发了以太网模块, 用于现场信息的采集和控制。

以太网连接技术的最大优势之一, 就是无论是诊断数据还是控制信号, 都能在网络内部和不同网络之间进行传送。在实际现场工程中还能节省大量的劳动力和材料成本, 因为它不需要安装过多现场 I/O 模块机架, 也节省了遍布各处的通信线缆。以太网用单一电缆取代了众多的接线。大量设备都可以通过这条电缆联网, 而且一旦建立了以太网连接, 设备的功能测试就成为一件非常简单的事情, 用户只需要从任何一台联网的 PC 上直接“Ping”一下希望测试的设备即可。

第一作者: 周大勇, 男, 1978 年出生, 2010 年于中国科学院上海应用物理研究所获博士学位

收稿日期: 2013-10-09, 修回日期: 2014-03-01

SSRF 控制系统是建立在以太网之上的, 所有的设备控制、数据获取、数据监测都要通过以太网来进行。目前在上海光源所使用的绝大部分 PLC 设备控制器都具有以太网连接功能, 主要应用如下:

(1) 横河 FA-M3 系列, 以太网连接, 驱动程序为 EPICS Device/Driver Support for Network-based Intelligent Controllers, 应用在直线电子枪控制系统、上海光源机器保护系统、增强器电源连锁控制系统。

(2) 西门子 S7-300 系列, 以太网连接, 驱动程序为 s7plc EPICS driver, 应用在调制器控制系统。

(3) 欧姆龙 CPM2A 系列, RS232 转以太网连接, 驱动程序为 SSRF 控制组自行开发, 应用在储存环公共直流源控制系统。

所有设备控制都可以通过以太网连接至中央控制系统, 并且在 EPICS 系统下都有相应的设备驱动程序可以使用。因此 SSRF 在设备控制中基本上采用以太网技术为基础的通讯方式。

2 以太网及工业以太网

以太网是当今现有局域网采用的最通用的通信协议标准。该标准定义了 LAN 中采用的电缆类型和信号处理方法。以太网在互联设备之间以 10–100 Mbps 的速率传送信息包, 双绞线电缆型号为 10 Base T。以太网由于其低成本、高可靠性以及 10 Mbps 的速率而成为应用最为广泛的以太网技术。许多制造供应商提供的产品都能采用通用的软件协议进行通信, 开放性好。

以太网具有的优点: (1) 具有相当高的数据传输速率, 能提供足够的带宽; (2) 由于具有相同的通信协议, Ethernet 和 TCP/IP 很容易集成到信息技术(IT)世界; (3) 能在同一总线上运行不同的传输协议, 从而能建立控制系统的公共网络平台或基础构架; (4) 在整个网络中, 运用了交互式 and 开放的数据存取技术; (5) 沿用多年, 已为众多的技术人员所熟悉, 市场上能提供广泛的设置、维护和诊断工具, 成为事实上的统一标准; (6) 允许使用不同的物理介质和构成不同的拓扑结构。

近些年来, 随着网络技术的发展, 以太网进入了控制领域, 形成了新型的以太网控制网络技术。这主要是由于控制系统向分布化、智能化控制方面发展, 开放的、透明的通讯协议是必然的要求。目前通信速率为 10 M、100 M 的快速以太网广泛应用, 千兆以太网技术也已成熟, 10 G 以太网正在研究, 其速率比目前的现场总线快很多。

工业以太网的优点: (1) 基于 TCP/IP 的以太网采用国际主流标准, 协议开放、完善不同厂商设备, 容易互连, 具有互操作性; (2) 可实现远程访问, 远程诊断; (3) 不同的传输介质可以灵活组合, 如同轴电缆、双绞线、光纤等; (4) 网络速度快, 可达千兆甚至更快; (5) 支持冗余连接配置, 数据可达性强, 数据有多条通路抵达目的地; (6) 系统容易几乎无限制, 不会因系统增大而出现不可预料的故障, 有成熟可靠的系统安全体系; (7) 可降低投资成本; (8) 现场设备信息可以通过以太网送到主控室, 操作员可以在主控室直接使用查看现场运行情况, 现场设备也可以通过网络获得控制信息。

上海光源设备控制采用的设备控制器(主要是 PLC)都带有以太网接口, 这些都标志着工业以太网已经成为真正开放互连的控制网络的发展方向。工业以太网在传统以太网技术的基础上, 通过采用双工通信、交换机、信息优先级等技术, 使有实时要求站点的通信通过交换机实现透明的转发, 不存在信道共享引起的竞争问题, 还可以方便地实现优先级排队机制, 使紧急信息的传达到最快。在以太网的协议中加入实时功能, 采用高速背板交换或微处理器交换, 响应时间是确定的, 足以满足大多数场合的实时控制要求。

具有以太网连接的 PLC 可以直接连接至控制网络; 不具有以太网连接功能的 PLC, 也可以通过协议转换, 连接至控制网络。采用以太网技术的设备控制器的控制系统结构, 如图 2 所示。

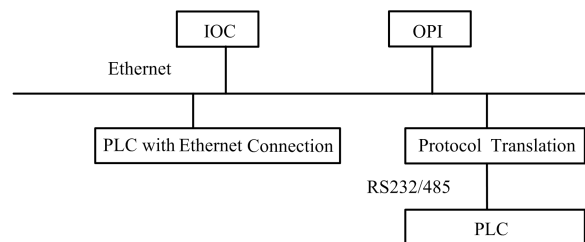


图2 设备控制器网络连接
Fig.2 Device controller network configuration.

3 基于以太网技术的设备控制

目前 SSRF 中使用的 PLC 主要包括: YOKOGAWA 公司的 FA-M3R^[4] 系列 PLC, SIEMENS 公司的 S7-300 系列 PLC, OMRON 公司的 CPM2A 系列 PLC。

3.1 YOKOGAWA FA-M3R 系列 PLC

SSRF 中的机器保护系统、磁铁电源连锁保护系统、真空阀门控制系统和电子枪控制系统采用了 YOKOGAWA 公司的 FA-M3 系列 PLC。通讯过程如图 3 所示。

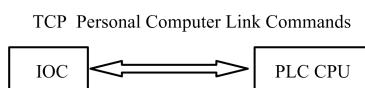


图 3 FA-M3 PLC 与 IOC 通讯示意

Fig.3 Communication between FA-M3 PLC and IOC.

在 EPICS 环境下已经有了一系列完整 Device/Driver 支持模块，这些模块包括：通用驱动模块、通用设备支持模块和对于所支持的设备所用到的特定的设备模块(Device-specific module)^[5]。其软件结构如图 4 所示。

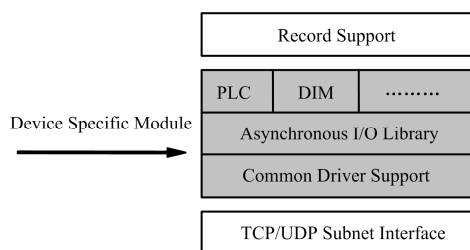


图 4 FA-M3 设备驱动结构

Fig.4 Architecture of FA-M3 PLC driver's software.

3.1.1 设备特定模块(Device-specific module)

设备特定模块的主要功能是建立一个能被发送到远端设备，解析响应消息，并能通过解析数据库记录的 link field 来获得地址信息的命令(Commands)，每个设备特定模块必须具备如下 3 个功能：

(1) 连接域解析器(Link Field Parser)：在初始化 IOC 时，通过对实时数据库记录中的 Link Field 的解析来得到特定通道(Channel)的地址信息。

(2) 命令建构器(Command Constructor)：建立一个命令，发送给远端指定地址的设备；如果操作是写(write)的话，能从 IOC 记录缓存(Record Buffer)中传送数据命令消息(Command Message)。

(3) 响应解析器(Response Parser)：在响应消息(Response Message)到达时解析其内容，在操作为读(read)时将包含在消息中的数据传送到 IOC 记录缓存(Record Buffer)。

3.1.2 异步 I/O 库模块(Asynchronous I/O Library)

异步 I/O 库模块通过一系列应用程序编程接口(Application Programming Interface, API)来支持上层的设备特定模块，在这些 API 中包含了 EPICS 中异步设备支持的技术细节。异步 I/O 库模块有两个主要函数：

(1) 通用的初始化函数。初始化函数启动连接域解析器来确定远端设备和要读/写的地址。初始化函数也初始化一种数据结构，该结构需要在调用记录结束时执行回叫(Call back)。

(2) 通用的读/写函数。读/写函数在一次异步 I/O 中被调用 2 次，分别是初始化和 I/O 处理完成时。初始化时，它调用命令建构器来形成一条消息(message)，并把 I/O 请求放在 MPF (Message Passing Facility)队列中，然后通知该次事件(event)的 MPF。在 I/O 处理完成时，读/写函数什么也不做，因为响应解析器在函数调用之前已经传送好数据。

以上两个函数可以成为 EPICS 中 DEST (Device Support Entry Table)中特定的记录/设备支持模块的成员函数。

3.1.3 通用驱动支持(Common Driver Support)

通用驱动支持会建立一个 MPF，因为每个通讯服务器(Communication server)运行于不同的远端设备之上（每个远端设备称为 server）。所有对于远端设备的 I/O 请求都会在 MPF 的队列中排序。一个 MPF 包含以下线程：

(1) 发送任务(Send Task)：从 I/O 队列中获得 I/O 请求，调用命令建构器将信息字节放到缓存中，并将其发送给远端设备，然后阻塞(block)，直到 Receive Task 得到一个响应消息。

(2) 收取任务(Receive Task)：等待响应消息到来，消息到达后调用响应解析器来解析消息，然后使被阻塞(blocked)的 Send Task 线程转到下一个循环中。最终生成一个回叫(Call Back)请求来完成此次异步 I/O。

(3) 超时处理(Timeout Handler)：当 watch-dog 中的计时器到达计时时间时，取消此次 I/O 处理。同时生成一个回叫信息，ERROR。

YOKOGAWA FA-M3 系列 PLC 在其 CPU 内存中对于安装于系统的模块都设置了相应的存储区域，通过 PLC 的以太网模块，应用其电脑通讯连接命令(Personal Computer Link Command)，IOC 可以直接访问其 CPU 相应的存储区域，实现 IOC 对 PLC 的控制。电脑通讯连接命令和响应格式如图 5 所示。

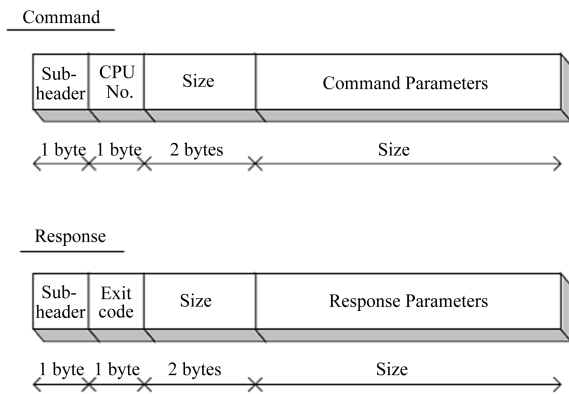


图 5 数据连接命令数据帧

Fig.5 Data frame of personal computer link command.

Sub header 大小为 1 个字节, 第 1 位是命令/响应(Command/Response)标志位: 0 表示命令, 1 表示响应; 剩余 7 位为命令/响应类型标志, 标识请求传送的命令类型。CPU number 大小为 1 个字节, 可以设置值为 1-4, 表示要访问的 PLC CPU 号码 (一个系统内最多可安装 4 个 CPU)。Exit code 大小为 1 个字节, 表示命令执行结果, exit code 为 0 表示正常, 不为 0 表示执行命令时有错误发生, 不同的错误响应具有不同的值。Size 大小为 2 个字节表示命令或响应的字节大小。Command parameter 表示设备名称、访问的数量或其他信息, 实际内容基于发送的命令类型。Response parameter 包括命令的响应, 其大小和内容基于发送命令的类型。

3.2 SIEMENS S7 系列 PLC

SSRF 在调制器控制系统和增强器注入引出系统中使用 SIEMENS S7^[6]系列 PLC。EPICS 与西门子系列 PLC 采用内存数据交换的方式进行通讯: 即在 IOC 和 PLC 的内存区中各自使用一块内存用于数据通讯。通讯过程如图 6 所示。

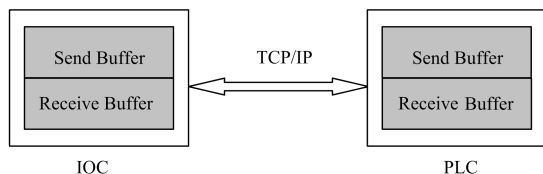


图 6 西门子 PLC 与 IOC 通讯示意

Fig.6 Communication between SIEMENS PLC and IOC.

通讯过程如下: 首先 PLC 与 IOC 通过 Ethernet 建立 TCP/IP 连接; 然后 PLC 将其内存区中 Send Buffer 的数据通过其以太网模块定时向 IOC 的 Receive Buffer 发送, PLC 的 Receiver Buffer 则定时的接受来自于 IOC Send Buffer 的数据。IOC 中运行的驱动软件在内存设置相应的 Send Buffer 和

Receive Buffer, 定时地将 Send Buffer 的数据一并发送到 PLC, 并将接收的数据放置于 Receive Buffer。IOC 和 PLC 中的 Send Buffer 和 Receive Buffer 可以根据需求来设定地址和大小。

采用该种通信方式需事先设定好 IOC 和 PLC 两端的通讯数据存储区域, 上位 IOC 只能处理 PLC 发送缓存区定时发送过来的数据, 并不能直接访问和控制 PLC 的内存; IOC 也只能接收 PLC 以太网模块定时发送过来的数据, 不能实时访问 PLC 的 CPU 内存。同样, PLC 在接收到 IOC 发送过来的数据之后, 还要根据事先约定的数据格式进行判断, 然后再进行下一步的控制处理。

3.3 OMRON CPM2A 系列 PLC

储存环公共直流电源底层设备控制采用 OMRON CPM2A^[7]系列 PLC, 与 OMRON CPM2A 系列 PLC 进行通讯要采用其 Host Link 协议。Host Link 通信是一种对话型的通信协议, 这种协议下, PLC 对由主计算机发送来的命令发送应答信号。在 PLC 里无需通信程序。要实现与 CPM2A 的通讯, 需要通过 RS232 口向其发送 Host Link 格式的命令。

该种型号 PLC 属于微型 PLC^[8-9], 并没有相应的以太网接口模块, 只能通过其 CPU 上的 RS232 串口与上位 IOC 进行通讯, 以此实现对将 PLC 所控制的开关量的回读、远程控制。EPICS 中所用的通讯协议为 Channel Access, 该协议基于 Ethernet 技术, 要实现上述需求, 需将串口信号转成 Ethernet 信号。MOXA 公司生产的串口服务器 NPort5610 具有串口到以太网的双向数据传输能力。因此可以通过 NPort5610 发送控制命令到 PLC 的串口。控制组根据需求已于 EPICS 下开发通过串口服务器 NPort5610 将 RS232 串口信号传送到 Ethernet 上的驱动。具体实施方案如图 7 所示。

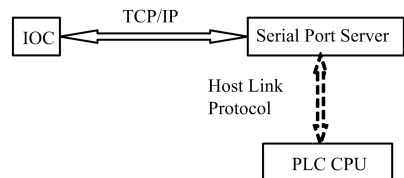


图 7 欧姆龙 CPM2A 与 IOC 通讯方式

Fig.7 Communication between OMRON CPM2A PLC and IOC.

4 结语

上海光源控制系统采用 EPICS 结构, 控制系统底层设备控制器大部分为 PLC。对于不同的设备控制器, 不同厂家采取的设备通讯模式不尽相同, 一

般主要通过现场总线进行。现场总线类型较多，如 DeviceNet、Foundation Field bus、Profibus 等。各种现场总线通讯标准的不一致性，不仅增加了系统开发的难度，而且不同种类的现场总线的使用，也加大了对于整个控制系统网络管理的难度。

SSRF 控制系统的 PLC 设备控制器使用以太网连接技术，不但简化了控制系统结构，而且通讯介质统一为以太网，大大减少了通讯线缆的连接，方便了系统维护和扩展；同时所有对于设备控制器的程序维护更新也都可以通过以太网连接来实现。

参考文献

- 1 Kraimer M R. EPICS: Input/Output Controller application developer's guide (Release 3.14.6)[DB/OL]. <http://www.aps.anl.gov/epics>, 2004
- 2 Hill J O. EPICS R3.14 channel access reference manual (Release 3.12)[DB/OL]. <http://www.aps.anl.gov/epics>, 1995
- 3 张炯. UNIX 网络编程实用技术与实例分析[M]. 北京: 清华大学出版社, 2002
ZHANG Jiong. The UNIX network programming techniques and examples of analysis[M]. Beijing: Tsinghua University Press, 2002
- 4 横河 PLC 编程手册[DB/OL]. <http://www.yokogawa.com/itc/menu/itc-Download-en.htm>, 2010
Henghe PLC programming manual[DB/OL]. <http://www.yokogawa.com/itc/menu/itc-Download-en.htm>, 2010
- 5 Odagiri J. EPICS device/driver support for network-based intelligent controllers[C]. Proceedings of ICALEPCS 2003, Gyeongju, Korea, 2003
- 6 EPICS using SLS S7PLC driver PLC configurations[DB/OL]. <http://epics.web.psi.ch/software/s7plc/YHLhtcPLCa.pdf>, 2012
- 7 S7PLC EPICS driver documentation[DB/OL]. <http://epics.web.psi.ch/style/software/s7plc/s7plc>, 2012
- 8 刘锴, 周海. 深入浅出西门子 S7-300 PLC[M]. 北京: 北京航空航天大学出版社, 2004
LIU Kai, ZHOU Hai. Explain profound theories in simple language Siemens S7-300 PLC[M]. Beijing: Beihang University Press, 2004
- 9 宋伯生. PLC 编程理论·算法及技巧[M]. 北京: 机械工业出版社, 2005
SONG Bosheng. The PLC programming theory and algorithms and techniques[M]. Beijing: Mechanical Industry Press, 2005

Application of Ethernet technology in SSRF control system

ZHOU Dayong LIU Dekang LIU Yajuan SHEN Liren

(Shanghai Institute of Applied Physics, Chinese Academy of Sciences, Jiading Campus, Shanghai 201800, China)

Abstract Background: With the development of computer technology and Ethernet technology, programmable logic controller (PLC) has the ability to access Ethernet with its Ethernet communication module, so the device controller can be connected directly to the Ethernet network. **Purpose:** The aim is to apply the Ethernet technology for the accelerator device controller to the upper-level control system. **Methods:** The Shanghai Synchrotron Radiation Facility (SSRF) control system is based on the large-scale software EPICS (Experimental Physics and Industrial Control System). The EPICS communication is mainly based on Ethernet technology. Control devices are connected to the EPICS either by their self-contained driver or by implementation of the appropriate Ethernet application program interface (API). **Results:** PLCs with Ethernet connection are widely used in SSRF device control system whilst other control devices are connected to EPICS by developing Ethernet API. **Conclusion:** The Ethernet technology ensures good reliability and easy maintenance of the SSRF device control.

Key words Ethernet, EPICS (Experimental Physics and Industrial Control System), Programmable Logic Controller (PLC), Device control

CLC TL503.6