基于 OPC Server 的 PC 与 S7-300/400 的通信

张俊彪,王鸿辉,何长安
(西北工业大学 自动化学院,陕西 西安 710072)

摘要:西门子 S7-300/400 系列可编程逻辑控制器(PLC)是基于现场总线网络的节点控制器,其通信协议不开放增加了在 Lab Windows/CVI 等平台上开发通信驱动软件的难度。提出利用 OPC(OLE for Process Control)接口技术解决应用软件与各种设备驱动程序的通信。在 PC 机上创建 OPC 服务器,使用 Simatic NET 软件建立 Profibus-DP 网络实现 OPC 服务器与 S7-300/400 系列 PLC 输入、输出接口点对点的连接。叙述了配置 PC 站、设置主/从机、与 PC 机建立连接的步骤。该方案已成功地应用于某控制系统中。

关键词:可编程逻辑控制器;OPC 服务器;通信
中图分类号:TN 915 **文献标识码**:A **文章编号**:1006-6047(2007)04-0083-04

0 引言

西门子 S7-300/400 可编程逻辑控制器(PLC)属于中大型器件,与 S7-200 系列相比缺少了自由口通信这一大特色,这样用户在通信中不可能自定义通信协议[1]。

西门子 S7-300/400 PLC 通信接口只有多点接口 MPI(Multi Point Interface)和分布式外设接口 DP(Decentralized Periphery),分别使用 MPI 协议和 Profibus 协议。但是这 2 种协议都不公开,使得该系列 PLC 与 PC 机通信实现变得困难。

某重型机械研究所承接的倒棱机控制系统中,PC 机在 Windows 环境下除了要实现与 S7-300 系列 PLC 通信外还要做高精度的闭环位置控制。采用西门子 WinCC 组态软件实现多任务处理时,WinCC 里封装了 S7-300/400 PLC 通信协议驱动使得两者通信很容易实现,但是位置控制系统的实时性却无法保证。为解决这一问题,以往的方法是用 2 台工控机,一台工作于 DOS 系统下做闭环控制,另一台工作于 WinCC 组态软件下实现 PC 机和 S7-300 PLC 通信和人机界面处理,2 台工控机用 RS-232 通信以协调工作,但成本过高,且方案不紧凑[2-3]。

OPC(OLE for Process Control)技术是一种各个仪器厂商普遍接受的工业化标准,它的出现解决了各仪器接口不统一而无法互联的问题。这里应用 OPC 技术实现 PC 机与 S7-300/400 系列 PLC 的通信。工控软件采用美国 NI 公司的虚拟仪器 Lab Windows/CVI,PC 机在 CVI 环境下调用 Windows 的 API 函数库里的多媒体定时器做高精度位置闭环控制,可以在一台工控机上保证控制实时性的同时实现与 PLC 通信及人机界面的处理任务。

收稿日期:2006-07-31;修回日期:2006-12-12

1 OPC 技术简介[4-5]

OPC 是用于工业控制领域的 OLE(Object Linking and Embedding)。按照 OPC 基金会的定义,OPC 是一套技术规范和工业标准,为基于 Windows 操作平台的工业应用程序提供高效的信息集成和交互功能的组件对象模型接口标准,以微软的分布式组件对象模型 COM/DCOM/COM+技术为基础,采用客户/服务器模式,提供自动化控制、设备管理和设备之间的软件应用互操作性和设备的互换性。OPC 的作用是为服务器和客户的链接提供统一和标准的接口规范。OPC 的服务器是数据的供应方,负责为 OPC 客户提供数据;OPC 客户是数据的使用方,处理 OPC 服务器提供的数据[6]。

OPC 是为解决应用软件与各种设备驱动程序的通信而产生的一个工业技术标准。使用 OPC 可以比较方便地把不同制造商提供的驱动或服务程序与应用程序集成在一起。OPC 在工业控制软件中,为不同类型的服务器与不同类型的客户搭建一座桥梁,通过这座桥梁,客户和服务器间形成即插即用的简单规范的链接关系,不同的客户软件能够访问任意的数据源,如图 1 所示。

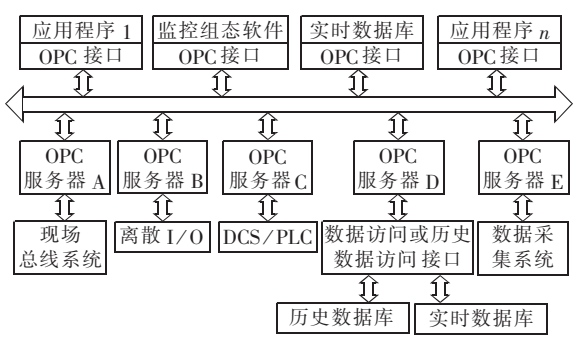

图 1 现场设备与应用程序基于 OPC 标准的连接图

Fig.1 OPC-based connections between field devices and applications

作为工业控制系统的一种核心数据交换技术，OPC标准可以应用在许多领域，并且其功能还在不断丰富发展之中。OPC适合于应用在很短时间内更新大量过程数据的工业场合。OPC接口可以适用在数据监控系统和管理控制台之间，从数据采集和监控(SCADA)系统或分布式控制系统(DCS)将数据传输到更高级的客户应用，实现在线数据监测。还可实现异构网段间的数据共享，实现PLC、DCS、FCS等不同类型控制系统和设备的集成。甚至只要在数据库系统上建立了OPC规范，OPC客户就可以与实时和历史数据库实现数据交互。OPC接口还可通过网络把最下层的控制设备的原始数据提供给作为OPC客户端的应用程序，也适用于应用程序和物理设备的直接连接，OPC是具有高度柔性的接口标准，屏蔽不同系统之间的差异，提供统一的数据访问接口，所以可以应用于多种场合[6]。

OPC标准的出现，为现场设备之间的互联及企业信息系统对现场设备的访问提供了一个高效、开放、可靠、互操作性好的解决方案。软硬件制造商、用户都可以从OPC的解决方案中获得方便，制造商可以专注于单一OPC接口的开发，用户按照OPC接口标准可以有更多的选择而不用考虑集成部件之间的兼容性问题。

OPC技术是基于组建对象模型COM(Component Object Model)技术构建的[7]。COM是一个在Windows下可执行的实体，该实体通过接口为其他实体使能。一个COM实体可同时被多个应用实体使用。COM定义了一个标准，将目标体定义为各个分离的单元，单元之间的连接通过过程变量实现。图2是一个4接口的COM构件，目标体之间连接只能通过定义的接口(Interface)，而不可能获得该构件的内部数据及代码。

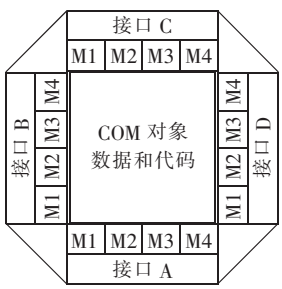

图2 COM交换接口

Fig.2 COM interface

客户机和目标体的连接是通过过程变量实现的。过程变量是COM定义的，是实现COM体和外界交换数据的唯一接口。OPC Interface技术应用基于客户服务器模型，在模型里，某个实体向其他实体提供服务是通过OPC Interface实现的。

将传递数据的OPC实体称为OPC服务器，访问OPC服务器的实体称为OPC客户端。客户端可以购买市场上成品软件实现，也可以用常用语言(如VB、C或C++语言)开发。客户端和OPC服务器通信是基于COM对象实现。客户端并不能直接接触到服务器内核，而是通过COM库(COM Library)实现，如图3、4所示①。

OPC数据存取DA(Data Access)服务器在结构上分为OPC Server、OPC Group、OPC Item 3层。其

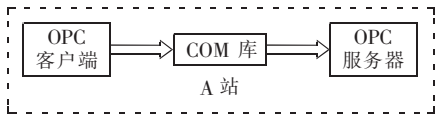

图3 本地PC机上的客户端与服务器基于COM的连接

Fig.3 COM-based connection between client and server in local PC

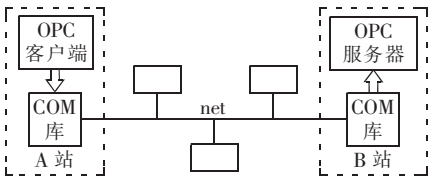

图4 远程PC机间客户端与服务器基于COM的连接

Fig.4 COM-based connection between remote PC client and PC server

中每个OPC Item对应于一个实际的硬件装置上的某个channel或port；每个OPC Group则包含了许多的OPC Item，同时并定义这些OPC Item更新的时间、方式，以及提供读取OPC Item值的接口；而每个OPC Server则包含若干个OPC Group，同时提供操作这些OPC Group的接口[8-9]。

2 通信实现方案构架[10-14]

Simatic NET是西门子公司一款基于OPC技术的自动化控制方案实现软件，支持多种通信协议，广泛应用于各类分布式自动化系统中。文中PC机和PLC之间基于OPC技术的通信通过该软件进行配置实现，两者间的通信是基于PC机里建立的2个虚拟站(Simatic 400-Station和Simatic PC Station)。2站之间的通信通过Profibus协议实现，其中PC站配置成OPC服务器，通过OPC标准接口和PLC实现通信。另外一端PC机上应用软件(如Lab Windows/CVI)可以作为OPC客户端去访问OPC服务器，从而实现客户端与S7-300/400系列PLC间的通信。

系统配置：1台PC机，通信模块CP 5613(安装在PC机的PCI总线槽里)，Simatic NET CD 11/2003软件1套，ET 200B，Profibus通信电缆1根。

硬件连接：安装Simatic NET CD 11/2003软件，在断电情况下将CP 5613安装在计算机PCI总线槽内。将通信电缆一头连接到CP 5613(DP主)，另一头连接到ET 200B(DP从)。检查连接端口，然后将两端的端口激活。

3 应用Simatic NET配置PC站

PC站由Simatic NET通信模块和应用软件构成。Simatic NET OPC Server就是典型的应用软件。PC站有2种工作方式：PG Operation和Configured Mode。后者应用于PC站应用软件和可编程器件(如S7-400)之间的通信。系统初始默认为PG Operation模式。在Station Configuration Editor里添加CP 5613

① Industrial communication with PG/PCSimaticNET Manual(DB). 西门子公司，2003.

后系统自动切换为 Configured Mode。

3.1 配置 PC 站

新安装的模块都要进行初始配置,应用 Simatic NET 对 PC 站进行配置,下面以 Configured Mode 模式为例说明配置步骤。

a. 在【开始】菜单里选择 Station Configuration 图标后打开。

b. 点击[station name],给 PC 站命名。

c. 点击【ADD】按钮,PC 站的模式自动设置为"Configured Mode"。此时可以添加模块,分别添加"OPC Server"、"Application"、"CP 5613",添加时给每个模块分配唯一的地址加以区别。

3.2 设置主从机

将 CP 5613 设置成 DP 主,创建一个 Step 7 环境下的工程,在该工程里 Simatic PC 站就如同本地 PC 的一个镜像,该站包括 OPC Server 和 CP 5613。下面介绍建立步骤。

a. 打开 Simatic Manager 组件,建立一个工程。

b. 添加 OPC Server 和 CP 5613,并对其分配对应的网络地址,该地址要和建立 PC 站时分配的地址相同。打开属性对话框对其他参数进行相应的设置。创建 CP 5613 时要注意将该模块设置为主系统(Master System)。添加 ET 200B,将其设置为从机,点击该属性,选择 16 位输入/输出模式。这时,在 NetPro 里,就可看到网络连接图。

c. 保存并编译该配置。该步骤完成后,当前配置即可保存在工程里,系统数据块也随即创建。

3.3 与 OPC 建立连接

完成 OPC Server 和通信组件设置后,分配过程变量,通过过程变量获得与 COM 体内部交换数据的条件。OPC Scout 可实现过程变量的指定、分配及监视。有 3 个操作步骤。

a. 按以下次序打开 OPC Scout 组件:【开始】→【Simatic】→【Simatic NET】→【Profibus】→【CP 5613_CP 6514】→【OPC Scout】。

b. 双击"OPC Simatic NET"后,系统连接到 OPC Server。

c. 分配过程变量(又称 OPC item),在建立 OPC item 前首先要建立一个 OPC Group。启动 OPC Scout 后自动弹出一个对话框,给 OPC Group 命名以标识该 OPC Group。退出该对话框,点击该 OPC Group,弹出另一对话框,要求建立 OPC item。OPC item 的类型分 3 类:I(输入)、O(输出)、DB(DB 块)。其中 I 和 O 是挂接 PLC 上的输入/输出点,为二进制状态,DB 块用于模拟量传送,其传送的数据类型有整型、实型和双精度型。只有和 PLC 完成连接后该对应的挂接点才能显示出来。根据实际需要添加对应的 OPC item,每个点都对应一个地址,该地址就是向 OPC 客户端开放的唯一识别。每添加一个 OPC item,该项就出现在主菜单的表格里,其状态信息也会有标识,例如,在"Quality"栏用"good"或"bad"表示该变量是否挂接好,还可以监视各状态变量的值。完成以上设置后,PLC 和 OPC Server 即可实现通信,通过 OPC Scout 可以实时监视通信数据的变化。

4 OPC 客户端访问 OPC Server

客户端采用美国 NI 公司的虚拟仪器 Lab Windows/CVI 开发,该软件是一种 C 语言下的虚拟仪器开发平台。提供访问 OPC Server 的标准接口。在该软件里有专用的访问 OPC 服务器的函数,如:DS_Open (const char *URL,DSEnum_AccessModes accessMode,DSCallbackPtr eventFunction,void *callbackData,DSHandle *DSHandle)。该函数用于创建客户端接口的一个数据点,和对应 OPC Server 中的一个 OPC item 建立通信连接,两者数据类型应该一致。其中,"URL"是指向一个 OPC Item 的地址,如"S7:[S7 connection_1]Q3.1,1"是一个地址,从该地址中可以看出 OPC Group 的名字为"S7",OPC item 为"S7 connection_1]Q3.1,1",即指向 PLC 的输出 I/O 点 3.1。该地址是用户在 OPC Scout 组件中添加每一项 OPC item 时自动生成。"DSHandle"是指向该地址句柄,即进行读写操作时标识该 OPC item 项。"accessMode"为数据访问形式,有 DSConst_Read(客户端读操作)、DSConst_Write(客户端写操作)、DSConst_ReadAutoUpdate(客户端自动读)以及 DSConst _WriteAutoUpdate(客户端自动写)4 种形式。其中,"自动读/写"与"非自动读/写"的区别是:使用前者时,客户端与 OPC Server 交换数据是定时自动的,而后者则是非自动的,在进行读/写操作后要用 DS_Update(DSHandle DSHandle)函数实现手动更新数据。另外,2 个进行读写操作的函数是 DS_GetDataValue(DSHandle DSHandle,unsigned int type,void *value,unsigned int size,unsigned int *dimension1,unsigned int *dimension2)和 DS_SetDataValue(DSHandle DSHandle,unsigned int type,const void *value,unsigned int dimension1,unsigned int dimension2)。其中"DSHandle"是使用 DS_Open 函数时确定的。"type"为访问数据的类型,有 CAVT_DOUBLE(双精度)、CAVT_FLOAT(实型)、CAVT_SHORT(短整型)、CAVT_CSTRING(字符串型)、CAVT_BOOL(布尔型)等。该类型的选择一定要与实际通信的数据类型一致。"value"为一变量,客户端交换的数据通过"value"传递到读/写函数里。若"value"是一个一维或二维数组,则数组的元素个数就要在该函数的 dimension1 和 dimension 2 中声明。若使用一维数组,则维数在 dimension 1 中声明,dimension 2 置 0。若使用二维数组,则将维数 1 和 2 分别放置在 dimension1 和 dimension 2 中,数组通常用在字符串的通信中。应注意,若某一通信端口被 DS_Open 函数设定为读/写属性时,则对端口的访问只能用函数 DS_GetDataValue/DS_SetDataValue。

5 结语

该套方案应用于成都某钢铁集团的钢管倒棱机系统中,于2005年12月调试成功。在实际运行中稳定可靠,通信速度较快,同时没有影响到闭环控制的精度,达到了预期的效果。但也存在一个小缺陷,因为OPC Server是建立在PC机上,一旦PC机重新启动,PLC不会再次搜寻网络,从而导致通信连接不上,这时需要重新复位PLC即可。在实际生产中,PC机工作在非间歇状态,所以对生产没有影响。总体看来,是一个比较成功的方案。

参考文献:

[1] 周晓平,姜建芳,苏少钰,等. S7-200系列PLC与监控计算机通信实现的研究[J]. 微计算机信息,2004,20(1):5-7.
ZHOU Xiao-ping,JIANG Jian-fang,SU Shao-yu,et al. Research of communication between S7-200 series PLC supervision computer[J]. Microcomputer Information,2004,20(1):5-7.

[2] 邹益仁,马增良,蒲维. 现场总线控制系统的设计和开发[M]. 北京:国防工业出版社,2003.

[3] 姜建芳,苏少钰,陈庆伟,等. 西门子S7-300系列PLC与PC机通信实现的研究[J]. 制造业与自动化,2003,25(1):52-54.
JIANG Jian-fang,SU Shao-yu,CHEN Qing-wei,et al. The disquisition on the communication between PC and Simentic S7-300[J]. Manufacturing and Automation,2003,25(1):52-54.

[4] 李南,薛孝存,王大海,等. 浅谈OPC技术[J]. 中国仪器仪表,2003(1):5-7.
LI Nan,XUE Xiao-cun,WANG Da-hai,et al. OPC technology summarizing[J]. China Instrument,2003(1):5-7.

[5] 邹云涛,吴重光. OPC技术初探及国内应用现状[J]. 石油化工自动化,2003(6):1-5.
ZOU Yun-tao,WU Chong-guang. OPC technology and its application status in China [J]. Automation in Petro-Chemical Industry,2003(6):1-5.

[6] 王鲲,袁中凡. OPC接口技术在工业自动化系统中的应用[J]. 中国测试技术,2005,31(1):95-97.
WANG Kun,YUAN Zhong-fan. Application of OPC technology in industry automation[J]. China Measurement Technology,2005,31(1):95-97.

[7] 亓军祥,唐伟,黄德先. 基于OPC技术的工控软件设计[J]. 山东建筑工程学院学报,2003,18(4):58-70.
QI Jun-xiang,TANG Wei,HUANG De-xian. Software design for industry control based on OPC specification[J]. Journal of Shandong University of Architecture and Engineering,2003,18(4):58-70.

[8] 顾键,王京春,黄德先. OPC-COM技术在工业自动化软件中的应用[J]. 计算机工程与应用,2002,30(6):207-209.
GU Jian,WANG Jing-chun,HUANG De-xian. OPC:application of the COM technology in industrial automation software[J]. Computer Engineer & Application,2002,30(6):207-209.

[9] 石林锁,王涛,刘顺波. 基于OPC规范的客户应用程序实现[J]. 微计算机信息,2003,19(5):68-71.
SHI Lin-suo,WANG Tao,LIU Shun-bo. The realization of client application based on OPC specification[J]. Microcomputer Information,2003,19(5):68-71.

[10] 高德欣,杨清,刘军,等. 利用OPC接口实现SCADA系统与PLC之间的通信[J]. 青岛科技大学学报,2006,27(1):66-69.
GAO De-xin,YANG Qing,LIU Jun,et al. Communication between SCADA system and PLC by the OPC interfaces[J]. Journal of Qingdao University of Science and Technology,2006,27(1):66-69.

[11] 高翔,张秋生,袁晓鹏. 基于OPC接口访问过程的实现[J]. 燃料与化工,2006,37(1):18-20.
GAO Xiang,ZHANG Qiu-sheng,YUAN Xiao-peng. Realization of process control based on OPC interface access[J]. Fuel & Chemical Processes,2006,37(1):18-20.

[12] 梁首发. S7-300可编程序控制器及工控组态软件Win CC应用[J]. 中国仪器仪表,2001(3):16-17.
LIANG Shou-fa. Application of S7-300 programmable controller and industrial control configuration software Win CC[J]. China Instrument,2001(3):16-17.

[13] 亢红波,马伯渊,商高平. PLC控制系统中基于OPC技术的多上位机解决方案[J]. 工业控制计算机,2006,19(1):68-69.
KANG Hong-bo,MA Bo-yuan,SHANG Gao-ping. Solution to multi senior computer based on OPC technology in PLC control system[J]. Industrial Control Computer,2006,19(1):68-69.

[14] 周宇峰,唐通林. OPC Web服务——过程控制系统信息集成的新方法[J]. 测试技术与自动化,2004(2):20-21.
ZHOU Yu-feng,TANG Tong-lin. OPC-Web service-new method of process control system information integration[J]. Test Technology and Automation,2004(2):20-21.

(**责任编辑:**汪仪珍)

作者简介:

张俊彪(1978-),男,陕西宝鸡人,硕士研究生,研究方向为测控、仿真与网络(**E-mail**:zjb908@126.com);

王鸿辉(1978-),男,苗族,贵州台江人,讲师,硕士,研究方向为液压伺服控制;

何长安(1938-),男,上海人,教授,博士研究生导师,从事非线性控制理论的研究。

Communication between S7-300/400 and OPC Server-based PC

ZHANG Jun-biao,WANG Hong-hui,HE Chang-an

(College of Automation,Northwestern Polytechnical University,Xi'an 710072,China)

Abstract: As S7-300/400 series PLC(Programmable Logic Controller) is node controller based on field bus net,it is difficult to develop the communication software on Lab Windows/CVI platform for its privacy of communication protocol. It is proposed to implement the communication between application software and device driver using OPC interfacing technology. An OPC(OLE for Process Control) server is built on local PC,and then a Profibus-DP net is created using Simatic NET software to realize the point-to-point connections between OPC server and inputs/outputs of S7-300/400. Steps to configure PC station,master/slave system and connections between PC and PLC are presented in detail. The method has been successfully applied in a control system.

Key words: PLC; OPC Server; communication