Computer Science and Application 计算机科学与应用, 2016, 6(3), 110-118
Published Online March 2016 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2016.63014

Hans汉斯

Program Transmission Method of PLC Equipments' Remote Monitoring Software Based on Virtual Serial Port

Hansi Chen[1], Hua Ye[1,2], Yanlan Yang[1,2]

[1]School of Automation, Southeast University, Nanjing Jiangsu
[2]Key Laboratory of Measurement and Control of Complex Systems of Engineering, Ministry of Education, Southeast University, Nanjing Jiangsu
Email: zhineng@seu.edu.cn

Received: Feb. 9th, 2016; accepted: Feb. 26th, 2016; published: Mar. 1st, 2016

Abstract

In order to facilitate trouble shooting and program debugging for the PLC equipment maintenance personnel when the equipments malfunction, the program transmission method of PLC equipments' remote monitoring software based on virtual serial port is designed. And this method realizes the efficient and stable transmission of the program. This software is developed based on the MFC (Microsoft Foundation Classes) platform in Microsoft.NET, which provides users a friendly operation interface. This software makes full use of multi-thread technique and serial communication control, building the transmission structure which is made of serial communication based on virtual serial port and network communication based on the TCP/IP protocol. The design of communication protocols and the concrete realization of communication interface are given with program transmission tested in this paper.

Keywords

Virtual Serial Port, PLC Program, Remote Monitoring, Serial Communication, TCP/IP

基于虚拟串口的PLC设备远程监控软件的程序传输方法

陈含思[1]，叶　桦[1,2]，仰燕兰[1,2]

文章引用: 陈含思, 叶桦, 仰燕兰. 基于虚拟串口的 PLC 设备远程监控软件的程序传输方法[J]. 计算机科学与应用, 2016, 6(3): 110-118. http://dx.doi.org/10.12677/csa.2016.63014

[1]东南大学自动化学院，江苏 南京
[2]东南大学复杂工程系统测量与控制教育部重点实验室，江苏 南京
Email: zhineng@seu.edu.cn

收稿日期：2016年2月9日；录用日期：2016年2月26日；发布日期：2016年3月1日

摘 要

为了方便PLC设备维护人员在设备出现故障时进行问题排查和程序调试，本文设计了基于虚拟串口的PLC设备远程监控的程序传输方法，实现了程序的高效稳定传输。本文使用Microsoft.NET的MFC开发平台编程实现，为用户提供友好的操作界面，并充分利用MFC的多线程技术和串口控件，搭建了基于虚拟串口的串口通信和基于TCP/IP协议的网络通讯的传输结构。本文给出了两种通讯方式下通讯协议的设计和通讯接口的具体实现，并对程序传输进行了测试。

关键词

虚拟串口，PLC程序，远程监控，串口通信，TCP/IP

1. 引言

PLC(Programmable Logic Controller)作为高性能的微机化自动化设备，目前在国内外已广泛应用于钢铁、石油、电力、机械制造、交通运输、环保等各个行业[1]。随着其应用的推广，控制对象越来越复杂，使用的环境越来越复杂，控制要求也越来越高，传统的 PLC 设备程序调试模式已难以适应发展的需求[2]。

设备远程监视及控制已经成为自动化设备行业中不可或缺的部分，在多设备、多使用场景的情况下，及时对 PLC 进行监控排除故障是有效解决问题的关键。当设备出现客户无法排除的故障时，维护人员如能及时的对 PLC 进行远程数据和程序监控，则能及时解除故障，减少客户解决问题的时间，提高设备的利用率。为了保证远程监控调试程序的便利性及高效性，本文在本地程序调试模式的基础上探讨通过虚拟串口以及网络监控的模式来进行 PLC 程序的远程上传与下载。

本文以欧姆龙公司 CP1H 型 PLC 设备为控制对象。运行在 PLC 设备上的程序由 PC 端的欧姆龙编程软件 Cx-programmer 进行编译，生成的 CXP 程序文件可以通过 USB 和 RS232 串口两种方式下载至 PLC [3]。虽然 USB 的传输速度快，但受到成本高、开发复杂、需要驱动程序支持等因素限制；串口传输的速度相对较慢，但其开发成本较低、本地对接方便且无需驱动程序支持，故本文选择串口作为程序传输的接口。

2. 软件总体设计方案

2.1. 软件整体架构

PLC 设备运行在各种工业环境中，通过安装在其上的 HLK-RM04 模块(串口—以太网—无线网模块)收集存储于 PLC 数据区的参数数据，进行回传以判断当前设备状态，当某参数超限时可判断设备出现某种故障。由于需要对多台设备进行监控，PLC 远程监控软件采用 C/S 模式，通过服务器端的数据库做统一的数据存储及转发。远程监控客户端安装在本地 PC 上，通过虚拟串口对与 Cx-programmer 软件互连，编写好的程序经服务器通过网络发送至 PLC。网络通信均采用 TCP/IP 协议，以保证传输数据的准确性。远程监控软件的架构如图 1 所示。

从结构上划分，PLC 远程监控系统主要由以下 4 个部分组成：

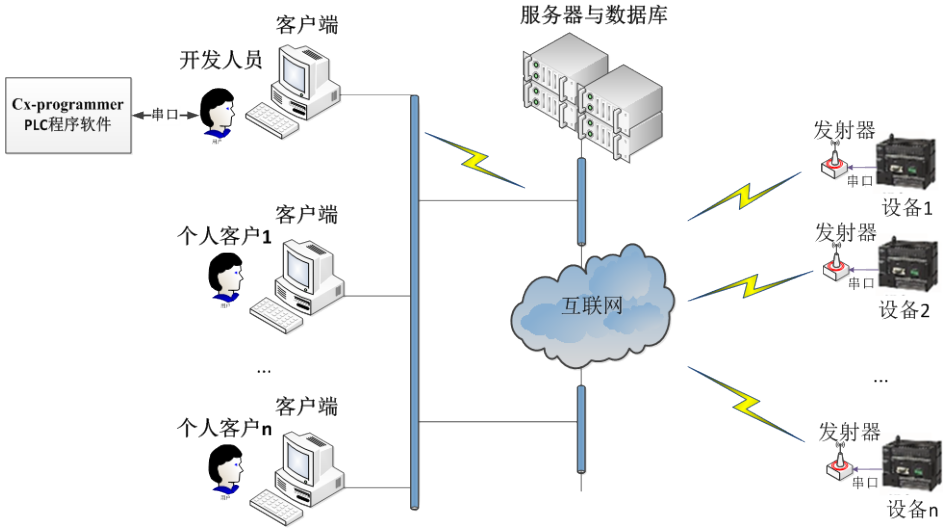

Figure 1. Architecture diagram of the PLC remote monitoring software
图 1. PLC 远程监控软件架构图

1) PLC 设备终端：包括 1 个欧姆龙 CP1H 系列 PLC 设备和 1 个 HLK-RM04 模块。PLC 通过 RS232 串口外接 HLK-RM04 模块，HLK-RM04 模块经过网络与服务器连接，进行数据的转发。

2) 服务器：由应用服务器和数据库组成，应用服务器负责收发数据、解析和存储数据，数据库主要是完成对用户信息、设备信息及 PLC 上传的部分数据进行存储，以供客户端访问。

3) 客户端：按照事先制定的通讯协议，和服务器以及 PLC 程序编译软件通信。客户端提供设备信息和用户信息显示及管理的功能，以及完成 PLC 程序的转发。

4) Cx-programmer 编程软件：是一个用于对欧姆龙 C 系列 PLC 进行编程、测试和维护设备配置的工具[4]，客户端通过虚拟串口与 CX-Programmer 连接，完成程序指令的转发。

2.2. 软件功能结构

PLC 远程监控软件采用 C/S 工作模式，服务器直接与 PLC 发射器相连，主要负责传输程序指令、定时收集设备参数以及存储数据。客户端软件是用户操作管理的直接接口，采用模块化思想设计，按层次可以分为网络通讯接口层、数据处理层和用户界面层。

网络通讯接口层主要负责客户端与服务器端交换数据，利用基于 TCP/IP 通讯协议的 Socket 编程实现；数据处理层用于解析服务器上传的数据和封装下发的程序命令等，定义了通讯单元类 CCommUnit 实现数据发送和等待接受数据线程；用户界面层为用户提供了良好的人机交互界面，用户通过操作菜单和各功能界面，满足监测、显示、设置、存储等应用需求，利用 MFC 编程技术完成操作界面的设计和各菜单、按钮的响应。远程监控软件功能结构如图 2 所示，程序传输主要由程序监控模块和数据处理、通讯接口层面完成。

3. 程序传输通讯方案

依据 PLC 程序下载与上传皆经过串口的特点，在通讯接口层面，客户端通过虚拟串口对来实现 RS232 转 TCP/IP 网络结构的构建，客户端与 Cx-programmer 编程软件通过串口连接，同时与服务器以网络传输；服务器端与客户端以及 PLC 的发射器均为网络连接，发射器完成网络数据和串口数据的转换，与 PLC 进行交互。程序传输路径如图 3 所示。

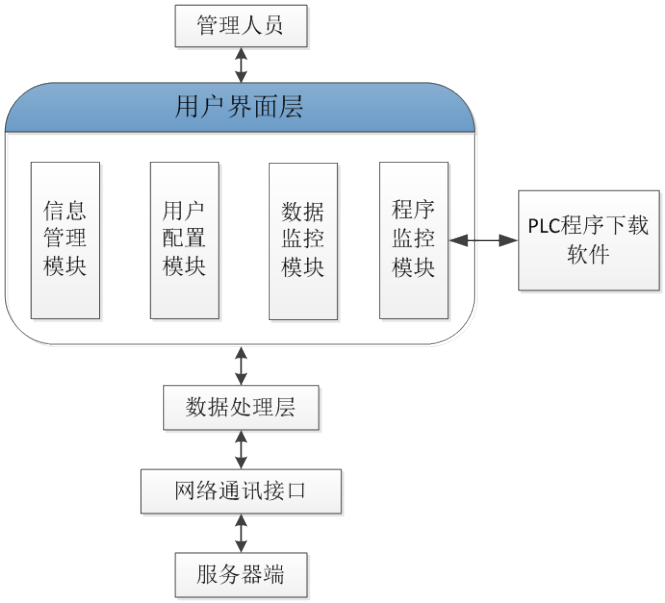

Figure 2. Function structure diagram of remote monitoring software
图 2. 远程监控软件功能结构图

Figure 3. Program transmission path diagram
图 3. 程序传输路径图

3.1. 通讯方式选择

本软件系统利用串口与网络来完成整个组网方案，因此选择串口通信与 Socket 通讯方式来支持。串口通信技术是基于串行通信接口标准的数据通信技术，本文采用 MSComm 控件进行串口通信的编程。服务器与客户端支持标准的 TCP/IP 通讯格式，使用 Socket 编程规范实现。

3.2. 虚拟串口配对

虚拟串口是用操作系统的虚拟驱动技术产生的串口(COM 口)，相对于计算机本身的硬件串口(COM1 等)来说，虚拟串口并不对应一个物理上的串口，而是为软件应用提供一个类似串口硬件设备的系统调用接口，以兼容原本使用本地串口的应用软件[5]。对于串口软件来说虚拟串口和硬件串口并没有区别。

3.2.1. 虚拟串口驱动

本文利用 VSPD(Virtual Serial Port Driver)软件进行串口的配对，它是由软件公司 Eltima 制作的一款本地虚拟串口软件，可以方便地实现多对串口的配对。在传输程序之前，需要先利用 VSPD 勾选所需的两个串口加入配对，Cx-programmer 软件与客户端所用串口应与配对的串口名称相对应。

3.2.2. 串口参数配置

一般而言，配对的两个串口参数应相同，即使用相同的波特率、奇偶校验位、停止位以及数据位，同时 Cx-programmer 软件和客户端的串口名称应与 VSPD 软件中配对的串口名称一致。PLC 与发射器之间以物理串口相连，但仍需设置统一的串口参数。其中，Cx-programmer 软件的串口参数配置如表 1 所示。

Table 1. Serial port parameter configuration information of Cx-programmer
表 1. Cx-programmer 软件的串口参数配置信息

串口名称	波特率	数据位	奇偶校验位	停止位
COM1	115,200	7	Even	2

3.3. 通讯协议制定

在程序传输过程中，服务器的主要功能是转发，即拼接指令与透明传输；而客户端则是联系 Cx-programmer 程序软件和 PLC 设备的桥梁，涉及串口通信和网络通讯两种通讯方式。

3.3.1. 基于串口通信的通讯协议

Cx-programmer 软件与 PLC 设备之间是一问一答式，先由程序软件发起连接，PLC 设备回复并成功连接后开始频繁的程序数据交互。在串口之间传输的皆是 PLC 程序指令，串口一个字符一个字符地传输。

串口通信指令格式为：数据—结束符，数据是具体的 PLC 程序，结束符为回车<CR>，以结束符作为判断一条指令的间隔符。

3.3.2. 基于网络通讯的通讯协议

客户端与服务器之间通过网络通讯，通讯指令有三种：控制指令和程序指令，以及保证连接状态的心跳包。其中，控制指令用于控制对某台具体编号设备传输程序的启动及停止，程序指令是对串口接收到的程序数据再封装成网络传输格式。

指令格式为：开始符—命令码—结束符，开始符为“@@”，结束符是“FEEF”，用以间隔一条指令。下面进行详细说明。

1) 控制指令：有两条指令，分别是通知服务器开始向某台设备传输程序的指令和断开连接的指令。启动指令的命令码为 PLC 设备的编号，即先告知服务器传输对象，服务器回复所指向 PLC 的状态，来判断当下是否可开始传输。停止指令的命令码是 ED，即停止程序传输，断开与服务器下载端口的连接。

2) 程序指令：是将串口传输来的指令(包括结束符<CR>)加上开始符和结束符。

3) 心跳：为了确保程序传输的稳定，保证客户端与服务器在传输过程中一直为连接状态，客户端需定时向服务器发送心跳。

4. 串口传输通讯设计

如前所述，客户端与 Cx-programmer 程序软件各开一个串口，通过虚拟串口配对连接，其与物理串口连接无异。串口通信的方式有多种，最常见的主要有两种：调用 API 函数和 MSComm 控件。利用 MFC (Microsoft Foundation Classes)开发环境本身已有的控件进行开发设计，不仅可以减少开发时间，节约开发投资，而且有利于保证系统的稳定性和可靠性[6]，因此本文采用 MSComm 控件进行串口通信的编程。

4.1. 基于 MSComm 控件的事件驱动通信

MSComm 控件具有完善的串行数据发送和接收功能，它屏蔽了通信过程中的底层操作，用户只需通过设置并监视其属性和事件，即可实现与被控制对象的串行通信。为了保证程序传输的高效性，控件选择实时性强、可靠性高的事件驱动通信方式，利用 OnComm 串口响应事件捕获通讯事件：当串口的接收缓存区中有字符时，OnComm 事件响应并开始一个一个字符读取缓存区中的数据，读至回车符时为一条完整的数据。

串口通信的基本步骤如下：1) 打开进行通讯的串口；2) 初始化串口：设置串口参数，设置接收区、

传输缓存区大小，设置缓存区可接收字符数，以及读取数据的模式；3) 根据通讯事件对数据进行发送和接收；4) 通讯结束关闭串口。

4.2. 多线程收发处理

对于 PLC 程序传输这种需要同时进行快速数据收发以及串口、网口转发的应用程序来说，创建多线程是比较理想的选择[7]。

从网口接收到的程序要从串口发送给编程软件，从串口接收到的数据要从网络端口发送至服务器。网络通讯采用发送指令线程和接收数据线程来共同处理收发数据，当接收数据线程接收到数据时，立即调用串口发送函数将接收到的数据转为字符发送到编程软件的串口。串口发送即在网络接收处理线程中完成，不另外开辟线程。

对于串口接收，由于串口事件响应函数的调用是同步阻塞的，所以开辟一条串口接收处理线程，用以等待串口响应接收以及向网口发送数据。在处理接收前，设立一个串口接收事件 g_OnComEvent 标志接收是否完成，初始为无信号，接收线程一直挂起。当串口响应函数 OnComm 从缓存区中读取串口接收的数据，并读到回车符，即读完一条数据时，将 g_OnComEvent 置为有信号，接收信号退出阻塞，调用网络发送函数将数据发送至服务器。接收数据线程的处理流程如图 4 所示。

5. 网络通讯设计

远程监控的重点是实现数据的远程传输，现场的 PLC 设备数据采集处理后经过局域网或广域网即可与监控软件互联起来，从而实现远程状态检测和远程程序的传输。远程监控的关键在于如何保证数据传

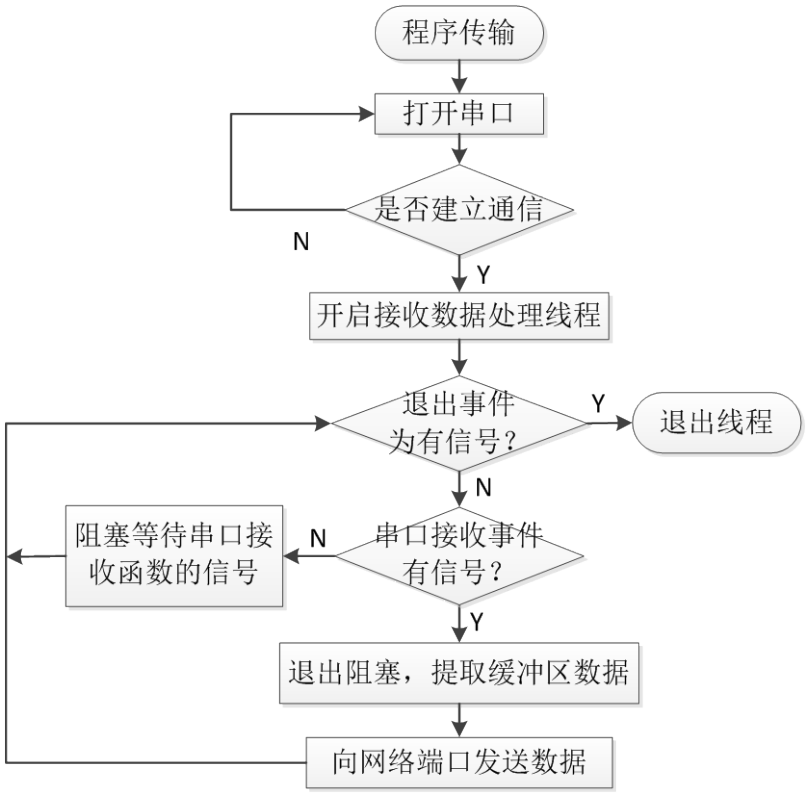

Figure 4. Flow-process diagram of receive data thread
图 4. 接收数据线程处理流程图

输的实时性和准确性[8]，因此本文选择面向连接、提供可靠的全双工数据通信的 TCP/IP 协议族进行主从问答式的实时传输。

5.1. 基于 Socket 的 TCP/IP 网络通讯

Socket 是面向客户端/服务器模型而设计的，针对客户端与服务器程序之间的相互通信而提供的通信机制[9]，采用 Windows Sockets 可以编写出基于 TCP/IP 协议的网络通信应用程序。

Socket 本身独立于 TCP/IP 通信协议，是工作在 IP 通信报文以及计算机应用层之间的网络编程接口，其中包含三种套接字：流式套接字，数据包套接字和原始套接字。流式套接字为应用层提供了一个面向连接的可靠的数据传输服务，可使网络层的传输报文向应用层无差错、无重复地按照顺序接收。因此为了能够及时并准确地传输设备的运行状况和程序，采用流式套接字(SOCK_STREAM)来实现服务器与客户端以及服务器与 PLC 发射器之间的数据收发。

根据通讯协议设计了底层通讯接口 TCPSocket 类，分配了发送数据和接收数据线程。封装好的通讯类在客户端进行网络发送时只需创建连接和调用 SendClient 函数；接收数据定义了状态回调函数 OnStatusChange 反馈网络连接状态，以及数据回调函数 OnDataArrived 返回服务器的数据。

5.2. 程序网络传输的设计

客户端与 PLC 设备的发射器之间的程序数据经过服务器通过网络传输。为了确保在程序调试过程中，能够稳定、安全地向某个确定的设备进行程序传输，客户端与 PLC 设备之间需要建立一对一的配对关系，此匹配由服务器完成。

当某台 PLC 接入服务器时，服务器先问询其设备编号(区分每台 PLC 的唯一标识符)，PLC 返回设备编号后注册加入服务器的设备队列。程序传输必须是对指定的设备进行，客户端首先连接服务器的下载端口，发送指令问询某编号的设备是否已注册，注册过的设备即匹配可建立连接。发送指令的格式为“@@” + 设备编号 + “FEEF”，服务器回复的数据如表 2 所示。

如表 2 所示，客户端发起连接时，设备未注册或已与其他客户端匹配时，不可连接。传输过程中可由客户端主动断开与服务器的连接，也可由 PLC 下线通知客户端断开连接，避免连接占用。客户端建立与设备的连接并进行传输的流程如图 5 所示。

6. 软件运行测试

6.1. 测试平台

测试时，Cx-programmer 程序软件需与客户端安装在同一台 PC 上，它们通过 VSPD 进行串口配对，并做统一的串口设置。CP1H 型欧姆龙 PLC 通过串口连接发射器，发射器通过网络接入 PC，PC 上可同时搭载客户端与服务器，也可以用一台 PC 做服务器，一台做客户端，构建起如图 1 所示的测试网络拓扑结构。

6.2. 测试结果

PLC 设备在上传或下载时一般是打包传输程序、I/O 设置及其他一些参数的配置信息，整体大小大约在几十 Mb 的范围内；而进行在线编程时，只向设备下载改动部分，程序包会更小，大概几十 Kb。程序传输速度主要受到串口波特率大小以及网络状况的影响。测试中，我们将波特率调至 CP1H 型 PLC 的最大波特率 115200，网络采用 GPRS 接入。客户端软件和 Cx-programmer 程序软件运行效果如图 6 和图 7 所示，可以看出，即使在网络传输较慢的情况下，Cx-programmer 程序软件也运行稳定，上载程序成功，软件设计达到预期的要求。

Table 2. Reply messages list of sever
表 2. 服务器回复消息列表

客户端状态	服务器回复数据	含义
建立连接	0000	成功建立连接
	0001	PLC 不在线，请稍后连接
	0002	当前 PLC 程序下载占用中，请稍后连接
程序传输中	0003	当前连接 PLC 已下线
	其他数据	程序指令

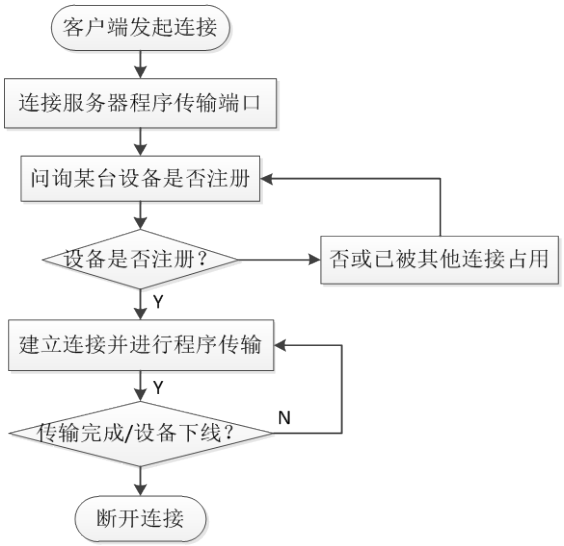

Figure 5. Flow-process diagram of connection between client and PLC
图 5. 客户端与设备建立连接的流程图

Figure 6. Running effect diagram of client
图 6. 客户端软件运行效果图

7. 结语

本文对基于虚拟串口的 PLC 远程监控软件的程序传输模块进行了详细设计，介绍了利用虚拟串口配对进行串口通信，以及基于 TCP/IP 协议的网络通讯方法，并进行了联机程序传输测试。远程监控程序传

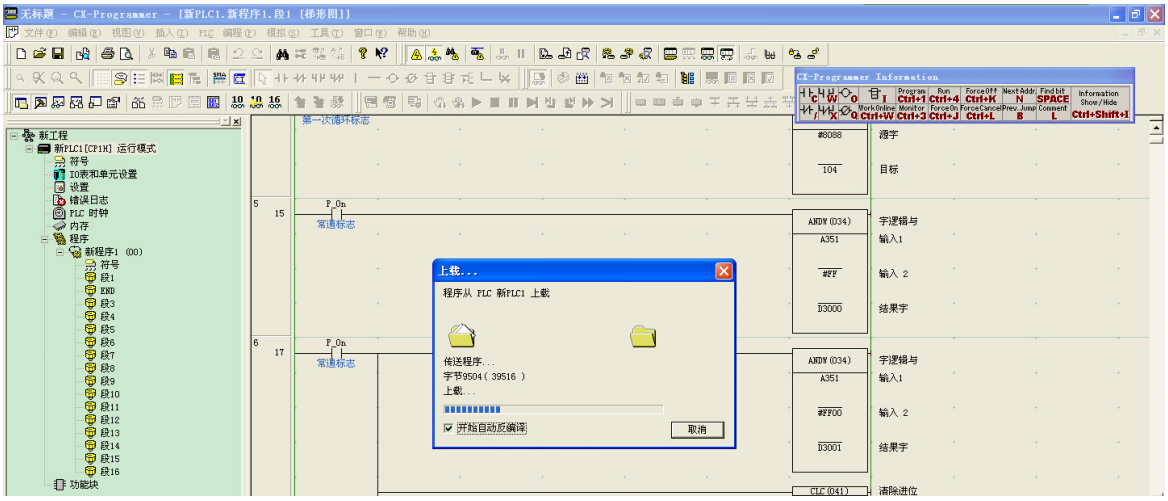

Figure 7. Program upload page of Cx-programmer
图 7. Cx-programmer 软件程序上载页面

输为 PLC 设备编程人员提供了一套稳定便利的传输程序方法，提高了设备程序调试和维护的效率。本方法对其他有类似要求的监控系统有一定的借鉴作用。

参考文献 (References)

[1] 刘天浩. 可编程控制器 PLC 的现状及应用分析[J]. 科技信息(科学教研), 2007(13): 318-456.

[2] 张全伟. Plc 设备应用与维护[J]. 数字技术与应用, 2010(3): 20.

[3] CP1H 型 PLC 产品规格书. 欧姆龙自动化(中国)有限公司[EB/OL]. http://www.fa.omron.com.cn, 2014, 12.

[4] CX-Programmer 使用指南. 欧姆龙自动化(中国)有限公司[EB/OL]. http://www.fa.omron.com.cn/products/family/1605/download/manual.html

[5] 江西财经大学国贸学院. 南昌. 开发虚拟串口驱动程序[N]. 计算机世界, 2005-01-03C15.

[6] 董红政, 王忠勇, 史晓鹏. 基于 MSComm 控件实现串行通信的方法[J]. 网络与通信, 2007, 23(27).

[7] Yang, L.F. (2008) The Programming Technique of Multi-thread Based on MFC. *Journal of Yangzhou Polytechnic College*, **12**, 38-41(Ch).

[8] 徐建, 贾民平, 许飞云, 等. 基于 TCP/IP 的状态监测系统通讯模块的研发[J]. 机械制造与自动化, 2007, 36(2): 85-87.

[9] 邓素杰. 基于 Socket 的 TCP/IP 网络通讯模式研究[J]. 计算机光盘软件与应用, 2013(20): 302-302, 304.