文章编号:1671-4598(2014)06-1871-04　　中图分类号:TP23　　文献标识码:B

基于 ARM+PFGA 的 PLC 系统通讯设计

谢从涩，蔡启仲，潘绍明，韦庆超，蒋林芳
（广西科技大学 电气与信息工程学院，广西 柳州 545006）

摘要：为提高 PLC 系统功能模块间通讯协议的通用性和可扩展性，对自主研制的 ARM+FPGA 构架小型 PLC 进行了通讯设计；在分析各类通讯数据的特点、实时性及可靠性要求的前提下，对 CAN 协议的应用层进行了扩展，采用数据单元法组织通讯数据，并对不同类型的数据定义了不同的数据单元格式，从而制定出了一种 CAN 扩展协议；另外，提出了以主机为中心的通讯模式，规定了通讯流程，确保了 PLC 主机执行程序的可靠性；经对通讯可靠性、通讯流量及编解码速度等测试表明，该协议通用性好，编解码效率高，达到了数据可靠传输的目的，提高了 PLC 系统的性能。

关键词：通信协议；PLC；通讯流程；CAN；应用层

Communication Design for PLC System Based on ARM+FPGA

Xie Congse, Cai Qizhong, Pan Shaoming, Wei Qingchao, Jiang Linfang
(College of Electric and Information Engineering, University of Technology, Liuzhou 545006, China)

Abstract: To improve function extension ability and communication protocol generality of PLC system, a communication is designed according to the independent research small PLC based on ARM+FPGA. According to communication real-time and reliability requirements, datas characteristics were analyzed and organized by a method of data unit. Different data units formats were defined. CAN protocol application layer was expanded. CAN extension protocol was formulated. To ensure the reliability of PLC host executing programs, a communication mode with PLC host as the center was proposed, and the communication process was made. The test shows, this extend protocol has a good applicability and high decoding efficiency, realizes reliable data transmission, and improves function expansion abilities.

Key words: communication protocol; PLC; communication process; CAN; application layer

0 引言

可编程逻辑控制器（PLC）具有编程简单、可靠性高的优点，在工业控制中应用广泛[1-2]。随着工业控制复杂性的增强，要求 PLC 通讯网络协议具有通用性，支持系统功能扩展、模块远程调试与测控以及信息的分散采集与集中处理。现有的 PLC 生产厂商各自采用的通讯方式不统一，且通讯协议不公开，相互之间难以互联。因此，本文利用 CAN 协议通讯距离长、可靠性高、协议开放性好的优点，为自主研制的基于 ARM（LPC1768）和 FPGA 的小型 PLC 设计了一种基于 CAN 总线的扩展通信协议。该协议支持远程通讯和自检，各功能模块安装地点不受通讯距离限制[3]，系统的灵活性和功能扩展能力较好。在应用层，针对各类通讯数据内部各个信息相互独立的特点，采用了数据单元的组织方式，方便了数据的编解码。另外，在通讯协议中提出了以 PLC 主机为主控的通讯模式，由主机控制 CAN 总线的使用权和发起通讯，既保证了 PLC 程序的可靠执行，又确保了数据传输的实时性。经协议编解码设计和功能测试，该扩展协议很适合 PLC 系统的数据传输，可靠性好，实时性强。

1 系统的总体设计方案

本文基于 ARM+FPGA 的小型 PLC 系统由 PLC 主机、手执编程器、远程 PC 机、现场监控观察模块（人机界面）及功能扩展模块组成[4]，如图 1 所示。

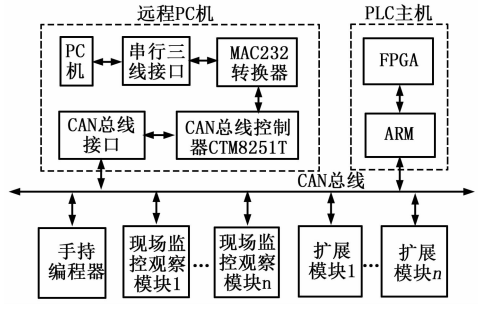

图 1 PLC 总体结构框图

各个模块通过 CAN 总线进行连接，以自定义 CAN 扩展协议完成通讯，从而组成一个完整的 PLC 系统，各模块均以 PLC 主机为通讯对象。其中，手执编程器用于软元件状态的查看与设定、PLC 程序的编辑编译和下载到 PLC 主机，以及读取 PLC 主机中的二进制 PLC 程序，将其反编译后供程序员查看和修改。PLC 主机接收到二进制代码后，ARM 部分将其进行静态编译和动态编译两次处理[5]，将软元件和立即数转换

收稿日期:2013-10-21； **修回日期**:2013-12-25。

基金项目:广西自然科学基金项目(2011GXNSFA018153);广西自然科学基金项目(0991067)

作者简介:谢从涩(1986-),男,广西贺州人,硕士研究生,主要从事过程控制与自动化装置方向的研究。

蔡启仲(1956-),男,湖南邵阳人,教授,主要从事智能控制方向的研究。

为地址，然后与FPGA一同完成指令的执行。人机界面主要完成软元件状态的查看、设定以及主机运行状态的显示。远程PC机通过串口和CAN收发控制器接入CAN网络，可在远程完成手执编程器和人机界面的功能。另外，扩展模块可为I/O扩展、A/D扩展、数字通信、联网和特殊功能等功能模块，以实现控制、检测以及通讯功能。

2 通讯方式选择

工业控制PLC系统的通讯方式，应具有以下几个特点[6]：

(1) 网络具有开放性。

(2) 支持不同PLC设备的集成和现有功能的扩展。

(3) 环境适用性及抗干扰能力强，成本低，设备兼容性好。

本设计选择CAN总线作为系统各模块间的通讯方式，是因为CAN总线具有开放性，任何具有CAN总线功能的器件，都可以方便地接入[7]，且总线可挂载设备多达110个，有利于系统功能的扩展。在传输特性上，CAN采用双绞线作为传输介质，成本低，通讯速度可高达1 Mbps/40 m，传输最远距离为10 km/5 kbps，可实现远程高速通讯，而且CAN协议具有节点出错自动退出功能，有利于提高PLC网络的抗干扰能力。另外，利用CAN模块的验收滤波器对总线上的数据进行过滤接收，可有提高PLC系统通讯的效率。基于以上优点，采用CAN通讯方式可以满足本设计的要求，使各功能模块形成一个系统网络，实现PLC各模块信息的分散与集中控制[7-8]。

3 通讯协议制定

3.1 通讯流程的规定

合理的通讯流程，对系统性能的提高具有重要的意义。在PLC系统中，各类数据的传输具有不同的特点。当进行程序的上传或下载时，通讯数据量大，可靠性要求高。因此，采用“请求＋响应＋应答”的通讯方式，通过应答来确认传送是否正确，以增强通讯的可靠性。当进行软硬件状态的读取和设定时，通讯量小，但实时性要求高，采用“无应答”通讯方式，省去应答环节来节约时间，以提高通讯的实时性。另外，为满足现场监控设备对PLC主机的实时控制，为人机界面设置CAN通讯的最高的优先级，并将PLC主机设为第二优先级，以确保可快速完成通讯。其余模块的优先级从高到低为：PC机、手持编程器、扩展模块[9]。

PLC指令的可靠执行，是PLC系统的最重要功能。PLC主机具有编程（top)、运行（run）两个工作状态，运行状态又分“输入采集”、“程序执行”、“输出刷新”3个阶段，在编程状态时，不执行PLC程序，运行状态时，所有通讯集中在“输入采集”和“输出刷新”阶段。在“程序执行”阶段不进行通讯，以保证PLC程序顺利执行。

PLC主机正常运行时，采集输入信息和刷新输出占了通讯的重要部分，其他模块向PLC主请求通讯的概率比较小，如果主机在每个扫描周期都依次询问各模块是否有通讯需求，则必然会导致主机扫描周期延长。因此，在正常运行时，禁止PLC主机CAN模块的接收中断，从CAN总线上接收到的通讯请求帧由CAN模块自行写入接收邮箱，整个过程不会打断主机PLC程序的执行。当PLC主机进入“输出刷新”阶段时，查询是否有CAN中断被挂起，如果有，则广播允许通讯命令，让各模块完成通讯要求，然后再进入下一个扫描周期；如果没有CAN中断被挂起，说明没有模块请求通讯，可直接进入到下一个扫描周期，节约了对各模块通讯询问的时间，有利于缩短了扫描周期。PLC主机的运行流程如图2所示。

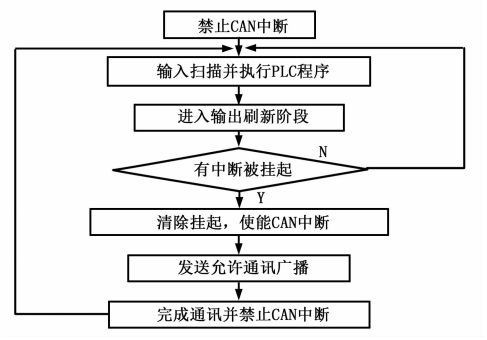

图2 PLC主机运行流程

当进行PLC程序下载通讯时，PLC主机先广播禁止任何模块请求通讯（功能码为0x0A)，然后将自身切换到编程状态(stop)，并以点对点通讯方式主动向待下载程序模块请求发送PLC程序。该通讯流程可以为程序下载提供独占式的CAN通道，有利于快速可靠下载PLC程序。完成程序下载后，PLC主机切换到运行状态（run)，开始执行新的程序。当手执编程器或者远程PC主机要求上传PLC程序时，考虑到程序员查看PLC程序的速度相对较慢，主机可以在继续运行的前提下，通过控制通讯数据量来减少通讯消耗的时间，从而不影响PLC程序的执行。本设计采用在每个“输出刷新”阶段上传10条程序，将整个程序在多个扫描周期内上传完毕。

为进一步增强帧通讯的可靠性，每进行一次新的数据传输时，发送方应立即启动一个超时定时器，在最大超时时间(50 ms）内如果没有接收到应答帧，则判断为超时，然后进行重新传输。接收模块在接收到第一个协时，也同时启动一个超时定时器，在超时时间内如果没有接收到下一帧，也判定为超时，并放弃本次传输。如果在最大超时时间内接收到了下一帧或，则刷新超时计时时间，重新进行计时。

3.2 基本帧结构的制定

通信协议是各模块有效交流，协调工作的基础。CAN多层结构协议只是对物理层和数据链路层进行了定义，所以在未定义的应用层上进行扩展是一个可行的办法。本设计参照CAN2.0B协议[10]、《电力负荷管理系统数据传输规约－2004》[11]及Modbus协议[12-13]的相关方法，并做了必要的简化，提出了“起始位＋数据长度＋源ID＋命令＋数据域＋CRC校验＋结束位”的自定义CAN扩展协议帧结构。该帧不携带数据时，字节数为8，不大于标准CAN协议一帧能携带的最大数据量，有利于提高通讯的实时性和降低通信量。另外，规定数据区可携带数据量不超过1 K字节，这样既满足了少量数据的快速传输，也避免了超长帧的使用。对帧长进行控制，可以降低传输时受干扰的概率，也减少了通讯失败重发时的数据量，达到提高抗干扰能力和降低通讯量的效果。制定的基本帧结构如表1所示。

其中，功能码0x00到0x03用于对软元件状态的读写，中

断读写的功能码的采用，是为了实现在 PLC 主机运行阶段实时读写软元件信息，加快响应速度。0x04 与 0x05 用于 PLC 程序的下载和上传，0x06 用于通讯完成的应答，以增强通讯的可靠性。0x07 用于实现软件切换主机工作状态，以提高控制的灵活性。0x08 用于开机时的硬件测试，各模块接收到主机广播的注册命令后，将自身 ID 发送给 PLC 主机以完成注册，若有模块在主机开机后接入，此模块应利用该功能码向主机请求注册。该注册过程，既检测了各模块通讯功能是否正常，也使主机可对新接入模块进行识别，从而增强了 PLC 系统可扩展能力。另外，0x09、0x0A 为广播功能码，用于 PLC 主机允许或禁止各模块请求通讯，以减少在 PLC 程序执行阶段受到的外部通讯影响，达到可靠执行 PLC 程序的目的。当 PLC 主机进入“输出刷新”阶段的时，以 0x09 广播询问是否有模块需要通讯。当进入“程序执行”阶段时，0x0A 禁止各模块向主机请求非中断型通讯。

表 1　基本帧结构

数据名	字节数	说明
起始位 0x68	1	0x68 表示一帧开头
数据长度	2	整帧数据长度
源 ID	1	0x00：PLC 主机　0x03：人机界面 0x01：手执编程器　0x04：扩展 1 0x02：远程 PC 机　0x05：扩展 2……
功能码	1	0x00：读软元件　0x06：读主机程序 0x01：写软元件　0x07：写主机程序 0x02：中断读软元件　0x08：确认/应答 0x03：中断写软元件　0x09：硬件注册 0x04：允许通讯　0x0A：禁止通讯 0x05：改写主机状态
数据区	可变	传输的数据
CRC 校验	2	数据头到数据区的校验
结束位 0x7e	1	数据帧结束

3.3　数据区协议

数据区为扩展协议的应用层，该层由帧系列域和若干个数据单元组成，以适应通讯数据特有的形式。例如，在进行 PLC 程序的上传、下载以及多个软元件状态读写时，每一条 PLC 指令或一个软元件，都具有自身完整的信息，与其他指令和软元件相互独立，均可以各自作为一个数据单元进行传输。应用层的格式如表 2 所示。

表 2　应用层格式

数据名	字节数	说明
帧系列域	1	各帧间传输的变化规则
数据单元 1	不定	一个数据点的信息
…		
…		
数据单元 n	不定	一个数据点的信息

帧系列域由两部分组成，高 6 位为帧发送计数器，用于检测是否有帧丢失，以增强增强通讯的可靠性。启动新的一次数据传输时，该计数器从 0 开始计数，每发送一帧，将其加 1。如果收方接收到前后两帧的帧计数器值不连续，或者在规定的时间内没有接收到下一帧，则判为传输丢帧或超时，然后进行通讯失败处理。低 2 位为帧首标志 FIR 和末帧标志 FIN。当需要传送的数据量超过基本帧可携带的最大值（1K 字节）时，需要分多帧传送，FIR 和 FIN 位用于标明分帧的情况，具体组合含义为：

（1）FIR＝0，FIN＝0 多帧的中间帧

（2）FIR＝0，FIN＝1 多帧的结束帧

（3）FIR＝1，FIN＝0 多帧的第一帧

（4）FIR＝1，FIN＝1 单帧

应用层中，数据单元域的数据格式根据传输数据类型的不同而各有差异。当数据为 PLC 指令时，数据单元的格式如表 3 所示。

表 3　应用层结构（PLC 指令传输）

数据名	字节数	说明
指令数据长度	1	指令的二进制编码长度
指令的数据	不定	指令的二进制编码

每条 PLC 指令经编译后，生成的二进制代码长度不一，所以在通讯协议中增加“指令数据长度”位用于传输长度信息。进行指令传送时，从第一条指令开始顺序填充数据域，如填充第 n 条指令后，数据区长度大于 1K 字节，则将第 n 条指令放入下一帧传送，并在第 $n-1$ 条指令后写入一个 0，标志不满 1K 字节，以便于解码时对有效数据的判断。

PLC 程序接收模块每接收到一个完整的 CAN 扩展帧后，需对该帧进行确认。确认帧中无数据单元，只有帧系列域，发送模块接收到应答帧后，才进入下一帧的传输。如果出现丢帧或者接收错误，则将上一个正确接收的帧的计数器值填入帧系列域，请求发送模块从该帧（断点）重新开始发送。

当待发送的数据为软元件信息时，数据单元的格式为表 4 所示。

表 4　应用层协议（软元件信息传输）

数据名	字节数	说明
软元件	1	0x00：X　0x01：Y 0x02：S　0x03：M 0x04：D　0x05：C 0x06：T
软元件编号	2	表示该中软元件的第几个
软元件值	2	写入软元件的值

一帧可同时操作多个软元件，一个软元件的信息为一个数据单元，依次排列。当为请求读取软元件状态时，数据单元不包含“软元件值”，其余与不变。当出现丢帧或传输错误时，重新进行新一轮通讯来完成通讯。

4　通讯协议的验证

数据的快速可靠传输，是通信协议适用的基本要求。对通信协议的验证，主要包括通信帧格式的验证和帧传输的稳定性。本设计的各个模块通过自带的 CAN 模块接入 CAN 网络。各个模块在开机后，将自身的 ID 写入验收滤波器的 RAM 表中，通过验收滤波器对 CAN 网络上的报文进行过滤，实现点对点通讯。

在协议测试过程中，为便于观察，将各模块收或发的数据通过串口发送到计算机上，通过串口调试助手进行显示。测试时，首先利用人机界面测试软元件设置的通讯。人机界面设置中间继电器 M10 的只为 16，定时器 T20 的值为 26，经编码打包后发送到 CAN 总线上，经观察，只有 PLC 主机接收到数据，实现了点对点的通讯。PLC 主机收到数据后，对 CAN 扩展帧检测 CRC 校验，然后按通信协议进行解包，取出源 ID、功能码、数据及其长度，通过串口调试助手查看，可知通讯完全正确。在测试有应答步骤的 PLC 程序传输时，利用手持编程器输入一段 PLC 代码，编码打包后向主机发送，主机正确接收后进行应答，手执编程器接收到应答帧后，确定程序下载成功，结束本次通讯。

5 结束语

本文为基于 ARM 与 FPGA 的小型 PLC 系统进行了 CAN 通讯设计，在进行通信协议制定时，充分考虑了协议的通用性、可扩展性以及可靠性和通讯效率，提出了一种适合各类数据传输的通讯格式，并针对各模块传送数据的不同，对应用层数据的组织形式进行了分别设计。另外，通过合理地对各模块通讯流程进行安排和选择适宜的通讯方式，有效提高了 PLC 主机工作效率和可靠性，降低了主机执行 PLC 程序时的扫描周期，从而提高了 PLC 主机的性能。经实验验证，本文设计的通讯协议满足了该小型 PLC 系统的通讯要求，且 PLC 系统具备了可扩展功能，以及远程调试、测控能力，实现了信息的分散采集和集中控制。

参考文献：

[1] 郭俊如. PLC 在工业控制中的地位 [J]. 内蒙古石油化工，2004，05：49－50.

[2] 张 嵩，术守喜，丁广乾. 基于 ARM 的嵌入式 PLC 的设计 [J]. 自动化与仪器仪表，2008，03：9－10，23.

[3] 王 祥，张太勤. 基于 CAN 总线的配电自动化系统研究 [J]. 广西工学院学报，2003，03：37－39，43.

[4] 罗功坤，刘步林，蔡启仲. 新型嵌入式 PLC 编程器的设计 [J]. 仪表技术与传感器，2011，09：64－66，69.

[5] 蒋玉新，蔡启仲，李克俭. 基于 ARM－FPGA 的 PLC 通讯与编译的设计 [J]. 微电子学与计算机，2013，06：165－168.

[6] 秦 健，李 娟，王东兴，吴嘉谓. 用于在线控监测的 PLC 扩展总线的设计 [J]. 微计算机信息，2009，28：51－52，28.

[7] 杨 慧，田 亮，田 敏. CAN 总线协议分析 [J]. 中国仪器仪表，2002，04：1－4.

[8] 郝战存. 可编程控制器发展综述 [J]. 河北工业科技，2004，02：53－56.

[9] 侯鸿佳，蔡启仲，陈文辉，等. ARM＋FPGA 组成的 PLC 结构的通信系统 [J]. 广西工学院学报，2012，01：14－19.

[10] Robert Bosch GmbH. CAN Specification Version 2.0 [S]. 1991.

[11] 国家电网公司生产运营部. Q/GDW130－2004. 电力负荷管理系统数据传输规约－2004 [S]. 2004，9.

[12] Modicon Inc. Modicon Modbus Protocol Reference Guide PI－MBUS－300. Rev. J [EB/OL]. June. 1996. /PI－MBUs－300. pdf. http：//www2. schneider－electric. com.

[13] 李月恒，项鹏，孙德辉. Linux 系统中 CAN 总线的 Modbus 通信实现 [J]. 计算机测量与控制，2011，07：1708－1710，1714.

（上接第 1864 页）

为了验证算法的有效性，分别采用基本 AGSO 算法和改进的 CAGSO 算法进行仿真，仿真 20 次，取网络覆盖率平均值进行比较，仿真结果如 6 所示。

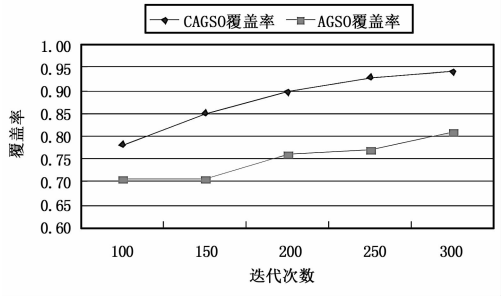

图 6 网络覆盖率比较图

表 2 策略对比图

迭代数	CAGSO 覆盖率（%）	AGSO 覆盖率（%）
100	78.33	70.32
150	85.14	70.66
200	89.51	75.89
250	92.97	76.99
300	94.11	80.87

如图 6 所示，CAGSO 算法能够快速、合理地给出网络覆盖优化方案。

4 结束语

本文提出了一种基于共轭梯度法改进的人工萤火虫算法 (CAGSO) 的 WSN 覆盖优化策略。共扼梯度法是利用已知点处的梯度构造一组共扼方向并沿着该方向进行搜索的方法，此方法经有限次迭代必达极小点。通过建立以覆盖率、节点利用率、能量均衡为准则的数学模型，然后用改进的 CAGSO 对该模型进行求最优解。仿真结果表明本文提出的改进算法能够加强萤火虫在空间的探索速度和能力，提高求解精度，有效应用于求解近似最优覆盖节点集，对传感器网络的优化效果更加有效。

参考文献：

[1] 叶 蓉，赵灵锴. 基于蚁群粒子群混合的无线传感器网络定位算法 [J]. 计算机测量与控制，2011，19 (3)：732－735.

[2] 王方石，须 德，吴伟鑫. 基于自适应阈值的自动提取关键帧的聚类算法 [J]. 计算机研究与发展，2005，42 (10)：1752－1757.

[3] 曾广朴，仲元昌，范会联. 混合无线传感网络覆盖优化的粒子群算法 [J]. 微电子学与计算机，2011，28 (8)：105－107.

[4] 贾 杰，陈 剑，常桂然. 无线传感器网络中基于遗传算法的优化覆盖机制 [J]. 控制与决策，2007，22 (11)：1289－1292.