基于 ARM+FPGA 的嵌入式安全 PLC 设计①

李明时[1,2], 马 跃[1], 尹震宇[1]

[1](中国科学院 沈阳计算技术研究所, 沈阳 110168)
[2](中国科学院大学, 北京 100049)

摘 要: 传统的 PLC 系统由于自身系统结构和处理器性能等问题, 在执行工业控制的过程中往往在执行了一定时间后系统就会发生惯性停机, 影响工业生产. 提出了基于 ARM+FPGA 高性能双处理器的嵌入式安全 PLC 结构模型, 可以大幅降低系统失效的概率, 提高工业控制可靠性. 本系统分为硬件结构和软件系统两大部分. 硬件部分采用了 1oo2D 双通道异构冗余安全体系结构, 两条通道配备有安全电路, 两个处理器之间设计有安全诊断电路, 通过交叉检测判断系统运行是否正常. 软件部分主要包括编译系统和执行系统, 编译系统将编写的 PLC 程序转换成机器可执行的代码也叫做目标代码, 再由执行系统进行目标代码的执行.

关键词: ARM; FPGA; 冗余结构; 1oo2D; 安全 PLC

Design of Embedded Security PLC Based on ARM+FPGA

LI Ming-Shi[1,2], MA Yue[1], YIN Zhen-Yu[1]

[1](Shenyang Institute of Computer Technology, Chinese Academy of Sciences, Shenyang 110168, China)
[2](University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: The traditional PLC system, due to the problems of its system structure and processor performance, in the process of the implementation in industrial control, often occurs the inertial downtime after a certain execution time, which influences the industrial production. The paper proposes the embedded security PLC structure model, which is based on ARM + FPGA dual processor with high performance, which can greatly reduce the probability of system failure, and improve the reliability of industrial control. This system is divided into hardware structure and software system of two parts. The hardware part adopts the double channel, which is equipped with a safety circuit, heterogeneous redundancy security architecture based on 1oo2d, and safety diagnosis circuit is designed between the two processors, determines whether a system running normally by cross detection. The software part mainly includes the build system and executive system, the build system writes PLC program into executable machine code which is called the target code, and then the execution system executes the target code.

Key words: ARM; FPGA; redundant structure; 1oo2D; security PLC

PLC 是一种实时性非常强的控制器, 在制造业和过程控制中占据了非常重要的位置. 经过多年的发展, PLC 系统已经比较成熟与完善, 是工业生产的核心部分. 随着 PLC 应用领域日益扩大, PLC 技术及其产品结构都在不断改进, 功能日益强大. 安全 PLC 系统已经成为当下工业控制领域最为重要的部分, 是 PLC 系统今后发展的大方向.

由于当前工业控制领域不断变化更新, 与传统概念相比更加的复杂, 存在的不确定因素更多, 所以对 PLC 控制要求也越来越高[9]. 随着嵌入式系统的不断发展, 利用系统硬件和软件资源构建嵌入式 PLC 系统有着广泛的应用前景, 具有良好的兼容性和开放性. 实时的嵌入式系统拥有增强系统运行可靠性、提高系统的开发效率、缩短系统研发周期的显著特点, 因此

① 基金项目:国家科技重大专项(2014ZX04009031)
收稿时间:2016-07-01;收到修改稿时间:2016-08-08 [doi: 10.15888/j.cnki.csa.005661]

基于实时的嵌入式系统进行安全PLC的设计已经逐渐成为当前 PLC 研发的一种主要方式.

ARM 处理器以及相似的一些性价比较高的微处理器的推出, 使得嵌入式系统得到了快速地发展, 而随着嵌入式技术的增强, 又使得基于嵌入式的 PLC 系统得到了长足的进步, 嵌入式 PLC 系统将会成为工业控制领域今后最主要的发展方向.

在现有的一些基于 ARM+FPGA 结构的 PLC 系统中, ARM 处理器负责处理相关 PLC 指令, 而 FPGA 处理器负责处理在系统执行过程中的一些逻辑, 两个处理器之间并没有进行交叉检测, 不能有效降低系统失效的概率, 提高系统安全性, 这便凸显出了本系统实际的研究意义与价值.

1　安全PLC

安全 PLC 是指系统本身或外接设备在系统运行的过程中出现执行问题或当机时, 仍然可以向处理器做出正确的反馈并且及时切断控制连接的可编程逻辑控制系统. 与普通 PLC 不同, 安全 PLC 不仅可以提供普通 PLC 的基本功能, 同样可以实现更为关键的安全控制功能.

本文中安全 PLC 主要通过以下技术创新点进行 PLC 系统安全性的提升:

① 设计有安全控制功能结构: 使用异构冗余处理结构, 完成安全控制功能.

② PLC 安全状态自检测: 包括线路检测、CRC 校验、错误自检以及双处理器交叉检测等.

③ 安全的编程环境: 针对安全 PLC 逻辑控制功能要求, 设计基于 IEC 61131-3 编程语言的编译器, 提供 PLC 辅助编程工具, 以满足安全控制功能时的逻辑控制功能需求.

④ PLC 硬件的功能安全设计: 采用 ARM+FPGA 的高性能双处理器 , 两条独立的通道并联接线, 配备有独立的安全电路, 两个处理器之间设计了一条安全诊断电路, 处理器通过诊断电路进行交叉检测, 进而可以判断系统运行的是否正常.

安全 PLC 主要是为安全级别较高的电子机器和工业设备而设计的, 用于对关键设备的控制和对其进行安全地使用. 提高PLC 系统的 SIL 安全等级可以大幅提高系统内部各个部件在自身安全周期中工作的可靠性和稳定性, 这对于工业控制创新和发展具有重要意义.

2　安全PLC的整体结构设计

本设计研究的是基于 ARM+FPGA 的双处理器异构冗余结构的嵌入式安全 PLC 系统, 分为 PLC 硬件结构和 PLC 软件系统两大部分. 安全 PLC 具备独立看门狗复位电路, 对信号的收集、分析处理和输出过程均使用了双核冗余结构的方式. 通过互为相异冗余的双数据处理系统, 实现基于冗余采集处理的安全控制系统, 满足数控系统的安全控制要求.

在安全 PLC 系统中, 两个处理器与 I/O 之间分别设计有各自的安全通信线路, 将使用 CRC 校验对安全处理器和安全 I/O 之间的通信进行诊断. 因此, 不仅要检查接收的数据是否等于发送的数据, 而且要检查数据的变化. 安全 PLC 功能结构主要包括以下四部分, 详见图 1-PLC 安全控制功能结构图.

① 双通道安全输入. 每一个外部输入都采取双通道输入方式连接到两个处理器.

② 双通道处理机制. 安全 PLC 内部使用了互为冗余的微出理器, 同时对每个安全功能进行控制和监控, 形成并联通道, 并行处理同一个安全过程. 多个监控系统互为冗余, 只有系统检测到该信号正常且允许输出.

③ 双通道安全输出. 安全 PLC 的输出电路内部使用了冗余结构, 对每一个输出节点进行更加准确稳定的控制, 以保证系统输出的安全性.

④ 安全诊断电路. ARM 处理器和 FPGA 处理器分别控制两条线路, 两条线路并连接线, 两个处理器之间设计有安全诊断电路, 在 PLC 系统进行安全控制的过程中, 两个安全处理器之间进行数据交互(如配置信息, 关键常量, 数据大小, 数据处理结果等)以完成交叉检测, 检查两条通道的处理结果是否一致, 从而进一步判断目前系统运行的是否正常[5].

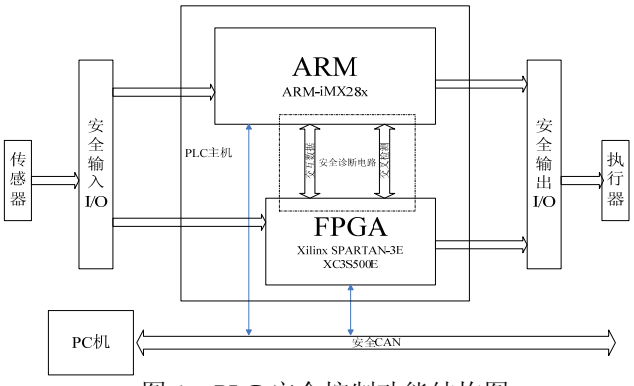

图 1　PLC 安全控制功能结构图

3 安全PLC硬件结构设计

硬件结构是整个安全 PLC 系统的可执行前提和安全控制基础, 为开发系统和运行系统提供了平台.

3.1 ARM+FPGA 处理器的选用

ARM 和 FPGA 处理器是本系统硬件结构的核心部分. 从本系统可以实际应用到的领域、开发的成本和开发的难易程度等因素来考虑, 本系统以 ARM-iMX28x 和 Xilinx SPARTAN-3E XC3S500E 芯片作为处理器.

iMX28x 处理器主频 454MHz, 支持 DDR2 和 NAND Flash, 并提供多达 5 路 UART、1 路 I2S 接口、1 路 I2C、1 路 SPI、1 路 USB Host 接口、4 路 12bit ADC、1 路 USB OTG 接口、1 路 10/100M 以太网接口、1 路 SDIO、支持电容式液晶屏和电阻式触摸屏、满足信息的采集以及更高水平的工业控制应用.

XC3S500E 芯片的等效逻辑门数为 50 万, 等价于 10476 个 LCs, 具有多达 158 个用户 I/O(含 65 个差分对 I/O), 73kB 的分布式 RAM, 360kB 的 RAM 和 20 个专用乘法器.

3.2 异构冗余的双数据处理系统

1oo2D 冗余结构是具有诊断功能的双通道处理系统, 结构内部具有两重 1oo1D 系统, 两条线路以并联的方式进行连接, 并拥有各自的控制线路, 提供了 1oo2 安全功能, 如图 2 所示.

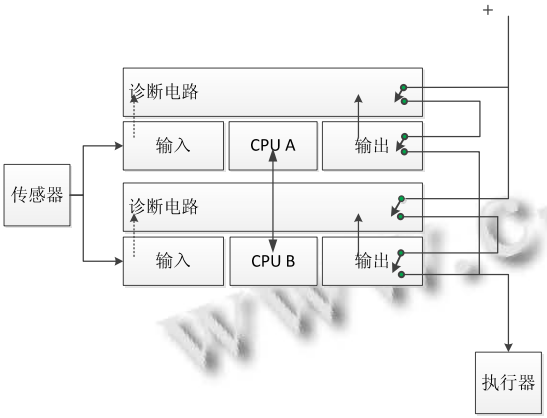

图 2 1oo2D 冗余结构

1oo2D 安全控制系统要求具有在一次错误发生时能降级到 1oo1D 系统的能力, 因此, 两个主控制模块之间要能够通过通信和信号判断对方模块的运行状态.

1oo2D 冗余安全系统两个通道独立运行, 使用软件进行自测试和自诊断, PLC 根据不同的系统状态, 进入故障安全模式或将故障检测出来. 使用软件检测硬件时, 从现场至处理器, 能够在误动作发生之前就可以发现它们. 在系统出现问题后, 系统可以降级到 1oo1D 的系统继续运行, 确保出现故障时整个系统的完整性. 七种冗余结构的安全性详见表 1[2].

表 1 冗余结构安全性

冗余结构	一次降级	二次降级	安全性	可用性
1oo1	系统停机	\	低	低
1oo2	系统停机	\	高	低
2oo2	1oo1	系统停机	低	高
2oo3	1oo2	系统停机	高	高
1oo1D	系统停机	\	低	高
1oo2D	1oo1D	系统停机	高	高
2oo4D	1oo2D	1oo1D	高	高

3.3 独立看门狗复位电路

使用独立的看门狗复位电路来监控设备是否正常及不正常时重启设备. 对于嵌入式 PLC 系统, 设备可能出现死机等现象. 但是, 这些设备不可能随时有工作人员监控, 因此一旦发生问题, 设备需要自行重启.

独立看门狗时钟由看门狗自身硬件提供, 不受 PLC 主时钟的影响. 在正常工作时, 检测 ARM+FPGA 产生的喂狗信号是否在一定时间内翻转, 如果喂狗信号产生翻转, 定时器的计数清零, 重新计时. 如果喂狗信号没有产生翻转, 则产生复位信号, 上述过程如此重复循环. 看门狗电路工作原理详见图 3.

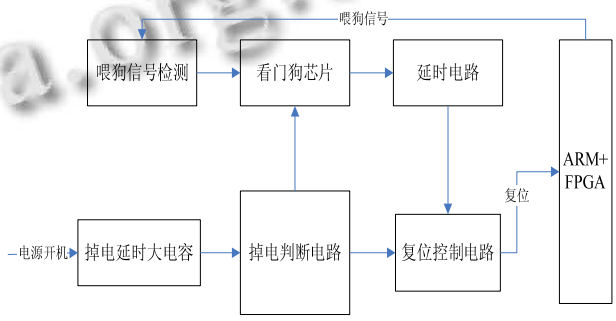

图 3 看门狗复位电路

4 安全PLC软件系统设计

安全 PLC 软件系统由编译系统和执行系统两大部分组成. 编译系统将编写的 PLC 源程序编译成与硬件平台相关的机器可执行代码, 执行系统通过执行开发系统中生成的可执行代码, 最后将正确处理后的信号输出到控制设备完成对机械设备的安全控制.

4.1 软件系统模块设计

安全 PLC 软件系统如图 4 所示包含编译系统和执行系统两大部分. 编译系统包含“程序编辑模块”、“程序编译、调试模块”以及“通信接口模块”三个模块[14], 执行系统包含“通信接口模块”、“运行内核模块”、以及“I/O 接口模块”三个模块.

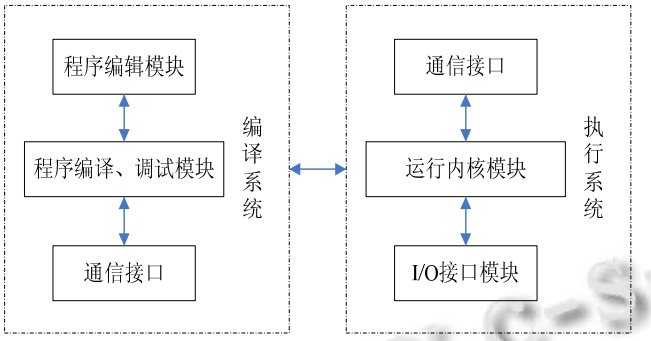

图 4　安全 PLC 软件系统结构图

4.2 CRC 校验

使用 CRC 校验对安全 CPU 和安全 I/O 之间的通信进行诊断, 利用除法及余数的原理来做错误侦测.

在实际进行校验时, 发送设备计算出 CRC 值并随数据一同发送给接收设备, 接收设备对收到的数据计算 CRC 值并与收到的 CRC 值进行比较, 如果两个 CRC 值不相同则说明通讯过程出现错误, 如果两个 CRC 值相同则说明通讯正常. 不仅要检查接收的数据是否等于发送的数据, 而且要检查数据变化的情况.

在进行 CRC 检验时, 发送装置与接收装置需要事先设定一个好除数也就是所谓的生成多项式, 一般记作 Z(x), 生成多项式的最高位与最低位必须是 1. 通常循环冗余校验的值是 8 位、16 位或 32 位的整数, 常用的 CRC 码的生成多项式有:

① 8 位: $CRC8=X^8+X^5+X^4+1$

② 16 位: $CRC16=X^{16}+X^{15}+X^5+1$

③ 32 位: $CRC32=X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X^1+1$

CRC 校验工作过程如图 5 所示.

在进行 CRC 计算前首先将代表发送数据的多项式 A(x)乘以 x^n, 其中 n 次幂是生成多项式 P(x)的最高次幂. 因为使用的是二进制乘法, 所以 $A(x)*x^n$ 的意思就是将 A(x)向左移 n 位, 用来存放余数 P(x), 所以实际发送的数据就变为 $A(x)* x^n+P(x)$. 在进行 CRC 计算时, 使用二进制也叫做模 2 运算法, 即加法不进位, 减法不借位, 这种算法的本质意义就是两个操作数进行逻辑异或运算[13].

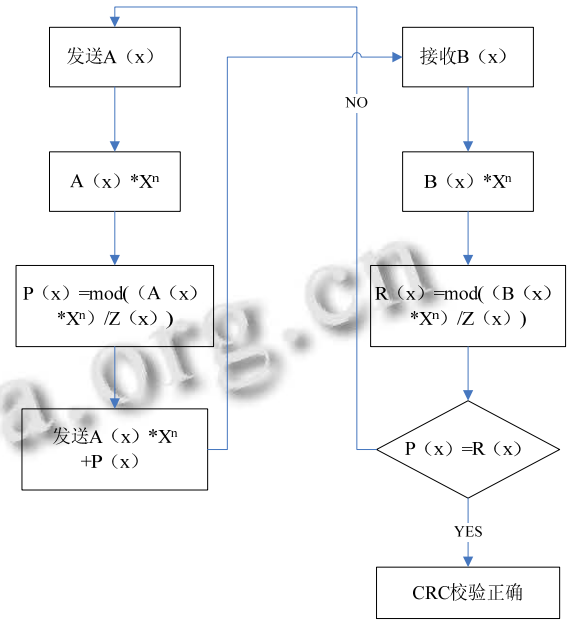

图 5　CRC 校验流程

5　实验方案

5.1 实验设计

本实验将从 CPU 占用率、内存占用率以及系统运行的实时周期这几方面对系统的性能进行验证.

① 在 LINUX 系统下运行 PLC 系统, 输入 top 指令查看当前 ARM 处理器和 FPGA 处理器的所在开发板的 CPU 占用率和内存占用率.

所使用开发板内存为 512MB, 如图 6 所示, 当前内存占用为 3868B, 内存占用率为 0.7%, CPU 占用率为 14%. 可见本 PLC 系统对内存的占用非常少, 对 CPU 的占用也不高, 可以满足绝大多数情况下的使用需要.

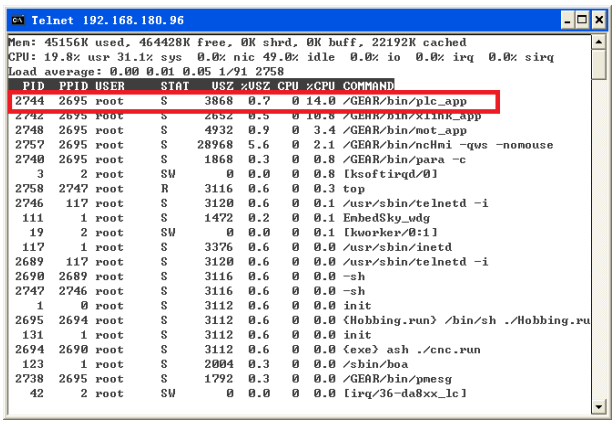

图 6　CPU 和内存占用率

② 计算 PLC 系统的实时周期.

使用梯形图编辑软件编写长度约为 500 行的逻辑指令，使用二进制转换插件将 LAD 文件转换为二进制文件，放入系统进行执行. 在 PLC 主循环执行之前，首先获取当前的系统时间，在 PLC 执行第一次循环之后，再次获取系统当前时间，通过前后两个时间可以算出进程的执行周期. 经过计算，完成此逻辑指令用时约为 2ms，如果将逻辑指令的长度提高到 1300 行左右，那么计算可得完成逻辑指令用时约为 4ms，实验流程如图 7 所示.

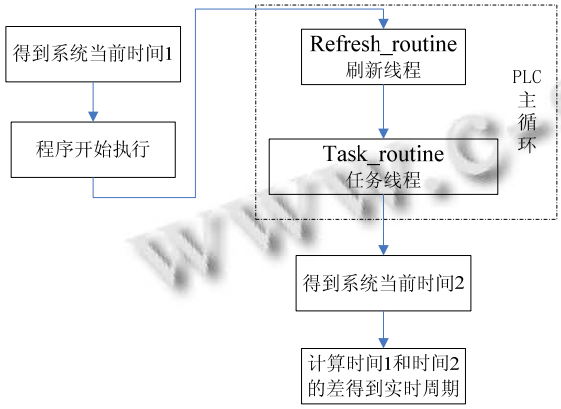

图 7 实时周期实验流程图

5.2 实验结论

通过实验结果可以看出本系统具有良好的综合性能，可以正确处理需要执行的逻辑指令，在稳定性与运行速度方面都显示出了良好的执行结果.

6 总结

本系统使用 ARM+FPGA 的双处理器结构，设计研究了基于 1oo2D 异构冗余模型的安全 PLC 系统，给出了安全 PLC 系统主要的安全控制功能结构、硬件系统的设计、编译系统的模块设计以及看门狗复位电路、CRC 校验等关键技术在本系统中的详细设计.

最近几十年来，一部分工业生产事故的原因是由于计算机控制系统的当机或错误执行所导致的，引起了人员的伤亡和设备财产的损失. 这些事件也提醒着国家、相关技术人员以及普通百姓，要强化对生产过程的危险性、建立工业安全流程的意识. 由于目前工业控制领域的先进化和高复杂化，传统 PLC 已经不能满足高安全性、高可用性的要求，本系统提出的对于提高 PLC 安全性的技术创新对于安全控制系统的发展有着重要的意义.

参考文献

1 季照平.基于单片机 ARM 嵌入式技术的数控系统的开发研究.轻工科技,2015,(11):47–68.
2 林通.基于 FPGA 的安全 ePLC 的研究[硕士学位论文].杭州:杭州电子科技大学,2015.
3 郑凌.基于 CPU_FPGA 的异构多核系统设计及并行编程模型研究[硕士学位论文].西安:西安电子科技大学,2014.
4 刘志颖,郑松.异构三重冗余控制系统的设计与可靠性评估.电气技术,2014,(4):54–59.
5 宋岩.基于 1oo2D 体系结构的高可用安全仪表.信息与控制,2013,42(4):521–528.
6 刘建康.基于 ARM_FPGA 的嵌入式数控系统硬件设计[硕士学位论文].哈尔滨:哈尔滨工业大学,2013.
7 任慰.以实时操作系统为中心的嵌入式系统平台化设计研究[博士学位论文].武汉:华中科技大学,2013.
8 栾朋.基于嵌入式 ARM 的 PLC 设计与实现[硕士学位论文].沈阳:沈阳理工大学,2013.
9 王麟琨,方晓时,王春喜.功能安全 PLC 标准化进展及技术概述.中国仪器仪表,2012,(8):40–45.
10 张兰洋.浅析安全 PLC 的性能和结构.科技向导,2012,(6):153.
11 韩雪涛,韩广兴,吴瑛.PLC 梯形图及语句表.北京:人民邮电出版社,2012.
12 黄金柱.异构双处理器系统功能安全设计方法研究[硕士学位论文].武汉:华中科技大学,2012.
13 王志学,麦晓冬,符睿.循环冗余校验原理分析及硬件实现.科技信息,2011,(7):44–81.
14 黄晓斌.基于嵌入式 Linux 的软 PLC 系统设计与实现[硕士学位论文].长沙:中南大学,2008.
15 华镕.常规 PLC 和安全 PLC 的区别.仪器仪表标准化与计量,2007,(4):6–9.
16 John KH, Tiegelkamp M. IEC 61131-3: Programming Industrial Automation Systems. Berlin: Springer-Verlag, 2010.