

基于 FPGA 的双 CPU 容错控制器设计

李登静, 范守文

(电子科技大学机械电子工程学院, 成都 610054)

摘要: 基于冗余容错思想, 设计基于现场可编程门阵列的双 CPU 容错控制器。该容错控制器在故障情况下可通过回溯重载进行故障判定和系统性能恢复, 控制器控制律在传感器失效时能进行自我重构。仿真结果表明, 该容错控制器通过冗余 CPU 的切换和控制律的重构实现了系统故障情况下的容错纠错功能。

关键词: 容错; 重构; 现场可编程门阵列

Design of Dual CPU Fault-tolerant Controller Based on FPGA

LI Deng-jing, FAN Shou-wen

(School of Mechatronics Engineering, University of Electronic Science and Technology of China, Chengdu 610054)

【Abstract】 Based on the idea of redundant fault-tolerance, this paper designs a dual CPU fault-tolerant controller based on Field Programmable Gate Array(FPGA). It can detect faults and resume system performance through checkpoint reload in case of failure, and control law can self-reconfigure when sensor faults occur in the system. Simulation results show that fault-tolerance and fault rectification functions can be achieved by switching the redundant CPU and reconfiguring the control law in case of system failure.

【Key words】 fault-tolerance; reconfiguration; Field Programmable Gate Array(FPGA)

1 概述

随着半导体技术的发展, 现场可编程门阵列(Field Programmable Gate Array, FPGA)技术在控制领域的应用越来越广, 与专用集成电路(ASIC)技术相比, 基于 FPGA 的嵌入式系统具有设计和开发周期短、设计成本和风险低、集成度高、维护和升级方便、可靠性高等特点, 同时, FPGA 所具有的并行运算能力和可重构性使其在解决诸如直线插补运算、高速加工、可重构性等问题中显示出了独特的优势^[1-2], 其作为嵌入式处理器, 在嵌入式系统设计领域已占据越来越重要的地位。

容错技术是提高系统可靠性的重要技术之一。冗余容错技术是利用硬件或软件冗余提高系统可靠性的一种方法, 是系统稳定、可靠、有效、持续运行的重要保证, 其广泛应用于过程控制、机器人系统、航空航天测试与控制系统、工业自动化等控制领域。本文基于冗余容错思想, 结合 FPGA 的特点和优势设计了双 CPU 容错控制器。

2 容错控制器结构和工作原理

图 1 为基于 FPGA 的容错控制器, 其内部由通信模块、电机控制模块、计数器模块、ROM 模块、I/O 模块、双 CPU 仲裁结构等构成。双 CPU 是控制器的核心, 它通过通信模块与外部主机进行数据交换, 并根据程序执行的结果输出相应的控制信号给电机控制模块。ROM 模块用于储存开机自检程序和系统执行指令, 存储逻辑用于储存控制过程中的回溯信息和 CPU 与外部主机交换的数据。电机控制模块的输出连接到实际的芯片引脚上, 以驱动相应的功率驱动电路。计数器模块用于对编码反馈信号进行计数, 并将结果传输给 CPU 进行处理。I/O 模块用于容错控制器与外围器件的连接。各功能模块集成在控制器内部, 因此, 硬件电路的结构较为稳定。

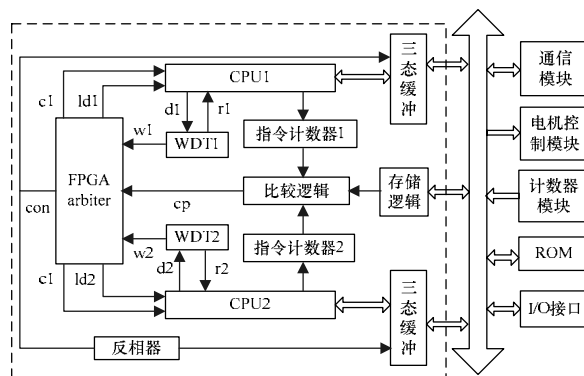


图 1 容错控制器内部结构

2.1 双 CPU 仲裁结构与故障恢复

CPU 故障包括瞬时故障和永久故障^[3], 本文控制器具有的故障恢复机制能对 2 种故障进行判断和恢复, 故障的恢复由状态机实现。图 1 虚线部分为双 CPU 仲裁结构。互为备份机的 CPU1 和 CPU2 具有相同的工作机制, 它们在 FPGA arbiter 的控制下工作。现以 CPU1 为工作机对图示加以说明: (1)CPU1 正常运行时, 向 WDT1 发出周期性脉冲信号 d1, 同时, 指令计数器 1 不断对 CPU1 执行的指令计数, 且当指令计数器溢出时, 当前执行指令处的环境参数(回溯信息)将被存入回溯点(checkpoint)存储逻辑。(2)当 CPU1 故障时: 1)WDT1 发出复位信号 r1(令 CPU1 复位)和报告信号 w1(通知 FPGA arbiter 已发生错误); 2)故障点参数被存储于存储逻辑;

基金项目: 国家自然科学基金资助项目(50775027)

作者简介: 李登静(1981-), 男, 硕士研究生, 主研方向: 基于 FPGA 的容错纠错技术; 范守文, 博士、教授、博士生导师

收稿日期: 2009-05-20 E-mail: lidengjing@163.com

3)指令计数器 1 重置初值;4)FPGA arbiter 在收到错误报告 w1 后立即发出信号 ld1 使 CPU1 重载前一回溯点参数。然后 CPU1 重新执行回溯点指令,当执行到故障点(指令计数器 1 计数值与故障点时刻的执行指令数相等时,比较逻辑发出信号 cp)时,如果 WDT1 工作正常,则认为 CPU1 发生了瞬时故障,系统将正常运行,如果 FPGA arbiter 再次收到 WDT1 发出的错误报告信号 w1,则认为 CPU1 发生了永久故障, FPGA arbiter 立即发送控制信号(c1 和 c2)切换 CPU1 和 CPU2,同时,对三态缓冲发送控制信号 con,禁止 CPU1 与内部总线进行数据和指令传送,而使能 CPU2 与内部总线的通信。

2.2 时钟同步

在本切换控制系统中,信号 w1, w2 由 WDT1 和 WDT2 分别发出,它们对于 FPGA arbiter 来说是异步输入信号,由于逻辑器件内部延时等因素的影响,2 个信号同时发生跳变的瞬间可能产生“竞争与冒险”,使 FPGA arbiter 的输出信号中产生毛刺,并且毛刺信号会不断累积,从而对系统产生不稳定的控制作用,因此本系统设计采用“信号同步法”,即由 FPGA arbiter 发出全局同步时钟信号 clk,使 w1, w2 同步输入 FPGA arbiter 中,以消除电路中的毛刺信号^[4]。

2.3 系统性能和故障恢复时间

系统性能判断标准是 CPU 执行指令的时间与系统完成该指令所消耗的总时间之比。对于本系统而言,系统除正常执行指令外,每次进行回溯存储和故障恢复时的状态转移都要消耗系统时间,使系统性能下降。假设指令计数器的长度为 L ,每次回溯存储 M 字,消耗 M 个时钟周期,每次状态转移消耗 S 个时钟周期,执行每条指令平均时间为 t ,则系统性能 $P = Lt / (Lt + M + 2S)$,系统故障恢复时间(T)为上次回溯点到故障时指令(X)的执行时间与故障恢复状态转移时间之和,即 $T = Xt + 2S, 1 \leq X \leq L$ 。假设 $M = 100, t = 1, S = 5, X = L/2$,则 $P = L / (L + 110), T = L/2 + 10$ 。图 2 为指令计数器长度 L 与系统性能 P 的关系,可以看出,在 $L = 1000$ 时,系统性能达到 90%,随后,系统性能增长缓慢。图 3 为指令计数器长度 L 与故障恢复时间 T 的关系,两者呈线性关系。

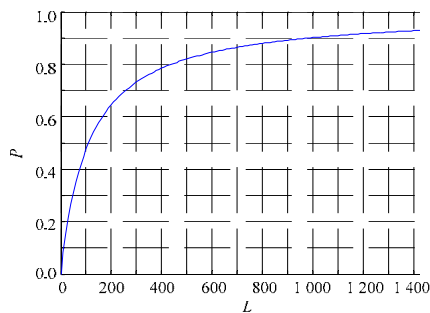


图 2 指令计数器长度 L 与系统性能 P 的关系

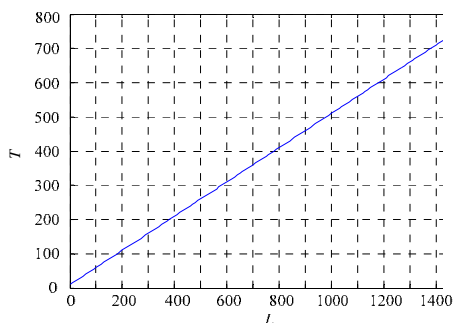


图 3 指令计数器长度与故障恢复时间的关系

综合 2 项实验结果, $L = 1000$ 时, $T = 510$, 可达到系统性能与恢复时间的平衡点。

3 控制律重构

3.1 重构方法

本文对图 4 所示的单输入单输出闭环反馈控制系统传感器失效重构方法进行研究,针对此系统,文献[5]提出采用其他完好控制回路分摊失效传感器控制作用而进行重构的方法。本文提出用前一级反馈回路补偿失效传感器控制作用的重构方法,此方法计算简单,且适用于最小相位系统和非最小相位系统。

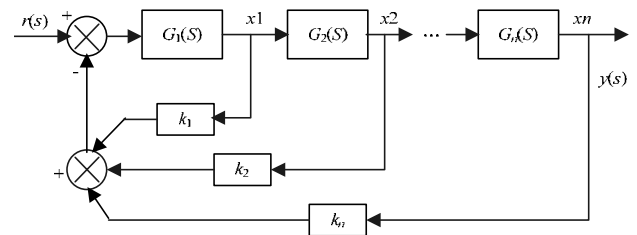


图 4 单输入单输出闭环反馈控制系统

如图 4 所示, $G_i(s)$ 是开环传递函数, $k_i, i = 1, 2, \dots, n$ 是传感器增益。设系统中第 i 个传感器失效,则重构控制率为

$$k_m' = k_m, m = 1, 2, \dots, i-2, i+1, i+2, \dots, n \quad (1)$$

$$k_{i-1}' = k_{i-1} + G_i(s)k_i \quad (2)$$

即第 i 个传感器失效时只需重构第 $i-1$ 个反馈增益,其余反馈增益保持不变。如果 $i = 1$,即第 1 个传感器失效,则重构控制律为

$$k_n' = k_n + k_1 / G_2(s)G_3(s) \cdots G_n(s) \quad (3)$$

$$k_m' = k_m, m = 2, 3, \dots, n-1 \quad (4)$$

证明:失效前,系统的闭环传递函数为

$$\varphi(s) = y(s)/r(s) = G_1(s)G_2(s) \cdots G_n(s) / (1 + G_1(s)k_1 + G_1(s)G_2(s)k_2 + \cdots + G_1(s)G_2(s) \cdots G_n(s)k_n) \quad (5)$$

当第 i 个传感器失效后,其重构闭环传递函数为

$$\begin{aligned} \varphi'(s) = & G_1(s)G_2(s) \cdots G_n(s) / (1 + G_1(s)k_1 + \cdots + \\ & G_1(s)G_2(s) \cdots G_{i-2}(s)k_{i-2} + G_1(s)G_2(s) \cdots G_{i-1}(s)k_{i-1}' + 0 + \\ & G_1(s)G_2(s) \cdots G_{i+1}(s)k_{i+1} + \cdots + G_1(s)G_2(s) \cdots G_n(s)k_n) \end{aligned} \quad (6)$$

令 $\varphi(s) = \varphi'(s)$,由式(5)和式(6)得

$$k_{i-1}' = k_{i-1} + G_i(s)k_i$$

因此,式(2)得证。

当第 1 个传感器失效时,没有前级反馈回路进行补偿,可以采用第 n 级反馈回路进行补偿。经计算,重构律为

$$k_n' = k_n + k_1 / G_2(s)G_3(s) \cdots G_n(s)$$

因此,得式(3)。

3.2 设计实例

对图 4 的反馈系统取 $n = 5$,得到五阶控制系统,设系统传递函数分别为

$$G_1 = 2.5 / (1.25s + 1), G_2 = 2 / (2s + 1), G_3 = 1.6 / (s + 1),$$

$$G_4 = 1.25 / (0.625s + 1), G_5 = 4 / (2.5s + 1)$$

传感器增益分别为

$$k_1 = 5.850, k_2 = 25.555, k_3 = 27.800,$$

$$k_4 = 14.114, k_5 = 10.764$$

当 $s = 0$ 、 k_1, k_2, k_3, k_4, k_5 分别失效时,重构反馈增益见表 1。

表 1 传感器失效重构增益结果

	k_1	k_2	k_3	k_4	k_5
k_1 失效	0.000	25.555	27.800	14.114	10.764
k_2 失效	56.960	0.000	27.800	14.114	10.764
k_3 失效	5.850	70.035	0.000	14.114	10.764
k_4 失效	5.850	25.555	45.443	0.000	10.764
k_5 失效	5.850	25.555	27.800	57.170	0.000

以 k_3 失效为例,进行了仿真分析,结果如图 5、图 6 所示。可以看出,本文重构方法对应的响应曲线更早达到稳态值,且响应过程更接近于原系统的响应过程,容错性能优于文献[5]所述的重构方法。

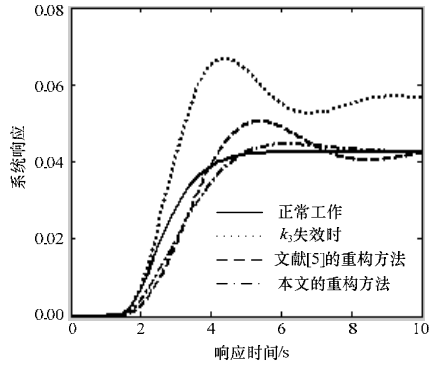


图 5 系统阶跃信号响应曲线

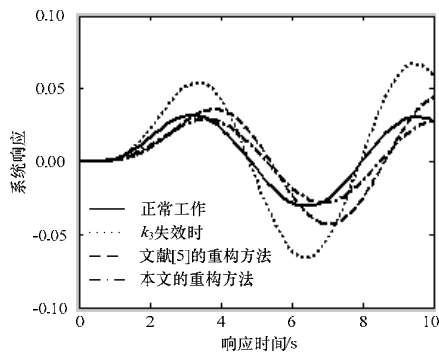


图 6 系统正弦信号响应曲线

4 仿真实验

本设计采用 Altera 公司 Cyclone 系列的 EP1C6Q240C8 芯片,使用 QuartusII 作为 EDA 设计工具,应用超高速集成

电路硬件描述语言 VHDL 进行设计输入。其仿真波形如图 7 所示。仿真中,利用信号 w1, w2 出现的低电平分别模拟 CPU 出现的故障。从仿真图可以看出,双 CPU 的切换出现在故障控制器重新执行到故障点而再次出现故障报告信号后。

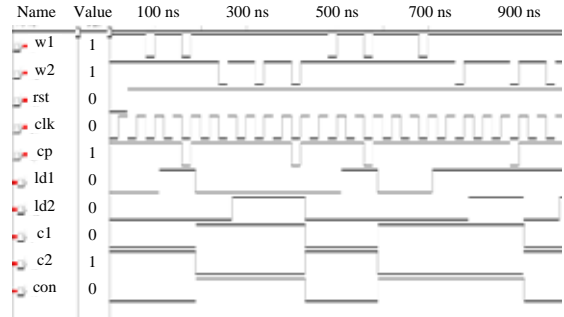


图 7 仿真波形图

5 结束语

双 CPU 结构的 FPGA 容错控制器能以较少的硬件开销使系统获得较高的可靠性,且控制器具有有效的故障判别功能和故障恢复机制,可使系统在故障情况下消耗较短的故障恢复时间,保持较高的系统性能。此外,本文针对控制系统传感器故障提出了一种新的控制律重构方法,最大限度地对失效传感器的控制作用进行了补偿,改善了控制器的容错性能。

参考文献

- [1] Oldknow K D, Yellowley I. Design, Implementation and Validation of a System for the Dynamic Reconfiguration of Open Architecture Machine Tool Controls[J]. Machine Tools & Manufacture, 2001, 41(6): 795-808.
- [2] Osornio-Rios A R, Romero-Troncoso R J, Herrera-Ruiz G. The Application of Reconfigurable Logic to High Speed CNC Milling Machines Controllers[J]. Control Engineering Practice, 2008, 16(6): 674-684.
- [3] 彭和平, 时晨. 面向空间应用的双核容错微处理器的研究与实现[J]. 宇航学报, 2007, 28(1): 188-193.
- [4] 宋威, 方聪明. 多 FPGA 设计的时钟同步[J]. 计算机工程, 2008, 34(7): 245-247.
- [5] 葛建华, 孙伏贤. 状态反馈控制系统的容错控制策略[J]. 自动化学报, 1991, 17(2): 191-197.

编辑 张帆

(上接第 237 页)

5 结束语

业务寻址与交换技术是基于双网可视电话的公共信息服务平台技术的重要组成部分^[5],在广东省农村信息化的示范区建设中,基于双网可视电话的公共信息服务平台得到了规模应用,其组网方式灵活,业务安全可控。实践证明本文论述的双网融合可视电话的业务寻址与交换技术适用于电信商业运营的层次组织及业务代理架构。

参考文献

- [1] 廖永红, 江虹. 双网多媒体可视电话研制报告[R]. 广州: 广东

轻工职业技术学院, 2008.

- [2] 胡颖. 基于 SIP 协议多媒体软电话的研究与实现[D]. 西安: 西安电子科技大学, 2007.
- [3] 董世容, 邓亚平, 余萍. 适合家用的可视电话技术方案[J]. 重庆邮电学院学报, 2006, 18(6): 784-787.
- [4] 廖永红, 李洛. 高离散 P2P 会议模型带权基因衍生算法[J]. 计算机工程与应用, 2008, 44(20): 124-128.
- [5] 廖永红, 李洛. 构建嵌入式多媒体电话的泛应用框架[J]. 计算机工程与设计, 2008, 29(24): 6264-6268.

编辑 张帆