

文章编号:1001-9081(2009)08-2143-03

嵌入式高可靠性异构双机冗余系统的设计

满梦华,原 亮,丁国良,巨政权,宋 亮

(军械工程学院 计算机工程系,石家庄 050003)

(manmenghua@hotmail.com)

摘 要:以复杂电磁环境下嵌入式控制系统的可靠运行作为设计目标,提出了基于 ARM 和 FPGA 的可重构双机并行处理模型,以期运用备份策略保证系统可靠性。进而,利用马尔可夫过程模型分析此系统的抗电磁干扰能力,证明本模型能够有效地提高系统可靠性。

关键词:可靠性;异构;ARM;FPGA;冗余;热备份;马尔可夫过程

中图分类号: TP303 **文献标志码:** A

Embedded dual-computer redundant system design with high reliability and heterogeneous structure

MAN Meng-hua, YUAN Liang, DING Guo-liang, JU Zheng-quan, SONG Liang

(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang Hebei 050003, China)

Abstract: To realize reliable operation of embedded control system under complicated electromagnetic environment, a reconfigurable dual-computer parallel model based on ARM and FPGA was proposed. The standby strategy was adopted to guarantee system reliability. The anti-electromagnetic interference ability of the system was analyzed using Markov process model.

Key words: reliability; heterogeneous structure; ARM; FPGA; redundancy; hot-standby; Markov process

0 引言

随着电子技术的飞速发展,大规模集成电路及嵌入式计算机在武器装备中得到广泛应用,已成为现代武器装备正常运转的基石。然而,随着各种军用电磁辐射体、高功率微波武器以及强摧毁、高破坏性武器的出现,使战场电磁环境变得十分复杂。这使高科技武器装备对嵌入式控制系统的效率、可靠性、安全性提出了更苛刻的要求^[1]。在提高系统可靠性和安全性方面,避错设计和容错设计是两项关键技术^[2]。借鉴容错设计良好的有效性和可行性^[3],本系统利用异构冗余模型实现容错技术,设计了一种嵌入式高可靠性异构双机冗余系统。

1 系统体系结构

鉴于不同制作工艺芯片抗电磁干扰能力的差异性,系统采用 AISC 制作工艺的 ARM 芯片和 FPGA 制作工艺的 ALTERA EP2C35 芯片作为两个子系统的处理核心,实现异构冗余模型,互为备份,互相查错,并行工作^[4],提高系统整体的可靠性和抗电磁干扰能力,如图 1 所示。

ARM 子系统以 S3C2440 嵌入式处理器为核心,包括独立的 SDRAM、FLASH 以及外设接口,能够独立高效地运行。FPGA 子系统以 CycloneII EP2C35 为核心,包括独立的 SDRAM、FLASH、串行配置芯片 EPCS64 以及外设接口,可以运行自主知识产权电路模块,或者运行二次开发的 NiosII 处理器系统,具有较高的灵活性^[5],其物理结构如图 2 所示。

两子系统可以互不干扰地独立并行运行相同的任务,其中一个作为主机系统掌握整个系统的控制权,另一个作为备

机系统来实现冗余备份,它们互为在线监测模块,确保系统的可靠运行。为了提高系统整体的可靠性,在体系结构的设计中实现了下面三种在线监测方法。

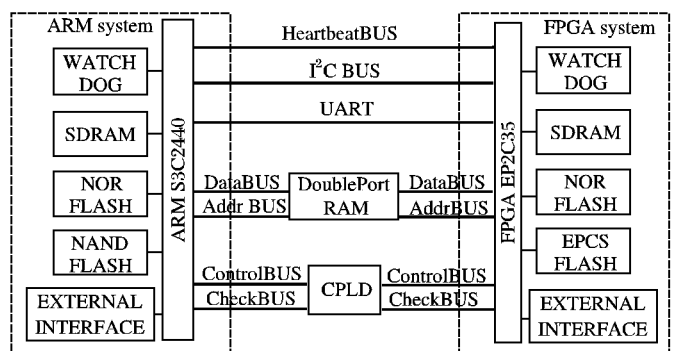


图 1 异构双机冗余系统体系结构

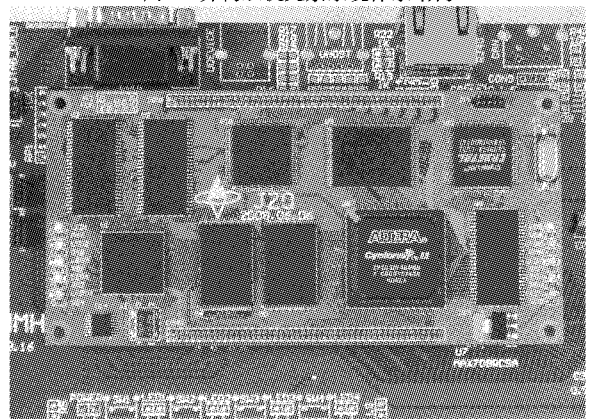


图 2 双机系统实物图

收稿日期:2009-03-04。 基金项目:国家 863 计划项目(2007AA01Z454);国防科技重点实验室基金项目(9140C8702020803)。

作者简介:满梦华(1984-),男,河北沧州人,硕士研究生,主要研究方向:智能检测与诊断; 原亮(1955-),男,山东青岛人,教授,主要研究方向:智能检测与诊断。

1.1 自监视定时器

在每个子系统的设计中都包括有自监视定时器,即“看门狗”电路。系统上电自检通过后,此定时器会自动启动,它要求系统在规定的时间内更新监视定时器中的计数值。否则,监视定时器会自动复位本地子系统,同时通过 CPLD 中的报警模块向另一个子系统通报故障。如果发生故障的是主机系统,则备机系统接管整个系统,并通过切换模块切换系统输出。此后,正常运行的子系统监测故障子系统的复位情况,如果没有复位成功,则对故障子系统进行断电操作,确保系统的安全性。

1.2 “心跳”总线

两个子系统之间通过周期性交互的数据来判断对方工作是否正常,实时地监听对方的“心跳”信号^[6]。本系统设计了专用的“心跳”总线连接两异构子系统,它们定时向对方发送自己的“心跳”信号。一旦某个子系统在系统预先规定的时间内没有检测到对方发送的“心跳”信号,就认为对方发生了故障。当主机系统发生故障时,备机系统接管系统控制权,升级为主机系统,切换系统输出,复位故障子系统,甚至可以对故障子系统进行断电操作。

当“心跳”总线本身发生物理故障,或受到电磁干扰而发生紊乱时,两子系统就不能正确地判断对方的工作状态。一种情况是两子系统都检测不到对方的“心跳”信号,备机系统就会错误地切换系统的控制权,即“误切换”。另一种情况是备机系统检测到的“心跳”信号不是来自主机系统而是来自其他干扰,备机系统不会响应主机系统的故障而不会切换系统的控制权,即“不切换”。针对以上两种问题,系统设定备机系统“心跳”周期大于主机系统的“心跳”周期,这样主机系统就会提前处理备机系统“心跳”停止的故障,使备机系统没有机会切换系统控制权。此策略有效屏蔽了“误切换”现象。系统采取了冗余“心跳”物理路径、提高“心跳”信号复杂度的策略,即两系统交互信号的路径拓展到 I2C 总线和 UART 总线,同时提高交互信号的复杂度,有效地鉴别干扰,屏蔽“不切换”现象。

1.3 关键信息备份

S3C2440 基于 ASIC 工艺,而 EP2C35 基于 FPGA 工艺。因此在复杂电磁环境下,两子系统对于相同的任务,其运算控制的准确度和可靠性具有一定的差异性。双机冗余运行时,两子系统将关键数据备份到双端口存储器中,读取对方的任务进程、备机系统跟踪主机系统任务处理轨迹。当主机系统出现故障,需要主机系统与备机系统切换角色或复位系统时,此技术就会加速系统任务定位,提高系统的实时性和可靠性。

2 可靠性策略

系统上电初始化成功后,默认以 ARM 子系统为主机系统、FPGA 子系统为备机系统执行系统任务。根据任务对系统功耗、复杂度、性能和可靠性要求的不同,可以采取不同的备份策略。最为常用的是双机热备份策略,其原理如图 3 所示。

系统上电后,主机系统获得外设控制权,输出外设控制信号,接管整个系统。而备机系统不输出外设控制信号,利用“心跳”总线与主机系统相互监视、运行相同的任务,完成相同的功能。本策略规定自监视定时器控制机制优先级高于“心跳”监视控制机制,即当子系统产生故障时,优先进行相

应自监视定时器的复位操作。此规定的目的在于使主机系统不会被备机系统轻易切换,从而造成“乒乓切换”的现象,降低系统的性能。

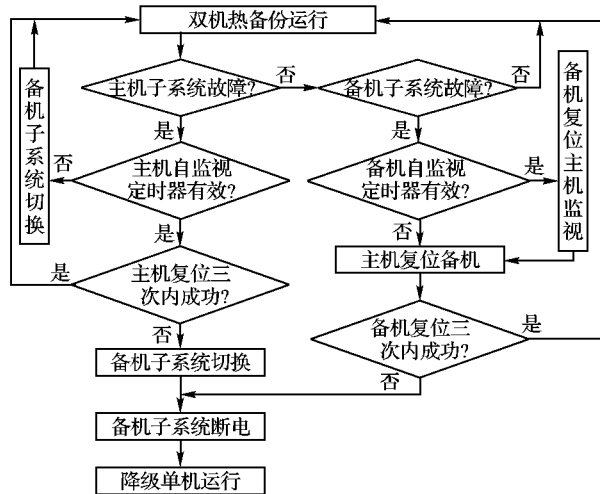


图3 双机热备份策略原理图

热备份策略可以有效降低系统切换控制权的时间延迟,提高了系统的故障处理和故障恢复的实时性,但是也带来系统功耗增加、复杂度升高的问题。

因此,在处理对于系统可靠性要求不高的普通任务时,尚可利用双机冷备份策略以降低系统的功耗,但其控制和分析方式更为复杂。

3 系统可靠性分析

离散时间、离散状态的马尔可夫过程是一个高效反映动态系统工作状况的数学模型^[7],可以依此分析异构双机冗余系统的可靠性。针对系统应用热备份策略处理任务的过程,特作如下几点说明。

1) 对于组成本系统冗余结构的 ARM 子系统和 FPGA 子系统,其工作状态在正常状态、可预测故障状态和不可预测故障状态之间动态转换,即系统的工作状态是两个子系统工作状态的有限集。

2) 系统从状态 i 转换到状态 j 的概率只与状态 i 有关,而与系统经历的工作过程无关。

3) 两子系统的在某种特定的电磁干扰下的寿命分布符合指数分布。

4) 在很短的时间内,电磁干扰不会改变。即在很短的时间内只会产生一次故障,系统故障覆盖率为 c 。

5) 在相同的电磁干扰环境下,两子系统发生故障的概率不同,ARM 子系统故障率 $\lambda_1 \in [0, 1]$,FPGA 子系统故障率 $\lambda_2 \in [0, 1]$ 。

应用双机热备份冗余策略,系统工作状态马尔可夫模型如图 4 所示。

系统状态设定如下:

0: 系统无故障,可靠模式;

1: FPGA 子系统无故障运行,ARM 子系统出现可预测故障,可靠模式;

2: FPGA 子系统无故障运行,ARM 子系统出现不可预测故障,可靠模式;

3: ARM 子系统无故障运行,FPGA 子系统出现可预测故障,可靠模式;

4: ARM 子系统无故障运行, FPGA 子系统出现不可预测故障, 可靠模式;

5: 两子系统都出现可预测故障, 系统故障模式;

6: 系统出现不可预测故障, 系统危险输出模式。

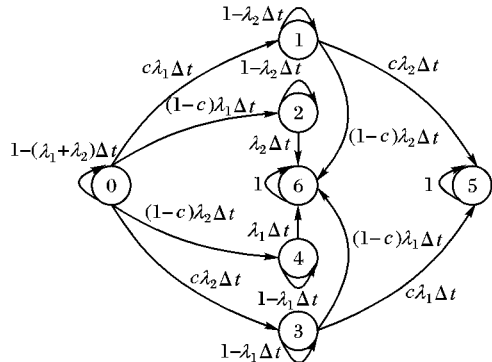


图4 系统马尔可夫模型

根据系统的状态转换图, 列出系统在连续时间域上状态转移概率的马尔可夫方程组:

$$\begin{cases} Y_0'(t) = -(\lambda_1 + \lambda_2)Y_0(t) \\ Y_1'(t) = -\lambda_2 Y_1(t) + c\lambda_1 Y_0(t) \\ Y_2'(t) = -\lambda_2 Y_2(t) + (1-c)\lambda_1 Y_0(t) \\ Y_3'(t) = -\lambda_1 Y_3(t) + c\lambda_2 Y_0(t) \\ Y_4'(t) = -\lambda_1 Y_4(t) + (1-c)\lambda_2 Y_0(t) \\ Y_5'(t) = c\lambda_1 Y_3(t) + c\lambda_2 Y_1(t) \\ Y_6'(t) = \lambda_1 Y_4(t) + (1-c)\lambda_1 Y_3(t) + \lambda_2 Y_2(t) + \\ (1-c)\lambda_2 Y_1(t) \end{cases}$$

各状态概率初始值为 $Y_0(0) = 1, Y_1(0) = Y_2(0) = Y_3(0) = Y_4(0) = Y_5(0) = Y_6(0) = 0$, 求出方程组的解为:

$$\begin{cases} Y_0 = e^{-(\lambda_1 + \lambda_2)t} \\ Y_1 = c(1 - e^{-\lambda_1 t})e^{-\lambda_2 t} \\ Y_2 = (1-c)(1 - e^{-\lambda_1 t})e^{-\lambda_2 t} \\ Y_3 = c(1 - e^{-\lambda_2 t})e^{-\lambda_1 t} \\ Y_4 = (1-c)(1 - e^{-\lambda_2 t})e^{-\lambda_1 t} \\ Y_5 = c^2(e^{-(\lambda_1 + \lambda_2)t} - e^{-\lambda_2 t} - e^{-\lambda_1 t} + 1) \\ Y_6 = (1-c)(1+c)(e^{-(\lambda_1 + \lambda_2)t} - e^{-\lambda_2 t} - e^{-\lambda_1 t} + 1) \end{cases}$$

系统可靠度^[8]为:

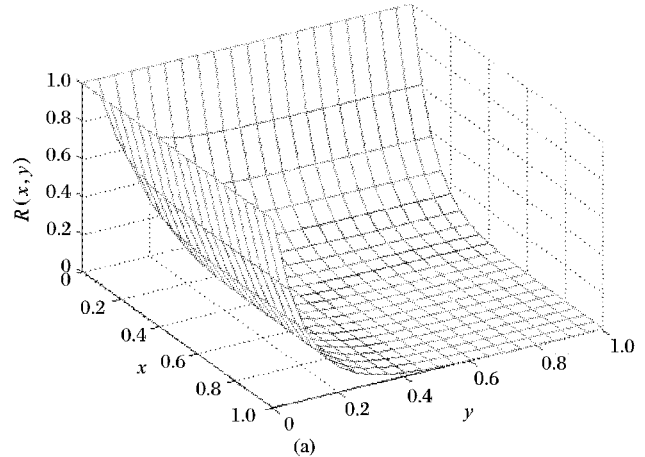
$$R(t) = Y_0(t) + Y_1(t) + Y_2(t) + Y_3(t) + Y_4(t) = e^{-\lambda_2 t} + e^{-\lambda_1 t} - e^{-(\lambda_1 + \lambda_2)t}$$

当可靠运行时间 t 要求为 100 时, 利用 Matlab 分析可靠度函数 $R_{t=100}(\lambda_1, \lambda_2)$ 随故障率 λ_1 和 λ_2 的变化趋势如图 5 所示。

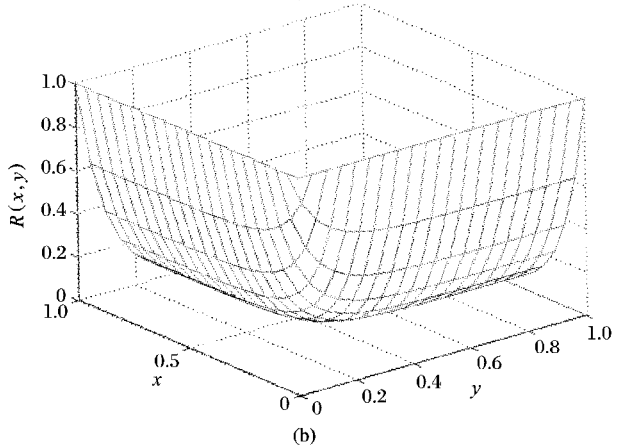
图 5 以 λ_1 为 x 轴, λ_2 为 y 轴, $R_{t=100}(\lambda_1, \lambda_2)$ 为 z 轴。

此函数图像特点为: 1) 当 λ_1 或 λ_2 接近于零时, $R_{t=100}(\lambda_1, \lambda_2)$ 趋近于 1; 2) 当 λ_1 接近于 1 时, 系统可靠度趋近于 $e^{-\lambda_2}$; 当 λ_2 接近于 1 时, 系统可靠度趋近于 $e^{-\lambda_1}$; 3) 当 λ_1 或 λ_2 发生突变时, $R_{t=100}(\lambda_1, \lambda_2)$ 却保持在一个比较稳定的值。

以上函数反映了本系统运用热备份策略时的可靠性量化指标, 可以解释如下: 1) 只要有一个子系统可靠运行就能保证整个系统有较高的可靠度; 2) 系统安全运行时“智能”地选择高可靠度的子系统处理任务; 3) 当某一个子系统的可靠性急剧下降时, 整个系统的可靠性变化不大。即系统的可靠度具有一定的稳定性。



(a)



(b)

图5 可靠度函数曲面图

4 结语

本设计考虑到复杂电磁环境下异构芯片对相同的电磁干扰具有不同的敏感特性及其故障率 λ 存在很大差异性的特点, 提出了基于异构双机冗余模型并运用双机热备份策略, 有望大幅度提高恶劣电磁环境下嵌入式控制系统的可靠性。该方式对于其他具有高可靠性要求的系统设计同样具有一定的指导意义。

参考文献:

- [1] 吴会丛. 基于 EHW 的芯片级电磁损伤自修复技术研究[D]. 石家庄: 军械工程学院, 2006.
- [2] LALA P K. 容错与故障可测性系统设计[M]. 孟永炎, 申晓留, 成煜中, 译. 北京: 中国铁道出版社, 1989.
- [3] TOWNEND P, XU J, MUNRO M. Building embedded fault-tolerant systems for critical applications: An experimental study[C]// IFIP World Computer Congress. Montreal, Quebec, Canada: [s. n.], 2002: 101-112.
- [4] 李建国, 陈松乔, 鲁志辉. 实时异构系统的动态分批优化调度算法[J]. 计算机学报, 2006, 29(6): 976-983.
- [5] 巨政权. 双核异构并行系统多功能平台的研究与实现[D]. 石家庄: 军械工程学院, 2008.
- [6] 党崇伦. 基于 FPGA 的关节伺服控制器容错技术研究[D]. 北京: 北京邮电大学, 2008.
- [7] WHITE A L, PALUMBO D L. State reduction for semi-Markov reliability models[C]// Proceedings of Annual Reliability and Maintainability Symposium. Los Angeles, CA, USA: IEEE, 1990: 280-285.
- [8] 董海鹰, 李军, 薛钧义. 双机冗余系统的非马尔可夫模型研究[J]. 铁道学报, 2002, 23(6): 35-38.