

三模冗余演化自修复系统设计及可靠性分析

巨政权¹, 郑见灵², 满梦华¹

(1 军械工程学院 静电与电磁防护研究所, 河北 石家庄 050003; 2 军械工程学院 计算机工程系, 河北 石家庄 050003)

摘 要: 将演化硬件与 TMR 技术相结合在系统级层面设计并实现了一款 ETMR 系统, 并以马尔可夫过程理论为基础探讨了其可靠性规律. 发现在任意区间上, ETMR 较之单模和 TMR 系统具有较高可靠性, 同时指出修复率与故障率比值是影响 ETMR 系统可靠度的主要因素, 且比值越大其可靠度接近于 1 的区间跨度越大. 系统构建方法及所得结论对于将 ETMR 系统应用于具体工程实践具有一定的启发和指导作用.

关键词: 三模冗余; 演化硬件; 自修复; 马尔科夫模型; 可靠性

中图分类号: TP273

文献标识码: A

文章编号: 1000-7180(2012)05-0029-05

Designed and Reliability Analysis of Triple Module Redundancy System with Evolvable Self-repairing

JU Zheng-quan¹, ZHENG Jian-ling², MAN Meng-hua¹

(1 Electrostatic and Electromagnetic Protection Institute, Ordnance Engineering College, Shijiazhuang 050003, China;
2 Department of Computer, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: Designed and realized an ETMR system based on EHW and TMR technologies, and analyzed its reliability with Markov's course theory. We found that ETMR system has higher reliability compared with the single mould and TMR system in any times, and the main factor of influence the ETRM system reliability was the ratio of repair rate and failure rate, further, the larger the ratio is, the bigger the interval span that its reliability approach 1 is. This method and conclusions has certain inspiration and guidance in applying ETMR system to the concrete project practice.

Key words: TMR; EHW; self-repair; Markov model; reliability

1 引言

演化硬件 (Evolvable Hardware, EHW) 的提出, 为系统容错提供了新的方法和手段^[1-2]. 演化硬件也称进化硬件或仿生硬件, 是一种具有自组织、自适应、自修复特性的新型智能硬件, 较之传统的容错手段, 它以演化算法作为组合优化和全局搜索主要工具, 以可编程器件作为硬件电路实现载体与评估手段, 在不依赖先验知识和外力的推动下, 通过进化获得满足给定要求的电路和系统结构, 使得系统能够在线自适应调整其内部结构, 以适应内部状态和外部工作环境的变化^[3-4].

文献[4]针对空间粒子辐射导致 FPGA 逻辑电路局部故障情况, 将演化硬件与三模冗余 (Triple module Redundancy, TMR) 技术相结合, 提出一种具有芯片级在线自修复能力的强容错 TMR 系统结构. 借鉴此思想, 本文将演化硬件与 TMR 技术相结合, 设计并实现了一款具演化自修复能力的 TMR 系统, 即三模冗余演化自修复系统 (ETMR), 并对其进行了可靠性建模和分析.

2 系统设计

2.1 系统架构及工作流程

传统 TMR 系统不具备模块修复功能, 仅容忍

收稿日期: 2011-09-12; 修回日期: 2011-10-23

基金项目: 国家自然科学基金项目 (60971042)

一个模块发生故障的情况,当两个及以上模块发生故障时,系统功能失效. ETMR 系统利用演化硬件的自修复功能,当某个模块出现故障,系统触发相应

机制对故障模块进行在线演化修复. 待修复成功后,系统恢复到一个新的“初始状态”,从而大幅提高系统可靠性. ETMR 系统架构如图 1 所示.

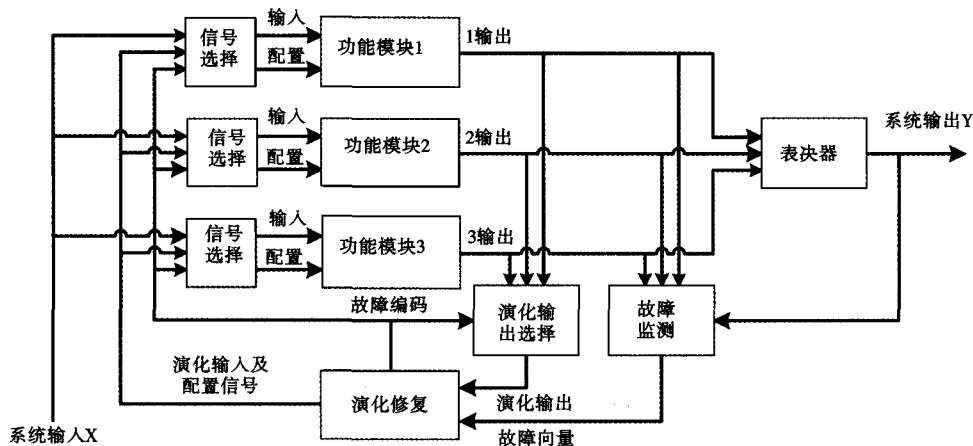


图 1 ETMR 系统架构

ETMR 系统较之传统 TMR 系统增加了故障监测、演化修复模块以及其它相应控制、选择机制. 系统上电后,演化修复模块根据各功能模块状况逐个进行初始演化配置,使其具有完整的系统功能. 其后,系统进入工作状态,演化修复模块进入故障等待状态. 同时故障监测模块对各功能模块进行实时监测,当检测到某个功能模块发生故障,便通过故障向量报告给演化修复模块. 演化修复模块根据故障向量进行故障编码,闭锁故障报告,触发演化修复机制. 同时,各模块根据故障编码完成相应信号控制. 此时,演化修复模块与故障功能模块形成一个独立的闭环系统,在不影响其它模块正常工作的同时实现故障模块在线演化修复. 演化修复完毕,演化修复模块解锁故障报告,同时故障编码置 0,系统恢复到 ETMR 状态. 其工作流程如图 2 所示.

2.2 输出表决及故障监测机制

表决是从多个不同硬件模块不太可靠的冗余输出中获取高可靠或更精确的数据作为系统输出的一种手段. 表决输出结果由具体的表决算法确定^[5],本系统中以“三中取二”的方式进行表决. 若各功能模块输出结果分别为 A 、 B 、 C ,表决结果为 D ,则有:

$$D = A \cdot B + A \cdot C + B \cdot C \quad (1)$$

$$D_i = A_i \cdot B_i + A_i \cdot C_i + B_i \cdot C_i \quad (2)$$

其中 $\cdot$ 为逻辑与运算, $+$ 为逻辑或运算, D_i 为第 i 位输出值.

系统对功能模块故障实时监测,其判定方法为:功能模块输出与系统输出实时比对,若某个功能模

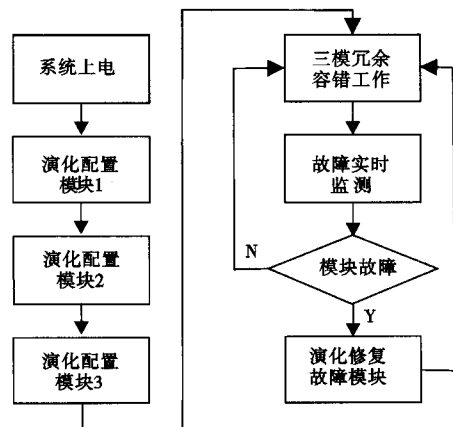


图 2 ETMR 系统工作流程

块与系统输出不一致,则认为此模块发生“故障”. 此方法在两个及以上模块发生故障时,判定失效,此情况暂且不予考虑. 若系统输出为 m 位, F_1 、 F_2 、 F_3 分别用于指示功能模块 1、2、3 的故障状况 (1 故障, 0 正常), 则有:

$$F_1 = A_0 \oplus D_0 + A_1 \oplus D_1 + \dots + A_{m-1} \oplus D_{m-1} = \sum_{i=0}^{m-1} A_i \oplus D_i \quad (3)$$

$$F_2 = B_0 \oplus D_0 + B_1 \oplus D_1 + \dots + B_{m-1} \oplus D_{m-1} = \sum_{i=0}^{m-1} B_i \oplus D_i \quad (4)$$

$$F_3 = C_0 \oplus D_0 + C_1 \oplus D_1 + \dots + C_{m-1} \oplus D_{m-1} = \sum_{i=0}^{m-1} C_i \oplus D_i \quad (5)$$

其中 $\oplus$ 为逻辑异或运算. 将式 (2) 代入 (3) (4)

(5)式,化简可得到由功能模块输出进行故障判定方法:

$$F_1 = \sum_{i=0}^{m-1} (A_i \cdot \overline{B_i} \cdot \overline{C_i} + \overline{A_i} \cdot B_i \cdot C_i) \quad (6)$$

$$F_2 = \sum_{i=0}^{m-1} (\overline{A_i} \cdot B_i \cdot \overline{C_i} + A_i \cdot \overline{B_i} \cdot C_i) \quad (7)$$

$$F_3 = \sum_{i=0}^{m-1} (\overline{A_i} \cdot \overline{B_i} \cdot C_i + A_i \cdot B_i \cdot \overline{C_i}) \quad (8)$$

2.3 故障阻塞及演化修复机制

故障阻塞是指演化修复阶段演化修复模块对故障报告不做任何反应的情况。故障阻塞机制可有效阻止系统在演化修复阶段,另一功能模块发生故障而使系统进入一个判定失效、演化修复不断循环的混乱状态。演化修复机制主要用以控制演化修复模块在演化修复前后的各项控制活动,其过程如图3所示。

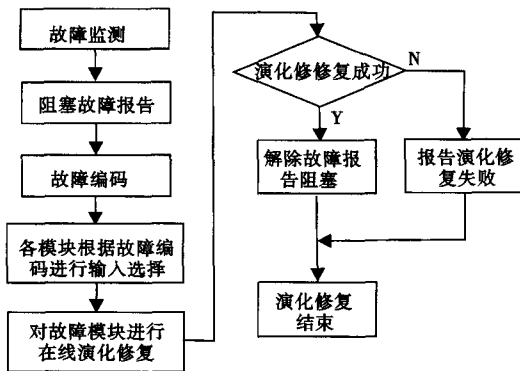


图3 系统演化修复机制

3 硬件实现

ETMR系统可由电路承载系统和演化修复系统两部分组成。电路承载系统用以构建功能模块电路及实现相应信号选择机制,可在线配置成相应功能电路,并可将输出反馈给演化修复系统。演化修复系统是整个ETMR系统的核心,输出表决、故障监测、演化修复以及其它相应控制、选择机制等功能模块均包含于此系统。

3.1 电路承载系统

以Altera公司Cyclone II FPGA芯片EP2C5Q208为配置核心,外围以Texas Instruments公司的可配置多功能器件SN74LVC1G98为分立单元,构建一个6×6可配置阵列。各分立单元的连接、配置全部在FPGA内部完成,通过对FPGA的不同配置可形成不同类型的片外可重配置阵列,其原理及配置方式在一定程度上借鉴了文献[6]

所构建的片内虚拟可重配置阵列。电路承载系统架构和硬件实现如图4所示。

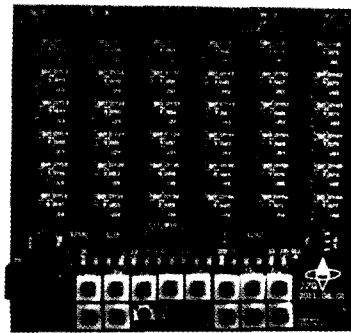
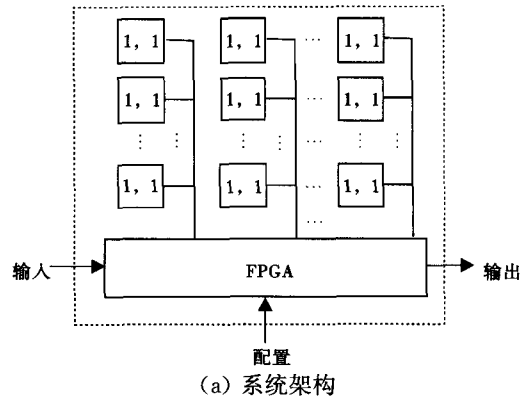


图4 电路承载系统

3.2 演化修复系统

如图5所示,演化修复系统由以EP2C5Q208为核心的SOPC系统构建。包括1片64 Mb SDRAM MT48LC2M32B2作为系统内部存储器;1

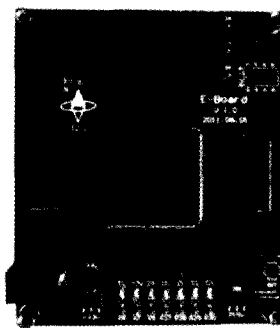
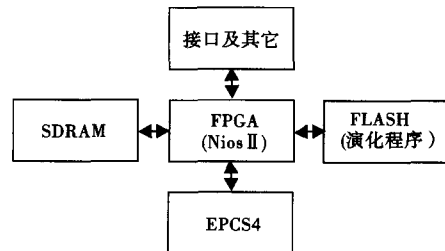


图5 演化修复系统

片 32Mb NOR FLASH Am29LV320D 用于存储相关演化程序;串行配置芯片 EPCS4 用于存储 FPGA 相关配置信息.保证了基于 FPGA 内部所构建 NIOS II 处理器运行的演化程序有效存储和高效运行.各功能模块可通过 Quartus II 软件具体编程实现.

4 系统可靠性分析

ETMR 系统状态是一个不断变化的动态过程,但从一状态切换到另一状态的概率固定不变,可用马尔可夫过程理论对其进行可靠性建模加以仿真分析.

4.1 系统可靠性建模

ETMR 系统一旦检测到故障,即刻进行故障闭锁,并进行演化修复,对故障真假不加判定.检测到故障模块并进入演化修复状态可认为是一个瞬时状态.若对系统功能模块关联状态不加限制,则系统具有以下五种状态:

状态 0:三个功能模块全部正常,系统处于完好状态;

状态 1:两个功能模块正常,一个功能模块修复,表决后系统输出正常,处于可靠状态;

状态 2:一个功能模块正常,一个功能模块故障,一个功能模块修复.由于在修功能模块输出不确定,致使表决后系统输出结果不确定(有时正确有时错误).但修复后系统转至状态 1,为完好状态,所以可认为此状态系统倒向安全侧.

状态 3:两个功能模块故障,一个功能模块修复.由于两故障功能模块输出相同,表决结果为错误输出.在修模块修复后,其输出与两故障模块输出不同,再次被判定为“故障”模块,系统陷入对此模块无限循环修复的故障状态.

状态 4:三个模块故障,表决后系统输出错误,且检测不出故障模块,系统进入一个稳定的故障状态.

为降低问题的复杂度,在此仅考虑每一时刻最多只能有一个模块发生状态转移的情况,则系统存在 0、1、2、3 四种状态.假设系统故障仅发生在功能模块上,失效率为 λ ,演化模块对其修复率为 μ ,可得 ETMR 系统状态空间马尔科夫模型,如图 6 所示.

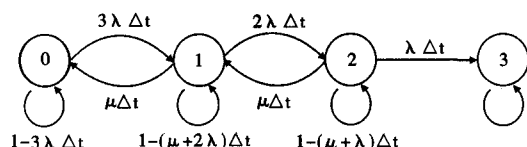


图 6 ETMR 系统状态空间马尔科夫模型

若 $p_i(t)$ ($i=0,1,2,3$) 表示 t 时刻系统处于状态 i 的概率,由全概率公式可得系统的马尔可夫模型方程组:

$$\begin{cases} \dot{p}_0(t) = -3\lambda p_0(t) + \mu p_1(t) \\ \dot{p}_1(t) = 3\lambda p_0(t) - (\mu + 2\lambda) p_1(t) + \mu p_2(t) \\ \dot{p}_2(t) = 2\lambda p_1(t) - (\mu + \lambda) p_2(t) \\ \dot{p}_3(t) = \lambda p_2(t) \end{cases} \quad (9)$$

初始时刻 $t=0$,系统所有功能模块完好,微分方程组(9)初始条件为: $p_0(0)=1, p_1(0)=0, p_2(0)=0, p_3(0)=0$.

系统可靠度为状态 0、1 时的概率和,即:

$$R_{ETMR}(t) = p_0(t) + p_1(t) \quad (10)$$

4.2 系统仿真分析

微分方程组(9)理论上可通过拉普拉斯变换求出 $p_0(t)$ 、 $p_1(t)$ 、 $p_2(t)$ 、 $p_3(t)$,但求解过程比较复杂,故采用 MATLAB 中微分方程求解函数 ode45 进行仿真求解. ode45 函数的用法及微分方程组具体求解方法 MATLAB 帮助文档及文献[7-8]均给出了详细过程,稍作修改便可对微分方程组(9)进行仿真求解,故此不再赘述.

4.2.1 λ, μ 对 ETMR 系统可靠性影响情况分析

分别取 (λ, μ) 为 $(0.0001, 0.001)$ 、 $(0.0001, 0.01)$ 、 $(0.0001, 0.1)$ 、 $(0.0001, 1)$ 、 $(0.0005, 0.005)$ 、 $(0.0005, 0.05)$ 、 $(0.0005, 0.5)$ 、 $(0.0005, 1)$,对微分方程组(9)仿真求解,可得系统可靠度 $R(t)$ 随 λt 变化曲线如图 7 所示.

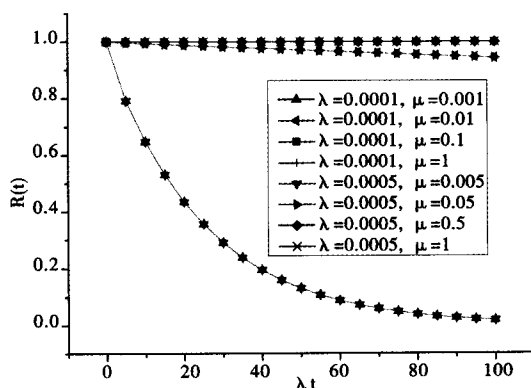


图 7 ETMR 系统可靠度 $R(t)$ 与 λt 关系曲线

由图 7 可知:

(1) 修复率 μ 与故障率 λ 比值一定时,系统可靠度曲线重合,即 ETMR 系统可靠度与 $k=\mu/\lambda$ 有关,与具体的 μ, λ 取值无关.此结论经多次仿真验证均成立.

(2) 当 k 值一定时,随着 λt 的增大,系统可靠度

逐渐降低,且 k 值越大可靠度降低越缓慢. 区间 $(0, \infty)$ 上, λt 相同时 k 值越大系统可靠度越高.

(3) 当 $\mu=1$ 时,系统可靠度恒为1. $\mu=1$ 表明系统中故障模块可瞬时修复,转化为正常模块,此时系统仅有0,1两种状态,可靠度恒为1.

(4) 在区间 $(0, 100)$ 上,当 $k=1\ 000$ 时,可靠度曲线与 $\mu=1$ 时基本重合,但随 λt 值的不断增大将逐渐下降. 所以 ETMR 系统在从0开始的某个区间上其可靠度接近于1,与无故障系统可靠性等效;且 k 值越大,此区间跨度越大.

4.2.2 ETMR、TMR、单模系统可靠性比对分析

传统 TMR 及单模系统可靠度计算公式分别为: $R_{\text{TMR}}(t)=3e^{-2\lambda t}-2e^{-3\lambda t}$, $R_s(t)=e^{-\lambda t}$. 由于 ETMR 系统可靠度曲线由 k 值确定, λ 取0.001, μ 分别取0,0.001,0.01,0.1,1,足以分析其可靠度规律状况. 单模、TMR 及不同取值下 ETMR 系统可靠度曲线如图8所示.

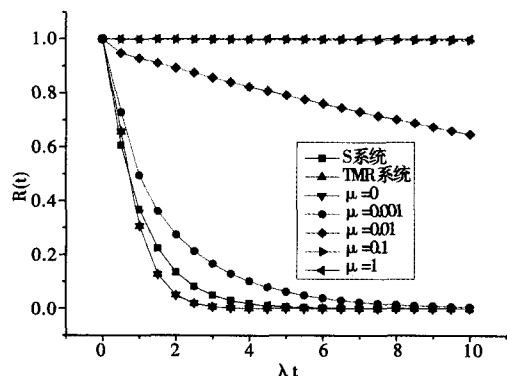


图8 三种系统可靠度曲线比对

由图8可知:

(1) 单模系统与 TMR 系统可靠性曲线存在交点,即有 $R_{\text{TMR}}(t)=R_s(t)$,解方程 $e^{-\lambda t}=-2e^{-3\lambda t}+3e^{-2\lambda t}$, λt 分别为0, $\ln 2(0.6931)$, ∞ , 对应 $R(t)$ 为1, 0.5, 0. 所以 TMR 与单模系统在系统初始、无穷大及 $\lambda t=\ln 2$ 三时刻可靠度相等. 区间 $(0, \ln 2)$ 上 TMR 高于单模系统可靠度, 区间 $(\ln 2, \infty)$ 上单模高于 TMR 系统可靠度, 即 TMR 系统工作时可信区间为 $(0, \ln 2/\lambda)$.

(2) 当 $\mu=0$ 时, ETMR 与 TMR 可靠度曲线重合, 收缩为 TMR 系统. 工程实践中 μ 大于 λ , 即 $k>1$ 时系统修复性才有意义. 由图8知 $k=1$ 时 ETMR 系统可靠度曲线均高于 TMR 和单模系统, 故任意区间上 ETMR 较之 TMR 和单模系统均具有较高的可靠性.

(3) λ 一定时, 三种系统 $R(t)$ 均随 λt 增大逐渐降低, 符合电子系统寿命规律.

5 结束语

本文设计并实现了一个较之 TMR 和单模系统具有较高可靠性的 ETMR 系统, 并对其可靠性进行了分析, 所得结论对于系统可靠性设计及实践应用具有一定指导意义. ETMR 系统在单个模块出现故障时可较好实现系统的演化修复, 但两个及以上模块同时发生故障时, 系统将完全失效. 对两个及以上模块发生故障时的系统容错机制, 以及同一时刻多个模块发生状态转移时系统可靠性情况, 将于另文讨论.

参考文献:

- [1] 刘尚合, 孙国至. 复杂电磁环境内涵及效应分析[J]. 装备指挥技术学院学报, 2008, 19(1): 1-5.
- [2] 刘尚合, 原亮, 褚杰. 电磁仿生学——电磁防护研究的新领域[J]. 自然杂志, 2009, 31(1): 1-7.
- [3] 王晓艳, 姚睿. 使用 SystemC 设计片上自演化系统[J]. 微电子学与计算机, 2011, 28(6): 22-25.
- [4] 姚睿, 王友仁, 于盛林, 等. 具有在线修复能力的强容错三模冗余系统设计及实验研究[J]. 电子学报, 2010, 38(1): 177-183.
- [5] 揣锦华, 姚蔚华, 常博. 一种聚类算法在容错计算机系统中的应用[J]. 微电子学与计算机, 2009, 26(7): 92-94.
- [6] Sekanina L. Evolutionary functional recovery in virtual reconfigurable circuits[J]. ACM Journal on Emerging Technologies in Computing Systems, 2007, 3(2): 1-22.
- [7] 杨其国. 基于 Markov 过程的冗余系统可靠性分析[J]. 计算机仿真, 2011, 28(1): 356-359.
- [8] 王丽华, 徐志根, 王长林. 可维修三模冗余结构系统的可靠度与安全度分析[J]. 西南交通大学学报, 2002, 37(1): 103-107.

作者简介:



巨政权 男, (1980—), 博士研究生.
研究方向为电磁防护理论与技术.