第 32 卷 第 21 期 计 算 机 工 程 2006 年 11 月
Vol.32 No.21 Computer Engineering November 2006
·工程应用技术与实现· 文章编号：1000—3428(2006)21—0249—03 文献标识码：A 中图分类号：TP302.8

TMR 整体硬化技术及其在电控系统中的应用

原 亮，丁国良，刘文冰，黄飞云，赵 强
(军械工程学院计算机工程系，石家庄 050003)

摘 要：在对 TMR 的容错运行机制予以分析讨论的基础上，针对一种 DC 电机控制系统进行了基于 FPGA 芯片的“整体硬化”研究和具体实现。该方式既从原理上摆脱了传统的程序控制概念，消除了“程序跑飞”的隐患，又在结构上减少了因部分硬件单元的故障而导致系统功能整体受损的可能。因此，整个系统在 EMI 测试环境下表现出了良好的抗干扰性能。

关键词：TMR；容错；嵌入式系统；FPGA；EMI

TMR Hardening and Its Application in Control System

YUAN Liang, DING Guoliang, LIU Wenbing, HUANG Feiyun, ZHAO Qiang
(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003)

【Abstract】 According to the basic principle of TMR (three module redundancy), the details are discussed and implemented in a fault-tolerance DC motor controller, which is not composed of any kind of traditional CPU but only FPGA chip structured by VHDL language. Since there is no program in this embedded system, there will be no dangerous of IP corruption that all program-based CPUs tend to suffer. Apart of that, if any single module in FPGA becomes invalid, it will be isolated immediately from the system, and the other two will take the responsibility of keeping the system running correctly. This approach increases the reliability of the embedded applications above in the presents of EMI.

【Key words】 TMR; Fault tolerance; Embedded system; FPGA; EMI

在以嵌入式计算机为核心的控制系统中，各类信息总量越来越大，其技术和功率的密集度与实时性的要求也越来越高，但其工作环境却随着复杂的应用要求而愈加苛刻，致使有些电子零部件可能在事先无法察觉和没有任何征兆的情况下突然失效。在某些恶劣环境下运行的系统中，还有可能出现芯片的局部毁损甚至是“单粒子翻转”的情况发生[1]。一般而言，任一模块的毁损或故障均有可能使整个系统受到影响。因此，如何保证整体可靠性始终是控制系统设计领域的重点研究内容。

对此，本文基于较为先进的 FPGA 芯片以及已有的成熟技术、开发平台和测试手段，在对 TMR(Triple Modular Redundancy)容错原理仔细分析和研究之后，进行了整体的“硬化”实现，以求有效解决上述问题。在此基础上，结合相应的无刷直流(DC)电机容错控制系统实物模型，探讨了能在相关控制系统发生故障后自动将其故障部分探测并予以屏蔽的技术，以及继续保持系统正常运行的方法。

1 控制系统的整体硬化

现场可编程门阵列(FPGA)器件是一种基于查找表结构的可编程逻辑电路，其逻辑结构是通过向相关的静态存储单元加载配置数据来实现的，不同的数据流对应于不同的系统结构。使用时一般先用 VHDL 或类似的硬件描述语言进行编程，以期实现某一具体的逻辑功能。然后，通过相应的开发环境将设计方案编译形成特定格式的数据流文件，进而下载至 FPGA 的片内 RAM，以决定 FPGA 中各个电路的逻辑关系并设置其工作状态。从理论上讲，如果芯片具有足够的规模，可以将任一控制系统的所有逻辑功能全部使用描述语言予以描述，进而下载至一片 FPGA 中，从整体上硬化形成为“单片系统”。

目前，大规模的 FPGA 芯片往往包含了几十万甚至上千万的基本门电路，可以方便地形成嵌入式应用中所需的完整控制系统。与一般以单片机为核心的控制系统相比，这种方式具有较为突出的优势。首先是减少了芯片数量，所有任务均置于可重新配置的 FPGA 芯片中予以完成，各类信号延迟时间可以限制在 ns 级，具有高速、稳定的特点。其次，系统各项功能的实现全部由电路的结构保证，完全没有传统意义上的“程序”，因此不存在任何因其“跑飞”而造成故障的问题。再者，在不更动电路板和芯片的前提下，能够直接对其硬件进行功能变更及结构升级。

2 TMR 基本原理

冗余技术是诸多提高可靠性的手段之一[2]，往往经增加备份系统的方法进行。然而，传统的冗余方式会使整个系统的功耗、体积和造价等指标变差，况且，各个分系统间尚需通过其他方式进行相互的协调[3]，反而会增加发生新的故障的机会。因此，在嵌入式控制系统的应用中时常受限。随着 FPGA的出现，情况发生了很大的变化。此类芯片的体积、功耗很小，方便易用，成本低廉，而且芯片内部空间及配置方法的潜力巨大，可为实现新型的冗余方式提供理想的实验平台。

基金项目：国家自然科学基金资助重点项目“电磁脉冲对微电子器件及设备作用机理与防护基础研究”(50237040)；国家自然科学基金资助面上项目“恶劣环境下芯片级自恢复系统的演化硬件机制研究”(60471022)

作者简介：原 亮(1955－)，男，硕士、教授，主研方向：智能检测与故障诊断，EHW 理论及实现；丁国良，博士生、副教授；刘文冰、黄飞云，硕士生；赵 强，教授、博导

收稿日期：2005-11-07 **E-mail：**yltgzy@yahoo.com.cn

2.1 “全等模块”和“表决运行”

若将原先的控制系统看为一个完整的功能“模块”，就可将数个此类结构、功能相同的模块看作为“全等模块”，并由此综合而成一个“多模块”系统。这些模块若是共享同一输入信号，自然具有全等的输出。工作时，全等模块的所有输出先经比较器两两相减校验。若某一模块输出有误，则会使相应的相减结果出现非 0 值，通过判断便可立即确认并予以封锁，以此实现具有“容错”功能的“表决运行”。

在实际的实现过程中，既可按照综合方式在一片FPGA中设计、完成所有的全等功能模块(F_j)和包含了比较器的表决模块(M)，又可按照分布方式将全等功能模块、表决模块分别设计到几片独立的FPGA中。无论使用哪种方式，一旦表决模块发现错误，系统就将按照表决的多数方式运行，进而将出错模块屏蔽。尽管如此，这种结构的效能并非正比于全等模块的数量，因为模块数量增多的本身又将带来新的隐患。一般而言，由 3 个模块所形成的TMR结构最为简便、易于实现。若将TMR结构完成于一个芯片中，则构成“单片TMR系统”。此即本文描述的重点。

2.2 TMR 结构模型

在单片FPGA实现的TMR模型中，主要包括了 3 个全等的功能模块$F_{j=1,2,3}$和一个表决模块M，如图 1 所示。

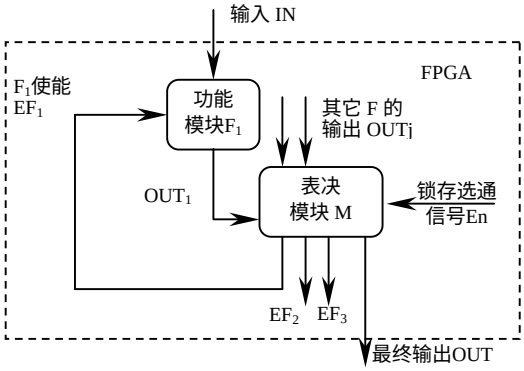

图 1 单个 FPGA 的 TMR 模型结构

为简化起见，图 1 中只画出一个功能模块F_1，其余功能模块的结构与之相同。3 个功能模块输入端以并联方式连接至同一输入信号I，所有功能模块F_j的输出OUT_j(j=1…3)则只连接到表决模块M。正常情况下，经M表决输出功能模块使能信号EF_j(j=1…3)分别使能相应的功能模块F_j。

表决模块 M 由比较器、表决器和锁存器组成，如图 2 所示。

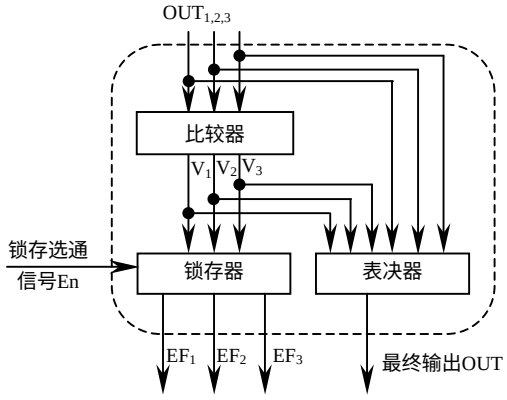

图 2 表决模块 M 结构

若有某一模块发生错误，表决器可以根据比较器输出的V_j按照真值表(表 1)找到出错的功能模块，进而产生表决结果EF_j'，锁存后就得到了相应的模块使能或封锁信号EF_j，使能正常的功能模块，封锁出错的功能模块。对表决结果而言，此即“非 0 剔除”的概念，而对系统而言，便可实现独立运行、结果校验以及进行模块之间的故障认定与仲裁，以保证某个功能模块出现毁损情况后，系统仍能继续正常运行。

表 1 TMR 比较器真值表

O_1 O_2 O_3	V_1 V_2 V_3	F_1 F_2 F_3
0 0 0	0 0 0	√ √ √
0 0 1	1 1 0	√ √ ×
0 1 0	1 0 1	√ × √
0 1 1	0 1 1	× √ √
1 0 0	0 1 1	× √ √
1 0 1	1 0 1	√ × √
1 1 0	1 1 0	√ √ ×
1 1 1	0 0 0	√ √ √

注：表中“√”表示功能模块正常，“×”表示功能模块出错。

因系统只能使用一个表决模块，所以该模块可能成为薄弱环节。但从功能与结构等诸多方面说来，全等模块远较表决模块复杂，况且全等模块一共有 3 个。所以全等模块所占总的逻辑单元数(或硅片面积)要远远大于表决模块所占用的单元数。因此，就所遭受粒子轰击的概率而言，表决模块要小很多。只要表决模块未受影响，系统就能有效解决其它模块的问题。

3 系统实现与测试

在许多装备中，因大量使用电机而使原本狭小的空间内电磁干扰问题急增。同时，电机控制系统本身又同时包含了弱电和强电两大典型环节。因此，特选定具有较高工程应用价值、又对电磁干扰十分敏感的 DC 电机控制器作为基于 TMR 技术的整体硬化实例进行研究。

3.1 原理与实现

对于DC电机而言，旋转输出就是一个判断转子当前位置、并通电使其转至下一个位置的过程[4]。相应的控制系统亦可由多种方法实现。本文所述系统中，共有 3 个起着核心作用的位置解算模块构成TMR结构中的全等模块。在进行相应的电路描述和仿真后，下载至大规模FPGA芯片ACEX1K50中予以“整体硬化”，进而再与相关电路一起，形成一个完整的单片TMR系统，如图 3 所示。此外，作为对照，控制系统亦分别使用其它多种类型的CPU以常规设计方式完成。就这些系统而言，虽各个板卡的基本电路不同，但其物理尺寸、主要器件排布格式统一，全部按照某实际装备中某型电机所需要的功率、空间等要求进行设计和制作，并直接使用同一套电机和功率驱动模块进行测试，以提高不同系统之间的可比性。

图 3 电机和 TMR 驱动系统实物图

3.2 测试与分析

在各项抗干扰的实验中，常规的电磁脉冲效应实验最为典型[5]，因而在本系统测试中加以使用。实验的具体方法分为辐照和注入两种。因TMR驱动系统的电磁脉冲效应实验属于系统电路效应实验，电路复杂且难以进行良好的隔离，所以，采用辐照法更为合适。此外，辐照法能够较为真实地模拟电子系统受电磁脉冲干扰的情形，比较接近实际情况，并能给出宏观结果，适合于计算机类系统效应实验[6]。

在室温为 24.0℃、湿度为 45.2%、符合IEC61000-4-2 标准的实验环境下，选用日本三基公司的NoiseKen ESS-200AXESD模拟器，对以不同芯片实现的相同功能系统分别在其运行过程中进行静电放电测试。测试电压由低到高，直至系统在某一电压下连续出现 5 次工作异常。数据采集系统选用TDS680B数字存储示波器，采样速率为 5Gs/s，带宽为 1GHz。测试结果如表 2 所示。

表 2 使用不同芯片的相同功能系统的极限承受电压(单位：kV)

芯片类型	单片机		DSP	CPLD 与 FPGA		
具体型号	Atmel AT2051	Intel 80C196	TI TMS320LF2407A	Lattice 1032E	Altera EP1K50	Altera EP1K50(TMR)
放电电压	＋2.5	＋3.5	＋4.0	＋6.5	＋8.5	＋28.0

表 2 数据说明，对同样的 EP1K50 芯片而言，使用 TMR 结构后的抗扰能力能够得到很大改善，尤其是 TMR 结构控制器比传统程序方式的 CPU 控制器有着数量级的提高。此时，一般干扰造成的局部逻辑混乱将不再是导致系统停机的主要原因。鉴于目前尚无法模拟宇宙射线所造成的单粒子翻转效应的实验，所以对于“抗翻转”的功能暂时难下定论，只得留待日后再行研究。

3.3 后续工作

(1)重构表决模块。如前所述，表决模块无法再用 TMR 结构予以加强。然而，因其逻辑及功能远较控制电路为简，可以将其分离于 FPGA 芯片之外。通过精心测试，能够挑选、使用比 FPGA 芯片抗干扰能力更强的中小规模集成电路芯片构成，使其抗扰等级高于主控电路使用的 FPGA，以此首先保证表决模块的正常工作。从而尽量消除所有隐患。

(2)引入演化技术。仿照自然界中以碳为基的生物进化过程，有可能在现有FPGA芯片或更大规模的芯片上实现可控的“硅基进化”，这就是“演化硬件(EHW)”技术[6]。其基本思想是基于演化算法，对集成电路芯片中可重配置的逻辑单元进行重配和组合，使其体系结构、连接方式以及局部功能均可根据环境的变化而通过演化予以适应，从而自行实现动态调整或优化。

(3)探讨自修复机制。在TMR的基础上结合EHW技术的方式，将比单纯的容错运行或单纯的进化方式具有更多的优势。因其至少可以实现基于芯片内部或外部冗余结构所进行的逻辑功能自我复制和受损电路的自行避让或修复，使得系统完全可能从容错运行状态恢复至正常的功能运行状态。此时，故障单元的功能则因进化而得到替代、部分恢复甚至“痊愈”。在整个故障处理过程中，原有的TMR结构至少可以保证系统的基本运行而赢得宝贵的进化时间，进而结合表 1 内容重新形成完整的TMR结构[7]，即最终能以自修复方式将故障模块恢复功能。其基本流程如图 4 所示。

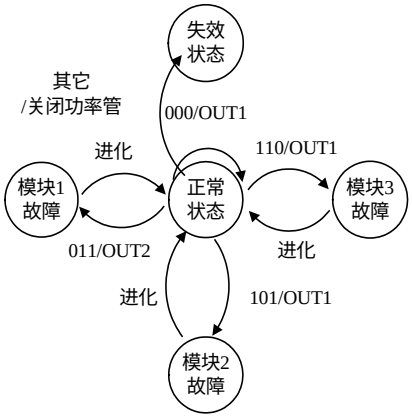

图 4 TMR－EHW 工作流程

4 结束语

综上所述，容错运行是军事和自动化等领域中非常具有挑战性的课题，亦是集多门学科为一体、容多项技术于一身的前沿性领域。控制系统所起的作用越大，其故障所造成的危害也会越大，从而使得容错运行技术尤显重要。另外，新技术、新器件的迅速涌现，亦使此类直接面向应用的研究更加现实、可行。依托于“强电磁场环境模拟与防护技术”国防科技重点实验室，前述系统业已全面完成并投入到了有关电磁防护研究的后续实验之中。其它正以 TMR-EHW 方式进行的故障后容错、代偿直至恢复正常功能运行的各类实验，又为实现嵌入式控制系统高度可靠的性能要求提供了全新的设计思路和实现方法，并可望具有较高的学术价值和广阔的应用领域。

参考文献

1 熊剑平. 微小卫星数据存储器单粒子作用的检测及纠错[J]. 中国空间科学技术, 2000, 6(20).

2 孙立辉, 原　亮. 基于 CAN 总线的多机冗余系统设计[J]. 计算机测量与控制, 2002, 12(10).

3 郭浩翔, 袁由光. 一种三模冗余容错服务器的容错机制[J]. 舰船电子工程, 2003, (23)1.

4 王晓明. 电动机的单片机控制[M]. 北京: 航空航天大学出版社, 2002.

5 侯民胜, 刘尚合, 王书平. 单片机系统在核电磁脉冲辐照下的效应研究[J]. 强激光与粒子, 2001, 13(5).

6 Yao X. Following the Path of Evolvable Hardware[J]. Communications of the ACM, 1999, 42(4).

7 王国庆. 演化硬件在容错技术中的应用研究[D]. 石家庄: 军械工程学院, 2004.