한국항행학회 논문지 제14권 제1호 2010년 2월

항공용 임베디드 시스템을 위한 Triple Module Redundancy 구조의 임베디드 하드웨어 신뢰성 평가

A Study on the Triple Module Redundancy ARM processor for the Avionic Embedded System

이동우*, 김병영*, 고완진*, 나종화*

Dong-Woo Lee*, Byeong-Young Kim*, Wan-Jin Ko* and Jong-Whoa Na

요 약

항공 임베디드 시스템은 고신뢰성 설계가 매우 중요하다. 본 논문에서는 고신뢰성 항공 임베디드 시스템 연구를 위하여 Triple Modular Redundancy(TMR) 구조의 하드웨어를 설계하였다. TMR 구조의 하드웨어가 단일 프로세서 구조의 하드웨어보다 얼마나 신뢰성이 향상 되었는지를 연구하기 위하여, ARM 프로세서와 TMR ARM 프로세서의 축소된 형태의 시뮬레이션 모델을 개발하였고 각각의 신뢰성을 평가하는 연구를 수행하였다. 신뢰성 평가는 RTL을 이용한 시뮬레이션 기반 오류 주입 시뮬레이션 기법을 이용하였다. 주입된 오류별로 타겟 시스템의 상태변화를 분석하여, 오류 복구비율을 계산하였다. 실험결과 TMR ARM의 오류복구 능력은 ARM에 비해 최대 10배 이상 향상되었으며, 특히 permanent fault에서 더 강인함을 확인 하였다.

Abstract

The design of avionic embedded systems requires high-dependability. In this paper, we studied the dependability of the triple modular redundancy (TMR) hardware for highly reliable aviation embedded system. In order to evaluate the dependability of the base ARM processor and the TMR ARM processor, we developed the simulation model of the reduced ARM and TMR ARM processors and performed the simulation fault injection for the analysis of the dependability of the two targets. In the fault injection experiments, we calculated the error recovery rate of the two the processor models. From the experimental results, we could confirm that the reliability of the TMR ARM processor was greater than the single ARM processor by ten times in some cases.

Key words : avionic embedded system, triple modular redundency, fault injection, dependability

I. 서 론

끊임없이 발전하는 반도체 공정 및 설계기술의 발달은 이제는 여러 모듈들이 하나의 칩으로 통합되는 system-on-chip, package-on-a-chip과 같은 형태의 고집적 하드웨어 제품들의 출시를 가능케 하였다. 이러한 고직접 제품들은 설계요구사항의 복잡도의 증가를 초래하는데 이러한 복잡도의 증가는 시스템의 기능

* 한국항공대학교 항공전자 및 정보통신공학부 (College of of electronics, Telecommunication & Computer Engineering,Korea Aviation University)
· 제1저자 (First Author) : 이동우
· 투고일자 : 2009년 11월 10일
· 심사(수정)일자 : 2009년 10월 27일 (수정일자 : 2010년 2월 20일)
· 게재일자 : 2010년 2월 28일

의 고성능화, 소형화, 저 전력화 등의 기술의 도입하여 해결할 수 있다. 그러나 이러한 반도체 기술의 발전의 반작용으로 1) 설계복잡도 증가에 따른 설계상 오류의 증가 [1], 2) 반도체의 고속화에 따른 칩 내에 결함허용범위(noise margins) 감소로 인한 오류 민감도 증가와 같은 심각한 문제의 발생을 함께 초래하였다. 이러한 오류의 증가는, 항공 임베디드 시스템에서 반드시 해결해야 할 문제들이다.

이렇듯 발로 증가하는 오류문제를 해결하기 위하여 다양한 연구가 진행되어 왔다[3-5]. 오류를 극복하는 방법에는 여러 가지가 있지만 그 중에서 많이 사용되는 방법들 중의 하나는 Architectural 수준에서 고장감내형 시스템을 설계하는 것이다[3-5]. 고장감내형 시스템은 시스템에 발생한 오류를 처리하여, 정상동작을 유지 할 수 있도록 하는 시스템이다. 고장감내형 시스템은 오류의 처리를 위해 오류 검출, 고립, 회복하는 메커니즘을 사용한다.

본 연구는 ARM7 프로세서를 목표로 설정하여 ARM7 프로세서의 전체 기능들 중에서 가장 중요한 부분을 Electronic System Level (ESL) 도구를 이용하여 설계하였다. ELS 도구는 현재 가장 많이 사용되고 있는 SystemC를 이용하여 reduced SystemC ARM 프로세서를 설계하였다. 이 프로세서를 확장하여 Triple Modular Redundancy (TMR) 구조의 프로세서인 TMR ARM을 설계하였다. 개발된 ARM과 TMR ARM 프로세서 모델의 오류처리 능력을 검사하기 위하여 오류주입 시뮬레이션을 수행하였다. 오류주입 시뮬레이션의 결과를 분석하여 설계한 프로세서 모델에 대한 오류처리 능력을 검증 하였다. TMR ARM은 단일 ARM 프로세서에 대비하여 transient fault 주입 시 최대 2.4배, permanent fault 주입 시 최대 10.5배의 오류 복구 능력 향상을 보였다. 따라서 항공 전자장비에서 TMR 구조가 가격적인 측면에서는 2배 이상의 증가를 초래하지만, 신뢰성이 높은 것을 확인하였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존에 연구된 오류회복 기법과 시스템을 설명한다. 3장에서는 설계한 ARM과 고장감내형 기법을 적용한 Module Level TMR ARM을 설명한다. 4장에서는 설계한 프로세서 별 오류주입 시뮬레이션 결과를 설명하고, 5장에서 결론을 맺는다.

Ⅱ. 오류회복 기법

2-1 Forward Error Recovery

Forward error recovery기법은 오류발생에 따른 검출 및 복구를 시간적인 손실 없이 처리하는 오류복구 기법을 통칭한다. Forward error recovery를 적용한 프로세서는 오류 검출과 복구를 위해 추가적인 하드웨어(redundant hardware) 또는 오류를 검출 복구 할 수 있는 정보(redundant information)를 프로세서 데이터에 부여한다. 추가적인 하드웨어의 경우 redundant copy module을 통해 동일한 작업을 병렬적으로 수행하고, 수행결과를 voter로 비교한다. 결과가 다른 모듈의 값은 오류가 발생한 것으로 간주하고 제거한다. 추가적인 정보의 경우 오류 검출 및 보정 코드인 CRC 또는 해밍 코드를 적용한다. Forward Error Recovery 기법은 오류 발생 시 즉각적으로 시스템 복구가 가능하다. 따라서 실시간 시스템에 적용 가능하다. 그러나 추가적인 하드웨어나 정보는 시스템의 비용이 증대되는 요인이 된다. Forward Error Recovery 기반 시스템으로는 Fail-over System, DMR system, TMR system 등이 있다[7].

2-2 Backward Error Recovery

Backward Error Recovery 기법은 오류의 발생이 탐지되면, 시스템의 상태를 이전 상태로 회귀하여, 오류가 발생한 명령어를 재 수행하는 기법(Rollback and Re-execution)이다 Backward error recovery 기법은 적은 하드웨어 자원을 요구하지만, 회귀할 시스템의 중간 상태를 일정시간마다 checkpoint에 저장해야 한다. Backward error recovery는 오류검출 방법에 따라 두 가지 기법으로 분류할 수 있다. 1) 정확한 오류 검출을 기반으로 하는 기법으로 Fujitsu SPARC 64 V, IBM Z-Series, SRTR(Simultaneous and Redundantly Threaded Processor with Recovery), CRTR(Chip-Level Redundantly Threaded Processor with Recovery)과 같은 시스템과 기법이 있다. 2) 확률적인 오류 검출을 통해 시스템 rollback을 수행하는 Exposure Reduction via pipeline Squash, Fault screening with pipeline squash and re-execution 기법이 있다[7].

Ⅲ. FT_ARM(Fault Tolerant ARM) 설계

3-1 ARM 설계

본 연구에서 사용한 프로세서 모델은 ARM7을 기반으로 하고 있다. RISC 구조의 ARM은 load-store 구조, fixed-length 32bit 명령어, 3-address 명령어 형식 등의 특징을 가지고 있다. ARM의 구조와 특성에 대한 보다 자세한 사항은 참고문헌[6]을 참고하기 바란다.

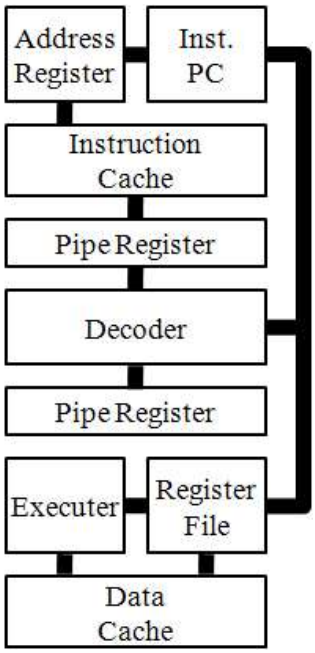

그림 1 ARM구성도
Fig.1.ARM block diagram.

본 연구에서는 ARM7 프로세서 코어를 SystemC로 설계 하였다. 그림 1은 설계한 ARM의 구성도 이다. 그림에서 보는바와 같이 ARM 프로세서의 구성요소를 모델링하고, 각각의 모듈을 통합하였다. 각 모듈의 간략한 설명은 다음과 같다.

- Increase(Inc) PC : Decoder의 제어 신호에 따라, Register File에서 받은 PC(Program Count)값을 증가.
- Address Register : 현재 PC값을 저장하고, Instruction cache로 주소와 제어신호를 전송.
- Instruction Cache : Address Register로부터 주소를 넘겨받아 해당 번지의 명령어를 Instruction Fetch Pipeline Register로 전송.
- Pipe Register : 파이프라인 동작을 위한 모듈,
- Decoder : Instruction Fetch로부터 명령어를 인가받고, operand, operator 분리.
- Register File : 1) Inc로부터 PC 값을 입력 받아, 저장하고, 다시 Inc로 Feed back, 2) 분기명령을 수행하기 위해서 Register file은 CPSR 값을 디코더로 전송하여, 해당 명령어의 실행 여부 판단 3) 디코더로부터 데이터 요청을 받으면, 인가 받은 주소 값에 해당하는 번지의 데이터를 Executor로 전송 4) Executer 혹은 Data cache로부터 데이터를 전송 받으면 내부에 기록.
- Executer : decoder에서 생성된 제어신호와 register file의 데이터 값을 전송. 제어신호에 따라 연산을 수행.
- Data cache : Executer를 통해 전송받은 제어신호에 따라 read/write 동작을 수행.

설계한 프로세서 모델의 검증을 위하여 Mibench의 jpg, gsm의 일부 코드를 선정하였으며, ARM사의 ARM developer suite(ADS)[8]로 binary file을 생성하였다. 생성된 binary file들은 명령어 메모리 모델에 적재하여 co-simulation을 실행하였다.

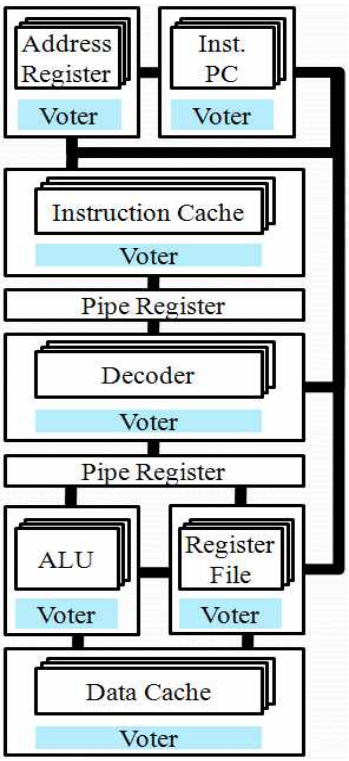

그림 2 TMR ARM구성도
Fig.2.TMR ARM block diagram.

3-2 Module Level TMR ARM 설계

TMR ARM 프로세서는 세 개의 ARM 프로세서의 모듈 별로 voter를 추가하여, micro-architecture 수준에서의 TMR 구조를 개발하였다(그림2). 각 모듈의 출력 단에 연결되어 있는 voter는 3개 모듈의 수행 결과를 입력 받아, 모듈의 출력 값을 비교한다. 출력 값 비교를 통해 오류발생 여부를 알 수 있으며, 오류 값을 제거 하고, 정상 값을 다음 모듈로 전달한다.

Ⅳ. 오류주입 실험과 결과분석

오류주입은 SystemC fault injection(SyFI) 환경을 사용하였다[9]. SyFI는 systemC로 설계한 시뮬레이션 모델에 대한 오류주입 환경을 제공한다. SyFI는 kernel 기반 오류주입 기법을 적용하여, 다양한 오류주입 시나리오를 설정 할 수 있다. 또한 SyFI는 Electronic System Level 기반 오류주입 시뮬레이션을 수행하여, 하드웨어와 소프트웨어의 통합된 시스템 환경을 대상으로 오류주입 실험을 수행 할 수 있다. 오류주입 시나리오는 1) 오류발생 유형, 2) 오류발생 빈도, 3) 오류발생 위치로 설정한다. 오류발생 유형은 오류로 발생하는 에러 값을 의미한다. 본 실험에서는 Stuck-at-0(ST0), Stuck-at-1(ST1) 값을 각각 설정 하였다. 오류발생 빈도는 오류가 발생하는 간격으로서 1 클락 사이클 동안 오류가 유지되는 일시적인 오류(Transient, 이하 T로 표기)와, 오류 값이 시뮬레이션 종료까지 지속되는 영구적 오류(Permanent, 이하 P로 표기)로 설정 한다. 오류발생 위치는 프로세서 모델에 오류를 주입하는 위치로서 임의적 방법(random)과 선택적 방법으로 설정할 수 있다. 본 논문에서는 임의적 방법에 의하여 오류주입을 수행 하였다. 이와 같은 오류주입 속성을 통해 4가지 오류주입 시나리오(TST0, TST1, PST0, PST1)를 작성하였다. 오류주입은 ARM과 TMR ARM 각각 2000회씩 수행 하였다.

그림 3은 오류주입에 의한 시스템의 상태 변화를 설명하고 있다. 그림에서 보는바와 같이 실험결과의 분류는 Fault Active(FA), System Failure(SF), Fault recovery(FR)로 분류 할 수 있다. 1) Fault Active는 시스템에 반영된 오류의 개수를 의미한다. 2) System Failure는 시스템에 발생된 오류에 의해 잘못된 연산을 수행하고, 그 결과를 Data Memory에 저장한 횟수이다. 3) Fault Recovery는 시스템에 발생된 오류가 오류 처리 알고리즘에 의해 복구 되거나, 또는 영향이 없는 오류(benign fault)로 소멸하여, 정상적인 동작을 한 경우이다.

표 1은 오류주입 실험결과를 정리한 것이다. 본 연구에서는 오류주입 시뮬레이션을 수행한 횟수 중 Fault Recovery 된 오류주입 비율을 통해 각 프로세서의 오류에 대한 강건성을 평가 하였다. ARM 프로세서의 경우 오류유형과 테스트벤치 소프트웨어에 따라 fault recovery의 편차가 심하다. 특히 1) transient fault에 비해 permanent fault를 주입할 경우, 2) stuck-at-1에 비해 stuck-at-0을 주입할 경우, 3) Telcom 프로그램에 비해 JPG 프로그램을 수행할 경우 fault recovery rate가 낮게 나오는 것을 확인 할 수 있었다. 반면 TMR ARM의 경우, 모든 실험 군에서 유사한 fault recovery rate을 보이고 있다. 또한 ARM비하여 최대 10배 이상의 fault recovery rate의 상승을 확인 할 수 있다. 이를 통해 TMR ARM이 ARM에 비해 오류에 월등이 강인함을 확인 할 수 있다.

표 1. FT_ARM 오류주입 실험결과
Table 1. Fault injection result of FT_ARM

프로그램		TST0(1) : Transient Stuck-at-0(1) PST0(1) : Permanent Stuck-at-0(1)					
		ARM			TMR ARM		
		FA	SF	FR	FA	SF	FR
JPG Program	TST0	654	400	254 (38.8%)	612	20	592 (96.7%)
	TST1	1417	708	709 (50.0%)	1388	21	1367 (98.4%)
	PST0	1384	1177	207 (14.9%)	1402	43	1359 (96.9%)
	PST1	2000	1608	392 (19.6%)	2000	47	1953 (97.6%)
Telcom Program	TST0	593	125	470 (79.2%)	566	5	561 (99.1%)
	TST1	1400	231	1169 (83.5%)	1439	2	1437 (99.8%)
	PST0	1318	904	414 (31.4%)	1239	23	1216 (98.1%)
	PST1	2000	1817	183 (9.15%)	2000	77	1923 (96.1%)

Ⅴ. 결 론

본 연구는 Safety-Critical embedded system의 개발을 위해 단일 프로세서 구조와 Triple Modular Redundancy(TMR) 구조의 임베디드 하드웨어 개발 및 신뢰성을 비교하였다. 검증대상은 Electronic system Level 도구인 SystemC를 이용하여 설계하고, 신뢰성 시험 평가는 kernel 기반 simulation 오류주입 툴인 SyFI를 이용하였다. 각 오류모델별로 2000회의 random 오류주입 실험을 수행하여 target의 상태변화를 분석 하였다. 시험결과 ARM 모델을 TMR ARM 모델로 설계할 경우, 오류복구 비율이 transient fault에서 최대 2.4배, permanent fault에서 최대 10.5배 향상되는 것을 확인 하였다. 결과를 통해 TMR ARM 프로세서 ARM 비하여 3배 이상의 비용이 증대되지만, 높은 신뢰성을 보장할 수 있어 고신뢰성 임베디드 시스템에 적합함을 확인 하였다. 향후 이와 같은 연구를 통해 프로세서 개발 전에 알 수 없는, 오류처리 능력, 오류처리에 따른 지연시간 등의 성능 지표를 산출 할 수 있을 것으로 생각된다.

감사의 글

본 논문은 국토해양부 항공선진화사업의 연구비 지원(과제번호 #07항공-항행-03)에 지원에 의함

참 고 문 헌

[1] David C. Black, Jack Donovan, Bill Bunton, Anna Keist, "SystemC:Form The Ground Up" *Springer*, 2004.

[2] L.Anghel, M. Rebaudengo, M. Sonza, Reorda, M. Violante "Multi-level Fault Effects Evaluation" *R. Velazco et.al. Radiation Effects on Embedded Systems*, pp69-88, 2007

[3] Nicholas J. Wang, Sanjay J. Patel "ReStore: Symptom-Based Soft Error Detection in Microprocessors" *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING,* VOL. 3, NO. 3, JULY-SEPTEMBER 2006.

[4] T.M.Austin "DIVA: A Reliable Substrate for Deep Submicron Microarchitecture Design" *in 32nd Annual International Symposium on Microarchitecture(MICRO),* pp.196~207, 1999.

[5] Francesco Abate, Luca Sterpone, and Massimo Violante "A New Mitigation Approach for Soft Errors in Embedded Processors" *IEEE TRANSACTIONS ON NUCLEAR SCIENCE,* VOL. 55, NO. 4, AUGUST 2008.

[6] 나종화, 류대현, 김대영 공역 "ARM System -on-Chip 구조" 홍릉과학출판사.

[7] Shubu Mukherjee "Architecture Design For Soft Errors" *Morgan Kaufmann Publishers*.

[8] http://www.freescale.com

[9] Dongwoo Lee, Jongwhoa Na, "A Novel Simulation Fault Injection Method for Dependability Analysis" *IEEE Design & Test Computers,* 11-12. 2009

이 동 우 (李東雨)

2008년 2월 : 한국항공대학교 항공전자공학과(석사)
2008년 3월~현재 : 한국항공대학교 항공전자공학과(박사과정)
관심분야 : SoC Design, Fault Tolerant Design & Simulation

김 병 영 (金炳映)

2008년 2월 : 한국항공대학교 항공전자공학과(학사)
2008년 3월~현재 : 한국항공대학교 항공전자공학과(석사과정)
관심분야 : SoC Design, Reliability

고 완 진 (高完震)

2009년 2월 : 한국항공대학교
항공전자공학과(학사)
2009년 3월~현재 : 한국항공대학교
항공공전자공학과(석사)
관심분야 : Fault Tolerant, Reliability

나 종 화 (羅宗和)

1985년 2월 : 서강대 전자공학과 졸
1988년 : Wayne State University석사
1995년 : University of Arizona 박사
2005년 ~ 현재 : 한국항공대학교
공전자공학과 부교수
관심분야 : 컴퓨터 시스템