ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 23-04-43
316
j.inst.Korean.electr.electron.eng.Vol.27,No.4,683~686,December 2023
https : //doi.org/10.7471/ikeee.2023.27.4.683

소프트 에러 발생 시 자동 복구하는 이중 코어 지연 락스텝 프로세서의 설계

Design of a Delayed Dual-Core Lock-Step Processor with Automatic Recovery in Soft Errors

김 주 호*, 양 성 현*, 이 성 수*★

Juho Kim*, Seonghyun Yang*, and Seongsoo Lee*★

Abstract

In this paper, we designed a Delayed Dual Core Lock-Step (D-DCLS) processor where two cores operate same instructions with delay and the result is compared to mitigate soft errors and common mode failures in automotive electronic systems. Because D-DCLS does not know which core an error occurred in, each core must be recovered to the point before the error occurred, but complex hardware modifications are required to return all intermediate values on the pipeline stage. In this paper, in order for easy hardware implementation, all register values are saved to a buffer whenever a branch instruction is executed. When an error is detected, the saved register values are automatically restored, and then 'BX LR' instruction is executed to return to the last branch point. The proposed D-DCLS processor was designed using Verilog HDL and was confirmed to continue normal operation after automatically recovering error.

요 약

본 논문에서는 차량 전자 시스템에서 소프트 에러와 공통 고장에 대응하기 위해 두 개의 코어를 지연 동작시킨 후 그 결과를 비교하는 D-DCLS(Delayed Dual Core Lock-Step) 프로세서를 설계하였다. D-DCLS는 어느 코어에서 에러가 발생했는지 알 수 없기 때문에 각 코어를 에러가 발생하기 이전 시점으로 되돌려야 하는데 파이프라인 스테이지 상의 모든 중간 계산값을 되돌리기 위해서는 복잡한 하드웨어 수정이 필요하다. 본 논문에서는 이를 쉽게 구현하기 위해 분기 명령어가 실행될 때마다 모든 레지스터 값을 버퍼에 저장해 두었다가 에러가 발생하면 저장된 레지스터 값을 복구한 후 'BX LR' 명령어를 수행하여 해당 분기 시점으로 자동 복구하도록 하였다. 제안하는 D-DCLS 프로세서를 Verilog HDL로 설계하여 에러가 감지되었을 때 자동으로 복구한 후 정상 동작하는 것을 확인하였다.

Key words : Delayed Lock-Step, Dual Modular Redundancy, Dual-Core Processor, System Reset, Core Recovery, Soft Error, Branch

* School of Electronic Engineering and Department of Intelligent Semiconductor, Soongsil University (Student, Student, Professor)
★ Corresponding author
E-mail: sslee@ssu.ac.kr, Tel: +82-2-820-0692
※ Acknowledgment
This work was supported by the R&D Program of the Ministry of Trade, Industry, and Energy (MOTIE) and Korea Evaluation Institute of Industrial Technology (KEIT). (20023805, RS-2022-00155731, RS-2022-00232192)
Manuscript received Dec. 11, 2023; revised Dec. 18, 2023; accepted Dec. 19, 2023.

Ⅰ. 서론

현대 자동차의 핵심 부품인 전자 제어 장치(ECU)는 차량의 다양한 기능을 통합적으로 제어하는 핵심 시스템으로써 안전성과 신뢰성이 매우 중요한 고려 사항이다. 그러나 방사선이나 전자파에 의해 발생하는 소프트 에러는 일시적으로 발생하기 때문에 감지하기 어렵고 설계 오류가 아니기 때문에 대응하기도 쉽지 않다. 이러한 소프트 에러는 ECU의 성능과 신뢰성을 저하시키고 차량 안전이 저하될 수 있다.

이러한 문제점을 해결하기 위해 지연 시간을 두고 동일한 연산을 세 개의 코어에서 수행하여 그 결과를 다수결로 비교한 후 최종 결과를 확정하는 D-TCLS(Delayed Tripple Core Lock-Step) [1]-[4]가 제안되었다. D-TCLS는 세 개의 코어가 지연되어 동작하므로 여러 코어에서 동시에 같은 오류가 발생하지 않도록 설계되었으며 하나의 코어에서 소프트 에러가 발생해도 정상적으로 동작한다. 그러나 이 아키텍처는 세 개의 코어를 사용하여 전체 시스템의 크기가 커지는 단점이 있다. 본 논문에서는 코어 크기를 줄이고자 지연 시간을 두고 동일한 연산을 두 개의 코어에서 수행하여 그 결과를 비교하여 소프트 에러를 감지하는 D-DCLS(Delayed Dual Core Lock-Step)[5] 프로세서를 설계하였다.

D-DCLS는 코어 두 개만을 사용하므로 어떤 코어에 에러가 발생했는지를 판단할 수 없다. 그러므로 에러가 발생하면 고장 난 코어를 판단하지 않고 에러가 발생하기 전으로 복구하도록 설계하였다. 제안하는 D-DCLS 프로세서는 ARM사의 Cortex-M3 프로세서 코어[6]와 AHB Lite 버스를 이용해 구성하였으며 IDEC(IC Design Education Center)에서 제공하는 설계 도구를 사용하여 Verilog HDL로 설계한 후 Xilinx사의 Vivado를 사용하여 검증하였다.

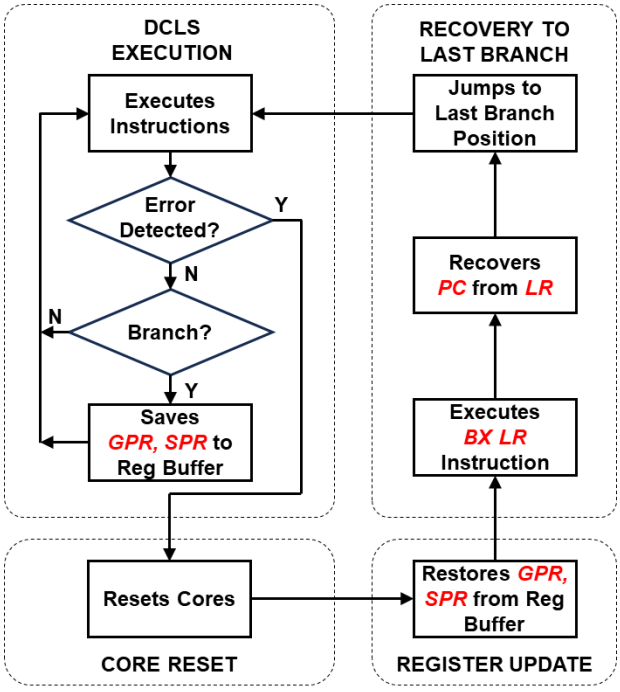

Fig. 1. Flowchart of the proposed D-DCLS processor.
그림 1. 제안하는 D-DCLS 프로세서의 순서도

Ⅱ. 하드웨어 수정을 최소화하는 오류 복구 방법

D-DCLS 프로세서에서 소프트 에러로 인한 오류의 감지는 두 개의 코어가 출력한 값이 일치하는지를 보면 되기 때문에 비교적 간단하다. 그러나 두 개의 코어만 사용하면 어느 코어에서 오류가 발생했는지를 알 수 없기 때문에 두 개의 코어를 모두 리셋하고 오류가 발생하기 이전 시점으로 되돌려야 한다. 이때 파이프라인 스테이지 상의 모든 계산값까지 되돌려야 하는데 이 과정이 상당히 어렵고 복잡하다. 제안하는 D-DCLS 프로세서는 이를 간단하게 구현하기 위해서 다음과 같은 기법을 사용하였다.

(1) 분기(Branch) 시에 GPR, SPR 저장

ARM 프로세서에서 분기가 이루어지면 코어에서 플러시(Flush)가 발생하며 코어 내의 모든 명령어와 파이프라인 스테이지 내의 중간 계산값이 초기화된다. 따라서 오류가 발생했을 때 가장 최근의 분기 시점으로 되돌아가도록 설계하면 파이프라인 스테이지 상의 중간 계산값을 별도로 되돌릴 필요가 없어져서 하드웨어가 간단해진다.

단, 가장 최근의 분기 시점까지 되돌아가기 위해서는 해당 시점의 레지스터 값으로 복구할 필요가 있으며 이를 위해 제안하는 D-DCLS 프로세서는 분기(Branch) 명령어가 실행될 때마다 그림 1과 같이 메인 코어의 General Purpose Register(GPR)와 Special Purpose Register(SPR) 값들을 별도의 버퍼에 저장해놓는다.

(2) BX LR 명령어를 이용한 복구

제안하는 D-DCLS 프로세서는 오류 복구를 위해 'BX LR' 명령어[6]를 사용한다. 'BX LR'은 Link register(LR)에 저장된 주소를 읽어와 현재 Program Counter(PC) 값을 해당 주소로 업데이트하는 역할을 수행하는 명령어로 복구 과정에서 중요한 역할을 한다.

제안하는 D-DCLS 프로세서는 오류가 발견되면 가장

최근에 수행한 분기 시점에 별도의 버퍼에 저장해둔 GPR, SPR 값들을 LR을 포함하여 두 코어에 패치하고 그 다음에 'BX LR' 명령어를 수행한다. 이를 통해 오류 발생 시 최근에 수행한 분기 지점으로 정확하게 복구가 이루어진다.

'BX LR' 명령어의 활용은 오류 이전 분기 명령이 수행되던 시점으로 정확히 복구하는 동시에 오동작하고 있는 코어의 파이프라인 스테이지 상의 모든 중간 계산값을 초기화하여 이후 정상 동작을 가능하게 해준다. 이러한 방법을 통해 IP 형태로 도입된 프로세서 코어의 복잡한 파이프라인 스테이지를 수정하지 않고도 손쉽고 정확하게 D-DCLS 프로세서를 구현할 수 있다.

Ⅲ. 오류 발생 시 최근 분기 시점으로의 복구 동작

제안하는 D-DCLS 프로세서는 그림 1의 순서도에 따라 동작하며 그 아키텍쳐는 그림 2와 같다. 에러가 발생하면 코어를 초기화하고 레지스터 값을 미리 저장한 값으로 되돌린 다음에 분기 명령어 패치를 통해 가장 최근의 분기 시점으로 복구를 완료한다. 각 단계에 대한 설명은 다음과 같다.

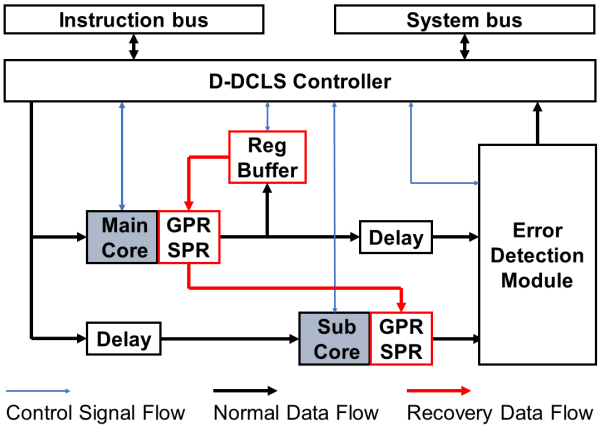

Fig. 2. Architecture of the D-DCLS processor.
그림 2. 제안하는 D-DCLS 프로세서의 아키텍쳐

(1) DCLS EXECUTION

오류 발생 시 복구를 위해 코어가 동작하는 도중에 분기 명령어가 실행될 때마다 코어 내부의 GPR, SPR값을 별도 버퍼에 안전하게 저장한다. 분기 명령어가 실행될 때마다, 현재의 GPR 및 SPR 값을 계속 업데이트하여 최신 상태를 유지한다.

(2) CORE RESET

오류가 발견되면 오류 복구를 위해 모든 코어를 초기화한다.

(3) REGISTER UPDATE

가장 최근 분기 시점에서 버퍼에 저장해 둔 GPR 및 SPR 값을 LR을 포함하여 각 코어로 복사한다. 이로써 오류 발생 이전 상태로 복구가 가능하다.

(4) RECOVERY TO LAST BRANCH

각 코어에 'BX LR' 명령어를 패치하여 LR값을 불러와 PC값을 업데이트한다. 이를 통해 각 코어는 오류 발생 이전의 가장 최근 분기 상태로 동기화되면서 복구를 완료한다.

Ⅳ. 설계 및 검증

본 논문에서 제안하는 D-D친 프로세서의 아키텍쳐는 그림 2와 같다. 서브 코어는 공통 모드 고장을 피하기 위해서 메인 코어보다 지연된 입력값을 받게 된다. 메인 코어는 분기 명령어가 탐지될 때마다 GPR, SPR값을 별도 버퍼로 옮긴다. 오류 탐지 모듈은 메인 코어의 지연된 출력값과 서브 코어의 현재 출력값을 비교하여 오류를 탐지한다. 오류 탐지 모듈이 D-DCLS 컨트롤러로 오류 감지 신호를 보내면 D-DCLS 컨트롤러는 각 코어를 초기화하고 GPR, SPR값을 복구한 다음에 'BX LR' 명령어를 패치한다. 이 아키텍처는 프로세서 코어에서 파이프라인 스테이지 내부의 중간 계산값을 저장하고 복구할 필요가 없기 때문에 하드웨어 구현이 간단하고 프로세서 코어 내부를 수정하는 과정에서 발생할지 모르는 설계 오류를 최소화할 수 있다.

시뮬레이션에서는 소프트 에러를 유발하기 위해 무작위 숫자를 코어 내부 레지스터에 주입하였다. 먼저 오류 발생 이전의 최근 분기 명령어가 실행된 단계에서는 분기 명령어가 감지되면 해당 시점의 메인 코어의 GPR와 SPR 값을 버퍼에 안전하게 저장한다. 동작 도중 에러가 탐지되면, 그림 3의 ⓐ와 같이 코어를 초기화한다. 초기화 이후에는 그림 3의 ⓑ에서 확인할 수 있듯이 'BX LR' 명령어가 패치된다. 이는 그림 3의 ⓒ와 같이 PC값이 0x00000792 주소로 이동함을 의미한다. 이로써 시스템은 에러 발생 이전의 상태로 정확하게 돌아가며 안정적으로 복구됨을 확인할 수 있다.

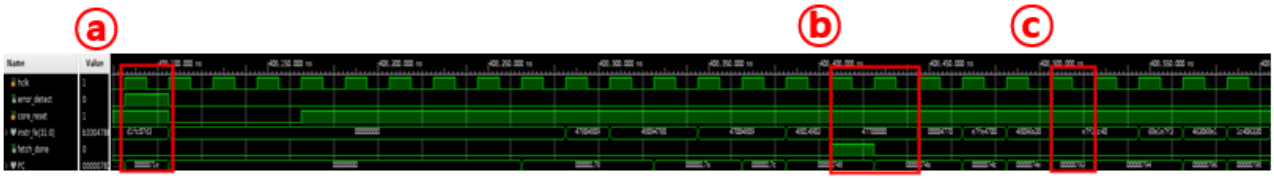

Fig. 3. Waveforms of error occurrence, detection, and recovery.
그림 3. 오류 발생, 감지 및 복구 과정 파형

V. 결론

본 논문에서는 소프트 에러 및 공통 고장과 같은 안전 및 신뢰성 문제에 대한 효과적인 대응책으로 D-DCLS 프로세서를 설계하였다. 이 아키텍처는 선행 연구인 D-TCLS의 오류 복구 기능을 이어가면서도 두 개의 코어만을 사용하여 하드웨어 크기를 많이 줄일 수 있다. BX_LR 명령어를 활용한 복구 메커니즘은 오류가 발생한 코어의 GPR 및 SPR 값들을 복구하고 LR 주소로 최근에 분기한 시점의 PC 값을 이동시키는 역할을 한다. 이를 통해 오류가 발생하기 이전의 최근 분기 상태로 코어를 자동으로 복구할 수 있다. 특히 이 기법은 코어 내부의 파이프라인 스테이지를 수정할 필요가 없어서 구현이 간단하고 혹시 모르는 설계 오류를 최소화할 수 있다. 이러한 D-DCLS 프로세서의 구현을 통해 차량 전자 시스템의 안전성을 높이는데 기여할 것으로 기대된다.

References

[1] W. Lee, K. We, S. Kim, and C. Lee, "Simulator Structure for Lockstep ECU,", *Proceedings of Korea Computer Congress,* pp. 1508-1510, 2017.
[2] S. Yang, J. Choi, and S. Lee, "Design of Delayed Triple-Core Lock-Step Processor with Memory Rollback for Automotive Applications," *J.inst.Korean. electr.elctron.eng.*, vol.26, no.4, pp.628-632, 2022.
[3] S. Yang, "Design of a triple-core, delay-locked loop system with memory rollback capability using ARM Cortex cores," *Master Thesis, Soongsil University,* 2023.
[4] S. Yang, J. Kim, and S. Lee, "Design of a Delayed Triple-Core Lock-Stop Processor with Auto-Recovery from Soft Errors," *J.inst.Korean. electr.elctron.eng.*, vol.27, no.2, pp.165-171, 2023.
[5] K. Marcinek and W. Pleskacz, "Variable Delayed Dual-Core Lockstep (VDCLS) Processor for Safety and Security Applications," *MDPI Electronics,* vol.12, no.2, pp.464-481, 2023.
DOI: 10.3390/electronics12020464
[6] ARM, "Cortex-M3 Devices Generic User Guide", https://developer.arm.com/documentation/dui0552/a/?lang=en