철도신호용 임베디드시스템의 고장모드도출에 관한 연구

A Study on the Failure Mode Identification of Railway Signaling Embedded System

신덕호* 이재호* 이강미* 김용규*

Shin, ducko Lee, Jae-Ho Lee, Kang-Me Kim, Young-Kye

ABSTRACT

This paper is about the study on the failure mode identification of railway signaling embedded system thru which quantitative reliability and safety can be compared reciprocally. Frequency of each failure mode makes possible to compare the reliability of each system and frequency of dangerous failure is used as the measurement standards for system safety. Therefore, this paper provides both reliability-related failure mode and safety-related failure mode by modeling the railway signaling embedded system.

1. 서 론

본 논문은 철도신호분야에 사용되는 임베디드시스템(Embedded System)의 신뢰성과 안전성을 정량적으로 표현하여 상호비교를 가능하게 하는 고장모드의 도출에 대한 연구이다. 고장모드별 발생빈도는 서로 다른 시스템의 신뢰성 비교를 가능하게 하며, 사고와 관련된 위험측고장에 대한 발생빈도는 안전성확보의 평가기준으로 사용된다. 따라서, 본 논문에서는 철도신호분야에 사용되는 임베디드 시스템을 모델링하여 신뢰성 및 안전성에 대한 각각의 고장모드를 제시한다.

2. 본 문

임베디드시스템은 전원이 인가되면 스스로 부팅하여 임무를 수행하는 최소단위로 정의할 수 있다. 따라서, 마이크로프로세서 또는 마이크로컨트롤러를 포함한 하드웨어구조는 기존의 계전기베이스 전기시스템에 비하여 크기와 전력소모량이 혁신적으로 감소하게되고, 소프트웨어에 의한 제어는 시스템의 업그레이드와 변경이 간소화 되어 철도분야에서 다양하게 사용되고 있다.

특히 철도분야에서 가장 많은 제어를 담당하는 신호분야에서는 전자연동장치, 건널목보안장치, 고속선 ATC장치, 기존선 ATP장치 등 다양한 분야에 적용되고 있다. 하지만 마이크로프로세서를 기반으로 하는 임베디드시스템은 약전으로 구동되므로 환경적인 영향을 많이 받게 되었으며, 오류를 포함하는 소프트웨어에 의해서도 고장이 빈번하게 발생하고 있다. 철도신호분야에서 제어를 담당하는 임베디드시스템의 고장은 간단하게는 정상동작을 표시하는 LED의 고장과 같이 유지보수의 불편을 초래할 수 있으며, 심각하게는 신호기의 제어출력이나 궤도회로의 입력관련 고장과 같이 열차의 충돌이나 추돌을 발생시킬 수 있다.

* 한국철도기술연구원, 열차제어연구팀, 회원

E-mail : ducko@krri.re.kr

TEL : (031)460-5442 FAX : (031)460-5449

따라서, 본 논문에서는 이러한 철도신호분야에서 사용되는 임베디드시스템을 모델링하여, 제어기 내부에서 발생되는 고장의 영향을 판단하여 안전측과 위험측고장에 대한 발생빈도를 정량적으로 산출하였다.

2.1 임베디드시스템 모델링

마이크로프로세서를 사용한 임베디드제어기의 최소구성은 그림 1과 같이 Reset회로, 제어버스디코더, 동작클럭, 타이머, 메모리, 병렬IO, 직렬IO로 간략화 할 수 있다. 또한 이러한 기본구성을 내장한 마이크로컨트롤러를 사용하는 제어기의 내부도 유사하게 간소화 할 수 있다.

위험측고장에 대한 고장모드의 영향을 분석하기 위해서는 제어기에 임무를 부여하여야 한다. 따라서 본 논문에서 제시한 임베디드시스템 모델은 다른 제어기로부터 시리얼통신으로 수신된 데이터를 바탕으로 병렬IO를 Vital제어하는 임무를 부여하였다. 이러한 경우는 선로전환기 전환을 요구하는 전자연동장치의 안전필수기능을 모델한 것이다.

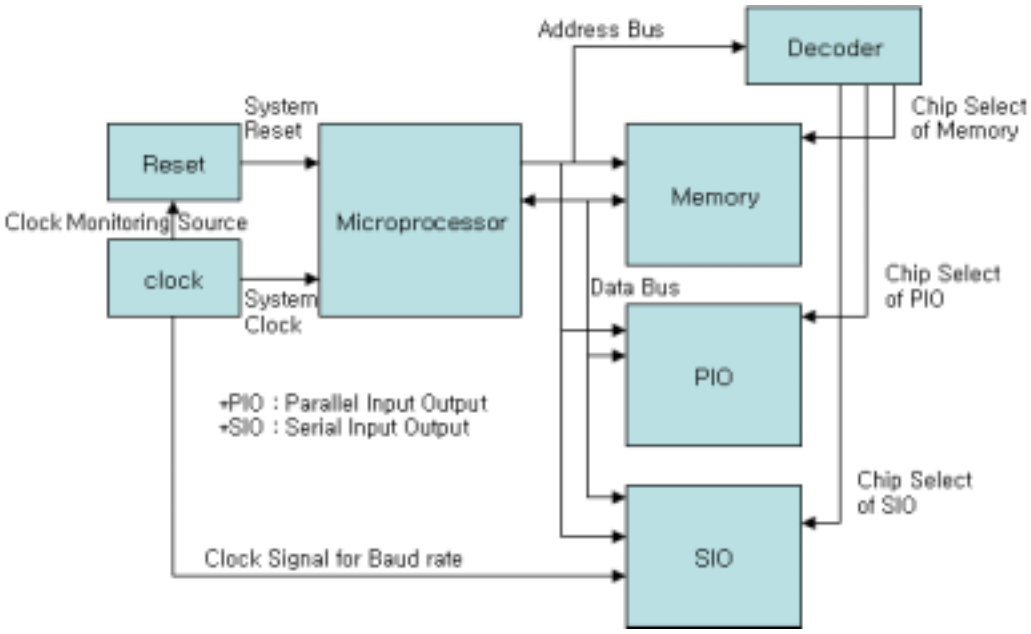

그림 1. 임베디드시스템 모델의 구성도

그림 1에서 마이크로프로세서는 시스템클럭, 리셋입력, 디바이스 데이터입력을 받아 연산을 수행하고, 그 결과를 어드레스버스와 데이터버스를 통해 디코더를 통해 선택된 디바이스로 전송하여 제어를 수행하는 기본적인 임베디드시스템의 최소구성이다.

일반적으로 철도신호분야에 임베디드시스템을 적용하기 위해서는 그림 1의 직렬입출력디바이스인 SIO에 RS232, RS422, RS485, Ethernet, 광통신 등의 해당 응용분야 목적에 부합하는 어댑터를 추가하여 직렬데이터를 송수신하지만, 본 논문에서는 다양한 제어기의 공통 핵심부분에 대한 분석을 목적으로 하므로 어댑터는 모델링에서 제외하였다. 또한, 동일한 사유에 의해 병렬입출력디바이스인 PIO의 어댑터도 제외하였다.

2.2 임베디드시스템 모델의 FMEA

FMEA(Failure Mode and Effect Analysis)를 위해서는 제어기의 목적 및 최소한의 동작조건이 전제되어야 한다. 본 논문에서는 앞의 2.1에서 언급한 바와 같이 SIO를 통해 입력된 전문을 분석하여 PIO를 통해 Vital 제어를 수행하는 철도신호분야의 대표적 응용사례를 모델링된 제어기의 응용프로그램으

로 가정하였으며, 다음과 같은 추가적인 가정이 FMEA수행을 위해 사용되었다.

가. Reset회로는 Clock으로부터 System Clock과 동일한 Clock Monitoring Source를 입력받아 리트리거블원샷(일정한 주파수에 해당하는 클럭입력이 수신되지 않으며, 자동으로 리셋을 수행)방식으로 결함을 검출한다.
나. 제어기로 입력되는 시리얼정보는 CRC등의 정보여분(Information Redundancy)을 이용하고, 재시도 등의 시간여분(Time Redundancy)을 사용하여 전문에 포함된 결함을 검출한다.
다. 소프트웨어에 의해 결함이 검출되면 PIO는 현재상태를 유지한다.
라. 소프트웨어 재기동시 PIO는 초기화 된다.
마. PIO의 출력이 결함에 의해 변경되는 경우를 위험측으로 정의한다.
바. 전원은 분석의 범위에서 제외한다.

위의 가정을 고려하여 임베디드시스템을 구성하는 하부구성요소별 FMEA를 실시하면 표 1과 같다. 또한 구성요소별 FMEA 수행의 기준이 되는 고장모드는 설계경력이 있는 엔지니어의 경험에 의해 선택되었다.

표 1. 임베디드시스템 모델의 FMEA

분석대상	고장률 표 기	고장모드	고장영향	고장결과
Clock	λ_{clock}	클럭없음	Reset 회로에 의해 고장이 검지되고 MP는 Reset이 걸리므로 PIO는 현재상태 유지	안전측고장
		정상보다 늦음		
		정상보다 빠름	빨라진 Clock에 의해 SIO입력의 텔레그램이 깨지므로 S/W에 의해 PIO는 이전상태 유지	안전측고장
Reset	λ_{reset}	요구하지 않은 Reset	MP를 초기화하고 S/W의 구동을 억제하므로 PIO는 이전상태를 유지	안전측고장
MP	λ_{MP}	무응답(동작하지 않음)	PIO의 제어출력은 이전상태를 유지	안전측고장
		잘못된 연산수행 (SIO입력에 대한 오류)	MP의 PIO출력결과를 예상할 수 없음	**위험측고장**
		잘못된 연산수행 (PIO출력에 대한 오류)		
Decoder	$\lambda_{decoder}$	출력없음	MP의 요청에 따른 디바이스가 선택되지 않음 (PIO는 이전상태를 유지)	안전측고장
		잘못된 출력	MP의 요청에 따른 디바이스가 잘못 선택되는 경우 PIO의 출력이 변경될 수 있음	**위험측고장**
Memory	λ_{memory}	저장된 데이터의 결함(사용하는 영역)	PIO의 제어출력상태를 변경할 수 있음.	**위험측고장**
		저장된 데이터의 결함(사용하지 않는 영역)	PIO의 제어출력상태를 변경하지 않을 수 있음	안전측고장
PIO	λ_{PIO}	이전상태가 변경되는 고장	PIO의 제어출력은 변경	**위험측고장**
		이전상태를 유지하는 고장	PIO의 제어출력은 이전상태 유지	안전측고장
SIO	λ_{SIO}	입력이 MP에 전송되도록 수신버퍼에 저장되지 않음(이전상태 유지)	PIO의 제어출력상태 변경 없음	안전측고장
		입력전문에 대하여 순간적인 결함에 의해 가용한 데이터로 오류발생	MP에 의해 수신재시도 하므로 PIO의 제어출력상태 변경 없음	안전측고장

*MP : Microprocessor, S/W : Software

2.3 고장결과별 발생빈도

표 1의 FMEA결과에 따라 고장결과를 “안전측고장”과 “위험측고장”으로 나누어 각각에 대하여 산출하면 각각 (식 1)과 (식 2)와 같이 표현할 수 있다.

$$\lambda_{functionalfailure} = \lambda_{clock} + \lambda_{reset} + \lambda_{MP} + \lambda_{decoder} + \lambda_{memory} + \lambda_{PIO} + \lambda_{SIO} \quad \text{(식 1)}$$

$$\lambda_{Dangerousfailure} = \lambda_{MP} + \lambda_{decoder} + \lambda_{memory} + \lambda_{PIO} \quad \text{(식 2)}$$

따라서, (식 1)과 (식 2)의 기능고장에 대한 수식과 위험측고장에 대한 수식에 해당 디바이스의 고장률을 대입하여 표 2의 전기전자제어기의 안전무결성레벨(SIL, Safety Integrity Level) 고장률의 범위와 비교하여 임베디드시스템의 SIL을 평가할 수 있다. 표 2에서 신뢰성측면의 고장률은 (식 1)과 같이 기능상실에 대한 SIL의 할당범위이며, 표 2의 위험측고장률은 (식 2)와 같이 위험측 고장의 발생빈도에 대한 SIL의 할당범위이다.

표 2. SIL레벨에 따른 고장률 범위

SIL	신뢰성측면의 고장률(/Hour)	안전성측면의 위험측고장률(/Hour)
4	≧1E-5 to 1E-4	≧1E-9 to 1E-8
3	≧1E-4 to 1E-3	≧1E-8 to 1E-7
2	≧1E-3 to 1E-2	≧1E-7 to 1E-6
1	≧1E-2 to 1E-1	≧1E-6 to 1E-5

3. 결론

본 논문에서는 철도신호분야에 사용하는 임베디드시스템을 모델링하여 FMEA를 통해 안전측과 위험측고장에 대한 발생빈도를 각각 산출하였다. 기존 임베디드시스템의 고장률 산출에 사용되던 방법인 사용부품의 고장률을 모두 더하는 방식은 사고의 원인이 되는 위험측고장에 대한 정량적인 고장률산출이 불가능하였으며, 이러한 단점을 보완하기 위해 본 논문에서는 부품단위 FMEA를 통해 고장모드별 영향을 평가하고, 영향의 결과를 안전측과 위험측으로 정량화 하기 위한 방법을 제안하였다.

이러한 연구는 최근 철도신호분야에서 논의되고 있는 정량적 평가지표에 의한 안전확보를 위해 필요한 위험측고장률 산출을 임베디드시스템을 대상으로 적용하기 위한 방안을 제시하였으며, 향후에는 응용분야에 따라 복잡도가 증가하는 다양한 구조의 임베디드시스템에 대한 FMEA와 고장모드에 대해서도 연구가 진행될 것이다.

참고문헌

1. Dhiraj K. Pradhan(1996), “Fault-Tolerant computer system Design”, Prentice Hall.
2. 김영태(2006), “철도신호제어시스템(개정4판)”.
3. Barry W. Johnson(1989), “Design and Analysis of Fault-Tolerant Digital Systems”.
4. MIL-STD-1629A(1980),“Procedures for Performing a FMECA”.