한국철도학회논문집
제9권 제6호 2006년 ▌ pp. 725-731

자기검사회로를 이용한 대기이중계구조 결함허용제어기의 설계 및 신뢰도평가에 관한 연구

A Study on Design and Reliability Assessment for Embedded Hot-Standby Sparing FT System Using Self-Checking Logic

신덕호† · 이재호* · 이강미** · 김용규*
Ducko Shin · Jae-Ho Lee · Kang-Mi Lee · Young-Kyu Kim

Abstract

Hot Standby sparing system detecting faults by using software, and being tolerant any faults by using Hardware Redundancy is difficult to perform quantitative reliability prediction and to detect real time faults. Therefore, this paper designs Hot Standby sparing system using hardware basis self checking logic in order to overcome this problem. It also performs failure mode analysis of Hot Standby sparing system with designed self checking logic by using FMEA (Failure Mode Effect Analysis), and identifies reliability assessment of the controller designed by quantifying the numbers of failure development by using FTA (Fault Tree Analysis)

Keywords : Hot-Standby Sparing(대기이중계), Self-Checking Logic(자기검사회로), FMEA(Failure Mode Effect Analysis), Reliability(신뢰도), Fault-Tolerance(결함허용)

1. 서 론

대기이중계(Hot-Standby Sparing)시스템은 제어기 내부에서 발생된 결함(Fault)을 검출하여 결함발생 제어기를 격리(Isolation)하고, 하드웨어 여분(Redundancy)을 사용하여 기능요구사항을 계속 수행하는 대표적인 하드웨어 여분구조의 결함허용(Fault Tolerance)시스템이다[1].

철도신호분야에서는 제어기 내부에서 결함이 발생하면 시스템이 기능을 상실하여 대규모 지연 등의 막대한 손실이 발생하거나 사고의 원인이 되므로 가용도(Availability)향상 및 안전성(Safety)확보를 목적으로 제어기를 결함허용 구조로 설계한다. 기본적인 가용도의 향상 외에도 다중계구조 제어기에 기대되는 기능요구사항을 주어진 시간동안 유지시킨다는 관점에서 신뢰도(Reliability)와도 밀접한 관계를 갖는 이중계구조 제어기의 사용은 철도신호분야의 전자연동장치, 궤도회로장치, 차상제어장치와 같은 응용분야에 이미 일반화된 설계이다[2]. 철도신호분야에서 이중계구조로 제어기를 설계하는 필요성은 각각의 시스템에 대하여 평균고장시간(MTBF) 및 연간서비스시간(Up Time)에 대한 정량적 목표의 만족을 시스템도입의 요구사항으로 제시하고 있으므로, 이를 만족하기 위해서는 다중계구조로 제어기를 설계해야 하기 때문이다.

본 논문의 2장에서는 하드웨어 여분을 사용한 결함허용 시스템에서 대기이중계구조 제어기에 대한 정의와 소프트웨어를 사용한 결함허용 구조의 문제점을 제시하였으며, 3장에서는 하드웨어로 자기검사회로(Self-Checking Logic)를 설계하기 위한 요구사항을 제어기 계절체에 대한 FMEA(Failure Mode Effect Analysis)를 사용하여 도출하고, 도출된 요구사항을 만족하기 위한 자기검사회로의 설계 및 설계된 자기검사회로를 포함한 대기이중계구조 제어기의 신뢰도를 평가하여 하드웨어기반 결함허용 시스템의 신뢰성 및 안전성의 정량적 평가를 수행하였다.

† 책임저자 : 회원, 한국철도기술연구원, 전기신호연구본부 공학박사
E-mail : ducko@krri.re.kr
TEL : (031)460-5442 FAX : (031)460-5449
* 회원, 한국철도기술연구원, 전기신호연구본부 책임연구원 공학박사
** 회원, 한국철도기술연구원, 전기신호연구본부 연구원

2. 소프트웨어기반 대기이중계구조 제어기

2.1 하드웨어 여분을 이용한 결함허용

제어기 내부에서 발생된 결함을 허용하여 시스템의 기능요구사양을 유지하는 결함허용시스템은 하드웨어여분, 소프트웨어여분, 정보여분, 시간여분 등의 다양한 여분을 사용하여 표 1과 같이 결함을 허용한다[3].

표 1에서 하드웨어여분의 경우 짝수개의 여분으로 구성하는 능동형 이중계구조는 각 여분의 연산결과를 비교하여 불일치를 통해 결함을 검출하며, 2 out of 3와 같이 수동형 TMR (Tripple Modular Redundancy)구조는 다수결논리에 의해 발생된 결함을 은폐(Masking)하는 것이 기본개념이다[3].

표 1. 결함허용을 위한 여분

여분형태	허용결함	적용 예
하드웨어	제어기내부 부품 및 소프트웨어의 결함	Standby Sparing 2 out of 3
소프트웨어	소프트웨어 개발에 포함된 코딩 오류 및 컴파일러 오류	N-Version Programing
시간	노이즈 등의 일시적 데이터결함	재시도 후 비교
정보	데이터 통신에서 발생하는 일시적 데이터 결함	CRC Checking

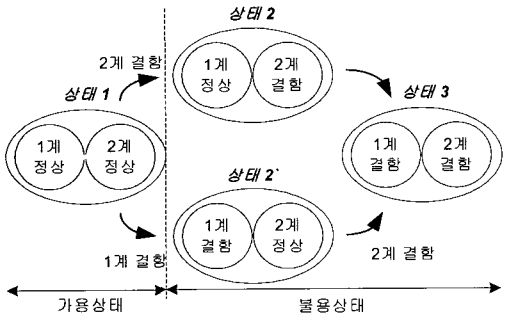


그림 1. 결함의 검출을 위한 이중계구조 상태다이어그램

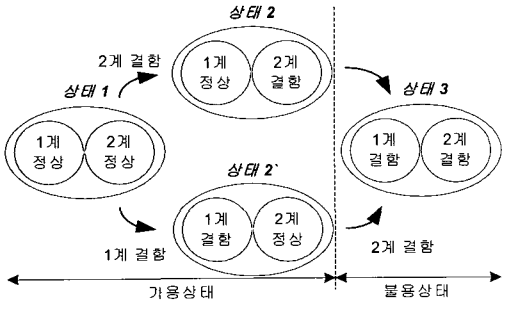


그림 2. 결함의 허용을 위한 이중계구조 상태다이어그램

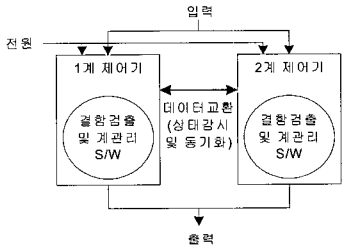
대기이중계구조 제어기는 표 1의 하드웨어여분에 포함되며, 한 번에 한 개씩 발생하는 결함의 허용을 위해 동일한 구조의 제어기를 복수로 구성하는 제어기를 대기이중계구조로 정의한다[3]. 이중계구조 제어기는 그림 1과 그림 2에서와 같이 결함의 검출을 목적으로 하는가와 허용을 목적으로 하는가에 따라 결함발생에 따른 기능유지의 여부가 서로 상이하므로 반드시 구분되어야 한다.

따라서 그림 2와 같이 결함허용을 목적으로 한 이중계구조 제어기를 구성하기 위해서는, 제어기 내부에서 발생한 결함을 검출하여 결함이 발생된 제어기를 격리(Location)하고 제외시키기 위한 결함검출 논리가 반드시 포함되어야 한다.

2.2 소프트웨어기반 결함검출의 대기이중계시스템

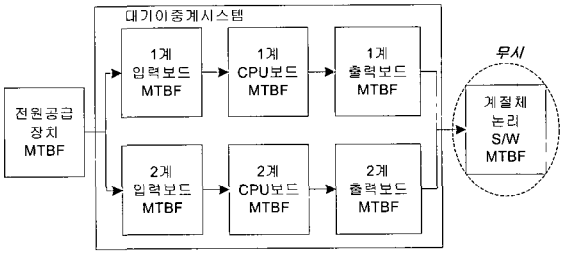
결함허용을 위한 이중계구조 제어기에서 결함의 발생을 검출하여 발생된 부분을 격리하기 위한 방안으로 가장 선호되는 방법이 그림 3과 같은 구조의 소프트웨어 결함검출 논리를 내장한 이중계구조의 구성이다.

하지만 결함검출 및 여분관리를 수행하는 핵심기능이 소프트웨어로 구성됨에 따라 다음과 같은 문제점이 발생한다. 첫째 결함검출 및 여분관리를 수행하는 소프트웨어의 고장률을 정량적으로 산출할 수 없다. 둘째 계간의 통신에 의존하는 소프트웨어 결함검출 방식에서 통신인터페이스의 결함발생 또는 소프트웨어 내부의 오류(Error)는 결함발생에도 불구하고 두 계가 모두 정상으로 인식하여 각기 다른 출력을 발생하는



*S/W(Software)

그림 3. 소프트웨어기반 결함검출방식의 이중계구조의 구성도



*MTBF(Mean Time Between Failure), RBD(Reliability Block Diagram)

그림 4. 소프트웨어기반 결함검출방식의 이중계구조의 RBD

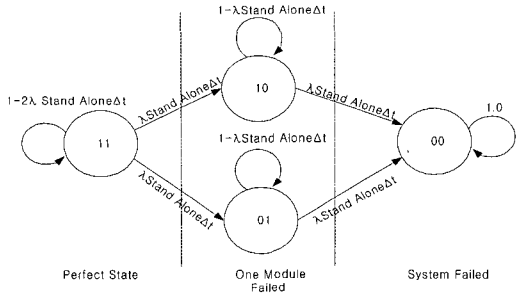


그림 5. 대기이중계구조의 이론적 상태천이도

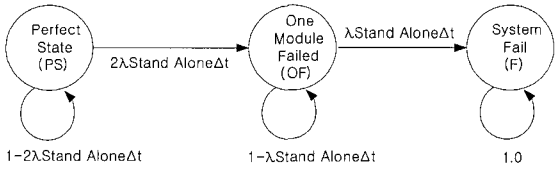


그림 6. 대기이중계구조의 이론적 Markov모델

위험측고장 상태로 발전될 수 있다.

특히 첫 번째의 경우 그림 4와 같이 소프트웨어의 고장률은 0으로 가정하여 시스템의 신뢰도를 모델링하게 되어, 예측신뢰도와 시험에 의한 입증신뢰도간 차이발생의 주요 원인이 된다.

그림 3의 이중계구조를 시스템 상태천이도로 표현하면 그림 5와 같다.

그림 5의 상태천이도를 Markov모델링하면 그림 6과 같이 표현할 수 있으며, PS상태와 OF상태까지를 시스템의 정상상태로 구분하여 신뢰도함수를 식 (1)과 같이 이론적으로 제시할 수 있다.

$$R_{HotStandby}(t) = p_{PS}(t) + p_{OF}(t) = 2e^{-\lambda t} - e^{-2\lambda t} \quad (1)$$

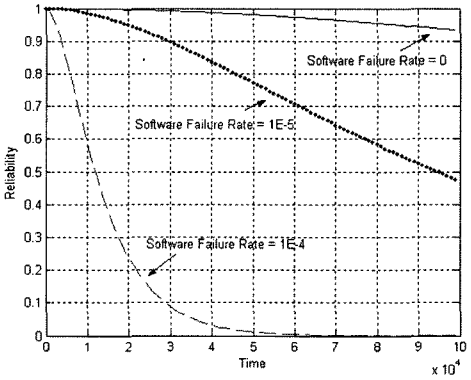
$$\lambda_{HotStandby} = \frac{\lambda}{\sum_{i=n-q}^{n} \frac{1}{i}} = \frac{2\lambda}{3} \quad (2)$$

λ = Single Module Failure

이러한 이중계구조 신뢰도의 이론적 모델은 그림 4의 RBD에서 제시한 바와 같이 이중계구조의 여분관리에 해당하는 결함검출, 격리, 제외, 재구성에 해당하는 모든 소프트웨어의 고장률을 0으로 가정한 결과이다. 따라서 전원공급장치(λ_{PSU}), 입력보드(λ_{IN}), CPU보드(λ_{CPU}), 출력보드(λ_{OUT})의 고장률을 10^{-6} 로 가정하고, 여분관리 소프트웨어의 고장률(λ_{SW})을 각각 0, 10^{-5} 및 10^{-4}로 가정하여 이중계구조 시스템의 MTTF와 시간에 따른 신뢰도를 예측하면 표 2 및 그림 7과 같은 결과를 얻을 수 있다.

표 2. 여분관리 소프트웨어 고장률별 이중계구조 시스템 MTTF

계관리SW 고장률(/Hour)	고장률 산출수식(/Hour)	MTTF (Hour)
0	$\lambda_{PSU}+[2/3(\lambda_{IN}+\lambda_{CPU}+\lambda_{OUT})]+0$	333,333
10^{-5}	$\lambda_{PSU}+[2/3(\lambda_{IN}+\lambda_{CPU}+\lambda_{OUT})]+10^{-5}$	76,923
10^{-4}	$\lambda_{PSU}+[2/3(\lambda_{IN}+\lambda_{CPU}+\lambda_{OUT})]+10^{-4}$	9,708



*PSU의 고장률은 시뮬레이션에서 제외

그림 7. 여분관리 소프트웨어 고장률별 이중계구조 시스템 신뢰도

2.3 소프트웨어기반 대기이중계구조의 문제점

위 2.2의 기술적 문제점과 소프트웨어 고유의 단점을 정리하면 소프트웨어기반 대기이중계구조의 대표적 문제점은 다음과 같다.

- 순차수행을 전제로 하는 소프트웨어는 결함검출에 대한 실시간검출이 불가능하다.
- 위험측고장인 제어기 출력의 예측불가 상태에 대한 정량적 발생빈도를 산출할 수 없다.

첫 번째 문제점에 대해서는 멀티태스킹 구조의 소프트웨어 포팅을 적용하여 결함의 검출시간을 단축시킬 수 있으나, 멀티태스킹도 결함검출 알고리즘이 수행되는 소프트웨어 모듈을 OS 틱타이머에 의한 멀티쓰레드로 수행하므로 결국에는 순차적 결함검출 알고리즘의 수행의 형태가 되어 하드웨어 수준의 실시간 결함검출은 불가능하다.

두 번째 문제점은 결함의 검출을 위한 이중계구조 제어기의 소프트웨어 고장률을 무시한 표 2의 결과와 같이 전체시스템의 신뢰도목표 만족여부를 설계단계에서 추정하기에 부적절하며, 시운전을 통한 신뢰도입증치가 예측치와 불일치하게 되는 주요 원인이 된다. 또한 철도신호분야와 같은 안전기반 시스템에서는 제어기에 대한 기능상실에 대한 고장률뿐만 아니라, 여분관리 기능과 같은 특정기능에 대한 고장률을 활용하여 위험원에 대한 발생빈도를 정량적으로 예측하고 입증한다.

이러한 연구를 위해서는 FMEA(Failure Mode Effect Analysis)나 HAZOP(Hazard and Operability) Study와 같은 기능별 고장의 발생빈도 및 심각도에 대한 정량화가 필수적이다. 소프트웨어기반 이중계구조 제어기의 경우 고장률을 무시한 데이터를 사용하고 있으나, 그림 7에서와 같이 소프트웨어의 고장률은 전체시스템 신뢰도예측에 무시할 수 없는 요인으로 작용함을 알 수 있다.

따라서 대기이중계구조의 필수기능인 결함검출, 격리, 재구성과 같은 여분관리기능에 대한 고장률을 정량화하기 위해서는 하드웨어기반의 자기검사회로의 적용이 검토되어야 한다.

3. 자기검사회로내장 대기이중계제어기 설계

2장에서 제시한 소프트웨어기반 이중계구조의 단점은 각 여분에 결함을 검출하여 해당 제어기를 제외시키기 위한 논리를 하드웨어 로직으로 구현함으로써 보완할 수 있다. 하지만, 소프트웨어 결함검출 알고리즘과 동일하게 자기검사회로는 정의된 결함검사항목에 대한 결함검출만을 수행하므로, 검사항목의 선정에 시스템의 신뢰도가 종속된다. 따라서 본 논문에서는 자기검사회로의 검사항목선정을 고장모드의 분석을 수행하여 도출하였으며, 도출된 기능요구사양에 따라 제어기를 설계한 후 FMEA기법을 사용하여 분석하였다.

3.1 자기검사회로의 기능요구사항 및 설계

본 논문의 2장에서와 같이 결함의 검출에 의한 허용을 위한 이중계구조 제어기의 고장모드를 동작계와 대기계로 분류하고 결함의 검지와 관련된 송수신정보를 기준으로 고장메커니즘을 분석하면 표 3과 같다.

따라서 표 3의 고장메커니즘에 대한 결함허용을 위한 자기검사회로의 요구사항을 다음과 같이 도출하였다.

표 3. 이중계구조 결함허용 메커니즘의 고장모드

고장모드	해 설
결함검지실패 (동작계)	동작계에서 발생한 결함의 검지실패
결함검지실패 (대기계)	대기계에서 발생한 결함의 검지실패
결함검지전송 오동작(동작계)	동작계 고장검지의 결함발생으로 대기계에 활성화 신호 전송
결함검지전송 오동작(대기계)	대기계 고장검지의 결함발생으로 동작계에 대기계고장신호 전송
결함검지수신 오동작(동작계)	동작계의 결함발생으로 정상동작 중인 대기계를 고장으로 인식
결함검지수신 오동작(대기계)	대기계의 결함발생으로 정상동작 중인 동작계를 고장으로 인식

- 단일계마다 설치되는 자기검사회로는 해당 단일계의 고장(프로세서, 메모리, 직렬통신 입출력, 병렬통신 입출력 및 인터페이스소자)을 검출한다.
- 결함이 검출되면 결함고립을 위해 해당 단일계를 이중계구조에서 제외시킨다.(바이탈 전원차단회로에 의한 전원차단)
- 결함발생으로 인한 단일계의 제외를 정상동작중인 단일계로 전송하여야 한다.

위 요구사항을 만족하도록 그림 8과 같이 자기검사회로를 설계하였다.

이중계구조에서 각각의 제어기 내부에 그림 9와 같이 설치된 그림 8의 자기검사회로는 프로세스 폭주로 인한 할트(HALT), 예외처리 오류(Exception Error) 등의 프로세스 정지를 검지하기 위해 "HALT감시회로"를 내장하여 프로세서가 주기적으로 데이터버스, 어드레스버스, 제어버스를 통해 "HALT감시회로"에 정상동작정보를 기록하지 않으면 결함검출신호(논리 0)가 발생한다.

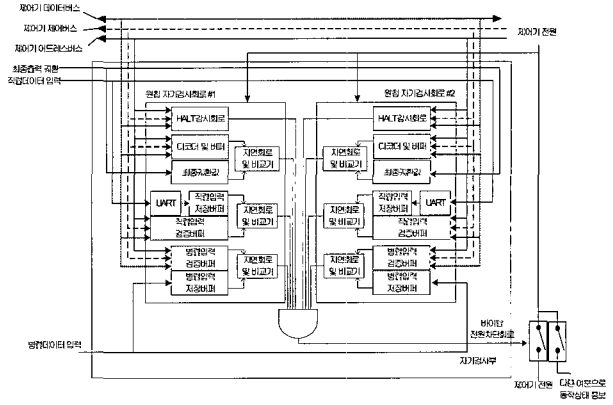


그림 8. 자기검사회로의 내부구성도

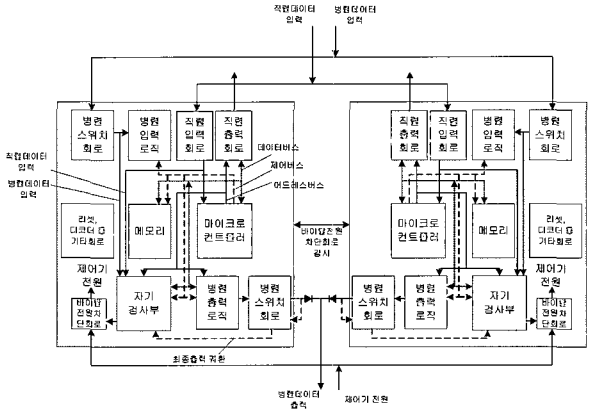


그림 9. 자기검사회로가 각각 내장된 대기이중계구조 제어기

그림 8의 "최종궤환값"과 "디코더 및 버퍼"는 그림 9에서와 같이 제어기의 출력신호가 스위칭소자를 통과하여 다시 궤환된 신호를 "최종궤환값"으로 입력받고, 제어기가 발생한 출력신호와 동일한 데이터를 "디코더 및 버퍼"에 데이터버스, 어드레스버스, 제어버스를 사용하여 기록함으로써, "지연회로 및 비교기"에 의해 하드웨어적으로 비교되어 제어기의 병렬출력로직 또는 병렬스위치회로에서 결함이 발생하면 "디코더 및 버퍼"의 값과 "최종궤환값" 레지스터에 저장되는 값이 불일치하므로 "지연회로 및 비교기"는 결함검출신호(논리 0)를 발생한다. "UART(Universal Asynchronous Receiver/Transmitter)+직렬입력저장버퍼"와 "직렬입력검증버퍼"는 그림 9에서와 같이 제어기로 입력되는 직렬데이터 입력(RS232, RS422, RS485, 광통신, 이더넷 등)에 대하여 직렬입력회로를 통과한 디지털 직렬데이터가 "UART+직렬입력저장버퍼" 레지스터로 저장되고, 마이크로컨트롤러 내부의 UART에 의해 입력된 디지털 정보가 데이터버스, 어드레스버스, 제어버스를 사용하여 "직렬입력검증버퍼" 레지스터에 기록함으로써, "지연회로 및 비교기"에 의해 하드웨어적으로 비교되어 마이크로컨트롤러의 UART 또는 자기검사회로에서 결함이 발생하면 "UART+직렬입력저장버퍼"의 값과 "직렬입력검증버퍼" 레지스터에 저장되는 값이 불일치하므로 "지연회로 및 비교기"는 결함검출신호(논리 0)를 발생한다.

프로세서의 정지관련 검출회로의 결함검출신호, 최종출력의 검사를 통한 오출력발생관련 결함검출신호, 직렬데이터 입력관련 결함검출신호, 병렬데이터 입력관련 결함검출신호는 각각의 이중화된 자기검사회로의 출력을 모두 논리곱의 형태로 종합하여 "HALT감시회로" 또는 "지연회로 및 비교기"에서 하나라도 결함검출신호(논리 0)가 발생하면 해당 제어기의 전원을 차단하여 결함발생에 대하여 능동적으로 해당 제어기를 제외시킨다.

순수하드웨어로 구성된 자기검사회로는 실시간으로 비교동작을 계속 수행한다. 따라서 각각의 레지스터 값을 비교할 때 프로세서의 처리속도를 고려하기 위해 비교기는 지연회로를 내장하며, 지연 값은 제어기내부의 마이크로 컨트롤러의 성능에 따라 좌우된다.

3.2 설계된 대기이중계구조 시스템의 FMEA

FMEA는 해당 기능 또는 인터페이스에 대하여 고장모드(Failure Mode)를 기준으로 고장의 원인 및 영향의 체계적 분석을 목적으로 한다. 따라서 이중계시스템의 FMEA를 위해서는 대상기능 및 고장모드에 대한 정의가 선행되어야 한다.

본 논문에서는 철도신호분야에서 다중계로 구성하고 있는 응용분야인 전자연동장치 또는 궤도회로장치와 같은 응용분야에 대한 기능분석은 FMEA에서 제외하고, 이중계시스템의 결함허용 메커니즘을 대상으로 분석한다.

FMEA기법을 사용하여 시스템의 고장에 대한 영향을 분석하기 위한 양식은 시스템의 신뢰성을 분석하는 기관이나 국가에 따라 약간의 차이점이 있다. 이러한 차이점은 시스템의 신뢰성확보를 제3의 기관이나 운영기관으로부터 평가를 받기 위해 양식에 대한 사전승인을 받아야 한다.

따라서 본 논문에서는 FMEA양식의 건전성확보를 위해 미국방규격 MIL-STD-1629A(1977)에서 제시하는 FMEA양식지[4]를 사용하여 표 4와 같이 이중계구조 결함허용 메커니즘에 대한 FMEA를 수행하였다.

표 4 FMEA의 고장모드는 ERTMS/ETCS의 제어기간 데이터 전송[5]에 대한 고장모드를 적용하였으며, 여분간의 결함검지상태 교환은 접점신호를사용하여 설계하였으므로, 결함발생에 의해 실패하는 실패(Deletion)와 결함이 발생하지 않았는데도 결함의 발생으로 판단하는 가장(Masquerade)을 기준으로 하였다.

표 4 FMEA의 고장영향평가를 수행하면 FMEA를 수행하지 않았을 때는 정량적으로 고장발생확률의 예측이 불가능한 위험측고장의 발생확률 및 자기검사회로의 결함을 포함한 시스템의 고장률의 산출이 가능해 진다.

표 4 FMEA에서는 케이블 및 제어기의 설치와 관련된 인적 오류는 고장의 분석에서 제외하였다.

3.3 설계된 대기이중계구조 제어기의 고장률평가

자기검사회를 내장한 그림 9와 같은 제어기의 기능상실에 대한 고장률과 위험측 동작에 대한 고장률을 산출하기 위해 표 5와 같이 구성요소의 고장률을 가정하였다.

식 (2)의 대기이중계구조 고장률 산출식을 이용하여 자기검사 회로를 내장한 이중계구조 제어기의 고장률을 평가하면 식 (3)과 같다.

$$\lambda_{Hot\ Standby} = \frac{2}{3}(\lambda_{con} + \lambda_{SCL} + \lambda_{CB}) = 2.001 \times 10^{-6}/Hour \quad (3)$$

또한 표 4의 FMEA를 통해 대기이중계구조 제어기의 위험측고장인 제어기 출력의 예측할 수 없는 상태에 대한 발생빈도를 FTA(Fault Tree Analysis)를 사용하여 그림 10과 같이 정량화 하였다.

따라서 순수 하드웨어로 자기검사회로를 구현하고, 자기검사회로를 내장하여 설계한 대기이중계구조 제어기의 신뢰도 평가결과는 표 6과 같다.

본 논문 2장에서 제시한 소프트웨어기반 이중계구조 제어

표 4. 이중계구조 결함허용 메커니즘의 FMEA

System : 하드웨어 여분을 이용한 이중계구조 결함허용 제어기
Indenture Level : Default
Reference Drawing : 이중계구조 제어기의 설계도면
Mission : 이중계구조 결함허용 메커니즘의 FMEA

Date : 2006.11.23
Sheet :1of 1
Compiled By ducko
Approved By ducko

색인	분석 대상	기능	고장모드	원인	고장영향			고장검지방법	설계대책
					국부영향	제어기 결과	응용단계 결과		
DK_tmp	이중계의 단일결함에 대한 허용실패	결함검지실패 (동작계)	실패 (DELETION)	1. 자기검사회로 결함	검지실패	위험측 고장	제어기 불용	자기검사회로의 결함검출	자기검사회로의 동기이중화를 통한 처리결과 비교에 의한 결함검출
			가장 (MASQUERADE)	1. 자기검사회로 결함	검지실패	위험측 고장	제어기 불용		
		결함검지실패 (대기계)	실패 (DELETION)	1. 자기검사회로 결함	검지실패	위험측 고장	제어기 불용		
			가장 (MASQUERADE)	1. 자기검사회로 결함	검지실패	위험측 고장	제어기 불용		
		결함검지전송 오동작(동작계)	실패 (DELETION)	1. 자기검사회로 결함 2. 전원차단회로 결함	검지실패	위험측 고장	제어기 불용	자기검사회로의 결함검출	자기검사회로의 동기이중화를 통한 처리결과 비교에 의한 결함검출 및 2접점 바이탈 계전기를 사용하여 전원차단회로 구현
			가장 (MASQUERADE)	1. 자기검사회로 결함 2. 전원차단회로 결함	동작계 차단	대기계 동작	제어기 가용		
		결함검지전송 오동작(대기계)	실패 (DELETION)	1. 자기검사회로 결함 2. 전원차단회로 결함	검지실패	동작계 단독동작	제어기 가용		
			가장 (MASQUERADE)	1. 자기검사회로 결함 2. 전원차단회로 결함	대기계 차단	동작계 단독동작	제어기 가용		
		결함검지수신 오동작(동작계)	실패 (DELETION)	1. 전원차단회로 감시 입력 결함	정상동작	동작계 단독동작	제어기 가용	전원차단회로 감시회로의 결함검출	전원차단회로 감시입력을 자기검사회로의 결함검출이 가능한 병렬스위치 입력으로 구현
			가장 (MASQUERADE)	1. 전원차단회로 감시 입력 결함	정상동작	동작계 단독동작	제어기 가용		
		결함검지수신 오동작(대기계)	실패 (DELETION)	1. 전원차단회로 감시 입력 결함	동작계 차단 및 대기계 대기상태유지	무응답	제어기 불용		
			가장 (MASQUERADE)	1. 전원차단회로 감시 입력 결함	대기계 출력	위험측 고장	제어기 불용		

표 5. 자기검사회로를 내장한 하부구성요소의 고장률

하부구성요소	고장률 (/Hour)	기타	기호
제어기모듈	1E-6	이중계를 구성하는 단일 모듈의 고장률	λ_{con}
자기검사회로	2E-6	이중계를 구성하는 단일 모듈 내부의 이중화된 자기검사회로	λ_{SCL}
바이탈 전원 차단회로	1E-9	-	λ_{CB}

표 6. 자기검사회로를 내장한 이중계구조 제어기의 신뢰도

신뢰도	고장률(/Hour)	MTTF(Hour)
기능상실	2.001E-6	499,750
위험측고장	1E-9	1,000,000,000

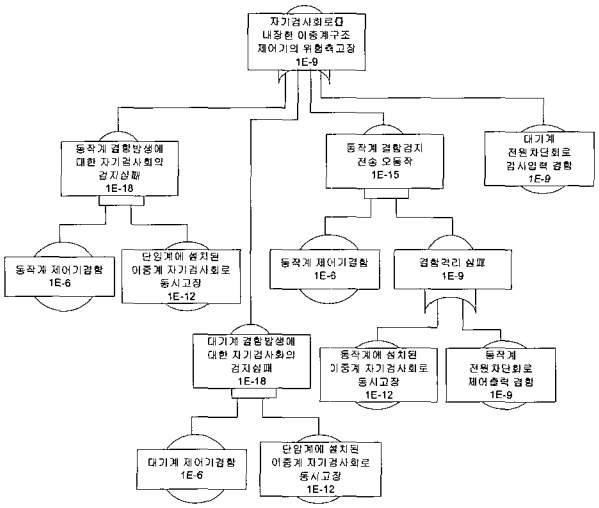


그림 10. 자기검사회로를 내장한 이중계구조 제어기의 위험측고장 FTA

기의 두 가지 문제점의 해결을 위해 제시된 하드웨어기반 자기검사회로를 내장한 이중계구조 제어기는 하드웨어의 장점인 병렬처리가 가능한 프로그래머블 로직으로 구현하였으며, 자기검사회로를 이중으로 사용하여 신뢰도를 확보하였다.

소프트웨어기반 이중계구조 제어기의 단점인 위험측고장과 같은 특정 고장형태에 대한 정량적인 발생빈도의 예측은 표 5와 같이 정량적인 수치화가 용이한 하드웨어 고장률을 입력데이터로 사용하여 표 4의 FMEA를 통해 그림 10과 같이 FTA를 수행하면 표 6과 같이 위험측고장에 대한 발생빈도를 예측하여 실제 시스템의 고장률을 보다 현실적으로 추정할 수 있다.

4. 결 론

본 논문은 철도신호분야 제어기의 결함을 하드웨어 여분을 이용하여 허용하는 대기이중계구조 제어기와 관련하여 소프트웨어기반 여분관리구조의 문제점인 순차수행으로 인한 결함검출의 지연시간과 자기검사의 실패확률에 대한 정량화를 보완하기 위해 하드웨어 기반 자기검사회로를 내장한 대기이중계구조 제어기의 설계를 제안하고 평가하였다. 결함허용능력(Fault Coverage)은 시스템에서 발생된 결함에 대한 허용여부에 대한 평가기준으로써, 정의된 결함의 검출기능이 설계에 포함되었는지 여부를 나타낸다. 본 논문에서 사용된 FMEA를 통한 고장모드의 분석과 FTA를 이용한 발생빈도의 정량화는 결함허용 제어기의 신뢰성향상을 위해 향후에도 지속적으로 연구될 것이다.

참 고 문 헌

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".
5. UIC (2003), "ERTMS/ETCS-Class1, FMEA for Interface to/from an Adjacent RBC-in Application Level2".