철도신호 대기이중계구조 제어기의 향상된 신뢰도평가방법에 관한 연구

論 文
56-9-12

A Study on the Advanced Reliability Assessment Method about Hot-Standby Sparing System for Railway Signaling

閔 根 泓† · 李 鐘 宇*
(Geun-Hong Min · Jong-Woo Lee)

Abstract - This paper suggests the advanced reliability assessment tool for railway signaling Hot-Standby sparing system. Existing reliability assessment for Hot-Standby sparing system controller is done by using single module mean failure rate based on approximated Hot standby sparing system function. Although approximated Hot standby sparing system function can be applied to various Hot standby sparing system, however, it is not able to reflect the exact system structure. In this paper, we suggest the advanced reliability function by identifying changeover-related failure factors and common failure mode which is not considered in existing approximated Hot standby sparing system reliability function via developing Hot standby sparing system model for railway signaling and applying FMECA to this model. Also, we compare reliability assessment results for model system to reliability assessment for existing system.

Key Words : 이중계구조, 결함허용, 전자연동장치, 신뢰도평가, FMEA, 공통모드고장

1. 서 론

오늘날 철도신호는 역구내 열차의 진로제어 및 역간 열차의 간격제어를 안전하게 수행하기 위한 설비이다. 이러한 신호설비의 고장(Failure)은 열차의 대규모지연, 열차의 충·추돌, 열차탈선 등의 심각한 결과의 원인이 되므로 높은 신뢰성과 안전성의 확보를 위한 구조로 설계시 고려되어야 한다[1]. 이중계구조(Standby Sparing)는 철도신호 제어기 내부에서 발생된 결함(Fault)의 허용(Tolerant)을 목적으로 하드웨어 여분(Redundancy)을 적용한 설계 방법이다[2].

하드웨어 여분은 비교에 의한 능동결함허용을 개념으로 한 이중계 및 사중계(Dual-Duplex)구조 외에도 다수결에 의한 수동결함허용을 개념으로 삼중계(2 out of 3)구조 등 다양한 설계가 현장에서 사용되고 있다. 철도신호에서 하드웨어 여분구조 중 최소여분을 사용하여 결함허용을 구현함으로써 가장 적용빈도가 높은 이중계구조 제어기는 진로제어를 위한 지상제어장치 중 전자연동장치, 간격제어를 위한 차상신호제어장치에 적용되고 있으며, 이중계구조 제어기의 신뢰도를 정량적으로 평가해야만 시스템 신뢰도 요구사항의 만족여부를 평가할 수 있다.

본 논문에서는 기존 대기이중계구조 제어기의 신뢰도평가 방식을 설명하고 분석하여 문제점을 제시하고, 고장모드영향분석(FMEA, Failure Mode Effect Analysis)기법을 적용한 이중계구조 제어기의 계절체 관련 고장률 및 공통모드고장(Common Mode Failure)을 선별하여 향상된 이중계구조 신뢰도평가 방법을 제안한다. 또한 제안된 방법의 향상을 입증하기 위해 철도신호분야에서 사용되는 내장형제어기의 일반적 구성을 모델로 제시하여 기존 신뢰도평가방식과 향상된 방식으로 각각 신뢰도를 평가하고 그 결과를 비교한다.

† 교신저자, 正會員 : 서울산업대학교 철도전문대학원 박사과정, 감사원 감사전략본부
E-mail : mingh@bia.go.kr
* 正 會 員 : 서울산업대학교 철도전문대학원 교수, 공학박사
接受日字 : 2007年 7月 11日
最終完了 : 2007年 8月 2日

2. 본 론

2.1 이중계 제어기의 신뢰도 모델링

신뢰도는 규정된 조건하에서 의도하는 기간 동안 목표한 기능을 발휘할 확률로 정의되며[3], 정량적인 신뢰도의 평가는 평균수명인 평균고장수명(MTTF, Mean Time To Failure : 고장발생시 수리가 불가능함)과 평균고장간격(MTBF, Mean Time Between Failure : 고장발생시 수리가 가능함.)을 사용하여 시불변 형태로 평가하는 방법과 전자부품으로 구현되는 철도신호 제어기의 경우 고장의 모델을 지수고장모델을 사용하여 신뢰도함수로 나타낸다.

2.1.1 철도신호 대기이중계(Hot-standby Sparing)구조 제어기

단일결함의 발생을 검출하고 격리하여 요구하는 기능을 수행하는 이중계구조 제어기는 동작계와 대기계로 구성된다. 이중계구조 제어기는 대기계의 상태에 따라 Hot-standby Sparing과 Cold-standby Sparing으로 구분할 수 있으며, 철도신호에서 사용하는 전자연동장치 및 차상제어장치 등 대부분이 이러한 2개의 구조 중에서 선택하여 사용하고 있다. Hot-standby Sparing은 동작계가 정상동작일 경우 대기계는 동작계와 동일하게 입력을 받아 처리결과에 해당하는 출력만 차단된 상태로 유지하다가, 동작계의 결함검출시 동작계

출력을 차단하고 대기계의 출력을 발생시키는 구조이다[4].

본 논문에서는 신뢰도평가 결과의 향상을 입증하기 위한 모델의 간소화를 위해 Hot-standby Sparing으로 연구범위를 제한한다.

2.1.2 대기이중계구조 제어기의 정량적 신뢰도평가

대기이중계 제어기는 그림1과 같은 상태천이도를 갖는다. 그림1의 상태천이도에서 상태 "11"은 동작계와 대기계가 모두 정상동작 상태이며, "10" 또는 "01"은 동작계 또는 대기계에서 결함이 발생하였지만 하드웨어 여분에 의해 결함이 허용되어 시스템이 가용한 상태이다. 또한 상태 "00"은 동작계와 대기계에서 모두 결함이 발생하여 시스템을 사용할 수 없는 상태이다.

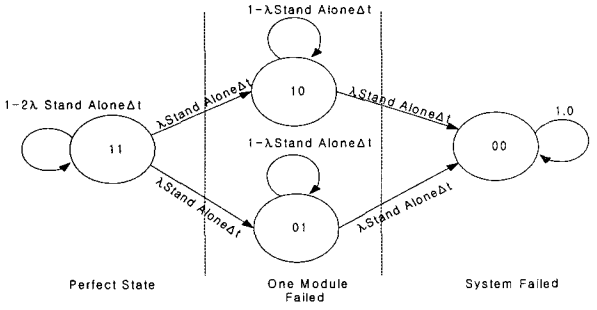

그림 1 대기이중계 제어기의 상태천이도

Fig. 1 A State-diagram of a Hot-standby sparing controller

따라서 대기이중계구조 시스템의 가용상태는 "11", "10", "01"이며, 이러한 상태를 마코브(Markov) 모델링하여 시간에 따른 신뢰도함수 $R(t)$와 시불변 고장률 λ로 근사하면 식(1) 및 (2)와 같이 모델링 된다[5]. 식(1)은 대기이중계구조의 시간에 따른 신뢰도변화를 관찰하는데 사용되며, 식(2)는 시스템의 신뢰도 블럭다이어그램(RBD, Reliability Block Diagram) 작성시 대기이중계구조 제어기에 해당하는 고장률을 산출하기 위해 사용된다.

$$R(t) \equiv 2e^{-\lambda t} - e^{-2\lambda t} \tag{1}$$

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

그림1의 상태천이도를 마코브 모델링하여 산출한 식(1)의 신뢰도 함수는 "모든 결함은 한 번에 하나씩 발생한다."와 "발생된 결함은 다른 결함의 원인이 되지 않는다."는 조건을 전제로 한다. 또한 식(2)의 "n"은 작동 중인 여분의 개수이며, "q"는 시스템 고장을 발생시키지 않은 작동 여분의 개수이다. 또한 대기이중계구조를 식(2)로 근사화하기 위해서는 "모든 부품은 처음부터 작동한다."와 "근사치는 처음 고장시간을 나타낸다."는 두 가지 전제를 조건으로 한다[5].

2.1.3 철도신호 제어기의 고장률 산출

위와 같이 시변 및 시불변 정량적 신뢰도는 고장률 λ를 입력으로 사용한다. 전자부품으로 구성된 철도신호 제어기의 고장률은 단위시간당 고장발생확률로써 /hour의 단위로 산출된다. 고장률의 산출은 시스템개발 수명주기의 설계단계에서는 MIL-HDBK-217, BELCORE, TELCORDIA, PRISM 등의 고장률예측 규격이나 지침을 통해 정량화가 가능하며, 수명주기의 시운전단계에서 발생된 고장의 분석을 통해 입증하고 있다[6].

따라서 고장률은 부품단위로 예측 또는 입증된 고장률을 바탕으로 단일계와 대기계의 고장률을 각각 산출하므로 고장률의 건전한 산출은 대기이중계로 구성된 제어기의 신뢰도 평가결과에 많은 영향을 준다.

2.1.4 기존 대기이중계 모델의 신뢰도평가 문제점

단일계를 구성하는 제어기 내부의 구성요소에 대한 직렬 또는 병렬구성에 따라 단일계의 고장률이 산출된다. 본 논문에서는 기존 대기이중계 모델에 적용하는 단일계 고장률의 정량적 평가방식 설명을 위해 그림2와 같이 철도신호에서 사용하는 전자연동장치 및 차상제어장치 등에 적용된 일반적 제어기 모델을 제안한다.

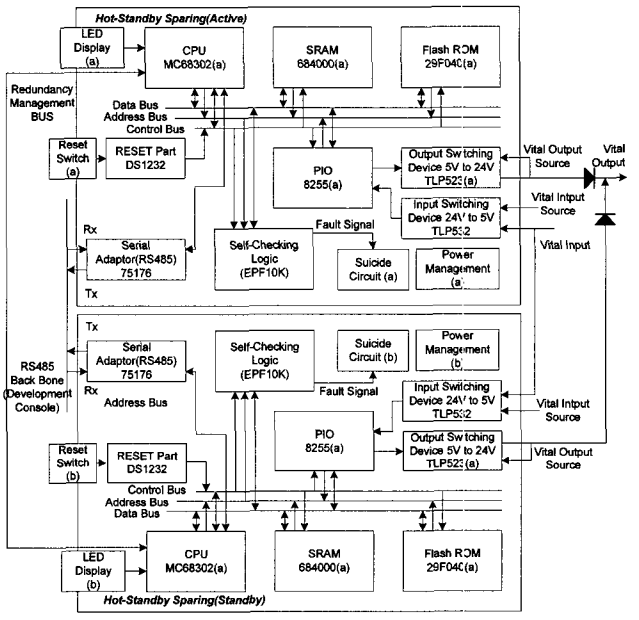

그림 2 철도신호 대기이중계 제어기 모델

Fig. 2 A Hot-standby controller for railway signaling

그림2는 DC24V의 신호계전기 조건을 입력받아 프로그램된 임무를 기준으로 DC24V의 신호계전기 제어출력을 발생시키는 단일계 제어기를 대기이중계로 구성한 철도신호의 기본 제어기 모델이다. 동작계와 대기계는 각각 마이크로컨트롤러, SRAM, Flash ROM, RESET회로의 기본구성을 포함하고, 단일계 내부에 발생된 연산오류, 스위칭 소자오류, 병렬 입출력(PIO, Parallel Input Output)오류를 검지하기 위한 자기검사회로(Self-Checking Logic) 및 결함발생시 단일계 차단을 위한 회로차단기(Suicide Circuit)를 내장한다.

동작계와 대기계의 데이터 비교는 이중계의 경우 동작계와 대기계의 불일치발생시 결함의 발생여부만 파악이 가능하고 발생위치는 파악이 불가능한 이중계구조의 단점을 보완하기 위해 단일계의 결함 발생은 자기검사회로가 검출하

고 결함검출시 차단회로 동작에 의해 정상동작 트리거신호(Heart Beat Signal)를 대기계와 동작계가 상호 감시하는 구조이다. 마지막으로 시리얼어댑터(Serial Adaptor)는 개발과정에서 필요한 콘솔로써 실제 동작에서는 사용되지 않는다

*기존 대기이중계 모델의 신뢰도평가*는 그림2의 일반적인 철도신호 대기이중계 제어기의 단일계 고장률을 표1과 같이 부품단위 고장률을 합하여 4.645430X10-6/hour로 산출한다.

표 1 단일계 고장률 산출 예

Table 1 Example of calculation for single mode failure rate

단일계 구성부품	기호	Failure rate per hour (10^{-6})	수량	Failure rate per hour (10^{-6})
MC68302	λ_{CPU}	0.025189	1	0.025189
684000	λ_{SRAM}	0.063352	1	0.063352
29F040	λ_{Flash}	0.005696	1	0.005696
TLP523	λ_{SW24}	0.220860	1	0.220860
TLP532	λ_{SW5}	0.220860	1	0.220860
EPF10k	$\lambda_{Self\,Checker}$	2.486389	1	2.486389
DS1232	λ_{RESET}	0.060934	1	0.060934
75176	$\lambda_{Serial\,Adap}$	0.253600	1	0.253600
8255	$\lambda_{\Pi O}$	0.198550	1	0.198550
LED	$\lambda_{\leq D}$	0.100000	6	0.600000
Reset Switch	$\lambda_{Reset\ Switch}$	0.010000	1	0.010000
Suicide Circuit	$\lambda_{Suicide\ \circ\ uit}$	0.200000	1	0.200000
Power Management	$\lambda_{Pow.\ Manag.}$	0.300000	1	0.300000
Sum				4.645430

따라서 표1의 단일계 구성부품은 단일계의 자기검사회로에서 단일계 구성부품의 발생결함 검출 여부에 따라 계절체(Changeover) 수행여부가 결정된다. 예를 들어, LED 및 Reset Switch에서 발생된 결함이 검출되어 계절체를 수행하지 않는데도 불구하고 식(1) 및 식(2)의 단일계 고장률에 포함시키면 정확한 시스템 신뢰도를 평가하는데 부정적 요인으로 작용한다. 또한 동작계와 대기계가 결함에 의한 차단을 상호 인식하기 위해 설계된 여분관리버스에서 결함이 발생하면 동작계와 대기계가 동시에 동작계로 인식하여 출력을 발생시킬 수 있는 제어기 전체의 고장상태가 된다. 이러한 고장은 단일계 결함이 정상동작중인 여분에 영향을 미치는 공통모드고장으로써 대기이중계의 신뢰도 평가를 위한 식(1)의 결함의 독립성관련 전제에 위배된다.

그러므로 본 논문에서는 이러한 대기이중계구조 제어기의 신뢰도 평가시 구성부품별 고장영향의 분석을 수행하지 않는 기존 방식의 문제점을 FMEA를 적용하여 계절체와 관련없는 고장성분 제거 및 공통모드고장을 고려한 신뢰도 모델링을 제안한다.

2.2 FMEA를 적용한 대기이중계구조 제어기의 신뢰도 모델링

FMEA는 제어기에서 발생된 결함이나 고장의 영향을 분석하여 특정 상태를 유도하는 고장의 발생요인만 분류하는 기법으로써 기존에는 여러 개의 하부장치로 구성된 시스템에서 모듈고장이 전체시스템에 미치는 영향을 분석하기 위해 일반적으로 사용되었다. 본 논문에서는 대기이중계구조 제어기를 구성하는 단일계의 구성부품들을 대상으로 FMEA를 적용하여 계절체와 관련된 고장을 도출한다.

2.2.1 단일계의 FMEA

FMEA의 대상이 되는 구성요소를 표1의 단일계 구성요소로 설정하고 부품단위 고장모드별 단일계의 최종결과를 분석하면 표2와 같다. 표2에서와 같이 개발을 위해 설계되었으나 실제 제어에는 사용되지 않는 시리얼어댑터, 제어기의 상태를 운영자가 모니터링하기 위한 LED에서 발생된 결함은 대기이중계구조 제어기의 계절체 원인이 되지 않으므로 단일계 고장률의 산출에서 제외되어야 한다. 그리고 마이크로컨트롤러의 여분관리 버스결함, 차단회로와 전원관리 소자의 차단요구시 차단실패와 같은 공통모드고장이 고려되어 시스템 상태천이도가 변경되어야 한다.

따라서 FMEA에 의해 도출된 계절체 관련 구성부품의 고장률 및 고장률의 합은 표3과 같으며, 공통모드고장을 고려한 상태천이도의 변경은 다음 항에서와 같이 향상된 신뢰도 평가를 위해 새롭게 모델링 된다.

표 3 FMEA에 의한 모델시스템의 계절체 관련 고장률

Table 3 Changeover related failure rates of the model system by FMEA

단일계 구성부품	기호	Failure rate per hour (10^{-6})	수량	Failure rate per hour (10^{-6})
MC68302	λ_{CPU}	0.025189	1	0.025189
684000	λ_{SRAM}	0.063352	1	0.063352
29F040	λ_{Flash}	0.005696	1	0.005696
TLP523	λ_{SW24}	0.220860	1	0.220860
TLP532	λ_{SW5}	0.220860	1	0.220860
EPF10k	$\lambda_{Self\,Checker}$	2.486389	1	2.486389
DS1232	λ_{RESET}	0.060934	1	0.060934
8255	$\lambda_{\Pi O}$	0.198550	1	0.198550
Reset Switch	$\lambda_{Reset\ Switch}$	0.010000	1	0.010000
Suicide Circuit	$\lambda_{Suicide\ \circ\ uit}$	0.200000	1	0.200000
Power Management	$\lambda_{Pow.\ Manag.}$	0.300000	1	0.300000
Sum				3.791830

2.2.2 공통모드고장을 고려한 대기이중계구조 모델링

대기이중계구조 제어기의 각 단일계가 모두 완전한 상태 "11"에서 동작계 또는 대기계의 계절체관련 고장(λ_{SM})이 발생하면 "01" 또는 "10"으로 천이되며, 유지보수 이전에 동작계에서 다시 λ_{SM}이 발생하면 "00"상태가 된다. 하지만 "11"상태에서 공통모드고장(λ_{CM})이 발생하면 시스템은 즉시 "00"상태로 천이된다. 그림1의 대기이중계구조 제어기의 일반화된 상태천이도는 그림2의 모델이 갖는 공통모드고장을 반영하면 그림3과 같이 변경된다.

표 2 이중계구조 제어기의 단일계 FMEA

Table 2 Single mode FMEA of A Hot-standby sparing controller

분석대상	구성부품	고장모드	고장영향			고장검지방법	설계대책
			영향	단일계 결과	이중계 결과		
단일계	마이크로컨트롤러 (MC68302)	무응답	제어불능	결함격리	계절체	자기검사회로의 Watch-dog회로 동작	자기검사회로에 의한 결함검출-격리-허용(계절체)
		가용한 오류데이터 입출력	연산오류	결함격리	계절체	동일연산의 반복처리(시간여분)를 통해 결함검출	
		가용하지 않은 오류데이터 입출력	제어불능	결함격리	계절체	자기검사회로의 체커로직에 의해 결함검출	
		여분관리 버스 결함	제어불능	결함확산	제어기 고장	대기이중계구조의 단점인 여분관리 데이터의 결함은 검출불가	하드웨어 여분끼리 정상동작을 확인하지 않도록 설계변경
	SRAM메모리 (684000)	가용한 오류데이터 출력	연산오류	결함격리	계절체	동일연산의 반복처리(시간여분)를 통해 결함검출	자기검사회로에 의한 결함검출-격리-허용(계절체)
		가용하지 않은 오류데이터 출력	연산오류	결함격리	계절체	자기검사회로의 체커로직에 의해 결함검출	
	Flash메모리 (29F040)	가용한 오류데이터 출력	연산오류	결함격리	계절체	동일연산의 반복처리(시간여분)를 통해 결함검출	자기검사회로에 의한 결함검출-격리-허용(계절체)
		가용하지 않은 오류데이터 출력	연산오류	결함격리	계절체	자기검사회로의 체커로직에 의해 결함검출	
	24 to 5V 스위칭소자 (TLP523)	논리 "0" 또는 "1"로 고정(Stuck at fault)	제어불능	결함격리	계절체	출력신호의 궤환입력을 출력데이터와 비교하여 결함검출 입력은 반복처리(시간여분)을 통해 결함검출	자기검사회로에 의한 결함검출-격리-허용(계절체)
		지속적인 상태변화(Chattering)	제어불능	결함격리	계절체		
	5 to 24V 스위칭소자 (TLP532)	논리 "0" 또는 "1"로 고정(Stuck at fault)	제어불능	결함격리	계절체	출력신호의 궤환입력을 출력데이터와 비교하여 결함검출 입력은 반복처리(시간여분)을 통해 결함검출	자기검사회로에 의한 결함검출-격리-허용(계절체)
		지속적인 상태변화(Chattering)	제어불능	결함격리	계절체		
	자기검사회로 (EPF10K)	무응답	제어불능	결함격리	계절체	마이크로컨트롤러의 Watch-dog 회로 동작	마이크로컨트롤러에 의한 결함검출-격리-허용 (계절체)
		가용한 오류데이터 출력	연산오류	결함격리	계절체	동일연산의 반복처리(시간여분)를 통해 결함검출	
		가용하지 않은 오류데이터 출력	제어불능	결함격리	계절체	자기검사회로의 체커로직에 의해 결함검출	
	리셋칩 (DS1232)	논리 "Reset"상태로 고정(Stuck at fault)	제어불능	결함격리	계절체	자기검사회로의 Watch-dog회로 동작	자기검사회로에 의한 결함검출-격리-허용(계절체)
		지속적인 상태변화(Chattering)	제어불능	결함격리	계절체		
	시리얼어댑터 (75176)	가용한 오류데이터 입출력	기능고장	-	-	검출불능	사용하지 않는 기능이므로 결함검출기능 없음
		가용하지 않은 오류데이터 입출력	기능고장	-	-	검출불능	
	병렬IO (8255)	논리 "0" 또는 "1"로 고정(Stuck at fault)	제어불능	결함격리	계절체	출력신호의 궤환입력을 출력데이터와 비교하여 결함검출 입력은 반복처리(시간여분)을 통해 결함검출	자기검사회로에 의한 결함검출-격리-허용(계절체)
		지속적인 상태변화(Chattering)	제어불능	결함격리	계절체		
	현시장치 (LED)	논리 "0" 또는 "1"로 고정(Stuck at fault)	표시고장	-	-	검출불능	운영자와의 인터페이스에는 지장이 있으나, 제어기의 기능수행에 영향 없음 (계절체 발생 안함)
		지속적인 상태변화(Chattering)	표시고장	-	-	검출불능	
	리셋버튼 (Reset Switch)	논리 "Reset"상태로 고정(Stuck at fault)	제어불능	결함격리	계절체	자기검사회로의 Watch-dog회로 동작	자기검사회로에 의한 결함검출-격리-허용(계절체)
		지속적인 상태변화 (Chattering)	제어불능	결함격리	계절체		
	차단회로 (Suicide Circuit)	불필요한 차단	제어불능	결함격리	계절체	대기계의 동작계 Heart-beat감시동작에 의해 동작계 차단감지	동작계와 대기계의 동작상태 감시논리에 의해 계절체 발생
		차단요구시 차단실패	제어불능	결함확산	제어기 고장	동작계 차단실패로 인하여 위험측고장 발생	
	전원관리소자 (Power Management)	불필요한 차단	제어불능	결함격리	계절체	대기계의 동작계 Heart-beat감시동작에 의해 동작계 차단감지	동작계와 대기계의 동작상태 감시논리에 의해 계절체 발생
		차단요구시 차단실패	제어불능	결함확산	제어기 고장	동작계 차단실패로 인하여 위험측고장 발생	

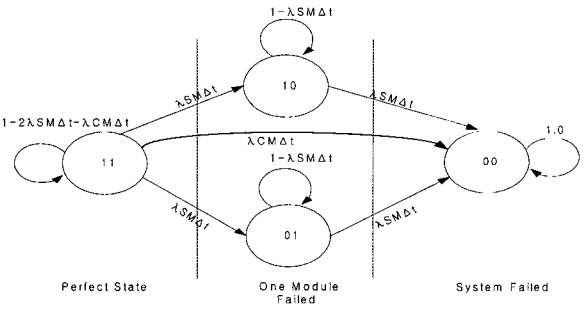

그림 3 공통모드고장이 고려된 제어기의 상태천이도

Fig. 3 A State-diagram of controllers take account of the common mode failure

그림3의 상태천이도를 마코브 모델링을 사용하여 간소화하면 그림4와 같다.

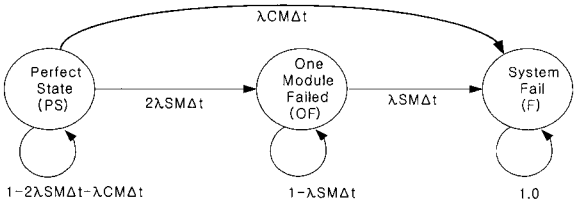

그림 4 공통모드고장이 고려된 대기이중계구조 제어기의 Markov모델

Fig. 4 The Markov Model of A Hot-standby sparing controller take account of the common mode failure

그림4의 상태별 확률을 구하면 식(3)과 같다.

$$p_{PS}(t+\Delta t)=(1-2\lambda_{SM}\Delta t-\lambda_{CM}\Delta t)p_{PS}(t) \tag{3}$$
$$p_{OF}(t+\Delta t)=2\lambda_{SM}\Delta t p_{PS}(t)+(1-\lambda_{SM}\Delta t)p_{OF}(t)$$
$$p_F(t+\Delta t)=\lambda_{CM}\Delta t p_{PS}(t)+\lambda_{SM}\Delta t p_{OF}(t)+p_F(t)$$

식(3)에서 p_{PS}는 시스템 완전상태(Perfect State), p_{OF}는 단일계고장(One Module Failure), p_F는 동작계와 대기계가 모두고장(System Failure)이다. 마코브모델은 고정된 시간 Δt동안에 천이가 발생하므로 불연속 모델(Discrete-time Model)이다. 따라서 천이가 임의 시간에 발생하는 것에 대하여 마코브모델을 시행하면 연속 마코브모델을 식(4)와 같이 얻을 수 있다.

$$\frac{p_{PS}(t+\Delta t)-p_{PS}(t)}{\Delta t}=-2\lambda_{SM}p_{PS}(t)-\lambda_{CM}p_{PS}(t) \tag{4}$$
$$\frac{p_{OF}(t+\Delta t)-p_{OF}(t)}{\Delta t}=2\lambda_{SM}p_{PS}(t)-\lambda_{SM}p_{OF}(t)$$
$$\frac{p_F(t+\Delta t)-p_F(t)}{\Delta t}=\lambda_{CM}p_{PS}(t)+\lambda_{SM}p_{OF}(t)$$

Δt를 "0"으로 놓으면, 식(5)와 같은 미분형태의 수식을 얻을 수 있다.

$$\frac{dp_{PS}(t)}{dt}=-2\lambda_{SM}p_{PS}(t)-\lambda_{CM}p_{PS}(t) \tag{5}$$
$$\frac{dp_{OF}(t)}{dt}=2\lambda_{SM}p_{PS}(t)-\lambda_{SM}p_{OF}(t)$$
$$\frac{dp_F(t)}{dt}=\lambda_{CM}p_{PS}(t)+\lambda_{SM}p_{OF}(t)$$

Laplace 변환을 이용하면 식(6)을 얻을 수 있다.

$$sP_{PS}(s)-p_{PS}(0)=-2\lambda_{SM}P_{PS}(s)-\lambda_{CM}P_{PS}(s) \tag{6}$$
$$sP_{OF}(s)-p_{OF}(0)=2\lambda_{SM}P_{PS}(s)-\lambda_{SM}P_{OF}(s)$$
$$sP_F(s)-p_F(0)=\lambda_{CM}P_{PS}(s)+\lambda_{SM}P_{OF}(s)$$

여기서 $P_{PS}(s)$,$P_{OF}(s)$는 $p_{PS}(t)$,$p_{OF}(t)$의 Laplace 변환의 형태이고, $P_F(s)$는 $p_F(t)$의 Laplace 변환 형태이다. $p_{PS}(0)$는 $p_{PS}(t)$의 $t=0$에서의 초기 값을 의미한다. 따라서 시스템의 분석에서 $t=0$에 해당하는 초기상태에는 시스템이 완벽하게 구성되었음을 전제로 하므로, $p_{PS}(0)=1$, $p_{OF}(0)=0$, $p_F(0)=0$이다. 결과적으로 Laplace 변환 방정식을 다시 정리하면 식(7)이 되며,

$$P_{PS}(s)=\frac{1}{s+2\lambda_{SM}+\lambda_{CM}} \tag{7}$$
$$sP_F(s)-p_F(0)=\lambda_{CM}P_{PS}(s)+\lambda_{SM}P_{OF}(s)$$
$$P_F(s)=\left(\frac{1}{s}\right)\left(\frac{\lambda_{CM}}{s+2\lambda_{SM}+\lambda_{CM}}\right)+\lambda_{SM}\left(\frac{1}{s}\right)\left(\frac{2\lambda_{SM}}{s+2\lambda_{SM}+\lambda_{CM}}\right)$$

Laplace 변환의 결과를 역변환 하면 식(8)이 된다.

$$p_{PS}(t)=e^{-(2\lambda_{SM}+\lambda_{CM})t} \tag{8}$$
$$p_{OF}(s)=2\lambda_{SM}e^{-\lambda_{SM}t}-2\lambda_{SM}e^{-(2\lambda_{SM}+\lambda_{CM})t}$$
$$p_F(s)=\frac{\lambda_{CM}}{2\lambda_{SM}+\lambda_{CM}}-\frac{\lambda_{CM}}{2\lambda_{SM}+\lambda_{CM}}e^{-(2\lambda_{SM}+\lambda_{CM})t}+\frac{2\lambda_{SM}^2}{2\lambda_{SM}+\lambda_{CM}}-\frac{2\lambda_{SM}^2}{2\lambda_{SM}+\lambda_{CM}}e^{-(2\lambda_{SM}+\lambda_{CM})}$$

따라서, 대기이중계구조 제어기의 신뢰도는 시스템이 기능요구사항을 수행할 수 있는 PS, OF에 있을 확률이므로 식(9)와 같은 그림2 구조 제어기에 대한 신뢰도 함수를 얻을 수 있다.

$$R(t)=e^{-(2\lambda_{SM}+\lambda_{CM})t}+2\lambda_{SM}e^{-\lambda_{SM}t}-2\lambda_{SM}e^{-(2\lambda_{SM}+\lambda_{CM})t} \tag{9}$$
$$=(1-2\lambda_{SM})e^{-(2\lambda_{SM}+\lambda_{CM})t}+2\lambda_{SM}e^{-\lambda_{SM}t}$$

기존방식인 식(1)에 적용되는 단일계 고장률은 식(10)과 같으며,

$$\lambda=\lambda_{CPU}+\lambda_{SRAM}+\lambda_{Flash}+\lambda_{SW24} \tag{10}$$

FMEA를 적용한 계절체관련 단일계고장률 λ_{SM}과 공통모드고장률 λ_{CM}은 다음 식과 같다.

$$\lambda_{SM} = \lambda_{CPU} + \lambda_{SRAM} + \lambda_{Flash} + \lambda_{SW24to5} + \lambda_{SW5to24} + \lambda_{Self\ Checker} + \lambda_{RESET} + \lambda_{PIO} + \lambda_{Reset\ Switch} + \lambda_{Suicide\ Circuit} + \lambda_{Power\ Management} \quad (11)$$

$$\lambda_{CM} = \lambda_{CPU} + \lambda_{Suicide\ Circuit} + \lambda_{Power\ Management}$$

2.3 고장률 합에 의한 신뢰도평가와 FMEA를 적용한 신뢰도평가 결과비교분석

기존 대기이중계구조 제어기의 신뢰도 평가방식인 모든 부품의 고장률 합에 의한 신뢰도 평가결과와 본 논문에서 제안하는 FMEA에 의한 계절체 관련 고장률 및 공통모드고장을 고려한 신뢰도평가 결과를 비교하면 신뢰도함수에 의한 평가결과가 그림5와 같다.

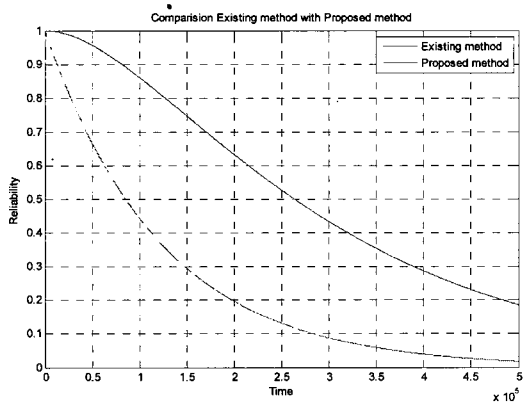

그림 5 기존방식과 향상된 방식에 의한 신뢰도변화 비교
Fig. 5 A comparison of reliability between conventional method and proposed method

그림5와 같이 500,000시간(약 60년)에 대한 대기이중계구조 제어기의 신뢰도는 기존평가방식과 FMEA를 적용한 제안된 방식 간에 차이가 있음을 알 수 있다. 이러한 차이는 기존에 사용하는 대기이중계구조 제어기의 일반화된 신뢰도 모델 식(1)의 가정인 "발생된 고장은 다른 고장의 원인이 되지 않는다." 즉 "공통모드고장은 고려하지 않는다."의 가정으로 인해 발생하는 차이이다. 공통모드고장을 고려하지 않는 이유는 대기이중계구조라 하더라도 구현하는 과정에서 그 구조가 매우 다양하므로 식(1)과 같이 근사화된 모델을 적용하였기 때문이다. 하지만 철도신호에 사용되는 그림2와 같은 대기이중계구조 제어기는 본 논문의 FMEA분석결과와 같이 동작계와 대기계간의 통신 및 자기검사회로에 의한 차단과 전원관리 관련 부품이 공통모드고장으로 작용한다.

따라서 대기이중계구조 제어기의 정확한 신뢰도평가를 위해서는 본 논문에서 제안된 FMEA에 의한 공통모드고장 및 계절체 관련 고장률에 대한 분석이 요구된다. 다양한 대기이중계구조 제어기의 신뢰도를 식(1)과 같이 근사화 된 수식을 사용하는 경우에는 신뢰성평가결과의 정확성이 저하되어 시스템의 운영효율저하 및 효율적 유지보수의 장애요인인 된다. 그러므로 FMEA를 적용하여 시스템 구조에 따른 정확한 상태다이어그램을 모델링해야만 하드웨어 여분을 사용하는 목적인 높은 신뢰도의 시스템을 얻을 수 있다.

2.4 제안된 신뢰도평가 방법에 의한 신뢰도향상 설계변경

신뢰도평가의 목적은 시스템 구성요소별 고장률을 근거로 시스템 신뢰도를 평가하여 유지보수 및 개량을 위한 데이터로 활용하기 위함이다. 시스템 신뢰도는 구성요소 고장률에 종속되므로 시스템 신뢰도를 향상시키기 위해서는 고장률을 감소시켜 시스템의 신뢰도를 높여야 한다. 따라서 신뢰도의 향상을 위해서는 시스템 고장률을 감소시켜야 한다. 고장률을 감소시키기 위한 방법으로는 보다 높은 품질의 부품을 사용하거나, 부품의 용량과 부품에 걸리는 부하의 비율인 디래이팅(Derating)을 조절하는 방법이 있다. 신뢰도향상을 위해 기존에는 변경대상부품의 선정을 표1의 부품별 고장률 중 가장 높은 고장률을 갖는 부품의 품질을 개선하는 방법을 사용하고 있다. 하지만 본 논문에서 제안하는 FMEA를 적용한 신뢰도평가가 선행된다면 대기이중계구조 제어기의 신뢰성에 가장 큰 영향을 미치는 공통모드고장을 도출하여 공통모드고장과 관련된 부품을 변경하여 보다 효과적인 신뢰도향상을 달성할 수 있다.

예를 들어 모델시스템의 신뢰도향상을 위해 표1의 단일계 고장성분 중 가장 높은 고장률을 갖는 자기검사회로(EPF10k)의 고장률($\lambda_{Self\ er}$)을 0.4×10^{-6}/hour 만큼 향상된 부품으로 교체하는 경우보다 FMEA적용에 의해 도출된 공통모드고장관련 부품인 차단회로($\lambda_{Suicide\ uit}$)와 전원관리소자($\lambda_{Power\ Management}$)의 고장률 합을 0.4×10^{-6}/hour 만큼 감소시키면 그림6과 같이 시스템 신뢰도가 자기검사회로 부품의 교체보다 향상된다. 따라서 동일한 고장률 감소치에 대하여도 기존 변경부품 선정방식보다 FMEA결과에 근거한 설계변경의 결과가 시스템 신뢰도를 더욱 향상시킬 수 있다.

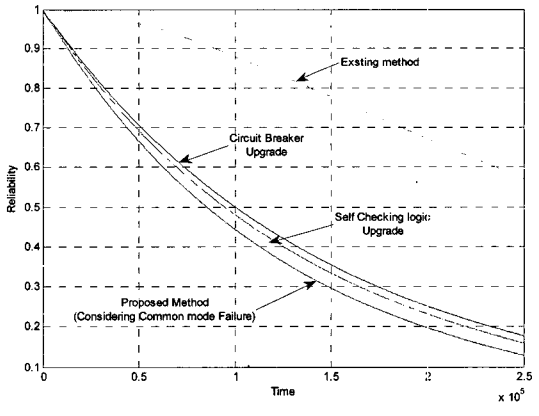

그림 6 고장률감소 후 기존방식에 의한 신뢰도평가
Fig. 6 A reliability assessment by conventional method as failure rate decrease

본 논문에서 제안하는 FMEA적용에 의한 대기이중계구조 시스템의 신뢰도평가는 공통모드고장을 고려하여 보다 실제에 근접한 시스템의 신뢰도를 평가할 수 있으며, 시스템 신뢰도 향상을 위한 설계변경의 선택기준을 제시하여 최적의 설계변경을 지원한다.

3. 결 론

본 논문은 대기이중계구조 제어기에 대한 기존의 신뢰도 평가방식 문제점을 분석하여 이것의 문제점을 보완하기 위해 FMEA를 적용하여 보다 정확한 제어기의 신뢰도 평가방안을 제시하고, 제어기의 신뢰성향상을 위한 설계 변경시 FMEA를 근거로 변경부품의 선택을 위한 기준을 제시하였다. FMEA적용은 최근 철도신호분야에서 안전관련 위험측고장률의 산출을 위해 적용하는 기법으로써 본 논문을 통해 위험측고장률의 산출뿐만 아니라 계절체와 같이 시스템의 특정 상태 천이에 대한 정량적 발생확률 계산에 적용 가능함을 보였다.

FMEA 적용에 의한 계절체 관련 고장률산출의 건전성을 입증하기 위해 철도신호분야의 일반적인 대기이중계 제어기 구조를 모델링하고, 모델을 대상으로 FMEA를 적용하여 계절체 및 공통모드고장과 관련된 고장률을 고려한 신뢰도를 평가하고 결과를 기존방식의 결과와 비교하였다.

FMEA를 적용한 계절체 관련 고장률 산출은 시스템의 정확한 신뢰도평가를 위한 향상방안이며, 특히 철도신호분야의 전자연동장치와 같이 상용CPU보드를 포함하여 대기이중계구조 제어기를 구성하는 경우 상용보드에서 제공하지만 제어와 관련되지 않은 기능이나, 자기검사회로에 의해 결함이 검출되지 않는 구성부품의 고장률을 제외함으로써 보다 시스템의 신뢰도를 정확하게 평가할 수 있다.

참 고 문 헌

[1] "열차제어시스템 안전성능평가 및 사고방지 기술개발 (1차년도 보고서)", 한국철도기술연구원, 2006

[2] Barry W. Johnson, "Design and analysis of fault-tolerant digital systems", Addison-Wesley Publishing Company, pp51-80, 1989.

[3] 신덕호 외, "한국형고속철도 열차제어시스템 하부구성요소 신뢰도예측에 관한 연구", 한국철도학회논문집, 제9권, 제4호, p419-424, 2006.

[4] Dhiraj K. Pradhan, "Fault-Tolerant Computer System Design", Prentice Hall PTR, pp8-52, 1996.

[5] Preston R. MacDiarmid, John J. Bart, "Reliability Toolkit: Commercial Practices Edition", RAC, pp156-162.

[6] MIL-HDBK-2155, "FRACAS : Failure Reporting Analysis, Corrective Action System".

저 자 소 개

민 근 홍 (閔 根 泓)

1951년 5월 27일생. 199년 서울산업대학교 전자계산학과 졸업, 1992년 연세대학교 공학석사, 2007년 현재 서울산업대학교 철도전문대학원 박사과정, 1995년~현재 감사원 감사전략본부

Tel : 02-2011-3329
Fax : 02-2011-2455
E-mail : mingh@bai.go.kr

이 종 우 (李 鐘 宇)

1953년 3월 20일생. 1983년 한양대학교 기계설계학과 졸업. 1986년 Ecole Centrale de Nantes 석사, 1993년 Universite de Parise VI 공학박사, 1994년~2005 한국철도기술연구원 전기신호연구본부 책임연구원, 2005~현재 서울산업대학교 철도전문대학원 교수

Tel : 02-970-6874
Fax : 02-978-6874
E-mail : saganlee@snut.ac.kr