한국철도학회논문집
제10권 제5호 2007년 ▌ pp. 527-532

신뢰도모델링에 의한 이중계제어기 전원공급방식 설계에 관한 연구

A Study on Power Supply Method Design for Hot Standby Sparing System via Reliability Modeling

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

Abstract In this paper, we suggest those two design plans for power supply method of Hot Standby Sparing System; one is the plan using MTBF based on Constant Failure Rate, and the plan using Reliability Function is the other. Traditionally, RBD (Reliability Block Diagram) is used for reliability prediction which is required to meet any requirements before system operation. However, the system that has redundancy, such as Hot Standby Sparing System, is not suitable for system reliability modeling using combination model, such as RBD. In this paper, therefore, we demonstrate that for redundancy controller, redundancy modeling design toward fault occurrence design is more effective to build up a system with higher reliability and achieve the effectiveness of loss cost due to maintenance and failure occurred in operation, rather than combinational modeling design.

Keywords : Hot-Standby Sparing, RBD (Reliability Block Diagram), Failure Rate, Reliability, Fault- Tolerance, Markov Model

요 지 본 논문은 철도신호에서 사용되는 이중계제어장치의 전원공급방식에 대하여 상수고장률을 기반으로 하는 평균고장률에 의한 설계와 신뢰도함수에 의한 설계방안을 제안한다. 일반적으로 시스템 운영이전에 신뢰도 요구사항 만족을 위한 시스템의 신뢰도예측은 RBD모델을 사용하였다. 하지만 이중계제어장치와 같이 여분을 갖는 시스템의 신뢰도는 RBD와 같은 조합모델에 의해 정확한 신뢰도를 모델링하기에 부적합하다. 따라서 본 논문에서는 다중계구조 제어기의 설계과정에서 단순조합모델에 의한 설계방식 선정보다는 결함발생에 대한 여분구조의 모델링을 통한 설계방식 선정이 보다 정확한 신뢰도를 갖는 시스템구축을 가능하게 하며, 운영중에 발생되는 유지보수비용 및 고장으로 인한 손실비용의 효율화를 위해 필요함을 입증한다.

주 요 어 : 대기이중계, 고장률, 신뢰도, 결함허용, 마코브모델링

1. 서 론

시스템의 신뢰도는 주어진 시간에 임무를 정확하게 수행할 확률로써 철도신호분야에서는 열차제어장치와 전자연동장치와 같이 제어기의 고장이 열차지연을 발생시켜 대규모 운영손실을 발생하므로 정량적인 기준을 제시하여 시스템수명주기 전반을 관리하고 있다[1].

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

특히 신호시스템과 같이 전자화된 제어기의 고장패턴은 일정한 패턴을 가지지 않는 우발고장(Random Failure)[2]으로써 관련규격이나 사용실적에 의해 정량적으로 제시되는 평균고장률을 사용하여 제어기별 신뢰성과 안전성의 요구사항 만족여부를 평가한다.

일반적인 시스템의 신뢰도관리는 개념설계, 상세설계, 제작, 시험, 설치까지의 과정에서는 기능요구사항에 대한 상실이나, 서비스제공의 불능과 같이 특정 상태에 대한 발생빈도로 제시되며, 평균고장시간(MTBF, Mean Time Between Failure), 평균서비스상실시간(MTBSF, Mean Time Between Service Failure) 등으로 정량화하여 관리하고 있다. 신뢰성 요구사항

은 위에서 언급한 서비스제공의 불능과 같이 특정 상태를 요구하는 경우에 고장모드영향분석(FMEA, Failure Mode Effect Analysis)과 같은 특정 상태발생빈도 정량화를 위한 분석단계를 거쳐야 하며, 본 논문에서와 같이 별도의 고장정의를 선언하지 않는 경우에는 모든 부품의 고장발생률을 고려한다. 즉, 모든 고장성분을 고려하여 모델링을 수행한다.

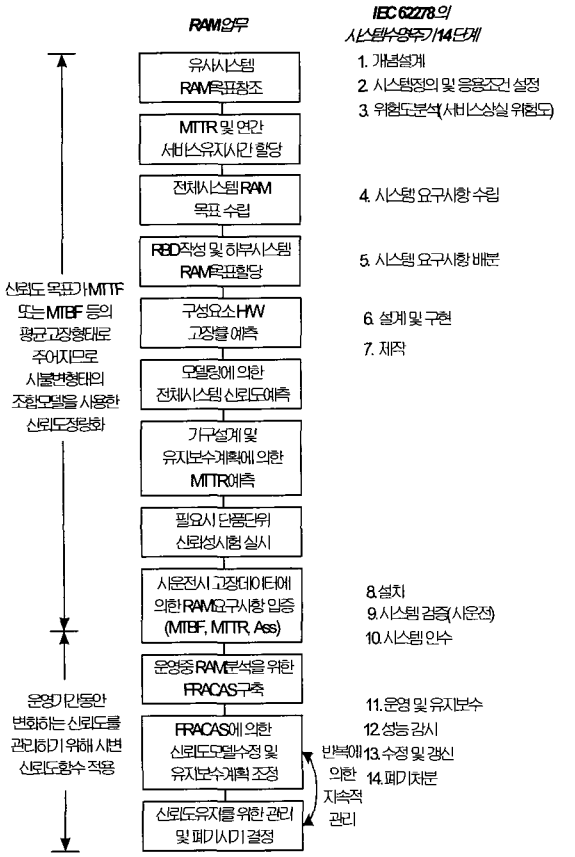
그림 1은 시스템 수명주기동안 시스템이 최종사용자에게 인수되기 전까지 신뢰도 목표를 만족하기 위한 신뢰도관리를 보여준다[3].

운영이전까지 시스템신뢰도의 기준이 되는 MTBF는 평균값으로써 운영기간에 관계없이 변화되지 않는다. 이는 전자부품으로 구성된 신호시스템 신뢰도의 가장 큰 특징인 상수고장률 영향 때문이다. 따라서 시스템의 운영이 시작되면 운영기간에 따라 시스템신뢰도를 평가하는 기준으로 신뢰도함수 $R(t)$를 많이 사용한다. $R(t)$의 함수도 여러 가지가 있으나 상수고장률을 갖는 전자시스템의 고장특성은 지수모델에 적합하므로 식 (1)과 같은 신뢰도함수를 적용하여 신뢰도변화 추이에 따라 유지보수 및 시스템 교체주기를 결정하는 관리를 수행한다. 그러므로 설계단계에서도 $R(t)$를 고려하여 설계하면 운영이후에 효율적인 유지보수와 시스템의 사용시간을 연장할 수 있다.

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

λ = 장치(또는 시스템)의 고장률

본 논문은 단일결함허용을 목적으로 하드웨어 여분을 사용하는 다중계구조 제어기에 대해서 이중계의 정의를 만족하는 평균고장률이 동일한 두 가지 방식의 전원설계를 제안하고 각각의 신뢰도를 평가하여 설계방식별 신뢰도와 교체주기를 분석한다. 이러한 분석을 통해 다중계구조 설계 시 신뢰도목표의 만족뿐만 아니라 운영자로의 시스템 인수단계 이후의 운영효율도 설계단계에서 고려해야 함을 입증한다.



FRACAS : Failure Reporting Analysis, Corrective Action System
MTTF : Mean Time To Failure
RAM : Reliability, Availability, Maintainability
Ass : Steady State Availability

Fig. 1. Reliability Management at Each Life Cycle Phase

2. 이중계제어기와 전원공급방식 설계

2.1 단일계별 전원공급과 전원장치 이중화 설계

제어기의 신뢰성확보를 위해 우발고장특성을 갖는 전자제어기의 결함발생을 억제하는 기술을 통칭하여 결함허용(Fault Tolerance)설계라고 하며, 결함의 검출(Detection), 은폐(Mask) 및 재구성(Reconfiguration)을 통해 결함을 허용한다. 결함허용을 위해 사용되는 기술의 대표적 사례는 여분(Redundancy) 구조이며, 여분에는 하드웨어, 소프트웨어, 시간, 정보 등이 이용된다.

본 논문의 범위인 이중계제어기는 위와 같은 범주에서 능동하드웨어여분(Active Hardware Redundancy)을 사용한 결함허용 기법의 대표적인 방법으로써 철도신호분야에 널리 사용되고 있다.

이중계구조 제어기설계를 전원공급방식에 따라 그림 2의

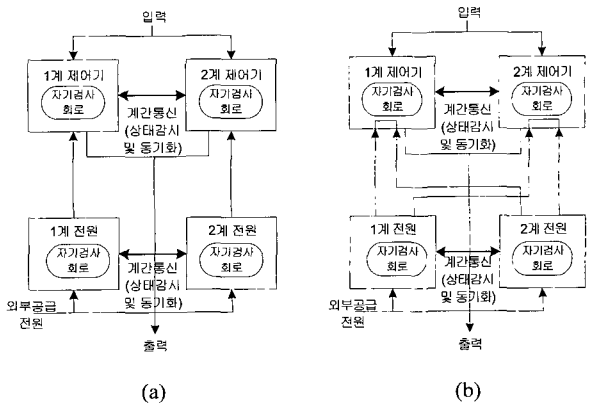


Fig. 2. Hot-Standby Sparing Controller Design by Power Supply Method

Table 1. Characteristics of Hot-Standby Sparing Controller Power Supply

	대표적 적용기술	기술적 특징
단일계별 전원공급	RS422/485 Ethernet Isolated Buffer	제어기와 전원공급장치가 쌍을 이루며 각 쌍의 기준전압이 다르므로 회로단락 관련 고장모드의 결함허용에 용이하다. 쌍을 이루는 제어기와 전원장치 중 어느 하나에 결함이 발생해도 쌍의 절체가 발생한다.
전원장치 이중화	RS232 Digital UART Buffer Dual-Port Memory	제어기와 전원공급장치가 각각 결함발생에 따라 절체가 수행되므로 절체관련 오동작이 방지된다. 기준전압이 동일하므로 결함발생 모듈의 제외 시 완전한 전기적 분리가 수행되어야 한다.

(a)와 같은 "단일계별 전원공급"과 그림 2 (b)와 같은 "전원장치 이중화"의 설계방법을 사용할 수 있다. 또한 각 설계의 기술적 특징은 표 1과 같다.

2.2 이중계제어기 전원공급방식별 RBD에 의한 신뢰도

RBD는 조합모델의 한 가지 방법으로써 고장률을 알고 있는 하부시스템으로 구성된 전체시스템의 신뢰도를 계산하기에 적합하다[4]. 또한 도식화된 표현으로 전체시스템의 신뢰도를 일목요연하게 볼 수 있으며, 전체시스템 신뢰도목표에 따라 하부시스템의 신뢰도목표를 할당하고 관리하기에 용이하기 때문에 그림 1의 설계 및 제작단계에서 가장 많이 사용되고 있는 방법이다.

$$\lambda_{Type(a)} = \frac{2}{3}(\lambda_{CPU} + \lambda_{PSU}) \tag{2}$$

$$\lambda_{Type(b)} = \frac{2}{3}\lambda_{CPU} + \frac{2}{3}\lambda_{PSU} = \frac{2}{3}(\lambda_{CPU} + \lambda_{PSU}) \tag{3}$$

식 (2)와 (3)에 적용된 이중계고장률의 수식은 수리를 고려하지 않은 다중계의 근사식 (4)를 적용한 것이다[5].

$$\lambda_{(n-q)/n} = \frac{\lambda}{\sum_{i=n-q}^{n} \frac{1}{i}} \tag{4}$$

n = 온라인 유닛의 수
λ = 각 온라인 모듈의 고장률
q = 결함발생 후 기능유지를 수행하는 유닛의 수

따라서 RBD를 적용하면 그림 2의 두 가지 설계의 고장률

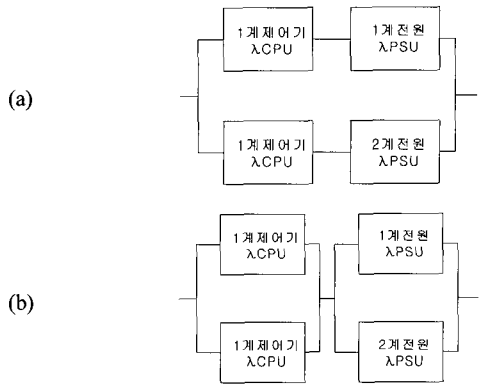


Fig 3. Hot-Standby Sparing Controller RBD by Power Supply Method

이 동일하므로, 신뢰도에 해당하는 MTTF(MTTF=1/λ)가 동일하여 설계자는 기술적 특징과 비용측면을 고려하여 설계방식을 선택한다. 하지만 두 가지 설계의 신뢰도가 동일하게 나오는 이유는 RBD가 여분을 갖는 하드웨어 시스템과 같이 상태모델링이 필요한 시스템의 신뢰도모델에는 적합하지 않고[6], 적용된 대기이중계구조 신뢰도수식도 근사화된 수식을 사용하였기 때문이다.

2.3 이중계제어기 전원공급방식별 신뢰도함수

여분을 갖는 시스템의 결함발생에 대한 복잡한 상태천이를 고려하여 신뢰도함수를 산출하기 위해 본 논문에서는 상태모델수립에 대한 마코브모델링을 사용하여 각 설계의 신뢰도함수를 도출하였다.

마코브모델을 위해서는 먼저 이중계구조 제어기와 이중계구조 전원공급장치의 연결방식에 대한 상태모델을 수립한다[7].

2개의 제어기와 2개의 전원공급장치이므로 4개의 정상과 고장상태에 따라 시스템의 상태는 24인 16가지의 상태를 추정할 수 있다.

본 논문에서 제시한 전원공급방식 중 그림 2의 (a)단일계별 전원공급설계에 대한 상태다이어그램은 그림 4와 같이 표현한다.

그림 4의 동그라미는 각각의 상태를 의미하며, 동그라미 내부의 첫 번째 줄은 1계와 2계의 제어기의 상태이며, 두 번째 줄은 1계와 2계에 연결된 제어장치의 상태를 의미한다. 각각의 상태는 "1"은 정상, "0"은 결함발생을 의미한다. 그림 4에서 백색상태는 완벽한 상태이거나 결함이 발생해도 제어기에 기대된 기능이 수행되는 상태이며, 음영처리된 부분은 제어기가 기능요구사항을 수행하지 못하는 가용하지 않은 상태를 의미한다. 마지막으로 빗금 처리된 부분은 그림 2의 (a)단일계별 전원공급방식의 특징에 따라 단일계 또는 해당 전원공

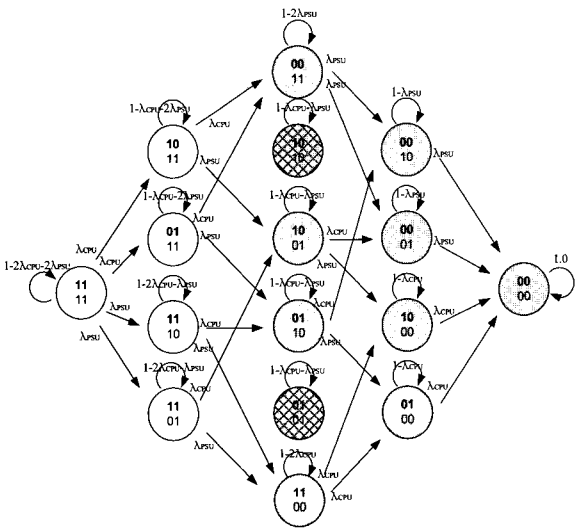


Fig 4. State Diagram of Power Supply Method for Single Redundancy

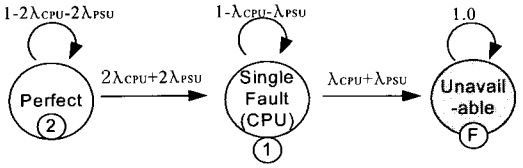


Fig 5. Markov Model of Power Supply Method for Single Redundancy

급장치의 결함발생으로 인해 절체가 발생하므로, 차단된 단일계 또는 전원공급장치의 결함발생은 고려하지 않기 때문이다. 그림 4의 상태다이어그램을 마코브모델하면 그림 5와 같다.

그림 5의 마코브모델에서 가용한 상태인 상태 ②와 상태 ①에 대하여 불연속수식을 작성하면 식 (5)과 같다.

$$\begin{aligned} p_2(t+\Delta t) &= (1-2\lambda_{CPU}\Delta t-2\lambda_{PSU}\Delta t)p_2(t) \\ p_1(t+\Delta t) &= (2\lambda_{CPU}+2\lambda_{PSU})\Delta t p_2(t) \\ &\quad +(1-\lambda_{CPU}\Delta t-\lambda_{PSU}\Delta t)p_1(t) \end{aligned} \tag{5}$$

식 (5)를 연속수식으로 변환하고 초기값을 고려하여 미분형태로 변환한 후 Laplace 변환을 수행한다. Laplace 변환시 상태 ②의 초기값 "1"과 상태 ①의 초기값 "0"을 적용하여 Laplace 역변환을 실시하면 식 (5)는 식 (6)과 같이 정리된다.

$$\begin{aligned} p_2(t) &= e^{-(2\lambda_{CPU}+2\lambda_{PSU})t} \\ p_1(t) &= 2e^{-(\lambda_{CPU}+\lambda_{PSU})t}-2e^{-(2\lambda_{CPU}+2\lambda_{PSU})t} \end{aligned} \tag{6}$$

제어기의 신뢰도는 가용한 상태확률의 합이므로 단일계별 전원공급방식구조의 신뢰도는 식 (7)과 같다.

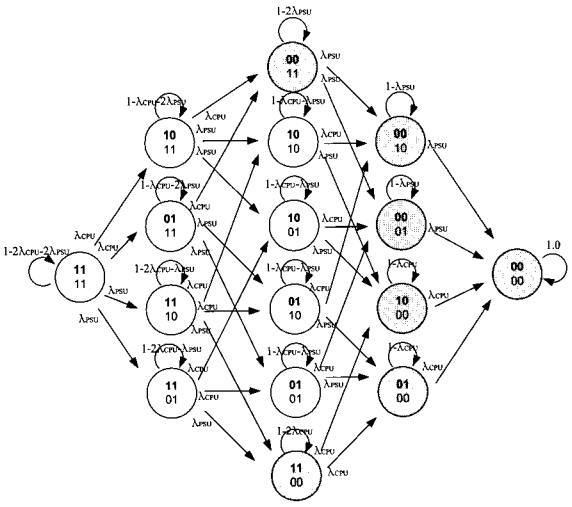


Fig 6. State Diagram for Power Duplication

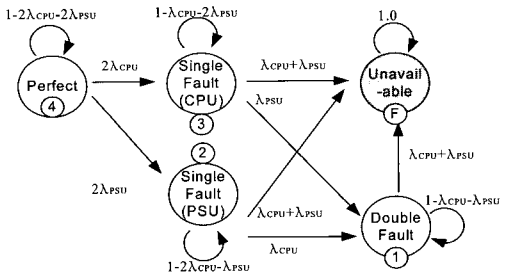


Fig 7. Markov Model for Power Duplication

$$\begin{aligned} R(t) &= p_2(t)+p_1(t) \\ &= 2e^{-(\lambda_{CPU}+\lambda_{PSU})t}-e^{-(2\lambda_{CPU}+2\lambda_{PSU})t} \end{aligned} \tag{7}$$

본 논문에서 제시한 두 번째 제어기의 전원공급 설계방식인 그림 2의 (b)전원장치 이중화설계에 대한 상태다이어그램은 그림 6과 같이 표현한다.

그림 6의 상태다이어그램을 위와 동일한 방법으로 마코브모델하면 그림 7과 같다.

그림 7의 마코브모델은 상태 ④, ③, ②, ①인 가용한 상태에 대하여 불연속수식을 작성하면 식 (8)과 같다.

$$\begin{aligned} p_4(t+\Delta t) &= (1-2\lambda_{CPU}\Delta t-2\lambda_{PSU}\Delta t)p_4(t) \\ p_3(t+\Delta t) &= 2\lambda_{CPU}\Delta t p_4(t)+(1-\lambda_{CPU}\Delta t-2\lambda_{PSU}\Delta t)p_3(t) \\ p_2(t+\Delta t) &= 2\lambda_{PSU}\Delta t p_4(t)+(1-2\lambda_{CPU}\Delta t-\lambda_{PSU}\Delta t)p_2(t) \\ p_1(t+\Delta t) &= 2\lambda_{PSU}\Delta t p_3(t)+2\lambda_{CPU}\Delta t p_2(t) \\ &\quad +(1-\lambda_{CPU}\Delta t-\lambda_{PSU}\Delta t)p_1(t) \end{aligned} \tag{8}$$

식 (8)을 연속수식으로 변환하고 초기값을 고려하여 미분

형태로 변환한 후 Laplace 변환을 수행하고, 상태 ④의 초기값은 "1"과 나머지 상태초기값 "0"을 고려하여 Laplace 역변환은 식 (9)와 같이 정리된다.

$$
\begin{aligned}
p_4(t) &= e^{-(2\lambda_{CPU}+2\lambda_{PSU})t} \\
p_3(t) &= 2e^{-(\lambda_{CPU}+2\lambda_{PSU})t} - 2e^{-(2\lambda_{CPU}+2\lambda_{PSU})t} \\
p_2(t) &= 2e^{-(2\lambda_{CPU}+\lambda_{PSU})t} - 2e^{-(2\lambda_{CPU}+2\lambda_{PSU})t} \\
p_1(t) &= p_1(t) = 4e^{-(\lambda_{CPU}+\lambda_{PSU})t} - 4e^{-(2\lambda_{CPU}+\lambda_{PSU})t} \\
&\quad - 4e^{-(\lambda_{CPU}+2\lambda_{PSU})t} + 4e^{-(2\lambda_{CPU}+2\lambda_{PSU})t}
\end{aligned} \tag{9}
$$

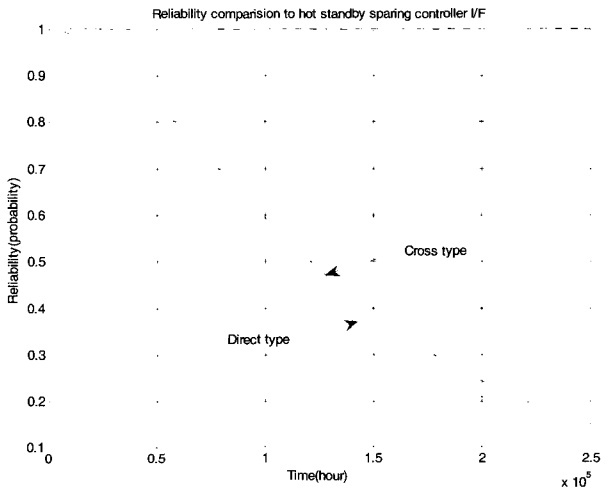
제어기의 신뢰도는 가용한 상태확률의 합이므로 전원장치 이중화방식의 신뢰도는 식 (10)과 같다.

$$
\begin{aligned}
R(t) &= p_4(t)+p_3(t)+p_2(t)+p_1(t) \\
&= 4e^{-(\lambda_{CPU}+\lambda_{PSU})t} - 2e^{-(2\lambda_{CPU}+\lambda_{PSU})t} - 2e^{-(\lambda_{CPU}+2\lambda_{PSU})t} \\
&\quad + e^{-(2\lambda_{CPU}+2\lambda_{PSU})t}
\end{aligned} \tag{10}
$$

2.3 설계별 신뢰도함수의 비교분석

식 (7)의 단일계별 전원공급방식의 신뢰도와 식 (10)의 전원장치 이중화방식 신뢰도함수에 λ_{CPU}와 λ_{PSU}를 각각 10-5/hour와 10-6/hour로 가정하여 시뮬레이션하면 각각의 신뢰도는 그림 8과 같이 단일계별 전원공급방식보다 전원장치 이중화방식의 신뢰도가 높다.

그림 8의 제어기와 전원공급장치 고장률 가정에 따른 각 신뢰도함수에서 10,000시간을 1년으로 가정하는 경우, 10년 후의 단일계별 전원공급방식의 신뢰도는 약 60%이며, 전원장치 이중화방식의 신뢰도는 약 55%로 나타난다.



*Direct Type : 단일계별 전원공급방식
*Cross Type : 전원장치 이중화방식

Fig 8. Reliability Comparison Over Time By Power Supply Method

위와 같은 시간에 따른 신뢰도변화에 따라 유지보수임무선정 및 실시주기가 선정되며, 유지보수를 하지 않는 동안 1-$R(t)$에 해당하는 실패율에 따른 손실비용에 차이가 발생하므로, 신뢰도함수의 차이는 운영이 시작된 이후에는 무시할 수 없는 요건으로 작용하게 된다.

운영이 시작된 제어기의 신뢰도함수 및 고장정보에 의한 입증신뢰도를 이용하여 시스템의 신뢰도를 개선하거나 유지하기 위해 설계를 변경하는 것은 사실상 불가능하다. 이는 변경된 설계로 인한 시스템의 고장모드영향분석을 다시 수행해야 하며, 안전성과 관련해서는 변경된 설계로 인한 신규 위험원이 등장할 수 있기 때문이다.

3. 결 론

본 논문은 철도신호분야의 시스템수명주기별로 수행되는 신뢰성관리와 관련하여 일반적으로 사용되는 RBD와 같은 조합모델을 적용한 다중계구조 제어기의 신뢰도모델링 기반 설계의 문제점을 이중계구조제어기의 전원공급방식의 두 가지 설계를 들어 입증하였다. 최종사용자가 요구한 신뢰도목표가 MTTF 또는 MTBF와 같은 평균값으로 주어지는 경우에 조합모델을 근거로 하드웨어 여분을 사용한 다중계구조 제어기를 설계하면 시스템의 사용개시 이후 시간에 따라 변화하는 신뢰함수의 정확한 예측이 어려우며, 신뢰성기반 유지보수(RCM, Reliability Centered Maintenance)와 같이 시스템 신뢰성 및 비용의 최적화를 위한 업무의 정확성을 저하시키는 원인이 된다.

따라서 본 논문에서 보인바와 같이 다중계구조 제어기의 설계과정에서 단순조합모델에 의한 설계방식 선정보다는 결함발생에 대한 여분구조의 모델링을 통한 설계방식 선정이 보다 정확한 신뢰도를 갖는 시스템구축을 가능하게 하며, 운영중에 발생되는 유지보수비용 및 고장으로 인한 손실비용의 효율화를 위해 검토되어야 한다.

참 고 문 헌

1. IEC 62278 (2002), "Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)", pp.19-64.
2. 신덕호, 외, 한국철도학회(2006), "한국형고속철도 열차제어시스템 구성요소 신뢰도예측에 관한 연구", 제9권 제4호, p.419-424.
3. 신덕호 외, 한국철도학회(2006), "자기검사회로를 이용한 대기이중계구조 결함허용제어기의 설계 및 신뢰도평가에 관한 연구", 제9권 제6호, p.725-731.

4. John Moubray,Elsevier (1997), "Reliability Centered Maintenance II", pp.12-14.
5. Jan Pukite, Paul Pukite, IEEE Press (1998), "Modeling for Reliability Analysis", p.37-65.
6. Reliability Analysis Center, RAC (1993), "Reliability Toolkit: Commercial Practices Edition", p.161.
7. Barry W. Jhonson, Addison-Wesley Publishing Company (1989) "Design and Analysis of Fault-Tolerant Digital System", p.199 -214.

(2007년 9월 20일 논문접수, 2007년 10월 10일 심사완료)