

# 공통고장모드를 고려한 대기 이중계 구조의 철도 시스템 신뢰도 분석

## Reliability Analysis of Hot-Standby Sparing System with Common Cause Failures for Railway

박찬우\* · 채은경 · 신덕호

Chan-woo Park · Eunkyung Chae · Duck-ho Shin

**Abstract** Failures of railway systems can result in train delays or accidents, and therefore high reliability is required to ensure safety of railway systems. To improve reliability, railway systems are designed with redundant systems so that the standby system will continue to function normally even if the primary system fails. Generally, overall system reliability can be evaluated by the reliabilities of the parts of the whole system and the reliability of the redundant system considering common failures in case of each system is not conform physical, functional and process independent. In this study, the reliability of the hot-standby sparing system is analyzed the independent systems and dependent systems with common failures. The reliability for the standby system can be effectively analysed using Markov models, which can model the redundant configuration and the state transition.

**Keywords** : Reliability, Hot-Standby sparing system, Common cause failure, Markov model, Railway system

**초 록** 철도시스템의 고장은 운행지연 또는 철도사고의 원인이 될 수 있으며, 철도안전을 확보하기 위하여 높은 신뢰성이 요구된다. 철도시스템은 신뢰도 및 가용도를 높이기 위하여 동일 시스템을 다중으로 구성하여 동작 중인 시스템에 고장이 발생한 경우에 대기 시스템이 정상 동작을 수행하도록 설계한다. 일반적으로 시스템의 신뢰도는 시스템을 구성하는 각 요소의 신뢰도를 사용하여 분석하며, 시스템간의 물리적, 기능적, 프로세스적 독립이 보장되지 않는 다중 시스템의 경우는 다중 시스템에 동시에 고장을 유발하는 공통원인고장을 고려하여야 한다. 본 논문에서는 철도 시스템에서 사용되고 있는 대기 이중계 시스템에 대하여 각 시스템이 독립일 경우와 공통원인고장을 고려한 종속일 경우에 대한 신뢰도를 분석하였다. 신뢰도 분석을 위하여 다중계 구조의 다양성과 시스템 상태 전이별로 모델링이 가능한 마코브 모델을 사용하였으며, 공통고장모드의 분석 유무의 차이점 평가를 통해 시스템 신뢰도평가의 정확도 향상 방안을 제시한다.

**주요어** : 신뢰도, 대기 이중계, 공통원인고장, 마코브 모델, 철도 시스템

### 1. 서 론

철도시스템의 고장(Failure)은 대규모 운행지연 또는 철도사고의 원인이 될 수 있으므로 높은 수준의 신뢰성(Reliability)이 요구되며 철도안전을 확보하기 위해 신뢰도 및 위험측고장률(Dangerous Failure Rate)을 평가하도록 철도적용 RAMS 국제표준(IEC 62278)에서 권고하고 있다[1]. 신뢰도는 주어진 시간 동안 시스템이 정상 동작할 확률로써 정의된 시간 동안의 시스템 서비스 불능에 대한 확률인 불신뢰도의 역수 개념이다. 일반적으로 높은 수준의 신뢰도를 갖는 시스템을 구현하기 위해서는 고장률(Failure Rate)이 낮은 요소들로 시스템을 구성 할 수 있으나, 이러한 구조의 시스템에서 단일 고장이 발생하는 경우 더 이상 시스템이 기능을 수행할 없기 때문에 신뢰도와 함께 제시되는 가용도(Availability) 목표의 달성을 위해서는 하드웨어 여분(Hardware Redundancy)을 갖는 결합허용 구조로 시스템을 구성하여 신뢰도와 가용도 요구사항을 만족토록 한다.

현재 철도시스템에서는 구성부품의 단일결합을 허용하기 위해 다양한 형태의 하드웨어 여분 구조를 사용하고 있으며, 본 논문에서는 철도 시스템 중 전차연동장치, 궤도회로장치 등 에서 사용빈도가 높은 대기 이중계 구조(Hot-standby Sparing Architecture)에 대한 신뢰도를 분석하였다. 다중계 구조는 각 하드웨어가 물리적, 기능적, 수명주기 단계적으로 독립을 보장하

\*Corresponding author. E-mail: cwpark@krii.re.kr.

© 2017 The Korean Society for Railway. All rights reserved.

<https://doi.org/10.7782/JKSR.2017.20.3.349>

는 경우와 종속일 경우로 구분할 수 있으며, 안전필수 분야(Safety Critical)에서는 종속을 최소화하기 위해 단일의 결함(Fault)의 영향이 여분으로 확산(고장격리의 실패)되는 공통원인고장(CCF, Common Cause Failure)을 고려하여야 한다[2].

본 논문에서는 대기 이중계 시스템에 대하여 공식을 이용한 기존의 방식과 공통고장모드를 고려한 신뢰도를 각각 분석하였으며, 신뢰도 분석을 위한 모델링은 다중계 구조의 다양성과 고장 후 상태 전이별로 모델링(Sate Diagram Modeling)이 가능한 마코브 모델(Markov Model)을 사용하였다. 독립 대기 이중계 시스템 및 공통원인고장을 고려한 대기 이중계 시스템의 신뢰도를 분석하여 그 결과를 비교하고 기존 대기이중계 시스템의 신뢰도 평가 결과와 비교하여 신뢰도평가의 정확도 향상방안을 제시한다.

## 2. 본 론

### 2.1 대기 이중계 구조

#### 2.1.1 대기 이중계 구조

결함허용설계에서 물리적 하드웨어 여분을 사용하여 하드웨어 모듈 단위 또는 시스템 단위로 다중화하는 것은 가장 일반적인 결함허용(Fault Tolerance) 방법이며, 하드웨어 여분기법은 수동방식(Passive Hardware Redundancy), 능동방식(Active Hardware Redundancy), 복합 방식(Hybrid Hardware Redundancy)으로 구분할 수 있다[3]. 수동방식은 결함의 검출보다는 은폐(Masking)를 목적으로 하며 하드웨어를 3개 이상의 홀수로 구성하여 다수결(Majority Voting)의 논리로 출력을 결정하여 결함을 은폐한다. 능동방식은 결함을 검출하고 결함이 발생한 하드웨어를 시스템에서 격리(Isolation)하며 결함을 회복하는 것을 목적으로 하며, 하드웨어를 2개 이상으로 구성하여 각각의 비교를 통해 결함이 검출된 하드웨어를 격리하고 여분의 하드웨어로 동작한다. 철도시스템은 안전을 확보하기 위하여 결함을 검출하고 격리하는 능동방식을 많이 사용하며, 열차운행 지연을 방지하기 위하여 결함이 발생한 경우에 하드웨어가 절제하는 시간을 최소화할 수 있는 대기 이중계 방식을 사용한다[4,5].

여분을 사용하는 시스템 설계는 장치의 중량, 크기, 소비전력, 비용 등을 증가시키게 되며, 시스템의 구성요소가 늘어나면 신뢰성 향상에 장애가 될 수 있어 최적의 여분 설계가 중요하다. 철도시스템은 여분을 최소화한 대기 이중계 구조를 많이 사용하고 있으며, 대기 이중계는 동일한 2개의 하드웨어를 동시에 동작(출력은 동작계만 발생)하도록 구성하여 동작계(Active) 하드웨어에서 고장이 발생한 경우에 대기계(Standby)로 출력 절제(Change over)를 통해 정상기능유지의 신뢰도가 개선된다[6].

#### 2.1.2 공통원인고장(Common Cause Failure)

공통원인고장은 단일 결함(Single Fault)으로 인해 하드웨어 여분 전체의 기능유지가 불가능해지는 고장의 유형으로써, 대기 이중계 구조의 시스템에서 공통원인고장이 발생하면 동작계와 대기계가 동시에 고장이 발생하여 시스템의 서비스가 정지된다. 공통원인고장은 각 하드웨어 구성의 기능적, 물리적, 수명주기 과정이 완전히 독립되지 않은 경우에 발생할 수 있으며 시스템의 신뢰도에 영향을 준다. 일반적인 철도시스템은 동일한 2개의 하드웨어를 물리적으로는 독립을 보장하도록 구성한다. 그러나 하드웨어의 개발 수명주기 프로세스는 동일하며, 동일 기능을 수행하여 독립성을 보장하기 어렵기 때문에 신뢰도 평가를 위하여 공통원인고장을 고려하여야 한다.

#### 2.1.3 신뢰도 모델링

신뢰도를 정량적으로 평가하기 위하여 신뢰도 함수는 평균고장시간(Mean Time Between Failure, MTBF) 또는 고장률의 함수로 표현할 수 있다. 철도시스템은 동일한 하드웨어 2개로 구성되어 각 하드웨어의 고장률은 동일하며, 각 하드웨어에 대한 고장률은 MIL-HDBK-217, Telcodia 등의 표준을 사용하여 정량화가 가능하여 신뢰도함수를 고장률함수와의 관계로 표현한다[4]. 고장률함수는 지수함수, 고장률이 시간에 관계없이 일정하다고 가정하면, 신뢰도함수는 지수고장법칙에 따라 시간에 대하여 고장률의 지수함수로 표현할 수 있다.

### 2.2 신뢰도 분석

#### 2.2.1 독립을 보장하는 대기 이중계 구조 신뢰도 분석

대기이중계 구조의 하드웨어가 독립을 보장하는 경우 Fig. 1과 같은 마코브 체인으로 모델링할 수 있다. 상태  $N$ 은 2개의 하드웨어가 모두 정상 동작상태이며 상태  $O$ 는 2개 중 1개의 하드웨어가 고장이 발생하여 대기계로 절제되어 정상동작이 가능한 상태이며 상태  $F$ 는 2개 하드웨어 모두 고장이 발생하여 정상 동작이 불가능한 상태를 표시한다.  $s$ 는 단일 하드웨어의 고장률을 의미하며 동일한 하드웨어 2개로 구성되어 고장률은 동일하다.

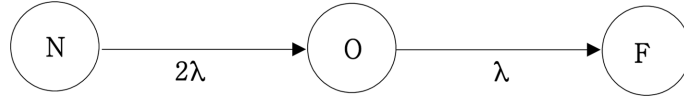


Fig. 1. Continuous time Markov chain for hot-standby sparing system.

상태  $N$ 을 유지하는 총시간을 나타내는 확률변수를  $t_N$ , 상태  $O$ 를 유지하는 총시간을 나타내는 확률변수를  $t_O$ 로 표시하면 상태  $F$ 를 나타내는 시간에 대한 확률변수  $t_F$ 는 식(1)과 같이 표시할 수 있다.

$$t_F = t_N + t_O \quad (1)$$

상태  $N$ 에 대한 고장확률밀도함수  $f_N(t)$ 와 상태  $O$ 에 대한 고장확률밀도함수  $f_O(t)$ 는 고장률에 대한 함수로 식(2)와 식(3)과 같이 표현할 수 있으며 라플라스변환을 하면 식(4)와 식(5)와 같다.

$$f_N(t) = 2\lambda e^{-2\lambda t} \quad (2)$$

$$f_O(t) = \lambda e^{-\lambda t} \quad (3)$$

$$F_N(s) = \int_0^{\infty} e^{-st} f_N(t) dt = \frac{2\lambda}{s+2\lambda} \quad (4)$$

$$F_O(s) = \int_0^{\infty} e^{-st} f_O(t) dt = \frac{\lambda}{s+\lambda} \quad (5)$$

확률변수  $t_N$ 과  $t_O$ 는 독립이고  $t_F$ 는 식(1)의 관계가 있으므로  $F_F(s)$ 는 식(6)과 같이  $t_N$ 과  $t_O$ 의 중합(Convolution) 형태로 표현할 수 있으며  $F_F(s)$ 를 라플라스 역변환하면 식(7)과 같이  $f_F(t)$ 를 구할 수 있다.

$$F_F(s) = F_N(s) \cdot F_O(s) = \frac{2\lambda}{s+2\lambda} \cdot \frac{\lambda}{s+\lambda} = \frac{2\lambda}{s+\lambda} - \frac{2\lambda}{s+2\lambda} \quad (6)$$

$$f_F(t) = 2\lambda e^{-\lambda t} - 2\lambda e^{-2\lambda t} \quad (7)$$

시간  $t$ 에 상태  $N$ 에 있을 확률을  $P_N(t)$ , 상태  $O$ 에 있을 확률을  $P_O(t)$ , 상태  $F$ 에 있을 확률을  $P_F(t)$ 로 정의하면 식(8)을 만족하며  $f_N(t)$ 과  $f_F(t)$ 를 적분하여 식(9), 식(10), 식(11)과 같이 구할 수 있다.

$$P_N(t) + P_O(t) + P_F(t) = 1 \quad (8)$$

$$P_N(t) = \int_{t_N=t}^{\infty} f_N(t) dt_N = \int_{t_N=t}^{\infty} 2\lambda e^{-2\lambda t_N} dt_N = e^{-2\lambda t} \quad (9)$$

$$P_F(t) = \int_{t_F=0}^t f_F(t_F) dt_F = \int_{t_F=0}^t (2\lambda e^{-\lambda t_F} - 2\lambda e^{-2\lambda t_F}) dt_F = 1 - 2e^{-\lambda t} + e^{-2\lambda t} \quad (10)$$

$$P_O(t) = 1 - P_N(t) - P_F(t) = 1 - e^{-2\lambda t} - (1 - 2e^{-\lambda t} + e^{-2\lambda t}) = 2e^{-\lambda t} - 2e^{-2\lambda t} \quad (11)$$

시간  $t$ 에서의 신뢰도, 즉 시간  $t$ 에서 정상동작할 확률은 식(12)와 같으며 평균 수명 수기도 식(13)과 같이 구할 수 있다.

$$R(t) = 1 - P_F(t) = P_N(t) + P_O(t) = 2e^{-\lambda t} - e^{-2\lambda t} \quad (12)$$

$$MTBF = \int_0^{\infty} t \cdot f_F(t) dt = -\left. \frac{dF_F(s)}{ds} \right|_{s=0} = \frac{3}{2\lambda} \quad (13)$$

제안한 방법으로 구한 신뢰도는 마코브 모델링을 통한 신뢰도 결과와 동일하다.

### 2.2.2 공통원인고장을 고려한 신뢰도 분석

대기이중계 구조의 하드웨어는 Fig. 2는 공통원인고장(CCF)을 고려한 마코브 체인이다. 상태  $N$ , 상태  $O$ , 상태  $F$ 는 그림 1과 동일한 상태이며 상태  $N$ 에서 공통원인고장이 발생한 경우 2개의 하드웨어가 모두 고장으로 정상동작이 불가능한 상태  $F$ 로 이동한다.  $\lambda$ 는 단일 하드웨어의 전체 고장률을 의미하며  $\lambda_C$ 는 공통원인고장에 의한 고장률,  $\lambda_O$ 는 공통원인고장을 제외한 모든 고장률을 의미한다. 따라서 다음의 관계가 성립한다.

$$\lambda = \lambda_O + \lambda_C \quad (14)$$

상태  $F$ 를 나타내는 시간에 대한 확률변수  $t_F$ 는 공통원인고장이 발생할 확률( $p_1$ )의 경우에는  $t_N$ 과 같고 공통원인고장이 발생하지 않는 확률( $p_2$ )의 경우에는 식(1)과 같다. 따라서 각 고장이 발생할 확률을 고려하면  $t_F$ 는 식(16)와 같다.

$$p_1 = \frac{2\lambda_C}{2\lambda_O + 2\lambda_C}, \quad p_2 = \frac{2\lambda_O}{2\lambda_O + 2\lambda_C} \quad (15)$$

$$t_F = p_1 t_N + p_2 (t_N + t_O) = \left( \frac{2\lambda_C}{2\lambda_O + 2\lambda_C} \right) t_N + \left( \frac{2\lambda_O}{2\lambda_O + 2\lambda_C} \right) (t_N + t_O) \quad (16)$$

상태  $N$ 에 대한 고장확률밀도함수  $f_N(t)$ 와 상태  $O$ 에 대한 고장확률밀도함수  $f_O(t)$ 는 고장률에 대한 함수로 식(2)와 식(3)과 같이 표현할 수 있으며 라플라스변환을 하면 식(4)와 식(5)와 같다.

확률변수  $t_N$ 과  $t_O$ 는 독립이고  $t_F$ 는 식(16)의 관계가 있으므로  $F_F(s)$ 는 식(17)과 같이  $t_N$ 과  $t_O$ 의 중합(Convolution) 형태로 표현할 수 있으며  $F_F(s)$ 를 라플라스 역변환하면 식(18)과 같이  $f_F(s)$ 를 구할 수 있다.

$$F_F(s) = p_1 F_N(s) + p_2 F_N(s) \cdot F_O(s) = p_1 \frac{2\lambda}{s+2\lambda} + p_2 \frac{2\lambda}{s+2\lambda} \cdot \frac{\lambda}{s+\lambda} = p_1 \frac{2\lambda}{s+2\lambda} + p_2 \left( \frac{2\lambda}{s+\lambda} - \frac{2\lambda}{s+2\lambda} \right) \quad (17)$$

$$f_F(t) = p_1 2\lambda e^{-2\lambda t} + p_2 (2\lambda e^{-\lambda t} - 2\lambda e^{-2\lambda t}) = 2\lambda(p_1 - p_2)e^{-\lambda t} + 2\lambda p_2 e^{-2\lambda t} \quad (18)$$

시간  $t$ 에 상태  $N$ 에 있을 확률  $P_N(t)$ 는 식(9)와 같고, 상태  $F$ 에 있을 확률  $P_F(t)$ 는 식(19)와 같으며, 상태  $O$ 에 있을 확률  $P_O(t)$ 는 식(20)과 같다.

$$P_F(t) = \int_{t_F=0}^t f_F(t_F) dt_F = \int_{t_F=0}^t 2\lambda(p_1 - p_2) e^{-\lambda t_F} + 2\lambda p_2 e^{-2\lambda t_F} dt_F = 1 - 2p_2 e^{-\lambda t} - (p_1 - p_2) e^{-2\lambda t} \quad (19)$$

$$P_O(t) = 1 - P_N(t) - P_F(t) = 1 - e^{-2\lambda t} - 1 - 2p_2 e^{-\lambda t} - (p_1 - p_2) e^{-2\lambda t} = -2p_2 e^{-\lambda t} + 2p_2 e^{-2\lambda t} \quad (20)$$

시간  $t$ 에서의 신뢰도, 즉 시간  $t$ 에서 정상동작할 확률은 식(21)와 같으며 평균 수명 수기도 식(22)과 같이 구할 수 있다.

$$R(t) = 1 - P_F(t) = P_N(t) + P_O(t) = (p_1 - p_2) e^{2\lambda t} + 2p_2 e^{-\lambda t} = \frac{\lambda_C - \lambda_O}{\lambda} e^{-2\lambda t} + \frac{2\lambda_O}{\lambda} e^{-\lambda t} \quad (21)$$

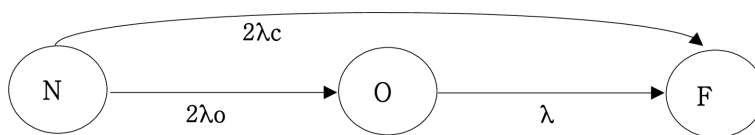


Fig. 2. Continuous time Markov chain for hot-standby sparing system with CCF.

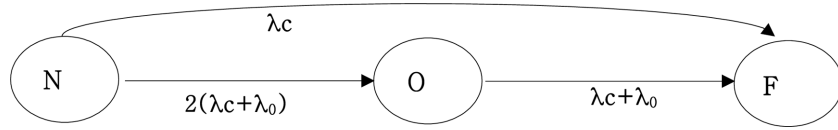


Fig. 3. Continuous time Markov chain for hot-standby sparing system with CCF in Min & Lee[6].

$$MTBF = \int_0^{\infty} t \cdot f_F(t) dt = - \left. \frac{dF_F(s)}{ds} \right|_{s=0} = \frac{p_1 + 3p_2}{2\lambda} = \frac{\lambda_c + 3\lambda_o}{2\lambda^2} \quad (22)$$

대기이중계에 대한 신뢰도는 다양한 문헌에서 분석되었으며, 공동모드고장을 고려한 신뢰도 분석은 기존 연구[6]에서 마코브 모델을 사용하여 분석하였다.

기존의 대기 이중계 신뢰도 연구[6]에서는 Fig. 3과 같이 상태 N에서 공동원인고장이 발생하여 상태 F로 전이하는 고장률을  $\lambda_c$ 로 두었고, 상태 N에서 상태 O로 전이하는 고장률을  $2(\lambda_c + \lambda_o)$ 으로 두고 분석하였다. 반면에 본 논문에서는 상태 N에서 상태 F로 전이하는 고장률은 2개의 하드웨어에서 공동원인고장이 발생하는 고장률이기 때문에  $2\lambda_c$ 로 두었으며, 상태 N에서 상태 O로 전이하는 고장률은 2개의 하드웨어에서 공동원인을 제외한 고장률  $2\lambda_o$ 로 두고 마코브 모델로 분석하였다. 결과적으로, 기존의 대기 이중계 신뢰도 연구[6]은 상태 N에서 상태 O로 가는 고장률에 공동원인고장이 고려되었고, 상태 N에서 상태 F까지의 고장률에 공동원인고장이 다시 반영되었다. 따라서 기존의 대기 이중계 신뢰도 연구[6]는 상태 N에서 공동원인고장이 두 번 고려되어 평균 고장시간이 짧게 예측되었다.

### 2.2.3 공동원인고장과 신뢰도 관계의 사례분석

철도시스템의 내장형제어기 활용비율은 ICT 발전과 활용용이성으로 인해 급격히 확산되고 있으며, 승객편의사항뿐 아니라 열차운행안전에 직접적 기능을 수행하는 신호시스템 분야까지 널리 활용되고 있다. 이러한 내장형제어기의 신뢰도와 가용도 확보를 위해 Fig. 4와 같이 전자연동장치, 궤도회로장치, 전널목제어기, 차상신호장치 등에서는 대기이중계구조로 제어기를 구성하고 있다[4,5].

대기이중계 구조는 일반적으로 동작계와 대기계를 구분하여 구성하며, 시스템 요구사항의 수행을 위해 외부 입력에 대한 정보테이블의 공유와 계간 상태감시를 위해 각각의 계가 정보를 송수신한다. 이러한 계간 정보송수신을 위해서는 공유메모리, 접점신호 등의 방법도 사용되지만 가장 구성이 간단한 방법으로 직렬통신을 이용한 정보전송이 많이 사용되며, 이러한 구조의 시스템을 고장모드영향 및 심각도분석(FMECA, Failure Mode Effect and Criticality Analysis)을 수행하면 모든 계의 서비스 불능이 상태의 고장모드(Failure Mode)에 시스템의 신뢰도가 종속되고, 이러한 고장모드들은 결함트리분석(FTA, Fault Tree Analysis)을 통해 공동고장모드로 작용함을 확인할 수 있다.

본 논문에서 제시한 계간 공동고장모드로 인한 신뢰도평가의 영향을 분석하기 위해 Table 1과 같이 일반적인 제어기의 고장률을 가정하여 공동고장모드 분석 전후의 영향을 평가한다. Table 1의 고장률은 대기 이중계 신뢰도 연구[6] 및 기존에 수행한 신뢰도 분석 프로젝트 사례를 참고하여 본 논문에 맞게 가정한 수치이다.

고장률을 가정한 Table 1의 단일계의 평균고장시간(MTBF, Mean Time Between Failure)은 고장률의 역수인 평균고장수명

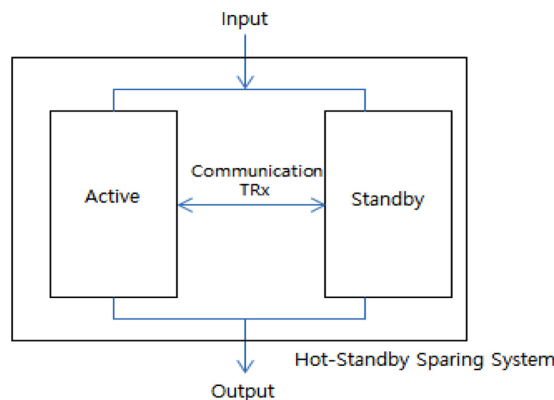


Fig. 4. Generic architecture of hot-standby sparing system on railway.

Table 1. Sample component failure rate of the hot-standby sparing system.

No	Function block	Failure rate( $10^{-6}/h$ )	??
1	CPU	2.00	
2	Communication for each redundancy	2.50	CCF
3	Memory	3.00	
4	Reset	0.50	
5	Parallel input/Output	1.00	
6	Serial input/Output	1.00	
Total		10	Single module

(MTTF, Mean Time To Failure)로 근사하면 100,000 시간이다. 이러한 단일계를 대기이중계로 구성하는 경우 가장 쉬운 방법은 미국 신뢰성센터에서 발행한 Reliability Took Kit 등의 핸드북[7]에서 제공하는 식의 활용이며, Reliability Took Kit[3]의 대기이중계 고장률은 식 (23)과 같다. 식(23)은 공통원인고장을 고려하지 않고 고장률을 지수분포로 가정할 경우 정확한 값이다.

$$\lambda_{Hot-Satnadby\ System} = \frac{2}{3}\lambda_{Single\ Module} \quad (23)$$

기존의 철도에서 대부분의 이중계 신뢰성 분석에서는 공통원인고장을 고려하지 않고 식(23)의 결과를 적용하였다. 그러나 전자동장치, 궤도회로장치, 건널목제어기, 차상신호장치 등에서는 Fig. 4와 같이 대기이중계구조로 제어기를 구성하고 있으며, 시스템의 완전한 독립을 보장할 수 없기 때문에 공통원인고장을 가지고 있다. Fig. 4는 동작계와 대기계 중 하나의 통신모듈에서 고장이 발생하면, 전체시스템이 고장상태가 되어 기능을 수행하지 못하는 예를 나타낸다.

위 식 (23)에 따라 대기이중계구조 제어기의 신뢰도를 산출하면, 고장률은  $6.67e-6/h$ (MTBF = 150,000시간)으로 평가되며, 고장률의 역수가 평균 수명 수기가 되므로 식(23)의 역수인 대기이중계의 평균 수명 수기는 식(13)과 동일한 결과로 산출되며, 이는 라플라스 변환을 이용한 본 논문의 마코브 방정식의 모형이 정확하다는 것을 보여준다.

공통고장모드를 고려하여 모델링한 식 (22)를 적용하면 동일한 단일계구조 제어기의 신뢰도는  $\lambda_o$ 와  $\lambda_c$ 가 각각  $7.5e-6/h$ 와  $2.5e-6/h$ 가 되므로 대기이중계구조 제어기 전체의 고장률은  $8.00e-6/h$ (MTBF = 125,000시간)으로 평가된다.

따라서 공통모드고장에 대한 정확한 모델링을 고려하지 않은 경우에는 20% 이상의 평균고장시간이 과평가 됨을 알 수 있으며, 이러한 평균고장시간의 부정확성은 예방유지보수(PM, Preventive Maintenance)주기 조정과 교정유지보수(CM, Corrective Maintenance)를 위한 예비품의 수급은 물론 열차정시율에 해당하는 가용도에도 부정확 요인으로 작용한다. 장기적으로는 신뢰도 함수에 대한 지수모델을 사용하는 경우 Fig. 4와 같이 사용기간에 비례하여 시스템의 과평가 효과는 증가됨을 관찰할 수 있다.

### 3. 결 론

철도시스템의 고장은 운행지연 또는 철도사고의 원인이 될 수 있어 높은 신뢰성이 요구되며, 신뢰도를 높이기 위하여 대기이중계 시스템이 사용된다. 대기 이중계 시스템은 시스템간의 독립성이 보장되지 않으면 이중계 시스템에 동시에 고장을 유발하는 공통원인고장을 고려하여야 한다. 본 논문에서는 대기 이중계 시스템에 대하여 공통원인고장이 고려되지 않은 경우와 공통원인고장이 고려된 경우의 신뢰도를 분석하고 결과를 비교하였다. 대기 이중계 시스템을 마코브 체인으로 모델링하였으며 2개 시스템이 정상인 상태, 1개 시스템이 고장인 상태, 2개 시스템이 모두 고장인 상태를 유지하는 각 시간에 대한 확률변수와 고장확률밀도함수를 사용하여 신뢰도를 분석하는 방법을 제안하였다. 제안된 방법으로 공통원인고장을 고려하지 않은 경우와 공통원인고장을 고려한 대기 이중계 시스템의 신뢰도를 분석하였으며, 제안된 방법으로 공통원인고장을 고려하지 않은 대기 이중계 시스템의 신뢰도를 분석한 결과와 기존 신뢰도 분석과 비교하여 제안된 방법이 보다 정확한 시스템 신뢰도평가에 기여함을 확인하였다.

구체적으로는 공통원인고장과 신뢰도의 관계를 분석하기 위하여 일반 제어기의 고장률을 가정하여 공통고장 모드 분석 전후의 영향을 평가하였다. 사례 분석결과 공통원인고장에 대한 정확한 모델링을 고려하지 않은 경우 평균고장시간이 20% 이상 과평가 되는 것을 확인하였으며, 신뢰도 함수에 지수모델을 적용하는 경우 사용기간에 비례하여 과평가의 효과가 증가하는 것을 확인하였다.

평균고장시간의 부정확성은 예방유지보수를 위한 주기조정과 교정유지보수를 위한 예비품의 수급에 부정확 요인으로 작용하며, 열차정시율에 해당하는 가용도 분석에도 영향을 준다. 철도시스템에 적용되는 대기 이중계는 시스템간의 독립성을 보장하기 어려운 경우가 대부분으로 공통원인고장을 고려하여 신뢰도를 분석하여야 하며, 신뢰도 분석 방법 및 결과를 제시하였다.

본 논문에서는 지수분포를 가정하여 신뢰도를 모델링하였으나, 다른 분포함수를 가정하는 경우에는 직접적으로 마코브 분석을 할 수 없다. 마코브 분석을 적용하기 위해서는 가정한 분포를 단계형 확률변수(phase-type(PH) random variable)[8]로 변환하는 과정이 필요하며, 이러한 과정에서 수치적인 분석이 복잡해 질 수 있어, 향후 이에 대해 연구가 요구된다.

## 후 기

본 연구는 한국철도기술연구원의 주요사업의 연구비 지원으로 수행되었습니다.

## References

- [1] International Electronical Committee (2002) Railway Application-Specification and Demonstration of RAMS, International Standard, IEC 62278:2002.
- [2] International Electronical Committee (2007) Communication, signalling and processing systems - Safety related electronic systems for signalling, International Standard, IEC 62425:2007.
- [3] B.W. Johonson (1989) Design and Analysis of Fault-Tolerant Digital Systems, Addison-Wesley, 47-168.
- [4] D.S. Duck, J.H. Lee, K.M. Lee, Y.K. Kim (2006) A Study on Design and Reliability Assessment for Embedded Hot-Standby Sparing FT System Using Self-Checking Logic, *Journal of the Korean Society for Railway*, 9(6), pp. 725-731.
- [5] D.S. Duck, K.M. Lee, J.H. Lee, Y.K. Kim (2007) A Study on Power Supply Method Design for Hot Standby Sparing System via Reliability Modeling, *Journal of the Korean Society for Railway*, 10(5), pp. 527-532.
- [6] G.H. Min, J.W. Lee (2007) A Study on the Advanced Reliability Assessment Method about Hot-Standby Sparing System for Railway Signaling, *The Transactions of the Korean Institute of Electrical Engineers*, 56(9), pp. 1589-1595.
- [7] The Rome Laboratory (1993) Reliability Engineer's Toolkit, Air Force Materiel Command, pp. 89-92.
- [8] M.F. Neuts (1981) *Matrix Geometric Solutions in Stochastic Models-an Algorithmic Approach*, John Hopkins University Press, pp. 41-80.

(Received 18 April 2017; Revised 15 May 2017; Accepted 10 June 2017)

**Chan-woo Park:** cwpark@krri.re.kr

Railroad Safety Research Division, Korea Railroad Research Institute, 176, Cheoldo bangmulgwan-ro, Uiwang-si, Gyeonggi-do, 437-757, Korea

**Eunkyung Chae:** ddial@krri.re.kr

Railroad Safety Research Division, Korea Railroad Research Institute, 176, Cheoldo bangmulgwan-ro, Uiwang-si, Gyeonggi-do, 437-757, Korea

**Duck-ho Shin:** ducko@krri.re.kr

Railroad Safety Research Division, Korea Railroad Research Institute, 176, Cheoldo bangmulgwan-ro, Uiwang-si, Gyeonggi-do, 437-757, Korea