# 내장형 철도신호제어시스템의 정량적 RAMS 평가에 관한 연구
# A study on Quantitative Evaluation of Railway Signaling Embedded Control System

신덕호* 이종우* 김종기* 이영훈* 김백현* 이기서**
Ducko shin Jong-woo LEE Jong-ki KIM Young-hun LEE Back-hyun KIM Key-soe LEE

ABSTRACT

This paper is presented to a theory comparing each different systems by quantitatively analyzing reliability, availability, maintenance and safety. Reliability R(t) produced by the method here is used for MTBF calculation of system as reliability of normal state. It is possible to produce the failure rate of unsafety state through modelization of system only to use the failure rate, after yielding the failure rate of failure mode to each unsafety sate in case that unsafety state is defined with the function of systems applied.

## 1. 서 론

1970년대 이후 마이크로프로세서를 사용한 내장형(Embedded) 시스템은 제어를 목적으로 하는 산업용제어기 분야에서 매우 빠른 성장을 거듭했다. 2001년도 세계 마이크로프로세서 전체 생산량 47억 3,000만개 중 97%가 컴퓨터 이외의 기기에 사용되었으며, 철도산업에서도 마이크로프로세서를 기반으로 하는 제어시스템의 비중은 급속도로 증가하고 있다.

정보통신분야 강국인 국내에서도 마이크로프로세서를 사용한 제어시스템의 철도산업에의 적용이 매우 빠른 속도로 진행되고 있으나, 시스템의 안전이 무엇보다 중요시되는 철도산업의 특성상 마이크로프로세서를 사용한 내장형 시스템 평가기술의 체계적인 구축이 이루어지지 않아 급성장하는 기술의 철도로의 도입에 걸림돌이 되고 있다. 따라서 시급히 요구되는 내장형 시스템의 평가기술을 개발하여, 시스템의 신뢰도(Reliability), 가용도(Availability), 유지보수도(Maintainability) 및 안전성(Safety)을 평가하는 체계적인 기술이 요구되고 결함의 발생에 대한 허용 및 높은 신뢰도와 유지보수도를 갖는 안전한 시스템의 제시가 요구되고 있다.

본 논문에서는 내장형 시스템으로 구성된 철도신호제어시스템의 신뢰도, 가용도, 유지보수도 그리고 안전도를 정량적으로 측정하여 서로 상이한 시스템을 비교하거나, 시스템의 특성을 향상시키기 위한 접근에 대하여 연구하였다.

## 2. 본 론

결함허용 시스템의 평가방법은 정량적(Quantitative)과 정성적(Qualitative)의 두 가지로 나누어 볼 수 있다. 정성적인 측정은 설계과정에서 얻을 수 있는 결과로 예를 들어 부분적인 설계의 호환성과 시스템에 사용된 결함허용기법의 수준을 의미한다. 정량적인 평가기술은 두 개 이상의 시스템을 비교할 때 사용한다. 예를 들어 시스템의 신뢰도, 가용도, 유지보수도, 기대수명(Mission Life) 또는 결함적용범위(Fault Coverage)가 여기에 속한다. 본 논문에서는 철도신호제어분야의 내장형 시스템의 평가를 위해 사용되는 방법에 대하여 구체적으로 연구하였다.

* 한국철도기술연구원, 정회원
** 광운대학교 정교수, 정회원

### 2.1 정량적 평가방법

앞에서 언급한 바와 같이 정량적인 평가는 시스템의 평가결과를 수치화 하여 시스템간 비교를 가능하게 한다. 예를 들어 하나의 시스템이 다른 독립된 시스템보다 신뢰도가 높다거나, 중량과 비용이 다른 시스템에 비해 낮다는 등이다. 따라서 이때 사용된 신뢰도, 중량 그리고 비용이 정량적인 평가결과이며, 응용대상에 따라 중량과 비용이 중요시되거나 신뢰도 또는 결함허용능력이 중요시되기도 한다.

본 논문에서는 고장률(Failure Rate), MTTF(Mean Time To Failure), MTBF(Mean Time Between Failure), 결함허용능력(Fault Coverage), 신뢰도 분석(Reliability Analysis), 안전성분석(Safety Analysis), 가용도 분석(Availability Analysis), 유지보수 분석(Maintainability Analysis)등의 정량적인 평가방법들을 제시하였다.

(1)고장률과 신뢰도 함수(Failure Rate and Reliability Function)

직관적으로 고장률(Failure Rate)은 시스템이 주어진 시간동안 동작하면서 발생된 소자 또는 시스템의 고장 횟수이다. 이러한 고장률은 시스템특성의 정량적인 산출에 기본이 되며 일반적으로 $\lambda$로 표현한다. 만약 시스템이 가용수명기에 있어서 고장률을 상수 $\lambda$로 표현한다면 미분의 결과는 다음과 같은 $\lambda$의 지수 함수로 표현할 수 있다. 따라서 고장률은 시스템의 신뢰도 $R(t)$의 주요 요소임을 알 수 있다.

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

신뢰도와 시간사이에서의 지수관계는 지수고장 법칙(Exponential Failure Law)이라고 알려져 있으며 이 상태는 상수 고장률 함수로 신뢰도는 시간에 대해 지수적으로 변화한다.

지수고장법칙은 전자부품에 대한 해석과 시간과 신뢰도사이에서의 관계를 접근하는데 매우 중요하며 광범위하게 사용되고 있다.

(2)고장률 산출(Failure Rate Calculation)

시스템의 분석을 위해 가장 중요한 것은 구성요소의 정확한 고장률 산출이다. 고장률 산출에 사용되는 가장 일반적인 근거는 미 국방성(United States Department of Defense-USDOD)의 MIL-HDBK-217표준이다. 이 표준의 수식들은 실험데이터와 디바이스의 동작과 고장의 분석을 통해 얻어진 전기소자의 고장률 모델에 의해 연구되었다. 따라서 고장률 계산에 중요한 파라미터로 사용되는 것이다. 예를 들어 MIL-HDBK-217B 모델에서는 직접회로(IC)의 고장률방정식을 다음과 같이 제시하였다.

$$\lambda = \pi_L \pi_Q ( C_1 \pi_T + C_2 \pi_E) \pi_P \quad \text{Failures per Million Hours}$$

$\pi_L$ = Learning Factor
$\pi_Q$ = Quality Factor
$\pi_T$ = Temperature Factor
$\pi_E$ = Environmental Factor
$\pi_P$ = Pin Factor
$C_1$, $C_2$= Complexity Factors

Learning Factor( $\pi_L$)는 IC 생산에서의 제작공정의 종합적 완숙성을 의미하며, Quality Factor( $\pi_Q$)는 소자가 사용된 정도를 의미하며 많은 사용자에 의해 검증되고 시험된 정도를 표시한다. 온도 Factor $\pi_T$는 동작온도, 패키지 기술, 전력소모 등의 디바이스 기술에 대한 함수이다. 또한 환경 Factor $\pi_E$는 환경함수이고, Pin Factor $\pi_P$는 IC 패키지의 핀에 대한 함수이다. 마지막 Factor는 복잡도 Factor $C_1$과 $C_2$이다.

복잡도는 논리회로의 게이트 수, 선형회로의 TR, 메모리의 Bit수이다. MIL-HDBK-217에서는 소자의 특성에 따른 고장률산출 공식을 제공하며, 신뢰도를 예측하는 많은 분야에서 아직도 이 표준에 맞추어 소자의 고장률을 예측하고 있다.

(3)결함허용능력(Fault Coverage)

결함허용 시스템의 설계와 분석에 중요한 요소 중에 하나가 결함허용능력이다. 결함허용능력은 결함의 존재와 시스템의 극복확률을 사용하여 수학적으로 정의된다. 결함허용능력의 수학적 표현은 다음과 같다.

$$C = P(\text{Fault Recovery} \mid \text{Fault Existence})$$

대부분 시스템의 결함허용능력 평가를 위한 접근은 시스템에서 발생할 수 있는 모든 결함을 명세하고 결함의 발생에 대한 검출 목록과 결함이 제한된 목록, 결함이 억제된 목록 그리고 결함에 대하여 시스템이 극복된 목록을 개발하는 방법을 사용한다.

### 2.2 신뢰도 모델링(Reliability Modeling)

신뢰도는 시스템에 중요한 요소이다. 시스템을 표현하는 거의 모든 요소들이 신뢰도를 기본으로 한다. 신뢰도의 산출을 위한 분석적 접근에서는 조합적 모델링(Combinatorial Modeling)과 마코브모델링이 일반적으로 사용된다. 조합모델링은 시스템을 단위시스템의 구성에 따라 직렬과 병렬에 의해 신뢰도를 계산하는 방식으로 매우 널리 알려진 방법이다. 시스템 부품레벨에서 모듈단위 신뢰도 계산에 가장 많이 사용되는 조합모델링을 사용하여 모듈의 신뢰도를 산출한다.

조합적 모델링은 여러 가지 시스템 동작 상태에서의 확률적 기법이다. 사건의 확률은 시스템 신뢰도평가 양식으로 계산된 시스템의 동작을 주도한다. 일반적으로 시스템의 신뢰도는 시스템을 구성하는 각각의 요소의 신뢰도를 사용하여 구해진다.

직렬과 병렬의 두 가지 모델이 일반적으로 사용된다. 직렬시스템에서는 구성하는 모든 요소들이 올바르게 동작해야만 시스템이 정상동작하고, 병렬시스템에서는 시스템이 정상동작하기 위해 최소 하나의 요소가 올바르게 동작하면 된다. 일반적으로 시스템은 직렬과 병렬의 서브시스템들을 조합하여 구성한다. 따라서 직렬과 병렬구조에 대하여 검토하고 각각을 모델링한다.

조합 모델링에서 가장 어려운 점은 대다수의 복잡한 시스템이 조합방식(Combinatorial Fashion)으로 모델 하는 것이 용이하지 않다는 것이다. 신뢰도 블록다이어그램의 구현이 난해하고 시스템의 신뢰도 수식 유도가 매우 복잡하다. 추가적으로 시스템의 신뢰도에 매우 중요한 요소인 Fault Coverage도 조합 모델에 의해 신뢰도 표현을 하기 어려워진다. 따라서 이러한 경우에 마코브모델이 사용한다. 마코브모델은 다중계의 구조를 갖는 시스템과 같이 결함허용을 위해 재구성 또는 모듈의 제외를 시도하는 구성에 유리하며, 시스템의 상태천이도를 산출하여 상태천이에 따른 고장률을 계산한 후 마코브모델에 의해 상태간 고장률을 간소화시킨다. 그림1은 이중계로 구성된 자동열차제어장치(ATC) 지상연속정보송신기의 상태천이 모델링이며, 그림2는 지상연속정보송신기의 마코브모델을 사용한 간소화이다.

그림2의 마코브모델을 통해 식(1)과 같이 지상연속정보송신기의 상태확률방정식을 유도하여 Laplace 변환을 통해 식(2)의 상태별 확률을 계산한다.

이중계로 구성된 자동열차제어장치 지상연속정보송신기는 PS(Perfect State)와 OF(One module failed)의 상태에서 모두 기능을 발휘하므로, 자동열차제어장치의 MTBF 산출에 사용되는 시스템 신뢰도는 다음과 같이 구할 수 있다.

$$R_{RXI}(t) = p_{PS}(t) + p_{OF}(t) = 2e^{-\lambda_{RXI}t} - e^{-2\lambda_{RXI}t}$$

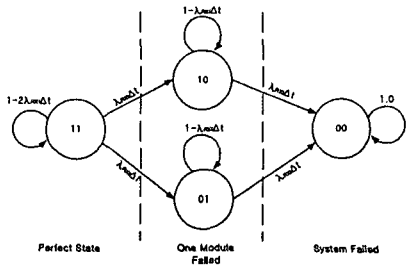


그림1. 지상연속정보송신기의 상태모델링

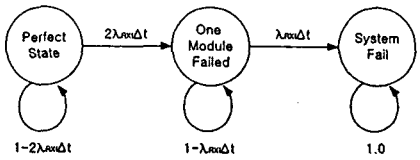


그림2. 지상연속정보송신기의 마코브모델

$$p_{PS}(t+\Delta t) = (1-2\lambda_{RXI}\Delta t)\,p_{PS}(t)$$

$$p_{OF}(t+\Delta t) = 2\lambda_{RXI}\Delta t\,p_{PS}(t) + (1-\lambda_{RXI}\Delta t)\,p_{OF}(t)$$

$$p_F(t+\Delta t) = \lambda_{RXI}\Delta t\,p_{OF}(t) + p_F(t)$$

식1. 지상연속정보송신기의 상태확률방정식

$$p_{PS}(s) = e^{-2\lambda_{RXI}t}$$

$$p_{OF}(s) = 2e^{-\lambda_{RXI}t} - 2e^{-2\lambda_{RXI}t}$$

$$p_F(s) = 1 - 2e^{-\lambda_{RXI}t} + e^{-3\lambda_{RXI}t}$$

식2. 지상연속정보송신기의 상태별확률

### 2.3 안전도 모델링

시스템의 안전성은 시스템이 정확하게 동작하거나, 고장났을 경우 안전한 특성을 가질 확률이다. 안전측(Safe)과 위험측(Unsafe)의 개념은 응용분야에 따라 차이가 있다. 대부분의 경우 시스템에서의 안전은 고장이 발생했을 경우 시스템의 전원을 차단하는 것이다. 하지만 몇몇 응용분야에서는 시스템의 전원 차단이 심각한 결과를 초래할 수 있다. 따라서 안전측 분석을 위해서는 시스템의 고장이 안전한 고장인지 위험측(Unsafe)고장인지를 명확히 구분해야하며, 응용분야에 따라서 분명하게 명시되어야 한다.

안전성은 시스템의 고장상태(Failed State)를 두 부분으로 분리한 마코브 모델을 사용하여 모델링된다. 즉 시스템 고장상태(Failed State)는 FS라고 표기하는 안전측 고장(Failed Safe)와 FU라고 표기하는 위험측 고장(Failed Unsafe)으로 분류한다.

단일 모듈로 구성되고, 고장률은 $\lambda$, 결함검출능력 C를 갖는 자기진단(Self-Diagnostics)이 가능한 단순한 시스템의 마코브 모델을 그림3에 표현하였다.
마코브 모델을 사용하여 그림3의 시스템을 안전성 수식으로 표현하면

$$S(t) = p_O(t) + p_{FS}(t)$$

가 된다. 여기서 S(t)는 안전성, $p_O(t)$는 시간 t에서 시스템이 정상 동작할 확률이며, 그리고 $p_{FS}(t)$는 시간 t에서 시스템의 안전측 상태로 존재할 확률이다. 위의 안전도 S(t)의 정의에 따라 안전도를 구하면

$$S(t) = p_O(t) + p_{FS}(t) = C + (1-C)e^{-\lambda t}$$

가 된다. 따라서 초기시간 t = 0에서 시스템의 안전성은 "1"이 되며, 시간이 무한대로 확장되는 경우 시스템의 안전성은

$$S(\infty) = C$$

가 된다.

즉 시스템의 결함검출(Fault Detection)능력이 완벽(C=1)하다면 시스템은 완벽히 안전하고, 반대로 시스템의 결함검출 Coverage가 존재하지 않는다면(C=0) 시스템은 위험측으로 고장나게 된다.

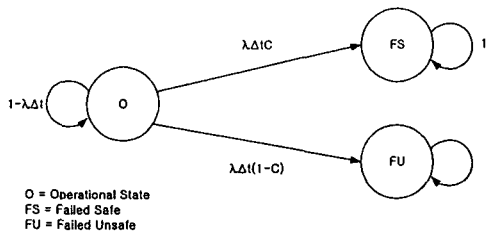

그림3. 안전도산출을 위한 3상태 마코브모델

### 2.4 가용도 모델

많은 컴퓨터관련 제조업체들은 시스템이 고객이 사용하는 동안 항상 사용 가능할 확률(가용도)을 동작하는 동안 시스템이 고장 없이 동작할 확률(신뢰도)보다 비중 있게 다룬다.

결과적으로 시스템의 중요부분은 복구가 가능하도록 설계하였으며, 이 수리율(Repair Rate)은 시스템의 가용도에 매우 큰 영향을 준다. 가용도를 표시하는 A(t)는 시스템이 주어진 시간동안 임무수행이 가능할 확률이다. 따라서 가용도는 시스템이 초기 설치되어 동작한 시간의 합으로 시스템이 동작된 시간을 나눈 값으로 근사된다. 즉, 가용도는 시스템이 임무를 수행할 수 있는 시간의 백분율이다.

초기상태 t = 0에서 시스템이 정상적으로 동작되고 시간이 흐름에 따라 시스템이 기능을 수행하고, 고장이 발생되어 수리가 수행된다. 따라서 시스템이 동작을 정확히 수행하는 시간 $t_{op}$ hours 와 수리 또는 수리를 위해 대기하는 시간을 $t_{repair}$ hours라고 하면, 총 시간 $t_{current}$는 $t_{op}$와 $t_{repair}$의 합이다. 그러므로 가용도는 다음과 같이 표현된다.

$$A(t_{current}) = \frac{t_{op}}{t_{op} + t_{repair}}$$

위 식에서 $A(t_{current})$는 시간 $t_{current}$에서의 가용도이다. 평균값 또는 정상상태(Steady-State)가용도는

$$A_{ss} = \frac{N(MTTF)}{N(MTTF) + N(MTTR)} = \frac{MTTF}{MTTF + MTTR}$$

이 된다. 하지만 단순시스템(Simplex System)의 MTTF와 MTTR은 고장률(Failure Rate)과 수리율(Repair Rate)과 관련이 깊으므로, 고장률과 수리율로 다시 표현하면

$$A_{ss} = \frac{\frac{1}{\lambda}}{\frac{1}{\lambda} + \frac{1}{\mu}} = \frac{1}{1 + \frac{\lambda}{\mu}}$$

이며, 단일시스템의 시간에 따른 가용도는 그림4와 같이 일정한 값에 수렴한다.

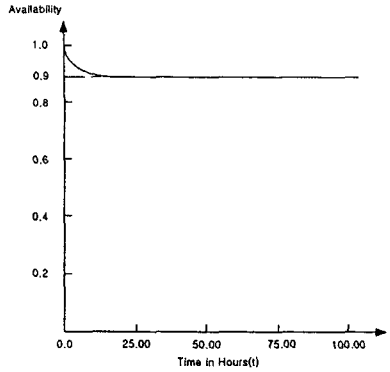


그림4. 단일시스템의 시간에 따른 가용도

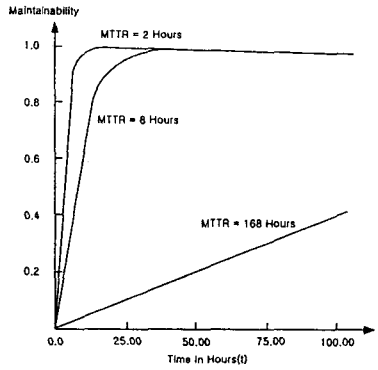


그림5. MTTR에 따른 유지보수도

### 2.5 유지보수도 모델

유지보수성(Maintainability)은 고장난 시스템이 보수되어 주어진 시간에 복구될 확률이다. 시간 t에 대한 유지보수성은 M(t)로 표현한다. 즉, M(t)는 고장난 시스템이 t와 동일하거나, t이전에 복구될 확률이다.

유지보수성의 모델링에 중요한 파라미터는 수리율(Repair Rate) $\mu$이며, 수리율을 사용하여 유지보수도를 표현하면 다음과 같다.

$$M(t) = 1 - e^{-\mu t}$$

그림5는 수리율과 유지보수도의 관계를 표현한 그림이다.

## 3. 결 론

본 논문은 시스템의 신뢰도, 가용도, 유지보수도 및 안전도를 정량적으로 산출하여 서로 상이한 구조의 시스템을 비교하기위한 이론을 제시하였다. 본 논문에서 제시된 방법으로 산출되는 시스템의 신뢰도 R(t)는 정상상태 신뢰도로써 시스템의 MTBF 산출에 사용된다. 해당 시스템의 임무에 따라 위험측 동작이 정의되는 경우에는 각 위험측동작에 대한 고장모드의 고장률을 산출하여, 이 고장률만을 사용하여 시스템을 모델링함으로써 시스템의 위험측고장률도 산출이 가능하다.

### 참고문헌

[1] "Design and Analysis of Fault-Tolerant Digital Systems" written by Barry W. Johnson Edited by Addison-Wesley.1989.

[2] "Fault-Tolerant and Fault Testable Hardware Design" written by parag K. Lala. 1985.

[3] "Fail-Safe Inteface for VLSI : Theoretical Foundations and Implementation" Michael Nicolaidis, Member, IEEE Computer Society. Vol. 47. No. 1 JAN. 1998.