한국철도학회논문집
제8권 제2호 2005년 | pp.170-175

TFM에 대한 내장형제어기의 위험측고장률 예측에 관한 연구

A study on a Prediction of Dangerous Failure Rate in the Embedded System for the Track Side Functional Module

신덕호[1] · 이재훈[2] · 이기서[3]
Ducko SHIN · Jae-Hoon LEE · Key-Seo LEE

Abstract

This study presents a prediction of a failure rate in a safety required system that consists of a embedded control system, requiring a satisfaction of a quantitative safety requirement. International Standards are employed to achieve a regular procedures in the whole life cycle of a system, for the purpose of a prediction and a evaluation of a fault that might be able to be happened in a system. This International Standards uses SIL (Safety Integrity Level) to evaluate a safety level of a system. SIL is divided into 4 levels, from level 1 to level 4, and each level has functional failure rate and dangerous failure rate of a system. In this paper we describe the conventional method to predict the dangerous failure rate and propose a method using hazard analysis to predict the dangerous failure rate. The conventional method and the technique using hazard analysis to predict the dangerous failure rate are made a comparison through the control modules of the interlocking system in KTX. The proposed method verify better effectiveness for the prediction of the dangerous failure rate than that of the conventional method.

Keywords : Safety Critical System(안전필수시스템), PHA(예비위험원분석), Hazard(위험원), HIA(위험원도출 및 분석), HAZOP(Hazard and Operability) Study, SIL(안전무결성레벨)

1. 서 론

본 논문은 안전성확보가 요구되는 내장형제어기로 구성된 시스템의 고장률예측에 대한 연구이다. 안전필수시스템은 시스템으로 인해 발생할 수 있는 사고를 예측하고 평가하여 수명주기 전반에 걸쳐 안전성확보의 입증절차를 수행하도록 권고하는 국제규격이 사용되고 있으며, 이러한 규격은 안전의 정도를 판단하는 등급으로 안전무결성레벨(Safety Integrity Level)을 사용하고 있다. 이러한 안전무결성레벨은 1부터 4까지의 분류를 통해 시스템이 가져야 할 성능측고장률과 위험측고장률을 제시하고 있으며, 본 논문에서는 시스템의 위험측고장률 만족여부를 입증하기 위한 방법으로 한국형고속철도 열차제어시스템 전자연동장치 현장제어모듈을 대상으로 미국방성(United States Department of Defense) 전자부품 고장률예측지침 MIL-HDBK-217에 의한 고장률을 예측하고, 위험원분석을 통한 위험측고장률을 산출하여 각 겨로가의 비교를 통해 안전확보를 증명하였다[1,2].

기존에 사용되는 안전무결성레벨 만족을 위한 시스템 고장률예측은 단일시스템의 경우에, 시스템 구성요소의 고장으로 인한 영향의 분석 없이 구성요소의 고장률 평균으로 예측이 수행되었다. 내장형 시스템을 구성하는 요소들의 고장률은 시간에 대하여 고장률이 변하지 않는다고 가정하는 미국방성 전자부품 고장률예측 지침서인 MIL-HDB-217을 사용한다[2]. 따라서 시스템의 안전성에 따라 목표로 정해진 고장률에 대한 만족여부를 단일시스템을 구성하는 요소들의 평균으로 계산하며, 내장형 제어기가 여분을 갖는 구조로 구성된 경우에는 병렬로 연결된 제어기가 모두 고장이 나야 위험측으로 고장난다는 가정을 사용하여, 두 제어기의 고장확률을 곱하여 위험측고장률을 예측하였다[3].

1 정회원 한국철도기술연구원 전기신호연구본부 주임연구원, 광운대학교 제어계측공학과, 박사과정
2 정회원 광운대학교 제어계측공학과, 박사과정
3 정회원 광운대학교 정보제어공학과, 교수

본 논문에서는 기존에 사용하던 시스템의 기능상실을 발생시키는 고장의 정의를, 사고로 발전되는 고장과 단순한 기능저하로 전이되는 고장으로 분류하여 사고로 발전되는 고장에 대한 안전성활동을 수행하였다. 따라서 시스템에 요구되는 안전무결성레벨에 따른 위험측고장률을 사고의 원인이 되는 위험원에 대한 발생확률로 도출하였다.

2. 본 론

2.1 안전무결성레벨의 할당

안전무결성레벨(Safety Integrity Level)은 위험원으로 인해 발생할 수 있는 리스크의 크기를 사회적으로 받아들일 수 있는 수준으로 완화시키기 위한 규제를 의미한다. 따라서 사고의 발생빈도와 심각도의 크기를 근거로 안전무결성레벨을 할당하여 안전대책의 수립을 체계적으로 관리하기 위한 기준이다.

철도신호시스템은 전기/전자/프로그래머블 제어기에 대한 의존도가 매우 높다. 따라서 철도신호시스템에 사용되는 이러한 제어기의 기준으로 유럽규격(EN)이나 국제규격(IEC)에 서는 철도신호시스템의 하드웨어, 소프트웨어, 문서화에 대한 각각의 규격을 제정하였으며, 이러한 규격에서 제시하는 안전대책의 관리기준으로 안전무결성레벨을 사용한다.

안전무결성레벨은 안전관련, 안전필수분야의 전기/전자/프로그래머블 제어기의 국제규격인 IEC61508에서도 시스템에서 발생할 수 있는 고장으로 인한 리스크의 크기를 평가하여, 위험원의 발생을 억제하기 위한 안전대책의 수립과 관리를 위한 기준으로 안전무결성레벨을 사용하고 있다. 안전무결성레벨의 할당은 철도신호시스템 신뢰성, 가용성, 유지보수성, 안전성입증을 위한 문서화규격인 IEC62278의 시스템 수명주기별 활동내역으로 인해 할당된다. 안전무결성레벨의 할당(Safety Integrity Level Allocation)은 시스템 설계단계 이전에 실시되는 개념정립 및 위험원분석을 통한 리스크평가의 결과로써, 하부시스템 단위별, 또는 전체시스템에 대하여 안전무결성레벨이 할당된다.

위험원의 분석은 전체시스템을 대상으로, 안전성활동에 의한 안전대책수립을 목적으로하며, 시스템내부의 위험원에 의한 리스크가 얼마나 감소되는지를 예측하고, 리스크감소를 위한 전체 시스템측면의 안전대책을 수립하여 추후 시스템 안전요구사항(System Safety Requirement)으로 사용하게 되는 예비위험원활동(PHA, Preliminary Hazard Analysis)을 수행한다. 예비위험원활동의 완료 후에는 시스템의 기능요구사항, 운영시나리오, 인터페이스 요구사항을 토대로 위험원도출 및 분석(HIA, Hazard Analysis and Identification)을 실시한다. 위험원 도출을 위한 기법은 여러 가지가 있으며, 대표적으로 HAZOP(Hazard and Operabiltiy) Study기법 등이 사용된다.

이러한 위험원도출 기법들은 전체시스템을 구성하는 하부시스템 또는 기능단위로 인해 발생할 수 있는 위험원을 얼마나 체계적으로 도출할 수 있는지와 밀접한 관계를 갖으며, 도출된 위험원은 앞에서 수행된 예비위험원분석단계에서 분석된 위험원과의 연관성을 갖게된다.

예비위험원분석단계에서 도출된 위험원은 사고와 같이 결과에 밀접한 위험원이며, 위험원도출에 의한 위험원은 원인에 매우 밀접한 위험원이다. 따라서 위험원도출의 위험원들은 예비위험원분석단계에서 도출된 위험원의 원인이 되며, 이러한 위험원간의 상호연관성을 분석하면 시스템으로 인한 사고시나리오를 구성할 수 있다. 사고시나리오는 하부시스템 또는 기능별 안전무결성레벨 할당에 이용된다. 따라서 위험원목록 및 위험원간의 연관관계, 그리고 위험원의 발생빈도 억제 및 심각도 완화를 위한 대책들을 정리하여 위험원목록(Hazard Log)을 작성한다. 위험원목록은 안전대책수립시 대책의 중복과 누락의 방지를 위해 참조자료로 사용된다.

PHA에서 HIA까지의 과정인 위험원분석단계를 통해 위험원별 리스크를 평가하면, 리스크를 완화하기 위한 안전대책의 기준들이 결정된다. 이러한 기준이 안전무결성레벨이며, 위험원목록에 위험원별 기능 및 하부시스템목록을 참조하여 하부시스템단위 또는 전체시스템에 대한 안전무결성레벨이 할당된다.

안전무결성레벨이 할당되면 두 가지 측면에서 시스템이 안전기준을 만족함을 보여야 한다. 첫 번째는 안전관련, 안전필수분야 전기/전자/프로그래머블 제어기의 국제격인 IEC61508에서 제시하는 고장률에 대한 기준의 만족이며, 두 번째는 철도분야 소프트웨어의 국제규격인 IEC62279에서의 안전무결성레벨에 따른 사용기술과 평가방법의 권고안 준수이다.

첫 번째 방법은 정량적 안전기준이며, 두 번째 방법은 정성적 안전기준이다. 따라서 정량적인 안전성의 입증을 위해 고장률예측과 안전성시험을 수행한다.

본 논문에서는 정량적인 안전무결성레벨 기준인 고장률 기준의 만족여부를 입증하기 위한 고장률예측방법에서 기존의 위험원분석을 배제한 시스템위험측고장률예측방법을, 위험원 분석을 통한 고장률예측방법으로 제시하여 보다 신뢰할 수 있는 시스템의 위험측고장률예측을 제안한다.

2.2 안전무결성레벨과 위험측고장률

시스템의 고장률은 시간당 고장이 발생할 확률로 정의하며, 이러한 고장률은 시스템 성능측고장률과 위험측고장률로 분류한다. 분류의 기준은 발생된 고장이 시스템의 기능상실로 발전되는 경우에는 성능측고장률이며, 사고로 발전되는 경우 위험측고장률로 분류한다[7]. 안전필수시스템관련 국제규격에서 제시하는 성능측고장률은 Table 1, 위험측고장률은 Table 2와 같다.

Table 1. Basic Failure Rate with SIL in Performance[1]

SIL	성능측면의 고장률(/Hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 2. Basic Dangerous Failure Rate with SIL in Performance[1]

SIL	안전측면의 위험측고장률(/Hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

2.3 내장형제어기의 위험측고장률예측

내장형제어기 고장률예측은 미국방성의 전자부품 고장률 예측 지침인 MIL-HDBK-217을 사용한다. MIL-HDBK-217은 전자부품의 실험데이터수집과 동작 및 고장의 분석을 통해 전자부품의 고장률 모델링을 목적으로 연구되었다. 그러므로 대부분의 안전필수시스템의 고장률예측에 중요한 참조자료로 MIL-HDBK-217을 사용하며 고장률을 상수화시키는 것이 가장 큰 장점이다.

다음은 MIL-HDBK-271의 집적회로(Integrated Circuit) 모델이다[2].

$$\lambda = \pi_L \pi_Q (C_1 \pi_T + C_2 \pi_E) \pi_P$$

$$\pi_L = \leq arningfactor$$

$$\pi_Q = qualityfactor$$

$$\pi_T = temperaturefactor$$

$$\pi_E = environmentalfactor$$

$$\pi_P = \pi nfactor$$

$$C_1, C_2 = complexityfactor$$

최근에는 MIL-HDBK-217 외에도 가전이나 일반전자제품 분야에서 Telcordia 또는 Bellcore등의 고장률모델링을 위한 지침을 사용하고 있다.

MIL-HDBK-217은 단위시스템의 고장률을 상수로 정의한다. 이러한 상수의 정의를 위해 전자부품의 고장률을 수리적으로 구성요소 특성에 따라 제공하고, 수식에 입력되는 Pi-factor에 따라 고장률을 상수화 시킨다.

2.3.1 단일시스템 고장률예측

시스템의 구성요소가 적을수록 고장률의 합도 작아진다. 따라서 낮은 고장률을 갖는 전자부품으로 구성된 단일시스템의 고장률은 상대적으로 낮다. 하지만 일반적인 내장형제어기의 설계에서 낮은 고장률의 부품으로 최소사양의 시스템을 구성해도, 능동소자가 포함되면 고장률을 10-6이하로 낮추는 것이 매우 어렵다[2]. 따라서 단일 구조로 구성되는 시스템은 안전무결성레벨 2등급 이하의 시스템에 주로 사용되며, 기능이 간단하거나 구성된 제어기로 인한 리스크의 크기가 크지 않은 경우에 사용된다[6].

Fig. 1은 한국형고속철도 열차제어시스템 전자연동장치의 현장제어모듈의 구성이다.

Fig. 1의 시스템의 구성요소를 MIL-HDBK-217을 적용하여 고장률을 예측하면 Table 3과 같다.

Table 3의 결과와 같이 안전필수시스템인 현장제어모듈의 단일계 고장률은 시스템의 기능을 수행할 수 없는 고장을 기준으로하며, 현장제어모듈 단일계고장률 2.325095×10^{-6}은 Table 1의 성능측고장률에 대한 안전무결성레벨 0-4에 모두 사용할 수 있다. 단일시스템인 경우 위험측고장률이 단일시스템의 고장률을 초과할 수 없으므로, 안전무결성레벨이 4인 전자연동장치 현장제어모듈에는 단일구조를 적용할 수 없다.

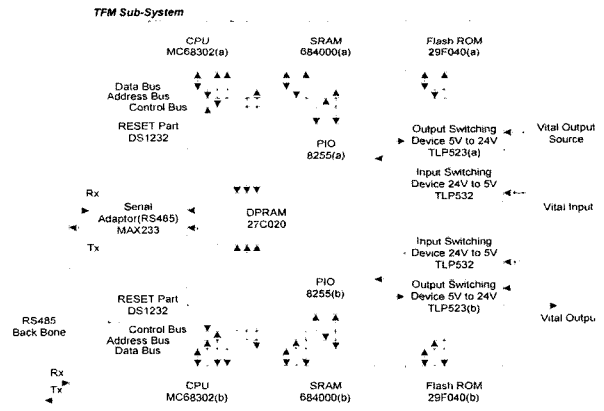

Fig. 1. TFM of the Korea High-Speed Rail for the Train Control System

즉 제시된 단일시스템의 시리얼 어댑터인 MAX233의 고장률이 위험측출력으로 직결되므로, 예측된 위험측고장률이 0.253595×10^{-6}이므로 SIL3이상에서는 이러한 단일구조를 사용할 수 없다. 따라서 이러한 단일시스템의 한계로 인해 안전무결성레벨 3이상의 시스템은 다중계 구조의 여분을 갖는 시스템으로 설계한다.

Table 3. Failure rate of Single Embedded System[2]

하부시스템	기호	단위시간당 고장률(10-6)	수량	기 타
TFM board	λ_{TFM}	2.325095	1	전체고장률
-MC68302	λ_{CPU}	0.503777	2	16Bit Microprocessor
-684000	λ_{SRAM}	0.126704	2	8Bit SRAM
-29F040	λ_{Flash}	0.011391	2	8bit Flash Memory
-TPL523	$\lambda_{SW24to5}$	0.220861	1	24V to 5V Switching Dev.
-TPL532	$\lambda_{SW5to24}$	0.220861	1	5V to 24V Switching Dev.
-27C020	λ_{DPRAM}	0.667491	1	8bit Dual-Port Memory
-DS1232	λ_{RESET}	0.121868	2	Reset Device
-MAX233	$\lambda_{SerialAda}$	0.253595	1	RS485 Serial Adaptor
-8255	λ_{PIO}	0.198545	2	Peripheral IO

2.3.2 여분을 갖는 시스템 고장률예측

여분을 갖는 시스템은 단일시스템으로는 만족시킬 수 없는 안전무결성레벨의 고장률준수 및 가용성의 향상을 위해 사용하는 설계방식이다. 위에서 제시된 전자연동장치 현장제어모듈을 2중으로 설계하여 시스템의 안전성과 가용성을 향상시킨다[3]. 이러한 여분구조의 위험측고장률예측을 위한 기존방식은 동일구조의 동작계와 대기계가 동시에 고장나야만 시스템이 위험측으로 고장난다는 논리를 적용하여 단일시스템의 고장률을 제곱하여 여분을 갖는 다중계제어기의 위험측고장률을 예측하였다. 전자연동장치 현장제어모듈의 경우 단일시스템 고장률을 제곱하면, $5.4060668 \times 10^{-12}$가 되어 SIL4에 적용할 수 있다는 위험측고장률 기존의 예측방식이다. 하지만 이러한 방식은 시스템의 위험원에 대한 분석을 수행이 어려웠을 때의 방식이며, 위험원의 발생으로 인한 사고로의 발전확률을 고려하지 않으므로 정확한 위험측고장률이라고 보기 어려웠다. 따라서 본 논문에서는 위험원 도출 및 분석을 통하여 시스템에서 발생할 수 있는 위험원에 대한 위험측고장률산출을 제안한다[1].

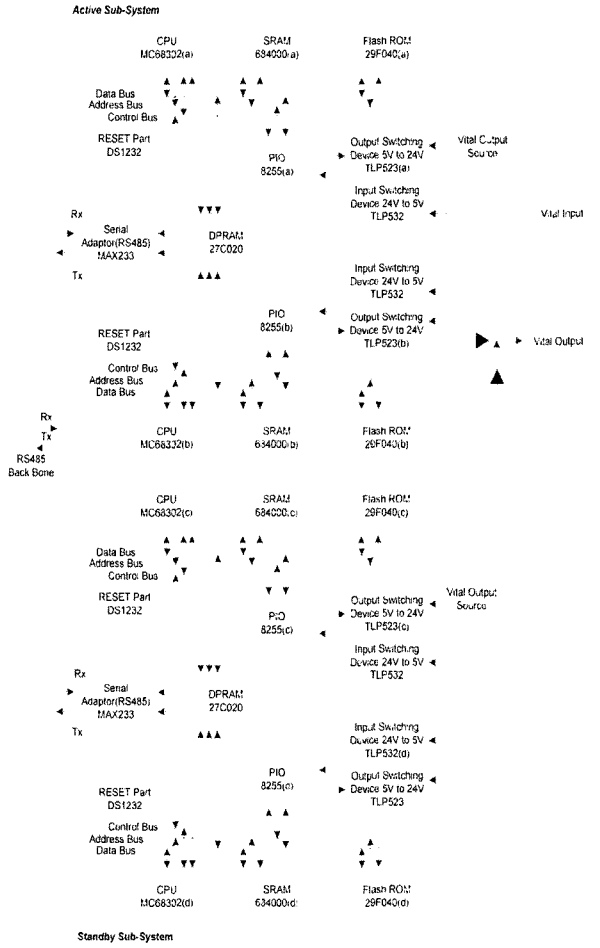

Fig. 2. Block Diagram of the TFM(Trakcside Functional Module)

2.4 위험원분석을 통한 위험측고장률의 예측

위험측고장률의 예측은 위험원 분석을 전제로 한다. 따라서 위험원분석에 의한 위험측고장률은 위험원에 대한 안전대책의 실패확률이다.

전자연동장치 현장제어모듈과 같이 선로전환기로의 잘못된 출력이 대형사고와 직결되는 바이탈 출력을 갖는 안전필수시스템은 안전무결성레벨 4를 요구한다. 바이탈 출력을 발생시키는 시스템은 해당 출력을 궤환형태로 구성하여, 병렬입출력소자의 고장을 검출하는 등의 Fig. 2와 같은 구조로써 Table 4와 같은 안전대책을 적용할 수 있다.

Table 4. Safety Activity of the Vital Output

구성요소	고장검출	안전대책
CPU	자기검사 또는 다중화	-대기이중계(Hot-Standby) -4중계(Dual-Duplex) -3중계 보팅구조(Triple Medula Redundancy)
메모리	코드이론 또는 다중화	
병렬입출력소자	궤환구성 또는 다중화	

안전대책이 모두 적용된 여분구조의 전자연동장치 현장제어 모듈은 선로전환기 제어모듈의 위험측고장률을 두 모듈이 동시에 고장났을 경우의 확률 5.4060668×10^{-12}로써, 단일시스템 고장률의 제곱으로 계산하는 것이 기존위험측 고장률에 의한 결론이다.

하지만 본 논문에서 제안하는 위험원분석을 통한 제어모듈의 위험측고장률은 다음과 같이 위험원분석을 통해 예측한다[4,5,7].

- 위험원명제 : 선로전환기의 잘못된 전환제어유지
- 위험원으로 인한 사고 : 선로전환기 도중전환으로 인한 탈선(인명피해)
- 위험원으로 인한 사고의 리스크평가 : 리스크레벨 I
- 리스크에 의한 선로전환기제어모듈의 안전무결성레벨 할당(SIL4)
- 위험원의 원인분석(사건의 논리합에 의해 사고발생)
  : 4개의 CPU가 동시에 고장
  : 결함검출을 위한 2개의 공유메모리가 동시에 고장
  : 병렬출력소자 2개가 동시고장
  : 사용메모리와 결함검출을 위한 공유메모리가 동시에 고장
  : 전문입력을 위한 시리얼 어뎁터 2개가 동시에 고장
  : 병렬출력의 스위칭소자 2개가 동시고장
  : 입력출력의 스위칭소자 2개가 동시고장

앞에서 제시한 위험원의 원인분석들은 각각의 동시고장확률을 곱하여, 모든 위험원의 원인을 더하면 보다 위험고장발생확률에 근접한 위험측고장의 발생확률이 된다. Table 3에서 제시된 구성요소별 고장률을 사용하여 본 논문에서 제시하는 위험원분석을 통한 위험측고장확률을 계산하면 다음과 같다.

$$
\begin{aligned}
&\lambda_{TFM\ Dangerous\ Failure\ Rate}\\
&=\lambda_{CPU}^{4}+\lambda_{DPRAM}^{2}+\lambda_{PIO}^{2}+\lambda_{SRAM}\lambda_{DPRAM}\\
&\quad+\lambda_{SerialAdop}^{2}+\lambda_{SW2to5}^{2}+\lambda_{SW5to24}^{2}\\
&=(0.503777\times10^{-6})^{4}+(0.667491\times10^{-6})^{2}\\
&\quad+(0.198545\times10^{-6})^{2}+(0.126704\times10^{-6})(0.667491\times10^{-6})\\
&\quad+(0.253595\times10^{-6})^{2}+2(0.220861\times10^{-6})^{2}\\
&=7.3141\times10^{-13}
\end{aligned}
$$

따라서 위험원분석을 통한 시스템의 위험측고장률 $\lambda_{TFM\ Dangerous\ Failure\ Rate}$는 7.3141×10^{-13}이다[2].

2.5 시스템고장률을 이용한 신뢰도 시뮬레이션

기존 단일시스템 동시고장확률로 예측한 위험측고장률과 본 논문에서 제시한 위험원분석을 통한 위험측고장률을 토대로 각각의 고장률을 지수특성의 고장성분을 갖는 시스템의 신뢰도산출식에 입력하여 시뮬레이션하면 Fig. 3과 같다.

Fig. 3을 통해 위험원분석을 통한 위험측고장률의 신뢰도가 단일시스템 동시고장확률을 토대로한 기존 고장률예측방식보다 높은 신뢰성을 갖음을 알 수 있다.

따라서 신뢰도의 시뮬레이션을 통해 설계를 보완하는 안전필수시스템 개발과정에서 위험원분석을 통한 위험측고장률예측방식을 활용하면, 막연히 안전무결성레벨에서 권고하는 위험측 고장확률 만족을 위한 시스템의 과잉설계를 방지할 수 있다.

3. 결 론

본 논문은 안전필수시스템의 안전대책 기준인 안전무결성레벨에서 정의한 시스템의 위험측고장률 만족여부 확인을 위한 고장률예측 방법을 제안하였다.

기존의 위험측고장률예측은 단일시스템으로 구성된 여분구조의 시스템이 동시에 고장나는 것을 위험측으로 가정하여 고장확률을 제공하여 고장률을 예측하는 방식을 사용하였으며, 본 논문에서 제안한는 방식은 사고로 발전되는 위험요인에 대한 분석을 통해 위험측 고장률을 예측하여, 보다 위험요인 발생가능성에 근접한 예측방안을 제시하였다.

기존예측방식과 제안된 예측방식을 한국형고속철도 열차제어시스템 전자연동장치의 현장제어부를 대상으로 실시하여, 각각의 고장률예측치를 제시하고 시스템의 신뢰도를 시

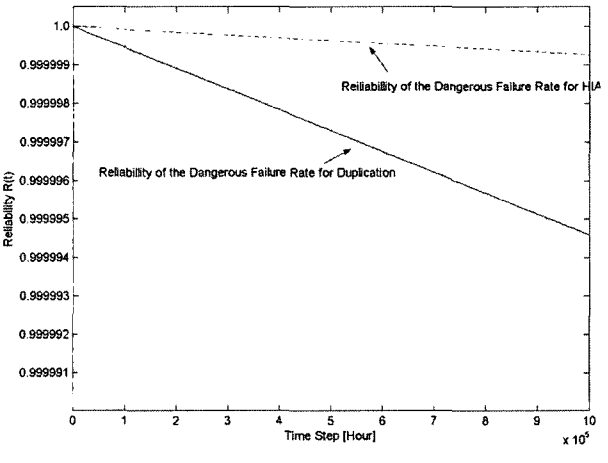

Fig. 3. Reliability Simulations for each λ

뮬레이션 하였다.

두 가지 방법으로 예측된 고장률에 의한 신뢰도 분석을 통해 효율적인 시스템 안전대책수립 및 안전확보를 위한 여분구조 설계방안을 제시하였다.

향후에는 정량적인 신뢰성, 안전성목표 만족을 위한 시스템의 최적설계에 대한 연구가 수행되어야 한다.

참 고 문 헌

1. International Standard IEC61508 "Functional Safety of Electrical/ Electronic/Programmable electronic Safety -related systems.
2. Relex Software Guidebook
3. Barry W. Johnson, 1989 "Design and Analysis of Fault-Tolerant Digital Systems"
4. Felix Redmill et al. 'System Safety : HAZOP and Software HAZOP', John Wiley & Sons, 1999
5. Defence Standard 00-58, 'HAZOP Studies on System Containing Programmable Electronics', 2000
6. 건설교통부, 고속철도기술개발사업 "열차제어시스템 안정화기술개발 2차년도 연차보고서"
7. nternational Standard IEC61882 "HAZOP Studies - Application guide"