

Tolerable Hazard Rate 도출을 위한 정량적 분석 기법 검토

정의진*, 김양모**

*한국철도기술연구원, **충남대학교

Several Quantitative Methods in order to Derive Tolerable Hazard Rate

Eui-Jin, Joung*, Yang-Mo, Kim**

*KRRRI(Korea Railroad Research Institute), **Chungnam National University

Abstract - It is very important to ensure system safety during the process of developing a system. Railway system is also devoting a great portion for the safety. Nowadays many countries leading railway industry have their own system assessment process according to the situation of their train control system. In this paper, several methods to derive Tolerable Hazard Rate are represented in the railway signalling system. the characteristics of those methods are also considered respectively.

1. 서 론

모든 시스템에는 결함이 존재하며, 이러한 결함은 결합양상에 따라 random fault와 systematic fault의 두 가지로 구분할 수 있다. random fault는 예측할 수 없는 방식으로 일어나는 고장상황에 적용되며, 이러한 결함의 대부분은 노후화로 인해 야기한다고 볼 수 있다. systematic fault는 설계 애러 또는 제조 공정 중의 잘못으로 인하여 동일한 환경에서 같은 종류의 부품 또는 장치에서 똑같은 고장을 일으키는 형태의 고장상황에 적용된다. 따라서 systematic fault는 주로 동일 원인의 고장형태로 나타나며, 설계 중에 적용되거나 제조 과정 중에 적용된다. 철도시스템에서도 마찬가지이며, 이러한 시스템의 결합 발생률을 줄이고 시스템의 안전성을 관리하기 위해서는 시스템이 갖고 있는 위험 요소를 파악하고 이를 정량적으로 분석하여 시스템에 맞는 요구사항을 제시함으로써 제조자들에게 적정 기준을 제시할 필요가 있다. 철도 신호시스템에서는 이러한 요구사항의 등급을 SIL(Safety Integrity Level)로서 제시하고 있다.

SIL 개념은 전기·전자 제어시스템에 대한 안전성 기본 규격인 IEC61508에서 뿐만 아니라 유럽 철도규격인 CENELEC의 EN50126, 50128, 50129에서도 언급하고 있다. SIL 단계가 높으면 높을수록 시스템 기능에 대한 요구사항은 더 어려워진다. 즉, SIL 4가 가장 높으며, 반면에 SIL 1은 가장 낮은 요구사항을 가진다. 또한 SIL 1에도 들지 않는 위험이 낮은 기능은 SIL 0로 둔다.

시스템의 SIL을 도출하기 위해서는 먼저 시스템이 갖고 있는 허용 가능한 위험률 즉, THR (Tolerable Hazard Rate)을 도출하여야 하는데 본 논문에서는 THR을 도출하기 위한 여러 기법들에 대하여 살펴봄으로써 정량적인 안전성 분석 방법에 대하여 살펴보고자 한다.

2. THR의 개요

2.1 용어 정리

- Tolerable Hazard Rate (THR : 허용 가능한 위험률) : 장치로 인해 야기될 수 있는 위험한 상황의 확률로 장치로부터 발생하는 위험도를 작게 하기 위하여 정해진다.
- Dangerous Failure Rate (Dangerous FR : 위험측 고장률) : 특정 설계로 구현된 장치의 고장 발생률. Dangerous Failure 확률이 THR보다 작을 경우, 장치는 안전하다고 볼 수 있다.
- Safety Integrity Level (SIL : 안전 무결도) : 시스템이 규정된 안전특성을 만족시키기 위해 요구되는 신뢰의 정도를 표시하는 수치.

2.2 SIL 등급에 따른 처리 절차

표 1은 철도 신호시스템에서 쓰이는 SIL 정도를 나타낸 것으로 각각의 경우에 대하여 나타낸 것이다. SIL 등급은 모든 안전성 지침의 기본이 되는 것으로 먼저 시스템의 고장률 또는 허용 가능한 위험률로부터 SIL을 도출하게 된다. 표 2는 CENELEC 규격에서 제시한 위험측 고장률(FR)과 허용 가능한 위험률 (THR) 정도에 따른 SIL 등급을 나타낸 것이다. 이와 같이 SIL 등급이 정해지면 각각의 SIL 등급에 따라서 이미 IEC나 CENELEC 규격에서 제안한 방법으로 시스템을 설계, 제작하도록 권고하고 있다. 국내에서는 SIL 등급에 맞추어 설계, 제작 지침을 제시한 규격이 없기 때문에 IEC61508 등에서 제시한 설계 방법 등을 참조할 수 있다. 표 3은 각 지침 중 소프트웨어 구조 설계 방법에 대하여 예를 들어 나타낸 것이다.

표 1. 철도신호시스템에서의 SIL 정도 ^[4]

SIL	안전성에 요구되는 무결성 단계	가혹도	사람 혹은 기기의 대안결과	서비스에 대한 결과	단위시간당 위험측 고장률 (Failure Rate)
4	매우높음	Catastrophic	다수 사망, 기기의 매우 큰 손실	주요 시스템 상실	$< 10^{-10}$
3	높음	Critical	사망 및 부상 기기의 중대 손실	주요 시스템 상실	$\geq 10^{-10}$ to $< 0.3 \times 10^{-8}$
2	중간	Marginal	부상 및 기기에 대한 중대 손실	심한 시스템 손상	$\geq 0.3 \times 10^{-8}$ to $< 10^{-7}$
1	낮음	Insignificant	사소한 손상	사소한 시스템 손상	$\geq 10^{-7}$ to $< 0.3 \times 10^{-6}$
0	안전성 관련 되지 않음	negligible	손상 없음	사소한 고장	

표 2. SIL 정도에 대한 FR 및 THR 정도

SIL	단위시간당의 위험률 고장률	기능 및 단위시간당 허용 가능한 위험률 (THR)
4	$FR < 10^{-10}$	$10^{-4} \leq THR < 10^{-3}$
3	$10^{-10} \leq FR < 0.3 \times 10^{-9}$	$10^{-3} \leq THR < 10^{-2}$
2	$0.3 \times 10^{-9} \leq FR < 10^{-7}$	$10^{-2} \leq THR < 10^{-1}$
1	$10^{-7} \leq FR < 0.3 \times 10^{-5}$	$10^{-1} \leq THR < 10^{-3}$

표 3. 소프트웨어 구조 설계^[1]

	SIL1	SIL2	SIL3	SIL4
1. 플트 검출, 진단	-	R	HR	HR
2. 오류검출·정정부호	R	R	R	HR
3a. 장애 어세션 프로그래밍	R	R	R	HR
3b. 안전성 백 기법	-	R	R	R
3c. 다양화 프로그래밍	R	R	R	HR
3d. 리커버리·블록 (RB)	R	R	R	R
3e. 후퇴 리커버리	R	R	R	R
3f. 전진 리커버리	R	R	R	R
3g. 재시행 플트·리커버리 기구	R	R	R	HR
3h. 기록된 실행결단 케이스	-	R	R	HR
4. 우미열화 (Graceful Degradation)	R	R	HR	HR
5. 인공지능(AI)-플트정정	-	NR	NR	NR

HR : SIL에서 높이 추천되는 수법이나 기술, 만약 이 기술이나 수법이 사용되지 않는 때는 이 방법을 사용하지 않는 논리적 해석을 상세히 기록해 둘 필요가 있다.

R : 만약 그룹 중 다른 기술이나 수법이 HR이 아니라면 적어도 하나의 기술이 요구되고 있는 것을 의미한다. : 추천하지 않는 기술이나 수법

NR : SIL에서 긍정적으로 추천할 수 없는 수법이나 기술, 만약 이 기술이나 수법을 이용할 경우에는 이 방법을 사용하는 논리적인 이유를 명확하게 기록해 둘 필요가 있다.

2.3 THR의 도출 과정

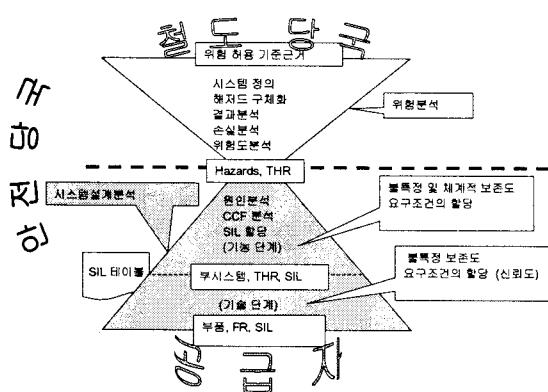


그림 1. SIL 설정을 위한 철도당국, 공급자, 안전당국의 역할

그림 2는 철도당국, 공급자, 안전당국 간의 관계를 토대로 SIL을 도출하는 상황을 도식화 하여 나타낸 것이다. 철도당국은 시스템 정의, Hazard 정의, 결과분석, 손실분석, 위험도 분석을 수행하여 해당 시스템의 SIL을 제시한 안전성 요구사항을 제시하고, 이때 공급자는 제시된 요구사항에 부합되는 시스템을 개발하기 위하여 고장의 원인분석, 공동 원인 고장(Common Cause

Failure : CCF)의 분석, 각 요소에 대한 SIL 할당 분석 등을 통하여 시스템의 기술적 구현 가능성, 비용분석 등을 한다. 경우에 따라서 철도 당국에서 제시한 값이 너무 엄격하여 기술적으로 구현이 어렵거나 비용 대비 효과면에서 큰 이득을 얻지 못하는 경우 안전 당국에서는 양측의 의견 및 분석 내용을 토대로 적정 SIL을 제시하게 된다. 여기에서 철도당국의 결과분석, 손실분석, 위험도 분석과정이 THR 도출 과정이라고 할 수 있다.

3. THR 산출 방법

3.1 ALARP

(As Low As Reasonable Practicable)

ALARP은 말이 뜻하는 바와 같이 실행 가능한 한 위험도를 낮춘다는 뜻으로 경제성 원칙에 입각하여 위험도를 낮추는 것이다. 이때 검토사항으로는 시스템에 내재되어 있는 위험도가 많은 사상자를 내는 치명적인 사건을 발생시키는지 검토하여야 한다. ALARP으로 위험도를 분석할 경우에는 두 가지 영역을 기본으로 한다. 즉 사건 발생 빈도와 사건의 심각도이다. 빈도영역은 보통 10배수로 구분하고 있으며(표 4), 심각도영역은 다음 표 5와 같이 정의할 수 있다. 이후 사건발생빈도와 사건의 심각도의 조합으로 ALARP 영역을 정의하게 된다.

표 4. 사건 발생빈도 (예)

내용	빈도 영역 (회수/년)	범주
자주 일어나는	10^{-1}	A
있을 수 있는	10^{-2}	B
아파끔 일어나는	10^{-3}	C
거의 일어나지 않는	10^{-4}	D
일어나지 않을 것 같은	10^{-5}	E
믿을 수 없는	10^{-6}	F

표 5. 사건의 심각도 (예)

안전성	고장 결과	심각도
심각하지 않음	몇몇 경상 사고	IV
경계에 있는	몇몇 중상 사고	III
심각한	1명의 사망 사고	II
파국적인	10명의 사망사고	I
재난을 초래하는	100명 이상의 사망 사고	0

표 6. ALARP 영역 (예)

A	T	I	I	I	I
B	T	T	I	I	I
C	T	T	T	I	I
D	N	T	T	T	I
E	N	N	N	T	T
F	N	N	N	T	T
	심각하지 않음 (IV)	경계에 있는 (III)	심각한 (II)	파국적인 (I)	재난을 초래하는 (0)

ALARP 방법은 집합적인 위험도를 고려하는 것으로, 시스템 요구사항에서는 ALARP 영역에 맞추어 각각의 서브 시스템에 대하여 각각의 THR이 도출되며, 이때 전체 시스템의 모든 부품 및 서브 시스템의 THR이 ALARP 요구사항을 만족하도록 하여야만 한다.

표 6에서 시스템이 T (Tolerable) 영역 또는 I (Intolerable) 영역에 있는 한 Hazard를 감소시켜야

하며, 만약 Hazard 감소 작업 도중 더 이상의 Hazard 감소에 너무 많은 노력이 필요하다면 Hazard 감소 작업을 T영역에서 멈출 수도 있다. 또한 기능 또는 서브시스템에 대한 ALARP 영역을 분할하면서 기능 및 서브시스템의 제한치를 계산할 수 있다.

3.2 MEM

(Minimum Endogenous Mortality)

MEM은 개개인의 위험도에 기본을 두어 분석을 하는 것으로 개개인의 사망률 중 가장 낮은 값을 기준으로 하여, 기술시스템이 전반적으로 허용 가능한 개인 위험 곡선을 결정토록 한다. 그 대상은 15세의 사람을 기준으로 하며, 이때의 자연사망률은 보통 년당 2×10^{-4} 로 알려져 있다. 기술적인 문제로 발생하는 사망사고가 시스템의 5% 이상 영향을 미쳐서는 않된다는 가정에 의하여 기술적인 문제로 인해 발생하는 사망률은 $10^{-5}/year$ 보다 큰 위험률로 시스템이 개개인에게 치명적인 위협을 가해서는 안된다는 것을 도출할 수가 있다. $10^{-5}/year$ 의 사망률이 철도시스템 전체에 해당한다면, 차량, 신호, 전력, 궤도로 나누어 각각의 하부시스템에서는 더욱 분할할 수가 있다.

이 수치는 철도 운영처의 사고 통계에 따라 조절될 수 있으며, 만일 신호시스템이 전체 철도시스템의 10% 정도로 개개인의 안전에 영향을 미친다면, 신호시스템으로 기인한 개별 허용 위험은 $10^{-6}/year$ 이 되며, 이는 철도 안전 분야에 있어서 많은 연구가 이루어진 유럽에서는 상당히 타당하고, 현실적인 수치로 받아들여지고 있다.

3.3 GAMAB

GAMAB의 원리는 매우 간단하다. 만약 $\lambda_{기존 고장률}$ 와 $\lambda_{신규 고장률}$ 가 각각 기존 시스템 및 새로운 시스템에 대한 위험축 고장률이라면, GAMAB 원리에서는 시스템이 다음과 같은 부등식 관계를 가지도록 요구하고 있다.

$$\lambda_{신규 고장률} \leq \lambda_{기존 고장률}$$

이 경우 위험축 고장률은 관련 사항의 발생 확률 ($\lambda_{관련사항 발생 확률}$, 예를 들어 시간당 열차 수)과 관련 사항의 고장률 ($P_{고장발생 확률}$)의 곱으로 정의할 수 있다. 즉,

$$\lambda_{고장률} = \lambda_{관련사항 발생 확률} * P_{고장발생 확률}$$

새로 만들어진 철도시스템은 기존의 등등한 시스템이 가지는 정도 이하의 위험수준을 가져야만 안전하다는 것이다. 이는 장기간의 실제 운행으로 안전이 입증된 시스템보다 같거나 적은 위험률을 가진다면 안전하다고 볼 수 있다는 관점에서 출발한 것이다. 따라서 GAMAB 접근방법은 기존 시스템은 관련된 위험이 허용 가능하다는 가정에 근거한다.

이 경우, 기존 시스템의 위험율은 다음과 같은 방법으로 도출할 수가 있다.

- 사고 통계의 평가
- 기존 시스템의 해저드 분석

위 분석 기법을 적용하여 THR을 산출한 후에 THR에 맞추어 각국의 철도신호시스템 기능별 SIL을 도출하면 표 7과 같다.

표 7. 철도신호시스템에 대한 각국의 SIL 할당 예⁽⁵⁾

기능	독일 DB	영국 BR	프랑스 SNCF	스위스 SBB	이태리 FS	오스트리아 OeBB
연동	4	4	4	4	4	4
선로전환	4	4	4	4	4	4
열차검지	4	4	4	4	4	4
열차제동	2	2	4	2	4	2
자동폐색	4	4	4	4	4	4
전념목제어	4	4	4	4	4	4
전념목 감시	4	4	NA	4	2/4	4
제어반	4	2	4	3	4	4
자동열차제어	4	4	NA	NA	4	NA
자동진로설정	2	2	NA	2	2	2

4. 결 론

THR을 도출하기 위한 세 가지 원리에 대하여 살펴보았다. MEM 접근방식은 하나의 기능이나 장치에 대하여 허용 가능한 위험률(THR)의 직접 계산이 가능하다. 계산 시에 필요한 몇 가지 요소의 위험도 할당시 몇 가지 사항에 대하여 가정이 필요하다. ALARP 접근방식은 상한 ALARP 값과 하한 ALARP 값을 두고 접근을 하며, 허용 가능한 위험률을 얻는데 있어서 좀 더 직접 관여한다. 위험축 고장 발생 확률이 있는 사항에 대하여 경제성과 실현 가능성 등을 따져 ALARP 영역 이하로 고장 발생 확률을 낮추는 접근방법이다. GAMAB 접근방식은 적용이 간단한데 기존 시스템과 새로운 시스템을 비교하여, 적은 부분만을 비교하면 되나, 기존 시스템의 분석이 선행되어야 한다. 즉 기존 시스템의 위험축 고장 발생 확률이 기준이 된다.

위험도 분석은 경제성 분석의 기초가 되어 과도한 기술개발을 줄이거나 적정투자를 유도하는데 근거로서 활용할 수 있다. 국내 철도신호 산업환경을 고려하면 안전성 평가나 위험도 분석작업이 쉽지만은 않은 작업일 수 있으나, 안전성 검증작업으로 전 세계적으로 요구되고 있으며, 국내 철도 산업의 발전 및 철도시스템의 안전성 확보를 위해서는 필요 불가결한 작업이라고 할 수 있다. 철도 시스템의 안전성 연구는 아직 초기 단계로 이 분야에 대한 지속적인 안전성 확보 및 평가 기술에 대한 연구가 필요하다고 하겠다.

(참 고 문 현)

- [1] International Electrotechnical Commission, IEC61508 parts 1-6, Functional safety of electrical /electronic/programmable electronic safety-related system.
- [2] CENELEC EN50126, Railway application The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS) Issue : March 2000
- [3] CENELEC Final Draft prEN 50128, Railway Applications Software for Railway Control and Protection Systems Issue : June 1997
- [4] CENELEC EN50129, Railway application Safety related electronic systems for signalling Issue : April 2000
- [5] Institution of Railway Signal Engineers(IRSE) report, Safety system validation with regard to cross acceptance of signalling systems by the railways, Issue : January 1992