철도신호시스템의 정량적 분석 기법을 통한 SIL 도출방안 검토

정의진*°, 김양모**
*한국철도기술연구원, **충남대학교

Quantitative analysis to derive SIL in the railway signalling system

Eui-Jin, Joung*°, Yang-Mo, Kim**
*KRRI(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 principles according to the situation of their train control systems. In this paper, several principles to derive Safety Integrity Level (SIL) are represented in the railway signalling system. The characteristics of those principles are also considered respectively.

1. 서 론

모든 시스템에는 결함이 존재하며, 이러한 시스템의 결함 발생을 줄이고 시스템의 안전성을 관리하기 위해서는 시스템이 갖고 있는 위험 요소를 파악하고 이를 정량적으로 분석하여 시스템에 맞는 요구사양을 제시할 필요가 있다. 요구사양에는 시스템의 안전성 확보를 위해서 제조자들이 도달해야하는 기준이 제시되어 있는데 철도신호시스템에서는 이러한 요구사항의 기준을 SIL (Safety Integrity Level)로서 제시하고 있다.

SIL 도출을 위해서는 THR(Tolerable Hazard Rate)의 도출이 선행되어야 하는데 주로 사용되는 THR 도출 원리로는 사건 발생빈도와 가혹도를 고려하여 THR을 산출하고, 안전성을 향상시키고자 하는 노력과 경제성을 고려하여 적정 수준을 제시하고자 하는 ALARP 원리와 인간의 내재 최소 사망률을 기준으로 THR을 도출하는 MEM 원리, 기존에 운영하는 시스템과 비교하여 그보다 적어도 같거나 높은 안전성을 얻어야만 한다는 GAMAB 원리의 세 가지가 있다. 본 논문에서는 SIL 제시를 위한 여러 가지 THR 도출기법들을 살펴봄과 함께 적정 예를 들어 서로의 특성을 비교하고자 한다.

2. THR의 개요

장치로 인해 야기될 수 있는 위험한 상황의 확률을 THR이라 하며, 시스템의 위험측 고장 발생률을 Dangerous Failure Rate 라고 하는데 이 Dangerous Failure Rate가 THR보다 작을 경우, 장치는 안전하다고 말할 수 있다. 또한 SIL이란 안전 무결도를 나타내는 것으로 시스템의 규정된 안전특성을 만족시키기 위해 요구되는 신뢰의 정도를 표시하는 수치이다. SIL은 시스템 안전도의 지침이 되는 값으로 시스템의 Dangerous Failure Rate 또는 THR로부터 SIL을 도출하게 된다. 표 1은 CENELEC 규격에서 제시한 Dangerous Failure Rate와 THR 정도에 따른 SIL등급을 나타낸 것이며, 표 2는 철도 신호시스템에서 쓰이는 SIL의 정도를 나타낸 것이다.

표 1. SIL 정도에 대한 FR 및 THR 정도

SIL	단위시간당의 위험측 고장률 (FR : Failure Rate)	기능 및 단위시간당 허용 가능한 위험률 (THR)
4	FR $\langle 10^{-10}$	$10^{-9} \le$ THR $\langle 10^{-8}$
3	$10^{-10} \le$ FR $\langle 0.3\times10^{-8}$	$10^{-8} \le$ THR $\langle 10^{-7}$
2	$0.3\times10^{-8} \le$ FR $\langle 10^{-7}$	$10^{-7} \le$ THR $\langle 10^{-6}$
1	$10^{-7} \le$ FR $\langle 0.3\times10^{-5}$	$10^{-6} \le$ THR $\langle 10^{-5}$

표 2. 철도신호시스템에서의 SIL 정도

SIL	안전성에 요구되는 무결성 단계	가혹도	사람 혹은 기기에 대한 결과	서비스에 대한 결과	단위시간당 위험측 고장률 (Failure Rate)
4	매우높음	Catastrophic	다수 사망, 기기의 매우 큰 손실	주요 시스템 상실	$\langle 10^{-10}$
3	높음	Critical	사망 및 부상 기기의 중대 손실	주요 시스템 상실	$\ge 10^{-10}$ to $\langle 0.3\times10^{-8}$
2	중간	Marginal	부상 및 기기에 대한 중대 손실	심한 시스템 손상	$\ge 0.3\times10^{-8}$ to $\langle 10^{-7}$
1	낮음	Insignificant	사소한 손상	사소한 시스템 손상	$\ge 10^{-7}$ to $\langle 0.3\times10^{-5}$
0	안전성 관련 되지 않음	negligible	손상 없음	사소한 고장	

3. THR 산출 원리

3.1 ALARP
(As Low As Reasonable Practicable)

ALARP은 말 그대로 실행 가능한 한 위험도를 낮춘다는 뜻으로 경제성 원칙에 입각하여 위험도를 낮추는 것이다. 이 원리는 영국에서 주로 쓰이면서 원리가 정립된 것으로 시스템의 내재 위험도로 많은 사상자가 발생하는 치명적인 사건에 대하여 검토한다. ALARP으로 위험도를 분석할 경우에는 사건 발생 빈도와 사건의 심각도의 두 가지 영역을 기본으로 한다. 빈도영역은 보통 10배수로 구분하고 있으며(표 3), 심각도영역은 다음 표 4와 같이 구분할 수 있다. 이후 사건발생빈도와 사건의 심각도의 조합으로 ALARP 영역을 정의하게 된다.

ALARP 원리는 집합적인 위험도를 고려하는 것으로, 시스템 구성시 ALARP 영역에 맞추어 각각의 서브 시스템의 THR을 도출하고, 이때 전체 시스템의 모든 부품 및 서브 시스템의 THR이 ALARP 요구사양을 만족하도록 하여야만 한다.

표 5에서 시스템이 T (Tolerable)영역 또는 I (Intolerable) 영역에 있는 한 Hazard를 감소시켜야

하며, 만약 더 이상의 Hazard 감소에 너무 많은 노력이 들어간다면 Hazard 감소작업을 T영역에서 멈출 수도 있다. 세부적으로는 기능 또는 서브시스템별로 ALARP 영역을 분할하여 기능 또는 서브시스템의 제한치를 계산할 수도 있다.

표 3. 사건 발생빈도 (예)

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

표 4. 사건의 심각도 (예)

안전성	고장 결과 (심각도)	범주
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 5. 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)

3.2 MEM
(Minimum Endogenous Mortality)

독일에서 제시한 안전성 원리로 MEM은 개개인의 위험도에 기본을 두어 개개인의 사망률 중 가장 낮은 값을 기준으로 하여, 기술시스템에 있어서 전반적으로 허용가능한 값을 결정한다. 내재 최소 사망률의 기준 대상은 15세 인간으로 하고 있으며 이때의 자연사망률은 년당 2×10^{-4}로 알려져 있다. 기술적인 문제로 발생하는 사망사고가 시스템의 5% 이상 영향을 미쳐서는 안된다는 요구사양에 의하여 기술적인 문제로 인해 발생하는 사망률은 10^{-5}/year보다 큰 위험률로 개개인에게 치명적인 위협을 가해서는 안됨을 알 수 있다. 10^{-5}/year의 사망률이 철도시스템 전체에 해당한다면, 차량, 신호, 전력, 궤도로 나누어 각각의 하부시스템에서는 더욱 세분할 수 있다.

이 수치는 철도 운영처의 사고 통계치에 따라 조절될 수 있으며, 만일 신호시스템이 전체 철도시스템의 10% 이내로 개개인의 안전에 영향을 미쳐야만 한다는 요구사양이 있다면, 신호시스템으로 기인한 개별 허용 위험은 10^{-6}/year이 된다. 본 수치는 철도 안전 분야에 있어서 많은 연구가 이루어진 유럽에서도 상당히 타당하고, 현실적인 수치로 받아들여지고 있다.

3.3 GAMAB
(Globalement Au Moins Aussi Bon)
Globally at least equivalent principle

GAMAB의 원리는 프랑스에서 제시한 안전성 원리이다. 만약 $\lambda_{\text{기존 고장률}}$와 $\lambda_{\text{신규 고장률}}$가 각각 기존 시스템과 새로운 시스템에 대한 위험측 고장률이라면, GAMAB 원리에서는 시스템이 다음과 같은 부등식 관계를 가지도록 요구하고 있다.

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

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

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

새로 만들어지는 시스템은 기존의 동등한 시스템이 가지는 수준 이하의 위험정도를 가져야만 안전하다는 것이다. 즉, 장기간의 운행경험으로 안전이 입증된 시스템과 비교하여 적거나 같은 위험률을 가진다면 안전하다는 것으로 GAMAB 접근방법은 기존 시스템은 관련된 위험이 허용 가능하다는 가정에 근거를 두고 있다.

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

- 사고 통계의 평가
- 기존 시스템의 해저드 분석

4. THR 산출 예

THR 도출방법에 대하여 구체적으로 살펴보기 위하여 아래 제시한 대상시스템을 ALARP과 MEM 원리에 따라서 THR을 산출하여 보았다.

4.1 분석 대상

- ATC (Automatic Train Control) 자동열차제어시스템
- 20개의 이중계 모듈로 구성
- 가정 : 자동열차제어시스템으로 야기되는 사망사고는 전체 사망사고의 10%

4.2 ALARP에 의한 산출

표 6. 사건 발생빈도, 심각도 및 관련 범주의 관계

빈도 영역 (회수/년)	범주
10^{-2}	A
10^{-3}	B
10^{-4}	C
10^{-5}	D
10^{-6}	E
10^{-7}	F
10^{-8}	G

고장 결과 (심각도)	범주
1명의 사망 사고	III
10명의 사망사고	II
100명의 사망 사고	I
1000명 이상의 사망 사고	0

표 7. 철도 시스템의 ALARP 영역

A	T	I	I	I
B	T	T	I	I
C	T	T	T	I
D	N	T	T	I
E	N	T	T	T
F	N	N	T	T
G	N	N	N	T
	III	II	I	0

표 7을 달리 나타내면 표 8과 같다.

표 8. 철도시스템의 ALARP 영역

사망자 수	년간 회수에 있어서 낮은 영역의 ALARP	년간 회수에 있어서 높은 영역의 ALARP
1	10^{-4}	10^{-2}
10	10^{-5}	10^{-3}
100	10^{-6}	10^{-4}
1000	10^{-8}	10^{-6}

표 8은 철도시스템 전체에 대한 ALARP 영역이며, 다음의 가정에 근거하여 ATC의 ALARP 영역을 표 9와 같이 도출할 수 있다.

- ATC로 인해 야기되는 사망사고는 전체사고의 10%
- ATC 고장 중 5%만이 사망자를 발생시킴
- ATC의 고장은 대부분 1~10의 사망사고 (100명 이상 사망자를 갖는 경우는 화재가 발생할 경우임)

표 9. ATC의 ALARP 영역

사망자 수	년간 회수에 있어서 낮은 영역의 ALARP	년간 회수에 있어서 높은 영역의 ALARP
1	$2*10^{-6}$	$2*10^{-2}$
10	$2*10^{-7}$	$2*10^{-3}$

표 9중 10명의 사망자에 대한 ALARP 영역을 고려하여 ATC의 THR을 도출하면 낮은 영역의 ALARP일 경우 $2*10^{-10}/hour$가 되며, 앞서의 가정에 의하여 각각의 단일모듈에 대한 THR은 $10^{-11}/hour$가 된다.

같은 방법으로 높은 영역의 ALARP에 대하여 ATC의 THR은 $2*10^{-7}/hour$, 단일모듈에 대한 THR은 $10^{-8}/hour$ 가 된다. 전체적으로 ATC 시스템의 안전무결도는 SIL 4임을 알 수 있다.

4.3 MEM에 의한 산출

인간의 내재 사망률을 기본으로 하여 ATC의 위험률은 $10^{-6}/year$이며, ATC 고장 중 5%만이 사망사고로 이어진다면, 사망사고를 일으키는 확률은 $2*10^{-5}/year$가 된다. 따라서 THR은 $2*10^{-9}/hour$ 가 된다. 따라서 ATC의 안전무결도는 SIL 4임을 알 수 있다.

5. 결 론

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

위 원리에 따라서 ATC 시스템에 대하여 ALARP과 MEM을 비교한 결과는 다음과 같음을 알 수 있다.

- MEM 접근방법에서 도출된 위험률 범위는 ALARP 접근법으로 도출한 범위보다 작다.
- 도출된 SIL은 두 방식 모두 같다. 즉 ALARP과 MEM 접근방법으로 도출한 SIL은 모두 SIL4 이다.
- MEM 접근방법 적용시에는 먼저 내재 사망자수에 대한 결정이 이루어져야 한다.

안전성 분석작업은 많은 데이터와 여러 사람의 노력이 함께 요하는 작업이다. 따라서 한국 상황에 맞는 안전성 기준을 제시하기 위해서는 많은 관련 데이터의 축적 및 안전성 확보 및 평가 기술에 대한 지속적인 연구가 필요하다고 하겠다.

[참 고 문 헌]

[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