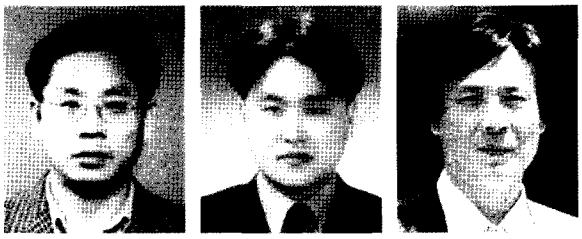
철도신호시스템에서의 향상된 안전성확보방안에 대한 연구



이종우 * 신덕호 ** 이기서***

ABSTRACT

This paper discuss advanced safety in the railway signaling system. The specified methods and HAZOP about Hazard identification and analysis of railway signalling system were studied, and loss analysis and ALARP model in order to calculate safety as a standard capacity were proposed.

It was also resulted from Hazard identification, analysis and evaluation by applying advanced safety to the railway signalling system.

1. 서 론

안전성 기술은 주로 자연재해방지를 목적으로 한 것이었지만, 산업혁명 이후 기계회된 동력을 사용하게 됨에 따라 인간-기계 계에 있어서의 안정성이 새로운 문제로 대두되어 왔다. 이 경우 안전성이란 인간의 과실 또는 기계 고장으로 인해 인간이 위해를 입거나 장치가 파손되는 상태가 없는 것이라고 할 수 있다. 따라서 안전성 기술은 안타까운 사고의 경험에서 교훈을 얻어 진보를 이룩한 많은 실례가 바탕이 된다. 1954년

■주■■
1) * 한국철도기술연구원 책임연구원, 정회원 ** 한국철도기술연구원 주임연구원, 정회원 *** 광운대학교 정교수, 정회원

연속해서 일어난 최초의 제트 여객기 코멧토의 공중분해 사고는 사고이후 진행된 철저한 사고원인 규명으로 항공기 안전성설계에 큰 영향을 끼쳤다. 또 1957년 영국의 윈즈켈에서 발생한 원자로 화재사고는 「죽음의 재」가 외부에까지 튀어 날아가 큰 소동을 일으켰으며, 역시 이 사고는 원자로의 안전성관리분야에 큰 영향을 미쳤다.

전기철도시스템은 궤도, 차량, 신호 및 급전전철 등의 시스템이 조합하여 열차를 운행할 수 있도록 구성된다. 또한 철도시스템은 궤도를 따라 고속으로 운전하고, 제동거리가 길며, 고전압으로써 동작을 한다. 그러므로 철도시스템은 운용에 있어서 많은 사고위험성을 내포하고 있다. 철도사고는 탈선, 열차간의 충·추돌, 사람과 열차 및 자동차와 열차의 충돌, 열차와 침입물 간의 충돌, 화재, 감전, 추락 등을 포함하고 있다.

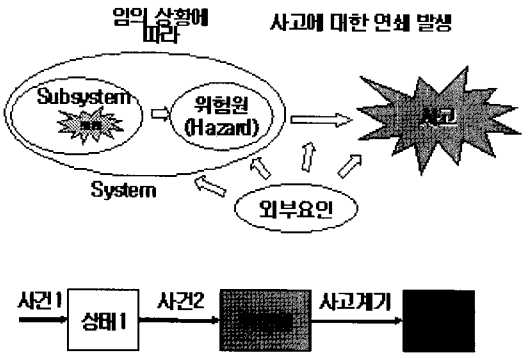
철도는 국가의 중추적인 물류를 담당하고 있으므로, 잦은 철도사고는 교통수단으로써의 철도신뢰도를 낮추어, 결과적으로는 국민이 철도이용을 기피하게 된다. 따라서 철도이용률의 향상을 위해서 안전성을 반드시 확보하여야 한다.

철도에서의 안전확보는 속도향상, 운용효율 향상 등과 더불어 매우 비중 있게 추구되고 있는 목표중의 하나이다. 본 논문에서는 철도의 안전성확보방법에 관한 연구를 소개한다.

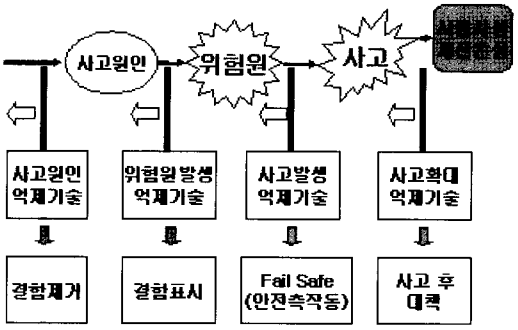
2. 사고 및 안전성 기술

2.1 사고발생순서

사고의 발생은 그림1에서 나타난 것과 같이 어떤 원인의 발생에 의해서 내·외부 요인으로 인해 위험원(Hazard)로 전이되고, 다시 내·외부의 요인에 의해서 사고로 전이된다.



〈그림 1〉 사고의 발생은 어떤 원인에 의해서 위험원으로 전이되고 다시 위험원은 사고로 전이된다.



〈그림 2〉 사고방지를 위한 안전성 적용기술

사고는 위에서 기술한 것처럼 인간에 대해서는 부상, 불구가 되게 하고 혹은 생명을 잃게 하는 것, 혹은 재산(의 기능)을 잃게 하는 것이다. 사고를 발생시키는 원인은 여러 가지가 있다. 사고는 위험원을 발생시키는 원인과 사고를 발생시키는 원인 및 그 결과 사고로 이어지는 사고발전과정으로 나타낼 수 있다. 그림1에서는 사고발생진전 순서를 나타내고 있다. 사고가 발생하기 위해서 다양한 원인에 의해서 사고의 원인이 발생하고, 과도상태로 전환되어 사고로 이어지게 된다. 사고를 발생시키는 사고원인이 있으며, 사고의 원인으로부터 위험원이 발생되고, 위험원과 관련된 계기의 발생으로 인해 사고로 이어진다. 사고가 발생되는 관계는 장치 혹은 시스템의 고장에 의해서, 위험원발생 상태로 전이되고, 다시 위험원에서 사고로 확대되어 진다.

2.2 안전성기술

안전성을 확보하기 위해서 그림2와 같이 사고원인이 발생하지 못하도록 각 단계에서 적절한 대책을 강구하여 사고로 발전되지 않도록 한다. 예를 들어 사고원인이 발생하지 않도록 결함을 제거하며, 결함이 발생하였을 경우 해저드 상태로 도달하지 않도록 결함발생표시 기능을 갖추거나, 해저드에서 사고로 이어지지 않도록 안전측 동작을 유도하고, 사고가 발생하였을 경우 사고가 확대되지 않도록 하며, 사고 후 처리 방법을 강구하는 것 모두가 안전성기술 확보라 할 수 있다.

3. 안전성확보방안

3.1 위험원 규명 및 분석(Hazard Identification and Analysis)

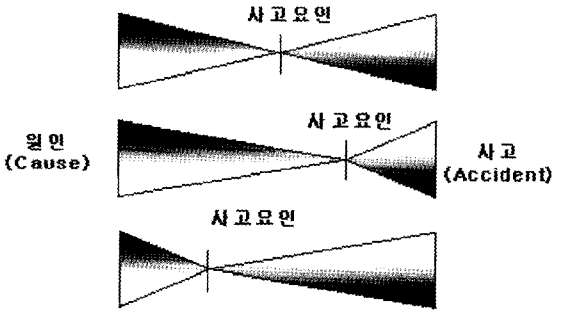
3.1.1 위험원규명

위험원의 규명은 안전성을 확보하는데 가장 기본적인 요소 중의 하나이다. 위험원이 없다면 위험원으로부터 기인되는 사고는 없다. 즉 위험원 도출에 실패한다면 위험원으로부터 기인되어 발생될 수 있는 사고를 방지할 수 없다.

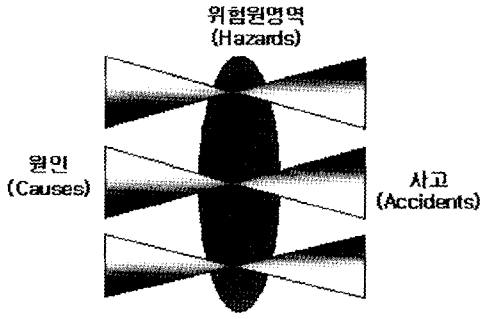
위험원의 규명은 다양한 방법으로 접근할 수 있다. 그 중 대표적인 방법들로는 "그렇다면 무엇이 나타나는가", 상호작용의 특별한 면을 가지고 관찰하는 "상호 매트릭스 방법", 시스템의부품 간의 상호작용을 관찰하는 "부분분석", "무엇"과 "어떻게"를 연관하여 "검사항목"을 제정하는 방법, 시스템의 기능고장과 고장의 영향을 분석하는 "FMEA" 및 부품과 부품간의 상호작용을 조사하고, 설계영역에서 벗어나는 것의 가능성을 조사하여 원인과 결과의 연관관계를 조사하는 " HAZOP : Hazard and Operability"의 방법이 있다.

위험원들에 대한 규정방법은 다양하다. 어떤 위험원들은 사고와 유사하고, 어떤 것은 근본 원인에 가깝다. 따라서 위험원의 위치는 시스템의 특성에 종속된다. 그림3은 위험원의 위치를 도식적으로 나타낸 것이다. 기존 위험원 목록에서 위험원들의 규정 수준에는 상당한 차이가 존재한다. 예를 들어 "한 구역에 동시에 두 대의 열차가 있다면" 이것은 사고에 상당히 근접해 있는 것이다. 반면에 "열차 운영자간의 인터페이스(상호접촉)의 부적절한 관리"는 사고의 근본 원인과 유사하다. 이러한 문제는 위험원들에 대한 규정을 어렵게 하는 원인으로서 이와 같은 문제를 피하기란 상당히 어렵다고 본다. 이것은 원인과 사고 사이에 존재하는 다양한 변수 때문이다. 주요 손실 사고는 원인에서 사고까지의 많은 단계와 관련되지만, 적은 손실은 단계가 매우 적기 때문이다.

위험도가 매우 높은 위험원(예, 동시에 한 구역에 두



〈그림 3〉 사고원인, 위험원 및 사고관계는 다양한 연결관계



〈그림 4〉 위험원 정의의 모호성

대의 열차)의 내부에는 해당하는 많은 하위 위험원들을 추가시킬 수 있다. 이러한 위험원의 추가는 부수적인 문제를 파생시킨다. 예를 들면, 두 대의 열차가 같은 역 플랫폼에서 마주치는 등의 절차 적용상에 문제점이 발생한다.

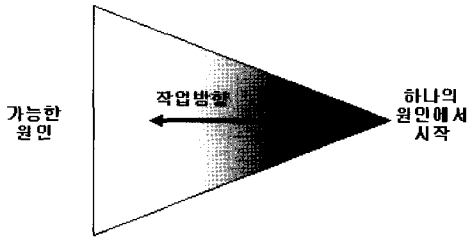
일부 위험원도출이 부족한 부분(Shortfall)은 기존 위험원목록 요소들의 규모에 비하여 상대적으로 광범위하고 모호한 성격을 포함하기 때문에 발생한다. 그림4는 이러한 문제점의 발생을 보인 것이다.

위험원을 광범위하게 정의하는 것은 위험도(위험) 모형에서 실질적인 사고 결과의 손실을 가져올 수 있으며, 모형화 과정에 상당히 주의하지 않으면 정확성과 이해부족의 결과를 초래한다. 특히 철도시설에 대한 부적절한 작업, 기본시설과 조화되지 않는 열차 이동 등의 위험원은 매우 포괄적으로 정의된다.

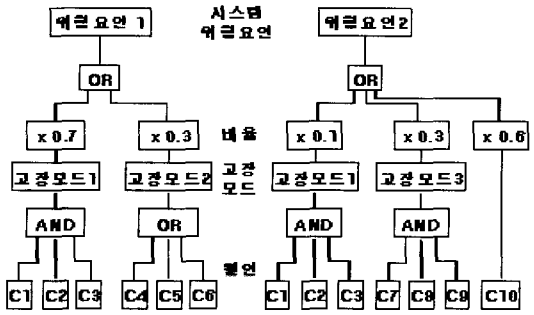
3.1.2 위험원분석

위험원 분석은 위험원 발생원인을 규명하는 것이다. 위험원 분석에 많이 쓰는 방법 중의 하나가 FTA(Fault Tree Analysis)이다. FTA는 부품고장에서 서브시스템의 조합, 하위단계의 사건 및 각각의 원인측면에서 최상위 위험원을 분석하는 방법이다. 이 분석방법은 나무구조를 생성하기 위해서 "and" 및 "or" 게이트를 이용해서 최상위 고장원인을 아래로 분석해 가는 방법으로 구성되어 있다. "and"는 게이트에 연결된 모든 원인의 조합결과로서 발생되는 결과에 사용되며, "or"는 원인 중에 하나라도 발생하면 결과로 될 때 사용된다. FTA는 고장에서 역방향으로 작업을 수행하여 원인을 규명하는 것이 되기 때문에 각각의 최상위 위험원에 대해서 생성되는 나무구조를 산출하는 연역적 방법이다. FTA 방법을 그림5에서 보여주고 있다.

위험원의 원인인 여러 종류의 고장은 위험원에 연결되어, 고장모드에 따라서 발생확률을 할당한다. FTA



〈그림 5〉 원인에서 결과로 진행하는 작업



〈그림 6〉 FTA를 이용한 위험원도출 및 확률할당

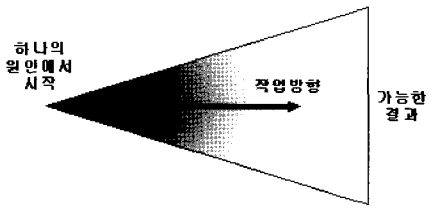
를 사용한 분석 예를 그림6에서 나타낸다.

FTA 방법은 시스템에 따라서는 대단히 복잡하거나, 부분적으로는 논리를 따라도 전체적인 구조가 보이지 않는 경우도 있다. 그림6에서는 고장검지의 나무와 같이 시스템 위험원을 발생시키는 고장모드에서 시작되어 최종적으로 부품 혹은 그 고장 모드에 이르는 과정을 모델화하였다.

3.1.3 HAZOP(Hazard and Operability)

앞에서의 위험원 규명 및 분석방법은 위험원 규명과 분석을 각각 분리하여 수행하였다. 위험원 도출의 한 가지 방법인 HAZOP은 설계목적에 관한 결함(Fault)으

〈그림 7〉 원인에서 결과로 진행하는 작업



〈그림 8〉 원인에서 결과로 진행하는 작업

로부터 시작을 하며, 가능한 원인을 찾기 위해 역방향으로 작업을 진행하고 결과를 알기 위해 순방향으로 작업을 진행한다.

실제에 있어서 어느 방법도 완벽한 위험원을 규명할 수 없으며, 실제적으로는 위에서 제시된 방법을 조합하여 사용하는 것이 최선의 방법이다. HAZOP과 FMEA는 서로 다른 측면에서 검토하므로 상호보완적이다. 또한 FTA(Fault Tree Analysis)와 ETA(Event Tree Analysis)는 상위단계에서 규명된 위험원을 분석하는데 상호보완적이다.

3.2 위험원의 결과

위험원에서 기인된 사고의 결과를 분석하기 위해 FMEA(Fault Mode Effect Analysis)를 사용한다. FMEA는 고장모드와 그 영향으로 인식되기도 하지만, 실제로는 결함모드와 그 결함의 영향을 검토하여야 한다. 따라서 결함형태가 시스템에 미치는 영향을 검토한다. 이 방법은 추론적인 방법이며, 그림7은 FMEA의 개념을 나타낸 것이다.

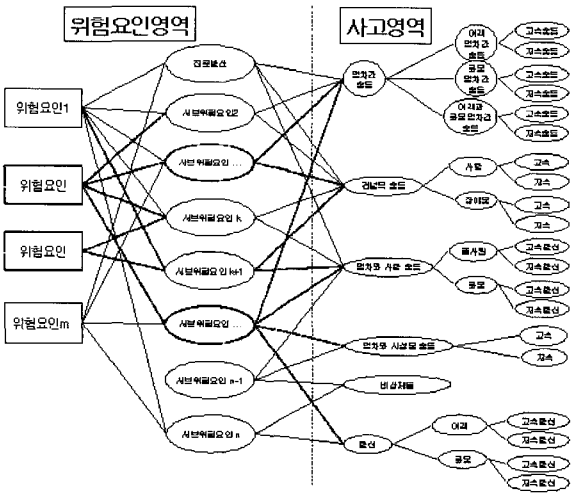
그림7에서는 하나의 원인에 의해 하나 혹은 다단계의 시퀀스를 거쳐서 사고로 발전되게 된다. 결과분석 방법으로는 여러 가지 방법이 제시될 수 있다. 그림8에서는 위험원으로부터 사고결과까지 이르는 사고 시나리오를 소개한다. 이 시나리오에서는 위험원이 다양한 서브 위험원으로 진행될 수 있으며 궁극적으로는 사고로 이어질 수 있다. 따라서 사고 시나리오의 분석을 위해서 FMEA, FMECA 및 ETA를 사용한다

FMEA(Fault mode and effects analysis)는 결함율이 높은 결함모드를 설계변경에 의해 사전에 제거하는 방법이다. 따라서 이러한 목적을 달성하기 위해서는 시스템이나 기기가 내장하는 결함모드를 전부 열거하고, 열거된 각각의 결함모드에 의한 고장이 발생한 경우에 시스템이나 기기에 어떠한 영향을 미치는가를 해석하고, 고장이 발생하는 원인, 고장이 시스템이나 기기, 운전자 등 인간에 미치는 영향과 결함 검출법 등을 검토하고 그 결과 안전성을 해칠 가능성이 큰 결함모드를 설계단계에서 제거한다.

3.3 손실분석

철도에서의 손실분석은 승객, 승무원, 철도원 및 공중을 대상으로 하여 추정을 수행한다. 사람의 손실분석은 사망, 장애, 부상 등으로 나누어지며, 사망은 인원수로 정의되고, 장애는 치료 후 평생동안 장애를 가지고가는 경우로 정의된다. 인사사고는 형사적인 책임이 있지만, 궁극적으로는 비용으로 산정될 수 있다.

"위험도" 는 다음과 같이 정의할 수 있다. 위험도(Risk)는 특정한 위험원에 관해서 피해가 발생하는 빈



〈그림 9〉 위험원→하부위험원→사고결과로 이어지는 그래프 형식의 사고추론 맵의 구성

도와 그 피해가 크기를 나타내는 지표이며, 다음과 같이 정량적으로 표기가 가능하다.

· 위험도(Risk)= (발생확률) × (사고의 결과)

위험도 평가 단위는 산업분야에서 여러 해 동안에 사용되어 왔으며, 미 육군에서는 중요도에 따라 각기 다른 위험도를 정하여 사용하고 있다. 위험도는 우선권이 설정되어 제어대책에 적용되고 있다. 위험도를 정량적으로 정의하는 것이 부적절한 경우는 다음과 같이 위험도의 레벨을 결정하여 적용한다. 따라서 발생확률과 결과의 개연성은 정성 및 정량적 값으로 분류될 수 있다.

예를 들어서 확률은 다음과 같이 정성적인 값으로 분류할 수 있다.

〈표 1〉 발생빈도의 분류

· 자주(Frequent)	$f \rangle 10^{-1}$	빈번하게 발생되는 것
· 종종(Probable)	$10^{-1} \rangle f \rangle 10^{-2}$	일생운용동안 여러 회 발생되는 것
· 가끔(Occasional)	$10^{-2} \rangle f \rangle 10^{-3}$	일생운용동안에 가끔 발생할 수 있는 것
· 거의(Remote)	$10^{-3} \rangle f \rangle 10^{-6}$	일생운용동안에 가끔 발생할 가능성이 있는 것
· 없음(Improbable)	$f \rangle 10^{-6}$	발생할 가능성이 전혀 없는 것

10^{-1}은 10,000 작동에 1번을 의미한다.

〈표 2〉 사고결과의 크기

· 치명 (Catastrophic)	$\cos t \rangle 2 \times 10^{6}$ USD	생명의 위험, 시스템 손실 : 다수의 사망 혹은 다수의 심각한 부상)
· 심각 (Critical)	$10^{6} \rangle \cos t \rangle 10^{5}$ USD	심각한 상처, 병, 큰 시스템 손상 : 1인 사망, 1인의 심각한 부상
· 상당 (Marginal)	$10^{5} \rangle \cos t \rangle 10^{4}$ USD	가벼운 부상 혹은 병, 작은 시스템 손상 : 손상을 일으킬 수 있는 가능성의 내포
· 무시 (Negligible)	$\cos t \rangle 10^{3} \rangle$ USD	가벼운 부상 · 병, 시스템 손상에 이르지 않는 것

사고의 결과는 다음과 정성적인 항목으로 분류할 수 있다.

확률과 사고결과의 정성적 확률평가를 이용한 것이 표2에 나타나 있다.

〈표 3〉 위험도 분류의 설정 예

	치명적	심각	상당	무시가능
빈번	1	3	7	13
종종	2	5	9	16
가끔	4	6	11	18
거의	8	10	14	19
없음	12	15	17	20

표3에서 숫자는 위험의 순서를 나타내며, 미 육군규격(System Safety Program Requirement)에서 유래한 것이다. 이 숫자는 위험평가 코드로 알려져 있으며, 각 항목에 대한 중요도를 나타내며, 제어의 필요성을 나타낸다.

① 위험평가코드 1 ~ 5 : 수용불가-위험도를 반드시 저감해야함

② 위험평가코드 6 ~ 9 : 부적정-모든 가능한 제어수단을 사용해야하며, 잠재위험도에 대한 문서화된 허용안을 가지고 있어야 한다.

③ 위험평가코드 10 ~ 17 : 조건부가-잠재위험도에 대한 문서화된 허용 안을 가지고 승인됨

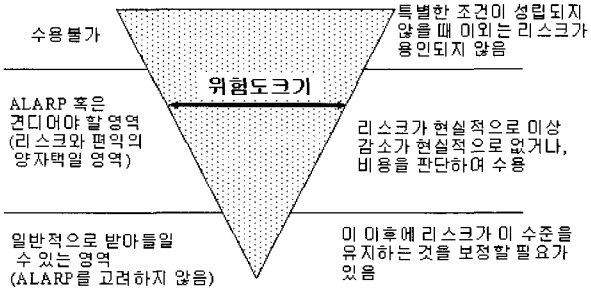
④ 위험평가코드 18 ~ 20 : 허용가능

〈표4〉 정량적인 위험도 예

빈 도	사건결과			
	치명적	심각	상당	무시가능
100~999 / 10000 년인원	1	3	7	13
10~99 / 10000 년인원	2	5	9	16
1.0~9.9 / 10000 년인원	4	6	11	18
0.10~0.99/10000 년인원	8	10	14	19
0.010~0.099/10000년인원	12	15	17	20

3.4 안전성확보영역

안전성의 확보여부를 결정하는 크기는, 주관적, 상대적으로 정의된다. 이것을 결정하기 위한 하나의 사고방식으로서, ALARP(As Low As Reasonably Practicable :실제 적용할 수 있을 정도로 위험이 작음)모델이 있



〈그림 10〉 ALARP 모델

다. ALARP 모델은 그림10에서 나타내는 것처럼 작은 위험도라면 허용 가능, 큰 위험도는 허용불가, 그 중간이라면, 편익과의 균형을 생각하여 설정한다라는 모델이다. 역삼각형은 감수해야 되는 위험도가 높은 위치(그림10의 위쪽)에 있어, 위험도를 그것 이상 감소해야 하는 비용도 커지는(그림10의 위쪽에서의, 삼각형의 가로방향의 넓어지기) 현상을 나타내고 있다.

일반적으로 안전은, 숫자로는 표시할 수 없는 것이라고 되어 있다. 또는 어느 정도의 레벨 이하라는 사고방식은 허용할 수 있다고 해도, 비용과 성능을 생각하고, 비용과의 균형으로 안전을 생각한다라는 것은 일반적이지 않다. 이것은 안전을 희생으로 해서 비용을 삭감하는 경향을 엄하게 제한하기 위한 것이며, ALARP에서도 이것을 고려하여 각 영역에 있어서의 기준으로서 다음과 같은 정의를 사용하였다.

· 허용불가영역

"대단히 특별한 조건이 성립된 경우를 제외하면, 이 위험도는 용인하지 않는다"

· ALARP영역

"위험도가 제한영역 이상으로 감소되는 상황을 제외하고, 비용이 너무 든다고 판단되었을 때 받아들인다"

· 허용되는 영역

"이후에도 위험도가 제시된 수준을 유지함을 보증해 갈 필요가 있음"을 엄격히 적용한다.

따라서 안전성의 구분은 허용불가영역, 위험을 다스린 영역, 및 위험이 존재하지 않는 영역 3단계로 나눈다. 안전이 확보되었다는 이야기는 허용되는 영역이나 제어가능단계(ALARP)에서는 안전성이 확보되었다고 할 수 있다.

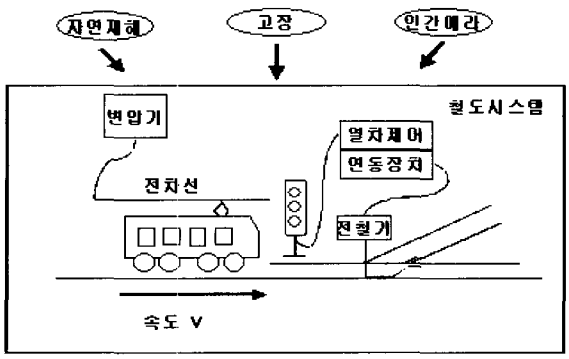
안전의 정도라는 것은, ALARP 모델의 부분에서 기술했듯이, 비용과 편익과의 관계로 변한다. 즉, 안전의 정의는 상대적이며 주관적인 것이다. 그러므로, 안전평가는 사회적인 허용범위 혹은 사회적 위험도와 밀접한 관계를 갖는다.

〈표 5〉 안전성확보를 위한 방안과 실현예

안전성 차량 신호	차량정상	차량비정상
신호 정상		· 기관사가 신호를 무시하고 위험신호를 통과하는 경우가 있다. · 차량의 제동장치가 작동 불능인 경우가 있다.
신호 비정상	· 신호기가 덜 제한적인 신호를 현시하여 위험신호시에 열차가 통과 하는 경우가 있다.	· 여러 가지의 경우가 발생
	· 미확보된 진로를 열차가 진입하는 경우가 있다.	
궤도 비정상	· 궤도선형 틀림이 큰 경우	
전철 비정상	· 접지시스템이 불완전한 경우	

4. 안전성 기술

철도분야 안전성기술의 가장 기본은 사고를 방지하기 위해서는 무조건 정지를 한다는 것이다. 따라서 이러한 안전성기술은 다음 표와 같은 수단에 의해서 구현되고 있다.



〈그림 11〉 간략화된 철도시스템

철도이외의 분야에서는 각각 독특한 안전성기술이 확립되어 있다. 따라서 시스템의 역할에 따라서 "안전한 상태"가 각각 틀리기 때문에 사용되는 안전성기술도 약간의 차이가 있다. 하지만 안전성기술의 기본기술은 몇 가지 종류로 집약할 수 있다.

5. 철도분야의 적용예

5.1 철도시스템

위에서 언급한 것과 같이, 철도에서 안전성 확보를 위한 예를 다음과 같이 제시하였다. 철도 시스템의 구성은 그림 와 같이 선로, 열차, 신호 및 급전 시스템으로 이루어져 있다. 열차가 주행을 하면서 발생될 수 있는 사고는 탈선, 충 · 추돌, 화재, 추락 및 감전 등의 사고가 발생하여 왔다.

그림11은 간략화된 철도시스템을 나타낸 것이며 그림에서 열차는 궤도 위를 주행 하고, 신호기는 열차의 주행을 허가하며, 연동장치는 진로를 설정함으로서 진로를 허가하고, 변압기는 전차선에 전력을 공급한다.

5.2 위험원 규명, 분석 및 평가

그림 11에서 나타나는 위험원을 규명하기 위해서 시스템(부품)과 시스템(부품)간의 상호작용을 조사하고, 설계영역에서 벗어나는 상태가 존재하는지를 조사하였으며, 원인과 결과의 연관관계를 조사하는 HAZOP의 방법을 활용하였다.

그림 11에서 표현된 시스템에 대하여 비정상적인 작동에 의한 사고를 발생시킬 수 있는 위험원을 도출 할 수 있다.

〈표 6〉 Hazop이용한 위험원 도출방법

차량 신호	차량정상	차량비정상
신호 정상		· 기관사가 신호를 무시하고 위험 신호를 통과하는 경우 · 차량의 제동장치가 작동 불능인 경우가 있다
신호 비정상	· 신호기가 덜 제한적인 신호를 현시하여 위험 신호 시에 열차가 통과하는 경우가 · 미확보된 진로를 열차가 진입하는 경우가 있다.	· 여러 가지의 경우가 발생
궤도 비정상	· 궤도선형 틀림이 큰 경우 · 궤도 게이지가 비정상인 경우	
전철 비정상	· 접지시스템이 불완전한 경우	

HAZOP의 활동은 각 시스템이 비정상적으로 동작을 할 경우에 따른 것을 고려하여 위험원을 도출하였다. 위의 활동에 의해서 도출된 위험원 다음과 같다.

① 기관사가 위험신호를 무시하고 통과
② 차량의 적절한 제동력 상실
③ 덜 제한적인 신호현시
④ 미확보된 진로의 진입
⑤ 궤도틀림
⑥ 궤간틀림
⑦ 접지시스템 불량

〈표 7〉 위험원 도출 및 분석, 위험평가 예

번호	위험원	원인	잠재적 결과	피해	발생확률및 피해크기
1	기관사가 위험 신호를 무시하고 통과	기관사 실수 신호기 시야불량	· 충추돌 · 비상제동	· 승객 · 종사원 · 차량파손	1
2	차량의 적절한 제동력상실	제동장치고장	· 충돌	· 승객	4
3	덜 제한적인 신호현시	입력 값 고장	· 충추돌 · 탈선	· 승객	5
4	미확보된 진로진입	신호기 고장	· 충추돌	· 승객 · 종사원	2
5	궤도틀림	유지보수 불량	· 탈선	· 승객	3
6	궤간틀림	유지보수 불량	· 탈선	· 승객	2
7	접지시스템불량	자연열화	· 감전	· 종사원 · 공중	4

HAZOP활동에 의해서 도출된 위험원을 근거로 위험원을 발생시키는 원인과 그 위험원으로 기인되는 사고를 도출하여야 한다. 표7은 간략하게 나타낸 위험원분석이다. 발생확률의 설정은 이제까지의 사고기록을 조사하여 확률을 계산하며, 피해의 크기는 사망 혹은 부상의 정도에 따라서 할당을 한다. 발생자료가 없다면 시뮬레이션 등을 통하여 발생확률과 피해를 추정할 수 있다. 발생확률 및 피해크기는 앞 절의 손실분석에서 수행한 것에 따라서 임의로 할당을 하였다.

〈표 8〉 위험원과 위험원에 대한 대책

번호	위험원	원인	저감안			안전성 검증
			방법	발생 확률	위험측 고장율 요구사양	
1	기관사가 위험 신호를 무시하고	기관사 실수 신호기 시야 통과불량	열차자동 정지장치의 채용	10^{3} /h	10^{6} /h	가속수명시험
2	차량의 적절한 제동력 상실	제동장치 고장	제동장치의 다중화채용 및 제동력의 증대	10^{3} /h	10^{6} /h	
3	덜 제한적인 신호현시	입력 값 고장	이중화 채용	-	10^{9} /h	
4	미확보된 진로진입	신호기 고장	이중화 채용	-	10^{9} /h	
5	궤도틀림	유지보수 불량차량	자동계측 도입	10^{3} /h	10^{6} /h	
6	궤간틀림	유지보수 불량차량	자동계측 도입	10^{3} /h	10^{6} /h	
7	접지시스템불량	자연열화	공통접지	10^{3} /h	10^{6} /h	

5.3 안전성확보방안

표7의 모든 위험원은 수용불가의 형태로서 반드시 대책을 세워 위험도를 저감하여야 한다. 표8은 위험원이 사고로 전이되는 것을 방지하도록 하는 대안이 될 수 있다.

6. 결 론

본 논문은 철도신호시스템에서 발생할 수 있는 사고의 원인인 위험원에 대하여 정의하고, 위험원이 사고로 이어지는 과정을 개념적으로 정리하였으며, 시스템에 포함된 위험원을 최소화 또는 차단시켜 사고를 방지하기 위한 방안을 안전성확보방안으로 제시하였다.

앞에서 제시된 안전성확보방안은 위험원의 규명 및 분석을 수행하여 위험원으로부터 발생할 수 있는 사고를 추측하고, 발생된 손실을 산출할 수 있는 절차를 제시하였으며, 이러한 활동을 체계적으로 제안하였다.

향후에는 제시된 안전확보방안을 수행하기 위한 세부수행절차 및 시스템분석기법에 대한 연구가 수행되어야 한다.

참고문헌

[1] 荻原春生, 岸 政七, ニュ・テック◎シリ・ズ 信號理論入門 -情報通信の基礎- 朝倉書店, 2000.

[2] 久保田 博, 鐵道重大事故の歴史, グランプリ出版, 2000.

[3] 坂下榮二, 世界の安全規格・認・便覽, 日本規格協會, 1996.

[4] 菅野文友, 信賴性工學, 電子情報通信學會大學シリ・ズJ-3, コロナ社, 1980.

[5] 江崎 昭, 輸送の安全からめた鐵道史, グランプリ出版, 1998.

[6] 菱沼好章, 信號保安・鐵道通信入門, 鐵道業務セミナ・No. 2, 中央書院, 1991.

[7] 吉村 寛, 吉越三郎, 信號, 交友社, 1991.
[8] 運輸省鐵道局 監修, 數字でみる鐵道2000, 財團法人 運輸政策研究機構, 2000.
[9] 鐵道總合技術研究所, 列車保安制御 システムの 安全性技術指針, 1996
[10] CENELEC Standard EN 50126, EN 50128, ENV 50129, 1997.
[11] IEC 61508-1 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems Part 1: General Requirements, IEC, 1998.
[12] IEC 61508-2 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC, 2000.