철도 안전 설비의 정량적 위험평가 기술

최 권 희* · 김 유 호* · 이 종 우** · 송 중 호** · 송 광 열***
*(주)에이알텍 기술연구소 · **서울과학기술대학교 철도전문대학원
***한국철도시설공단 신호제어처

Technical Review on the QRA of Railway Safety Facilities

Kwon-Hee Choi* · You-Ho Kim* · Jong-Woo Lee** · Joong-Ho Song** · Kwang-Yeol Song***
*R/D division, ARTech Co., Ltd
**Graduate School of Railroad, Seoul National University of Science and Technology
***Signaling and Control Division, Korea Rail Network Authority

Abstract

The overall goal of a safety based railroad system is either to eliminate hazards in designing or to minimize the possibility of it. In order to indicate system safety or low risk although it may not be possible to achieve zero risk conditions, first, it shall ensure that any disasters would occur due to system operation because the prescribed specifications are properly fulfilled and there are no failures of any kind. Second, the risk of faults or failures leading to a mishap must be eliminated or minimized by using fault-tolerance or fail-safe procedures. This paper will attempt to summarize the personal and social risk criterion at widely scattered points, presently used as a safety approach in all over EU, in order to establish the step by step procedures of the detailed standard for railway facilities. In addition, we present the new safety analysis method using the SIL-based evaluation standard and the Reachability Graph of the Petri Net.

Keywords : risk acceptance criteria, individual risk, societal risk, ALARP, ALARA, QRA, Petri Net

1. 서 론

최근 국토해양부는 철도시설에 대한 안전성 설계와 평상시 유지보수 목적으로 제정(2005.10.27)된 『철도시설 안전기준에 관한규칙』을 전면개정(2011.6.7)하였다[1].

철도시설의 안전성 분석은 기존 철도사고사례 자료를 통하여 개인적 위험기준과 사회적 위험기준에 따라 정량적 위험도 분석 방법으로 수행하게 된다. 이를 위하여 철도시설에 대한 잠재적인 위험 원인, 가능한 시나리오, 사건발생 가능성, 사고영향, 사고발생확률, 피해정도 등을 세부적으로 분석하여야 한다.

철도시스템에서 안전우선 시스템을 설계하고 평가하는 전반적 목표는 위험요소를 제거하거나, 그것이 불가능하다면 위험요소의 발생 확률이 매우 낮도록 설계하여 시스템의 위험성을 최소화 시키는 것이다.

위험도 제로(Zero risk)를 달성하기는 어렵지만, 시스템 안전성 또는 저위험성을 표시하기 위해서는 첫째, 규정된 사양이 올바르게 실행되고 있고, 동작하는 시스템으로 인해 어떠한 재난도 발생하지 않는다는 것을 보장해야 한다. 둘째, 고장의 위험성으로 인해 재난으로 진행되는 고장을 제거하거나 또는 고장안전, 결함허용 등과 같은 절차를 이용하여 이를 최소화 시켜야 한다. 위험발생 가능성을 완전히 제거할 수 없는 경우에는 위험조건으로의 노출시간을 최소화하여 위험성을 줄여야 한다.

✝ 본 연구는 철도건설 경쟁력 확보를 위한 제반연구(안전설비분야) 용역과제에 의해 이루어진 논문임.
✝ 교신저자: 최권희, 서울시 금천구 가산동 50-3 대륭포스트타워6차 909호
M · P: 010-2290-8089, E-mail: triple333@paran.com
2011년 7월 20일 접수; 2011년 9월 20일 수정본 접수; 2011년 9월 21일 게재확정

따라서 본 논문은 철도시설 안전세부기준의 단계별 절차를 수행하기 위해 최근 EU에서 활동하고 있는 정량적 위험도 수행기준인 개인적 위험수준과 사회적 위험수준을 폭넓게 요약하였다. 또한 기능안전규격(IEC 61508)에 기반한 안전고장비율(SFF)과 진단유효범위(DC)를 살펴보고 안전무결성레벨(SIL) 평가기준과의 관계를 살펴보고자 한다. 끝으로 복잡한 시스템에 대해 전반적 도달가능성 집합을 만들지 않고서도 안전성을 분석하는 역방향 도달성 그래프 접근법을 제시한다.

2. 법적 기준 및 현안 문제점

2.1 철도시설 안전기준에 관한 규칙

최근 국토해양부는 철도시설에 대한 안전성 설계와 평상시 유지보수 목적으로 제정된『철도시설 안전기준에 관한 규칙』을 개정하였고, 제12조(선로의 안전설비)에 대한 세부 사항은 “국토해양부장관이 정하여 2011년 8월 3일에 『철도시설 안전세부기준』이 공시되었다[2]. 따라서 개정된『철도시설 안전세부기준』에 따라 연구를 진행하였다.

2.2 고속철도 안전설비의 분류

철도시설 안전기준에 관한 규칙 제32조(선로의 안전시설)에는 다음과 같이 안전설비를 분류한다[2].

① 주행하는 열차의 차축 온도를 일정거리마다 측정하여 차축의 과열로 인한 탈선사고를 사전에 예방하기 위한 차축온도검지장치.
② 철도를 횡단하는 고가차도나 낙석 또는 토사붕괴가 우려되는 지역에 자동차나 낙석 등이 선로에 침입하는 것을 검지하는 지장물검지장치.
③ 철도차량 차체의 하부 부속품이 철도차량에서 이탈되어 매달린 상태로 주행하는 경우 이로 인하여 궤도 사이에 부설된 신호시설물이 파손되는 것을 방지하기 위한 끌림검지장치.
④ 지진이 발생한 경우 지진규모에 따라 선로에 미치는 최대 지반가속도 값에 따라 열차를 감속 운행하거나 운행을 중지시킬 수 있는 지진감시시스템.
⑤ 폭우·강풍·폭설 등 기상상태를 검지하여 기상이 악화된 경우에 열차를 감속운행하거나 운행을 중지시킬 수 있는 기상설비.
⑥ 제설작업이 곤란한 지역에서 선로전환기를 작동할 수 있도록 눈을 녹여주는 융설(融雪)장치.
⑦ 철도시설보수자가 지정된 장소에서 선로를 횡단하고자 하는 경우 당해 장소에 열차가 접근하는지의 여부를 확인하여 주는 열차접근확인장치.
⑧ 본선터널 안에서 작업하는 보수자 또는 순회자의 안전을 위하여 본선터널 안으로 접근하는 열차가 있는지의 여부를 알려주는 본선터널경보장치.
⑨ 레일 온도 상승으로 인한 레일 장출 위험을 예방하기 위한 레일온도검지장치.

그러나 철도시설 안전세부기준에는 안전성 분석을 수행하기 위한 세부적인 수행방안이 제시되어 있지 않아 정량적 위험성 평가를 수행하는 데 어려움이 있다.

3. 정량적 위험성 평가

3.1 QRA 정의

QRA(Quantitative risk assessment)란 위험의 상대적인 크기를 파악하기 위한 방법으로 위험크기를 정량화시켜 개인적, 사회적 위험기준과 비교하여 주요시설물의 안전성을 평가하는 방법이다. 이러한 정량화된 위험의 크기를 사회적 위험기준과 비교하여 철도시설의 적정성을 평가할 수 있으며, 위험의 크기는 다음과 같이 정량화 할 수 있다[3].

위험(Risk)=사고발생확률(Frequency)×손실(Fatalities)

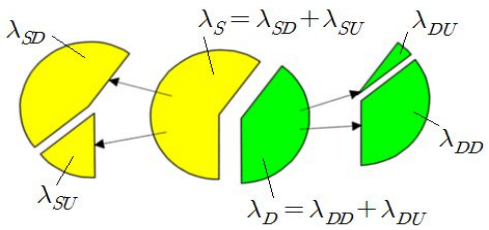
정량적 위험분석은 사고발생확률과 사망자의 관계를 확률-사망자 곡선(Frequency number of fatalities- curve, FN-curve)으로 그림 4와 같이 표현할 수 있다. 곡선을 나타내는 평면은 안전성에 대한 수용여부 및 안전성 향상을 위한 추가적인 조치여부를 판단할 수 있는 영역 또는 기타 유사한 방법의 영역으로 구분되며 확률-사망자 곡선이 위치하는 영역의 기준에 의해 위험을 평가한다.

정성적(Qualitative) 또는 정량적(Quantitative) 위험성 분석에 사용하는 위험 수준을 규정하는 기본 원칙에는 2가지가 있다[4][5]. 즉 ‘합리적으로 가능한 낮은(As low as reasonably possible, ALARP) 수준’ 그리고 ‘합리적으로 달성 가능한 낮은(As low as reasonably achievable, ALARA) 수준’이다. ‘낮은(Low)’, ‘합리적(Reasonably)’, ‘가능한(Possible)’ 그리고 ‘달성 가능한(Attainable)’과 같은 용어의 정의는 극도로 주관적이고, 보수적인 의미로 해석되기 쉽다. 따라서 정량적 위험성의 관점에서 이들 기준을 좀 더 명백한 한계로 정의하는 공학적인 방법과 모델이 필요하다.

3.2 안전고장비율 및 진단유효범위

정량적 위험성 평가를 위해서는 IEC 61508에서 권고하는 안전고장비율(Safe Failure Fraction, SFF)과 진단유효범위(Diagnostic Coverage, DC)를 안전무결성레벨(SIL) 평가기준과의 관계를 정의하여야 한다[3].

[그림 1]에 하부시스템의 고장률을 표시 하였다. 대부분의 시스템은 고장이 발생하면 안전측 고장(Safe failures, λ_S)과 불안전측 고장(Unsafe failures, λ_{SU})으로 구분되며, 각각에 대해 자기진단기능을 통해서 안전측 고장 검지가 가능한지(λ_{SD}), 불안전측 고장 검지가 가능한지(λ_{DD}) 그리고 안전 및 불안전 고장에 대해 검지가 불가능한지(λ_{SU}, λ_{DU})를 각각 포함한다. 여기서 우리는 시스템의 고장으로 인해 불안전측 고장을 검지하지 못하는 경우에 대해 주목하고자 한다.



[그림 1] 하부시스템의 고장률

과거 이 분야의 오랜 연구결과에 따르면, 대체로 하부시스템 고장률은 마이크로프로세서와 같은 계산요소 부품들은 15%, 센서류는 50% 그리고 액추레이터와 같은 최종 출력단에 연결되는 부품들은 35%의 통상적인 고장률을 가진다[6].

'진단유효범위(DC)'라는 말은 그 의미가 분명해 보인다. 즉, 모든 고장에 대해서 거의 100% 안전한 상태를 유지하면 진단유효범위가 높다는 것을 의미한다. 이와 같은 피상적 해석은 잘못된 것이며 이로 인해 시스템 개발 과정에서 난관에 부딪힐 수 있다.

<표 1> 안전고장비율(SFF)과 SIL과의 관계

안전고장비율(SFF)		하드웨어 고장허용(N)		
Type A	Type B	N=0	N=1	N=2
-	0 %…<60 %	-	SIL1	SIL2
0 %…<60 %	0 %…<60 %	SIL1	SIL2	SIL3
0 %…<60 %	90 %…<99 %	SIL2	SIL3	SIL4
≥90 %	≥99 %	SIL3	SIL4	SIL4

진단유효범위가 '높다'라는 구체적인 정량화 기준은 IEC 61508-2에 따라 진단유효범위는 <표 1>과 같이 안전무결성레벨(SIL)과 관련이 있다. 여기서 Type A는 간단한 하부시스템으로서 모든 부품의 잠재적 결함 및 고장이 완전하게 알려져 있는 경우를 말하며, Type B는 보다 복잡한 하부시스템으로서 잠재적 결함을 완전하게 알 수 없는 경우를 말한다. 또한 하드웨어 고장허용(N)은 각 안전기능에 결함이 발생 시, 계속적으로 필요 기능을 실행시키기 위한 하드웨어 장치 기능을 나타낸다.

'안전고장비율(SFF)'과 '진단유효범위(DC)'에 대한 정의는 식 (1)과 식 (2)와 같이 나타낼 수 있다[3].

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} \quad (1)$$

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} \quad (2)$$

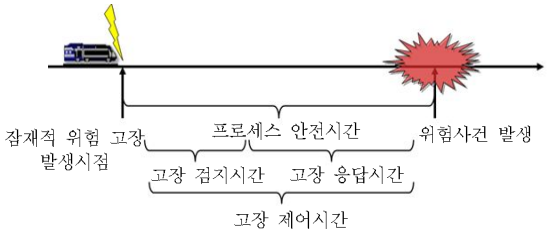
식 (1)과 식 (2)로부터 하부시스템의 위험한 고장, 위험 검지 및 안전고장비율 등과 같이 오류의 개수가 아니라 발생 확률을 고려해야 한다.

<표 1>을 개략적으로 보면 진단유효범위가 높을수록 SIL 수준이 더 높다고 생각할 수 있지만, 지나치게 자기진단기능에 의존하는 것은 바람직하지 않다. 결함 발생 확률이 높은 소수의 오류를 잘 처리하면 SFF가 확실히 1(또는 100%)에 근접해진다. 이러한 개념을 알고 나면 향후 '안전 부품' 개발 시 어디에 중점을 두어야 할 것인지 분명하게 파악할 수 있다. 즉, 오류 발생 개수를 기록하는 대신 오류 발생 확률을 정량화해야 한다. 결함의 대부분은 사람의 실수 때문에 발생한 오류를 비롯해 PCB 단락, 규정 범위를 벗어난 EMC 방출 및 공급 전압 변동 등과 같이 외부에서 비롯된 오류 때문에 발생하므로 반드시 검출하여 처리해야 한다.

3.3 프로세스 안전시간 및 응답시간

[그림 2]에 프로세스 안전시간과 응답시간을 표시 하였다. 프로세스 안전시간(Process safety time)이란 시스템이 가지고 있는 잠재적 위험고장 발생과 위험사건 발생 간의 경과시간을 말한다. 예를 들면, V [km/h]로 주행하고 있는 열차가 차축온도과열(Axle overheating)이라는 잠재적인 위험 요소로 인해 선로의 어느 시점에서 발생하였다고 가정한다. 열차에는 차축의 온도상승을 검지하는 수단이 없다고 할 때, 프로세스 안전시간이 경과하면 차축과열로 인해 열차탈선과 같은 심각

한 경지에 이르게 될 것이다. 이제, 차상 또는 지상에 차축온도를 검지하는 수단이 있다고 가정한다. 동일한 개념으로 잠재적 위험에 대한 고장정보를 검지시점과 고장에 대한 응답시간이 전체 고장 제어시간 범위를 초과한다면 위험사건으로 전개되는 것은 필연적이다. 따라서 프로세스 안전시간 내에서 초기의 잠재적 위험 크기를 검지하여 시간변화에 따라 위험의 크기가 증가하는지를 관측하는 것이 전체 프로세스 안전시간을 충분히 확보하는데 중요한 변수로 작용한다.



[그림 2] 프로세스 안전시간과 응답시간

4. 정량적 위험도 분석 수행기준

정량적 위험도 분석 수행기준은 엔지니어링 위험성의 기본 분류의 관점에서 영향을 받는 3가지 요소, 즉, 안전성(개인적 위험성 및 사회적 위험성), 경제성(잠재적 경제적 손실, 건설 스케줄) 및 환경에 기인하는 복합체적 속성을 가진다[7]. 또한 경제적 손실이나 시간지연과 같은 몇 가지 양적 지수뿐 아니라 잠재적 환경손상, 인간생활의 통화(通貨)가치 및 공적 영향 등과 같은 수량화되지 않은 수많은 지수를 기반으로 확립되어 있으므로, 위험성 수용기준의 확정은 복잡하고 어려운 논쟁적 작업이다. 위험성 분석수행기준은 개인적, 사회적, 경제적, 환경적 위험으로 분류되지만, 본 논문에서는 공중사상사고를 평가하는 개인적 위험기준과 사회적 위험기준에 대해서만 기술한다.

4.1 개인적 위험기준

철도시설 분야에서 개인적 위험(Individual risk)이란 철도 위험시설 주변에서 개인이 사상할 수 있는 확률로 나타낸 것을 말한다[8]. 또한 네덜란드 주택 공간계획 및 환경부(VROM)에서 정의한 바에 따르면 개인적 위험이란 어느 위치에 영구히 존재하는 보호받지 않은 평균 인원이 위험한 어느 행위로 인해 사고로 사망할 수 있는 확률이라 하며, 식 (3)으로 표현한다[7].

$$IR = P_f \cdot P_{df} \qquad (3)$$

여기서 P_f는 실패 확률이고,P_{df}는 영구히 보호받지 않는 개인이 존재한다고 가정한 상태에서 실패하는 경우에 어느 한 개인이 사망할 확률이다.

개인적 위험성은 매우 주관적이며 그 개인이 실제로 자발적인지 비자발적인지 여부와 관계없이 개인의 선입적 애호(先入的 愛好)에 따라 결정된다.

식 (3)의 정의에 따라 네덜란드 주택, 공간계획 및 환경부(VROM)는 개인적 위험도 기준을 매년 10^{-6}보다 낮은 위험성은 합리적으로 달성 가능한 한 낮은 수준(ALARA)으로 설정하고 있다. 또한 영국 위생안전 위원회 사무국(HSE)도 개인적 위험성 IRHSE의 정의를 통해서, 수용할 수 없는 지역, 허용 가능한 지역 그리고 폭넓게 수용할 수 있는 지역을 고려하여, 위험성의 허용 가능성을 $IR_{HSE} \leq 10^{-6}$으로 설정하고 있다[7][8].

그러나 허용 가능한 지역과 수용할 수 없는 지역 사이의 경계에는 작업자와 공공 양쪽에 널리 적용할 수 있는 어떠한 기준도 제공되지 않았다. 이 외에도 체코 공화국과 오스트리아의 개인적 위험목표 수준은 10^{-6}으로 규정되어 있다[8].

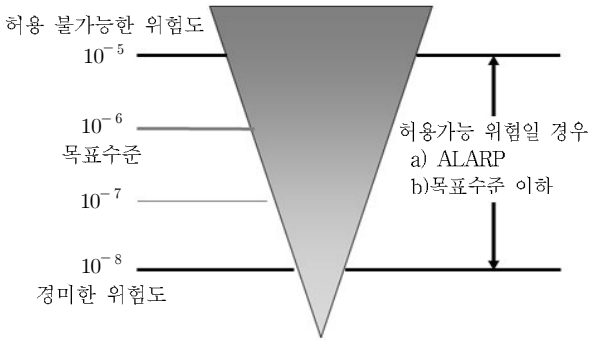
이들 자료에 근거하여 철도운영에 의해 개인이 연간 사상을 입을 확률과 관련된 위험도와 승객, 직원 그리고 공중(Public)과 관련한 모든 위험노출 그룹을 판별할 필요가 있다. 그러나 확인된 모든 노출 그룹의 개인 위험도에 대한 정량적 평가를 행하는 것은 실용성이 적다. 따라서 위험에 노출되어 있는 철도 종사자의 개인적 위험도 평가의 일례로서, 열차 운영회사에서 종사하는 승객과 열차운전자, 철도기반시설물을 관리하는 운영회사의 승객, 열차운전자, 선로주변 작업자, 철도건널목을 이용하는 일반직원 그리고 정거장 운영회사의 플랫폼, 승강구 직원 등을 고려할 수 있다.

만약 각 그룹의 개인 위험도가 허용되는 영역 내에 있다는 것을 보여줄 수 있으면 각 운영기관의 운영과정에서 노출된 모든 그룹에 대한 개인 위험도 역시 허용되는 영역 내에 있다고 할 수 있다. 영국의 경우 <표 2>와 같이 여객 위험도와 공중사상 위험도에 대한 개인적 위험도 범주를 제시하고 있다[8].

<표 2> 개인적 위험도 범주

그룹	허용 상한선	국가 안전계획	승인영역
여객 위험도 (일반 여행자)	1×10-4/year (년간 10,000명 중 하나)	133백만 여행객 중 하나 즉, 3.75×10-6/year (500 journeys/year)	1×10-6/year (100만명 중 하나)
여객 위험도 (여객 승무원)	1×10-3/year (년간 1,000명 중 하나	5×10-5/year (년간 20,000명 중 하나)	1×10-6/year (100만명 중 하나)
공중사상 위험도 (철도 주변)	1×10-4/year (년간 10,000명 중 하나	1×10-6/year (년간 100만명 중 하나)	1×10-6/year (100만명 중 하나)

국내 기준은 아직 정의되지 않았으나 조사된 문헌에 의해 승객과 열차운전자, 선로주변 작업자 및 공중에 대한 안전성 분석의 기준은 [그림 3]에 도시한 것처럼 개인적 위험기준을 10^{-6}으로 설정한다.



[그림 3] 개인적 위험 기준

4.2 사회적 위험기준

사회적 위험(Societal risk)이란 "규정된 위험을 인식함에 따라, 어느 주어진 모집단의 규정된 해악(害惡) 레벨로 인한, 고통을 받는 수많은 사람과 빈도(頻度)사이의 관계"라고 정의한다[9]. 개인적 위험도가 특정 위치에서의 사망 확률을 제공하는 경우, 사회적 위험도는 해악이 영역 내에서 정확하게 어떤 위치에서 발생하는지 여부에 관계없이 전체 영역에 대한 수치를 제공한다. 그리고 ALARP, 위험성 매트릭스, FN 곡선, PLL(생명의 잠재적 손실), FAR(치명적 사고발생 비율), VIIH(건강 장애 및 상해 값), ICAF(설비광고 함축 비용) 및 LQI(생명 특질 지수) 등과 같은 사회적 위험성이 제한된 많은 기준이 있다[7].

사회적 위험성은 Farmer F.R.(1967)[10]이 처음 사용했고, 당초에는 원자력 산업의 위험성을 평가할 목적으로 도입된 FN 곡선을 이용하여 그래픽으로 표현하는 경우가 적지 않았다. 이 유명한 곡선은 2중 대수 척도를 이용하여 발생초과 확률을 재난발생수의 함수로 식(4)와 같이 표시한다.

$$1-F_N(x)=P(N>x)=\int_x^{\infty} f_N(x)dx \qquad (4)$$

여기서 $f_N(x)$는 매년 재난 발생수의 확률 밀도 함수(PDF)이고, $F_N(x)$는 매년 재난 발생수의 누적 확률 분포 함수(CPDF)로서 매년 재난 발생수보다 작은 확률을 표시한다.

이와 같이 FN 곡선은 누적빈도와 사고로 인해 발생되는 예상 사망자수로 표현된다. 예를 들면, 어떠한 가상 사고에 의한 예상 사망자의 수는 위험지역 내의 인구밀도와 사망자확률의 곱을 면적으로 적분함으로써 계산할 수 있다. 영국에서 화재로 10명 이상의 사망자가 발생할 기회는 연간 1회이며, 철도 사고로 인해 100명 이상의 사망자 또는 심각한 상해가 발생할 기회는 15년에 1회 꼴로 나타난다[8].

몇몇 국가에서는 FN 곡선 기준선을 이용하여 다양한 위험 활동의 위험성을 제한한다. 이들 표준은 식(5)와 같이 표시할 수 있다[7].

$$1-F_N(x)<\frac{C}{x^n} \qquad (5)$$

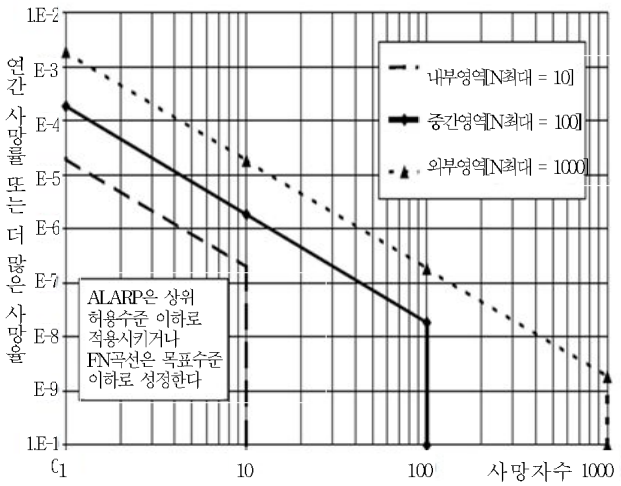
여기서 n은 제한선의 기울기이고 C는 그 제한 선의 위치를 결정하는 상수다. $n=1$인 표준을 중립 위험성이라고 부른다. $n=2$라면, 그 표준은 역(逆) 위험성이라고 한다. 일반적으로, 그 표준의 일부로, ALARA(또는 ALARP) 지역을 그 한계선 아래로 결정했는데, 여기서는 위험성을 합리적으로 달성 가능한 한 (또는 가능한 한) 낮은 수준으로 감소시킨다. <표 3>에는 FN 곡선을 제한시키는 몇몇 국제적 기준의 계수값을 수록하였다.

<표 3> FN 곡선을 제한시키는 국제적 기준

국가	n	C	위험 속성
영국(HSE)	1	0.01	중립 위험성
중국, 홍콩	1	0.001	중립 위험성
네덜란드(VROM)	2	0.001	역 위험성
덴마크	2	0.01	역 위험성

영국의 경우, "사회는 일반적으로 1명의 사망사고가 발생하는 10건의 사고보다 10명의 사망사고 한 건에 더 관심을 가진다(HSE 2004a)" 즉, 예방을 원칙으로 하고 있다. 사실상, 위험 회피가 포함되어 있는 위험 기준은 다수의 결과 사건에 대한 예방책이다. 다수의 결과 사건은 위험도 저감을 위해 편중적으로 더 많은 노력을 쏟아야 하는 다수의 불확실성과 반드시 관련되어야 한다(영국 위험허용도 정책의 불균형 원칙). 이는 결과적으로 제안된 위험 회피계수에 반영되어 있으며, 제시된 사회적 위험수준은 몇 가지 위험 영형을 기초로 한다. 예로서, 노출된 인구수가 제시되어 있는 내부영역(위험원에 가장 인접해 있음), 중간영역 그리고 외부 영역을 들 수 있으며, [그림 4]와 같이 영역을 나누어 표시할 수 있다.

사회적 위험수준을 표시하는 간단한 척도로서 생명의 잠재적 손실이라고 불리는 연간 재난 발생수의 예상 값으로 $E(N)$을 사용한다. 댐이나 해양 플랫폼의 위험성을 규제하는 경우, 그 기준은 $E(N)<10^{-3}$(재난/년) 및 $E(N)<10^{-2}$(재난/년)으로 제안하고 있다[11][12].



[그림 4] 사회적 위험기준 제안 일례

사회적 위험기준은 핵 반응로, 위험설비, 해양설비, 철도시설과 같은 잠재적 위험설비 등의 시설물 용도에 따라 다르며, 시설물의 위험도가 커질수록 엄격한 기준이 적용된다. 이 기준은 경제규모, 국민의식수준 등 여러 가지 여건에 따라 국가별로 상이하며, 우리나라의 경우 사회적 위험기준이 미정립된 상태이다. 따라서 조사된 문헌에 따라 사회적 위험기준을 [그림 4]에 도시한 기준 범위 내에서 설정하는 것이 바람직하다.

5. 안전성 분석

안전우선 시스템(Safety-critical system) 설계의 전반적 목표는 위험요소를 제거하거나 그것이 불가능하다면 위험요소의 발생 확률이 매우 낮도록 설계하여 위험성을 최소화 시키는 것이다. 시스템이 안전하다거나 또는 위험성이 낮다는 것을 나타내기 위해서는, 첫째, 규정된 사양이 올바르게 실행되고 있고 어떠한 고장도 발생하지 않으므로 시스템의 작동으로 인한 어떠한 재난도 발생하지 않을 것임을 보장해야 한다. 둘째, 고장의 위험성으로 인해 재난으로 진행되는 고장을 제거하거나 또는 고장안전, 결함허용과 같은 절차를 이용하여 이를 최소화 시켜야 한다. 위험발생 가능성을 완전히 제거할 수 없는 경우에는 위험조건에 대한 노출시간을 최소화하여 위험성을 줄여야 한다.

Petri Net의 도달가능성 그래프(Reachbility graph)를 이용하면, 트랜지션 점화(Transition firing) 시퀀스에 의해서 초기 상태로부터 그 시스템이 도달할 수 있는 가능한 모든 상태를 그래프로 식별할 수 있기 때문에 그 시스템 설계가 위험성이 높은 상태에 '도달'할 수 있는지 여부를 판단할 수 있다[13]. 그러나 복잡한 시스템은 그래프의 크기가 폭발적으로 증가하므로 도달성 그래프를 작성하는 것은 비현실적이다. 따라서 본 논문에서는 전반적 도달가능성 집합을 만들지 않고서도 안전성을 분석할 수 있는 방법을 기술한다.

안전성을 분석하는 한 가지 방법은 위험성이 높은 상태로부터 역(逆)방향으로 검토하여 위험성이 높은 상태에 도달할 수 있는지 여부를 결정하는 것이다. 이 접근법은 분석목표가 시스템이 어느 특정 고장상태에는 결코 도달할 수 없다는 것을 입증하는 경우에만 유용하다. 이 역방향 접근법은 위험성이 높은 상태의 수가 비교적 적은 것을 고려한 경우에만 충분히 실용적이라고 밝혀졌다.

위험성이 높은 상태에 도달할 수 있다면 초기상태로부터 위험성이 높은 상태에 이르는 경로에는 반드시 임계상태가 존재한다. 그렇지 않으면 모든 시간 Petri Net의 실행은 위험성이 높은 상태가 되기 때문에 설계를 완전히 다시 해야 한다. 위험성이 높은 상태에는 절대로 도달할 수 없도록 하기 위해서는 최초의 임계상태에서 역(逆)방향으로 전개하면서 위험한 경로를 취하지 않도록 설계하는 것이 최선책이다.

역방향 접근법에 의한 안전성 분석방법은 철도 건널목 시스템(Railroad Crossing System, RCS)을 예를 들어 설명한다. RCS는 경합 및 병행성과 같은 복잡한 요소를 갖고 있기 때문에 간단한 사례연구로써 널리 사용되어 왔다[13]. 철도 건널목 제어시스템은 열차가 도로와 선로(Railroad) 교차로에 접근하거나 출발할 때 차단기의 상·하 방향의 움직임을 감시한다. RCS는 1) 차단기, 2) 경고 시스템, 3) 교통 흐름과 점멸등 신호를 감시하는 능동적 교통 제어 시스템, 4) 접근하는 열차를 감지하는 센서 시스템으로 구성된다. 여기서, RCS는 단선을 사용한다고 가정한다.

앞서 언급한 RCS 요소를 기반으로 Petri Net를 구성함으로써 기능적 모델을 생성할 수 있다. 위 조건을 충족하는 Petri Net 모델을 [그림 5]에 나타낸다. 이 Petri Net과 초기 마킹 M_0를 사용하여 RCS 동작 분석 시 사용할 수 있는 도달성 트리를 [그림 6]과 같이 구축한다. 이 트리는 순방향 도달성 분석 방법을 사용하여 해석할 수 있다. 이를 위해, 활성화된 트랜지션 점화에서 도달할 수 있는 초기 마킹과 발생 가능한 모든 마킹들로 트리를 구성한다. 도달성 트리에서 각 가지의 마지막 마킹은 이미 트리에 나타난 것과 동일하다.

다음 고장분석을 수행하기 위해 결함트리분석(FTA)을 사용한다. 이를 위해서는 아주 엄격한 결과 위주로 위험원을 확인한다. 위험도가 일어날 확률은 모든 확인된 위험도들과 동일하다고 가정한다. 여기에서는 시스템이 단순하기 때문에 FTA에 대한 별도의 트리는 나타내지 않았다.

마지막으로, 역방향 도달성 분석 및 최종 마킹 또는 위험원 상태(Hazardous state)로써 식별된 위험원을 사용하여 FT-PN을 분석한다. Petri Net과 대응하는 역방향 도달성 트리를 [그림 7]에 나타내었다. 역방향 도달성 트리는 M1=<1,0,0,1,0>과 M2=<0,1,0,1,0>인 두 개의 초기 마킹을 위험으로 식별한다. 마킹 M1은 열차가 접근하고 있는 데 차단기가 내려져 있지 않은 상태를 나타내며, 마킹 M2는 열차가 접근하고 있는 데 신호등이 녹색이 아닌 상태를 나타낸다.

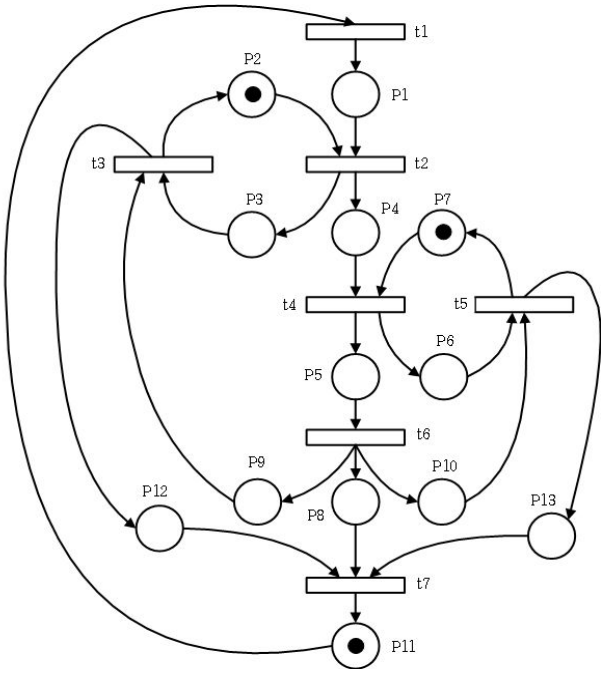
그러므로 Pertri Net 모델에서는 이들 위험원을 인식한 후, 플레이스 P_1과 P_4 또는 플레이스 P_2와 P_4가 동시에 토큰을 소유하지 않도록 인터록 회로를 구성하여 안전성을 확보할 수 있다.

플레이스

P1 =	열차 접근	P8 =	열차 건널목 통과
P2 =	차단기 하강 준비	P9 =	차단기 신호수신
P3 =	차단기 상승 준비	P10 =	신호등 신호수신
P4 =	신호등 변경	P11 =	종료
P5 =	건널목 내 열차 진입	P12 =	차단기 상승
P6 =	적색 신호등 준비	P13 =	신호등 재 변경
P7 =	녹색 신호등 준비		

트랜지션

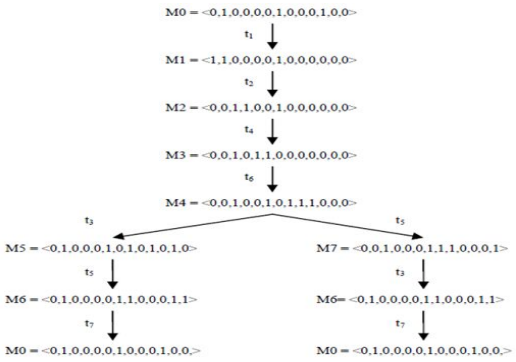
t1 =	열차 접근 검지	t5 =	적색 신호등 전환
t2 =	차단기 하강	t6 =	열차 출발 검지
t3 =	차단기 상승	t7 =	시스템 초기상태로 복귀
t4 =	녹색 신호등 전환		



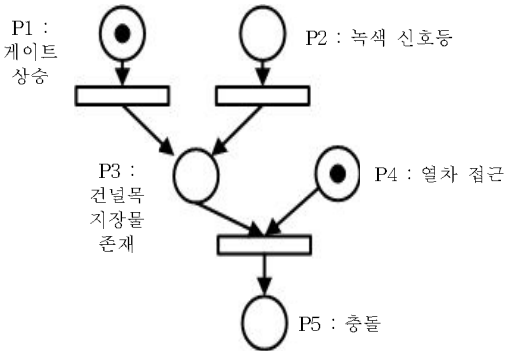
[그림 5] RCS에 대한 Petri Net 모델

6. 결 론

위험성 수용 기준 및 계산에는 상이한 여러 산업 및 엔지니어링에 대한 기본적이고 특수한 관계가 있다. 그러므로 위험성 수용 기준의 결정은 포괄적인 여러 경로 및 많은 기술적 지식이 뒤엉킨 복잡한 작업이다. 그리고 좀 더 연구를 진행시켜야 하는 많은 문제점들이 남아 있다. 특히 우리나라는 정량적 위험성 분석에 필요한 위험성 수용기준이 없기 때문에 선진국에서 사용되고 있는 기준 및 방법으로 정량적 위험평가를 수행하였다. 또한 Petri Net의 도달성 트리를 이용하여 안전성 분석을 수행하는 사례를 제시하였다. 향후에는 이들 기준 및 방법을 사용하여 정량적인 데이터 산출 및 편익비용에 대한 연구가 수행될 예정이다.



[그림 6] RCS에 대한 순방향 도달성 트리



[그림 7] 역방향 도달성 트리를 이용한 Petri Net

7. 참 고 문 헌

[1] "철도시설 안전기준에 관한 규칙", 국토해양부, 2011.6.7.
[2] "철도시설 안전세부기준", 국토해양부, 2011.8.3.
[3] "Functional safety of electrical/electronic/ programmable electronic safety-related systems", IEC 61508, 2010.
[4] Melchers RE, Society. Tolerable and the ALARP principle. In: Melchers RE, Stewart MG, Editors.

Probabilistic risk and hazard assessment. Netherlands: Balkema, 1993:243-295.
[5] Sharp JV, Kam JC, Birkinshaw M. Review of criteria for inspection and maintenance and artic engineering (OMAE 1993), Vol.2, New York: ASME, 1993:363-371.
[6] JOSEF BÖRCSÖK, EVZUDIN UGLJESA, "Markov Models for 2004 Architecture for Safety Related Systems", 6th WSEAS Int. Conference on Computational Intelligence, Man-Machine Systems and Cybernetics, Tenerife, Spain, December 14-16, 2007
[7] Hu Qunfang, Huang Hongwei, "The overview and study on the modeling of risk acceptance criteria for tunnel and underground engineering", The second Japan-China Joint Seminar for the Graduate Student in Civil Engineering Nagasaki, Japan 2005. 8.26-30
[8] V.M. Trbojevic, "Risk criteria in EU", Risk Support Limited, London, U.K.
[9] Institute of Chemical Engineering, Nomenclature for hazard and risk assessment in the process industries, 1985.
[10] Farmer FR (1967): Siting Criteria - a New Approach, Atom, Vol 128, pp 152-170 and presented at the IAEA Symposium on Containment and Siting, 3-7 April 1967, Vienna.
[11] D.S. Bowles, L.R. Anderson, J.B. Evelyn, T.F. Glover, D.M. van Dorpe, Alamo dam demonstration risk assessment, ASDSO meeting, 1999.
[12] USBR, US Department of interior Bureau of Reclamation, Guidelines for achieving public protection in dam safety decision making, 1997.
[13] NANCY G. LEVESON AND JANICE L. STOLZY, "Safety Analysis Using Petr Nets", IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. SE-13, NO. 3, MARCH 1987.

저 자 소 개

최 권 희

인하대학교 공학대학원 전기공학과에서 석사학위를 취득하였으며, 서울과학기술대학교 철도전문대학원에서 박사수료. (주)현대로템을 거쳐 현재 (주)에이알텍 근무 중. 관심분야 : 신뢰성 및 안전성 분석/평가, 제어시스템 해석 및 동적 모델링 등.

주소: 인천광역시 남동구 만수동 한국아파트 104동 210호

김 유 호

건국대학교 전기공학과를 졸업하고 연세대학교 전기공학과에서 석사학위를 취득하였으며, 동대학원에서 박사과정 진행 중. 현재 (주)에이알텍 대표이사, 관심분야 : 철도신호, 열차운행제어 및 초전도 응용 등.

주소: 경기도 용인시 수지구 성복동 84 강남빌리지 107동 1802호

이 종 우

한양대학교 기계공학과를 졸업하고, 프랑스 Pierre et Marie Curie 대학에서 공학박사를 취득하였으며. 한국철도기술연구원 책임연구원을 거쳐 현재 서울과학기술대학교 철도전문대학원 철도전기신호공학과 부교수, 관심분야: 열차제어, 안전성 및 신뢰성 등

주소: 서울 강남구 개포동 655-2 현대아파트 220동 104호

송 중 호

서울공대 전기공학과를 졸업하고, 동대학원에서 공학석사를 취득하였으며, 한국과학기술원 전기 및 전자공학과 공학박사. 한국과학기술연구원 지능제어연구센터 책임연구원을 거쳐 현재 서울과학기술대학교 전기공학과 부교수, 관심분야 : 전력변환장치, 대체에너지, 전력품질 등

주소: 서울시 서초구 서초4동 삼풍아파트 15동 205호

송 광 열

명지대학교 공과대학 전기공학과에서 석사학위를 취득하였으며, 한국고속철도건설공단을 거쳐 현재 한국철도시설공단 전기사업단 신호제어처 열차제어부장으로 재직 중. 관심분야 : 철도신호 및 열차운행제어 등.

주소: 서울시 광진구 광장동 현대아파트 801동 607호