FTA/ETA 기법을 이용한 철도신호시스템의 위험 분석 및 위험성 평가에 관한 연구

A Study on Hazard Analysis and Risk Assessment of Railway Signal System Using FTA/ETA Method

백영구[1] , 박영수[2] , 이재훈[3] , 이기서[4]

Baek, Young-Gu Park, Young-Su Lee, Jae-Hun Lee, Key-Seo

Abstract

In this paper, it was proposed that hazard analysis and risk assessment about railway signal systems using FTA(Fault Tree Analysis) and ETA(Event Tree Analysis) one of the reliability analysis methods executed and output value based on the hazard baseline of CENELEC and EC 61508 producted, and also the SIL(Safety Integrity Level)/THR(Tolerable Hazard Rate) about the system set.

On the basis of this principle, more systematic standardizations are required to operate railway system and in the future, we hope that safety and reliability of signal equipment will be better improved.

1. 개 요

현재 대·내외적으로 급속도로 발전하는 철도 신호설비의 안전성 및 신뢰성을 판정하고자 하는 판단기준의 근거를 확보하고, 첨단 컴퓨터 및 통신 기술의 철도 신호시스템과 접목을 위한 연결체계 기반을 구축, 철도 신호설비의 위험성(Hazard) 및 위험(Risk) 분석 기술 정립, 안전성 관리체계 형상화의 필요성이 새롭게 그 중요성을 더하고 있다.

1980년대 이전에는 국제 철도 연합(UIC)의 기술연구소(ORE)등에 의한 열차 신호 시스템의 안전성 확보를 위한 기술 지침의 규격화의 노력이 실시되었다. 그 이후 철도관련 선진국 각 국가별로 안전규격이 독자적으로 마련되었는데, 그 대표적인 예가 독일의 MÜE8004이다. 1980년대 이후에 접어들면서 일반 산업분야, 주로 공정제어 분야에서 사용되는 기기를 대상으로 하는 안전성 규격 IEC 61508을 제정하게 되었다.

1) 광운대학교, 제어계측공학과, 석사과정, 정회원
2) 철도청, 사무관, 정회원
3) 특허청, 정회원
4) 광운대학교, 제어계측공학과, 정교수, 정회원

최근 유럽에서는 유럽 전자 표준화 위원회 (CENELEC : Commite European de Normalisation ELECtrotechnique)에서 철도시스템을 위한 안전성 규격 즉, EN 50126, EN 50128, ENV 50129를 제정하였다. CENELEC의 이러한 규격의 목적은 참여국가간의 안전성 진술(Safety Case)의 상호 인증을 구현하기 위한 것이다. 이런 이유로 CENELEC 규격은 일부의 항목에서는 매우 심도 있게 다루어지며 또한 유사한 다른 규격들보다 더욱 규정적이다. 또한, CENELEC 규격은 IEC 61508을 철도신호 적용분야의 특정한 요구사항에 맞게 변형시킨 것으로 보아도 무방하다.

유럽의 이러한 동향과 더불어, 아시아 주변 국가들도 이러한 체계화에 주력하고 있다. 가까운 일본은 위와 같은 세계적인 추세에 발맞추기 위해 IEC 61508 및 CENELEC의 EN 50126과 EN 50129에 기초하여 자체적인 안전성체계를 구축하고 있는 실정이다.

본 논문에서는 기존에 있던 많은 신뢰도 분석 방법 중에서 위험 분석 및 원인 분석에 주로 사용되는 결함 목 분석과 사건 목 분석방법을 사용하여, 유럽을 중심으로 하는 표준인 CENELEC과 IEC 61508의 규격에 따른 시스템의 위험 분석에 대한 기술적인 내용을 근거로 하여 시스템의 안전 무결성 정도와 허용 가능한 위험성을 정량화 하였으며, 이러한 분석 기술을 철도신호 시스템 중에서 건널목 보호 장치에 적용하여, 그에 따른 안전 무결성 정도와 허용 가능한 위험성 값을 도출하였다.

2. 시스템의 위험 분석 절차

시스템의 위험성 분석에 있어서 잘못된 시스템의 분석으로 인하여 예측할 수 없는 결과를 초래하게 되므로 해당 시스템에 대한 정의는 위험성 및 위험분석에 있어서 중요한 열쇠가 된다. 이러한 시스템이 정의되고 나면 위험성 정립단계에 들어서게 되는데, 일반적으로 위험성 정립은 제품, 절차, 시스템의 체계적인 분석 또는 수명주기 전반에 걸쳐 발생할 수 있는 불리한 조건(위험성)들을 결정하기 위해 수행하는 과정을 모두 포함한다. 몇몇 불리한 조건은 인간에게 유해한 잠재적인 영향이나 환경 피해 또는 경제적 손실을 발생시키는 위험성을 가지고 있다.

시스템에 내에서 발생할 수 있는 고장 원인의 대책으로 시스템 최적의 안전성을 획득하기 위하여 안전 무결성(SIL) 개념이 사용된다. CENELEC 에서는 시스템 무결성을 정량화 하는 것이 타당치 못하다고 여겨 시스템 단위에서 발생하는 고장(우발고장을 포함)을 방지하는 대응책 간에 균형을 이루기 위한 수단으로 안전 무결성이 사용된다. 하지만, 오늘날에는 특정 안전 무결성 정도가 어떻게 충족되느냐 하는 안내가 상당히 포괄적이지만 시스템 안전 목표로부터 시스템 요소의 안전 무결성 정도 또는 허용 할 수 있는 시스템의 위험도를 유도해 내는 절차와 규정이 엄격히 규정되어 있지 않다는 것이다. 이러한 문제점을 해결하기 위한 협력적인 접근법을 CENELEC Working Group A10에서 고안하였다. 아래그림은 시스템의 위험성 분석 및 위험 분석의 절차를 도식화 한 그림이다.

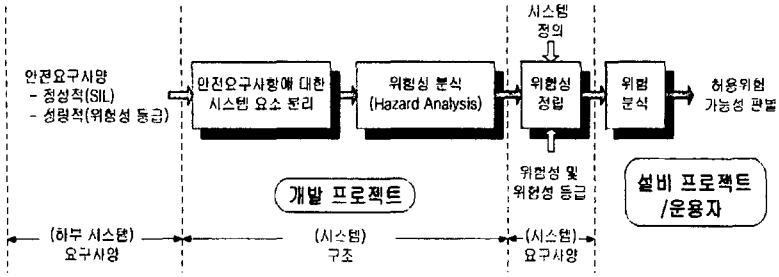

그림 1. 위험성 분석 및 위험 분석 개요

그리고 다음 표는 이러한 안전 무결성 정도에 대하여 CENELEC과 IEC 61508에서 각각 정의한 사항이다.

표 1. CENELEC 안전 무결성 정도의 정의

안전 무결성 정도	연속/고수요 운전 유형 (단위 요소별 단위 시간당 위험한 고장률)	중요도
4	$< 10^{-10}$	작다
3	$10^{-10} \leq \sim < 0.3\times10^{-8}$	⇓
2	$0.3\times10^{-8} \leq \sim < 10^{-7}$	
1	$10^{-7} \leq \sim < 0.3\times10^{-5}$	크다

표 2. IEC 61058 안전 무결성 정도의 정의

안전 무결성 정도	시간에 대한 허용 위험성(THR) 및 함수	중요도
4	$THR < 10^{-8}$	작다
3	$10^{-8} < THR < 10^{-7}$	⇓
2	$10^{-7} < THR < 10^{-6}$	
1	$10^{-6} < THR < 10^{-5}$	크다

위와 같은 안전 위험성 정도에 따른 위험성 평가가 이루어지고 난후 위험성등급의 순위가 결정되게 되는데, 단순한 위험성 등급 순위는 모든 규명된 위험성에 대한 관련 중요도 설정과 더불어 이에 근거하여 가장 중요한 위험성에 초점을 둔 더 나은 위험성 평가에 노력을 집중하기 위해 적용되어져야 한다. 위험성 평가에 뒤 이은 각 단계 내에서 각각 규명된 위험성에 관한 손실이 결정되어질 때, 각각의 위험성에 상대적인 순위는 그에 대한 더 나은 분석의 심도와 깊이를 안내하기 위해 사용되어져야 한다. 낮은 순위의 위험성은 보다 제한된 정성적 처리만을 요구하게 될 것이며, 반대로 작은 수치를 나타내는 가장 중요한 위험성은 보다 상세한 정량적인 평가를 정당화 할 것이다. 이러한 정량화 한 결과 값으로 시스템의 안전 무결성 정도가 결정되어진다. 아래 그림은 시스템의 위험성 분석에 있어서 전체적인 개요를 도식화한 그림이다.

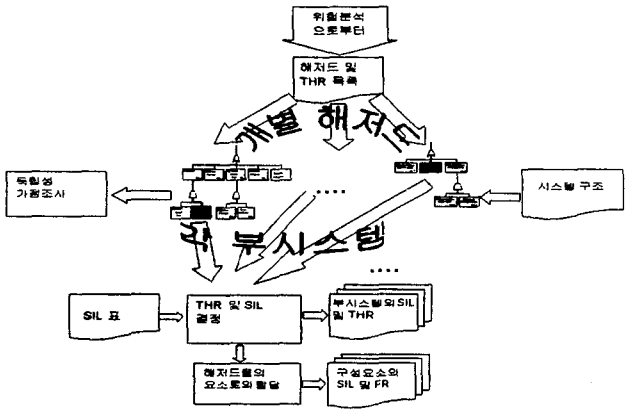

그림 2. 시스템 위험성 분석의 요약

이제까지 살펴본 것과 같은 형식으로, 시스템의 위험성 평가가 이루어진다. 다음은 이러한 평가를 바탕으로 실제 정량화 하기위한 분석기법들을 도입하여 시스템을 평가하였다.

3. 결함 목 분석과 사건 목 분석의 기본 모델

본 논문에서는 결함 목 분석과 사건 목 분석을 이용하여 시스템 분석을 실시하였으며, 아래 그림들은 각각 결함 목 분석과 사건 목 분석의 기본 모델을 나타낸 그림이다.

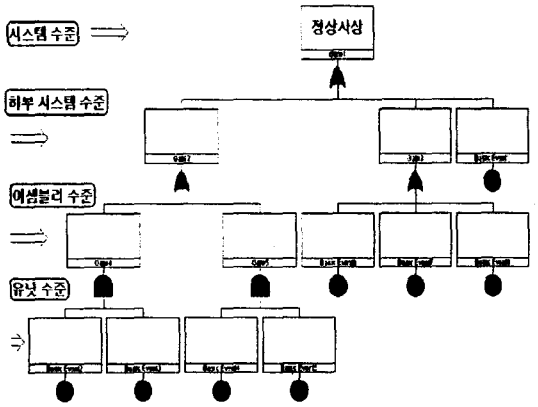

그림 3. 결함 목 분석의 기본 모델

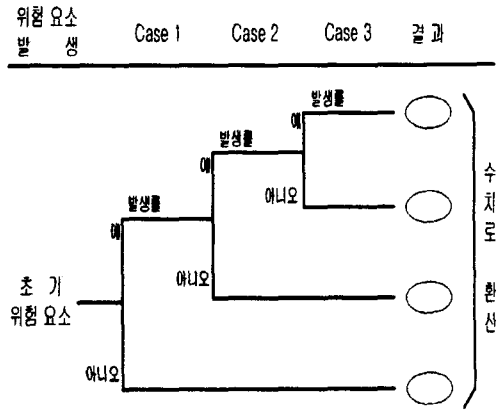

그림 4. 사건 목 분석의 기본 모델

이를 바탕으로 실제 건널목 보안 장치에 이를 적용하여 분석하고자 한다.

4. 건널목 보호 장치의 위험 분석 및 결과 고찰

본 절에서는 위에서 살펴본 위험성 및 위험 분석 기술 지침을 바탕으로 건널목 보호 장치를 대상으로 실제적인 적용을 시도하였다. 이에 앞서, 이러한 분석은 방법의 예를 설명한 것이지 상세하고 실제적인 분석을 행하는 것이 아니며 이에 사용된 숫자들은 임의의 적당한 근사 값들을 적용하였음을 미리 밝혀둔다.

시스템 분석에 있어서 선행하여야 할 사항으로서 분석하고자 하는 시스템에 대한 정의는 도로상에 있는 사람을 위한 광신호기와 차상의 기관사를 위한 원방 신호기를 포함하는 자동 건널목 보호 장치로 하며, 가장 중요한 위험 요소인 "다가오는 열차로부터 시민을 보호하기 위한 보호 장치의 고장"에 대한 분석을 실시한다.

4.1 위험 분석

1) 위험 허용성

여기에서 ALARP(As Low As is Reasonably Practicable)나 유사한 위험 허용성 원칙을 적용하지 않고, 검토의 단순성을 위하여 고정목표치로서 Railtrack의 철도그룹안전의 벤치마크 수치를 이용한다. 이때, 개략적으로 허용 가능한 경계치를 정의하기 위하여 추가적인 계수 10을 더 고려하였다. 이는 일반적으로 통행인들의 개인별 위험은 10^{-6}/1년 보다 적어야 함을 의미한다.

2) 개별 위험의 결정

개별위험을 결정하기 위하여 다음의 경우를 고려해보자. 한 통근자가 1년에 규칙적으로 건널목을 1000번 정도 통과한다 할 경우, 이때 행인이나 자전거 등으로 지나가는 사람은 고려대상에서 제외한다. 경험상을 볼 때, 위험상태가 발생하면 개인이 위험상태에 노출되는 시간, 즉 보호 장치를 통과하는 시간은 위험상태가 지속되는 시간보다 매우 작다는 가정이 가능하다. 이는 우리의 계산에서 개인의 해저드 노출시간은 무시할 수 있음을 나타낸다. 조금은 심한 추정이지만, 보호 장치가 수리되거나 재조정되기까지의 위험 노출 지속시간(D_1)을 10시간으로 가정한다.

3) 사건 목 분석을 이용한 원인-결과 분석

결과를 결정하기 위하여 이전에 설정한 위험요인에 의하여 발생할 수 있는 결과를 분석하여 보면 다음과 같은 결과를 얻을 수 있다.

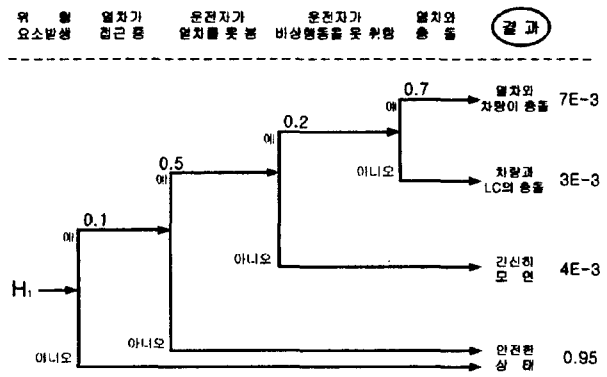

그림 5. 사건 목 분석을 이용한 원인-결과 분석

4) 손해 분석

위의 결과를 바탕으로 두 가지의 사고 유형과 초기 위험요소와 최종 사고사이의 외부위험감소율 발견할 수 있다. 위의 분석 결과를 바탕으로 아래와 같은 손해분석결과를 얻을 수 있다.

표 3. 손해 분석에 따른 위험 감소변수 결정

번호	사고(A_k)	위험 감소율(C^k_j)	치사율(F^k_j)
1	열차와 차량이 충돌	0.007	0.2
2	차량과 보호 장치의 충돌	0.003	0.05

5) 허용 가능 위험성 등급(THR) 결정

위에서 얻어진 결과 값을 바탕으로 다음과 같이 결정이 된다.

$$IRF_i = \sum H_j \times N_i \times [HR_j \times (D_j + E_{ij}) \times \sum A_k C^k_j \times F^k_j) \quad (1)$$

$$= 1000 \times HR_1 \times 10 \times (0.007 \times 0.2 + 0.003 \times 0.05) \leq TIR(\text{Tolerable Individual Rate}) = 10^{-6}$$

위 식으로부터 $HR_1 = 7 \times 10^{-8}$/시간 값이 산출되며, 이 값이 허용 가능 위험성 등급이 된다. 이는 대략 1회/1600년 정도의 위험요소 발생을 허락한다는 의미이다.

6) 결함 목 분석기법을 이용한 시스템 위험 분석

시스템을 분석하기에 앞서, 정상 사상(Top-event)을 정의해야 한다. 위의 분석을 바탕으로, 시스템의 정상사상을 보호 장치의 시민보호 기능고장으로 설정한 후 분석을 하면 다음과 같은 결과를 얻을 수 있다. 이때 주의할 점은 결함 목 분석에 있어서 모든 기본 사건(Basic event)들은 각각 독립적이어야 한다는 점이다.

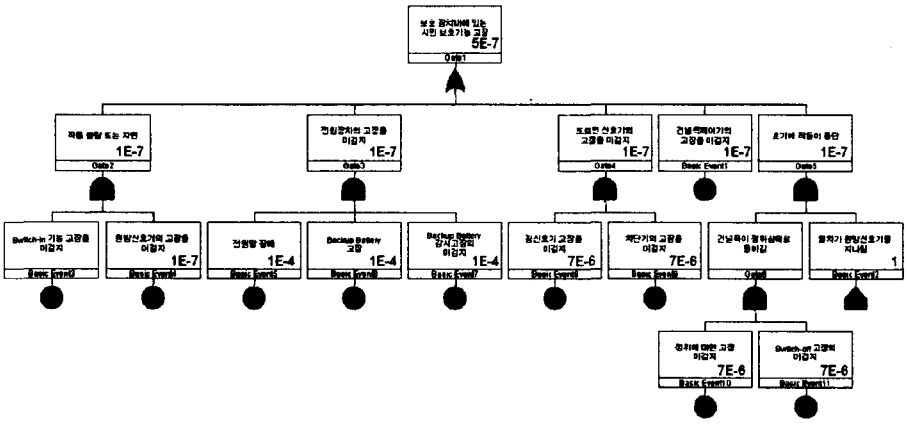

그림 6. 결함 목 분석기법을 이용한 시스템 위험 분석

위의 분석에서 정상 사상 다음 단계에는 각각 10^{-7}/시간의 위험성 등급을 설정하였다. 위의 분석에 어려운 점은 검지시간의 추정에 있다. Switch-in 과 같은 사건에서는 고장이 쉽게 검지된다. 왜냐하면 다음의 열차가 원방신호기 앞에서 정지하게 될 것이기 때문이다. 하지만, 신호기가 결코 위험을 나타내어 주지 않는 미 검지된 원방신호기의 고장과 같은 결함은 Switch-in 고장과 같은 다른 결함이 발생하기 전에는 결코 인식되지 않는다. 이를 해결하기 위한 방법으로는 원방신호기가 상위 사건의 위험성 등급을 그대로 상속하여 Switch-in 기능에는 아무런 요구조건을 두지 않는 것이다. 전원장치의 고장에 대해서는 10시간정도의 기간동안 전원 망 고장에 10^{-4}/시간 값을, 배터리 고장에는 1시간 정도의 평균검지시간에 10^{-4}/시간 값을 설정하였다. 그리고 배터리 감시기능의 미 검지 고장에 대해서는 1년 단위의 유지 보수 활동에 따른 검지의 결과로 10^{-4}/시간 값을 설정하였다. 이 결과 정상사상에 있어서 위험성 정도는 5×10^{-7}/시간 이라는 값을 얻을 수 있었다. 이러한 결과 값은 위에서 언급한 표를 안전 무결성 정도 표를 근거로 하여 안전 무결성 정도가 "3"이라는 것을 얻을 수 있었다.

5. 결론 및 향후과제

최근 철도신호 설비는 이전 신호방식에 따른 신호설비의 안전성 문제에 접근이 어려운 실정이므로, 컴퓨터 공학, 통신공학, 및 신뢰도 공학에 기초한 철도 안전성에 대한 체계적이고 분석적인 접근이 요구되고 있는 상황이다.

이에 따른 철도신호시스템의 중요성에 입각하여 CENELEC와 IEC61508 규격을 근거로 하여 신뢰성 분석 기법 중에 하나인 결함 목 분석과 사건 목 분석 기법을 이용하여 건널목 보호 장치에서 발생할 수 있는 위험 요소에 대한 위험성 분석 및 위험 평가를 정량화 하였다.

또한 이러한 결과 값을 바탕으로 안전 무결성 정도와 허용 위험성 등급 값을 산출하였으며, 이러한 정량적인 분석결과를 이용하여, 시스템에서 발생할 수 있는 고장원인을 사전에 예방하고, 각

각의 시스템 및 제품에 대한 안전 무결성 정도에 따른 중요도에 입각하여 그에 알맞은 조치를 사전에 취해야 할 것이다. 또한 발생한 고장에 대한 조치 또한 철저히 이루어 져야 할 것이다. 이를 바탕으로 실제 안전성 관련 종사자들이 이러한 방법 및 적용사례를 다른 부분에 쉽게 적용할 수 있도록 하였다.

본 논문에서 언급한 사항은 극히 일부에 지나지 않으나, 이를 바탕으로 향후 철도 시스템 및 운용에 있어서 보다 체계적인 표준화를 제정하는데 있어서 기초 자료로서의 역할을 하게 되고, 이를 기초로 하여 이론적인 분야에 너무 치우쳐 있는 신뢰성 및 안전성 분석이 제품을 설계하고 생산하는 사람으로부터 이를 사용하고 관리하는 모든 사람에게 보다 체계적이고 표준화된 과정으로 인식되어진다. 그리고 향후 이 분야의 지속적인 연구로 국내 철도 신호설비 뿐만 아니라 다른 설비들의 안전성 및 신뢰성 향상에 커다란 발전이 있기를 기대해 본다.

참고 문헌

1. RAMS에 대한 사양 및 증명-EN 50126(1998년 5월)
2. 철도제어 및 보호시스템에 대한 소프트웨어-prEN 50128(1998년 7월)
3. 철도신호에 대한 안전성 관련 전자 시스템-ENV 50129(1998년 5월)
4. 공정산업에 대한 기계화된 안전성의 응용-Draft 61508(1997년 6월)
5. 철도 응용, 위험성 고장률과 안전 무결성 정도(SIL) R009-001(1997년 7월)
6. System Safety Corp.(1998), "System Safety Analysis Handbook Second Edition"
7. CENELEC(1999), "Railway Applications Systematic Allocation of Safety Integrity Requirement"
8. 박경수(1999), "신뢰도 및 보전공학", 영지문화사
9. 김병석(2002), "시스템 안전공학", 형설출판사
10. 김원경 외(1998), "열차 신호시스템 안전성 확보", 한국철도기술 제 17호
11. Railtrack(1999), "Engineering Safety Management"
12. Neil Storey(1996), "Safety Critical Computer Systems", Addison-Wesley
13. 김원경(1999), "시스템 신뢰도 공학", 교우사