철도시스템 안전관리 체계개발에서 기능안전 표준을 반영한 아키텍처 모델의 활용

On the Use of Architectural Models Reflecting Functional Safety Standards in the Development of Rail Systems Safety Architecture

정 호 전* · 이 재 천*

Abstract

오늘날 기술의 발전으로 시스템들은 점차 대형화 복잡화 되어가고 있다. 이처럼 점차 대형화 복잡화 되어가고 있는 시스템들은 더욱 커진 사고 및 고장에 대한 위험을 내재하게 된다. 또한 대형 복합 시스템에서 발생하는 사고 및 고장은 바로 큰 재산피해나 인명피해와 직결 될 수 있다. 따라서 체계적인 안전관리의 필요성이 점차 커지고 있다. 이에 대응하여 철도, 항공, 해양 등의 산업에서는 각 산업에 적합한 안전관리체계를 수립하려 노력하고 있으며, 표준 및 매뉴얼을 제정하여 보급에 앞장서고 있다. 또한 시스템에서 전장품 및 소프트웨어가 차지하는 비중이 커지면서 기능안전이 안전분야의 이슈가 되고 있다. 이에 따라 IEC 61508, ISO 26262, IEC 61511 등 기능안전 관련 표준들이 제정되어 기능안전을 달성하기 위한 기반을 제공하고 있다. 한편 국내 철도산업에서도 철도안전법의 재정을 기점을 철도 산업전반에 걸쳐 많은 환경변화가 이뤄지고 있고 이에 대응하기 위해 철도 안전시스템을 바탕으로 한 안전관리체계를 구축하였다. 한편 다양한 운영체계를 갖고 있는 철도시설 및 운영기관이 존재하는 국가 철도 안전관리체계의 안전규제를 체계화하기 위해서는 체계적인 요구사항의 분석에 따른 시스템 아키텍처의 설정이 요구되고 있다. 이러한 아키텍처의 설정은 현재에 대한 분석과 미래의 철도안전시스템의 특성을 구조화하여 향후 비전을 프레임워크로 표현함으로서 구현이 가능해진다. 본 논문에서는 현재의 안전관리체계의 도입 배경 및 도입 현황에 대해서 분석하고, 최근 기존의 안전관리체계와 더불어 최근에 안전분야에서 이슈가 되고 있는 기능안전 표준을 반영한 안전관리체계의 구축을 위해 안전관리체계에 대한 아키텍처를 구현하고자 하며 이때, 모델링을 바탕으로 한 접근을 제시한다.

* 아주대학교 시스템공학과

I. 서 론

현대의 안전중시 시스템들은 과거와 비교해서 급격한 운영성능의 발전을 가져 왔고, 동시에 기능적으로도 매우 복잡해지게 되었다. 시스템이 점차 대형화 복잡화됨으로써, 시스템에서 발생할 수 있는 사고나 고장의 위험 또한 증가하고 있다. 특히 이런 안전중시 시스템들은 사고나 고장이 인명 및 재산피해로 직결되기 때문에 체계적인 안전관리가 필요하다[2]. 이에 따라 철도, 항공, 해양, 원자력 등의 산업분야에서는 안전관리체계에 대한 표준 및 매뉴얼을 제정하여 체계적인 안전관리 활동을 수행 할 수 있는 바탕을 제공하고 있다.

철도산업에서 기반시설과 운영의 상하 분리와 민영화를 추진해온 선진 철도 운영국에서는 철도안전법을 근간으로 하여 일관된 국가안전체계를 구축하고 안전관리를 제도적으로 시행하고 있으며, 강력한 안전규제를 집행하는 것이 세계적인 추세이다. 우리나라도 04년 철도운영공사와 시설공단이 발족됨으로써 철도산업의 구조 개편이 완성되었으며, 새로운 구조에서 철도의 안전을 확보하기 위해 정부가 제정한 철도안전법을 05년 10월을 기해 발효되었다. 철도안전법은 시설관리자와 철도의 운영자간 안전 인터페이스를 확보하고, 정부규제 중심의 국가적인 안전관리체계를 시행할 수 있는 법적 근거를 제공하게 된다.

일반적으로 철도시스템은 안전성 · 쾌적성 · 정시성을 최대한 만족시키는 공공교통 수단으로서 철도운영 선진국은 인간요소, 열차, 선로시설, 운영 · 제어, 유지보수 등 다양한 기술요소가 복합된 시스템 기술능력을 바탕으로 그동안의 다양한 시행착오를 거쳐 확립된 안전 확보 기술과 안전관리 경험에 의해 철도시스템의 운행안전을 확보하고 있다.

선진국의 경우 철도안전을 향상하기 위한 기술개발은 국가주도하에 전략적 · 집중적으로 투자하고 있다. 미국은 1980년 이후 지속적인 안전연구를 실시하여 1981년 대비 사고빈도를 65% 저감시킨 바 있다. 영국의 경우 철도안전표준위원회(Rail Safety & Standard Board)를 중심으로 체계적인 연구개발 프로그램을 시행중이며, 안전체계가 선진화되어있음에도 불구하고 안전연구 Rolling Plan을 위하여 최근 5년 동안 7개 연구 분야, 24개 연구주제에 7500만 파운드(1500억원)를 연구에 투자하고 있는 실정이다. 프랑스, 독일, 일본 등에서도 국가 연구기관 주도로 철도안전기술개발 및 관리시스템을 구축 운용 중에 있다. 따라서 우리나라도 더 이상 철도안전기술개발을 현 수준으로 방치할 수 없으며, 선진국 수준의 철도 종합 안전관리시스템을 확립할 수 있는 기술개발이 필요하다고 할 수 있다.

철도의 안전 확보 및 관리는 인간요소, 열차, 선로시설, 운영 · 제어, 유지보수 등 시스템 전반에 대한 위험분석 및 안전성 평가를 기본으로 하고 있으며, 대상 위험도를 사전에 제거하거나 적정수준으로 관리할 수 있는 시스템 차원의 안전성 평가 및 안전확보 기술이 필요하다.

현재 우리나라의 경우 사고발생 원인의 추적이나 안전성 평가에 대한 기술적 기반이 미흡한 상태로서 발효된 철도안전법의 효율적인 시행기반을 마련하기 위해서는 안전규제시스템의 정의 및 절차 개발, 안전규정체계의 정비, 세부안전기준의 제정, 안전

성 평가기술 개발, 시험평가기반의 구축, 중대사고 방지기술의 개발 및 안전정보 관리체계의 구축 등이 이루어져야 할 뿐만 아니라, 개발된 기술들이 연계되어 종합적인 안전체계 내로 편입되어야 할 필요가 있다.

대규모의 복잡한 시스템에서 안전체계 개발의 필수적 요소는 운영에 관련된 모든 시설, 장비, 운영실무, 인간요소들이 시스템의 임무를 수행함에 있어서 오류가 사전에 예방되거나 피하지 못할 오류가 발생하더라도 피해 없이 즉각 관리 가능한 체제를 확립하는 일이다. 이를 위해 철도시스템의 구성요소와 도출된 안전요건들이 서로 추적성을 유지하면서 형상관리 되는 것이 매우 중요하다. 이로 인하여 안전관리체계 내의 관련주체들의 역할과 기능을 설계하고 분담하여 실행할 때 철도시스템의 안전도 향상효과는 배가될 수 있을 것이다. 즉 철도안전시스템에 대한 아키텍처를 구성함으로써 현재의 시스템에 대한 분석과 미래의 철도 안전시스템의 특성을 구조화하여 철도 안전시스템의 안전도 향상을 달성 할 수 있다[3].

2. 문제의 정의

2.1 철도 안전관리체계의 정의

안전관리의 개념을 이해하기 위해서는 먼저 안전의 의미를 고찰할 필요가 있다. 개인적인 관점에 따라 철도안전의 개념은 다음과 같이 다양한 의미를 내포할 수 있다.

-무사고(사건 포함) - 일반 여객의 관점
-위해의 원인이거나 원인이 될 수 있는 위험상황 또는 위험가능성이 없는 상태
-불안전한 행동과 상태를 극복하려는 직원들의 태도(조직의 안전문화 반영)
-철도분야에서 수용할 수 있는 내재된 리스크 수준
-해저드를 인식하고 리스크를 관리하는 과정
-사고로 인한 손실(인명, 재산, 환경 훼손 등) 방지

또한 안전관리란 복잡하고 높은 안전성, 신뢰성이 요구 되어지는 시스템에 대해서 해당 국제규격에 따른 안전성 확보를 위해 수명주기에 따라 정의된 여러 활동들을 수행하는 것을 의미한다. 여러 가지 국제 및 산업 표준이나 지침에 따라 약간의 차이는 있지만 안전관리는 위험원식별, 리스크평가, 위험원 및 리스크 분석/평가 결과를 바탕으로 위험원 및 사고위험성 제거/감축 단계 등을 포함하고 있다[4-5].

위와 같이 정의된 안전을 확보하고 체계적인 안전관리를 수행하기 위해 안전관리체계를 구축 및 도입하고 있다. 안전관리시스템(Safety Management System, SMS)은 조직자신의 업무활동의 안전을 보증하기 위한 정책, 자원 그리고 절차를 통한 조직의 공식적인 계획(arrangement)이다.

효율적인 SMS는 조직이 효율적으로 위험도를 관리하고 확인할 수 있도록 돕는다.

이것은 조직이 규정적인 요구사항을 충족하고 자신의 안전 목적에 도달 할 수 있는 능력을 증명할 수 있도록 해 준다. SMS는 조직의 다른 활동으로부터 분리된 것으로 생각되어서는 안 된다. 조직의 다양한 목표(성능, 품질, 안전 등등)는 자주 동일한 절차에 의존한다. 그러므로 SMS는 조직 내의 모든 관리시스템과 통합되어야 한다. 효율적인 SMS에 대한 증거는 조직이 안전하게 관리할 수 있는 능력에 대한 확신을 제시한다. 이 증거는 조직의 시스템과 서비스가 통제와 준비가 효율적으로 관리된다는 것을 보증한다. 안전관리는 위험도 확인, 평가, 통제에 대한 것이다. 그리고 조직이 이것을 달성하기 위해서는 체계적인 접근방법이 핵심이다[6].

위와 같은 SMS에 대한 접근방법 및 사고를 가지고 현재 국내 철도안전관리체계는 구축되어 있으며, 안전관리체계 내에서 수행되어야 할 활동은 <그림 1>과 같이 제시되고 있다.

2.2 철도 안전관리 방식의 변화

안전관리체계 구성단계	각 단계별 활동
정책 결정 및 계획	정책 결정
	안전관리활동 수행조직 구성
	위험관리 및 안전보장 활동에 대한 계획 수립
위험관리	시스템 정의
	위험원 식별
	위험 분석
	위험 통제
안전보장	성능 모니터링
	사고 및 고장 보고 및 조사

<그림 1> 안전관리체계의 구성단계 및 단계별 수행 활동

역사적으로 철도안전은 점점 복잡해지는 법적 요구를 따르는 것에 초점이 맞추어져 있었다. 이 접근 방식은 최근에 까지 사용되어왔다. 하지만 모든 규정과 규제에도 불구하고 철도 사고는 끊임없이 발생하였다. 전통적인 방식은 발생한 사고에 대한 대응조치로 대책을 마련함으로써 사고의 재발을 방지하는 것이다. 최적의 제도 또는 요구

표준이라기보다는 최소기준을 만족하는 수준에 머무르고 있다.

안전에 대한 위험도를 수용 범위내로 유지시키기 위해서는 현대적 안전관리 지침은 종전의 사후적 대책을 탈피하여 사전대응방식으로 변화해야 한다. 더불어 실질적인 법률과 규제 요건, 승인된 절차가 효력을 갖고, 이러한 규정의 집행이 효과적으로 이루어지도록 다음과 같은 다양한 요소를 고려해야 한다.

-리스크관리기법의 과학적 적용
-고위관리자의 안전관리에 대한 의지(Commitment)
-조직의 안전문화 정착(안전권고안의 이행 증진, 안전 의사소통 장려, 재무 관리에 대한 관심처럼 적극적인 안전에 대한 관리)
-체크리스트 및 브리핑을 활용한 표준운영절차(Standard Operating Procedures)의 효과적인 이행
-처벌에 얽매이지 않고 효율적인 사건, 장애요인보고를 장려하는 환경(또는 문화)
-정상 운영상황에서 발생하는 안전과 관련된 정보를 수집하고 분석하며, 공유하는 시스템
-처벌목적이 아닌 안전의 구조적 결함을 발굴하는 사고와 심각한 사건 조사 관할권
-실무자를 위한 안전교육훈련(인적요소 포함)의 통합
-국가와 회사 간의 원활한 안전정보 교환을 통해 안전대책과 안전훈련 내용의 공유

이러한 요소를 바탕으로 현대의 철도안전관리는 사고 발생이후 대응하는 수동적인 안전관리가 아닌 사고발생이전에 미리 위험요소에 대한 관리를 수행함으로써 능동적인 사고에 대한 대처가 가능하도록 한다[7]. 이러한 안전관리 방식의 변화가 안전관리 체계에 반영되어 능동적인 철도안전관리가 이뤄져야 한다.

2.3 기능안전 개념의 도입

산업의 급속한 발전과 함께 인명의 피해 및 안전을 위협하는 큰 사고가 발생하기도 한다. 예를 들면 1976년 이탈리아 세베소 농약공장의 다이옥신 방출사고나 1984년 인도 보팔의 맹독 가스 유출사고 등이 있다.

종전에는 사고가 발생한 후에 대책을 강구하는 사후 대책형으로 대응했다. 그러나 이 방법으로는 사고를 방지할 수 없어 사전에 리스크를 평가해 사고를 예방할 필요성이 제기됐다. 또한 최근에 플랜트, 장도차, 원자력등의 산업에서 제어 부분의 전장품 및 소프트웨어의 비중이 증가해 전장품 및 소프트웨어 까지 포괄하는 안전규격이 요구됐다. 이에 ㄸ、라 IEC에서는 안전에 관한 공통의 사고 방식을 정한 ISO/IEC 51 가이드에 기초해, 기능안전에 관한 국제규격 IEC 61508을 제정했다. 또한 여러 산업분야에서는 IEC 61508을 각각의 산업에 적절히 변경하여 산업별 기능안전 표준을 제정하고 있다. 기능안전은 전장품 및 소프트웨어의 비중이 커지고 있는 현대의 시스템에서 반드시 고려되어야 할 문제이며, 각 산업분야 별로 지속적인 표준 제정이 이뤄지는 것에 비춰 보아 실제 산업분야에서도 중요성을 인식하고 대응하기 위해 노력하고 있음

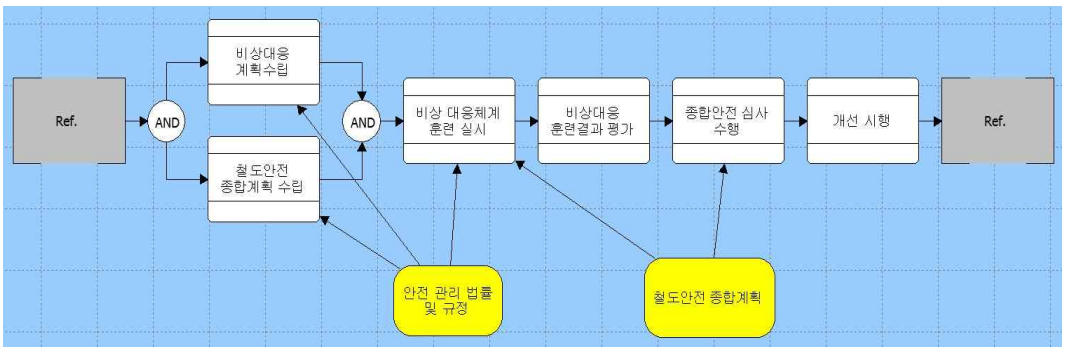
을 알 수 있다. 따라서 철도시스템의 안전관리체계에도 기능안전 표준에서 제시하고 있는 기능안전의 개념과 안전수명주기의 개념을 반영할 필요성이 있다.

3. 철도안전관리체계 아키텍처구현을 위한 모델링

3.1 철도안전관리체계 모델링

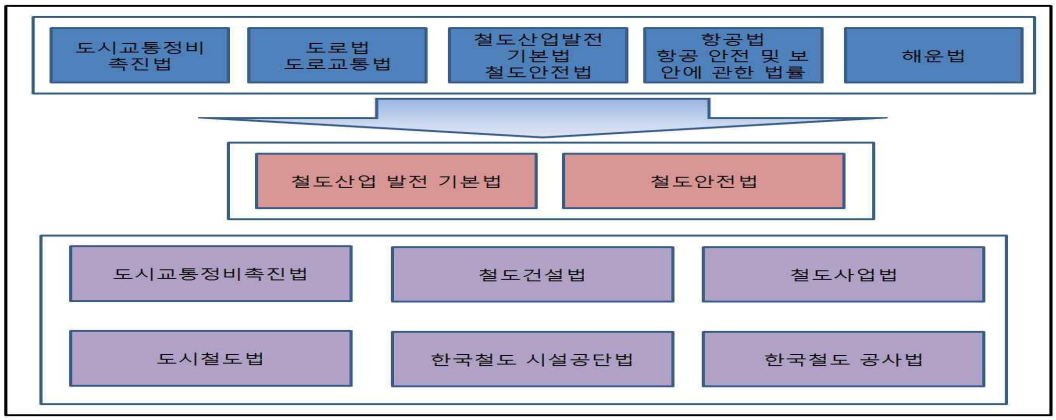
국내 철도 안전관리체계는 국내 철도안전법(시행령, 시행규칙 및 관련 고시 포함)을 근간으로 작성되었으며, 철도산업과 관련하여 캐나다, 영국, 호주의 안전관리시스템을 참고하였다. 현재 국내 철도안전관리체계는 <그림 2>와 같다.

3.2 철도안전계획체계 모델링



<그림 2> 국내 안전관리체계 모델

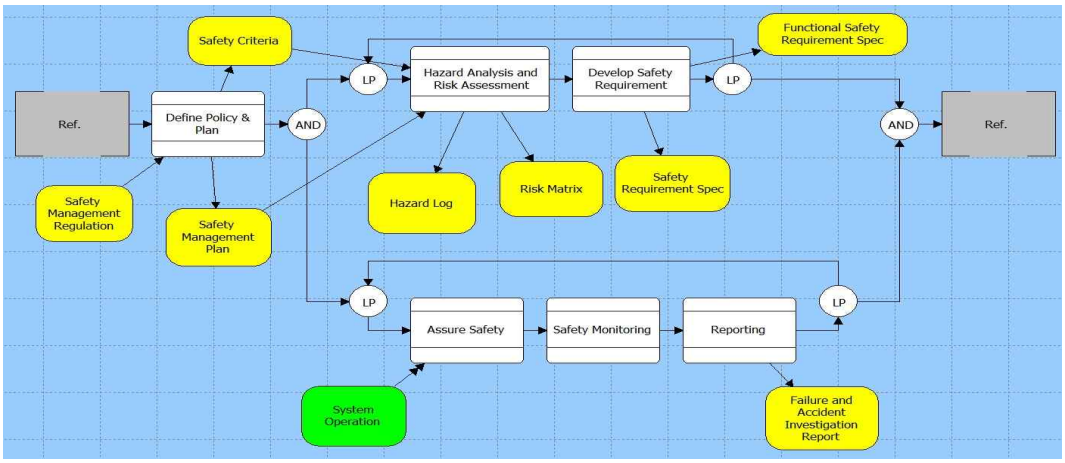
도시철도와 철도의 안전 측면에서의 법령체계를 체계화 하면 <그림 3>과 같다. <그림 3>에서 보는 바와 같이 철도는 철도산업 발전 기본법에 따라 철도 종합 안전계획을 철도 산업위원회에서 심의토록 하고 있다 법령 제 2조에 따르면 한국철도시설공단과 한국철도공사가 소유 건설 운영 관리하는 철도를 대상으로 하고 있다 따라서 도시철도는 전체 법조항의 적용대상에서는 제외되어 있으나 단서조항으로서 제 2장의 철도산업 발전기반의 조성조항에 따라 철도안전과 철도운영에 관한 중요정책 사항 등을 모든 철도에 대하여 적용하도록 하고 있으므로 도시철도 또한 철도 종합 안전계획의 수립대상이 된다. 철도산업 발전 기본계획의 제 3장 철도안전 및 이용자 보호 영역은 도시철도를 대상으로 정의하고 있지 않지만 도시철도법의 하위규칙에서 정의되고 있다 따라서 철도 산업위원회는 정책의 심의기능과 더불어 시설투자확대 산업지원 전문인력 교육훈련 교육과정 기술진흥 정보화촉진, 국제협력에 대한 도시철도와 철도의 공통시책을 심의대상으로 다루게 되며 실제 안전관리 시행과 집행에 대해서는 도시철도법에 의해 다루어지고 있는 상황이다.



<그림 3>철도시스템의 안전관련 법령 체계

3.3 기능안전 활동이 반영된 철도안전관리 프로세스 모델링

안전관리체계에 대한 아키텍처를 구현하기 위해 먼저 철도안전관리체계 내에서 수행되어야 할 철도안전관리프로세스에 대한 모델링을 수행하였다. 철도안전관리체계를 구성하고 있는 단계 및 세부 활동들을 식별하고 이를 EFFBD(Enhanced Functional Flow Block Diagram)를 이용하여 모델링 하였다. 또한 대표적인 기능안전 표준인 IEC 61508에서 제시하고 있는 안전수명주기 활동 및 산출물[3]을 기존의 안전관리체계에 반영하였다. <그림 4>와 같이 각 단계의 진행순서, 세부 활동들의 수행 순서 및 데이터의 입출력 등을 파악할 수 있다.



<그림 4> 기능안전 활동 및 산출물이 반영된 철도안전관리 프로세스 모델

4. 결론 및 요약

오늘날 점차 대형화 및 복잡화 되고 있는 시스템들은 개발 및 운용단계에서 많은 사고 및 고장의 위험을 내재하게 된다. 특히 안전중시 시스템들은 사고나 고장이 인명 및 재산피해로 직결되기 때문에 체계적인 안전관리가 필요하다. 이에 따라 철도, 항공, 해양, 원자력 등의 산업분야에서는 안전관리체계에 대한 표준 및 매뉴얼을 제정하여 체계적인 안전관리 활동을 수행 할 수 있는 바탕을 제공하고 있다. 이에 따라 국내 철도산업에서도 철도안전법의 재정을 기점을 철도산업 전반에 걸쳐 많은 환경변화가 이뤄지고 있고 이에 대응하기 위해 철도 안전시스템을 바탕으로 한 안전관리체계를 구축하였다. 한편 다양한 운영체계를 갖고 있는 철도시설 및 운영기관이 존재하는 국가철도 안전관리체계의 안전규제를 체계화하기 위해서는 체계적인 요구사항의 분석에 따른 시스템 아키텍처의 설정이 요구되고 있다. 이를 위해 본 논문에서는 첫째, 현재 국내철도산업에 도입되어 있는 안전관리체계에 대한 모델을 구현하였다. 둘째, 교통 및 철도시스템 안전 법령체계의 구조화와 철도시스템의 물리적 구성요소별 규제체계의 구조화를 모델을 통해 구현하였고, 이는 현재 시점에서의 철도시스템의 안전규제체계를 도출한 것이다. 셋째, 철도 안전관리체계 내에서 수행되어야 할 안전관리 프로세스에 대한 모델링을 구현하였다. 안전관리체계와 안전관리규제에 대한 구조화 및 모델링이 국내 철도 안전관리체계에 대한 상위수준의 아키텍처를 구현하기 위한 것이라면, 안전관리프로세스에 대한 모델 구현은 하위수준에서의 안전 관리체계의 아키텍처를 구현하기 위한 것이라 할 수 있다. 향후 철도안전관리체계를 구성하는 모든 구성요소들에 대한 인터페이스를 식별하여 철도 안전관련 법률, 수행활동, 입출력 데이터들이 모두 식별되는 수준의 아키텍처 프레임워크의 구현이 필요할 것이다.

5. 참 고 문 헌

[1] Introduction to SAFETY MANAGEMENT SYSTEMS, Transport Canada, 2001.
[2] System Safety Handbook, Federal Aviation Administration, 2000.
[3] Functional safety of electrical/electronic/programmable electronic safety-related systems,
[4] International Electrotechnical Commission Standard, IEC 61508, 2010.
[5] Road vehicles --Functional Safety--, International Organization for Standardization Standard, ISO
[6] 26262, 2011.
[7] The SAFECOM Program, "Public Safety Architecture Framework," Homeland Security, Washington, D.C., Feb 10, 2006.
[8] J. Langheim, B. Guegan, L. Maillet-Contoz, K. Maaziz, G. Zeppa, F. Philippot, S. Boutin, H. Aboutaleb, and P. David, "System architecture, tools and

modelling for safety critical automotive applications - the R&D project SASHA," in Proc. ERTS 2010, Toulouse, France, May 19-21, 2010.

[9] A. Berrado, E. El-Koursi, A. Cherkaoui, and M. Khaddour, "A framework for risk management in railway sector: application to road-rail level crossings," The Open Transportation Journal, pp. 34-44, May 2011.

[10] 박영수, 조연옥, 홍선호, "철도안전시스템 아키텍처 모델링을 통한 안전규제 체계화 방안 연구," 한국철도학회 추계학술대회, (주최) 한국철도학회, 2005년 11월 10-11일, pp. 7-14.

[11] 김상암, 조연옥, "위험도 기반 철도 안전관리시스템 아키텍처 개발," 한국철도학회 추계학술대회, (주최) 한국철도학회, 2011년 10월 20-22일, pp. 2517-2526.