시스템 엔지니어링을 적용한 국가 안전관리 체계 구성 방안
A constitution plan of national safety management system applied by systems engineering

조연옥* 윤혁진** 김상암** 곽상록** 한순우**
Cho, Yun-Ok Yoon, Hyuk-Jin Kim, Sang-Ahm Kwak, Sang-Log Han, Soon-Woo

Abstract

As technologies are developed and systems are complicated, hazards embedded in the system are also increasing. proving safety and managing the safetyis more scientific and organizational domain so that safety management system is pursuing to be activeformation detecting the factors of hazard and managing them beyond passiveway. In the future, in order to establish and manage national safety management system, it is important to have effective system and manage it and also more important that all the people related to target system has to change their recognition and to playroles in it.

Many railway safety measures reduce railway fatalities into half for last 10 years. But more improvement in railway safety is required to meet the social need after railway fire accident in Daegue. After the Daegue subway train fire accident, the Korean government has been trying to prepare a nation-wide railway safety program, a safety organization, and a Safety Act. To construct a nation-wide railway safety management program, system architecture was established.

1. 서론

철도산업에서 기반시설과 운영의 상하 분리와 민영화를 추진해온 선진 철도운영국에서는 철도안전법을 근간으로 하여 일관된 국가안전체계를 구축하고 안전관리를 제도적으로 시행하고 있으며, 강력한 안전규제를 집행하는 것이 세계적인 추세이다. 우리나라도 2004년 철도공사와 시설공단이 발족됨으로써 철도산업의 구조 개편이 완성되었으며, 새로운 구조에서 철도의 안전을 확보하기 위해 정부가 제정한 철도안전법이 2005년 10월을 기해서 발효되었다. 철도안전법은 시설관리자와 철도의 운영자간의 안전 인터페이스를 확보하고, 정부규제 중심의 국가적인 안전관리체계를 시행할 수 있는 법적 근거를 제공하게 되었다. 철도시스템의 안전관리규정체계 및 주기적인 안전프로그램의 개발과 실행은 철도 운행에 따른 사전 위험요인 도출에 의한 안전위험 제거 및 경감, 철도시스템의 신뢰성 저하로 유발될 수 있는 대형사고의 예방, 나아가 주기적인 안전점검과 성능확인에 의한 철도사고 발생 시 공공교통수단으로서 부담해야 하는 직·간접적인 사회적 손실 및 기회비용을 근본적으로 줄일 수 있고 국가수송체계의 경쟁력을 보장하는 대단히 중요한 분야이다[1, 2].

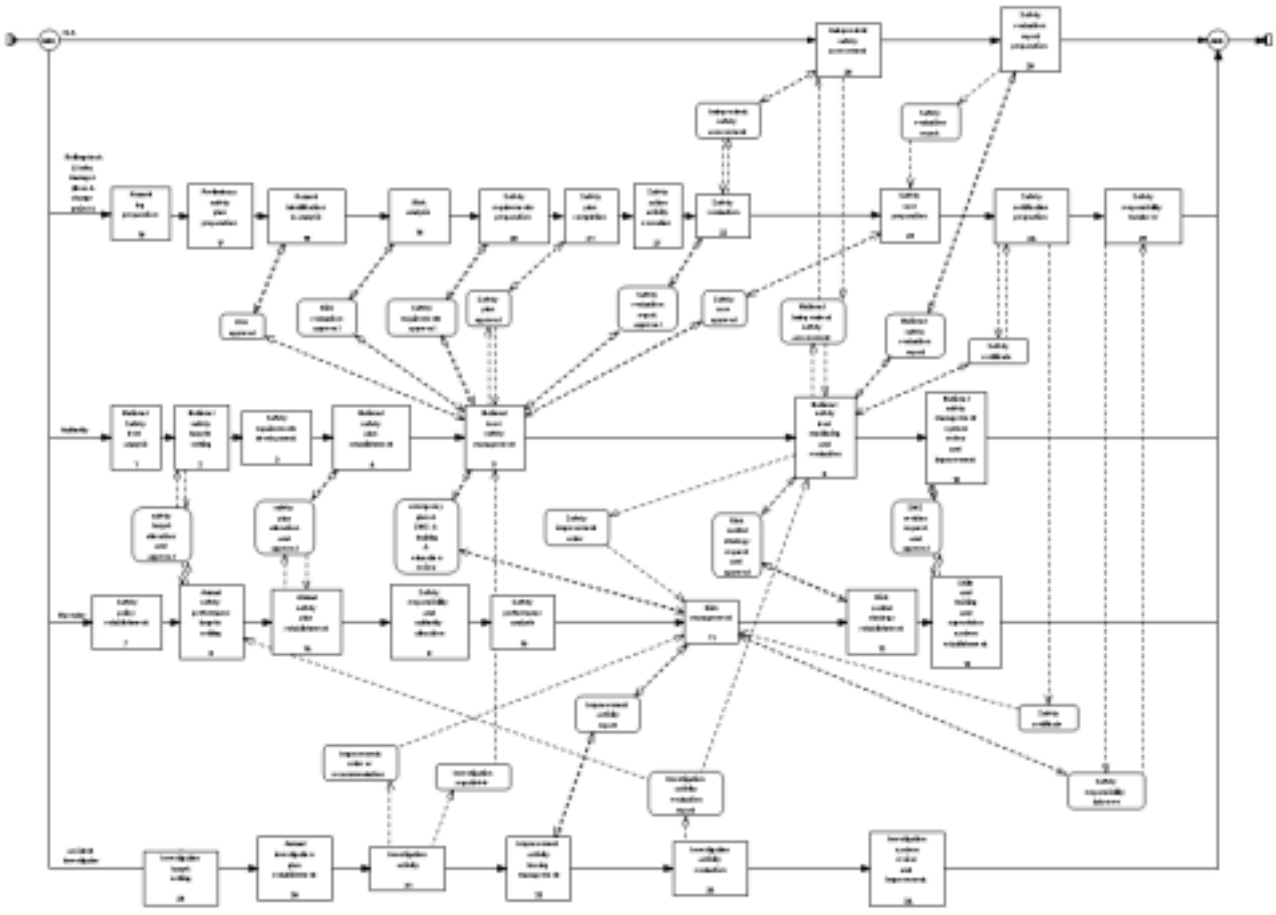
본 논문에서는 국가 차원의 안전관리 체계 구축 방안을 제시하였다. 당국, 철도 운영기관, 열차 및 시설 구축자, 독립평가기관, 사고조사위원회의 역할을 식별하고 기능을 할당하였다. 수립된 안전관리 체계는 위험도 정보를 기초로 하고 있으며, 위험도 정보에 따라 안전개선투자의 우선순위 설정, 투자 비용에 대한 효과의 정량적 분석, 사고 예방 비용을 도출하도록 되어 있다. 당국은 국가 안전 관리 요구사항을 철도 운영자에게 할당하고 철도 운영자는 이에 기반한 안전 관리 계획을 당국에 제출하여 승인받도록

* 한국철도기술연구원 안전기술연구팀 수석연구원, 정회원
E-mail : yocho@krri.re.kr
TEL : (031)460-5429 FAX : (031)460-5509
** 한국철도기술연구원 안전기술연구팀 선임연구원, 정회원

하고 있다. 해당 년도의 안전관리를 수행한 후에는 국가 안전 수준을 평가하여 차년도 안전 관리에 반영하도록 하여 철도 안전이 연속적으로 관리되도록 하였다.

2. 국가 안전 관리 체계

국가 안전관리체계(National Safety Management System)는 철도변경(신규차량, 신호체계) 및 운영과 관련된 리스크가 수용 가능한 수준으로 줄어든 것을 확인하기 위한 프로세스이다. [그림 1]은 일련의 안전관리 활동과 관련 주체간 상호작용을 보여주는 최상위레벨의 기능흐름도이다. 반복, 변경, 수 차례에 걸친 안전평가와 재작업은 안전관리에서 자연적으로 발생하는 업무방식이나 단순화되어 표시됨에 따라 이런 작업들은 그림에서 보여지지 않는다.



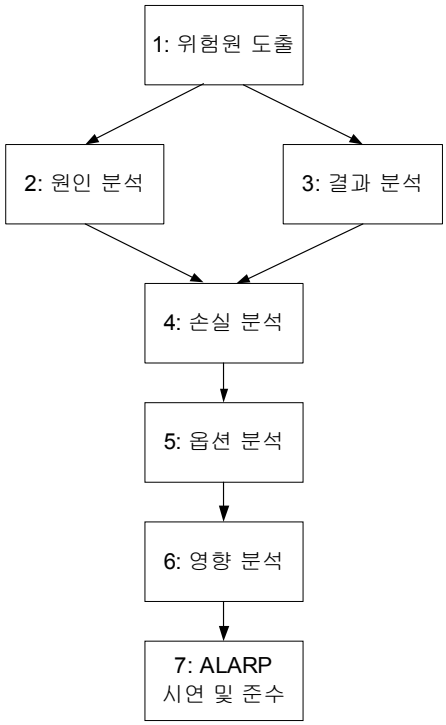
[그림 1] 국가 안전 관리 체계

국가 안전관리체계의 관련 주체로는 당국과 철도 운영기관, 철도차량 및 인프라 관리자, 사고조사위원회, 독립평가기관으로 범위를 설정하였다. 안전 라이프사이클은 국가 철도 안전 수준을 분석함으로써 시작한다. 철도 안전 수준 분석에서는 파악된 위험원 로그에 기초하여 리스크 평가를 진행한다. 리스크 평가 결과로부터 얻어진 현재 철도 안전 수준으로부터 국가 철도 안전 목표를 설정한다. 국가 철도 안전 목표는 철도 운영기관이 세우는 연간 철도 안전 성능 목표에 할당하고, 당국은 제출된 운영기관의 연간 철도 안전 성능 목표를 승인하는 역할을 하게 된다. 그런 다음 안전요구사항을 준비한다. 일단 안전요구사항이 결정되면 국가 안전 계획을 세우게 된다. 국가 안전 계획은 소방방재청의 안전 점검 계획과 안전 요구사항 데이터, 장기 수송안전계획, NSC의 비상사태 계획 등의 데이터를 기반으로 작성하게 되고, 운영기관의 연차 안전 계획과 연동하여 할당하고 승인하는 체계를 갖는다. 그런 다음 안전계획에서 정의된 안전 활동을 실천에 옮긴다. 여러 차례에 걸쳐 제 3의 독립기관에 의한 안전 진단평가를 수행해 볼 수도 있다. 일반적으로 초기단계에 행해지는 평가는 올바른 접근법을 사용했는지를 알아보기 위함이고, 말기단

계에 행해지는 것은 종합안전대책기술서에 사용될 증거를 제공하기 위해 실시된다. 안전관리 활동이 종료되면 운영기관은 종합안전대책기술서를 준비한다. 종합안전대책기술서에 대한 당국의 결재를 받아야 안전승인을 득할 수 있다. 안전승인을 받은 후에는, 시스템에 대한 안전책임이 실제 인프라 관리자와 같은 사용자에게 이전되기도 한다. 안전책임은 운영기간 동안 뿐 만 아니라 작동/작동중지/보관 동안에도 줄곧 지속된다. 당국은 안전 활동을 모니터링하고 평가한 이후에 개선 방향에 대한 결정을 하게 된다.

3. 위험원 도출과 리스크 평가

안전관리체계의 첫 번째 부분은 국가 안전 수준을 평가하는 것이다. 국가 안전 수준은 사고 데이터로부터 위험원을 도출하고 이에 따라서 리스크를 평가함으로써 현재 안전 수준을 식별하도록 하고 있다. 위험원 도출은 안전관리의 기본이다. 위험원을 도출하지 못한다면 이를 제거하거나 이와 관련된 리스크를 줄일 수 있는 어떠한 행동도 취할 수 없다. 그러나 안전여유 도입과 같은 일반적인 행동은 취할 수 있다. 정상 운행 동안에 발생할 수 있는 사고에 대해서만 고려할 것이 아니라 설치, 현장시험, 인수, 유지보수, 응급상황, 사용중지 및 보관 등과 같이 타 시간에 일어날 수 있는 경우도 고려해야 한다. 또한 변경사항이 영향을 미칠 수 있는 사람들을 고려하고 실수를 예방할 수 있도록 설계해야 한다. 위험원을 도출할 때는 철도와 인근에 발생할 수 있는 모든 영향요소를 고려해야 한다. 이와 같이 식별된 위험원에 대해서 리스크를 평가해야 한다. 리스크는 발생할 수 있는 사고와 피해에 대한 가능성을 측정하는 것이다. 이 두가지 요소는 모두 고려되어야 한다. 또한 조직은 누가 영향을 받는지도 고려해야 한다. 리스크 평가에는 위험원 도출과 리스크 감소가 거의 항상 동반된다. 시스템의 위험원은 정확한 리스크 평가가 이루어지기 전에 도출되어야 한다. 시스템이나 장비의 라이프사이클 동안 리스크 평가는 리스크 감소를 위한 입력과 성공에 대한 피드백을 제공해 준다. 리스크 평가는 [그림 2]의 7 단계를 따른다[3].



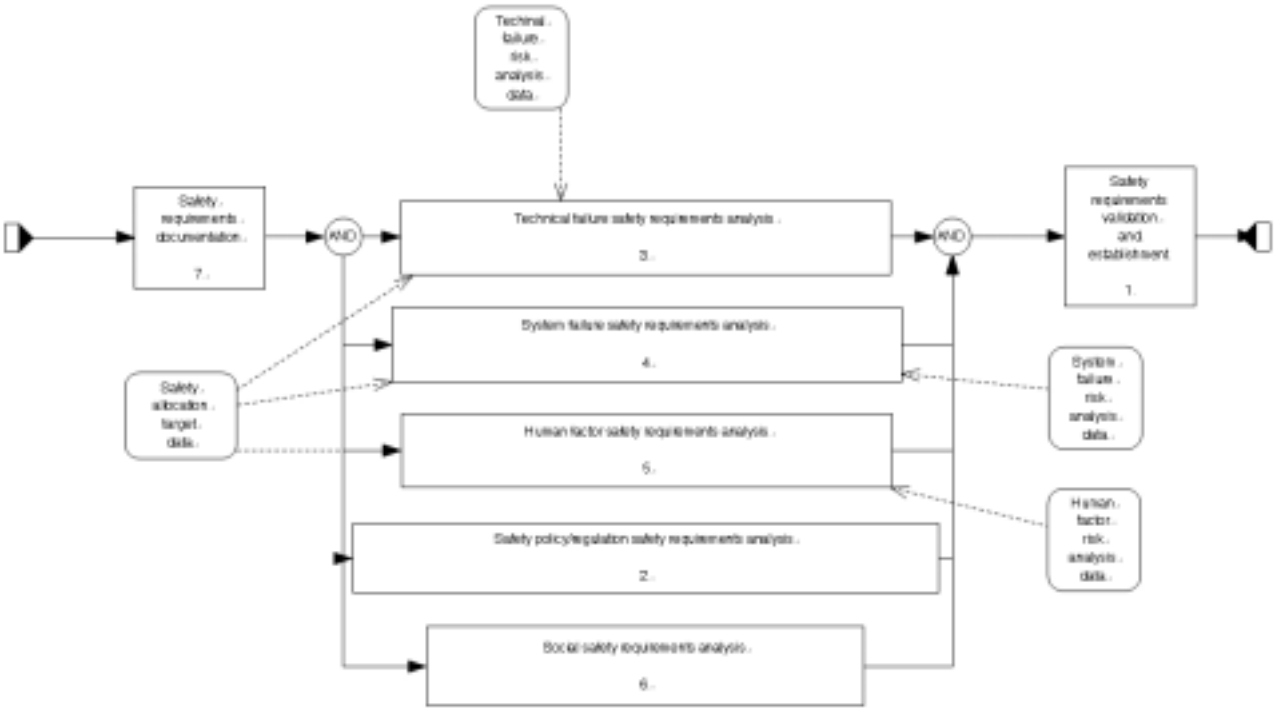
[그림 2] 리스크 평가 단계

위험원 도출은 위험원을 도출하고 순위를 정하는 것을 포함한다. 원인 분석은 위험원을 발생시킬 수 있는 주된 원인요소를 설정하는 것과 각 위험원의 발생 가능성을 추정하는 것을 포함한다. 결과 분석은 위험원으로부터 발생할 수 있는 중간조건과 최종결과를 설정하는 것과 각 위험원으로부터 발생하는 사고 가능성을 추정하는 것을 포함한다. 원인 및 결과 분석은 동시에 실시될 수 있다. 각 위험원에 대한 결과

는 손실의 범위(말하자면, 사람에 대한 손실, 환경이나 영업손실에 대한 피해)와 관련될 수 있다. 손실 분석은 리스크 감소를 위한 옵션을 고려하기에 앞서 안전손실에 대한 크기의 추정을 필요로 한다. 리스크 감소와 관리는 각 위험원에 대한 잠재 리스크 감소 방법들을 파악할 필요가 있다. 옵션 분석은 어떤 방법을 취할 것인지에 대한 결정과 수행 비용 산정을 절충하는 것이다. 영향 분석은 리스크 감소를 위하여 각 리스크 감소방법의 시행으로 발생된 순수효과를 평가하는 것이다. 리스크 감소는 조치들의 효과를 고려하기 위하여 이전 단계를 수정하면서 얻어진다. ALARP은 어떤 리스크 감소 조치가 도입되어야 하는지를 결정하고 나머지 리스크의 수용을 정당화 하는 것을 포함한다.

4. 안전요구사항 도출

안전요구사항은 제시된 안전 리스크가 허용 가능한 수준까지 줄어들었다고 확신할 때까지 계속된다. 주어진 위험원에 대해서는 우선적으로 이를 제거하기 위해 안전요구사항을 적용해야 한다. 이를 수행하는 것이 불가능할 경우에 한하여 시스템 설계에 대해 안전요구사항을 적용해야 한다. 그리고 합리적으로 허용할 수 있는 모든 리스크 감소 노력을 설계에 적용해 본 경우에 한하여 리스크 감소 옵션으로 절차와 교육을 고려해야 한다. [그림 3]은 안전요구사항을 도출하는 프로세스를 나타낸다.



[그림 3] 안전요구사항 도출

안전 요구사항은 정성적이나 정량적으로 표현될 수 있다. 시스템적인 결함이 발생할 수 있는 구성요소에 대한 무결성 요구사항을 만족시키기 위해서는 안전 무결성 레벨을 사용한다. 안전요구사양서는 이런 활동과정에서 얻은 정보를 세부 요구사항으로 통합한 것으로 시스템 안전 테스트와 평가 시 기본을 형성한다. 안전요구사항을 수립하는 활동은 안전 분석의 반복적인 성격을 반영하도록 되풀이하는 것이다.

5. 결론

철도종합안전기술개발사업의 목적은 철도안전 관리체계와 기술기반을 선진국 수준으로 제고하여 급증하는 기술적, 사회적 안전 위협요소에 적극 대응하고자함과 동시에, 철도시스템에 대한 종합 안전대책과 철도안전법의 효율적, 기술적 시행기반을 마련하는데 있다. 본 논문에서는 국내 실정에 맞는 위험도 기반의 안전관리체계 구성 방안에 대한 연구를 수행하였다. 당국, 철도 운영자, 철도 및 시설 관리자, 사고조

사위원회, 독립평가기관의 역할과 상호 인터페이스를 정의함으로써 국가전체의 철도 안전 관리를 위한 시스템을 구축하였다.

6. 참고문헌

1. 조연옥 외(2006), “철도안전 시스템엔지니어링 및 사업총괄”, 한국철도기술연구원.
2. 최요철, 조연옥(2006), “철도종합안전프로젝트를 위한 시스템엔지니어링 적용 체계 연구”, 한국철도학회논문집, 제9권 제4호, pp. 487-492.
3. Rail Safety and Standards Board(2005), "Engineering safety management", Railtrack.