

# 시스템 엔지니어링을 적용한 철도종합안전기술개발사업의 2차년도 성과물 검증 기준 및 결과

## Verification specifications and results of the railway total safety technology development project adopting systems engineering

한순우\*

윤혁진\*\*

신정무\*\*

김상암\*\*

조연옥\*\*

Han, Soon-Woo Yoon, Hyuk-Jin Shin, Jungmoo Kim, Sang-Ahm Cho, Yun-Ok

### ABSTRACT

To establish the national railway safety system, the railway total safety technology development project has been promoted by Ministry of Construction and Transportation (MOCT) since August 2004. The project is mainly focused on the prevention of a critical railway accident and the reduction of accident/mortality rate. To achieve its goal effectively, the project is composed of 15 sub-projects each of which can be categorized into three different technological area. This work deals with the verification results for the outcomes of the sub-projects carried out at the 2nd year of the project. A new verification procedure is developed and applied to the project based on the system engineering. Three criterions - The suitability of the realization of a function, the suitability of a physical structure, the suitability of a design analysis report - are used for the verifications. The verification results are investigated by calculating standard deviations of scores of each results.

### 1. 서 론

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 04년 철도운영공사와 시설공단이 발족됨으로써 철도산업의 구조개편이 완성되었으며, 새로운 구조에서 철도의 안전을 확보하기 위해 정부가 제정한 철도안전법이 05년 10월을 기해 발효되었다. 철도안전법은 시설관리자와 철도의 운영자간 안전 인터페이스를 확보하고, 정부규제 중심의 국가적인 안전관리체계를 시행할 수 있는 법적 근거를 제공하게 된다 [1].

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. 이를 위해 선진국의 경우 국가주도하에 철도안전을 향상하기 위

\* 한국철도기술연구원 안전기술연구팀

E-mail : scarus@krri.re.kr

TEL : (031)460-5565 FAX : (031)460-5509

\*\* 한국철도기술연구원 안전기술연구팀

\*\*\* 한국철도기술연구원 안전기술연구팀 수석연구원, 정회원

한 기술개발에 전략적·집중적으로 투자하고 있다.

이러한 배경 하에 우리나라에서도 더 이상 철도안전기술개발을 현 수준으로 방치할 수 없으며, 선진국 수준의 철도종합안전관리시스템을 확립할 수 있는 기술개발의 필요성이 대두되었다. 이에 건설교통부는 21세기 건강한 선진복지사회를 구현하는 범국가적 철도종합안전체계를 구축하기 위한 종합적이고 체계적인 철도종합안전기술개발사업을 2004년 8월부터 추진하고 있다[2].

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. 그러나 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, 안전성 평가기술 개발, 시험평가기반의 구축, 중대사고 방지기술의 개발 및 안전정보관리체계의 구축 등이 이루어져야 할 뿐만 아니라, 개발된 기술들이 연계되어 종합적인 안전체계 내로 편입되어야 할 필요가 있다. 이를 위해서는 Top-down 방식의 시스템 엔지니어링 기법에 의한 철도시스템 안전요건관리 및 사업관리가 필요하며, 앞에서 언급한 철도종합안전기술개발 사업 또한 이러한 시스템 엔지니어링에 기반하여 추진되고 있다.

시스템 엔지니어링에서 사용되는 도구들은 특히 시스템 요건, 기능, 거동 및 물리적 아키텍처를 비롯하여 안전규정/규격 요건과의 연관성을 정의하고 추적/관리하여 주기 때문에 문제의 정의와 해결책들을 체계적, 효율적으로 관리 할 수 있도록 도와준다[3]. 따라서 시스템 엔지니어링 기법을 사용하여 안전관리체계를 구축하고 사업을 관리하게 되면 복잡한 다제간 철도시스템의 성능 및 안전 기준을 확립하고 위험관리체계를 정착시킬 수 있게 된다. 또한 시스템 엔지니어링 기법은 과제간 성과의 관리 및 사업의 성과물 자체인 철도안전관리체계 내 모든 요소들의 통합적 관리와 이해당사자 간의 참여와 의사소통을 지원함으로써, 철도 시스템 안전계획 수립의 수준을 성숙시키는 데에도 많은 도움을 준다.

시스템 엔지니어링 기법에 있어서 시스템의 요구사항(system requirements)이 제대로 도출되었는지, 이 요구사항들이 시스템 개발 과정에서 제대로 충족되고 있는지를 살피는 것이 매우 중요하다. 이러한 맥락에서 '검증(verification)'이라고 불리는 단계는 필수적이라 할 수 있다. 시스템의 개발자는 검증을 통해서 시스템의 산출물이 의도한 요구 사항을 만족하고 있는지와 운용하고자 하는 환경에서 즉시 사용이 가능한지를 판단할 수 있다[4].

본 논문에서는 2007년 하반기에 마무리되는 철도종합안전기술개발사업의 2차년도 성과물에 대한 검증 기준 및 필요 문서의 도출 과정에 대해 언급하며, 이를 적용한 검증 결과에 대해 서술하려 한다.

## 2. 철도종합안전기술개발사업의 구성체계

서론에서 언급한 바와 같이 철도종합안전기술개발사업은 그 효율적인 추진을 위해 다음과 같이 3개 기술 분야로 나뉜 15개 세부과제로 구성되어 있다 (그림 1 참조). '철도안전체계 구축'이라는 사업의 목적을 달성하기 위해 각 과제별로 해결해야 할 시스템 요구사항을 할당했으며 이 시스템 요구사항에 대해 검증이 이루어진다. 철도사고 위험도 분석 및 평가체계 구축 과제의 시스템 요구사항을 예시하면 다음 표 1과 같다.

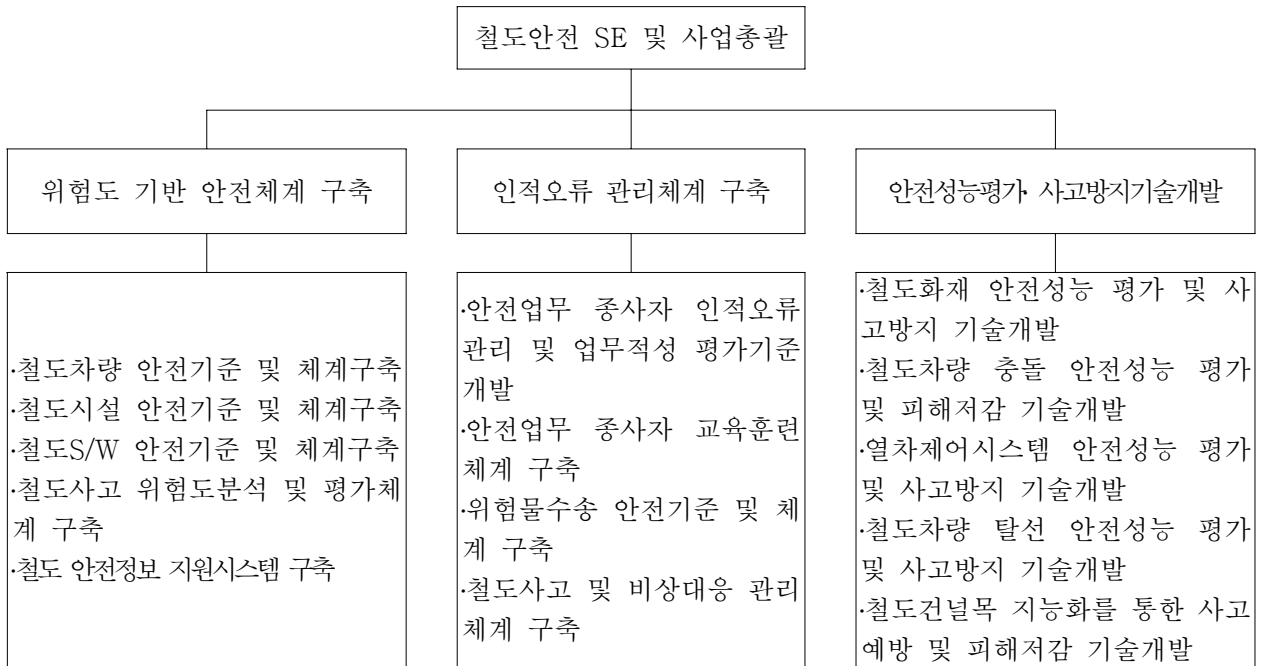


그림 1. 철도종합안전기술개발사업의 추진체계

표 1. 철도사고 위험도 분석 및 평가체계 구축 과제의 2차년도 시스템 요구사항

번호	시스템 요구사항
1	프로젝트는 철도사고 위험요인의 중대사고(충돌, 탈선, 화재 등) 진전기구를 전개해야 한다.
2	프로젝트는 철도사고 유형별 위험확률의 정량평가 기술개발을 해야 한다.
3	프로젝트는 철도사고 유형별 위험요인 진전에 따른 심각도 평가 모델을 전개해야 한다.
4	프로젝트는 철도시스템 안전요건의 변경에 따른 심각도 평가 모델을 전개해야 한다.
5	프로젝트는 철도시스템 위험요인 할당과 안전규정 요건과의 연계성을 부여해야 한다.

위에 예시한 시스템 요구 사항의 각 항목에 대해 검증을 수행하였다.

### 3. 성과물의 검증 기준

설계를 추상적으로 정의하자면 '특정한 목적을 달성하기 위한 대상물 또는 시스템을 고안'하는 것이라 할 수 있다. 특정한 목적을 달성하기 위해서는 그에 합당한 기능을 수행할 수 있어야 하는데 이러한 것들을 기능 요구사항(functional requirement)라고 한다. 이러한 기능 요구조건들을 만족시키기 위해서는 특정한 설계변수(design parameter)들이 있어야 하며 이러한 설계변수로부터 설계 대상물의 물리적 구조가 형성된다[5]. 시스템의 요구 사항을 충족시키기 위해서는 그에 해당하는 기능 요구사항과 설계 변수가 수반되어야 한다.

시스템의 요구사항을 관리함에 있어서 또 하나의 중요한 문서는 설계 분석 보고서(design analysis report)이다. 이는 요구사항에 기준한 결과물마다 작성되어 시스템의 특성 및 해당되는 기능 요구사항을 기술하게 된다. 이 설계 분석 보고서는 시스템 요구사항 별로 작성되며 다음과 같은 내용을 포함하게 된다.

- a. 요구 사항의 목적 및 필요성
- b. 요구 사항의 특성(special characteristics)
- c. 성과물과 요구 사항과의 적합성
- d. 설계기준
- e. 성과물의 내용

본 과제에서는 위에 언급한 세 가지 사항으로부터 다음과 같은 기준을 도출하여 검증에 활용하였다.

- a. 기능실현의 적합성
- b. 물리적 구조(architecture)의 적합성
- c. 설계분석보고서의 적합성

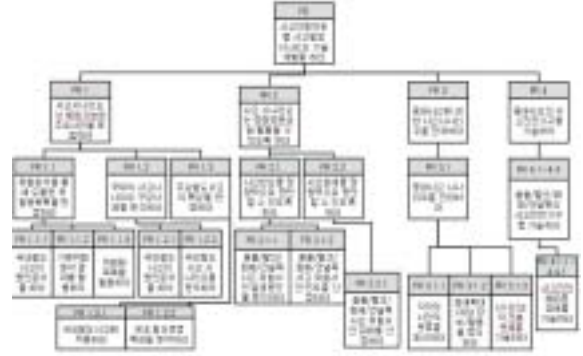
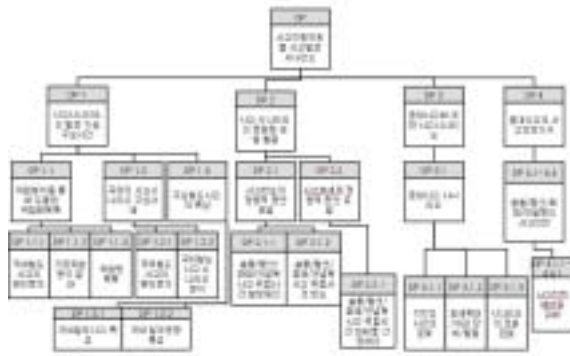
#### 4. 성과물의 검증 절차

본 과제는 ‘동료 검토(peer review)’를 통해 검증을 수행하였다. 각 세부과제 책임자들에게 당사자의 과제를 제외한 다른 3과제의 성과물 평가 자료를 배포하고 각 과제에 대해 평가를 수행토록 하였다. 따라서 과제별로 3명의 동료 검토가 이루어졌으며 검토 결과(항목별 점수)를 취합하여 평균을 계산하였다. 성과물 평가를 위해서 각 과제의 개별 시스템 요구사항마다 아래와 같은 자료를 작성하였다.

- a. 검증계획서 (그림 2 참조)
- b. 기능 구조도 (그림 3(a) 참조)
- c. 물리적 구조도(그림 3(b) 참조)
- d. 설계 분석 보고서

 Process : <b>Verification Plan(검증 계획서)</b>		ID No : Date : Revision Date :
SR-3. 프로젝트는 필요 사고안전 시나리오를 개발해야 한다.		
SR-3.1. 프로젝트는 필요 사고 상황대별 사고발생 시나리오 기술개발을 해야 한다.		
<b>Inputs :</b> - 검증 기술(Verification Technology) - 인터커링 문서, 기록적인 - 기술 개발 계획(Technical Plans) - 연구계획서 - PM(Project Management) - 요구사항 (Requirements) - 요구사항 문서 및 관련논문보고서 (SR재규) - 위험도 관리 VRTRM Templates - 설계정보 및 평가자료 - 사고 시나리오의 기능 아키텍처 - 물리 아키텍처 - 검증기준 (Verification Criteria) - 설계 분야 보고서 (DARs) - 시험 및 인증 자료 (NQA)	<b>Tasks :</b> - SR 검증 업무	<b>Outputs :</b> - 증명 VRTRM - JWCR
<b>Verification Specification (검증기준)</b> - 기능 (Function), 기능실현성의 적합성 (시스템 평가자 검토) - 물리적 구조 (Physical), 물리적 구조의 적합성 (시스템 평가자 검토) - DAR의 적합성, 상황대별 사고발생 시나리오 설계 근거 및 설계의 적합성 (전문가 검토) - 양호 시험 (NQA) - 안전성 시험, 내구성 시험 (NQA)		

그림 2. 검증 계획서의 예



(a) (b)

그림 3. 구조도의 예 (a) 기능 구조도, (b) 물리적 구조도

각 검토자는 위의 자료를 바탕으로 다음과 같은 과제물 검증 결과표를 이용하여 평가를 수행한다.

### 철도종합안전기술개발사업 과제물 검증 결과표

검증영역 소속 : \_\_\_\_\_ 실증 (인)

검증 과제명	철도사고 위험도 분석 및 평가체계 구축
DR	3 프로젝트는 철도 사고관련 시나리오를 개발해야 한다.
DR	51 프로젝트는 철도사고 진행단계별 사고발생 시나리오 기술개발을 해야 한다.

해당 평가 등급에 ✓ 표시 해주시기 바랍니다.

평가 항목	평가 등급				
	A	B	C	D	E
해당 성과를 검증할 위한 검증 방법은 적절히 선택되었는가					
업무분담구조 (WBS) 에 해당 작업을 위한 자원과 일정은 적절하게 할당되고 관리되었는가					
검증기준 1: 기능 설명의 적합성					
성도품이 가져야할 기능이 충실히 잘 표시되어 있는가					
기능적 솔루션의 레벨은 잘 정의되어 있는가					
검증기준 2: 물리적 구조의 적합성					
성도품의 물리적 구조가 충실히 잘 표시되어 있는가					
선택된 DR는 해당 DR을 만족시킬 수 있도록 적절하게 선택되었는가					
검증기준 3: 설계분석보고서의 적합성					
구현된 성과물은 요구사항을 충분히 반영하고 있는가					
성도품의 설계근거는 잘 표시되어 있고 적정인가					
성도품은 특장적인 특징을 지니고 있는가					
성도품의 내용이 잘 표시되어 있는가					
기타 의견					

A : 100점, B : 80점, C : 60점, D : 40점, E : 20점. 각 항목 균등 배점

그림 4. 시스템 요구 사항 검토를 위한 검증 결과표 예

## 5. 성과물의 검증 결과

앞에서 언급한 검증 기준 및 절차를 바탕으로 15개 전 과제의 모든 시스템 요구사항에 대해 검증을 수행하였으며, 각 과제마다 시스템 요구사항 별로 평균을 구하여 3절에서 언급한 검증 항목별로 나열하였다. 그림 5에는 그 예를 나타내었는데 이는 과제간의 상대적 점수를 비교하지 않은 채 원점수만을 나타내었다.

그러나 검증 결과를 보다 의미있게 만들기 위해서는 위와 같은 원점수의 계산보다는 동일 검증 항목에 대해 여타 과제들과의 비교를 통한 상대 평가를 수행하는 것이 필요하다고 판단된다. 이에 최종적으로는 각 항목에 대해 검증 기준별로 표준 점수를 구하여 보았다 (그림 6 참조). 이를 보면 이 세부 과제의 시스템 요구 사항 9.1 항목은 기능실현 및 설계 분석 보고서의 적합성 항목에서는 평균 이상의 평가를 받았으나 물리 구조의 적합성은 매우 낮은 평가를 받았음을 알 수 있다. 이와 같은 과정을 통해 각 세부 과제 책임자들은 자신들의 과제 성과물들이 어떠한 평가를 받았는지, 향후 과제를 수행함에 있어서 어떠한 부분을 극복해야 하는지에 대해 확실한 판단 근거를 갖게 된다.

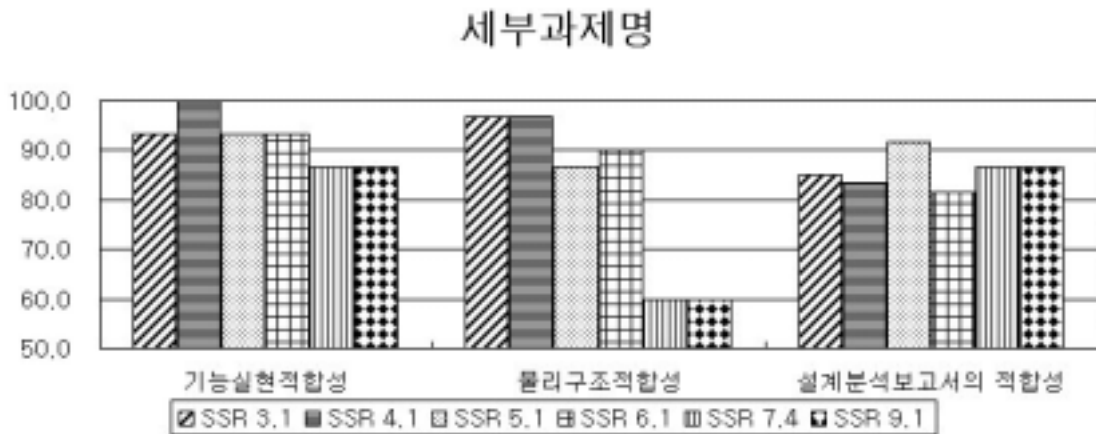


그림 5. 검증 결과의 예

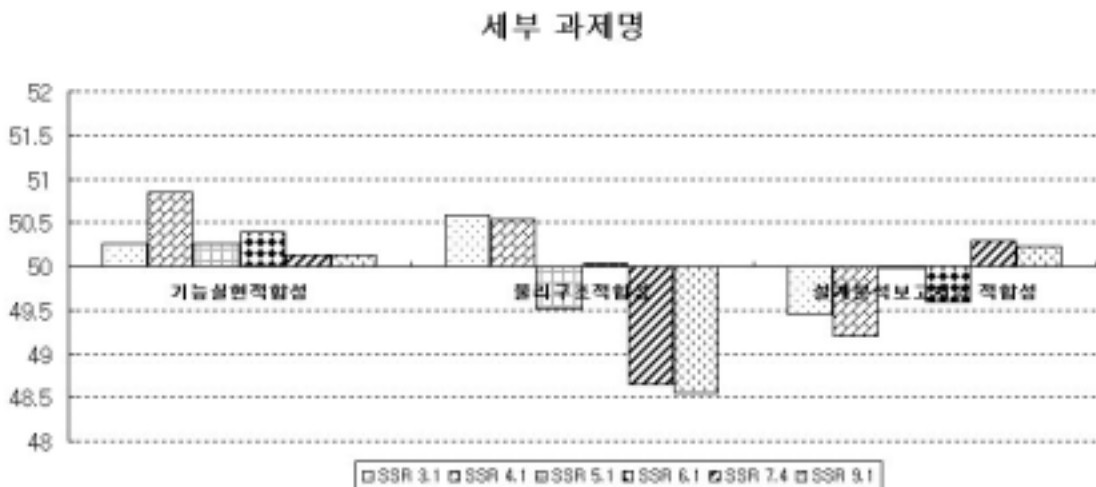


그림 6. 표준 점수화된 검증 결과의 예

## 6. 결 론

본 논문에서는 철도종합안전기술개발 사업의 2차년도 연구 성과에 대한 검증 기준과 그 결과에 대해 논의하였다. 본 사업은 시스템 엔지니어링 기법을 준용하여 추진되고 있으며 이에 있어서 필수적인 검증 절차를 위해 별도의 성과물 검증 프로세스를 차용하였다. 과제별로 설정된 시스템 요구사항 별로 기능실현의 적합성, 물리적 구조의 적합성, 설계분석보고서의 적합성을 검증 기준으로 삼았으며, 검증 계획서, 기능 구조도, 물리적 구조도, 설계분석 보고서 등을 토대로 동료 평가 체계를 통해 성과물을 검증하였다. 검증 결과는 표준 점수화되어 상대 비교를 통해 우수한 부분과 향후 보충해야 할 부분을 구분하였다. 이러한 검증을 통해 본 사업이 최종적으로 보다 우수한 결과물을 산출할 수 있으리라 여겨지며, 우리나라의 철도안전체계를 보다 확고하게 만들 수 있으리라 판단된다.

## 참고문헌

- (1) 건설교통부(2006), “제1차 철도안전종합계획 : 2006-2010”,
- (2) 건설교통부(2006), “철도종합안전기술개발사업 2차년도 중간보고서: 철도안전 시스템 엔지니어링 및 사업 총괄 연구보고서”, 연구보고서.
- (3) B. S. Blanchard and W. J. Fabrycky(2006), "Systems Engineering and Analysis", 4th ed., Prentice Hall.
- (4) Federal Aviation Ministration(2006), "NAS system engineering manual,"
- (5) 차성운, 박경진(2002), “공리적 설계”,동명사