

# 철도종합안전기술개발사업의 성과물 검증 프로세스 구축

## Construction of verification process for the railway total safety technology development project

윤혁진\*      한순우\*      김상암\*      최경진\*\*      조연옥\*\*\*  
Yoon, Hyuk-Jin   Han, Soon-Woo   Kim, Sang-Ahm   Choi, Kyung-Jin   Cho, Yun-Ok

---

### Abstract

Recently, many organizations such as, including government, railroad operational, railroad facilities management and research authorities have made a lot of efforts to identify and prevent hazards from leading to accidents and solve them all over the railroad industry. Railroad total safety technology development project conducted as one of national R&D projects has established business formation structure based on system engineering as an effort to define and give a solution to facing problems in the field of railroad. This paper is building procedures to verify the outcomes derived from this project. The verification process is the one for verifying the outcome produced in the final stage of the project or during the project. It makes sure that the system is satisfying the system requirements through verification of the outcomes produced after conducting the project for verification. We've made verification plan for technically reasonable verification using verification process developed through this research, and established master verification plan in the level of 15 detailed projects for interim and final outcomes produced.

---

### 1. 서론

철도산업의 구조개혁으로 건설주체와 운영주체가 분리됨에 따라 국가적인 안전관리체계를 구축하고 효과적으로 안전을 규제할 조치가 절실히 필요하게 되었다. 현재 수립중인 철도 종합안전대책과 철도안전법 시행을 효율적, 기술적으로 뒷받침하여 선진국 수준으로 철도사망사고율을 저감하여야 하나 그 동안 투자가 미흡했던 것이 사실이다. 현재 일본에 비해 인·km 당 사망자수는 9배 수준이며, 100만 km 당 중대열차사고율도 거의 2배 수준이다. 따라서 많은 인명 손상을 가져올 수 있는 화재, 충돌, 탈선 등 대형사고 위험요인을 사전에 제거하고, 사고 발생시 피해를 최소화할 수 있는 안전기술 개발 및 연구기반이 절실히 필요한 실정이다. 또한 고속철도를 운행하고, 철도건설이 확대됨에 따라서 철도차량, 시설 및 철도종사자에 대한 안전관리도 더욱 체계적으로 강화할 필요성이 제기되었다[1, 2].

이러한 문제점을 해결하기 위하여 국가에서는 선진국 수준의 범국가적 철도종합안전시스템을 구축하기 위하여 2004년 10월부터 2011년 8월까지 948억원을 투자하여 철도종합안전기술개발사업을 시행하고 있다. 이 사업에서는 철도안전법의 효율적 시행기반을 마련하기 위한 기술기준과 철도 안전성능 평가 및 중대사고 방지기술을 개발하고 있다. 15개 과제들에서 개발되고 있는 안전기준과 안전기술들은 철도 종합안전시스템이라는 대형 시스템의 요소와 하부 시스템들로서 상호 밀접한 인터페이스를 요구한다. 따라서 주어진 기간 내에 주어진 비용으로 내부적인 마찰을 균형있게 조정하여 최적의 시스템을 만들 수 있도록 사업에 맞는 시스템 엔지니어링 체계를 구축하여 운영하고 있다. 아직은 본 사업에서 도출되고 있는 성과물들이 요구사항을 잘 만족시키고 있는지 검증하는 체계가 완벽하지 않으며, 요구사항 관

---

\* 한국철도기술연구원 안전기술연구팀 선임연구원, 정희원  
E-mail : scipio@krri.re.kr

\*\* 한국철도기술연구원 안전기술연구팀 책임연구원, 정희원

\*\*\* 한국철도기술연구원 안전기술연구팀 수석연구원, 정희원

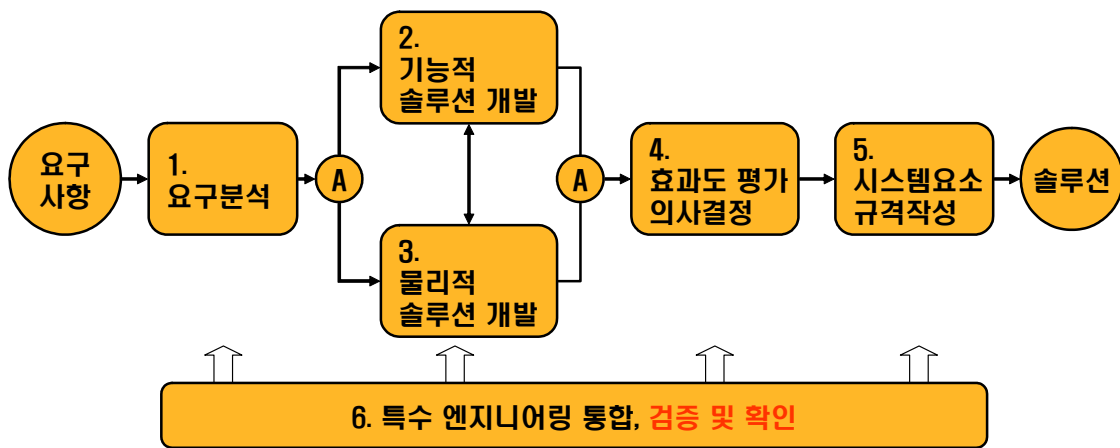
리 이외에도 성과물과의 검증을 연계시키는 체계 구축이 필요하다.

본 논문에서는 사업 성과물의 검증을 위해서 시스템 엔지니어링 검증 프로세스를 구축하였다. 성과물 검증 프로세스는 프로젝트를 수행하고 난 이후에 발생하는 성과물에 대한 검증을 통해 확정된 시스템요구사항을 만족하고 있는지를 확인하게 해준다. 본 연구를 통해서 개발된 성과물 검증 프로세스를 활용하여 기술적으로 타당한 검증을 위한 성과물 검증 계획서를 작성하였으며, 산출되는 중간 및 최종 성과물에 대한 15개 세부 과제차원의 종합적인 검증 계획을 수립하였다. 성과물에 대한 검증기준과 검증방법을 제시하였으며, 요구사항과의 추적성 확보를 위해서 검증 요구 사항 추적 매트릭스(VRTM)를 작성하였다.

## 2. 사업 성과물 검증 체계

검증은 적용 가능한 요구사항들이 만족되었는지를 확인하기 위하여 완성 시스템을 평가하는 것을 의미하며, 시스템 요구사항을 만족시키는데 있어서 진척도를 평가하고 변화하는 시스템 제품들 및 프로세스들의 효과성을 측정하기 위하여 요구되어지는 시스템 구성요소들이 수행하는 모든 과업, 행위, 그리고 활동들의 복합체이다.

검증 프로세스는 설계 솔루션이 시스템 요구사항들을 만족시키고 시스템이 운영 환경 내에서 그것이 의도한 대로 사용될 준비가 되어 있다는 것을 보증한다. 이는 검증된 시스템이 임무 필요, 성능, 인터페이스, 이해관계자 필요들을 달성하는 설계에 따르는 지를 시연할 수 있다는 것을 의미한다. 검증 프로세스(그림 1)는 진보적 연구 및 예비적인 분석들을 위한 개념으로부터 설계 및 개발, 생산의 완결, 제품 수락, 운영, 그리고 폐기 단계에 이르기까지 시스템의 생명주기의 모든 수준에 대해 시스템 발달을 지원한다.



[그림 1] 시스템 엔지니어링 기본요소

[그림 1]은 요구사항으로부터 솔루션을 얻는데 있어서 거쳐야할 시스템 엔지니어링 프로세스를 나타내며, 검증 프로세스는 요구분석에서부터 시스템 요소 규격 작성에 이르기까지 전 부분에 걸쳐서 수행될 수 있다[3]. 본 사업에서는 중간 혹은 최종 솔루션이 시스템 엔지니어링 프로세스를 따라서 수행되었고, 그 결과 요구사항을 잘 만족시키는지 여부를 판단하는데 주안점을 두고 체계가 구축되었다. [그림 2]는 본 사업에서 구축된 검증 계획서를 보여준다. 성과물의 검증을 위한 입력 자료로서는 검증기술, 기술개발계획, 요구사항, 설계정보 및 평가자료를 요구한다. 입력물인 검증기술은 3절에서 다루어질 검증방법들을 포함한다. 통합 기술 계획 프로세스를 통해서 개발되는 기술 개발 계획들은 검증의 시간적 조절과 절차를 포함하여 프로그램을 실행하기 위해 전체 비전을 상세하게 서술한다. 검증을 적절하게 수행하기 위해서 필요한 기술 개발 계획서들은 연구계획서, 종합검증계획서, PM, 과제 아키텍처를 포함한다. 요구사항 문서들은 요구사항 관리 프로세스의 출력물로서, 규제 기관 및 법에 의한 요구사항들뿐만 아니라, 고객 운영 요구사항들을 포함한다. 설계정보 및 평가자료는 제품 형상을 이해하는데 필수적이며, 기능 아키텍처, 물리 아키텍처, 검증기준, 설계분석보고서, 시험 및 입증 자료를 포함한다.

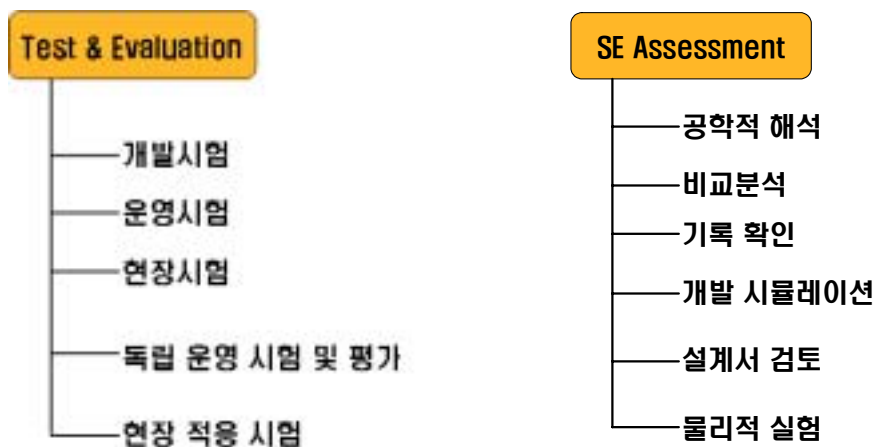
Process : <b>Verification Plan(검증 계획서)</b>		<b>ID No : SW-SR01-SSR03-VP-2005</b> Date : 9. 6. 2006 Revision Date :
SR : 1. 프로젝트는 철도분야 안전핵심 소프트웨어의 안전기준을 제시해야 한다.		
SSR : 1.3 프로젝트는 철도 소프트웨어 안전성 수명주기별 관리기준안을 제시하여야 한다.		
<b>Inputs :</b> - 검증 기술(Verification Technology) - 엔지니어링 분석, 비교검증 - 기술 개발 계획(Technical Plans) - 연구계획서 - MVP(종합검증계획서) - PM(Project Management) - 철도 소프트웨어 과제 Architecture - 요구사항 (Requirements) - 요구사항 문서 및 관련논증보고서 (SE제공) - 철도 소프트웨어 과제 VRTM Templates - 설계정보 및 평가자료 - 안전 관리기준의 기능 아키텍처 - 물리 아키텍처 - 검증기준 (Verification Criteria) - 설계 분석 보고서 (DARs) - 시험 및 입증 자료 (N/A)	<b>Tasks :</b> - SE 검증 업무	<b>Outputs :</b> - 수정 VRTM - RVCD
<b>Verification Specification (검증기준):</b> - 기능 (Function) : 기능실현성의 적합성 (시스템 평가자 검토) - 물리적 구조 (Physicals) : 물리적 구조의 적합성 (시스템 평가자 검토) - DAR의 적합성 : 안전관리기준(안) 설계 근거 및 설계의 적합성 (전문가 검토) - 성능 시험 (N/A) - 안전성 시험, 내구성 시험 (N/A)		

[그림 2] 검증 계획서

이와 같은 입력물들을 바탕으로 검증 팀이 SE 검증 업무를 담당하게 되며, 검증 결과로는 업데이트된 검증 요구사항 추적 매트릭스(VRTM)와 요구사항과의 검증 적합성 문서(RVCD)가 생성된다.

### 3. 검증 방법

검증 방법으로는 [그림 3]에 제시된 것과 같이 시험 및 평가 그리고 시스템엔지니어링 판단의 크게 두 가지 방법을 사용하였다[4].



[그림 3] 검증 방법

#### 3.1 시험 및 평가 검증(Test and Evaluation Verification)

시험 및 평가 검증 프로그램은 다음사항을 위해서 구성된다.

- 의사결정을 지원하기 위해 필수적인 정보를 제공한다.

- 기술 및 획득 위험을 평가하기 위해 필수적인 정보를 제공한다.
- 기술적 성능 규격서 및 목적의 달성을 검증한다.
- 시스템이 시스템의 의도된 목적에 맞도록 운영상 효과적이고 적합한지를 검증한다.

각 획득 관리 시스템 수명주기 단계에 따라 시험 및 평가 검증의 목적은 잠재적인 운영 위험을 경감시키고 그 단계에 적절한 시스템 성능을 시연할 수 있도록 하기 위함이다. 정량적인 기준은 획득 관리 시스템을 통해 진행되도록 하기 위해 하드웨어, 소프트웨어, 그리고 시스템 성숙을 위한 실제의 증거를 제공한다. 각 시험 및 평가 검증 단계는 다음 단계에 들어가기 전에 만족되어진 특정 마일스톤(입력 및 출력 기준)을 가지고 있어야 한다.

시스템 성능은 실제적인 운용 조건하에서 시험을 통해서 검증되는 것이 매우 바람직하다. 그러나 이러한 조건들은 시스템이 배치되고 난 후에야 가능하다. 배치에서 들어난 문제점들은 많은 비용을 들여 수정된다. 그러므로 조사, 분석, 그리고 시험의 조합은 초기에 문제점을 발견하기 위해서 프로그램 배치 기간에 종종 사용된다. 그것에 의하여 위험이 감소되고 성공적이며, 비용-효과적인 프로그램을 보증하는데 도움을 준다.

규격서에서 각 요구사항의 준수는 하나 이상의 방법을 검증 요구사항 추적 매트릭스(Verification Requirement Traceability Matrix[VRTM])에 나타난 것과 같이 검증되어야만 하며, 시험 및 평가 검증 방법들은 다음사항을 포함한다.

- **시연을 통한 검증(Verification by Demonstration)** : 이 방법은 특정한 시나리오 하에서 설계되어 기능을 수행하는 운영, 조정, 재형상을 통해 달성되는 검증을 포함한다. 이 방법은 실제적인 시연으로부터 요구사항의 준수를 검증하기 위해 사용된다. 엔지니어들에 의해서 이루어지는 관찰은 요구사항에 기반을 두고 사전에 결정된 응답과 비교된다. 이 검증 방법의 예로서는 정해진 상당한 시간 내에서 열차 비상시 비상대응 체계 시연이다. 시연은 서비스, 신뢰성, 유지보수성, 수송성, 그리고 인간공학 엔지니어링에 관한 요구사항들과의 준수를 검증하기 위해서 종종 사용된다.
- **시험을 통한 검증(Verification by Test)** : 이 방법은 기구가 있는지 없던지 적절한 조건하에서 적용 요소의 수집, 분석, 그리고 정량적인 데이터의 평가를 통해서 달성된다.
- **분석을 통한 검증(Verification by Analysis)** : 이 방법은 기술적 또는 수학적 평가, 수학적 모델 또는 시뮬레이션, 알고리즘, 차트, 회로 다이어그램, 그리고 대표적인 데이터를 통해서 달성된다.
- **검사를 통한 검증(Verification by Inspection)** : 이 방법은 실험실의 장비 또는 절차를 사용하지 않고 요구사항과의 일치치를 확인하기 위해서 아이템의 시각적인 검사, 서술적인 문서의 검토, 그리고 사전에 결정된 표준과의 적절한 특성들을 비교함으로써 달성된다. 조사는 일반적으로 비파괴적이며 시력, 청력, 후각, 촉각, 그리고 미각의 감각을 사용한다. 간단한 물리적 조종이나 기계적 및 전기적 측정 및 측량, 그리고 다른 조사 방법들을 포함한다. 조사는 구조 특징, 기량, 면적, 품질, 그리고 청결, 설치, 그리고 마무리 손질과 같은 물리적 조건뿐만 아니라 시스템의 물리적 설계 특징들을 종종 검증한다. 조사는 문서의 검토, 시스템 서술서, 그리고 사전에 결정된 표준과 실제적인 시스템을 비교하기 위한 다른 자료들을 포함하기도 한다.

### 3.2 시스템엔지니어링 판단을 통한 검증(Verification by Systems Engineering Assessment)

시스템엔지니어링 판단을 통한 검증은 시스템 최종제품이 시스템 요구사항을 만족시키는지 검증하기 위해 필요한 제품 및 서비스, 그리고 프로세스의 개발을 지원하기 위해서 수행된다. 검증 판단은 검증 요구사항 및 솔루션 대안을 위한 기준, 개념의 증거를 시연하기 위한 검증의 정의, 그리고 개발, 자격, 수락, 적절한 운영, 그리고 다른 시험에 대해 다루게 된다. 판단은 중대한 검증 방법 및 프로세스(분석을 통한 검증에서 사용된 중요 방법 및 가정 그리고 데이터의 검증 등)를 검증하기 위해 필요한 요구사항들과 절차들을 또한 고려한다.

검증 판단은 종합검증계획서(MVP)와 검증 활동의 결과로부터 얻어진다. 통합 기술 계획 프로세스에 따르면, MVP의 목적은 시스템 규격서의 요구사항을 만족시키는 시스템의 능력을 시연하는 모든 검증활동을 정의하는 것이다. 이러한 활동들은 충분한 데이터가 할당된 시간의 틀 내에서 최소한의 비용으로

제공되는 가를 보증하기 위해서 완전히 통합되어야만 한다. 제품 개발, 시험, 그리고 평가를 거쳐 검증 데이터의 지속적인 피드백은 위험을 줄이고 초기에 문제를 발견하기 위해서 필요하며, 최종목적은 생산 및 운영상 사용 전에 모든 요구사항들을 만족시키는 시스템 능력을 완벽하게 검증하는 것으로 시스템엔지니어링 판단 방법은 다음사항을 포함한다.

- **공학적 해석(Verification by Engineering Analysis)** : 이 프로세스는 시스템엔지니어링 분석, 특수 엔지니어링, 통계적 및 정량적 분석, 시뮬레이션, 그리고 모델링 등의 기술을 포함한다. 엔지니어링 분석은 시험이 타당하지 않을 때, 비교분석이 적용 불가능할 때, 그리고 조사가 부적절할 때에 사용된다.
- **비교분석(Verification by Similarity)** : 이 프로세스는 유사한 시스템의 시험 데이터, 형상, 그리고 적용례를 검토하여 요구사항에 준수하는지를 판단한다. 이 방법은 시스템의 설계 및 제조가 유사하고, 이전의 시스템이 동등하거나 그 이상의 규격서를 가지고 있을 때 사용된다.
- **기록 확인(Validation of Records)** : 이 프로세스는 시스템의 특징 및 요구사항들을 검증하기 위해 최종제품의 수락단계에서 제조 기록들을 검토한다.
- **개발 시뮬레이션(Simulation)** : 이 프로세스는 시스템의 모의실험용 모델을 사용하여 설계 특징, 시스템 거동, 그리고 성능을 검증한다.
- **설계서 검토 (Review of Design Documentation)** : 이 프로세스는 획득 검토, 설계 검토, 그리고 다른 평가로부터 나온 보고서 및 설계도면과 같은 설계 문서의 검토를 사용한다.
- **물리적 실험(Physical Examination)** : 이 프로세스는 미리 제정된 기준에 따라 물리적 아이템 또는 형상을 시각적으로 면밀하게 살핌으로서 요구사항에 준수하는지를 판단한다.

#### 4. 검증 요구사항 추적 매트릭스(VRTM) 개발

각각의 요구사항을 검증하기 위하여 사용된 전략 또는 방법을 요구사항과 추적성을 갖도록 하기 위해서 검증 요구사항 추적 매트릭스(VRTM)를 작성하였다. VRTM은 각각의 요구사항 (기능 요건, 성능 요건, 설계 요건 등)이 검증되는 방법, 검증과정이 수행되어야 하는 단계 및 적용 가능한 검증의 수준을 정의한다. [그림 4]는 본 사업을 위해서 작성된 VRTM의 예이다.

과제명		철도건널목 지능화를 통한 사고예방 및 피해저감 기술개발					
SR6		프로젝트는 건물목 시인성 평가용 검지장치를 개발해야 한다.					
	SSR	성과물	성과지표	검증 방법	활용방안	관련위험원	비고
2차년도 (2005)	건널목 시인성 평가기법 개발	시인성 평가기법	건널목의 시인성 평가기법의 적정성	공학적해석	SSR2를 위한 기본자료로 활용 건교부, 건설기관, 운영기관, 안전심사기관, 철도사고조사위원회 직접 사용	건널목-04,07	
	건널목 시인성 평가용 검지장치 개발	시인성 평가장치 철도건널목 시인성 평가 장치의 사용자 매뉴얼	건널목의 시인성 평가용 검지장치의 적정성	설계서검토 Test & Evaluation(Operational Test)	건교부, 건설기관, 운영기관, 안전심사기관, 철도사고조사위원회 직접 사용	건널목-04,07	

[그림 4] 검증 요구사항 추적 매트릭스(VRTM)

SR(System Requirements)에 따라서 성과물과 성과지표, 검증방법, 활용방안을 표시하도록 되어있으며, 작성된 VRTM은 검증종료 후에도 내용이 업데이트 되어 요구사항과 검증결과가 항상 추적성을 유지하도록 구성되어 있다.

## 5. 결론

철도종합안전기술개발사업의 성공적인 수행을 위해서는 사업 성과물들이 요구사항을 잘 만족시키고 있는지 검증하는 체계 구축이 절실히 필요하다. 본 논문에서는 사업 성과물의 검증을 위해서 시스템 엔지니어링 검증 프로세스를 구축하였다. 성과물 검증 프로세스는 프로젝트를 수행하고 난 이후에 발생하는 성과물에 대한 검증을 통해 확정된 시스템요구사항을 만족하고 있는지를 확인하게 해준다. 본 연구를 통해서 개발된 성과물 검증 프로세스를 활용하여 기술적으로 타당한 검증을 위한 성과물 검증 계획서를 작성하였으며, 검증 계획서의 입력물인 검증방법과 검증 요구사항 추적 매트릭스에 대해서 상세히 서술하였다. 구축된 검증 프로세스는 사업 성과물의 수준을 향상시키고, 효과적인 철도종합안전시스템을 구축하는데 일조할 것으로 생각된다.

## 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. INCOSE SEH Working Group (2006), "시스템엔지니어링 핸드북", 시스템체계공학원.
4. Air traffic organization(2004), “National Airspace System - system engineering manual”, Federal Aviation Administration.