J. Korea Saf. Manag. Sci. Vol. 15 No. 1 March 2013
http://dx.doi.org/10.12812/ksms.2013.15.1.51

ISSN : 1229-6783 (Print)
ISSN : 2288-1484 (Online)

철도시스템 개발에서 시스템 안전성을 고려한 설계검증 프로세스의 개선에 관한 연구

심 상 현* · 이 재 천*
*아주대학교 시스템공학과

On the Improvement of the Design Verification Process for the Development of Railway Systems with Systems Safety Considered

Sang-Hyun Sim* · Jae-Chon Lee*
*Dept. of Systems Engineering Ajou University

Abstract

As the human demand or desire on brand new systems otherwise equipped with new functions grows drastically, so does the complexity of the systems. With this trend, the systems are becoming bigger in scale and at the same time the safety requirements are more stringent in the development. Typical systems examples in such a situation may include high-speed railway systems, aero and space systems, marine systems, etc. Failure of those systems can cause serious damages on both the human being and wealth with social infrastructure. As such, it is quite necessary to ensure that the safety requirements be satisfied in the system development. To achieve this need, there could be a lot of solutions to take. In this paper, regarding safety, a special attention is given to the verification phase process, which is one of the intermediate phases of whole systems development process. More specifically, the ultimate concern is placed on how to carry out the design verification while ensuring the safety requirements. To do so, some improvements in the verification phase were proposed first. Then, the outcomes were combined with the systems safety process by generating an integrated process model to reach the goal. As a case study, application to a railway system was discussed, where strict safety requirements are usually necessary. It would be expected that the potential likelihood of failure with rail systems could be reduced if the results obtained are used effectively with some enhancement from further study.

Keywords : Systems Design Process, Systems Safety Process, Safety Analysis, Systems Engineering, Design Verification Process, Railway Systems

† 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2012R1A1A2009193)

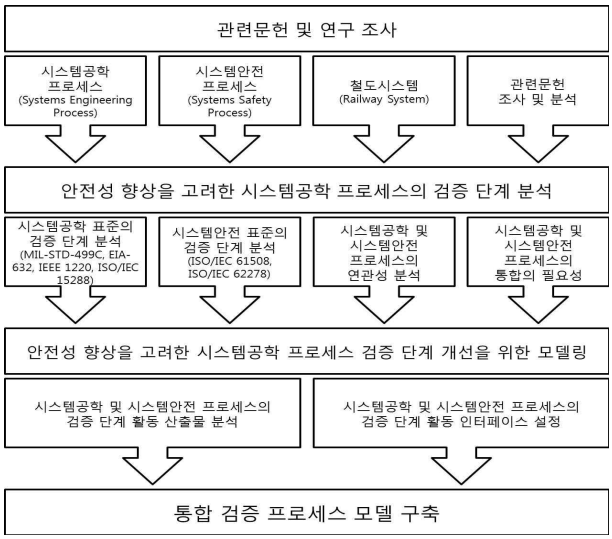
† Corresponding author: Prof. Jae-Chon Lee, Dept. of Systems Engineering, Ajou University, San 5, Woncheon, Yeongtong-Gu, Suwon, 443-749. Tel: 031-219-3941, E-mail: jaelee@ajou.ac.kr
Received January 20, 2013; Revision Received March 6, 2013; Accepted March 11, 2013.

1. 서 론

철도 및 항공 등 전기, 전자 부품 또는 장치들이 복합적으로 포함된 안전중시 시스템(Safety-Critical System)은 시스템의 고장이 치명적인 재난의 원인이 되어 사람의 생명과 밀접한 관계가 있거나, 심각한 손실 또는 재난을 주거나, 환경 파괴를 가능하게 하는 시스템들을 말한다. 사회기반 시설인 철도시스템은 고장 시 열차충돌 및 탈선 등 심각한 상황을 초래하기 때문에 개발 시부터 안전성 관리를 수행하는 정형적인 방법과 장애 복구 기능 등에 대하여 국제 표준 규격을 사용하여 적용하기를 요구하고 있다[1]. 최근 '의정부 경전철'의 사고(2012) 소식과 대형 시스템에 의한 고장, 사고로 인하여 시스템의 안전 설계에 대한 고려 부족으로 인한 시스템 안전 설계에 대한 요구가 증가하고 있다. 이러한 특성으로 인하여 시스템 설계 프로세스 전반에 걸쳐 안전성 확보에 대한 검증을 효과적으로 할 수 있어야 한다[2].

최근 국제사회에서는 ISO/IEC 등의 각종 규제규격 준수나 국제적인 인증을 요구하고 있다[1]. 따라서 시스템 설계 프로세스와 안전성 확보를 위한 프로세스가 중첩해서 적용이 되어야 하는 실정이다. 특히 철도시스템의 경우 시스템의 안전성을 확보하기 위한 시스템공학 프로세스를 통한 체계적인 프로세스가 필요할 뿐만 아니라 이를 기반으로 시스템의 수명주기 단계마다 안전성을 평가해야 한다[3]. 이러한 안전성 평가 방법을 시스템공학, 시스템안전 분석, 그리고 인간 요소를 기반으로 한 통합 시스템 설계 방법을 개발한 연구가 있었으나, 기능 중심의 위험원 분석 활동에 주로 초점이 맞춰져 있다[3]. 또한 IEC 61508은 국제 기능 안전 표준 규격으로서 시스템안전 프로세스에 관하여 언급하고 있으나 확률론적, 정량적 접근에 한정된 신뢰성공학의 배경이 강하다[4][5].

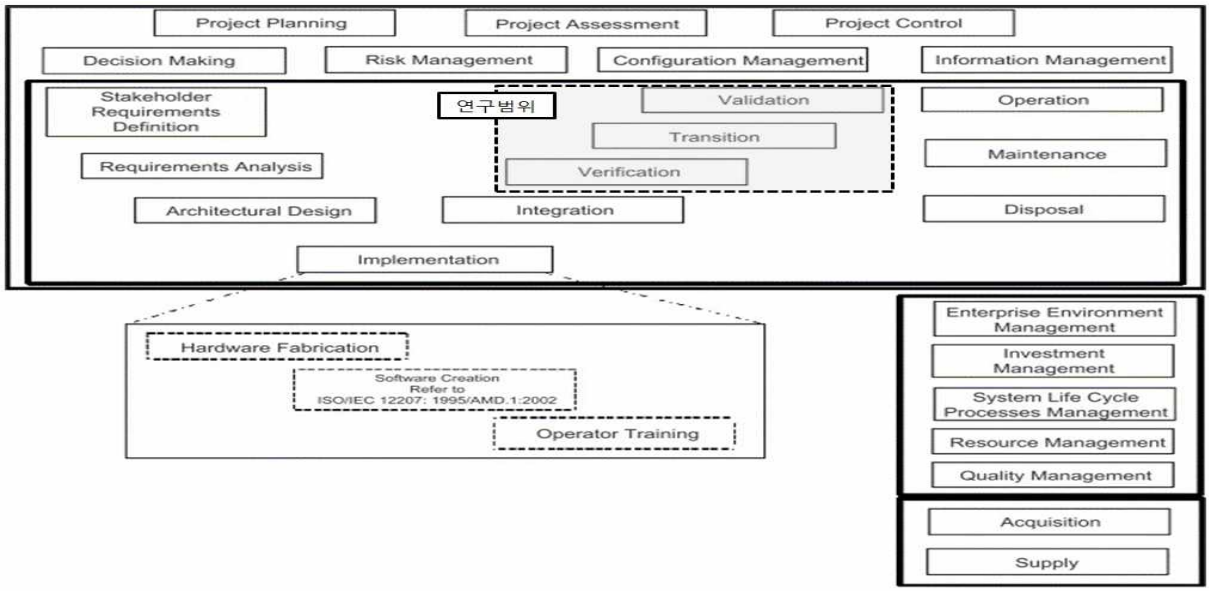
하지만 기존 연구를 통해서는 검증 단계에서의 시스템공학 프로세스와 시스템안전 프로세스의 수행에 따라 발생하는 데이터의 유기적인 상호 활동이 부족하다고 여겨진다. 이는 시스템공학 활동과 시스템안전 활동을 별개로 보는 관점으로 인해 발생하는 문제점이다. 따라서 시스템공학 활동과 시스템안전 활동을 통합하여 구축함으로써 시스템의 수명주기를 고려한 설계와 더불어 안전성 평가 활동까지 동시에 진행함으로써 시간과 비용을 줄일 수 있다. 다만 특정 대상 시스템에 따라 안전성 평가 활동 및 수치적 표현에 있어 어려움을 겪을 수 있기 때문에 대상 시스템에 맞게 프로세스를 수정하여 적용해야 할 필요가 있다[6].



<Figure 1> A conceptual diagram representing the objectives of the paper

철도시스템 개발 시 시스템공학 활동과 시스템안전 활동을 효과적으로 통합 구축하기 위해서는 먼저 수명주기 단계상에서 수행되는 시스템공학 프로세스를 정의해야만 하고 이와 함께 수행되는 시스템안전 프로세스를 정의해야만 한다. 먼저 안전성 확보를 위한 시스템안전 프로세스를 기존의 시스템공학 프로세스에 적용시키기 위해 철도시스템 개발 전반에 걸친 수명주기 단계를 이해해야 한다. 그리고 시스템의 수명주기 동안 시스템 설계의 상세수준을 제공하는 시스템공학 표준인 IEEE 1220의 프로세스를 통하여 전반적인 시스템 설계를 명확히 정의한다[7]. 이를 토대로 상호간의 인터페이스를 정의함으로써 검증 단계에서의 시스템공학 프로세스와 시스템안전 프로세스 사이의 활동과 상호 데이터 인터페이스 연결 측면을 다루어 실제 시스템 안전성을 확보하는 것은 매우 중요하다고 볼 수 있다.

따라서 시스템 설계에서의 시스템공학 프로세스를 분석하고, 또한 안전성 평가 수행이 효과적으로 이루어지기 위한 시스템안전 프로세스를 분석한다. 그리고 안전성을 확보하기 위하여 시스템공학 프로세스와 시스템안전 프로세스 활동들에 대한 연계방안을 제시한다. 이를 통해 철도시스템 개발 시 시스템 수명주기를 중심으로 시스템 검증 단계에서 체계적이며 효율적인 안전성 평가 업무수행과 후속 되는 안전관리 활동이 보다 더 일관되게 수행되도록 통합 검증 프로세스를 구축한다. 그리고 구축한 통합 검증 프로세스가 시스템안전 확보를 위한 체계적인 설계 접근을 하는지에 대해 검증한다. <Figure 1>을 통해 통합 검증 프로세스 구축에 대한 연구 수행 방법을 도식화 하였다.



<Figure 2> System life-cycle model of ISO/IEC 15288[8].

본 논문의 구성은 다음과 같다. 서론에서는 본 연구의 사회, 기술 및 연구 동향과 필요성을 제시하였고, 본론에서는 시스템공학 프로세스와 시스템안전 프로세스에 대해 시스템 수명주기를 고려하여 정의하였다. 또한 상호간의 데이터 인터페이스를 연결하고, 안전성 확보를 위한 활동들을 명시한다. 그리고 이를 기반으로 통합 검증 프로세스를 모델링한 내용을 기술하였다. 마지막으로 본 논문의 결과를 정리 및 요약하였다.

2. 문제의 정의

2.1 시스템공학 프로세스와 시스템안전 프로세스의 정의

시스템안전 확보를 위해 시스템공학 접근법을 도입의 토대로 본 연구에서는 국제 표준인 ISO/IEC 15288을 활용하였다. ISO/IEC 15288은 전체 시스템 수명주기를 고려한 표준이며, 여러 산업분야 표준들과도 폭넓게 다루어지고 있기 때문이다[8]. ISO/IEC 15288은 <Figure 2>와 같이 11단계로 시스템 수명주기에 대하여 기술하고 있다. 또한 Vee 모델을 기반으로 시스템 설계 활동을 권유하고 있다. 그리고 시스템 계층구조에 따라 시스템을 계층별로 세분화시켜 반복적이며, 점진적으로 설계를 수행한다.

국제 기능 안전 표준 규격인 IEC 61508은 기능 안전 시스템에 대한 요구사항 명세, 설계, 개발, 설치, 운영, 유지보수의 표준이다[4]. SIL(Safety Integrity Level)을 4등급으로 분류하고 각 레벨에 맞는 활동을 요구하고 있다. IEC 61508 시스템안전 프로세스는 수명주기를 고려하며 위험원 분석, 안전 요구사항 도출, 계획 수립, 실현, 점검, 확인, 운영 및 보수, 폐기 단계로 구성된다.

2.2 시스템공학 프로세스의 검증 단계 개선을 통한 안전성 향상의 필요성

철도시스템의 경우 수명주기가 현재까지 정확히 정의된 것은 없다. 일반적으로 시스템 수명주기를 5단계로 구분하면 개념단계(Concept), 정의단계(Definition), 개발단계(Development), 생산단계(Production), 폐기단계(Disposal)로 구분되어 진다[1]. 수명주기 관점에서 시스템공학은 요구사항 분석, 기능분석, 통합 등을 핵심프로세스로 구성한다[8]. 이를 위하여 이해당사자의 요구를 만족시키는 시스템의 인력, 제품 및 프로세스의 해결 방안 등을 전개 및 검증하기 위한 기술적 활동을 포함하는 접근 방법으로서 시스템공학 프로세스를 적용하게 된다.

시스템공학 프로세스는 여러 종류의 프로세스가 존재하며 대표적으로 MIL-STD-499C, IEEE 1220, EIA-632, ISO/IEC 15288로 구분할 수 있다. 이 표준들은 미 국방 규격 MIL-STD-499로부터 발전하였으며, 상호간의 유사한 주제를 다루고 있지만 약간의 방법적인 차이를 가지고 있으며 <Table 1>에 비교 기술하였다. 본 연구에서는 시스템 개발에 있어 상세 프로세스를 제공하는 IEEE 1220의 시스템공학 프로세스를 기반으로 개발하였다.

<Table 1> Summary of the verification & validation phases activities of the existing systems engineering standards.

특성	MIL-STD-499C-2005[9]	IEEE 1220-2005[7]	EIA-632-1998[10]	ISO/IEC 15288[8]
발행기관	The Aerospace Corporation	IEEE	EIA	ISO/IEC
제목	Systems Engineering	Application and Management of the Systems Engineering Process	Engineering a System	Systems Engineering-System Life Cycle Process
프로세스 구분	6개 프로세스	8개 프로세스	5개 프로세스 33개 요구사항	4개 프로세스
주요 활동	-프로세스 입력 -요구사항 분석 -기능 분석 -합성 -시스템 분석 및 통제 -프로세스 출력	-요구사항 분석 -요구사항 확인 -기능 검증 -합성 -설계 검증 -시스템 분석 -통제	-기술 관리 -획득 및 공급 -시스템 설계 -제품 구현 -기술 평가	-동의 프로세스 -기업 프로세스 -사업 프로세스 -기술 프로세스
검증(Verification)	4.2.1, 4.2.2, 4.2.3, 4.2.6	6.2	요구사항 25, 26, 27, 28, 29, 33	5.5.9
확인(Validation)	4.2.6	6.4 6.6	요구사항 30, 31, 32	5.5.7
특징	설계에 대한 검증 활동정의 및 획득관리지침으로 시험평가 관리	하위 단계까지의 검증 프로세스 상세 정의와 흐름을 제시	요구사항 별 검증 활동 내용 정의	수명주기관점에서 포괄적이고 간단하게 정의

안전성의 확보를 최우선으로 해야 하는 안전중시 시스템의 경우, 별도의 시스템안전 프로세스를 진행시켜 안전성을 검증받아야 한다. 시스템의 안전성을 확보하기 위한 노력은 다양한 관점과 접근방식을 통하여 실행하고 있으나[11], 시스템의 품질, 신뢰성, 가용성, 유지보수성, 안전성을 포괄하여 관리하기 위해서는 체계적인 프로세스를 활용할 수밖에 없는 상황이다.

2.3 시스템공학 프로세스와 시스템안전 프로세스의 연관성

2.2절에서 시스템 구조적 설계 활동의 중요성을 언급하였다. 또한 안전 등급에 따른 안전 분석 활동에 대해서도 기술하였다.

이는 시스템 분야 특성에 맞는 시스템 수명주기를 고려한 설계 프로세스가 다루어진다는 점에서 상호 연관성이 존재한다고 볼 수 있다. 다만 기존의 시스템안전 프로세스 관련 연구에서는 전반적인 안전 활동 관리나 초기 단계의 요구사항 수집에 대한 부분이 주로 체계적으로 다루어졌다[3]. 따라서 시스템공학 프로세스와의 연계를 통해 일반적인 시스템 설계에 있어 안전성 확보에 도움을 주리라 볼 수 있을 것이다.

2.4 시스템공학 프로세스와 시스템안전 프로세스의 통합의 필요성

산출물들이 일관적이고 체계적으로 설계 또는 계획되므로 기존의 시스템공학 검증 프로세스와 별도로 시스템안전 프로세스를 진행할 경우 2중의 인력과 중복된 비용이 발생하게 된다. 이를 위해 기존의 시스템공학 검증 프로세스와 병행할 수 있는 시스템안전 프로세스가 필요하다. 본 연구에서는 기존의 시스템공학 검증 프로세스에 시스템안전 프로세스를 병행할 수 있는 통합 검증 프로세스를 제안한다.

2.5 연구 목표 및 범위

상위 선행연구 분석을 통해 안전중시 시스템인 철도시스템의 검증 단계에서 시스템공학 프로세스와 시스템안전 프로세스의 데이터 인터페이스 연계를 통한 통합 검증 프로세스가 필요하다는 것을 인지하였다. 특히 시스템 수명주기를 고려할 때 시스템이 활용되기 전 단계인 검증 단계의 중요성 인식에 따라 안전성 확보 방안이 필요하다.

ISSN : 1229-6783 (Print)
ISSN : 2288-1484 (Online)

본 연구에서는 철도시스템 개발 과정에서의 안전성 향상을 위한 프로세스 정립을 위해 시스템공학 프로세스와 시스템안전 프로세스를 연계한 통합 검증 프로세스를 제안한다.

따라서 이렇게 제시된 통합 검증 프로세스를 바탕으로 전산지원 도구를 활용해 통합 검증 프로세스의 구축 및 검증에 관한 연구를 수행 하였다.

일반적으로 시스템공학에서 시스템 수명주기는 <Figure 1>에 도식화 한 것처럼 표현되며, 본 연구는 검증 단계(Verification & Validation)로 범위를 제한 및 설정 하였다.

3. 안전성 향상을 고려한 시스템공학 프로세스 검증 단계 개선을 위한 모델링

3.1 시스템공학 프로세스 및 시스템안전 프로세스 모델

2.1절에서는 시스템공학 및 시스템안전 프로세스의 방법 및 속성을 정의하였다. 이를 통해 통합 검증 프로세스 모델 구축을 통해 안전성 확보 활동의 체계화를 도모하고자 한다.

따라서 이를 구현할 모델 개발에 필요한 모델링 도구의 사용이 필요하였으며, 시스템공학 전산지원도구인 CORE®를 사용하였다. 전산지원도구를 이용해 기능 모델 표현 방법 중 EFFBD(Enhanced Function Flow Diagram)을 통해 모델링 하였다. 이는 각 활동의 입출력 정보를 표현 할 수 있어 프로세스 확인에 용이하다.

통합 검증 프로세스 모델은 시스템공학 프로세스를 중심으로 하여 구축되었으므로 기본적으로 시스템공학 표준을 충족시키고 있다. 따라서 통합 검증 프로세스 모델은 계층적으로 설계가 되어있으며, 요구사항 분석, 기능 분석, 시스템 설계를 수행하면서 안전 요소 분석 활동 및 시험 평가를 할 수 있도록 개발하였다.

3.2 모델링 절차 요약

통합 검증 프로세스 모델을 개발하기 위해, 다음과 같은 절차를 따랐다. 절차의 활동을 통한 결과들은 통합 검증 프로세스 모델에 반영되었다.

(1) 시스템 수명주기에서 검증 단계를 정의한다.
(2) 검증 단계에 적절한 설계 활동 및 안전성 확보 활동을 정의한다.
(3) 검증단계에 수행되는 설계 활동 및 안전성 확보 활동들의 산출물과 연계되는 시스템공학 프로세스를 정의한다.
(4) 시스템공학 프로세스와 시스템안전 프로세스 사이의 인터페이스를 식별한다.
(5) 인터페이스를 기반으로 상호 연관된 시스템 설계 데이터를 정의한다.
(6) 설계 활동 및 안전성 확보 활동의 산출물들이 서로 연계된 통합 검증 프로세스 모델을 정의한다.

3.3 통합 검증 프로세스 모델의 구조

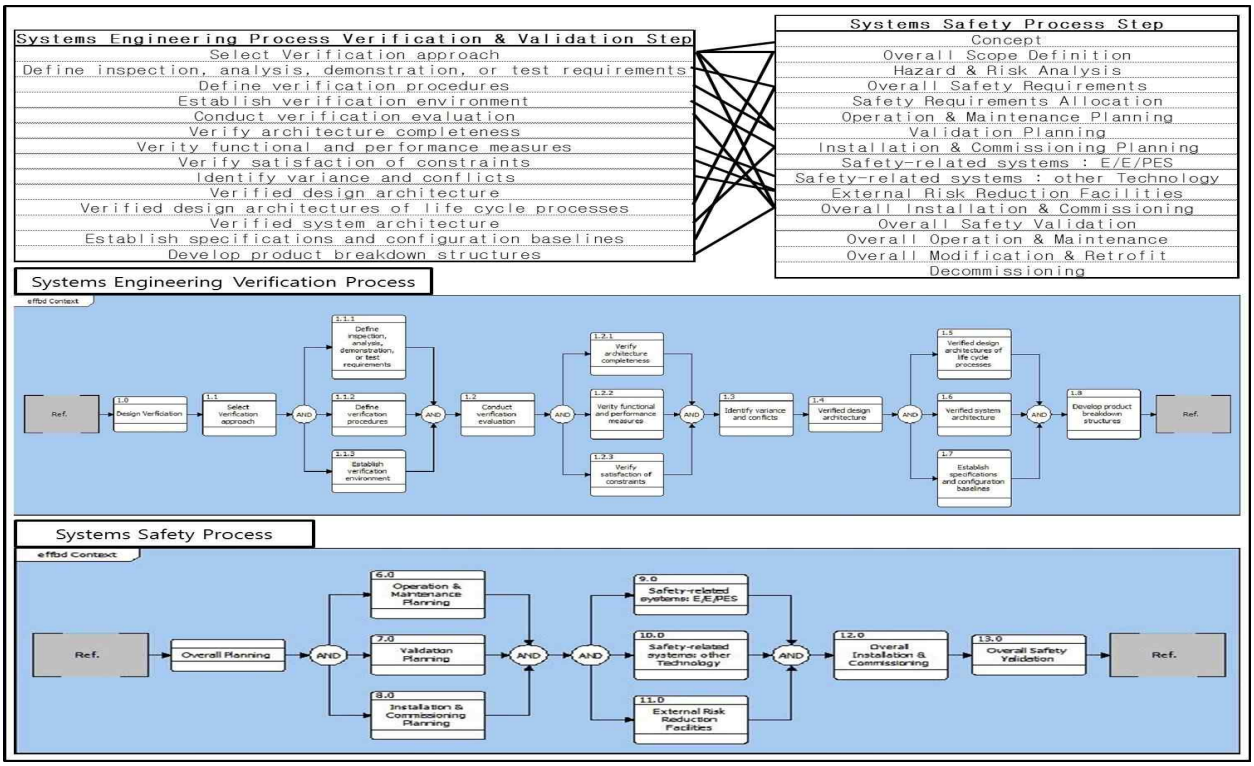
통합 검증 프로세스 모델은 시스템 수명주기 상에서 검증 단계 수준, 그 하위 수준에 시스템 설계 및 안전성 확보 활동으로 설계되어 있다. <Figure 3>에 시스템공학 검증 프로세스와 시스템안전 프로세스 사이의 인터페이스가 표현되며, 프로세스 상호간의 공통 요소 데이터의 교환이 표현되어 있다. 이를 통해 시스템공학 검증 프로세스와 시스템안전 프로세스 사이의 연계성이 많은 것을 확인할 수 있었으며 각 프로세스 고유의 특성을 가진 단계를 찾아낼 수 있었다. 각 프로세스의 고유의 특성을 가진 단계를 통합 검증 프로세스 모델에 반영함으로써 더욱 신뢰도 및 완성도를 높일 수 있었다. 산출물 데이터는 시스템 설계 및 안전성 확보 활동으로부터 발생되어 검증 단계 수준의 하위 수준으로 전개된다. 통합 검증 프로세스 모델의 활동들은 기능 블록으로 표현되어 있으며, 공통 요소와 산출물 데이터들은 데이터 블록으로 표현되어져 있다.

4. 통합 검증 프로세스 모델의 구축

4.1 통합 검증 프로세스 모델 구축을 위한 시스템공학 프로세스의 검증 단계 활동 산출물 분석

본 연구의 통합 검증 프로세스 모델은 2.4절에서 필요성을 기술하였다. 안전성 확보를 중심으로 활동 절차와 발생 데이터에 초점을 맞추어 모델을 구축하였다.

통합 검증 프로세스 모델 구축에 앞서 시스템공학 프로세스의 검증 단계 수행 시에 요구되는 시스템 설계 활동과 안전성 확보 활동에 따른 산출물의 분석을 수행하였으며, 이를 <Figure 4>에 도시하였다.



<Figure 3> Identification of the interfaces between the verification phase activities of the systems engineering process and systems safety process.

(1) 시스템공학에서 검증 단계의 정의 : 검증 단계에서 요구되는 시스템 설계 활동, 안전성 확보 활동의 정의.
(2) 시스템 설계 검증 및 안전 활동에 따른 산출물 정의 : 시스템 설계 검증 활동, 안전성 확보 활동에 따른 물리적 연결 및 산출물의 정의.
(3) 생성된 산출물들의 설계 요소 및 안전성 확보 요소 분석 : 시스템 설계 검증 활동, 안전성 확보 활동에 따른 산출물이 내포하고 있는 요소들의 분석.
(4) 산출물들의 통합 요소 분석 및 적용 : 시스템 설계 검증 및 안전성 확보 활동에 따른 산출물들의 공통 요소를 분석하고 이를 통합 검증 프로세스 모델의 기본 구성 요소로 적용.

4.2 시스템공학 프로세스의 검증 단계 활동과 시스템안전 프로세스간의 인터페이스 정의

<Figure 1>에서 보듯이 시스템공학 프로세스의 검증 단계의 활동은 수명주기를 기반으로 시스템 설계 초기 개념설계부터 수행되어야 함을 알 수 있다. 이를 위하여 IEEE 1220에서 제안하는 검증 프로세스를 기반으로 안전성 확보에 대한 검토 및 평가를 실행함으로써 핵심기술의 설계 및 개발부분에서 고려할 수 없는 부분을 검출하거나 개선시킬 수 있다. 따라서 철도시스템의 안전성을 향상시키는 검증 활동을 추진하기 위한 목적으로 IEEE 1220에서 정의하고 있는 15개 STEP에 근거하여 진행해야한다. 각 수행 단계별로 안전성 향상을 고려한 방법 적용을 고려해야만 한다.

앞의 2.2절에서 기술하였듯이 시스템안전 프로세스는 산출물 간의 추적성 확보가 부족하여 체계적으로 정리되지 않아 어려움을 겪는 면이 많다. 또한 일반적인 시스템 설계와 비교해볼 때 프로세스의 정교함이 떨어지는 측면이 있다.

<Figure 3>에 시스템공학 프로세스의 검증 단계 활동과 시스템안전 프로세스간의 인터페이스를 나타내었다. 인터페이스를 설정한 기준은 다음과 같다.

(1) 각각의 프로세스 사이에서 안전 요소를 고려한 기능적 연결.
(2) 시스템공학 프로세스의 검증 단계의 안전성 향상을 고려한 설계 및 안전성 확보 데이터간의 기능적 연결.
(3) 각각의 프로세스에서 도출되는 산출물간의 물리적 또는 기능적 연결.

시스템공학 프로세스와 시스템안전 프로세스의 검증 단계 활동 간의 인터페이스 정의를 통해서 4.1절에 제시한 검증 단계 활동별 산출물들이 상호간의 유기적인

Process 활동	Process 업무	시스템공학 프로세스의 Verification & Validation 단계 활동의 산출물															
		시험평가팀 구성도/담당업무	시험평가 요구사항 문서	요구사항-검증매트릭스	시험시제 요구서	시험시설 요구서	시험 인력 요구서	시험 자료 요구서	시험장비 요구서	시험평가 항목 자료	위험부담 평가 결과서	획득가치 평가 결과서	시험평가계획서	상세시험계획서	시험평가 준비 검토서	시험평가 중간보고서	시험평가 결과보고서
검증단계 전략활동	시험평가팀 구성	●															
	시험평가요구사항 정의		●	●					●								
	시험평가전략/접근방안 수립	●											●	●	●		
	시험시제 정의	●			●												
	시험시설 정의	●				●											
	시험인원 정의	●					●										
	시험 자료 정의	●						●									
	시험장비 H/W, S/W 정의	●							●								
검증단계 계획활동	시험평가 항목 정의	●								●					●		
	위험부담 평가									●	●		●	●			
	획득가치 평가									●		●	●	●			
	시험평가계획 작성	●								●			●				
	시험항목 상세시험계획	●								●				●			
검증단계 개발활동	시험시제 제작/통합	●			●												
	시험시설 개발	●				●											
	시험자료, 모델 개발	●						●									
	시험절차 작성	●											●		●		
	시험장비 H/W, S/W 개발	●							●								
	시험환경 검증	●						●			●	●			●		
	시험평가 준비검토	●								●					●		
검증단계 수행활동	검사 수행	●											●	●			
	해석 수행	●											●	●			
	시험환경 품질확인												●	●	●		
	시험/시연 수행	●											●	●	●		
	재설계/수정	●														●	
	평가결과검토	●														●	●
	결과보고/승인	●															●

<Figure 4> Identification of data linkages embedded between the verification phase activities and the outputs of verification & validation phase process of systems engineering.

관계를 가지고 있음을 알 수 있다. 또한 시스템 설계 검증 활동과 시스템안전 활동을 통해 산출되는 데이터 간의 추적성 및 기능 연결 흐름을 쉽게 볼 수 있다. 이는 통합 검증 프로세스 모델을 구축하는데 있어 4.1절에서 기술한 시스템공학 프로세스의 검증 단계 활동 산출물들의 공통 요소들이 시스템안전 프로세스와의 인터페이스를 토대로 연계될 수 있음을 보여준다.

4.3 통합 검증 프로세스 모델

<Figure 5>는 본 연구에서 제시하는 통합 검증 프로세스 모델의 활동 단계들을 표기하였다.

통합 검증 프로세스에서는 기능 분석이 끝난 후에 산출물과 안전 요구사항, 시험 및 평가 요소에 대하여 전반적인 통합을 통해 인터페이스를 정의한다. 이는 단순히 점검 및 확인 단계에서 검출할 수 없는 기능 요소들에 대한 모든 데이터를 검토할 수 있으며, 시험 및 평가 요소까지 고려함으로써 앞선 단계에서 고려한 프로세스 일정까지 포함한다.

시스템 전체 안전 확인 단계 후에 시스템 전체 안전 검증 단계를 추가함으로써 통합 단계에서 놓칠 수 있는 평가 부분들에 대하여 다시 검토를 함으로써 보완사항을 발견할 수 있으며, 안전 요구사항이 제대로 반영되었는지에 대해서도 검증할 수 있다.

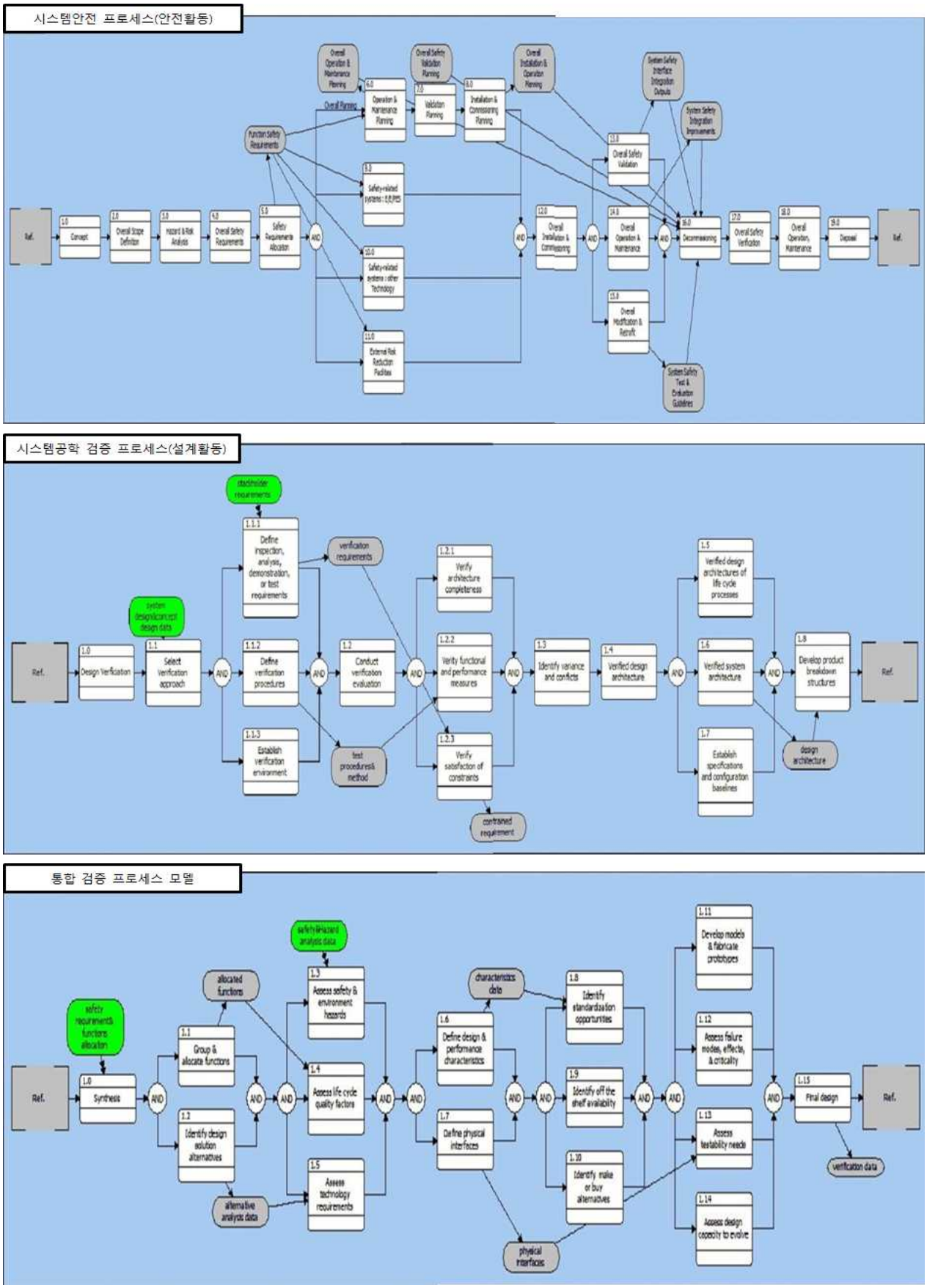
4.2절에서 정의된 인터페이스는 검증 단계 활동의 범위 및 기준선을 설정하는데 있어 요소 식별을 가능하게 해준다. 그리고 식별된 요소들의 속성을 명확하게 분류함으로써 인터페이스 및 안전 요소를 통합 검증 프로세스 모델에서 제시하며, 최종적으로 활동을 마치게 된다.

5. 구축된 통합 검증 프로세스 모델에 대한 검증

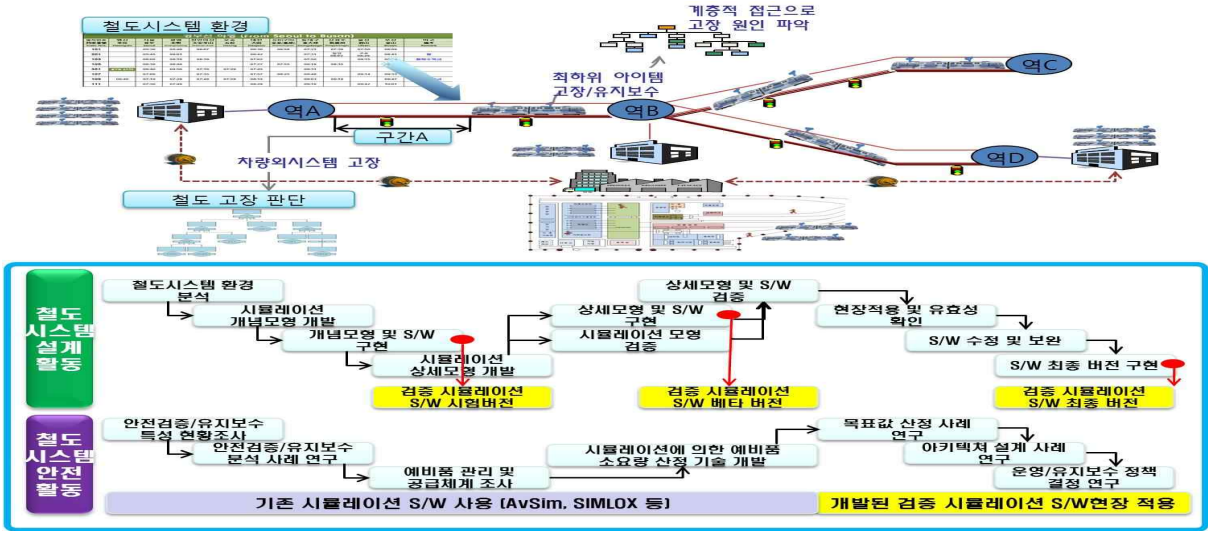
5.1 철도시스템 설계 적용 사례

5.1.1 대상시스템의 특징 및 범위

최근 이슈가 되고 있는 철도안전과 관련하여 국민의 신뢰도 회복과 더불어 대표적인 안전중시 시스템인 철도시스템의 안전성을 강화할 필요가 대두되었다. 따라서 철도시스템의 기능안전을 파악하고 이를 체계적으로 관리 및 검증하여 열차 사고를 방지할 수 있도록 대상시스템을 정하였다.



<Figure 5> Improvement of the verification phase of systems engineering process by reflecting safety requirements in the development of integration verification process model.



<Figure 6> Application of the resultant verification process model in the development of the verification S/W for railway systems.

코레일의 안전성 검증 지침은 안전성 검증에 필요한 실무방법과 절차를 정하는 사항으로 조문17개, 별표2개, 별지3개로 구성되어 있으며, 안전성 검증대상은 제도, 사업, 열차운행계획 및 철도물품과 시설물 등 열차안전 운행과 관련된 사항을 주요 대상으로 한다. 본 연구에서는 철도시스템의 방대한 안전성 검증 업무 중 시스템 계획단계의 요구사항에서부터 검증 단계에 해당하기까지의 프로세스에 대한 체계적 접근을 토대로 적용하였다.

5.1.2 대상시스템의 적용 결과

철도시스템의 안전성을 고려한 검증 단계를 수행함에 있어서 <Figure 5>에 정의된 통합 검증 프로세스 모델을 적용 시켰다. 통합 검증 프로세스 수행을 통해 설계 활동 및 안전성 확보 활동, 그에 따른 산출물과 산출물간의 인터페이스 및 흐름을 식별하여 <Figure 6>에 나타내었다.

검증 단계에서는 철도시스템 상위 수준의 안전성 확보 활동과 관련된 기능들을 도출하여 이에 대한 특성과 현황 분석을 하게 된다. 이러한 분석이 끝나게 되면 실질적인 기능과 관련된 설계 데이터와 안전성 확보 활동 산출물간의 관계를 설정한다. 관계 설정 사항을 토대로 모든 요소와의 추적성 연결을 통해 최종적으로 결과를 통합한다. 이 부분은 본 논문에서 말하는 인터페이스 정의를 토대로 진행된다. 이러한 통합된 결과를 바탕으로 철도시스템의 기능별 사항이나 안전 요건에 대하여 검증을 수행한다. 이러한 사항은 초기 설계 단계에서의 안전 요구사항까지 고려하는 시스템공학적 방법에 대한 내용이 검증 단계 활동을 통해 안전에 대한 요소들을 빠르게 확인할 수 있다.

따라서 최종적으로 검증 단계의 통합 검증 프로세스를 수행함에 따라 철도시스템 요구서를 바탕으로 최종 철도시스템 검증 평가서를 생성하게 된다. 이러한 설계 및 안전성 확보 활동을 통한 산출물이 통합적으로 운용되기 때문에 상호간의 데이터의 교환이나 데이터 사이의 유기적인 관계가 구성됨에 따라 효과적인 검증 단계를 수행하게 된다.

6. 결 론

본 연구와 관련하여 안전 설계에 대한 필요성을 느끼고 시스템안전 프로세스의 발전을 제시한 연구들이 있었다. 그러나 본 연구의 주안점은 시스템 개발에 있어 최종역인 검증 단계를 중요하게 바라보는 시스템공학 관점에 있다. 효과적인 검증 단계를 구성 및 수행함으로써 시스템공학 프로세스의 개선을 반영하고 궁극적으로 안전중시 시스템의 안전을 도모하는 것이 본 연구의 목표이다.

본 논문에서는 안전성 향상을 고려한 시스템공학 프로세스 검증 단계의 개선에 관한 연구를 수행하였다. 이를 위하여 시스템공학 프로세스의 검증 단계 개선을 위해 안전 성 확보 활동과, 검증 단계의 상세활동을 정의하였다. 앞서 선행된 IEEE 1220과 IEC 61508을 기반으로 시스템공학 프로세스 검증 단계의 안전 관련 요소들을 식별 및 산출물을 도출하고 이들 간의 관계를 파악하여 추적성을 확보한 기능 인터페이스를 정의하

였다. 이를 통해 도출된 통합 검증 프로세스를 시스템 공학 전산 지원 도구를 통하여 체계적으로 구축하였다.

철도시스템에 본 연구에서 제시하는 통합 검증 프로세스 모델을 적용하여 초기 안전 활동부터의 활동들을 효과적으로 검증할 수 있도록 함으로써 철도시스템에 대한 기능 및 기기간의 관계를 성숙시켜 안전성을 높일 수 있었다.

구축된 통합 검증 프로세스 모델은 안전 요구사항이 시스템 요구사항으로 구조화 될 수 있도록 하여, 검증 단계에서 보다 상세하게 검토될 수 있도록 하였다. 이는 안전중시 시스템에서 시스템공학 설계 검증 프로세스를 활용함으로써 안전 관련 활동 및 안전사고 요소에 대한 예방을 개선하고, 안전의식 확대 및 안전중시 시스템의 신뢰성을 높일 수 있을 것이다.

7. 참 고 문 헌

[1] S. J. Choi, M. H. Kim, B. S. Kim and H. J. Byun, "The Study on Introduction and Improvement of the Independent Safety Assessment for Railway System", Conferene of the Korean Society for Railway, the Korean Society for Railway, pp. 393-398, 2012.

[2] J. Martin, Ed(s). Systems Engineering Guidebook. 3rd ed. Boca Raton, Florida: CRC Press, 1997.

[3] J. H. Yoon and J. C. Lee, "A Study on Integrated SE Process for the Development of the Railway Systems with Safety Assessment Included.", Korean Society for Rail, vol. 11, pp. 19-26, 2009.

[4] IEC, "Functional Safety and IEC 61508," International Electrotechnical Commission, Tech. Rep., TR 61508-0, Sep. 2005, pp. 1-13.

[5] Minhye Yu and Kwan Seek Kim, "The Safey Standards and ASIC Development for the Electronics Stability Control System," in Proc. KSAE 2010 Annual Conference and Exhibition, Daegu, Korea, Nov. 24, 2010, pp. 2124-2128.

[6] Chris Hayhurst, Brett Murphy, Richard Anderson, Coourous Mohtadi, Jon Friedman, and Pieter Mosterman, "Verification and Validation Integrated within Processes Using Model-Based Design," in Proc. Proceddings of the 17th IFAC World Congress, 2008, pp. 1056-1061.

[7] IEEE Standard for Application and Management of the Systems Engineering Process, Institute of Electrical and Electronics Engineers Standard, IEEE Std 1220-2005, 2005.

[8] Systems and Software Engineering - System Life Cycle Processes, ISO/IEC Standard, ISO/IEC 15288, 2008.

[9] Systems Engineering, Department of Defense Standard, MIL-STD-499C, 2005.

[10] Processes for Engineering a System, Electronic Industries Alliance Standard, EIA-632-1998, 1999.

[11] General guidelines on system safety for ships, [KMS 002:2010], The Korean Shipbuilders' Association, 2010, pp. 1-16.

저 자 소 개

심 상 현

현 아주대학교 시스템공학과 박사과정. 관심분야는 시험평가, 모델기반 시스템공학, Modeling & Simulation 등.

주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 성호관 243호

이 재 천

현 아주대학교 시스템공학과 정교수. 서울대학교 전자공학과에서 공학사, KAIST 전기 및 전자공학과에서 공학석사 및 박사 학위를 취득. 미국 MIT에서 Post-Doc을 수행하였으며, Univ. of California (Santa Barbara)에서 초빙연구원, 캐나다 Univ. of Victoria (BC)에서 방문교수, KIST에서 책임연구원 재직. 이 후 미국 Stanford Univ. 방문교수 역임. 현재 연구 및 교육 관심분야는 시스템공학 및 Systems Safety에의 응용 등.

주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 서관 309호