철도시스템 개발에서 안전성 향상을 위한 시스템공학 프로세스의 검증 단계 개선에 관한 연구

On the Improvement of the Verification Phase of Systems Engineering Process for Safety Improvement in the Development of Railway Systems

심 상 현* · 이 재 천*
Sang-Hyun Sim* · Jae-Chon Lee*

Abstract

최근 현대사회는 자동차, 철도 및 항공 등 대형 복합 시스템의 체계 속에서 지내고 있으며, 고장 및 사고로 인한 시스템의 안전 설계에 대한 고려와 안전에 대한 인식이 증가하고 있다. 따라서 기존의 시스템공학 프로세스에서 다루는 시스템 설계에 대한 단계별 안전 활동의 강화의 필요성 역시 강조되고 있다. 그 중에서도 시스템 설계의 최종 활동에 해당하는 검증 단계 활동이 제대로 수행되어야만 초기에 의도한 시스템 설계의 안전도 향상을 바라볼 수 있을 것이다. 본 논문에서는 안전 활동을 고려한 시스템공학 프로세스의 검증 단계의 개선사항 도출과 모델링을 통해 안전중시 시스템인 철도 차량 운전실 시스템을 대상으로 적용 및 조정 구축에 대한 내용을 기술하고 있다. 본 연구의 결과를 토대로 향후 품질 향상 및 비용 절감과 데이터의 관리 및 추적 기능을 개선함으로써 안전사고 발생 가능성을 줄일 수 있을 것으로 기대된다.

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

* 아주대학교 시스템공학과

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. 최근 대형 시스템에 의한 고장, 사고로 인하여 시스템의 안전 설계에 대한 고려 부족으로 인한 시스템 안전 설계에 대한 요구가 증가하고 있다. 또한 안전성 관리를 수행하는 정형적인 방법과 장애 복구 기능 등 엄격한 규제를 요구하고 있다[1]. 이러한 특성으로 인하여 시스템 안전 설계 진행 시 시스템 설계 전반에 걸친 검증을 효과적으로 할 수 있어야 한다.

시스템공학은 전 수명주기를 고려한 총체적 접근으로서 시스템의 복잡성과 불확실성을 효과적으로 관리하여 시스템 개발을 성공시키는 기술이다. 이러한 기술은 시스템의 계층적인 관점에서 시스템의 내재된 위험원을 방지하거나 통제하기 위해 필요한 활동들에 대하여 성능 및 기능 등의 논리성을 확인하고, 시행오류를 줄일 수 있도록 목적을 두고 있다[2]. 안전중시 시스템들이 더욱 복잡해지면서, 성공적인 시스템 설계를 실현할 수 있도록 다학제적 접근 방법인 시스템공학 기술이 안전중시 시스템 개발에 확산되고 있다.

안전성 평가 방법을 시스템공학, 시스템 안전 분석, 그리고 인간 요소를 기반으로 한 통합 시스템 설계 방법을 개발한 연구가 있었으나, 기능 중심의 위험원 분석 활동에만 초점이 맞춰져 있다[3]. 또한 IEC 61508은 국제 기능 안전 표준 규격으로서 시스템안전 프로세스에 관하여 언급하고 있으나[4] 신뢰성공학의 배경이 강해, 확률론적, 정량적 접근에 한정되어 있다[5].

본 연구에서는 전 수명주기 동안 시스템 설계의 상세 수준을 제공하는 시스템공학 표준인 IEEE 1220-2005[6]을 기반으로 한다. 이를 통해 IEC 61508표준에서 제시하는 하드웨어와 소프트웨어의 기능 안전 검증 단계를 결합한 시스템공학 프로세스를 제안하고자 한다.

이를 위해 IEEE 1220표준의 시스템공학 프로세스와 IEC 61508표준의 시스템안전 프로세스의 비교를 통해 전 수명주기 동안의 프로세스를 분석한다. 시스템공학 프로세스는 시스템공학의 전 수명주기 관점에서 볼 때 시스템을 설계 및 개발하는데 있어서 안전성 평가를 위한 검증 확인 단계의 세부 기술적 측면에서 많은 취약점을 가지고 있다[3]. 따라서 시스템공학 프로세스를 통해 시스템 수명주기와 계층구조를 중심으로 시스템안전 프로세스의 검증 단계가 결합하여 안전 분석 수행이 효과적으로 이루어질 수 있도록 할 수 있다. 또한 안전 요구사항이 시스템 요구사항과 시스템 설계의 기능적 및 물리적 요소들과 동기화될 수 있도록 함으로써, 최종적으로 시스템 설계 검증 단계에서 안전성 평가가 반영된 시스템공학 프로세스를 평가한다.

본 논문의 구성은 다음과 같다. 서론에서는 본 연구의 기술 및 연구 동향과 필요성을 제시하였고, 관련자료 분석에 대하여 기술하였다. 본론에서는 시스템공학 프로세스 검증단계 개선사항에 대해 정의 및 시스템안전 프로세스의 안전성 평가 절차를 모델링 하여 결합한 내용을 기술, 결론에서는 본 논문의 결과를 정리 및 요약하였다.

2. 이론적 배경

2.1 시스템공학 표준의 검증 단계 활동

시스템공학 표준은 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 있다. 이에 대하여 <표 1>에 기술하였다.

<표 1> 시스템공학 표준에서 제시하는 Verification & Validation 단계 활동

특성	MIL-STD-499C-2005	IEEE 1220-2005	EIA-632-1998	ISO/IEC 15288
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
확인(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
검증(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

MIL-STD-499C[7] 시스템공학 프로세스에서의 시험검증 활동은 시스템공학 프로세스의 일부로 요구사항 분석, 기능분석 및 합성 활동에 확인활동이 포함되어 있다. 그러나 검증 활동은 설계 및 물리적 해법의 검증 및 확인(4.2.6)으로 구분하여 기술하고 있다. 6단계의 프로세스로 구성되어 있으며 다른 표준에 비하여 비교적 간단하게 서술되어 있다.

반면 IEEE 1220-2005[6] 시스템공학 프로세스에서는 기능 검증과 설계 검증으로 나누어 매우 세밀하게 프로세스를 정의하고 있으며 활동에 대하여 구체적인 언급을 하고 있다. 또한 활동구조와 흐름을 명확하게 제시하고 있어서 일반적인 시스템의 개발에 적용이 용이하다. 그래서 본 연구의 검증 단계가 개선된 시스템 공학 프로세스를 구성하는데 있어 바탕으로 제시하였다. 그러나 안전중시 시스템의 특수성을 고려해볼 때 안전 활동에 대한 프로세스는 명확하게 제시되지 않고 있다. 이러한 면을 본 연구에서 보완 발전 시켰다.

EIA-632[8] 시스템공학 프로세스에서는 기술 관리와 기술평가를 축으로 프로세스를 정의하고 있다. 시험평가는 기술평가의 4가지 프로세스에 포함되어 있으며 구체적인 절차보다는 요구사항 관점에서 활동을 정의하고 있다.

ISO/IEC 15288[9] 시스템공학 프로세스는 시스템 수명주기관점에서 5단계로 활동을 정의하고 있으며 구체적인 방법, 절차는 제시하지 않고 있다. 그러나 검증 프로세스의 핵심 활동을 잘 정의하고 있어 프로세스 개발에 참고하였다.

위의 시스템공학 표준들의 검증 단계 활동을 요약하면 다음과 같다.

(1) 시험평가 자원(시제품, 시설, 장비, 자료, 인원)을 시험 전에 정의하고 검증하여야 한다.
(2) 시스템 개발 초기에 시험평가를 계획하고 시스템의 위험부담을 감소하는 전략을 수립한다.
(3) 시스템 수명주기 관점에서 검증활동을 수행한다.

2.2 시스템안전 표준의 검증 단계 활동

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

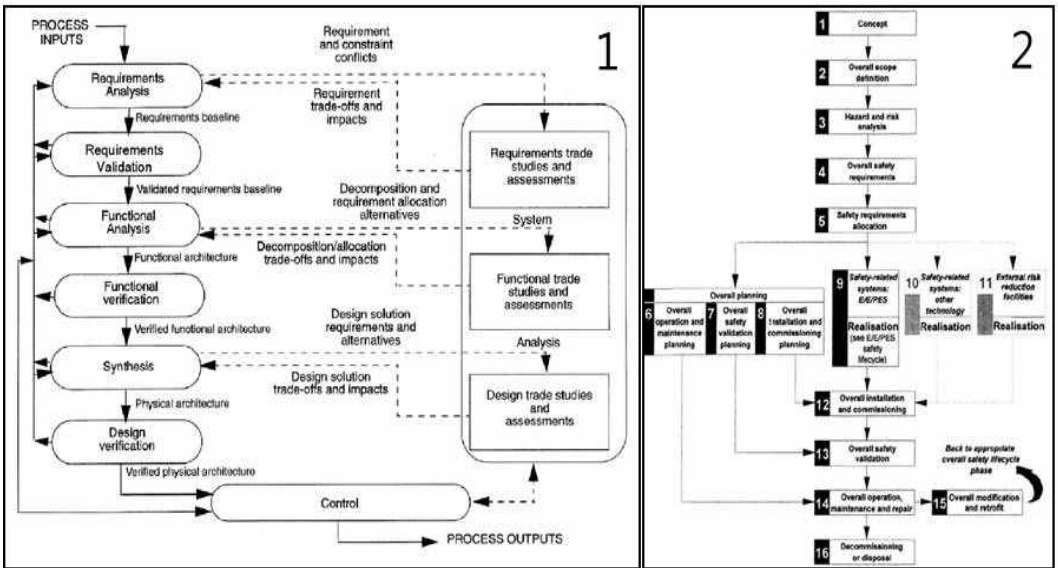
기존 연구를 살펴보면 안전중시 시스템인 선박 시스템에서도 시스템안전 프로세스에 대한 수명주기를 고려하였다[10]. 또한 각 시스템 분야 특성에 맞는 안전 확보 등이 활발히 연구되는 것을 알 수 있다. 그러나 기존의 시스템안전 프로세스 관련 연구에서는 전반적인 안전 활동 관리나 초기 단계의 요구사항 수집에 대한 부분이 주로 체계적으로 다루어졌다[11].

2.3 시스템공학 프로세스와 시스템안전 프로세스의 연관성

IEEE 1220표준에서는 시스템공학 프로세스를 8단계로 구분하고 있으며 주요 프로세스 내용은 <그림 1>과 같다. 본 논문과 관련 있는 단계는 5단계와 6단계이며, 이 중에

서 논증(validation) 및 검증(verification)부분을 유심히 살펴볼 것이다. 논증 및 검증 부분은 각 단계가 끝마칠 때마다 수행해야 하는 것으로서 시스템안전 프로세스와 연계를 위하여 모든 산출물에 대하여 논증 및 검증을 해야 한다고 판단된다.

IEC 61508표준에서는 시스템안전 프로세스를 수명주기 전반적으로 관리하며 상세 프로세스 내용은 <그림 1>과 같다. 위험 식별을 통해 위험 방지 및 완화를 목표로 하고, 제품개발에서 철저한 시험 수행을 통해 형상관리나 변경관리를 수행하도록 하고 있다. IEC 61508표준을 수명주기 관점에서 보았을 때 IEEE 1220표준과 요구사항 분석 및 논증 단계와 기능 분석 및 검증 단계까지는 유사한 점을 볼 수 있다. 하지만 IEEE 1220표준에서는 시스템안전 설계 검증 및 시스템 해석, 통제의 단계에 대해서는 언급이 되지 않고 있다.



<그림 1> IEEE 1220표준의 시스템공학 프로세스(1), IEC 61508표준의 시스템안전 프로세스(2)

따라서 시스템공학 프로세스에 시스템안전 프로세스의 안전 분석 활동을 각 단계마다 적용하여, 위험원 식별을 시스템설계 시부터 확인하여 결함에 대한 삽입을 최소화할 수 있다. 시스템공학 프로세스의 검증 단계 개선을 위해서는, 시스템설계와 시스템안전 활동 간의 인터페이스를 정의해야 한다. 인터페이스란 두 분야의 활동들이 어떠한 산출물들을 어느 시점에 주거나 받는지 정의한 것이다. IEEE 1220표준 검증 단계의 요소를 IEC 61508표준의 점검, 확인 단계의 요소와 연결하여 시스템공학 프로세스의 안전 활동에 대한 인터페이스를 정의하는 것이 중요하다고 볼 수 있다. 본 연구는 이를 기반으로 시스템공학 프로세스와 시스템안전 프로세스의 검증 단계를 통합한 개발 환경을 제시한다.

3. 안전 활동을 고려한 시스템공학 프로세스 검증 단계 개선

3.1 시스템공학 프로세스와 시스템안전 프로세스의 검증 단계 활동 비교

시스템공학 프로세스의 검증 단계 활동에서 중점적으로 살펴보아야 할 부분은 아래와 같이 구분할 수 있다.

(1) 검증의 내용이 불분명하거나 누락 및 오류 등이 있을 경우
(2) 시스템 환경의 상태가 시스템 설계상의 내용과 다를 경우
(3) 새로운 설계기법 및 방법 사용으로 시스템설계 비용의 절감 및 일정 단축 등의 효과가 나타나는 경우
(4) 이해당사자 요구사항의 변경 등의 경우

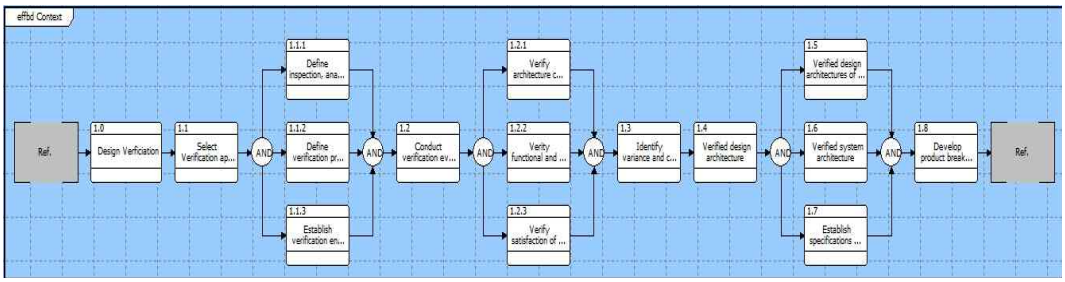
이와 같이 시스템공학 프로세스의 검증 단계의 활동은 시스템 설계 시 안전 확보에 대한 상세한 활동이 부족하므로 서로간의 긴밀한 조정이 필요하다.

시스템안전 프로세스가 산출물 간의 추적성 확보가 부족하여 체계적으로 정리되지 않아 어려움을 겪는 면이 많다. 또한 하드웨어와 소프트웨어별 기능 안전에 대하여 제시하지만 일반적인 시스템 설계와 비교해볼 때 프로세스의 정교함이 떨어지는 측면이 있다. 하지만 개별 프로세스의 검증 단계별 활동을 비교함으로써 검증 단계 과정에 참여하는 사용자의 관점으로 구조적으로 구분하는데 도움을 줄 것이다.

3.2 시스템공학 프로세스 및 시스템안전 프로세스의 검증 단계의 개선사항 도출

본 연구의 적용범위인 IEEE 1220표준의 시스템공학 프로세스의 검증 단계는 <그림 2>과 같으며, IEC 61508표준의 시스템안전 프로세스에서 6번부터 13번까지의 영역의 검증 단계 활동과 유사한 점이 있다. 이 부분의 활동은 설계의 일정 수립 및 확정, 이에 대한 수명주기를 고려한 활동과 이에 대한 검증이 일어나는 단계이다.

하지만 IEC 61058표준의 9번 영역에서 수명주기를 고려한 각각의 요구사항 도출, 아키텍처, 시스템 설계, 코딩, 통합, 시험 및 확인을 한 후 이에 대한 재통합을 거치게 된다. 이는 공통된 일련의 작업을 나누어 실행하는 것으로 중첩된 활동들의 나열이라고 밖에 볼 수 없다. 오히려 따로 실행을 하게 됨으로써 추후 재통합할 때 서로의 인터페이스를 고려하여 확인하는 작업과 다시 확인을 함으로서 일정과 비용의 낭비가 발생하게 된다.



<그림 2> IEEE 1220 표준의 시스템공학 프로세스 중 검증 프로세스

따라서 시스템안전 프로세스에서는 단순히 점검 및 확인 단계에 그치기 때문에 선행된 분석 활동에 대하여 효과적으로 검토하지 못하게 된다. 이는 시스템 설계 및 코딩 후 통합과정에서부터 취약점으로 여겨진다. 사전에 시스템공학 프로세스 절차에 맞춰 각 단계마다의 검증이 이루어졌다면, 추후 발생될 수 있는 오류 및 개선사항에 대한 조치가 빠르게 적용될 수 있을 것이다.

3.3 검증단계 개선에 의한 시스템공학 프로세스의 효용성

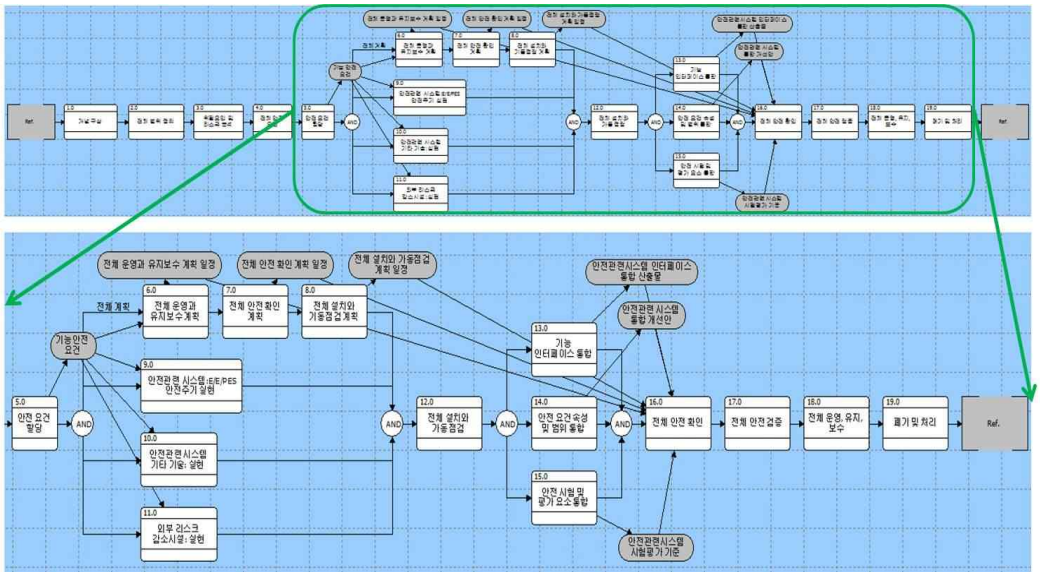
검증단계가 개선된 시스템공학 프로세스로 인하여 기존에 시스템공학 프로세스를 안전과 관련하여 더욱 상세 시킬 수 있다. 안전 분석 업무가 시스템공학 프로세스의 각 단계에 적용됨에 따라 시스템설계 초기부터 안전에 대한 고려를 하게 된다. 이는 신뢰성 향상과 추후 시스템을 유지 및 운영하는데 있어 도움을 줄 것이다. 또한 시스템설계의 상세 부분이 미약했던 시스템안전 프로세스를 보완하였기 때문에 기존에 시스템안전 프로세스의 개선된 형태라고도 볼 수 있다. 또한 위험원 분석 프로세스나 방법에 적용에 대해서도 전 수명주기 동안 관리할 수 있도록 시스템 설계 프로세스를 제시함에 따라 다양한 분야에서 활용할 수 있다.

4. 안전 활동을 고려한 시스템공학 프로세스의 검증 단계 모델링

4.1 시스템공학 프로세스의 모델링 절차

IEEE 1220 시스템공학 표준에서 제시하는 검증 단계는 안전요소 분석에 대한 상세 활동을 고려하지 않는다. 따라서 일반적인 안전 분석 활동에 대한 검증 단계를 제시하는 IEC 61508 표준과의 조정이 필요하다.

본 논문에서 제시하는 시스템공학 프로세스의 안전 활동을 고려한 검증 단계를 개선한 프로세스의 세부 모델은 <그림 3>와 같다. 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.



<그림 3> 검증 단계가 개선된 시스템공학 프로세스의 상세 활동 및 인터페이스 정의

개선된 시스템공학 프로세스는 안전 요건 할당 후에 기능 분석을 행하는 단계부터 산출물을 정의하였다. 이는 기존 연구에서 상위 단계의 안전 요구사항과 하위 단계의 기능 분석 간의 추적성 확보가 부족한 부분을 정리하는데 도움을 줄 것이다. 총 18단계의 활동으로 수행이 되고 각 활동의 상세 설명은 다음과 같다.

4.2 개선된 시스템공학 프로세스의 검증 단계의 상세 활동

안전 요건 할당을 통해 기능 안전 요건이 도출이 되면 기능 안전 요건은 전체 안전 계획과 안전주기, 기타 기술과 외부 리스크 감소시설에 대한 기능 분석의 입력의 아이템으로서 적용된다. 먼저 전체 운영과 유지보수 계획, 전체 안전 확인 계획, 전체 설치와 가동 점검 계획을 세우게 된다. 이는 안전중시 시스템의 시스템 안전 프로세스에서 안전요소 분석 활동에 대한 기준선을 설정하는데 도움을 준다. 이러한 기준선 설정은 안전 요소 식별을 가능하게 해주며, 식별된 요소들의 속성을 명확하게 분류함으로써 정제된 안전 요구사항을 얻을 수 있다.

그 후 수명주기를 고려한 안전중시 시스템의 절차와 기타 기능 및 기술 등에 대하여 분석을 하고 외부 안전 위험에 대한 기기 및 장비 시설에 대한 분석을 수행하게 된다. <그림 3>의 1번에서 4번까지의 절차는 IEC 61508표준에서 제시한 시스템안전 프로세스의 일반적인 절차 중의 하나이다. 안전 기능 분석이 적용될 수 있는 모든 사물에 대하여 적용할 수 있도록 한 점이 특화되었다고 볼 수 있다. 이러한 전반적인 시설 및 기능에 대한 분석이 끝나게 되면, 데이터들의 통합을 위해 전반적인 검토를 하게 된다.

<그림 3>의 5번 이후부터의 프로세스 활동은 본 연구에서 제시하는 개선된 시스템공학 프로세스 활동 단계들을 표기하였다. 주로 검증 단계 활동들에 대하여 보완되었다. 기존의 시스템안전 프로세스에서는 점검 및 확인 단계를 통해 안전 활동을 검토하고 전반적인 안전 확인을 한 후에 운영, 유지, 보수 단계에서 오류가 발견되면 그때서야 다시 프로세스의 수명주기 상위 단계로 돌아가 검토하는 단계로 구성되어있다.

하지만 개선된 시스템공학 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.

전체 안전 확인 단계 후에 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.

앞서 시스템공학 프로세스의 검증 단계에서 인터페이스 및 안전 요소에 대하여 정의를 하였다. 이러한 정의된 아이템들을 토대로 시스템공학 프로세스의 검증 단계의 범위 및 기준선을 설정하는데 있어 요소 식별을 가능하게 해준다. 그리고 식별된 요소들의 속성을 명확하게 분류함으로써 정제된 인터페이스 및 안전 요소를 제시한다. 이를 시스템공학 프로세스의 검증 단계 개선을 위한 모델에서 제시하며, 최종적으로 활동을 마치게 된다.

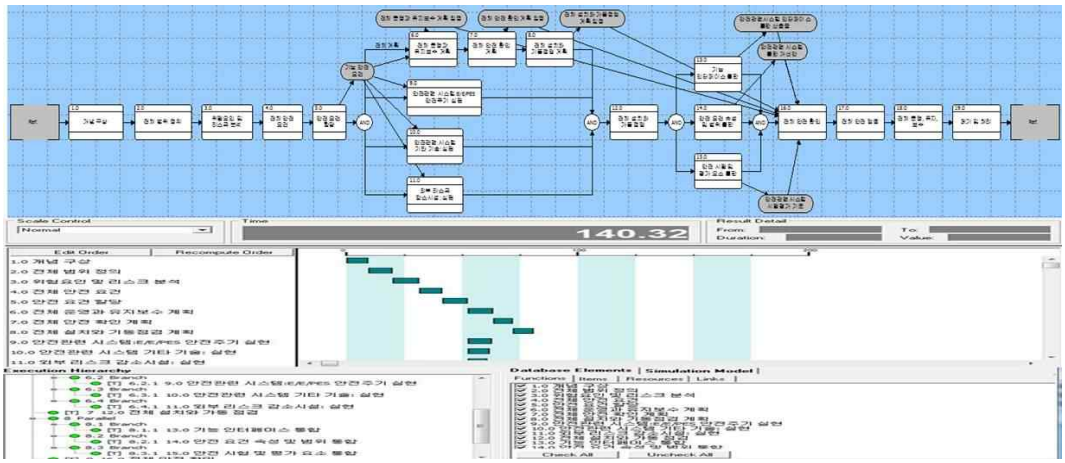
5. 개선된 시스템공학 프로세스 모델에 대한 검증

본 시스템공학 프로세스 모델은 시스템공학 프로세스를 중심으로 하여 구축되었으므로 기본적으로 시스템공학 표준을 충족시키고 있다. 본 시스템공학 프로세스 모델은 따라서 계층적으로 설계가 되어있으며, 요구사항 분석, 기능 분석, 시스템 설계를 수행하면서 안전 요소 분석 활동 및 시험 평가를 추가하였다. 이러한 시스템공학 프로세스 모델을 시스템공학 전산지원도구를 사용하여 수행할 수 있게 함으로써 산출물들의 추적성 관리 및 문서자동화 등의 이점을 가지게 된다.

5.1 전산 지원 도구를 통한 시뮬레이션

5.1.1 시뮬레이션 대상 및 범위

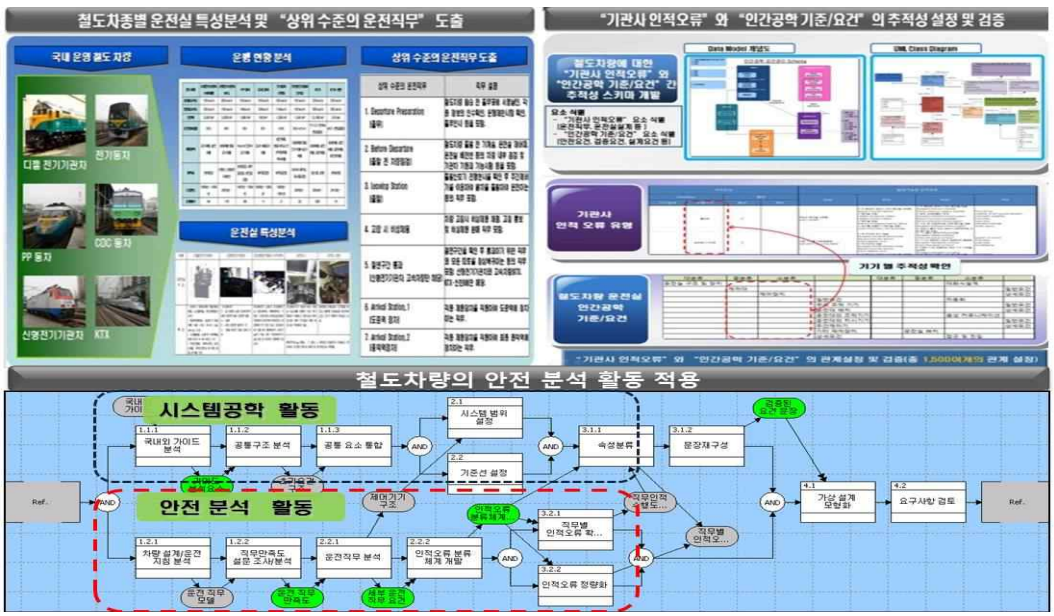
개선된 시스템공학 프로세스 모델이 실제 흐름에 충돌 없이 잘 수행되는지 파악하고, 각 프로세스 활동의 수행 시기가 서로 원하는 시기에 수행 되는지 전산지원도구를 통해 <그림 4>에서 확인하였다. 앞에서 언급한 시스템공학 전산지원 도구인 CORE® 을 통해 검증 가능한 모델링 기법인 EFFBD를 활용한 Time-Line analysis을 통해 시뮬레이션을 수행하였다.



<그림 4> 검증 단계가 개선된 시스템공학 프로세스의 시뮬레이션 검증

5.1.2 시뮬레이션 결과

시뮬레이션을 통해 잘못된 Trigger 데이터로 인한 잘못된 프로세스 수행 시기 등과 같은 프로세스 흐름에 관한 오류들을 확인하고 수정하였으며, 프로세스 조정으로 인한 변화 추이를 빠르게 확인하고 개선하였다. 분석 결과, 전체 흐름이 올바르게 수행되고 있음을 확인하였다. 특히 통합 및 검증 단계의 산출물과 후속 단계의 관계설정을 통해 각 단계의 인터페이스가 잘 정의되었음을 볼 수 있었다.



<그림 5> 개선된 시스템공학 프로세스를 토대로 철도차량 운전실 설계 시 검증 단계에 적용 사례

5.2 철도차량 시스템에 대한 적용 사례

5.2.1 대상시스템의 특징 및 범위

대표적인 안전 중시 시스템인 철도분야에서 철도차량 운전실 시스템의 기능안전을 파악하고 관리하여 열차 사고를 방지하는 시스템에 대하여 대상시스템을 정하였다.

신형전기기관차(NEL)는 비교적 최근(2003년)에 도입되어 최신의 운전실 제어기기 및 부분적으로 디지털 장비가 장착되어 있다. 하지만 디지털 시스템에 대한 사용성 평가 (Usability Test) 결과 새로운 시스템을 수시로 사용하면서도 필요이상으로 복잡하고 사용이 용이하지 않은 것으로 평가되었다. 이는 기관사의 운전직무에 대한 고려가 미흡한 상태에서 새로운 디지털 시스템을 장착함으로써, 기관사에게 혼란을 주고 있다는 것을 입증한다.

5.2.2 대상시스템의 적용 결과

시스템 설계에 있어 기관사 인적요인 및 활동에 따른 고려를 하지 않음에 따라 기관사의 실수 및 오류를 발생시켜 안전사고에 대한 위험성이 높아졌다고 볼 수 있다. 따라서 디지털 시스템의 효용을 극대화 및 철도차량 운전실의 안전 설계를 위해 본 논문에서 제시한 시스템공학 프로세스를 적용한 결과를 <그림 5>에 표시하였다.

이는 상위 수준의 운전직무와 관련된 기능들을 도출하여 이에 대한 특성과 현황 분석을 하게 된다. 이러한 분석이 끝나게 되면 실질적인 기능과 관련된 인적오류와 요구사항간의 관계를 설정한다. 관계 설정 사항을 토대로 모든 장비와의 추적성 연결을 통해 최종적으로 결과를 통합한다. 이 부분은 본 논문에서 말하는 인터페이스 정의를 토대로 진행된다. 이러한 통합된 결과를 바탕으로 기기의 기능별 사항이나 요건에 대하여 시험평가를 수행한다. 이러한 사항은 초기 설계 단계에서의 요구사항까지 고려하는 시스템공학적 방법에 대한 내용이 검증 단계 활동을 통해 기능 안전에 대한 요소들을 빠르게 확인할 수 있다.

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 시스템공학 프로세스의 검증 단계 개선을 위하여 안전 활동을 고려한 연구를 수행하였다. 시스템공학 프로세스의 검증 단계 개선을 위해 안전 요소 분석 활동과, 검증 단계의 상세활동을 정의하였다. 앞서 선행된 IEEE 1220표준과 IEC 61508표준을 기반으로 시스템공학 프로세스 검증 단계의 안전 관련 요소들을 식별하

고 이들 간의 관계를 파악하여 추적성을 확보한 기능 인터페이스를 정의하였다. 이를 통해 도출된 검증 단계가 개선된 시스템공학 프로세스를 시스템공학 전산 지원 도구를 통하여 논리적으로 검토하였다.

철도차량 운전실 시스템에 본 연구에서 제시하는 시스템공학 프로세스 모델을 적용하여 초기 안전 활동부터의 활동들을 효과적으로 검증할 수 있도록 함으로써 철도차량 운전실 시스템에 대한 기능 및 기기간의 관계를 성숙시켜 안전성을 높일 수 있었다.

구축된 시스템공학 프로세스는 안전 요구사항이 시스템 요구사항으로 구조화 될 수 있도록 하여, 검증 단계에서 보다 명확하게 검토하여 보완토록 하였다. 이는 안전중시 시스템에서 검증 단계에 시스템공학 기법을 활용함으로써 안전 관련 활동 및 안전사고 요소에 대한 예방을 개선하고, 안전의식 확대 및 안전중시 시스템의 신뢰성을 높일 수 있을 것이다.

6.1 향후 연구 방향

안전중시 시스템을 대상으로 여러 안전 전문가와 팀을 구성하여 상세 안전 요소 분석활동을 개발하고, 시스템 관점을 모델링을 해야 한다. 이를 통해 본 연구에서 주장하는 시스템공학 프로세스의 효용성과 타당성을 보이고, 더 나아가 안전중시 시스템을 위한 표준 및 기술 동향을 고려한 단기, 장기간의 발전계획을 수립하여야 한다.

7. 참 고 문 헌

[1] 최석중, 김문홍, 김병식, 변현진, "철도시스템의 안전성 검증제도 도입과 발전방향에 관한 연구", 한국철도학회 학술발표대회 논문집, 한국철도학회, pp. 393-398, 2012년 5월.

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

[3] 윤재한, 이재천, "안전중시 시스템을 위한 체계적인 설계 프로세스에 관한 연구", 대한안전경영과학회지, 대한안전경영과학회, 제11권 (3호), pp. 19-26, 2009년 9월.

[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 Eletronics Stability Control System," in Proc. KSAE 2010 Annual Conference and Exhibition, Daegu, Koera, Nov. 24, 2010, pp. 2124-2128.

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

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

[8] Processes for Engineering a System, Electronic Industries Alliance Standard, EIA-632-1998, 1999.
[9] Systems and Software Engineering - System Life Cycle Processes, ISO/IEC Standard, ISO/IEC 15288, 2008.
[10] 선박의 시스템안전에 관한 일반지침, [KMS 002:2010], 한국조선협회, 2010년, pp. 1-16.
[11] 박중용, "안전중시 시스템을 위한 동시공학적 설계 모델 (A Concurrent Design Model for Safety-critical Systems)", 학위논문(공학박사), 아주대학교, 시스템공학과, 수원, 2003년 8월.