한국철도학회논문집
제10권 제4호 2007년 ▌ pp. 438-443

철도 시스템 개발에서 시스템공학 프로세스와 안전성 평가를 동시에 고려한 통합 프로세스에 관한 연구

A Study on Integrated SE Process for the Development of the Railway Systems with Safety Assessment Included

윤재한† · 이재천* · 홍선호**
Jae-Han Yoon · Jae-Chon Lee · Seon-Ho Hong

Abstract

This paper proposes an integrated SE process for the development of railway systems with safety assessment included. Although the safety assessment process must be performed with SE process properly with good coordination, the interfaces between the two processes have not been clear. Thus, in many of safety critical system developments in Korea, it is difficult to assess safety in proper development phase. The process model proposed in this paper is based on both the concept of system life cycle and the repetitive use of SE process. In each of development phases, appropriate safety assessment methods are described. Also the evaluation of the integrated system incorporating safety factors is described. The resultant process model is expressed by the Enhanced Functional Flow Block Diagram (EFFBD) using a CASE tool. The model also allows timeline analysis for identifying activity flow and data flow, resulting in the effective management of process. In conclusion, the integrated process enable both the SE process and safety assessment process to cooperate with each other from early development phase throughout the whole system life cycle.

Keywords : SE Process, Safety Assessment Process, System Safety
시스템공학 프로세스, 안전성 평가 프로세스, 시스템 안전

1. 서 론

과거의 많은 시스템들은 개발 시 원하는 기능들을 구현하는 것에 대해 많은 노력을 기울였다면, 현대의 시스템들은 주변 환경, 외부 시스템, 사람 등에 미치는 영향들이 더욱 중요하게 고려되는 추세이다. 그 중에서도 사람들이 건강을 삶의 최우선으로 여김에 따라 시스템의 안전은 매우 중요한 문제가 되었으며, 안전성 확보 관련기술은 사회적으로 꼭 필요한 기술로 인식되고 있다.

시스템 안전성 확보 문제는 대형 공공 시스템, 군사 시스템, 민간 시스템 등 다양한 분야에서 제기되고 있으며, 최근에는 특히 교통 시스템과 관련하여 많은 관심이 집중되고 있다. 교통 시스템은 한 나라의 경제력에 영향을 미치는 물류 시스템의 근간이며, 일반 사람들이 주변에서 손쉽게 접하고 영향을 받는 범용적인 대형 복합 시스템이기 때문이다. 이 중에서도 철도 시스템은 가장 큰 지상 교통 시스템으로서, 개인뿐 아니라 나라에 까지 큰 영향을 끼치는 대표적인 안전 중시 시스템이다.

시스템 안전을 확보하기 위해서는 다양한 방법들이 존재하지만, 기본적으로는 시스템 초기부터 시스템의 위험원 (Hazard)를 식별하고 이에 대한 위험도를 평가하고 이를 경감시키는 활동이 가장 중요하다. 이러한 활동은 시스템 생명주기 전 단계에 걸쳐서 수행되어야 하며, 전 단계에 걸쳐 수행되는 시스템공학 활동에 따른 시스템 개념 및 아키텍처를 근간으로 시스템의 안전성을 관리해야 한다. 이는 시스템공학 프로세스를 기반으로 시스템 안전성 평가 프로세스를 수행해야 함을 의미한다[1].

철도 시스템 개발에서도 시스템의 안전성을 확보하기 위

† 책임저자 : 정회원, 아주대학교, 시스템공학과
E-mail : gleepeace@nate.com
TEL : (031)330-7661 FAX : (031)330-7119
* 아주대학교, 시스템공학과
** 한국철도기술연구원, 철도종합안전기술개발사업단 안전SE팀

해 시스템공학을 통한 체계적인 시스템 개발 프로세스를 수행해야 함은 물론, 이를 기반으로 시스템의 안전성을 각 수명주기 단계마다 평가해야 한다. 이를 위하여 철도 시스템의 생명주기 상에서 수행되는 시스템공학 프로세스를 정의하고 이와 함께 수행되는 시스템 안전성 평가 프로세스를 정의해야 한다. 그리고 상호간의 인터페이스를 명확히 정의하고 시간 흐름에 따라 시스템공학 프로세스와 안전성 평가 프로세스가 어떠한 활동을 하는지 그리고 어떠한 데이터를 주고받는지 명시해야 한다. 그러나 각각에 대해 잘 설명된 자료는 있지만, 인터페이스를 명확히 제시하는 자료가 부족한 실정이다.

본 연구에서는 철도 시스템과 같이 국가 교통 시스템 중 하나인 항공 시스템에서 적용되는 프로세스들을 통해 철도 시스템 개발을 위한 시스템공학 및 안전성 평가 프로세스를 제안한다. 이를 위하여, 미국 항공 시스템의 개념 단계부터 상세설계 단계까지의 시스템공학 프로세스를 기반으로 시스템의 안전성을 확보하기 위한 안전성 평가 프로세스를 분석하였다. 이를 통하여 생명주기에 따른 시스템공학 프로세스와 안전성 평가 프로세스의 활동을 정의하고, 시간 흐름에 따라 어떻게 동시에 수행되는지 표현하였다. 또한 시스템의 점진적인 개발 양상을 고려하여 반복적인 시스템공학 프로세스를 정의하였으며, 시스템공학 프로세스와 안전성 평가 프로세스간의 입출력 데이터를 정의하였다. 이러한 모든 내용을 EFFBD (Enhanced Functional Flow Block Diagram)을 통한 그래픽 모델로 작성하였으며, 철도 시스템 개발 프로세스 모델로 제안한다.

본 논문에서는 서론에 이어 제 2장에서는 제안하는 프로세스의 개념, 제 3장에서는 제안하는 프로세스의 개발 방법, 제 4장에서는 제안하는 프로세스의 모델링 결과에 대해 기술한다. 마지막으로 제 5장에서는 본 연구의 결론을 통해 논문을 마무리한다.

2. 통합 프로세스의 제안

2.1 통합 프로세스의 정의

본 논문에서 제안하는 프로세스는 시스템공학 프로세스와 안전성 평가 프로세스를 점진적인 개발을 고려하여 시스템 수명주기에 맞춰서 하나의 모델로 통합된 프로세스이다. 하나로 통합했단 의미는 철도 시스템 생명주기에 따라 시스템공학 프로세스를 통해 시스템이 개발될 때 안전성 평가 프로세스는 이와 동시에 어떻게 수행되며 두 프로세스 사이의 입출력 데이터를 명시한 것을 말한다.

2.2 통합 프로세스의 목적

시스템공학에서는 일반적으로 요구사항 분석, 기능 분석, 조합 등을 핵심 프로세스로 구성한다. 그리고 안전성 평가 프로세스의 경우, 특수 공학 (Specialty Engineering)으로 분류하고 시스템공학 프로세스와 동시에 수행하면서 시스템의 안전성을 평가한다[2]. 이는 시스템의 개념 단계서부터 시스템의 안전성을 평가해야 하며 그 단계에 적합한 방법으로 분석해야 함을 나타낸다. 이는 서론에 제시한 시스템 안전성 확보의 기본 개념과 같은 개념이다. 그럼에도 불구하고 시스템 수명주기의 각 개발 단계에 따라 두 프로세스가 어떠한 활동을 하고 어떤 데이터를 주고받는지 명시하는 자료가 없다. 각각을 설명하는 자료는 있지만 시스템공학 프로세스에서 어떠한 데이터를 안전성 평가 프로세스에서 쓰이는 지 정확히 규정지은 자료는 없다. 제안하는 프로세스는 시스템공학 프로세스와 안전성 평가 프로세스를 하나로 통합하여 철도 시스템 개발에서 수명주기 각 단계마다 시스템의 안전성을 확보할 수 있도록 한다. 또한 제안하는 프로세스를 그래픽 모델로 나타냄으로써 둘 사이의 인터페이스를 직관적으로 이해할 수 있도록 한다.

3. 통합 프로세스의 개발 방법

3.1 프로세스 개발 절차

우선, 프로세스가 수행되는 철도 시스템의 수명주기를 분석하여 각 시스템 개발 단계를 정의하였다. 이후, 시스템공학 프로세스와 안전성 평가 프로세스의 활동을 식별하고 시간 흐름에 따라 프로세스 각각을 모델링 하였다. 마지막으로 모델링된 각각의 프로세스를 서로 주고받는 데이터를 식별함으로써 서로의 인터페이스를 식별하여 통합하였다. 이 때, 시스템의 각 수명주기 별로 먼저 크게 모델링하고, 이후 각 시스템 레벨별로 반복적으로 수행되는 시스템공학 프로세스를 기준으로 반복적인 시스템 개발 양상을 모델링하였다. 이를 그림으로 표현하면 그림 1과 같다.

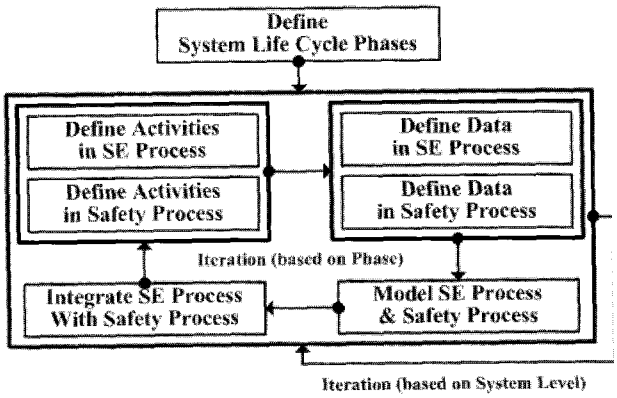

그림 1. 프로세스 개발 절차

3.2 프로세스 모델의 구성

프로세스 모델은 그림 2와 같이 크게 3 수준으로 구성된다. 제일 상위 수준은 프로세스를 시스템 수명주기 관점에서 바라보는 것이다. 시스템의 수명주기는 시스템의 개선 등으로 인해 순환될 수 있으므로, 최상위는 수명주기 순환을 고려하여 표현하였다. 두 번째 수준은 각 시스템 수명주기 단계 별로 수행되는 시스템공학 프로세스와 안전성 평가 프로세스를 나타내었다. 세 번째 수준은 시스템공학 프로세스와 안전성 평가 프로세스를 수행하기 위한 세부 활동 및 분석 기법을 나타내었다. 세 번째 수준 하위로는 좀 더 상세한 내용이 작성되어 있으며, 이런 모든 내용은 전산 지원 도구를 통해 EFFBD로 구축하였다.

3.3 프로세스 모델의 특징

그래픽 모델 활용으로 각각의 프로세스에 대한 이해를 증진시켰으며, 전산 지원 도구의 도움으로 프로세스의 내용을 효율적으로 접근 및 관리할 수 있게 하였다. 또한 제안하는 프로세스가 원하는 흐름대로 활동과 데이터가 흘러가는지 시간선 분석 (Timeline Analysis)를 통한 시뮬레이션이 가능하다. 이로 인해 프로세스 적용을 위한 프로세스의 조정 (Tailoring)이 용이하며, 조정된 프로세스에 대해 적용 전 비용 및 기간을 분석할 수 있다.

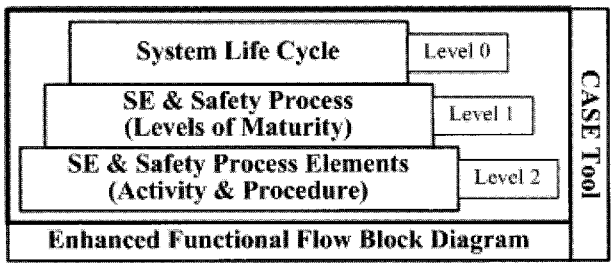

그림 2. 프로세스 모델의 구성

4. 통합 프로세스 모델

4.1 프로세스의 0 수준 모델: 수명주기

국내외에서 철도 시스템의 수명주기는 아직 정확히 정의된 바 없다. 본 연구에서는 철도 시스템이 국가 교통 시스템이므로 미국 항공 시스템의 수명주기를 바탕으로 수명주기를 정의하였다. 미국 항공 시스템의 수명주기는 다섯 단계로 구성되며, 각 단계는 다시 세부 단계로 나누어진다; 다섯 단계는 임무 분석, 투자 분석, 해결책 구현, 서비스 제공, 그리고 폐기이다[3]. 다섯 단계를 그림 3과 같이 모델링 하였다. 각 단계를 하나의 기능으로 표현하고 하나의 단계에서 다음 단계로 넘어가는데 이용되는 데이터를 표현하였다.

표 1. 각 수명주기 단계 마다 수행되는 안전성 평가

System Life Cycle	Safety Assessment Process
Mission Analysis	Develop Safety Plan
	Operational Safety Assessment
	Test Safety Assessment
Investment Analysis	Comparative Safety Assessment
	Program Safety Plans
	Preliminary Hazard Analysis
	Hazard Tracking and Risk Resolution
Solution Implementation	Sub-System Hazard Analysis
	System Hazard Analysis
	Operational & Support Hazard Analysis
	Health Hazard Analysis
	Hazard Tracking and Risk Resolution
	System Hazard Assessment Report
	System Safety Program Plan
	Safety Action Record
In-Service Management	Provide Status Reports

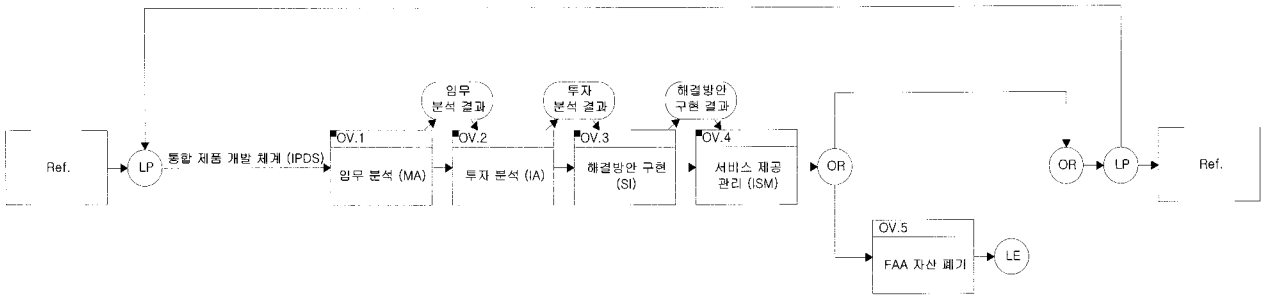

그림 3. 수명 주기 모델

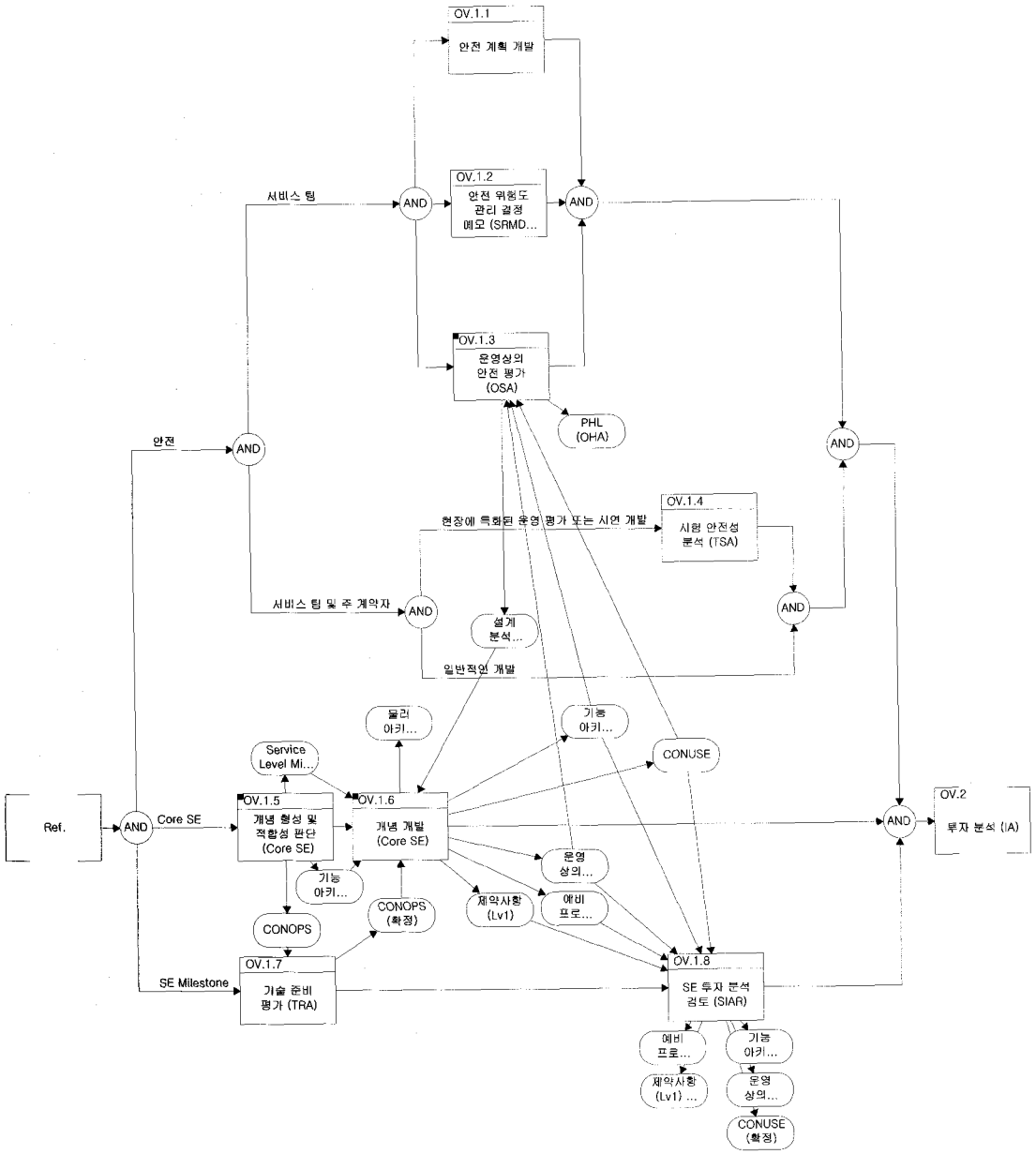

그림 4. 임무 분석 단계의 모델

4.2 프로세스의 1 수준 모델: 시스템 성숙도

프로세스를 표현함에 있어 시스템공학 프로세스의 반복 수행을 나타내기 위해, 시스템의 성숙 9 단계를 고려하였다: 개념 형석, 개념 적합성 평가, 개념 개발, 저-사실성 모델링, 고-사실성 모델링, 표본 시스템, 제품 성숙, 제품 승인, 그리고 서비스 제공[4].

시스템이 성숙함에 따라 각 단계 사이에 시스템 개발에 대한 검토 시점이 존재한다. 이러한 검토 시점에는 대표적으로 하위 13개가 존재한다[5]. 각 검토 시점을 표현함으로써, 시스템공학 프로세스와 안전성 평가 프로세스의 수행 시점을 동기화하였다.

CDR - Critical Design Review
FBR - Functional Baseline Review
FCA - Formal Configuration Audit
IARR - Investment Analysis Readiness Review
IBR - Integrated Baseline Review
ISPR - In Service Performance Review

PCA - Physical Configuration Audit
PDR - Preliminary Design Review
SIAR - SE Investment Analysis Review
SIR - Screening Information Request
SRR - System Requirements Review
TRA - Technology readiness Review
VRR - Verification Readiness Review

시스템공학에서는 요구사항 분석, 기능 분석, 합성, 검증 등의 여러 프로세스들이 존재한다. 이 중 요구사항 분석, 기능 분석, 합성을 핵심 프로세스로 분류하며[6], 본 연구에서는 핵심 프로세스만을 고려하여 프로세스를 정의하였다. 안전성 평가 프로세스의 경우는 시스템 수명주기에 따라 표 1과 같이 존재한다[7].

시스템공학 프로세스, 안전성 평가 프로세스, 시스템공학 마일스톤, 그리고 시스템 성숙 단계를 고려하여 그림 4와 같은 모델을 작성하였다. 각 성숙 단계들은 시스템공학 마일스톤으로 수행 시기가 분류 가능 하므로, 모델에서도 성숙 단계의 끝에 해당 마일스톤의 내용이 수행되도록 trigger 데이터를 이용하여 연관성을 표현하였다.

4.3 프로세스의 2 수준 모델: 프로세스 활동

반복적인 시스템공학 프로세스에 대한 안전성 평가 프로세스를 나타낸 모델의 하위에는 시스템공학 프로세스와 안전성 평가 프로세스의 세부 활동들에 대해 표현하였다. 이 수준에서 시스템공학의 구성요소들이 각 반복 단계마다 어떠한 입출력 데이터가 있는지 나타나며, 안전성 평가의 경우에도 실제 분석 기법들에 대한 데이터들이 식별된다. 시스템공학 프로세스의 모델은 그림 5, 안전성 평가 프로세스의 모델은 그림 6과 같다.

4.4 프로세스의 전체 활동 통합 모델:

정의된 프로세스가 수행되기 위한 활동들을 모두 하나의 모델로 다시 통합하였다. 앞에서 나타낸 모델들은 수준별로 프로세스 활동을 묶어서 계층적인 모델이라면, 이번 모델은 계층에서 가장 하부에 표현되어 있는 EFFBD 블록의 통합본이다. 이는 실제 수행해야 되는 활동들을 직관적으로 볼 수 있도록 하며, 실제 데이터의 사용을 명시한다. 구축된 모델은 다음 그림 7과 같다.

4.5 프로세스에 대한 시간선 분석

정의된 프로세스가 실제 흐름의 상충 없이 잘 수행되는지 파악하고, 각 프로세스 활동의 수행 시기가 서로 원하는 시기

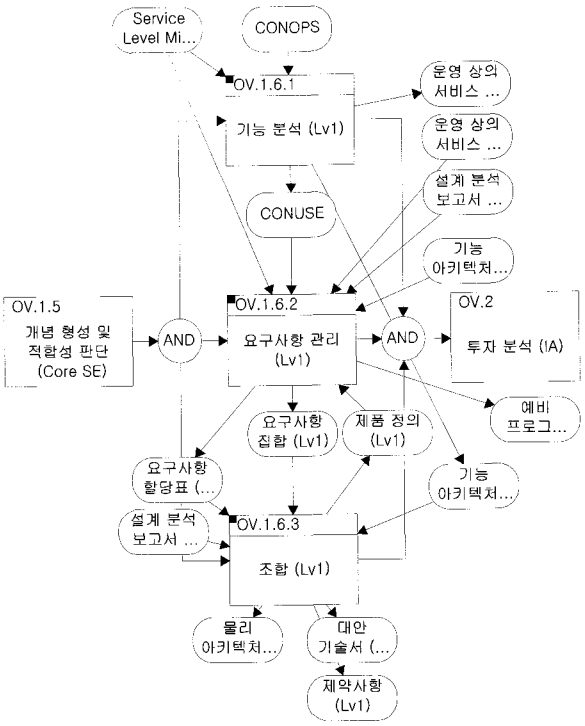

그림 5. 개념 형성 및 적합성 판단 수준의 모델

에 수행이 되는지 시간선 분석을 통해 확인하였다. 이를 통하여 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 바르게 수행되고 있음을 그림 8을 통해 확인하였다.

5. 결 론

시스템공학 프로세스와 안전성 평가 프로세스의 인터페이스를 파악하고 두 프로세스를 통합한 프로세스를 제안하고 모델링하였다. 프로세스의 모델을 통해 두 프로세스 간의 입출력 데이터를 확인하고 서로의 수행 시기를 확인하였으며, 시뮬레이션을 통해 프로세스 모델이 의도한 바대로 구축되었는지 확인하였다.

제안하는 프로세스를 통해, 철도 시스템 개발에서 생명주기 초반의 시스템 안전성 평가에 대한 수행 방법을 제시하였다. 또한 프로세스 모델을 통해 프로세스의 조정과 조정된 프로세스의 검증에 대한 편의를 도모하였다.

현재까지는 시스템 수명주기 중 시스템 상위 설계단계까지 프로세스가 자세히 정의되어 있으나, 향후에는 실제 시스템 구현 및 운영 단계에서의 안전성 평가의 내용을 보충할 필요가 있다. 또한 모델에서 표현된 시스템공학 핵심 프로세스만

으로는 안전성 평가 프로세스와의 연계가 부족하므로, 모델에서 제외된 검증 및 확인 프로세스나 형상 관리 프로세스 등을 통해 모델이 보완되어야 할 것이다.

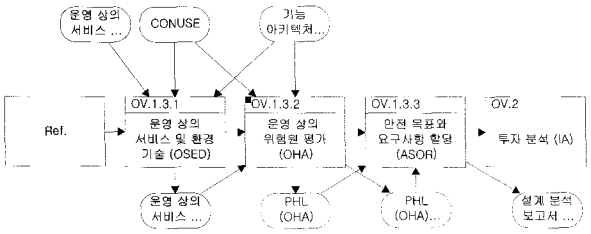

그림 6. 운영상의 안전성 평가 모델

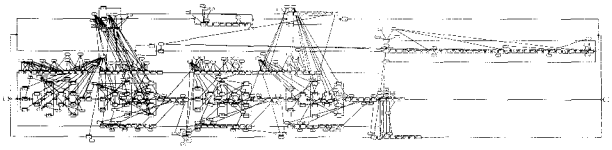

그림 7. 전체 활동 통합 모델

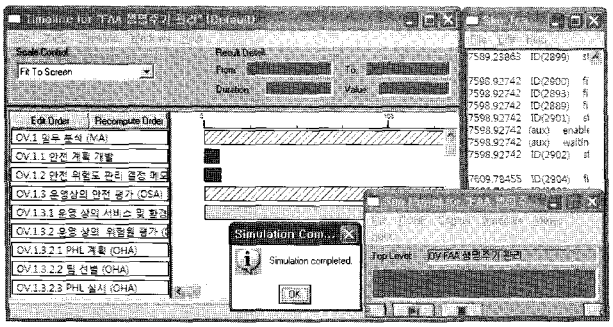

그림 8. 통합 프로세스에 대한 시간선 분석

참 고 문 헌

1. Clifton A. Ericson, II, (2005), "Hazard Analysis Techniques for System Safety", John Wiley & Sons, INC., p.1-94.
2. Cecilia Haskins, (2006), "Systems Engineering Handbook", INCOSE, p.(9.13 of 16)
3. The Federal Aviation Administration (FAA), System Engineering Manual Version 3.1, FAA, p.(3-1), 2006.
4. The Federal Aviation Administration (FAA), System Engineering Manual Version 3.1, FAA, p.(4.2-31), 2006.
5. The Federal Aviation Administration (FAA), System Engineering Manual Version 3.1, FAA, p.(4.2-22), 2006.
6. The Federal Aviation Administration (FAA), System Engineering Manual Version 3.1, FAA, p.(1-2), 2006.
7. The Federal Aviation Administration (FAA), Safety Risk Management Guidance For System Acquisitions Version 1.4, FAA, p.34, 2006.

(2007년 7월 12일 논문접수, 2007년 8월 22일 심사완료)